

Brottsdatalag – kompletterande lagstiftning

*Slutbetänkande av Utredningen om
2016 års dataskyddsdirektiv*

Stockholm 2017



STATENS OFFENTLIGA
UTREDNINGAR

SOU 2017:74

SOU och Ds kan köpas från Wolters Kluwers kundservice.
Beställningsadress: Wolters Kluwers kundservice, 106 47 Stockholm
Ordertelefon: 08-598 191 90
E-post: kundservice@wolterskluwer.se
Webbplats: wolterskluwer.se/offentligapublikationer

För remissutsändningar av SOU och Ds svarar Wolters Kluwer Sverige AB
på uppdrag av Regeringskansliets förvaltningsavdelning.

Svara på remiss – hur och varför

Statsrådsberedningen, SB PM 2003:2 (reviderad 2009-05-02).

En kort handledning för dem som ska svara på remiss.

Häftet är gratis och kan laddas ner som pdf från eller beställas på regeringen.se/remisser

Layout: Kommittéservice, Regeringskansliet

Omslag: Elanders Sverige AB

Tryck: Elanders Sverige AB, Stockholm 2017

ISBN 978-91-38-24675-7

ISSN 0375-250X

Till statsrådet och chefen för Justitiedepartementet

Den 17 mars 2016 bemyndigade regeringen statsrådet Ygeman att tillkalla en särskild utredare med uppdrag att föreslå hur EU:s direktiv om skydd av personuppgifter vid brottsbekämpning, brottmålshantering och straffverkställighet ska genomföras i svensk rätt. Regeringen beslutade samtidigt om direktiv för utredningen (dir. 2016:21).

Till särskild utredare förordnades från och med den 1 april 2016 numera f.d. överåklagaren Gunnel Lindberg.

Utredningen har antagit namnet Utredningen om 2016 års data-skyddsdirektiv (Ju 2016:06).

Till sakkunniga förordnades från och med den 1 april 2016 rättssakkunniga vid Justitiedepartementet Anna Westin och kansli-rådet vid Finansdepartementet Leena Mildemberger. Till experter utsågs juristen vid Datainspektionen Cecilia Agnehall, verksjuristen vid Ekobrottsmyndigheten Eva Bergholm Guhnby, personupp-giftsombudet, tillika verksjuristen, vid Säkerhetspolisen Fredrik Berglund, verksjuristen vid Tullverket Pernilla Jäderberg, verksju-risten vid Polismyndigheten David Kummel, advokaten Conny Larsson, sektionschefen vid Kriminalvården Eric Leijonram, senio-ra föredraganden vid Säkerhets- och integritetsskyddsnämnden Lisa Lundin, it-utvecklingschefen vid Åklagarmyndigheten Stephan Uttersköld, dåvarande juristen vid Domstolsverket Jonna Wiborn, verksjuristen vid Kustbevakningen Peter Åkesson och rättsliga experten vid Skatteverket Maria Östgren.

Jonna Wiborn entledigades från sitt uppdrag den 31 augusti 2016 och bitr. enhetschefen Amanda Rörby utsågs i hennes ställe. Amanda Rörby entledigades från sitt uppdrag den 3 april 2017 och chefsjuristen Charlotte Driving utsågs i hennes ställe. Lisa Lundin

entledigades från sitt uppdrag den 22 oktober 2016 och seniore föredraganden Fabian Holgersson utsågs i hennes ställe. Maria Östgren entledigades från sitt uppdrag den 23 augusti 2017 och Cecilia Agnehall den 4 september 2017.

Ämnesrådet vid Justitiedepartementet Sofie Lindblom har varit huvudsekreterare i utredningen från och med den 1 april 2016. Sekreterare i utredningen har varit verksjuristen Malin Lundberg från och med den 1 april 2016, hovrättsassessorerna Karin Månsson och Anja Nordfeldt från och med den 1 maj 2016, hovrättsassessorn Karin Brandqvist Sundblad från och med den 16 maj 2016 och hovrättsassessorn Maria Arnell från och med den 1 september 2016.

Utredningen överlämnade den 5 april 2017 betänkandet Brottsdatalag, SOU 2017:29.

Utredningen överlämnar härmed betänkandet Brottsdatalag – kompletterande lagstiftning (2017:74). De sakkunniga och experterna har i huvudsak ställt sig bakom utredningens överväganden och förslag. Uppdraget är härmed slutfört.

Stockholm i oktober 2017

Gunnel Lindberg

*/ Sofie Lindblom
Maria Arnell
Karin Brandqvist Sundblad
Malin Lundberg
Karin Månsson
Anja Nordfeldt*

Innehåll

Sammanfattning	23
1 Författningsförslag.....	33
1.1 Förslag till Säkerhetspolisens datalag (2018:000)	33
1.2 Förslag till domstolarnas brottsdatalag (2018:000)	61
1.3 Förslag till lag om ändring i rättegångsbalken	67
1.4 Förslag till lag om ändring i polislagen (1984:387).....	69
1.5 Förslag till lag om ändring i säkerhetsskyddslagen (1996:627).....	70
1.6 Förslag till lag om ändring i lagen (1996:701) om Tullverkets befogenheter vid Sveriges gräns mot ett annat land inom Europeiska unionen	71
1.7 Förslag till lag om ändring i lagen (1998:620) om belastningsregister	72
1.8 Förslag till lag om ändring i lagen (1998:621) om misstankeregister	73
1.9 Förslag till lag om ändring i lagen (2000:344) om Schengens informationssystem.....	74
1.10 Förslag till lag om ändring i lagen (2001:184) om behandling av personuppgifter i Kronofogdemyndighetens verksamhet	75
1.11 Förslag till lag om ändring i lagen (2001:185) om behandling av uppgifter i Tullverkets verksamhet	76

1.12	Förslag till lag om ändring i lagen (2001:617) om behandling av personuppgifter inom kriminalvården	78
1.13	Förslag till lag om ändring i lagen (2005:321) om tillträdesförbud vid idrottsarrangemang	84
1.14	Förslag till lag om ändring i lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet	85
1.15	Förslag till lag om ändring i offentlighets- och sekretesslagen (2009:400)	87
1.16	Förslag till lag om ändring i polisdatalagen (2010:361)	93
1.17	Förslag till lag om ändring i kustbevakningsdatalagen (2012:145)	121
1.18	Förslag till lag om ändring i lagen (2014:400) om Polismyndighetens elimineringsdatabas	133
1.19	Förslag till lag om ändring i lagen (2015:51) om register över tillträdesförbud vid idrottsarrangemang	137
1.20	Förslag till lag om ändring i åklagardatalagen (2015:433)	141
1.21	Förslag till lag om ändring i utlänningsdatalagen (2016:27)	150
1.22	Förslag till lag om ändring i tullagen (2016:253)	151
1.23	Förslag till lag om ändring i tullbrottsdatalagen (2017:447)	152
1.24	Förslag till lag om ändring i skattebrottsdatalagen (2017:452)	170
1.25	Förslag till lag om ändring i lagen (2017:496) om internationellt polisiärt samarbete	184
1.26	Förslag till lag om ändring i brottsdatalagen (2018:000) ...	189
1.27	Förslag till Säkerhetspolisens dataförordning (2018:000)	193
1.28	Förslag till domstolarnas brottsdataförordning (2018:000)	204

1.29	Förslag till förordning (2018:000) om underrättelseskyldighet för Kriminalvården	207
1.30	Förslag till förordning om ändring i förordningen (1970:517) om rättsväsendets informationssystem	211
1.31	Förslag till förordning om ändring i förordningen (1977:937) om allmänna förvaltningsdomstolars behörighet m.m.....	212
1.32	Förslag till förordning om ändring i folkbokföringsförordningen (1991:749)	213
1.33	Förslag till förordning om ändring i förordningen (1995:238) om totalförsvarsplikt	214
1.34	Förslag till förordning om ändring i förordningen (1995:1301) om handläggning av skadeståndsanspråk mot staten.....	215
1.35	Förslag till förordning om ändring i vapenförordningen (1996:70)	217
1.36	Förslag till förordning om ändring i förordningen (2001:682) om behandling av personuppgifter inom kriminalvården.....	218
1.37	Förslag till förordning om ändring i förordningen (2005:323) om tillträdesförbud vid idrottsarrangemang	241
1.38	Förslag till förordning om ändring i förordningen (2007:1141) med instruktion för Säkerhets- och integritetsskyddsmyndigheten	243
1.39	Förslag till förordning om ändring i offentlighets- och sekretessförordningen (2009:641)	245
1.40	Förslag till förordning om ändring i polisdataförordningen (2010:1155)	250
1.41	Förslag till förordning om ändring i kustbevakningsdataförordningen (2012:146)	261
1.42	Förslag till förordning om ändring i förordningen (2014:405) om Polismyndighetens elimineringsdatabas	267

1.43	Förslag till förordning om ändring i förordningen (2014:1103) med instruktion för Säkerhetspolisen	268
1.44	Förslag till förordning om ändring i förordningen (2015:54) om register över tillträdesförbud vid idrottsarrangemang.....	269
1.45	Förslag till förordning om ändring i förordningen (2015:476) om behandling av personuppgifter i Nationellt forensiskt centrums uppdragsverksamhet	270
1.46	Förslag till förordning om ändring i åklagardataförordningen (2015:575)	271
1.47	Förslag till förordning om ändring i tullbrottsdataförordningen (2017:450)	275
1.48	Förslag till förordning om ändring i skattebrottsdataförordningen (2017:458).....	282
1.49	Förslag till förordning om ändring i förordningen (2017:504) om internationellt polisiärt samarbete	288
1.50	Förslag till förordning om ändring i brottsdataförordningen (2018:000).....	294
2	Utredningens uppdrag och arbete	295
2.1	Utredningsuppdraget	295
2.2	Genomförandet av uppdraget.....	296
3	Brottsdatalagens innehåll	299
3.1	Ny reglering av dataskyddet	299
3.1.1	Dataskyddsreformen.....	299
3.1.2	Genomförandet av dataskyddsdirektivet.....	300
3.2	Innehållet i brottsdatalagen	301
3.2.1	Regler om behandlingen av personuppgifter.....	301
3.2.2	Personuppgiftsansvarigas skyldigheter	305
3.2.3	Enskildas rättigheter	308
3.2.4	Tillsyn	309
3.2.5	Sanktioner, skadestånd och rättsmedel.....	312

3.2.6	Överföring av personuppgifter till tredjeland och internationella organisationer	314
3.2.7	Ikraftträdande och övergångsbestämmelser	316
4	Framtida utformning av registerförfattningarna	317
4.1	Utgångspunkter	317
4.2	Det krävs anpassningar till den nya dataskyddsregleringen	318
4.3	Merparten av bestämmelserna är förenliga med dataskyddsdirektivet	319
4.4	Lagarnas tillämpningsområden	320
4.4.1	Tillämpningsområdet ska regleras	320
4.4.2	Vad innebär det ändrade tillämpningsområdet?	323
4.5	Ska registerförfattningarna reglera frågor som inte rör dataskydd?	324
5	Generella ändringar	327
5.1	Registerförfattningarna har likartat innehåll	327
5.2	En ny lagteknisk struktur	328
5.3	Bestämmelser som inte längre behövs	329
5.3.1	Hänvisningar till personuppgiftslagen	329
5.3.2	Hänvisningar till 2013 års lag	332
5.3.3	Syftet med lagarna	332
5.3.4	Automatiserad behandling	333
5.3.5	Bestämmelser om lagarnas uppbyggnad	334
5.3.6	Personuppgiftsombud	335
5.3.7	Behandling för diarieföring	335
5.3.8	Behandling av känsliga personuppgifter	336
5.3.9	Tillgången till personuppgifter	339
5.3.10	Särskilda upplysningar	341
5.3.11	Längsta tid för behandling	346
5.3.12	Upplysning om regleringen i offentlighets- och sekretesslagen	347

5.4	Behov av nya bestämmelser och anpassningar.....	348
5.4.1	Uppgifter om juridiska personer.....	348
5.4.2	Administrativa sanktionsavgifter	349
5.4.3	Skadestånd	352
5.4.4	Överklagande	353
5.4.5	Uppgifter till rättsstatistiken.....	354
5.4.6	Terminologin anpassas.....	355
5.5	Särskilt om längsta tid för behandling.....	356
5.5.1	Regleringen samlas	356
5.5.2	Bestämmelser om längsta tid för behandling oavsett ändamål	359
5.5.3	Bestämmelser om längsta tid för behandling för ändamål inom tillämpningsområdet.....	363
5.5.4	Omständigheter som påverkar längsta tid för behandling i underrättelseverksamhet	365
5.6	Särskilt om elektroniskt utlämnande.....	366
5.6.1	Olika former av elektroniskt utlämnande	366
5.6.2	Behovet av att kommunicera elektroniskt.....	367
5.6.3	Utlämnande genom direktåtkomst	370
5.6.4	Annat elektroniskt utlämnande tillåts i större utsträckning.....	371
5.7	Frågor om föreskriftsrätt m.m.	376
6	Tillåtna rättsliga grunder och behandling för nya ändamål.....	379
6.1	Ändamål eller tillåtna rättsliga grunder?	379
6.1.1	Dagens ändamålsbestämmelser	379
6.1.2	Bestämmelser om rättslig grund.....	381
6.1.3	Primära och sekundära ändamålsbestämmelser är bestämmelser om rättslig grund.....	383
6.2	Ny utgångspunkt i brottsdatalagen	386
6.3	Behandling för ändamål inom brottsdatalagens tillämpningsområde	387
6.3.1	Tillåtna rättsliga grunder för behandling	387
6.3.2	Behandling för nya ändamål	390

6.4	Behandling för ändamål utanför brottsdatalagens tillämpningsområde	394
6.4.1	Tillämpningen av dataskyddsförordningen.....	394
6.4.2	En prövning ska göras innan personuppgifter lämnas ut	397
6.4.3	Utförningen av regleringen	400
6.5	Uppgiftsskyldighet ersätter prövningen.....	404
7	Polisdatalagen	407
7.1	Polisdatalagen behöver anpassas	407
7.1.1	Nuvarande reglering	407
7.1.2	Polisdatalagen ges ett nytt namn	408
7.2	Allmänna bestämmelser.....	409
7.2.1	Tillämpningsområdet	409
7.2.2	Personuppgiftsansvar	416
7.2.3	En bestämmelse om hur lagen är uppbyggd	418
7.3	Grundläggande bestämmelser om behandling	418
7.3.1	Tillåtna rättsliga grunder och behandling för nya ändamål.....	418
7.3.2	Behandling av biometriska och genetiska uppgifter.....	420
7.3.3	Sökning på känsliga personuppgifter	423
7.4	Personuppgifter från transportföretag	427
7.4.1	Personuppgiftsbehandlingen bör regleras i polisens brottsdatalag.....	427
7.4.2	Begränsningar i möjligheterna att behandla personuppgifter	430
7.4.3	Uppgifter från transportföretag får göras gemensamt tillgängliga.....	432
7.4.4	Hur länge personuppgifterna får behandlas.....	433
7.5	Gemensamt tillgängliga uppgifter.....	434
7.5.1	Nya kategorier av personuppgifter får göras gemensamt tillgängliga.....	434
7.5.2	Sökning i gemensamt tillgängliga uppgifter.....	436
7.6	Längsta tid för behandling.....	441

7.7	Personuppgiftsbehandling i särskilda register	442
7.7.1	Dna-register.....	442
7.7.2	Fingeravtrycks- och signalementsregister	442
7.8	Personuppgiftsbehandling för forensiska ändamål	443
7.8.1	Vad är forensiska ändamål?	443
7.8.2	Regleringen av forensiska ändamål behålls.....	444
7.8.3	Behandling för nya ändamål	445
7.8.4	Behandling av känsliga personuppgifter	447
8	Tullbrottsdatalagen	451
8.1	Tullbrottsdatalagen behöver anpassas	451
8.1.1	Nuvarande reglering.....	451
8.1.2	Tullbrottsdatalagen ges ett nytt namn.....	451
8.2	Tillämpningsområdet	452
8.3	Grundläggande bestämmelser om behandling.....	453
8.3.1	Tillåtna rättsliga grunder och behandling för nya ändamål	453
8.3.2	Behandling av biometriska och genetiska uppgifter	455
8.3.3	Sökning på känsliga personuppgifter	456
8.4	Personuppgifter från transportföretag.....	460
8.4.1	Reglerna om personuppgiftsbehandling samlas ..	460
8.4.2	En i huvudsak oförändrad reglering.....	464
8.5	Gemensamt tillgängliga uppgifter	467
8.5.1	Sökning i gemensamt tillgängliga uppgifter	467
8.5.2	Uppgifter från transportföretag får göras gemensamt tillgängliga.....	469
8.6	Längsta tid för behandling	470
8.7	Övergångsbestämmelser till tullbrottsdatalagen	471
9	Kustbevakningsdatalagen	473
9.1	Kustbevakningsdatalagen behöver anpassas	473
9.1.1	Nuvarande reglering.....	473
9.1.2	Kustbevakningsdatalagen delas upp.....	473

9.2	Tillämpningsområdet.....	475
9.3	Grundläggande bestämmelser om behandling	478
9.3.1	Tillåtna rättsliga grunder och behandling för nya ändamål.....	478
9.3.2	Behandling av biometriska och genetiska uppgifter.....	480
9.3.3	Sökning på känsliga personuppgifter	481
9.4	Gemensamt tillgängliga uppgifter.....	484
9.4.1	Behandling för diarieföring ska undantas	484
9.4.2	En ny kategori av personuppgifter får göras gemensamt tillgängliga.....	484
9.4.3	Sökning i gemensamt tillgängliga uppgifter.....	485
10	Skattebrottsdatalagen	489
10.1	Skattebrottsdatalagen behöver anpassas.....	489
10.1.1	Nuvarande reglering.....	489
10.1.2	Skattebrottsdatalagen ges ett nytt namn.....	489
10.2	Tillämpningsområdet.....	490
10.3	Grundläggande bestämmelser om behandling	491
10.3.1	Tillåtna rättsliga grunder och behandling för nya ändamål.....	491
10.3.2	Behandling av biometriska och genetiska uppgifter.....	492
10.3.3	Sökning på känsliga personuppgifter	493
10.4	Gemensamt tillgängliga uppgifter.....	495
10.5	Övergångsbestämmelser till skattebrottsdatalagen	497
11	Åklagardatalagen.....	499
11.1	Åklagardatalagen behöver anpassas	499
11.1.1	Nuvarande reglering.....	499
11.1.2	Åklagardatalagen delas upp.....	500
11.2	Tillämpningsområdet.....	501
11.3	Grundläggande bestämmelser om behandling	504

11.3.1	Tillåtna rättsliga grunder och behandling för nya ändamål	504
11.3.2	Behandling av biometriska och genetiska uppgifter	506
11.3.3	Sökning på känsliga personuppgifter	507
11.4	Gemensamt tillgängliga uppgifter	508
12	Domstolsdatalagen.....	511
12.1	Behovet av ny reglering.....	511
12.1.1	Nuvarande reglering.....	511
12.1.2	Regleringen för domstolarna kräver särskilda överväganden.....	511
12.1.3	En särskild registerlagstiftning inom brottsdatalagens tillämpningsområde	512
12.2	Utgångspunkter för regleringen.....	513
12.2.1	Den nya lagen ska gälla utöver brottsdatalagen ..	513
12.2.2	Domstolsdatalagen kan bilda mönster.....	514
12.2.3	Vissa bestämmelser i domstolsdatalagen behövs inte.....	514
12.3	Allmänna bestämmelser	516
12.3.1	Tillämpningsområdet.....	516
12.3.2	Personuppgiftsansvar.....	519
12.3.3	Ska domstolarna utse dataskyddsombud?	520
12.3.4	Uppgifter om juridiska personer.....	521
12.4	Grundläggande bestämmelser om behandling.....	522
12.4.1	Tillåtna rättsliga grunder för behandling.....	522
12.4.2	Behandling för nya ändamål	524
12.4.3	Särskilda upplysningar	526
12.4.4	Behandling av personnummer.....	527
12.4.5	Behandling av biometriska och genetiska uppgifter	528
12.5	Sökning.....	529
12.5.1	Sökförbudet i brottsdatalagen ska inte gälla.....	529
12.5.2	Särskilda sökförbud.....	531
12.5.3	Tillåtna sökningar.....	534

12.6	Utlämnande av personuppgifter	535
12.6.1	Direktåtkomst	535
12.6.2	Elektroniskt utlämnande.....	536
12.7	Frågor om föreskriftsrätt	537
12.8	Administrativa sanktionsavgifter	539
12.9	Skadestånd.....	540
12.10	Överklagande	541
12.11	Övergångsbestämmelser.....	542
13	Lagen om behandling av personuppgifter inom kriminalvården	545
13.1	Lagen om behandling av personuppgifter inom kriminalvården behöver anpassas	545
13.1.1	Lagens nuvarande struktur.....	545
13.1.2	En omodern lagstiftning	546
13.1.3	Två olika registerlagar för kriminalvården	547
13.2	Allmänna bestämmelser.....	549
13.2.1	Tillämpningsområdet	549
13.2.2	Personuppgiftsansvar	552
13.3	Grundläggande bestämmelser om behandling	553
13.3.1	Tillåtna rättsliga grunder och behandling för nya ändamål.....	553
13.3.2	Behandling av biometriska och genetiska uppgifter.....	558
13.3.3	Utlämnande av personuppgifter	559
13.4	Kriminalvårdens register.....	560
13.4.1	Nuvarande reglering.....	560
13.4.2	Hur bör den framtida regleringen se ut?.....	562
13.5	Säkerhetsregistret.....	563
13.5.1	Reglering i lag	563
13.5.2	Registrering av häktade och intagna.....	565
13.5.3	Registrering av den som utövar våld eller hot	569
13.5.4	Registrering avseende andra.....	570
13.5.5	Sökning på känsliga personuppgifter	571

13.5.6	Direktåtkomst och annat utlämnande	572
13.5.7	Längsta tid som personuppgifter får behandlas ..	574
13.5.8	Föreskrifter.....	574
13.6	Bestämmelser som inte längre behövs.....	575
13.6.1	Sökning på känsliga personuppgifter	575
13.6.2	Tillgången till personuppgifter.....	575
13.6.3	Omprövning.....	576
13.6.4	Överklagande	577
13.7	Anpassningar av förordningen om behandling av personuppgifter inom kriminalvården	579
13.7.1	Behovet av översyn	579
13.7.2	Anpassningar till brottsdatalagen och kriminalvårdens brottsdatalag	579
13.7.3	Andra ändringar i förordningen	581
14	Säkerhetspolisens behandling av personuppgifter.....	585
14.1	Bakgrund.....	585
14.1.1	Säkerhetspolisens uppdrag och verksamhet	585
14.1.2	Säkerhetspolisens organisation	587
14.1.3	Regleringen av personuppgiftsbehandlingen.....	588
14.2	En ny lag för Säkerhetspolisens personuppgiftsbehandling.....	592
14.2.1	Allmänna utgångspunkter	592
14.2.2	En särskild lag för Säkerhetspolisens personuppgiftsbehandling	596
14.2.3	Lagens syfte	599
14.3	Lagens tillämpningsområde	600
14.3.1	Avgränsningen av tillämpningsområdet	600
14.3.2	Ska andra myndigheter tillämpa lagen?.....	604
14.3.3	Säkerhetspolisen ska även tillämpa brottsdatalagen	606
14.4	Regleringen ska utgå från regleringen i polisdatalagen	606
14.5	Allmänna bestämmelser	607
14.5.1	Förhållandet till annan lagstiftning.....	607
14.5.2	Personuppgiftsansvar.....	608

14.5.3	Definitioner	609
14.5.4	Uppgifter om juridiska personer	610
14.6	Ändamål och rättsliga grunder för behandlingen	611
14.6.1	Ändamål för behandling av personuppgifter	611
14.6.2	Primära och sekundära ändamålsbestämmelser är bestämmelser om rättslig grund	614
14.6.3	Rättslig grund för behandling – huvudregeln	617
14.6.4	Rättslig grund i undantagsfall för diarieföring och handläggning	619
14.6.5	Rättslig grund för behandling genom utlämnande	620
14.7	Grundläggande krav på behandlingen	622
14.7.1	Författningsenlig och korrekt behandling	622
14.7.2	Personuppgifter ska vara korrekta, adekvata och relevanta	622
14.7.3	Känsliga personuppgifter	625
14.7.4	Åtgärder för att säkerställa personuppgifternas kvalitet	631
14.8	Uppgifter från transportföretag	633
14.9	Gemensamt tillgängliga uppgifter	634
14.9.1	Allmänt om regleringen	634
14.9.2	Särskilda upplysningar	635
14.10	Behandling av personuppgifter i ostrukturerad information	638
14.10.1	Behovet av reglering	638
14.10.2	Undantag från kravet på särskilda upplysningar	640
14.11	Elektroniskt utlämnande	643
14.11.1	Elektroniskt utlämnande på annat sätt än genom direktåtkomst	643
14.11.2	Behovet av direktåtkomst	644
14.11.3	Direktåtkomst för vissa svenska myndigheter	648
14.11.4	Direktåtkomst för underrättelse- och säkerhetstjänster inom EU och EES	655

14.12	Sekretessbrytande bestämmelser	660
14.12.1	Uppgiftsskyldighet gällande rättsstatistik	660
14.12.2	Sekretessgenombrott gentemot svenska myndigheter.....	660
14.12.3	Sekretessgenombrott i övrigt	664
14.13	Längsta tid som personuppgifter får behandlas	665
14.13.1	Innebörden av nuvarande reglering.....	665
14.13.2	Hur länge får personuppgifter behandlas?	667
14.13.3	Personuppgifter som inte har gjorts gemensamt tillgängliga.....	668
14.13.4	Personuppgifter som har gjorts gemensamt tillgängliga.....	669
14.13.5	Personuppgifter som rör viss säkerhetshotande verksamhet	671
14.13.6	Ärenden om utredning av eller lagföring för brott	676
14.13.7	Möjlighet att förlänga tiden för behandling	677
14.13.8	Föreskrifter.....	678
14.14	Skyldigheter som personuppgiftsansvarig	680
14.15	Enskildas rättigheter.....	685
14.16	Sanktioner, skadestånd och rättsmedel	688
14.16.1	Ingen straffbestämmelse i den nya lagen	688
14.16.2	Sanktionsavgift bör inte få tas ut	689
14.16.3	Skadestånd	692
14.16.4	Överklagande	693
14.17	Överföring av personuppgifter till tredjeland och internationella organisationer	694
14.17.1	Utgångspunkter	694
14.17.2	Grundläggande förutsättningar för överföring ...	697
14.17.3	Tillåtna grunder för överföring.....	699
14.17.4	Överföring till andra mottagare	702
14.17.5	Villkor för användningen av personuppgifter	704
14.17.6	Dokumentationskrav	705

15	Tillsyn över Säkerhetspolisen	707
15.1	Det behövs en särskild reglering	707
15.2	Vem ska utöva tillsyn över Säkerhetspolisen?.....	711
15.2.1	För- och nackdelar med parallell tillsyn.....	711
15.2.2	Bör den parallella tillsynen bestå?	713
15.3	Tillsynsområdet.....	717
15.4	Tillsynen enligt Säkerhetspolisens datalag	718
15.4.1	Allmän tillsyn.....	718
15.4.2	Förhandssamråd och annat råd och stöd	720
15.5	Befogenheter vid tillsynen enligt den nya lagen.....	722
15.5.1	Undersökningsbefogenheter	722
15.5.2	Både förebyggande och korrigerande befogenheter behövs	723
15.5.3	Förebyggande befogenheter	724
15.5.4	Korrigerande befogenheter	725
15.6	Handläggningen av tillsynsfrågor	726
15.6.1	Kommunikationsskyldighet.....	726
15.6.2	Överklagande.....	727
15.6.3	Anmälningsskyldighet.....	728
15.7	Säkerhets- och integritetsskyddsnämndens tillsyn.....	728
15.7.1	Nämndens allmänna tillsyn.....	728
15.7.2	Kontroll på begäran av enskild	730
15.7.3	Anmälningsskyldighet.....	732
16	Register över tillträdesförbud vid idrottsarrangemang ..	735
16.1	Nuvarande reglering	735
16.1.1	Tillträdesförbudsregistret	735
16.1.2	Polismyndighetens roll.....	736
16.1.3	Idrottsorganisationernas roll	737
16.2	Två olika regleringar	738
16.3	Regleringen för Polismyndigheten	742
16.4	Regleringen för idrottsorganisationerna	744
16.5	Följdändringar.....	744

17	Övriga författningsändringar	747
17.1	Tystnadsplikt för dataskyddsbud.....	747
17.2	Sekretessfrågor.....	749
17.2.1	Följdändringar i offentlighets- och sekretesslagen	749
17.2.2	Sekretess för uppgifter i verksamhet för teknisk bearbetning och lagring	750
17.2.3	Sekretess för uppgifter som behandlas i strid med personuppgiftsregleringen.....	751
17.2.4	Sekretess för personuppgiftsincidenter	752
17.3	Lagen om internationellt polisiärt samarbete	753
17.4	Lagen om Polismyndighetens elimineringsdatabas	755
17.5	Hänvisningar till 2013 års lag ska upphävas	756
18	Ikraftträdande och övergångsbestämmelser	759
18.1	Ikraftträdande	759
18.2	Samma övergångsbestämmelser för flertalet författningar.....	759
18.2.1	Behovet av övergångsbestämmelser.....	759
18.2.2	Skadestånd	760
18.2.3	Sanktioner.....	760
18.3	Övergångsbestämmelser till Säkerhetspolisens datalag och domstolarnas brottsdatalag.....	761
18.3.1	Ärendehandläggning m.m.	761
18.3.2	Övergångsbestämmelser i övrigt.....	762
18.4	Särskilda övergångsproblem.....	764
18.4.1	Den nya dataskyddsregleringen medför särskilda övergångsproblem.....	764
18.4.2	Problemen med olika ikraftträdandetidpunkter	764
18.4.3	Problem om genomförandet av direktivet fördröjs	767

19	Konsekvenser	769
19.1	Allmänt om konsekvenserna.....	769
19.1.1	Anpassningar av registerförfattningarna.....	769
19.1.2	Två nya lagar men inga nya arbetsuppgifter.....	770
19.1.3	Modernisering av vissa författningar.....	771
19.2	Ekonomiska konsekvenser.....	773
19.2.1	Konsekvenser för staten.....	773
19.2.2	Konsekvenser för kommuner, landsting och enskilda.....	774
19.3	Konsekvenser för det brottsförebyggande arbetet.....	774
19.4	Konsekvenser i övrigt.....	775
20	Författningskommentar	777
20.1	Förslaget till Säkerhetspolisens datalag (2018:000).....	777
20.2	Förslaget till domstolarnas brottsdatalag (2018:000).....	832
20.3	Förslaget till lag om ändring i rättegångsbalken.....	844
20.4	Förslaget till lag om ändring i polislagen (1984:387).....	845
20.5	Förslaget till lag om ändring i säkerhetskylldslagen (1996:627).....	845
20.6	Förslaget till lag om ändring i lagen (1996:701) om Tullverkets befogenheter vid Sveriges gräns mot ett annat land inom Europeiska unionen.....	845
20.7	Förslaget till lag om ändring i lagen (2000:344) om Schengens informationssystem.....	846
20.8	Förslaget till lag om ändring i lagen (2001:185) om behandling av uppgifter i Tullverkets verksamhet.....	846
20.9	Förslaget till lag om ändring i lagen (2001:617) om behandling av personuppgifter inom kriminalvården.....	847
20.10	Förslaget till lag om ändring i lagen (2005:321) om tillträdesförbud vid idrottsarrangemang.....	861

20.11 Förslaget till lag om ändring i lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet	861
20.12 Förslaget till lag om ändring i offentlighets- och sekretesslagen (2009:400)	863
20.13 Förslaget till lag om ändring i polisdatalagen (2010:361) ..	865
20.14 Förslaget till lag om ändring i kustbevakningsdatalagen (2012:145)	901
20.15 Förslaget till lag om ändring i lagen (2014:400) om Polismyndighetens elimineringsdatabas	918
20.16 Förslaget till lag om ändring i lagen (2015:51) om register över tillträdesförbud vid idrottsarrangemang	920
20.17 Förslaget till lag om ändring i åklagardatalagen (2015:433)	922
20.18 Förslaget till lag om ändring i utlänningsdatalagen (2016:27)	936
20.19 Förslaget till lag om ändring i tullagen (2016:253)	936
20.20 Förslaget till lag om ändring i tullbrottsdatalagen (2017:447)	936
20.21 Förslaget till lag om ändring i skattebrottsdatalagen (2017:452)	957
20.22 Förslaget till lag om ändring i lagen (2017:496) om internationellt polisiärt samarbete.....	972
20.23 Förslaget till lag om ändring i brottsdatalagen (2018:000)	975

Bilaga

Bilaga 1 Kommittédirektiv 2016:21.....	979
----------------------------------------	-----

Sammanfattning

Uppdraget

Europeiska unionen har enats om en genomgripande dataskyddsreform som ska vara genomförd under våren 2018. Reformen omfattar dels en allmän dataskyddsförordning, dels ett dataskyddsdirektiv som behandlar dataskyddet vid bl.a. brottsbekämpning, lagföring och straffverkställighet. En konsekvens av reformen är att personuppgiftslagen kommer att upphävas och att all lagstiftning om personuppgiftsbehandling behöver ses över och anpassas.

Utredningens uppdrag är att föreslå hur det nya direktivet ska genomföras i svensk rätt genom en ny ramlagstiftning och att anpassa registerförfattningarna för myndigheterna i rättskedjan till de nya förutsättningarna. Utredningen ska också överväga om det finns anledning att reglera Säkerhetspolisens personuppgiftsbehandling separat.

Brottsdatalagen förutsätter en ny struktur

I delbetänkandet Brottsdatalag (SOU 2017:29) föreslår utredningen en ny lag, brottsdatalagen, som kommer att fylla ungefär samma funktion som personuppgiftslagen gör i dag i verksamhet som rör brottsbekämpning, lagföring, straffverkställighet och upprätthållande av allmän ordning och säkerhet. I brottsdatalagen finns de grundläggande bestämmelserna om hur personuppgifter får behandlas. Där regleras även personuppgiftsansvarigas skyldigheter, enskildas rättigheter och tillsynen över personuppgiftsbehandling. Brottsdatalagen innehåller vidare bestämmelser om administrativa sanktionsavgifter, skadestånd och rättsmedel.

Registerförfattningarna för myndigheterna i rättskedjan utgår i dag från personuppgiftslagen, antingen genom att registerförfatt-

ningen gäller i stället för personuppgiftslagen men hänvisar till bestämmelser i den eller genom att registerförfattningen gäller utöver personuppgiftslagen. Utredningen föreslår att registerförfattningarna ska gälla utöver brottsdatalagen och innehålla bestämmelser som innebär preciseringar, undantag eller avvikelser från bestämmelserna i den lagen. Bestämmelser i registerförfattningarna om bl.a. syfte, automatiserad behandling, personuppgiftsombud, behandling av känsliga personuppgifter och tillgången till personuppgifter ska därför upphävas. Det föranleder omfattande redaktionella ändringar i registerförfattningarna.

De registerförfattningar som reglerar personuppgiftsbehandling både inom och utanför brottsdatalagens tillämpningsområde renodlas så att de bara gäller vid personuppgiftsbehandling inom tillämpningsområdet. Det gäller lagen om behandling av personuppgifter inom kriminalvården, kustbevakningsdatalagen och åklagardatalagen. För domstolarna skapas i stället en ny lag för den personuppgiftsbehandling som ligger inom tillämpningsområdet. För att det ska vara tydligt att registerförfattningarna gäller utöver brottsdatalagen ges de nya namn.

Anpassningar och andra ändringar i de brottsbekämpande myndigheternas registerförfattningar

Tillämpningsområdet

I dag utgår tillämpningsområdet i de brottsbekämpande myndigheternas registerförfattningar från i vilken verksamhet personuppgiftsbehandlingen utförs. Det som kommer att bli avgörande för tillämpningen är i stället dels om myndigheten agerar i egenskap av behörig myndighet enligt brottsdatalagen, dels i vilket syfte personuppgifterna behandlas. Tillämpningsområdet blir därmed smälare än i dag, eftersom inte all personuppgiftsbehandling som utförs inom ramen för brottsbekämpning, lagföring, straffverkställighet eller upprätthållande av allmän ordning och säkerhet omfattas, t.ex. utlämnande av allmänna handlingar enligt tryckfrihetsförordningen eller för ändamål utanför brottsdatalagens tillämpningsområde.

Tillåtna rättsliga grunder och behandling för nya ändamål

Regleringen av för vilka ändamål de brottsbekämpande myndigheterna får behandla personuppgifter är i dag uppdelad i primära och sekundära ändamål. Regleringen föreslås i stort sett vara oförändrad när det gäller de primära ändamålen men det tydliggörs att det är fråga om bestämmelser om rättslig grund.

Innan personuppgifter behandlas för nya ändamål inom brottsdatalagens tillämpningsområde ska det enligt brottsdatalagen alltid prövas om det finns en tillåten rättslig grund för den nya behandlingen och om den är nödvändig och proportionerlig för det nya ändamålet. Det behöver däremot inte prövas om det nya ändamålet är förenligt med det ursprungliga. När personuppgifter behandlas för ändamål utanför tillämpningsområdet ska data-skyddsförordningen tillämpas. Utredningen föreslår att en prövning av nödvändighet och proportionalitet ska göras även innan personuppgifter behandlas för ändamål utanför brottsdatalagens tillämpningsområde. Någon prövning behöver dock inte göras om skyldighet att lämna uppgifter följer av lag eller förordning. Uppräkningen i de sekundära ändamålsbestämmelserna av i vilka situationer personuppgifter får tillhandahållas ersätts alltså av en särskild prövning både vid behandling för ändamål inom och utanför brottsdatalagens tillämpningsområde.

Behandling av känsliga personuppgifter

Brottsdatalagen förbjuder sökningar i personuppgifter i syfte att få fram ett personurval grundat på känsliga personuppgifter. I registerförfattningarna ska det göras undantag från förbudet som är anpassade till respektive myndighets behov av att kunna behandla känsliga personuppgifter. Brottsbekämpande myndigheter ska få använda t.ex. uppgifter som beskriver en persons utseende eller brottsrubriceringar ska vara tillåtet vid sökning i alla slags personuppgifter. Vid sökning i uppgifter som inte är gemensamt tillgängliga, dvs. som bara ett fåtal personer har tillgång till, ska sökning i syfte att ta fram personurval grundade på vissa känsliga personuppgifter få göras.

Längsta tid för behandling

I registerförfattningarna finns det bestämmelser om bevarande och gallring. De syftar till att skydda den personliga integriteten och reglerar inte bevarande och gallring i arkivlagens mening. De ska därför formuleras om så att det framgår att det är fråga om data-skyddsbestämmelser. Regleringen ska utgå från hur länge personuppgifter får behandlas. Någon ändring av hur länge olika typer av personuppgifter får behandlas görs i princip inte.

Utökade möjligheter till elektroniskt utlämnande

Regleringen av i vilken utsträckning personuppgifter får lämnas ut på medium för automatiserad behandling moderniseras för att möta de ökade behoven av att kunna kommunicera elektroniskt. Det blir tillåtet att lämna ut personuppgifter elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt.

Viss reglering flyttas till registerförfattningarna

Bestämmelserna om Polismyndighetens behandling av personuppgifter i registret över tillträdesförbud vid idrottsarrangemang flyttas till polisens brottsdatalog. Lagen om register över tillträdesförbud vid idrottsarrangemang renodlas så att den bara reglerar idrottsorganisationernas personuppgiftsbehandling.

Regleringen av Polismyndighetens, Säkerhetspolisens och Tullverkets behandling av personuppgifter som tillhandahålls av transportföretag flyttas till respektive myndighets registerförfattning.

En ny lag för domstolarna

Domstolsdatalogen reglerar i dag personuppgiftsbehandling både inom och utanför brottsdatalogens tillämpningsområde i domstolarnas rättskipande och rättsvårdande verksamhet. Den del av domstolarnas personuppgiftsbehandling som ligger inom tillämpningsområdet ska regleras i en ny lag, domstolarnas brottsdatalog. Den nya lagen utformas med domstolsdatalogen som mönster men anpassas till den systematik och terminologi som finns i övriga regis-

terförfattningar inom brottsdatalagens tillämpningsområde. Vissa frågor som hittills reglerats i förordning lyfts upp i lagen.

Allmän domstol ska tillämpa lagen när personuppgifter behandlas i syfte att handlägga mål och ärenden om utredning av eller lagföring för brott, ändring eller verkställighet av straffrättsliga påföljder eller upprätthållande av allmän ordning och säkerhet. Allmän förvaltningsdomstol ska tillämpa lagen när personuppgifter behandlas i syfte att handlägga mål och ärenden om verkställighet av häktning eller straffrättsliga påföljder. Till skillnad från i dag omfattar tillämpningsområdet inte personuppgiftsbehandling i den administrativa verksamheten som avser att på begäran lämna ut uppgifter ur mål eller ärenden.

Innan domstolar behandlar personuppgifter för nya ändamål inom brottsdatalagens tillämpningsområde ska de pröva om behandlingen är nödvändig och proportionerlig för det nya ändamålet. Vid behandling för nya ändamål utanför brottsdatalagens tillämpningsområde gäller dataskyddsförordningen. Någon prövning av om behandlingen är nödvändig och proportionerlig behöver inte göras om domstolsdatalagen ska tillämpas. En sådan prövning krävs däremot i andra fall, om inte skyldighet att lämna uppgifter följer av lag eller förordning.

Domstolarna ska inte tillämpa sökförbudet i brottsdatalagen. I stället ska motsvarande sökförbud som i domstolsdatalagen, som förbjuder användningen av uppgifter som avslöjar känsliga personuppgifter och uppgifter om brott eller misstanke om brott och nationell anknytning som sökbegrepp, gälla. Samma undantag från förbudet som finns i domstolsdatalagen ska gälla.

Regleringen av Kriminalvårdens personuppgiftsbehandling

Kriminalvårdens reglering har en annan struktur än övriga registerförfattningar, eftersom större delen finns i förordning. Regleringen anpassas till brottsdatalagen och blir mer lik övriga registerförfattningar. Utredningens uppdrag har dock inte omfattat att göra en total översyn av regleringen och någon ny lag föreslås därför inte, trots att alla bestämmelser ändras och lagen får en helt ny struktur.

Lagen ska tillämpas när kriminalvården behandlar personuppgifter i syfte att verkställa häktning eller straffrättsliga påföljder eller

biträda andra behöriga myndigheter när de utför arbetsuppgifter som omfattas av brottsdatalogens tillämpningsområde eller för att fullgöra internationella åtaganden. På samma sätt som för de brottsbekämpande myndigheterna ska behandling för nya ändamål föregås av en prövning av om behandlingen är nödvändig och proportionerlig för det nya ändamålet, oavsett om ändamålet ligger inom eller utanför brottsdatalogens tillämpningsområde.

Regleringen av säkerhetsregistret flyttas till lagen, moderniseras och görs mer generell. Uppgifter om den som är häktad eller verkställer fängelsestraff ska få registreras om personen utgör en säkerhetsrisk. Även uppgifter om personer som en registrerad har viss anknytning till ska få behandlas om det är absolut nödvändigt. Om det finns risk för att någon som verkställer en påföljd inom kriminalvården utövar våld eller hot mot personer i kriminalvårdens lokaler ska uppgifter om honom eller henne också få behandlas i säkerhetsregistret. Det görs undantag från sökförbudet i brottsdatalogen för sökningar i säkerhetsregistret i syfte att få fram personurval grundat på vissa känsliga personuppgifter.

Bestämmelserna om Kriminalvårdens underrättelseskyldighet bryts ut ur registerförordningen och placeras i en ny förordning.

En ny lag för Säkerhetspolisen

Regleringen utgår från dagens reglering och brottsdatalogen

Utredningen föreslår att det ska införas en ny lag om Säkerhetspolisens behandling av personuppgifter, Säkerhetspolisens datalag, som ersätter regleringen i polisdatalagen. Den regleringen ska bilda mönster för den nya lagen, som ska vara heltäckande och därför blir betydligt mer omfattande än dagens reglering. Den nya lagen följer i princip brottsdatalogens systematik och innehåll. Det innebär att bestämmelserna om grundläggande krav på behandling, den personuppgiftsansvariges skyldigheter, enskildas rättigheter, skadestånd, rättsmedel och överföring av personuppgifter till tredjeland i stort sett överensstämmer med brottsdatalogens bestämmelser.

Lagen ska gälla vid behandling av personuppgifter som rör nationell säkerhet i Säkerhetspolisens brottsbekämpande och lagförande verksamhet. När Säkerhetspolisen behandlar personuppgifter som inte rör nationell säkerhet i syfte att bekämpa och lagföra

brott ska myndigheten tillämpa brottsdatalagen och polisens brottsdatalag.

Rättslig grund för behandling av personuppgifter

Regleringen av för vilka ändamål Säkerhetspolisen får behandla personuppgifter är i dag uppdelad i primära och sekundära ändamål. Regleringen behålls i stort sett oförändrad men det tydliggörs att det är fråga om bestämmelser om rättslig grund – rättslig grund för behandling och rättslig grund för utlämnande.

Behandling av känsliga personuppgifter

Huvudregeln är att Säkerhetspolisen på samma sätt som i dag inte ska få behandla känsliga personuppgifter. Om uppgifter om en person redan behandlas ska de dock få kompletteras med känsliga personuppgifter om det är absolut nödvändigt.

Säkerhetspolisen får i dag använda uppgifter som avslöjar känsliga personuppgifter som sökbegrepp om det är absolut nödvändigt. Utredningen föreslår att samma sökförbud som i brottsdatalagen ska gälla för Säkerhetspolisen, dvs. att det ska vara förbjudet att göra sökningar i syfte att få fram ett personurval grundat på känsliga personuppgifter. Från förbudet görs det undantag. Det ska vara tillåtet att använda brottsrubriceringar, uppgifter om tillvägagångssätt vid brott och uppgifter som beskriver en persons utseende vid sökning. Även sökningar i syfte att få fram personurval grundat på flertalet känsliga personuppgifter ska tillåtas, om sökningen är absolut nödvändig.

Elektroniskt utlämnande

Säkerhetspolisen ska få lämna ut personuppgifter elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt.

Säkerhetspolisen ska få medge Polismyndigheten, Försvarmakten och Försvarets radioanstalt direktåtkomst till personuppgifter som har gjorts gemensamt tillgängliga och som Säkerhetspolisen behandlar för vissa syften. Även underrättelse- och säkerhetstjäns-

ter inom EU och EES ska få medges direktåtkomst till uppgifter som Säkerhetspolisen behandlar för vissa syften om det behövs för samarbetet mot terrorism. Sådan direktåtkomst ska dock endast få medges till personuppgifter i en avskild uppgiftssamling och regeringen ska underrättas innan direktåtkomst medges.

Längsta tid för behandling

Personuppgifter ska inte få behandlas under längre tid än vad som behövs för något eller några av de syften för vilka Säkerhetspolisen får behandla personuppgifter. Huvudregeln ska på samma sätt som i dag vara att personuppgifter som har gjorts gemensamt tillgängliga inte får behandlas längre än tio år efter det år då den senaste registreringen avseende personen gjordes. Uppgifter om personer som ännu inte fyllt 18 år ska dock inte få behandlas längre än fem år från den senaste registreringen. Personuppgifter som hänför sig till sådan säkerhetshotande verksamhet som avses i 18 och 19 kap. brottsbalken ska inte få behandlas längre än 40 år efter det år då den senaste registreringen gjordes. På samma sätt som i dag ska Säkerhetspolisen kunna besluta att personuppgifter får behandlas under längre tid om det finns särskilda skäl.

Tillsyn över Säkerhetspolisens personuppgiftsbehandling

Både Datainspektionen och Säkerhets- och integritetsskyddsnämnden ska på i huvudsak samma sätt som i dag utöva tillsyn över Säkerhetspolisens personuppgiftsbehandling.

Datainspektionen ska utöva allmän tillsyn över personuppgiftsbehandling enligt den nya lagen och ge råd och stöd till Säkerhetspolisen. Inspektionen ska i huvudsak ha samma befogenheter som enligt brottsdatalagen. Säkerhetspolisen ska dock inte kunna påföras administrativ sanktionsavgift.

Säkerhets- och integritetsskyddsnämnden ska utöva tillsyn över Säkerhetspolisens personuppgiftsbehandling och på begäran av enskild kontrollera om behandlingen av personuppgifter är författningssenlig.

Ikraftträdande och övergångsbestämmelser

De nya registerförfattningarna och ändringarna i de befintliga registerförfattningarna föreslås träda i kraft den 1 maj 2018. Det krävs särskilda övergångsbestämmelser för det nya sanktionssystemet och för ersättning för skador som har vållats före ikraftträdandet. Till de nya lagarna krävs det övergångsbestämmelser dels för mål och ärenden som rör behandlingen av personuppgifter som har påbörjats före ikraftträdandet men inte hunnit slutföras, dels för mål som har överklagats men som inte har hunnit slutföras inom den tiden.

1 Författningsförslag

1.1 Förslag till Säkerhetspolisens datalag (2018:000)

Härigenom föreskrivs följande.

1 kap. Allmänna bestämmelser

Syftet med lagen

1 § Syftet med denna lag är att skydda fysiska personers grundläggande fri- och rättigheter i samband med behandling av personuppgifter och att säkerställa att Säkerhetspolisen kan behandla och utbyta personuppgifter på ett ändamålsenligt sätt.

Lagens tillämpningsområde

2 § Denna lag gäller vid behandling av personuppgifter som rör nationell säkerhet i Säkerhetspolisens brottsbekämpande och lagförande verksamhet.

Lagen gäller i tillämpliga delar vid Polismyndighetens behandling av personuppgifter när myndigheten har övertagit en arbetsuppgift som rör nationell säkerhet från Säkerhetspolisen.

Vid behandling av personuppgifter enligt denna lag gäller inte lagen (2018:000) med kompletterande bestämmelser till EU:s dataskyddsförordning.

3 § Lagen gäller för sådan behandling av personuppgifter som är helt eller delvis automatiserad och för annan behandling av personuppgifter som ingår i eller är avsedda att ingå i en strukturerad

samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

Förhållandet till annan reglering

4 § I lagen (2017:496) om internationellt polisiärt samarbete och i föreskrifter som regeringen har meddelat i anslutning till den lagen, finns det särskilda bestämmelser om behandling av personuppgifter som följer av internationella överenskommelser. Om det i dessa författningar finns avvikande bestämmelser, ska de tillämpas i stället för bestämmelserna i denna lag.

5 § Bestämmelserna i denna lag ska inte tillämpas i den utsträckning det skulle inskränka skyldigheten enligt 2 kap. tryckfrihetsförordningen att lämna ut personuppgifter.

6 § I brottsdatalagen (2018:000) och polisens brottsdatalag (2010:361) finns det bestämmelser om Säkerhetspolisens behandling av personuppgifter i frågor som inte rör nationell säkerhet.

Personuppgiftsansvar

7 § Säkerhetspolisen är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför.

Polismyndigheten är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför.

Personuppgiftsansvaret omfattar all behandling av personuppgifter som utförs under respektive myndighets ledning eller på dess vägnar.

8 § Säkerhetspolisen får vara gemensamt personuppgiftsansvarig med annan endast i den utsträckning det följer av lag eller förordning eller om regeringen i ett enskilt fall beslutar om det.

Uttryck i lagen

9 § I denna lag används följande uttryck med nedan angiven betydelse.

<i>Uttryck</i>	<i>Betydelse</i>
Behandling av personuppgifter	En åtgärd eller kombination av åtgärder som vidtas i fråga om personuppgifter eller uppsättningar av personuppgifter, oavsett om det görs automatiserat eller inte, t.ex. insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämnande, spridning eller tillhandahållande på annat sätt, justering, sammanföring, begränsning, radering eller förstöring.
Biometriska uppgifter	Personuppgifter som rör en persons fysiska, fysiologiska eller beteendemässiga kännetecken, som tagits fram genom särskild teknisk behandling och som möjliggör eller bekräftar unik identifiering av personen i fråga.
Dataskyddsbud	En fysisk person som utses av den personuppgiftsansvarige för att självständigt se till att personuppgifter behandlas författningsenligt och på ett korrekt sätt.
Genetiska uppgifter	Personuppgifter som rör en persons nedärvda eller förvärvade genetiska kännetecken och som härrör från analys av ett spår av eller ett prov från personen i fråga.

Internationell organisation	En organisation och dess underställda organ som lyder under folkrätten eller ett annat organ som inrättats genom eller på grundval av en överenskommelse mellan två eller flera stater.
Mottagare	Den till vilken personuppgifter lämnas ut, med undantag av en myndighet som med stöd av författning utövar tillsyn, kontroll eller revision.
Personuppgift	Varje upplysning om en identifierad eller identifierbar fysisk person som är i livet.
Personuppgiftsansvarig	Den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter.
Personuppgiftsbiträde	Den som, med stöd av ett skriftligt avtal eller annan skriftlig överenskommelse, behandlar personuppgifter för den personuppgiftsansvariges räkning.
Registrerad	Den fysiska person som personuppgiften rör.
Tillsynsmyndighet	Den myndighet som regeringen utser att enligt denna lag utöva tillsyn över personuppgiftsbehandling.
Tredjeland	En stat som inte är medlem i Europeiska unionen eller Europeiska ekonomiska samarbetsområdet och som inte heller på grund av avtal med Europeiska unionen har en motsvarande ställning.
Tredje man	Någon annan än den registrerade, den personuppgiftsansvarige, dataskyddsombudet,

personuppgiftsbiträdet och sådana personer som under den personuppgiftsansvariges eller personuppgiftsbitrådets direkta ansvar har rätt att behandla personuppgifter.

Uppgift som rör hälsa

Personuppgift som rör en persons fysiska eller psykiska hälsa, inkluderande information om tillhandahållande av hälso- och sjukvårdstjänster som ger upplysning om personens hälsostatus.

Lagens tillämpning på uppgifter om juridiska personer

10 § Bestämmelserna om personuppgifter i följande paragrafer gäller också vid behandling av uppgifter om juridiska personer:

1. 7 § om personuppgiftsansvar,
2. 2 kap. 1–3 §§ om tillåtna rättsliga grunder för behandling av personuppgifter,
3. 3 kap. 2 och 3 §§ om gemensamt tillgängliga uppgifter,
4. 4 kap. 1–4 och 6–11 §§ om längsta tid som personuppgifter får behandlas, och
5. 5 kap. 5 § om tillgången till personuppgifter.

2 kap. Behandling av personuppgifter

Tillåtna rättsliga grunder för behandling av personuppgifter

1 § Personuppgifter får behandlas om det är nödvändigt för att utföra en arbetsuppgift i syfte att

1. förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar
 - a) brott mot rikets säkerhet,
 - b) terrorbrott, eller
 - c) tryckfrihetsbrott eller yttrandefrihetsbrott med rasistiska eller främlingsfientliga motiv,

2. utreda eller lagföra sådana brott som avses i 1, eller, efter särskilt beslut, annat brott,
 3. fullgöra uppgifter
 - a) i samband med personskydd av den centrala statsledningen och andra som regeringen eller Säkerhetspolisen bestämmer,
 - b) enligt säkerhetsskyddslagen (1996:627), eller
 - c) enligt utlännings- och medborgarskapslagstiftningen,
 4. fullgöra annan arbetsuppgift som rör nationell säkerhet och som anges i lag eller förordning eller särskilt beslut av regeringen, eller
 5. fullgöra förpliktelser som följer av internationella åtaganden.
- Arbetsuppgiften ska framgå av en lag, en förordning eller ett särskilt beslut i vilket regeringen uppdragit åt myndigheten att ansvara för en sådan uppgift.

2 § Personuppgifter som behandlas med stöd av 1 § får även behandlas om det är nödvändigt för att tillhandahålla information som behövs

1. för något av de syften som anges i 1 kap. 2 § brottsdatalagen (2018:000) hos Polismyndigheten, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket,
2. i en myndighets verksamhet, om informationen tillhandahålls inom ramen för myndighetsöverskridande samverkan mot brott,
3. i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst och i Försvarets radioanstalts försvarsunderrättelseverksamhet, om det finns särskilda skäl att tillhandahålla informationen,
4. i en myndighets verksamhet om Säkerhetspolisen enligt lag eller förordning ska bistå myndigheten med viss uppgift,
5. i brottsbekämpande verksamhet hos en utländsk myndighet eller mellanfolklig organisation, eller
6. i verksamhet hos utländsk underrättelse- eller säkerhetstjänst.

Personuppgifter som behandlas med stöd av 1 § får även behandlas, om det är nödvändigt för att tillhandahålla information till riksdagen och regeringen och, i den utsträckning skyldighet att lämna uppgifter följer av lag eller förordning, till andra.

I ett enskilt fall får personuppgifter som behandlas med stöd av 1 § även behandlas för att tillhandahålla information för något annat ändamål än de som anges i första och andra styckena, under

förutsättning att ändamålet inte är oförenligt med det ändamål som uppgifterna samlades in för.

3 § Personuppgifter får även behandlas om

1. det är nödvändigt för diarieföring, eller
2. uppgifterna har lämnats till Säkerhetspolisen i en anmälan, ansökan eller liknande och behandlingen är nödvändig för handläggningen.

Ändamål för behandling av personuppgifter

4 § Personuppgifter får behandlas bara för särskilda, uttryckligt angivna och berättigade ändamål.

Personuppgifter får inte behandlas för något ändamål som är oförenligt med det ändamål för vilket personuppgifterna ursprungligen behandlades.

5 § Säkerhetspolisen får behandla personuppgifter för vetenskapliga, statistiska eller historiska ändamål inom denna lags tillämpningsområde.

Grundläggande krav på behandling av personuppgifter

Laglig och korrekt behandling

6 § Personuppgifter ska behandlas författningsenligt och på ett korrekt sätt.

Personuppgifternas kvalitet

7 § Personuppgifter som behandlas ska vara korrekta och, om det är nödvändigt, uppdaterade.

Uppgifter som beskriver en persons utseende ska utformas på ett objektivt sätt med respekt för människovärdet.

8 § Personuppgifter som behandlas ska vara adekvata och relevanta i förhållande till ändamålen med behandlingen. Fler personuppgifter får inte behandlas än vad som är nödvändigt med hänsyn till ändamålen med behandlingen.

Känsliga personuppgifter

9 § Personuppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening eller som rör hälsa, sexualliv eller sexuell läggning får inte behandlas.

När uppgifter om en person behandlas får de dock kompletteras med sådana uppgifter som anges i första stycket om det är absolut nödvändigt för ändamålet med behandlingen.

10 § Säkerhetspolisen får behandla biometriska uppgifter endast om det är absolut nödvändigt för ändamålet med behandlingen. Genetiska uppgifter får inte behandlas.

11 § Personuppgifter som avses i 9 och 10 §§ betecknas som känsliga personuppgifter. Känsliga personuppgifter får behandlas med stöd av 3 §.

12 § Det är förbjudet att utföra sökning i syfte att få fram ett personurval grundat på känsliga personuppgifter.

Första stycket hindrar inte att brottsrubriceringar, uppgifter om tillvägagångssätt vid brott eller uppgifter som beskriver en persons utseende används vid sökning.

Första stycket hindrar inte heller sökning i syfte att få fram ett personurval grundat på etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller uppgifter som rör hälsa, sexualliv eller sexuell läggning, om sökningen är absolut nödvändig för något av de syften som anges i 1 §.

Åtgärder för att säkerställa personuppgifternas kvalitet

13 § Alla rimliga åtgärder ska vidtas för att personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålet med behandlingen utan onödigt dröjsmål rättas och för att förhindra att sådana uppgifter lämnas ut eller görs tillgängliga. Personuppgifter som är inaktuella ska uppdateras om det är nödvändigt.

14 § Alla rimliga åtgärder ska vidtas för att personuppgifter som behandlas i strid med 1–6, 8–10 eller 12 § eller 4 kap. 1 § första stycket, 2–4 eller 7–11 § utan onödigt dröjsmål raderas och för att förhindra att sådana uppgifter lämnas ut eller görs tillgängliga. Det samma gäller om radering krävs för att utföra en rättslig förpliktelse.

Om förutsättningarna i första stycket för att radera personuppgifter är uppfyllda men de behöver finnas kvar som bevisning, ska Säkerhetspolisen i stället utan onödigt dröjsmål begränsa behandlingen av uppgifterna.

Uppgiftsskyldighet och utlämnande av personuppgifter

15 § Personuppgifter som är nödvändiga för att framställa rättsstatistik ska lämnas till den myndighet som ansvarar för att framställa sådan statistik.

16 § Om det är förenligt med svenska intressen, får personuppgifter lämnas ut till

1. Interpol eller Europol, eller till en polismyndighet eller åklagarmyndighet i en stat som är ansluten till Interpol, om det behövs för att myndigheten eller organisationen ska kunna förebygga, förhindra, upptäcka, utreda eller lagföra brott, eller

2. utländsk underrättelse- eller säkerhetstjänst.

Personuppgifter får vidare lämnas ut till en utländsk myndighet eller mellanfolklig organisation, om utlämnandet följer av en internationell överenskommelse som Sverige har tillträtt efter riksdagens godkännande.

17 § Polismyndigheten har, trots sekretess enligt 21 kap. 3 § första stycket, 35 kap. 1 § och 37 kap. 1 § offentlighets- och sekretesslagen (2009:400), rätt att ta del av personuppgifter som har gjorts gemensamt tillgängliga och som behandlas med stöd av 1 § första stycket 1–3 a, om myndigheten behöver uppgifterna för något av de syften som anges i 2 kap. 1 § första stycket 1 eller 2 polisens brottsdatalog (2010:361).

18 § Försvarets radioanstalt och Försvarmakten har, trots sekretess enligt 21 kap. 3 § första stycket, 35 kap. 1 § och 37 kap. 1 § offentlighets- och sekretesslagen (2009:400), rätt att ta del av personuppgifter som har gjorts gemensamt tillgängliga och som behandlas med stöd av 1 § första stycket 1 eller 2, om den mottagande myndigheten behöver uppgifterna i sin försvarsunderrättelseverksamhet eller militära säkerhetstjänst.

19 § Personuppgifter får lämnas ut elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt.

Elektroniskt utlämnande genom direktåtkomst är tillåtet bara i den utsträckning som anges i 3 kap. 5–7 §§.

Personuppgifter från transportföretag

20 § Personuppgifter som tillhandahålls Säkerhetspolisen enligt 25 § polislagen (1984:387) får behandlas för något av de syften som anges i 1 § första stycket 1–3 a.

Personuppgifter som avses i första stycket får endast i ett enskilt fall behandlas för nya ändamål.

21 § Vid terminalåtkomst enligt 26 § polislagen (1984:387) får Säkerhetspolisen inte ändra eller på annat sätt bearbeta personuppgifterna.

Föreskrifter

22 § Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om

1. att personuppgifter får lämnas ut i andra fall än som anges i 15–18 §§,
2. begränsning av möjligheten att lämna ut personuppgifter elektroniskt enligt 19 § första stycket,
3. underrättelseskyldighet, och
4. sökning i personuppgifter.

3 kap. Gemensamt tillgängliga uppgifter

Allmän bestämmelse

1 § Detta kapitel innehåller särskilda bestämmelser för behandling av personuppgifter som görs eller har gjorts gemensamt tillgängliga. Personuppgifter som endast ett fåtal personer har rätt att ta del av anses inte som gemensamt tillgängliga.

Detta kapitel gäller inte när personuppgifter behandlas med stöd av 2 kap. 3 §.

Personuppgifter som får göras gemensamt tillgängliga

2 § Personuppgifter får göras gemensamt tillgängliga om det behövs för något av de syften som anges i 2 kap. 1 §.

Särskilda upplysningar

3 § Om det inte framgår av sammanhanget eller på något annat sätt för vilket ändamål som gemensamt tillgängliga personuppgifter behandlas, ska det tydliggöras genom en särskild upplysning.

4 § Om uppgifter som är gemensamt tillgängliga direkt kan hänföras till en person som inte är misstänkt för brott eller för att ha utövat eller komma att utöva brottslig verksamhet, ska det genom en särskild upplysning eller på något annat sätt framgå att personen

inte är misstänkt för brott eller brottslig verksamhet som avses i 2 kap. 1 § första stycket 1 eller 2.

Uppgifter om en person som kan antas ha direkt samband med sådan brottslig verksamhet som avses i 2 kap. 1 § första stycket 1 ska förse med en upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak. Någon upplysning behöver dock inte lämnas om det på grund av omständigheterna är onödigt.

Någon upplysning enligt andra stycket behöver inte heller lämnas om

1. uppgifterna ingår i en uppgiftssamling som har skapats för att bearbeta och analysera information och som enbart särskilt angivna tjänstemän har åtkomst till och
2. bearbetningen av uppgifterna inte har genomförts.

Direktåtkomst

5 § Polismyndigheten får för något av de syften som anges i 2 kap. 1 § första stycket 1 eller 2 polisens brottsdatalog (2010:361) medges direktåtkomst till personuppgifter som behandlas med stöd av 2 kap. 1 § första stycket 1–3 a. Direktåtkomsten får endast avse personuppgifter som har gjorts gemensamt tillgängliga.

6 § Försvarets radioanstalt och Försvarmakten får i försvarsunderrättelseverksamheten och den militära säkerhetstjänsten medges direktåtkomst till personuppgifter som behandlas med stöd av 2 kap. 1 § första stycket 1 eller 2. Direktåtkomsten får endast avse personuppgifter som har gjorts gemensamt tillgängliga.

7 § Om det behövs för samarbetet mot terrorism får en underrättelse- eller säkerhetstjänst i en medlemsstat i Europeiska unionen eller Europeiska ekonomiska samarbetsområdet medges direktåtkomst till personuppgifter i en avskild uppgiftssamling som Säkerhetspolisen upprättat i syfte att dela information med sådana mottagare. Uppgiftssamlingen får endast innehålla personuppgifter som behandlas med stöd av 2 kap. 1 § första stycket 1 b och har gjorts gemensamt tillgängliga.

Innan direktåtkomst medges en utländsk underrättelse- eller säkerhetstjänst enligt första stycket ska Säkerhetspolisen underätta regeringen.

Föreskrifter

8 § Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om underrättelseskyldighet vid direktåtkomst.

9 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om omfattningen av direktåtkomst enligt 5–7 §§ och om behörighet och säkerhet vid sådan åtkomst.

4 kap. Längsta tid som personuppgifter får behandlas

Allmän bestämmelse

1 § Personuppgifter får inte behandlas under längre tid än vad som behövs för något eller några av de syften som anges i 2 kap. 1–3 §§.

Det som sägs i första stycket hindrar inte att Säkerhetspolisen arkiverar och bevarar allmänna handlingar eller att arkivmaterial lämnas till en arkivmyndighet.

Vid automatiserad behandling gäller också de begränsningar som följer av 2–11 §§.

Personuppgifter som inte har gjorts gemensamt tillgängliga

2 § Trots det som sägs i 1 § andra stycket får personuppgifter som inte har gjorts gemensamt tillgängliga inte behandlas längre än

1. ett år efter det att ärendet avslutades, om de behandlas i ett ärende, eller

2. ett år efter det att de behandlades automatiserat första gången, om de inte kan hänföras till ett ärende.

Första stycket gäller inte personuppgifter i ärenden om utredning av eller lagföring för brott.

Gemensamt tillgängliga uppgifter i ärenden om utredning av eller lagföring för brott

3 § Om en brottsanmälan avskrivs på grund av att den påstådda gärningen inte utgör brott, får personuppgifterna i anmälan inte längre behandlas för ändamål inom denna lags tillämpningsområde. Om en brottsanmälan i annat fall inte har lett till förundersökning eller annan motsvarande utredning, får personuppgifterna inte behandlas för ändamål inom denna lags tillämpningsområde när åtal inte längre får väckas för brottet.

4 § Om en förundersökning har lett till åtal eller annan domstolsprövning, får personuppgifterna i förundersökningen inte behandlas för ändamål inom denna lags tillämpningsområde längre än fem år efter utgången av det kalenderår då domstolens avgörande fick laga kraft.

Om en förundersökning har lagts ner eller avslutats på annat sätt än genom åtal, får personuppgifterna i förundersökningen inte behandlas för ändamål inom denna lags tillämpningsområde längre än fem år efter utgången av det kalenderår då åklagarens eller förundersökningsledarens beslut meddelades.

Första och andra styckena gäller även personuppgifter i andra utredningar som handläggs enligt bestämmelser i 23 kap. rättegångsbalken.

5 § Om en förundersökning mot en person har lagts ner, om ett åtal har lagts ner eller om en frikännande dom har fått laga kraft, får personen inte längre vara sökbar som misstänkt.

Övriga gemensamt tillgängliga uppgifter

6 § Trots det som sägs i 1 § andra stycket får andra personuppgifter än de som anges i 3 och 4 §§ och som har gjorts gemensamt tillgängliga som längst behandlas under den tid som anges i 7–11 §§.

7 § Personuppgifter som behandlas för något av de syften som anges i 2 kap. 1 § första stycket 1 får inte behandlas längre än tio år efter utgången av det kalenderår då den senaste registreringen gjordes avseende personens anknytning till brottslig verksamhet.

Uppgifter om en person som vid tiden för registreringen inte fyllt 18 år får dock inte behandlas längre än fem år efter utgången av det kalenderår då den senaste registreringen gjordes avseende den unges anknytning till brottslig verksamhet, om någon ny registrering inte gjorts efter det att han eller hon fyllt 18 år.

8 § Personuppgifter som behandlas för något av de syften som anges i 2 kap. 1 § första stycket 3–5 får inte behandlas längre än tio år efter utgången av det kalenderår då den senaste registreringen gjordes avseende personen.

Uppgifter om en person som vid tiden för registreringen inte fyllt 18 år får dock inte behandlas längre än fem år efter utgången av det kalenderår då den senaste registreringen gjordes avseende den unge, om någon ny registrering inte gjorts efter det att han eller hon fyllt 18 år.

9 § Personuppgifter som behandlas i en sådan uppgiftssamling som anges i 3 kap. 4 § tredje stycket får inte behandlas längre än

1. tre år efter utgången av det kalenderår då den senaste registreringen gjordes avseende personens anknytning till brottslig verksamhet, om uppgifterna behandlas för något av de syften som anges i 2 kap. 1 § första stycket 1, och

2. tre år efter utgången av det kalenderår då den senaste registreringen gjordes avseende personen, om uppgifterna behandlas för något av de syften som anges i 2 kap. 1 § första stycket 3–5.

10 § Personuppgifter som hänför sig till sådan säkerhetshotande verksamhet som avses i 18 och 19 kap. brottsbalken som utövas av främmande makt, får inte behandlas längre än 40 år efter utgången av det kalenderår då den senaste registreringen gjordes avseende personens anknytning till brott eller brottslig verksamhet. För personuppgifter som behandlas i en sådan uppgiftssamling som anges i 3 kap. 4 § tredje stycket gäller 9 §.

11 § Om det finns särskilda skäl får Säkerhetspolisen besluta att personuppgifter får behandlas under längre tid än vad som anges i 7–10 §§, om uppgifterna fortfarande behövs för det ändamål för vilket de behandlas. Om personuppgifter behandlas med stöd av ett sådant beslut ska frågan om fortsatt behandling prövas på nytt senast vid utgången av det tionde kalenderåret efter beslutet eller, om det är fråga om uppgifter som avses i 9 §, senast vid utgången av det tredje kalenderåret efter beslutet. Tiden som personuppgifterna får behandlas får vid varje tillfälle förlängas med längst tio år eller, om det är fråga om uppgifter som avses i 9 §, med längst tre år.

Föreskrifter

12 § Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om att vissa kategorier av personuppgifter får fortsätta att behandlas för ändamål inom denna lags tillämpningsområde under längre tid än vad som anges i 3 och 4 §§.

13 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om

1. att personuppgifter, med avvikelse från 2 § första stycket och 7–11 §§, får behandlas under längre tid för arkivändamål av allmänt intresse och vetenskapliga, statistiska eller historiska ändamål, och
2. begränsning av behandlingen av personuppgifter för ändamål inom denna lags tillämpningsområde vid digital arkivering.

5 kap. Skyldigheter som personuppgiftsansvarig

Åtgärder för att säkerställa författningsenlig behandling

Tekniska och organisatoriska åtgärder

1 § Säkerhetspolisen ska, genom lämpliga tekniska och organisatoriska åtgärder, säkerställa och kunna visa att behandlingen av personuppgifter är författningsenlig och att registrerades rättigheter skyddas.

2 § Både vid beslut om hur behandlingen ska utföras och vid behandlingen ska Säkerhetspolisen, genom lämpliga tekniska och organisatoriska åtgärder, se till att dataskyddsprinciper säkerställs på ett effektivt sätt och att nödvändiga skyddsåtgärder integreras i behandlingen (inbyggt dataskydd).

3 § Säkerhetspolisen ska säkerställa att det i automatiserade behandlingssystem som regel endast är möjligt att behandla de personuppgifter som är nödvändiga för varje särskilt angivet ändamål med behandlingen (dataskydd som standard).

4 § Säkerhetspolisen ska säkerställa att det i automatiserade behandlingssystem förs loggar över personuppgiftsbehandling i den utsträckning det är särskilt föreskrivet.

Tillgången till personuppgifter

5 § Säkerhetspolisen ska se till att tillgången till personuppgifter begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter.

Konsekvensbedömning och förhandssamråd

6 § Kan en typ av ny behandling, eller betydande förändringar avseende redan pågående behandling, antas medföra särskild risk för intrång i registrerades personliga integritet, ska Säkerhetspolisen innan behandlingen påbörjas eller förändringen genomförs bedöma konsekvenserna för skyddet av personuppgifter.

Om konsekvensbedömningen visar att det finns särskild risk för intrång i registrerades personliga integritet eller om typen av behandling innebär särskild risk för intrång, ska Säkerhetspolisen samråda med tillsynsmyndigheten i god tid innan behandlingen påbörjas eller betydande förändringar genomförs.

Säkerheten för personuppgifter

7 § Säkerhetspolisen ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas, särskilt mot obehörig eller otillåten behandling och mot förlust, förstöring eller annan oavsiktlig skada.

Samarbete med tillsynsmyndigheten

8 § Säkerhetspolisen ska samarbeta med tillsynsmyndigheten när den utför uppgifter enligt denna lag och föreskrifter som har meddelats i anslutning till den.

Dataskyddsombud

9 § Säkerhetspolisen ska inom myndigheten utse ett eller flera dataskyddsombud och anmäla till tillsynsmyndigheten när dataskyddsombud utses och entledigas.

10 § Dataskyddsombud ska

1. självständigt kontrollera att Säkerhetspolisen behandlar personuppgifter författningsenligt och på ett korrekt sätt och i övrigt fullgör sina skyldigheter,

2. informera och ge råd till Säkerhetspolisen och de som behandlar personuppgifter under myndighetens ledning om deras skyldigheter vid behandling av personuppgifter,

3. på begäran ge Säkerhetspolisen råd vid en konsekvensbedömning och kontrollera att den genomförs på korrekt sätt,

4. vara kontaktpunkt för enskilda i frågor som rör behandling av personuppgifter, och

5. samarbeta med tillsynsmyndigheten och vara kontaktpunkt för den vid förhandssamråd och andra frågor som rör behandling av personuppgifter.

11 § Om Säkerhetspolisen bryter mot bestämmelser för behandling av personuppgifter och rättelse inte vidtas, ska dataskyddsombudet anmäla det till tillsynsmyndigheten.

Personuppgiftsbiträden

12 § Säkerhetspolisen får, om det är lämpligt, anlita personuppgiftsbiträden. När ett personuppgiftsbiträde anlitas, ska Säkerhetspolisen försäkra sig om att biträdet vidtar lämpliga tekniska och organisatoriska åtgärder för att behandlingen av personuppgifter ska vara författningensenlig och för att skydda registrerades rättigheter.

13 § Det ska finnas ett skriftligt avtal eller annan skriftlig överenskommelse om personuppgiftsbitrådets behandling av personuppgifter för Säkerhetspolisens räkning.

Ett personuppgiftsbiträde får inte utan skriftligt tillstånd av Säkerhetspolisen anlita ett annat personuppgiftsbiträde.

14 § Ett personuppgiftsbiträde och de som arbetar under bitrådets ledning får behandla personuppgifter bara i enlighet med instruktioner från Säkerhetspolisen.

Om ett personuppgiftsbiträde i strid med Säkerhetspolisens instruktioner fastställer ändamålen med och medlen för behandlingen, ska biträdet anses vara personuppgiftsansvarig för den behandlingen.

15 § Det som sägs om Säkerhetspolisens skyldigheter i 4, 5, 7 och 8 §§ gäller även för personuppgiftsbiträden som Säkerhetspolisen anlitar.

Föreskrifter

16 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om

1. åtgärder som avses i 1–4, 6 och 7 §§,
2. tillgången till personuppgifter,
3. skyldigheten att föra register över kategorier av behandling av personuppgifter,
4. skyldigheten att införa interna rutiner för anmälan av överträdelser, och
5. innehållet i avtal och överenskommelser enligt 13 §.

6 kap. Enskildas rättigheter

Rätten till information

Allmän information

1 § Säkerhetspolisen ska göra följande allmänna information tillgänglig för registrerade.

1. Myndighetens identitet och kontaktuppgifter.
2. Dataskyddsombudets kontaktuppgifter.
3. Ändamålen med behandlingen.
4. Rätten enligt 2 § att begära att få information om behandling av personuppgifter och att få del av dem.
5. Rätten att begära rättelse, radering eller begränsning av behandlingen enligt 6 och 7 §§.

Personrelaterad information

2 § Säkerhetspolisen ska till den som begär det utan onödigt dröjsmål lämna skriftligt besked om personuppgifter som rör honom eller henne behandlas. Behandlas sådana uppgifter ska sökanden få del av dem och få följande skriftliga information.

1. Vilka personuppgifter om sökanden som behandlas.
2. Varifrån personuppgifterna kommer.
3. Den rättsliga grunden för behandlingen.
4. Ändamålen med behandlingen.
5. Mottagare eller kategorier av mottagare av personuppgifterna, även i tredjeland eller internationella organisationer.
6. Hur länge personuppgifterna får behandlas eller, om det inte är möjligt att ange, kriterierna för att fastställa det.
7. Rätten att begära rättelse, radering eller begränsning av behandlingen enligt 6 och 7 §§.

Utlämnande enligt första stycket behöver inte omfatta personuppgifter som sökanden har tagit del av, om inte han eller hon begär det. Det ska dock framgå av informationen att personuppgifterna i fråga behandlas.

Begränsning av rätten till information

3 § Informationsskyldigheten i 2 § gäller inte i den utsträckning det är särskilt föreskrivet i lag eller annan författning eller annars framgår av beslut som har meddelats med stöd av författning att uppgifter inte får lämnas ut till den registrerade.

Om förutsättningarna i första stycket är uppfyllda, är Säkerhetspolisen inte skyldig att lämna ut skälen för beslut enligt första stycket eller beslut i fråga om rättelse, radering eller begränsning av behandlingen enligt 6 eller 7 §.

4 § Informationsskyldigheten i 2 § gäller inte personuppgifter i löpande text som inte fått sin slutliga utformning när begäran gjordes eller som utgör minnesanteckning eller liknande.

Informationsskyldigheten gäller dock om uppgifterna har lämnats ut till tredje man, behandlas enbart för vetenskapliga, statistiska eller historiska ändamål eller arkivändamål av allmänt intresse eller, när det gäller löpande text som inte fått sin slutliga utformning, om uppgifterna har behandlats längre än ett år.

5 § Om en begäran enligt 2 § är orimlig eller uppenbart ogrundad får Säkerhetspolisen avslå den.

Av 9 § andra stycket framgår att Säkerhetspolisen i vissa fall får ta ut avgift i stället för att avslå begäran.

Rätten till rättelse, radering och begränsning av behandlingen

6 § Säkerhetspolisen ska på begäran av den registrerade utan onödigt dröjsmål rätta eller komplettera personuppgifter som rör honom eller henne om de är felaktiga eller ofullständiga med hänsyn till ändamålet med behandlingen.

Om Säkerhetspolisen inte kan fastställa att personuppgifterna är korrekta ska behandlingen av uppgifterna i stället utan onödigt dröjsmål begränsas.

7 § Säkerhetspolisen ska på begäran av den registrerade utan onödigt dröjsmål radera personuppgifter som rör honom eller henne om de behandlas i strid med 2 kap. 1–6, 8–10 eller 12 § eller 4 kap.

1 § första stycket, 2–4 eller 7–11 §. Detsamma gäller om radering krävs för att Säkerhetspolisen ska utföra en rättslig förpliktelse.

Om förutsättningarna i första stycket för att radera personuppgifter är uppfyllda men de behöver finnas kvar som bevisning, ska Säkerhetspolisen på begäran av den registrerade i stället utan onödigt dröjsmål begränsa behandlingen av uppgifterna.

8 § Säkerhetspolisen avgör vilken åtgärd som ska vidtas med anledning av en begäran om rättelse, radering eller begränsning av behandlingen.

Avgiftsfri information

9 § Information enligt 1 § ska lämnas utan avgift. Information och uppgifter enligt 2 § ska lämnas utan avgift en gång per år.

Om någon begär information och uppgifter enligt 2 § oftare än en gång per år, får Säkerhetspolisen ta ut en rimlig avgift eller avslå begäran enligt 5 § första stycket.

Föreskrifter

10 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om

1. information enligt 1 och 2 §§,
2. avgift för information som avses i 2 §, och
3. kraven på en begäran enligt 2, 6 eller 7 §.

7 kap. Tillsyn

Tillsyn över personuppgiftsbehandlingen

1 § Tillsynsmyndigheten ska

1. utöva allmän tillsyn över personuppgiftsbehandling, och
2. ge råd och stöd till Säkerhetspolisen och personuppgiftsbiträden om deras skyldigheter enligt lag eller annan författning vid förhandssamråd eller när det i övrigt är påkallat.

2 § Bestämmelser om tillsyn över Säkerhetspolisens behandling av personuppgifter finns även i lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet.

Befogenheter

Undersökningsbefogenheter

3 § Tillsynsmyndigheten har rätt att av Säkerhetspolisen eller ett personuppgiftsbiträde på begäran få

1. tillgång till alla personuppgifter som behandlas,
2. upplysningar om och dokumentation av behandlingen av personuppgifter och säkerhets- och skyddsåtgärder,
3. tillträde till lokaler som Säkerhetspolisen eller ett personuppgiftsbiträde disponerar och tillgång till utrustning och andra medel för behandling av personuppgifter, och
4. det biträde och annan information som behövs för tillsynen.

Förebyggande befogenheter

4 § Om tillsynsmyndigheten bedömer att det finns risk för att personuppgifter kan komma att behandlas i strid med lag eller annan författning, ska myndigheten genom råd, rekommendationer eller påpekanden försöka förmå Säkerhetspolisen eller personuppgiftsbiträdet att vidta åtgärder för att minska den risken.

Tillsynsmyndigheten får utfärda en skriftlig varning för att planerad behandling av personuppgifter riskerar att stå i strid med lag eller annan författning. Detsamma gäller om pågående behandling riskerar att stå i strid med lag eller annan författning.

Korrigerande befogenheter

5 § Om tillsynsmyndigheten konstaterar att personuppgifter behandlas i strid med lag eller annan författning, eller att Säkerhetspolisen eller ett personuppgiftsbiträde annars inte fullgör sina skyldigheter, får tillsynsmyndigheten

1. genom sådana åtgärder som anges i 4 § första stycket försöka förmå Säkerhetspolisen eller personuppgiftsbiträdet att vidta åtgär-

der för att behandlingen ska bli författningsevenlig eller att uppfylla andra skyldigheter,

2. förelägga Säkerhetspolisen eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningsevenlig eller att fullgöra andra skyldigheter, eller

3. förbjuda fortsatt behandling om bristen är allvarlig.

Om ett föreläggande utfärdas ska det av föreläggandet framgå när åtgärderna senast ska vara genomförda och, om det är lämpligt, vilka åtgärder som ska vidtas.

Kommunikation

6 § Innan tillsynsmyndigheten fattar ett beslut enligt 5 § första stycket 2 eller 3, ska den som beslutet gäller ges tillfälle att inom en bestämd tid yttra sig över allt material av betydelse för beslutet, om det inte är uppenbart obehövligt.

8 kap. Skadestånd och rättsmedel

Skadestånd

1 § Den personuppgiftsansvarige ska ersätta den registrerade för den skada och kränkning av den personliga integriteten som behandling av personuppgifter i strid med denna lag, eller föreskrifter som har meddelats i anslutning till den, har orsakat.

Överklagande

Överklagande av Säkerhetspolisens beslut

2 § Beslut i fråga om rättelse eller komplettering enligt 6 kap. 6 § första stycket, radering enligt 6 kap. 7 § första stycket eller begränsning av behandlingen enligt 6 kap. 6 § andra stycket eller 6 kap. 7 § andra stycket, som har meddelats av Säkerhetspolisen i egenskap av personuppgiftsansvarig, får överklagas till allmän förvaltningsdomstol. Detsamma gäller beslut att inte lämna information enligt 6 kap. 2 § eller att ta ut avgift enligt 6 kap. 9 § andra stycket.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Överklagande av tillsynsmyndighetens beslut

3 § Tillsynsmyndighetens beslut enligt denna lag eller enligt föreskrifter som har meddelats i anslutning till den får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Beslut som inte får överklagas

4 § Andra beslut enligt denna lag än de som anges i 2 och 3 §§ får inte överklagas.

9 kap. Överföring av personuppgifter till tredjeland och internationella organisationer

Grundläggande förutsättningar för överföring

1 § Säkerhetspolisen får överföra personuppgifter som behandlas till ett tredjeland eller en internationell organisation. Det gäller även överföring av personuppgifter för behandling i ett tredjeland eller av en internationell organisation. Personuppgifterna får dock endast överföras om överföringen

1. riktas till en brottsbekämpande myndighet eller en underrättelse- eller säkerhetstjänst i ett tredjeland eller en internationell organisation med brottsbekämpande uppdrag och

2. omfattas av

- a) ett beslut om adekvat skyddsnivå enligt 3 §, eller
- b) tillräckliga skyddsåtgärder enligt 4 §, eller
- c) ett undantag för särskilda situationer enligt 5 §.

2 § Personuppgifter som Säkerhetspolisen har fått från en annan stat får överföras till ett tredjeland eller en internationell organisation endast om den stat som lämnat uppgifterna till Säkerhetspolisen har medgett att de överförs.

Tillåtna grunder för överföring

Beslut om adekvat skyddsnivå

3 § Om Europeiska kommissionen har beslutat att det finns en adekvat nivå för skyddet av personuppgifter i ett tredjeland, eller en viss geografisk eller på annat sätt angiven del av det, får personuppgifter överföras dit. Detsamma gäller om det finns ett sådant beslut avseende en internationell organisation.

Tillräckliga skyddsåtgärder

4 § Om det inte finns ett beslut om adekvat skyddsnivå enligt 3 §, får personuppgifter ändå överföras till ett tredjeland eller en internationell organisation om

1. skyddsåtgärder för personuppgifter har fastställts i ett avtal som ger tillräckliga garantier till skydd för registrerades rättigheter, eller

2. den myndighet eller organisation som uppgifterna ska överföras till på annat sätt garanterar tillräckligt skydd för dem.

Överföring i särskilda situationer

5 § Om det inte finns ett beslut om adekvat skyddsnivå enligt 3 § eller tillräckliga skyddsåtgärder enligt 4 §, får personuppgifter överföras till ett tredjeland eller en internationell organisation endast om överföringen är nödvändig för att

1. skydda den registrerades eller en annan fysisk persons vitala intressen, eller andra berättigade intressen för den registrerade,

2. i ett enskilt fall förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott,

3. i ett enskilt fall kunna fastställa, göra gällande eller försvara ett rättsligt anspråk som hänför sig till ett sådant syfte som anges i 2, eller

4. avvärja en omedelbar och allvarlig fara för allmän säkerhet.

Personuppgifter får inte överföras till ett tredjeland eller en internationell organisation om den registrerades intresse av skydd mot kränkning av grundläggande fri- och rättigheter väger tyngre

än det allmännas intresse av en sådan överföring som avses i första stycket 2 eller 3.

Överföring till andra mottagare

6 § Säkerhetspolisen får i ett enskilt fall överföra personuppgifter till någon annan mottagare än som anges i 1 § i ett tredjeland. Personuppgifterna får överföras endast om

1. det är absolut nödvändigt för att Säkerhetspolisen ska kunna utföra en arbetsuppgift enligt 2 kap. 1 eller 2 § och

2. det skulle vara ineffektivt eller olämpligt att överföra dem till en mottagare som anges i 1 § i det tredjelandet.

Personuppgifter får inte överföras enligt första stycket om den registrerades intresse av skydd mot kränkning av grundläggande fri- och rättigheter väger tyngre än det allmännas intresse av att överföringen görs.

Villkor om användningsbegränsning

7 § Om Säkerhetspolisen har fått personuppgifter från ett tredjeland eller en internationell organisation och det på grund av en överenskommelse med det tredjelandet eller den internationella organisationen gäller villkor som begränsar möjligheten att använda uppgifterna, ska Säkerhetspolisen följa villkoren oavsett vad som är föreskrivet i lag eller annan författning.

8 § Säkerhetspolisen får, vid överföring av personuppgifter till ett tredjeland eller en internationell organisation, ställa upp villkor som begränsar möjligheten att använda uppgifterna, om det krävs från allmän synpunkt eller med hänsyn till enskilds rätt.

Föreskrifter

9 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om dokumentation av överföringar.

1. Denna lag träder i kraft den 1 maj 2018.
2. Bestämmelsen i 5 kap. 4 § om loggning behöver inte tillämpas på automatiserade behandlingssystem som inrättats före ikraftträdandet förrän den 1 maj 2023.
3. Ärenden om tillsyn över Säkerhetspolisens personuppgiftsbehandling som rör nationell säkerhet i myndighetens brottsbekämpande eller lagförande verksamhet och som Datainspektionen eller Säkerhets- och integritetsskyddsnämnden inte har avgjort före ikraftträdandet handläggs enligt äldre föreskrifter.
4. Äldre föreskrifter gäller fortfarande för överklagande av beslut som meddelats före ikraftträdandet och som rör behandling av personuppgifter som rör nationell säkerhet i Säkerhetspolisens brottsbekämpande och lagförande verksamhet.
5. Bestämmelsen om skadestånd i 48 § i personuppgiftslagen (1998:204) gäller fortfarande för skada som har orsakats före ikraftträdandet vid behandling av personuppgifter som rör nationell säkerhet i Säkerhetspolisens brottsbekämpande och lagförande verksamhet.

1.2 Förslag till domstolarnas brottsdatalag (2018:000)

Härigenom föreskrivs följande.

1 kap. Allmänna bestämmelser

Lagens tillämpningsområde

1 § Denna lag gäller utöver brottsdatalagen (2018:000) när följande domstolar i egenskap av behöriga myndigheter behandlar personuppgifter.

1. Allmän domstol, om uppgifterna behandlas i syfte att handlägga mål eller ärenden om utredning av eller lagföring för brott, ändring eller verkställighet av straffrättsliga påföljder eller upprätthållande av allmän ordning och säkerhet.

2. Allmän förvaltningsdomstol, om uppgifterna behandlas i syfte att handlägga mål om verkställighet av häktning eller straffrättsliga påföljder.

Personuppgiftsansvar

2 § En domstol är personuppgiftsansvarig för den behandling av personuppgifter som den utför.

2 kap. Grundläggande bestämmelser om behandling

Tillåtna rättsliga grunder för behandling av personuppgifter

1 § Personuppgifter får behandlas om det är nödvändigt och syftet är att handlägga mål eller ärenden om

1. utredning av eller lagföring för brott,
2. verkställighet av häktning eller ändring eller verkställighet av straffrättsliga påföljder, eller
3. upprätthållande av allmän ordning och säkerhet.

Arbetsuppgiften ska framgå av en bindande unionsrättsakt eller av en lag, en förordning eller ett särskilt beslut i vilket regeringen uppdragit åt domstol att ansvara för en sådan uppgift.

2 § Förutsättningarna för att behandla personuppgifter, som behandlas med stöd av 1 §, för nya ändamål inom denna lags tillämpningsområde regleras i 2 kap. 4 § brottsdatalagen (2018:000).

Förutsättningarna för att behandla personuppgifter, som behandlas med stöd av 1 §, för nya ändamål utanför denna lags tillämpningsområde regleras i 2 kap. 22 § brottsdatalagen. Någon prövning enligt 2 kap. 22 § andra stycket brottsdatalagen krävs inte när domstolsdatalagen (2015:728) ska tillämpas.

Behandling av personnummer

3 § Personnummer, samordningsnummer och liknande identitetsbeteckningar får endast behandlas när det är motiverat med hänsyn till vikten av en säker identifiering eller något annat beaktansvärt skäl.

Bestämmelser om användning av sådana personuppgifter som anges i första stycket vid sökning finns i 8 §.

Sökning

Undantag från brottsdatalagens sökförbud

4 § Bestämmelserna i 5–10 §§ denna lag och föreskrifter som meddelats i anslutning till den gäller i stället för sökförbudet i 2 kap. 14 § brottsdatalagen (2018:000).

Känsliga personuppgifter och nationell anknytning

5 § Vid sökning i personuppgifter är det förbjudet att som sökbegrepp använda uppgifter som avslöjar sådana personuppgifter som anges i 2 kap. 11 och 12 §§ brottsdatalagen (2018:000) eller nationell anknytning.

Brott eller misstanke om brott

6 § I allmän domstol får sökbegrepp som avslöjar brott eller misstanke om brott inte användas vid sökning i personuppgifter

1. i mål eller ärenden som har avgjorts slutligt genom en dom eller ett beslut längre än fem år efter utgången av det kalenderår då avgörandet fick laga kraft, eller

2. i tvistemål.

7 § I allmän förvaltningsdomstol får sökbegrepp som avslöjar brott eller misstanke om brott inte användas vid sökning i personuppgifter i mål som

1. har avgjorts slutligt genom en dom eller ett beslut längre än tjugo år efter utgången av det kalenderår då avgörandet fick laga kraft, eller

2. handläggs av Migrationsöverdomstolen eller en migrationsdomstol.

Direkta personuppgifter

8 § Personnamn, personnummer, samordningsnummer och andra uppgifter som direkt kan hänföras till en fysisk person som är i livet får inte användas som sökbegrepp vid sökning i personuppgifter i brottmål som har avgjorts slutligt genom en dom eller ett beslut längre än fem år efter utgången av det kalenderår då avgörandet fick laga kraft.

Tillåtna sökningar

9 § Sökförbuden i 5–8 §§ hindrar inte sökning

1. i en viss handling eller i ett visst mål eller ärende, eller

2. med användande av särskilda beteckningar för identifiering av en viss mål- eller ärendetyp.

10 § Sökförbudet i 5 § hindrar inte att allmän förvaltningsdomstol använder uppgifter som avslöjar hälsa som sökbegrepp. Sådana uppgifter får dock inte användas vid sökning i personuppgifter i mål som

1. har avgjorts slutligt genom en dom eller ett beslut längre än tjugo år efter utgången av det kalenderår då avgörandet fick laga kraft, eller
2. handläggs av Migrationsöverdomstolen eller en migrationsdomstol.

Utlämnande av personuppgifter

11 § Personuppgifter får lämnas ut elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt. Elektroniskt utlämnande genom direktåtkomst är tillåtet bara i den utsträckning som anges i 12 § och föreskrifter som har meddelats i anslutning till denna lag.

12 § Direktåtkomst får endast medges

1. en allmän domstol,
2. en allmän förvaltningsdomstol, eller
3. en part eller partens ombud, biträde eller försvarare.

Direktåtkomst enligt första stycket 3 får endast avse personuppgifter i partens mål eller ärende.

Föreskrifter

13 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om ytterligare begränsning av

1. möjligheten att använda de sökbegrepp som anges i 6, 7 och 10 §§,
2. direktåtkomst enligt 12 § första stycket och om behörighet och säkerhet vid sådan åtkomst,
3. möjligheten att lämna ut personuppgifter elektroniskt enligt 11 §, och
4. behandling av personuppgifter som hänför sig till mål eller ärenden som har avgjorts genom dom eller beslut som har fått laga kraft.

3 kap. Administrativa sanktionsavgifter och rättsmedel

Administrativa sanktionsavgifter

1 § Sanktionsavgift får tas ut av den personuppgiftsansvarige vid överträdelse av bestämmelserna i

1. 2 kap. 1 § om tillåtna rättsliga grunder för behandling av personuppgifter, eller

2. 2 kap. 5–8 §§ om sökning.

Sanktionsavgiften ska vara minst 50 000 kronor och högst 20 000 000 kronor.

Skadestånd

2 § Vid behandling av personuppgifter enligt denna lag eller föreskrifter som har meddelats i anslutning till den ska bestämmelsen i 7 kap. 1 § brottsdatalagen (2018:000) om skadestånd tillämpas på motsvarande sätt.

Överklagande

3 § Bestämmelser om överklagande och om vilka beslut som får överklagas finns i 7 kap. brottsdatalagen (2018:000).

4 § En hovrätts, en tingsrätts eller en förvaltningsrätts beslut som överklagas enligt 7 kap. 2 § första stycket brottsdatalagen (2018:000) överklagas till kammarrätt. En kammarrätts beslut i sådana frågor överklagas till Högsta förvaltningsdomstolen.

Har Högsta domstolen eller Högsta förvaltningsdomstolen meddelat beslut som avses i 7 kap. 2 § första stycket brottsdatalagen får beslutet inte överklagas.

Kravet på prövningstillstånd i 7 kap. 2 § andra stycket brottsdatalagen gäller inte vid överklagande enligt första stycket.

1. Denna lag träder i kraft den 1 maj 2018.

2. Bestämmelserna i 2 kap. 6 § 1, 7 § 1, 8 § och 10 § 1 om begränsning av sökning i fråga om slutligt avgjorda mål och ärenden behöver inte tillämpas förrän den 1 januari 2019.

3. Ärenden om tillsyn över personuppgiftsbehandling, som rör behandling av personuppgifter vid handläggningen av mål och ärenden som avses i 2 kap. 1 § första stycket, som Datainspektionen inte har avgjort före ikraftträdandet handläggs enligt äldre föreskrifter.

4. Äldre föreskrifter gäller fortfarande för överklagande av beslut som meddelats före ikraftträdandet och som rör behandling av personuppgifter vid handläggningen av mål och ärenden som avses i 2 kap. 1 § första stycket.

5. Sanktionsavgift enligt 3 kap. 1 § får beslutas endast för överträdelser som har begåtts efter ikraftträdandet.

6. Bestämmelsen om skadestånd i 48 § personuppgiftslagen (1998:204) gäller fortfarande för skada som har orsakats före ikraftträdandet vid behandling av personuppgifter vid handläggningen av mål och ärenden som avses i 2 kap. 1 § första stycket.

1.3 Förslag till lag om ändring i rättegångsbalken

Härigenom föreskrivs att 28 kap. 12 a och b §§ rättegångsbalken ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

28 kap.

12 a §¹

Kroppsbesiktning genom tagande av salivprov får göras på den som skäligen kan misstänkas för ett brott på vilket fängelse kan följa, om syftet är att göra en *DNA-analys* av provet och registrera *DNA-profilen* i det *DNA-register* eller det utredningsregister som förs enligt *polisdatalagen* (2010:361).

Kroppsbesiktning genom tagande av salivprov får göras på den som skäligen kan misstänkas för ett brott på vilket fängelse kan följa, om syftet är att göra en *dna-analys* av provet och registrera *dna-profilen* i det *dna-register* eller det utredningsregister som förs enligt *polisens brottsdatalag* (2010:361).

12 b §²

Kroppsbesiktning genom tagande av salivprov får göras på annan än den som skäligen kan misstänkas för ett brott, om

1. syftet är att genom en *DNA-analys* av provet underlätta identifiering vid utredning av ett brott på vilket fängelse kan följa, och

2. det finns synnerlig anledning att anta att det är av betydelse för utredningen av brottet.

Analysresultatet får inte jämföras med de *DNA-profiler* som finns registrerade i register över

1. syftet är att genom en *dna-analys* av provet underlätta identifiering vid utredning av ett brott på vilket fängelse kan följa, och

Analysresultatet får inte jämföras med de *dna-profiler* som finns registrerade i register över

¹ Senaste lydelse 2010:363.

² Senaste lydelse 2010:363.

DNA-profiler som förs enligt *polisdatalagen* (2010:361) eller i övrigt användas för annat ändamål än det för vilket provet har tagits. *dna-profiler* som förs enligt *polisens brottsdatalag* (2010:361) eller i övrigt användas för annat ändamål än det för vilket provet har tagits.

Första stycket gäller inte den som är under 15 år.

Denna lag träder i kraft den 1 maj 2018.

1.4 Förslag till lag om ändring i polislagen (1984:387)

Härigenom föreskrivs att 26 § polislagen (1984:387) ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

26 §¹

Transportföretag får lämna uppgifter enligt 25 § på så sätt att de görs läsbara för Polismyndigheten eller Säkerhetspolisen genom terminalåtkomst.

Polismyndigheten och Säkerhetspolisen får ta del av uppgifter genom terminalåtkomst endast i den omfattning och under den tid som behövs för att kontrollera aktuella transporter. *Uppgifter som hålls tillgängliga på detta sätt får inte ändras eller på annat sätt bearbetas eller lagras av Polismyndigheten eller Säkerhetspolisen.*

Uppgifter om enskilda personer som lämnats på annat sätt än genom terminalåtkomst, ska omedelbart förstöras, om de visar sig sakna betydelse för utredning av eller lagföring för brott.

Polismyndigheten och Säkerhetspolisen får ta del av uppgifter genom terminalåtkomst endast i den omfattning och under den tid som behövs för att kontrollera aktuella transporter.

Denna lag träder i kraft den 1 maj 2018.

¹ Senaste lydelse 2014:588.

1.5 Förslag till lag om ändring i säkerhetsskyddslagen (1996:627)

Härigenom föreskrivs att 12 § säkerhetsskyddslagen (1996:627) ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

12 §¹

Med registerkontroll avses att uppgifter hämtas från ett register som omfattas av lagen (1998:620) om belastningsregister, lagen (1998:621) om misstankeregister *eller lagen (2010:362) om polisens allmänna spaningsregister*. Med registerkontroll avses också att uppgifter hämtas som behandlas med stöd av *polisdatalagen* (2010:361).

Med registerkontroll avses att uppgifter hämtas från ett register som omfattas av lagen (1998:620) om belastningsregister *eller* lagen (1998:621) om misstankeregister. Med registerkontroll avses också att uppgifter hämtas som behandlas med stöd av *polisens brottsdatalag* (2010:361) *eller Säkerhetspolisens datalag* (2018:000).

Denna lag träder i kraft den 1 maj 2018.

¹ Senaste lydelse 2010:365.

1.6 Förslag till lag om ändring i lagen (1996:701) om Tullverkets befogenheter vid Sveriges gräns mot ett annat land inom Europeiska unionen

Härigenom föreskrivs att 16 § lagen (1996:701) om Tullverkets befogenheter vid Sveriges gräns mot ett annat land inom Europeiska unionen ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

16 §¹

Transportföretag får lämna uppgifter enligt 15 § på så sätt att de görs läsbara för Tullverket genom terminalåtkomst.

Tullverket får ta del av uppgifter genom terminalåtkomst endast i den omfattning och under den tid som behövs för att kontrollera aktuella transporter. *Tullverket får inte ändra eller på annat sätt bearbeta eller lagra uppgifter som hålls tillgängliga på detta sätt.*

Tullverket får ta del av uppgifter genom terminalåtkomst endast i den omfattning och under den tid som behövs för att kontrollera aktuella transporter.

Uppgifter om enskilda personer som lämnats på annat sätt än genom terminalåtkomst, skall omedelbart förstöras, om de visar sig sakna betydelse för utredning och lagföring av brott.

Denna lag träder i kraft den 1 maj 2018.

¹ Senaste lydelse 1999:434.

1.7 Förslag till lag om ändring i lagen (1998:620) om belastningsregister

Häri genom föreskrivs att 1 b § lagen (1998:620)¹ om belastningsregister ska upphöra att gälla vid utgången av april 2018.

¹ Senaste lydelse av 1 b § 2013:331.

1.8 Förslag till lag om ändring i lagen (1998:621) om misstankeregister

Härigenom föreskrivs att 1 b § lagen (1998:621)¹ om misstankeregister ska upphöra att gälla vid utgången av april 2018.

¹ Senaste lydelse av 1 b § 2013:332.

1.9 Förslag till lag om ändring i lagen (2000:344) om Schengens informationssystem

Härigenom föreskrivs att 5 § lagen (2000:344) om Schengens informationssystem ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

5 §¹

Registret ska endast innehålla uppgifter som har behandlats av behöriga myndigheter i Schengenstaterna, i enlighet med respektive stats nationella lagstiftning.

Polismyndigheten får föra in uppgifter i registret endast om behandling av motsvarande slag av uppgifter är tillåten enligt *personuppgiftslagen* (1998:204), *polisdatalagen* (2010:361) eller annan svensk författning.

Polismyndigheten får föra in uppgifter i registret endast om behandling av motsvarande slag av uppgifter är tillåten enligt *brottsdatalagen* (2018:000), *polisens brottsdatalog* (2010:361) eller annan svensk författning.

Denna lag träder i kraft den 1 maj 2018.

¹ Senaste lydelse 2014:595.

1.10 Förslag till lag om ändring i lagen (2001:184) om behandling av personuppgifter i Kronofogdemyndighetens verksamhet

Härigenom föreskrivs att 1 kap. 3 a § lagen (2001:184)¹ om behandling av personuppgifter i Kronofogdemyndighetens verksamhet ska upphöra att gälla vid utgången av april 2018.

¹ Senaste lydelse av 1 kap. 3 a § 2013:336.

1.11 Förslag till lag om ändring i lagen (2001:185) om behandling av uppgifter i Tullverkets verksamhet

Härigenom föreskivs att 1 kap. 1 och 4 §§ lagen (2001:185) om behandling av uppgifter i Tullverkets verksamhet ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

1 kap.

1 §¹

Denna lag tillämpas vid behandling av personuppgifter i Tullverkets verksamhet, om behandlingen är helt eller delvis automatiserad eller om uppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

Bestämmelserna i 4–6 och 8 §§ samt 2 kap. gäller även vid behandling av uppgifter om juridiska personer.

Bestämmelserna i denna lag gäller inte behandling av *uppgifter* i den brottsbekämpande verksamhet som Tullverket bedriver. *För sådan behandling finns det särskilda bestämmelser i tullbrottsdatalagen (2017:447).*

Bestämmelserna i denna lag gäller inte *vid* behandling av *personuppgifter* i den brottsbekämpande verksamhet som Tullverket bedriver.

4 §²

Uppgifter får behandlas för tillhandahållande av information som behövs hos Tullverket för

1. bestämmande, redovisning, betalning och återbetalning av tull, annan skatt och avgifter,

2. övervakning, revision och annan analys- eller kontrollverksamhet,

¹ Senaste lydelse 2017:449.

² Senaste lydelse 2017:449.

3. fullgörande av ett åliggande som följer av ett för Sverige bindande internationellt åtagande, och

4. tillsyn, kontroll, uppföljning och planering av verksamheten.

Uppgifter som behandlas enligt första stycket får även behandlas för tillhandahållande av information som behövs i Tullverkets brottsbekämpande verksamhet enligt 2 kap. 5 § *tullbrottsdatalagen* (2017:447).

Uppgifter som behandlas enligt första stycket får även behandlas för tillhandahållande av information som behövs i Tullverkets brottsbekämpande verksamhet enligt 2 kap. 1 § *Tullverkets brottsdatalag* (2017:447).

Denna lag träder i kraft den 1 maj 2018.

1.12 Förslag till lag om ändring i lagen (2001:617) om behandling av personuppgifter inom kriminalvården

Härigenom föreskrivs i fråga om lagen (2001:617) om behandling av personuppgifter inom kriminalvården

dels att 1–16 §§ ska upphöra att gälla,

dels att rubrikerna före 1–10 §§ och 12 § ska utgå,

dels att det ska införas fyra nya kapitel, 1–4 kap., av följande lydelse,

dels att rubriken till lagen ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

Lag om behandling av personuppgifter inom kriminalvården

Kriminalvårdens brottsdatalag

1 kap. Allmänna bestämmelser

Lagens tillämpningsområde

1 § Denna lag gäller utöver brottsdatalagen (2018:000) när någon av myndigheterna inom kriminalvården i egenskap av behörig myndighet behandlar personuppgifter i syfte att verkställa häktning eller straffrättsliga påföljder eller biträda en annan behörig myndighet när den utför arbetsuppgifter för något av de syften som anges i 1 kap. 2 § brottsdatalagen.

Personuppgiftsansvar

2 § Kriminalvården är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför.

En övervakningsnämnd är personuppgiftsansvarig för den behandling av personuppgifter som nämnden utför.

2 kap. Grundläggande bestämmelser om behandling

Tillåtna rättsliga grunder för behandling av personuppgifter

1 § Personuppgifter får behandlas om det är nödvändigt för att utföra en arbetsuppgift i syfte att

1. verkställa häktning eller straffrättsliga påföljder,
2. förebygga, förhindra eller upptäcka brottslig verksamhet i samband med sådan verkställighet som anges i 1,
3. biträda andra myndigheter när de fullgör arbetsuppgifter för något av de syften som anges i 1 kap. 2 § brottsdatalagen (2018:000), eller

4. fullgöra förpliktelser som följer av internationella åtaganden.

Arbetsuppgiften ska framgå av en bindande unionsrättsakt eller av en lag, en förordning eller ett särskilt beslut i vilket regeringen uppdragit åt myndigheten att ansvara för en sådan uppgift.

2 § Förutsättningarna för att behandla personuppgifter, som behandlas med stöd av 1 §, för nya ändamål regleras i 2 kap. 4 och 22 §§ brottsdatalagen (2018:000).

Känsliga personuppgifter

3 § Kriminalvården får behandla biometriska uppgifter enligt de förutsättningar som anges i 2 kap. 12 § brottsdatalagen (2018:000).

Utlämnande av personuppgifter

4 § Kriminalvården får till en utländsk myndighet eller internationell organisation lämna ut de personuppgifter som behövs för

1. prövning och genomförande av överflyttning av straffverkställighet,
2. transitering och förvaring av en person som är frihetsberövad för brottsbekämpning, lagföring eller verkställighet av straff, eller
3. tillfällig överflyttning av en frihetsberövad person för brottsbekämpning, lagföring eller straffverkställighet.

Längsta tid som personuppgifter får behandlas

5 § Trots det som sägs i 2 kap. 17 § andra stycket brottsdatalagen (2018:000) får personuppgifter som behandlas automatiserat inte behandlas längre än tio år efter det att den senaste påföljden eller åtgärden avseende den registrerade helt har verkställts eller upphört.

I 3 kap. 7 § finns bestämmelser om hur länge personuppgifter i säkerhetsregistret får behandlas.

Föreskrifter

6 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om

1. vilka personuppgifter som får behandlas enligt 1 §,
2. utlämnande av personuppgifter i andra fall än som anges i 4 §,
3. frågor som rör elektroniskt utlämnande genom direktåtkomst,
4. längsta tid som personuppgifter får behandlas, och
5. att personuppgifter, med avvikelse från 5 §, får behandlas under längre tid för arkivändamål av allmänt intresse och vetenskapliga, statistiska eller historiska ändamål.

3 kap. Säkerhetsregistret

Rätten att föra register

1 § Kriminalvården får föra ett säkerhetsregister. I säkerhetsregistret får personuppgifter behandlas i syfte att

1. förebygga, förhindra eller upptäcka brott eller brottslig verksamhet på häkten och i kriminalvårdsanstalter eller i samband med annan straffverkställighet, och
2. säkerställa ordning och säkerhet på häkten, i kriminalvårdsanstalter och annan verksamhet som Kriminalvården bedriver.

Innehåll

2 § I säkerhetsregistret får uppgifter behandlas om en person som är häktad eller verkställer fängelsestraff och som är eller har varit placerad på säkerhetsavdelning.

I registret får även uppgifter behandlas om en person som är häktad eller verkställer fängelsestraff, om det finns risk för att han eller hon

1. under häktning eller verkställighet av fängelsestraff begår brott som inte är ringa eller deltar i brottslig verksamhet som innefattar brott för vilket det är föreskrivet fängelse i två år eller däröver,

2. förbereder rymning eller försöker rymma,

3. blir föremål för fritagning,

4. medverkar i eller på annat sätt bidrar till att allvarligt störa ordningen eller säkerheten på ett häkte eller i en kriminalvårdsanstalt, eller

5. utsätts för våld eller hot under verkställigheten.

3 § I säkerhetsregistret får även uppgifter behandlas om en person som verkställer en påföljd inom kriminalvården, om det finns risk för att han eller hon utövar våld eller hot mot eller otillbörlig påverkan på personal eller andra personer som uppehåller sig i kriminalvårdens lokaler.

4 § Om det är absolut nödvändigt för ändamålet med behandlingen enligt 1 §, får Kriminalvården i säkerhetsregistret behandla uppgifter om en person som har personlig anknytning till eller annan nära förbindelse med en person som anges i 2 §. Om den förstnämnde inte är häktad eller verkställer fängelsestraff ska det framgå genom en särskild upplysning.

Sökning

5 § Sökförbudet i 2 kap. 14 § brottsdatalagen (2018:000) hindrar inte sökning i personuppgifter i säkerhetsregistret i syfte att få fram ett personurval grundat på etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller uppgifter som rör hälsa, sexualliv eller sexuell läggning.

Direktåtkomst

6 § Polismyndigheten, Säkerhetspolisen, Ekobrottsmyndigheten och Åklagarmyndigheten får medges direktåtkomst till personuppgifter i säkerhetsregistret för något av de syften som anges i 1 kap. 2 § brottsdatalagen (2018:000).

Längsta tid som personuppgifter får behandlas

7 § Trots det som sägs i 2 kap. 17 § andra stycket brottsdatalagen (2018:000) får personuppgifter i säkerhetsregistret inte behandlas längre än fem år efter det att den registrerade blivit villkorligt frigiven från ett fängelsestraff eller annars helt har verkställt straffet eller, utan att ha dömts till sådan påföljd, har frigetts från häkte.

Föreskrifter

8 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om innehållet i säkerhetsregistret och om utlämnande av personuppgifter ur registret.

4 kap. Administrativa sanktionsavgifter och rättsmedel

Administrativa sanktionsavgifter

1 § Sanktionsavgift får tas ut av den personuppgiftsansvarige vid överträdelse av bestämmelserna i

1. 2 kap. 1 § om tillåtna rättsliga grunder för behandling av personuppgifter,
2. 3 kap. 4 § om särskild upplysning, eller
3. 2 kap. 5 § eller 3 kap. 7 § om längsta tid som personuppgifter får behandlas.

Sanktionsavgift får också tas ut vid överträdelse av föreskrifter som har meddelats i anslutning till denna lag om särskild upplysning eller om längsta tid som personuppgifter får behandlas.

Sanktionsavgiften ska vara minst 50 000 kronor och högst 20 000 000 kronor.

Skadestånd

2 § Vid behandling av personuppgifter enligt denna lag eller föreskrifter som har meddelats i anslutning till den ska bestämmelsen i 7 kap. 1 § brottsdatalagen (2018:000) om skadestånd tillämpas på motsvarande sätt.

Överklagande

3 § Bestämmelser om överklagande och om vilka beslut som får överklagas finns i 7 kap. brottsdatalagen (2018:000).

-
1. Denna lag träder i kraft den 1 maj 2018.
 2. Sanktionsavgift enligt 4 kap. 1 § får beslutas endast för överträdelser som har begåtts efter ikraftträdandet.
 3. Äldre bestämmelser ska gälla för överträdelser som har begåtts före ikraftträdandet.
 4. Äldre föreskrifter gäller fortfarande för överklagande av beslut som meddelats före ikraftträdandet och som rör behandling av personuppgifter vid verkställighet av häktning eller straffrättsliga påföljder eller biträde till andra behöriga myndigheter.
 5. Bestämmelsen om skadestånd i 48 § personuppgiftslagen (1998:204) gäller fortfarande för skada som har orsakats före ikraftträdandet vid behandling av personuppgifter enligt denna lag eller föreskrifter som har meddelats i anslutning till den.

1.13 Förslag till lag om ändring i lagen (2005:321) om tillträdesförbud vid idrottsarrangemang

Härigenom föreskrivs att 8 a § lagen (2005:321) om tillträdesförbud vid idrottsarrangemang ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

8 a §¹

En polisman eller annan anställd vid Polismyndigheten får fotografera en person som har eller skäligen kan antas få tillträdesförbud enligt denna lag i syfte att fotografiet ska kunna tillföras det register som Polismyndigheten får föra enligt *lagen (2015:51) om register över tillträdesförbud vid idrottsarrangemang*.

En polisman eller annan anställd vid Polismyndigheten får fotografera en person som har eller skäligen kan antas få tillträdesförbud enligt denna lag i syfte att fotografiet ska kunna tillföras det register som Polismyndigheten får föra enligt *5 kap. polisens brottsdatalog (2010:361)*.

Denna lag träder i kraft den 1 maj 2018.

¹ Senaste lydelse 2015:55.

1.14 Förslag till lag om ändring i lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet

Härigenom föreskrivs att 1, 3 och 4 §§ lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet ska ha följande lydelse.

Lydelse enligt SOU 2016:65

Föreslagen lydelse

1 §

Säkerhets- och integritetsskyddsnämnden (nämnden) ska utöva tillsyn över brottsbekämpande myndigheters användning av hemliga tvångsmedel och kvalificerade skyddsidentiteter och därmed sammanhängande verksamhet.

Nämnden ska även utöva tillsyn över *behandlingen* av personuppgifter i *Säkerhetspolisens* brottsbekämpande verksamhet. Tillsynen ska särskilt avse sådan behandling som avses i 2 kap. 10 § *polisdatalagen* (2010:361).

Nämnden ska även utöva tillsyn över *Säkerhetspolisens behandling* av personuppgifter som rör *nationell säkerhet* i brottsbekämpande och lagförande verksamhet. Tillsynen ska särskilt avse sådan behandling som avses i 2 kap. 9 och 10 §§ *Säkerhetspolisens datalag* (2018:000).

Tillsynen ska särskilt syfta till att säkerställa att verksamhet enligt första och andra styckena bedrivs i enlighet med lag eller annan författning.

Nuvarande lydelse

Föreslagen lydelse

3 §

Nämnden är skyldig att på begäran av en enskild kontrollera om han eller hon har utsatts för sådana tvångsmedel *eller varit föremål för sådan person-*

Nämnden är skyldig att på begäran av en enskild kontrollera om han eller hon

1. har utsatts för sådana tvångsmedel som avses i 1 § och

uppgiftsbehandling som avses i 1 § och om användningen av *tvångsmedel* och därmed sammanhängande verksamhet *eller behandlingen av personuppgifter* har skett i enlighet med lag eller annan författning. *Nämnden skall underrätta den enskilde om att kontrollen har utförts.*

om användningen av *dem* och därmed sammanhängande verksamhet har *varit* i enlighet med lag eller annan författning, *eller*

2. *varit föremål för sådan personuppgiftsbehandling som avses i 1 § och om den har utförts i enlighet med lag eller annan författning.*

Nämnden ska underrätta den enskilde om att kontrollen har utförts.

Nämnden får vägra att utföra kontroll om begäran är orimlig eller uppenbart ogrundad.

4 §

Nämnden har rätt att av förvaltningsmyndigheter som omfattas av tillsynen få de uppgifter och det biträde som nämnden begär. Även domstolar samt de förvaltningsmyndigheter som inte omfattas av tillsynen är skyldiga att lämna nämnden de uppgifter som den begär.

Nämnden har rätt att av förvaltningsmyndigheter som omfattas av tillsynen få de uppgifter och *upplysningar, den information* och det biträde som nämnden begär. Även domstolar och de förvaltningsmyndigheter som inte omfattas av tillsynen är skyldiga att lämna nämnden de uppgifter som den begär.

Denna lag träder i kraft den 1 maj 2018.

1.15 Förslag till lag om ändring i offentlighets- och sekretesslagen (2009:400)

Härigenom föreskrivs att 18 kap. 2 och 18 §§, 35 kap. 1, 4 a, 4 b §, 10 och 10 b §§ och 37 kap. 7 § offentlighets- och sekretesslagen (2009:400) ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

18 kap.

2 §¹

Sekretess gäller för uppgift som hänför sig till sådan verksamhet som avses i 2 kap. 7 § 1 eller 6 kap. 1 § 1 polisdatalagen (2010:361), om det inte står klart att uppgiften kan röjas utan att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas.

Sekretess gäller, under motsvarande förutsättningar som anges i första stycket, för uppgift som hänför sig till

1. *sådan verksamhet som avses i 2 kap. 5 § 1 skattebrottsdatalagen (2017:452),*

2. *sådan verksamhet som avses i 2 kap. 5 § 1 tullbrottsdatalagen (2017:447), eller*

3. *sådan verksamhet som avses i 3 kap. 2 § 1 kustbevaknings-*

Sekretess gäller för uppgift som hänför sig till sådan verksamhet som avses i 2 kap. 1 § första stycket 1 polisens brottsdatalag (2010:361) eller 2 kap. 1 § första stycket 1 Säkerhetspolisens datalag (2018:000), om det inte står klart att uppgiften kan röjas utan att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas.

Sekretess gäller, under motsvarande förutsättningar som anges i första stycket, för uppgift som hänför sig till *sådan verksamhet som avses i*

1. *2 kap. 1 § första stycket 1 Kustbevakningens brottsdatalag (2012:145),*

2. *2 kap. 1 § första stycket 1 Tullverkets brottsdatalag (2017:447), eller*

3. *2 kap. 1 § första stycket 1 Skatteverkets brottsdatalag*

¹ Senaste lydelse 2017:456.

datalagen (2012:145). (2017:452).

Sekretess enligt första stycket gäller inte för uppgift som hänförs till verksamhet hos Säkerhetspolisen och som har förts in i en allmän handling före år 1949.

För uppgift i en allmän handling gäller sekretessen i högst sjuttio år.

18 §²

Sekretessen enligt 17 § andra stycket hindrar inte att en uppgift lämnas ut enligt vad som föreskrivs i lagen (2000:344) om Schengens informationssystem och *polisdatalagen* (2010:361).

Sekretessen enligt 17 § andra stycket hindrar inte att en uppgift lämnas ut enligt vad som föreskrivs i lagen (2000:344) om Schengens informationssystem och *polisens brottsdatalag* (2010:361).

Lydelse enligt prop. 2016/17:208 Föreslagen lydelse

35 kap.

1 §

Sekretess gäller för uppgift om en enskilds personliga och ekonomiska förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till honom eller henne lider skada eller men och uppgiften förekommer i

1. utredning enligt bestämmelserna om förundersökning i brottmål,

2. angelägenhet som avser användning av tvångsmedel i brottmål eller i annan verksamhet för att förebygga brott,

3. angelägenhet som avser registerkontroll och särskild personutredning enligt säkerhetsskyddslagen (1996:627),

4. annan verksamhet som syftar till att förebygga, uppdaga, utreda eller beivra brott och som bedrivs av en åklagarmyndighet, Polismyndigheten, Säkerhetspolisen, Skatteverket, Tullverket eller Kustbevakningen,

5. register som förs av Polismyndigheten enligt 4 kap. *polisdatalagen* (2010:361) eller som

5. register som förs av Polismyndigheten enligt 5 kap. *polisens brottsdatalag* (2010:361) eller

² Senaste lydelse 2010:369.

annars behandlas med stöd av de bestämmelserna eller uppgifter som behandlas av Säkerhetspolisen med stöd av *6 kap. samma lag*,

6. register som förs enligt lagen

7. register som förs av Skatteverket enligt *skattebrottsdatalagen* (2017:452) eller som annars behandlas där med stöd av samma lag,

8. särskilt ärenderegister över brottmål som förs av åklagarmyndighet, om uppgiften inte hänför sig till registrering som avses i 5 kap. 1 §,

9. register som förs av Tullverket enligt *tullbrottsdatalagen* (2017:447) eller som annars behandlas där med stöd av samma lag, *eller*

10. register som förs enligt *lagen* (2010:362) om polisens allmänna spaningsregister.

Sekretessen enligt första stycket 2 gäller hos domstol i dess rättsskipande eller rättsvårdande verksamhet endast om det kan antas att den enskilde eller någon närstående till honom eller henne lider skada eller men om uppgiften röjs. Vid förhandling om användning av tvångsmedel gäller sekretess för uppgift om vem som är misstänkt endast om det kan antas att fara uppkommer för att den misstänkte eller någon närstående till honom eller henne utsätts för våld eller lider annat allvarligt men om uppgiften röjs.

Första stycket gäller inte om annat följer av 2, 6 eller 7 §.

För uppgift i en allmän handling gäller sekretessen i högst sjuttio år.

som annars behandlas med stöd av de bestämmelserna, eller uppgifter som behandlas av Säkerhetspolisen med stöd av *Säkerhetspolisens datalag* (2018:000),

(1998:621) om misstankeregister,

7. register som förs av Skatteverket enligt *Skatteverkets brottsdatalag* (2017:452) eller som annars behandlas där med stöd av samma lag,

8. särskilt ärenderegister över brottmål som förs av åklagarmyndighet, om uppgiften inte hänför sig till registrering som avses i 5 kap. 1 §, *eller*

9. register som förs av Tullverket enligt *Tullverkets brottsdatalag* (2017:447) eller som annars behandlas där med stöd av samma lag.

*Nuvarande lydelse**Föreslagen lydelse*4 a §³

Sekretess gäller i verksamhet som avser förande av *register enligt lagen (2015:51) om register över tillträdesförbud vid idrottsarrangemang* för uppgift om en enskilds personliga förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till *denne* lider men.

För uppgift i en allmän handling gäller sekretessen i högst sjuttio år.

Sekretess gäller i verksamhet som avser förande av *tillträdesförbudsregistret enligt 5 kap. polisens brottsdatalog (2010:361)* för uppgift om en enskilds personliga förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till *honom eller henne* lider men.

*Lydelse enligt SOU 2017:29**Föreslagen lydelse*

4 b §

Sekretess gäller hos en behörig myndighet enligt brottsdatalogen (2018:000) för uppgift i ett sådant personurval som avses i 2 kap. 14 § samma lag.

För uppgift i en allmän handling gäller sekretessen högst sjuttio år.

Sekretess gäller hos
1. en behörig myndighet enligt brottsdatalogen (2018:000) för uppgift i ett sådant personurval som avses i 2 kap. 14 § samma lag, och

2. *Säkerhetspolisen* för uppgift i ett sådant personurval som avses i 2 kap. 12 § *Säkerhetspolisens datalog (2018:000)*.

För uppgift i en allmän handling gäller sekretessen i högst sjuttio år.

³ Senaste lydelse 2015:53.

*Nuvarande lydelse**Föreslagen lydelse*10 §⁴

Sekretessen enligt 1 § hindrar inte att en uppgift lämnas ut

1. till en enskild enligt vad som föreskrivs i lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare,

2. till en enskild enligt vad som föreskrivs i säkerhets- skyddslagen (1996:627) *samt* i förordning som har meddelats med stöd i den lagen,

2. till en enskild enligt vad som föreskrivs i säkerhets- skyddslagen (1996:627) *och* i förordning som har meddelats med stöd i den lagen,

3. till en enskild enligt vad som föreskrivs i 27 kap. 8 § rättegångsbalken,

3. enligt vad som föreskrivs i – lagen (1998:621) om misstankeregister,

– *polisdatalagen* (2010:361),

4. enligt vad som föreskrivs i – *polisens brottsdatalag* (2010:361),

– *skattebrottsdatalagen*

(2017:452),

– *Kustbevakningens brottsdata-*

lag (2012:145),

– *tullbrottsdatalagen*

(2017:447),

– *åklagarväsendets brottsdata-*

lag (2015:433),

– *kustbevakningsdatalagen*

(2012:145),

– *Tullverkets brottsdatalag*

(2017:447),

– *åklagardatalagen*

(2015:433),

– *Skattverkets brottsdatalag*

(2017:452),

– *Säkerhetspolisens datalag*

(2018:000), *eller*

– förordningar som har stöd i dessa lagar, *eller*

– förordningar som har stöd i dessa lagar.

4. till en enskild enligt vad som föreskrivs i 27 kap. 8 § rättegångsbalken.

⁴ Senaste lydelse 2017:456.

10 b §⁵

Sekretessen enligt 4 a § hindrar inte att en uppgift lämnas ut enligt vad som föreskrivs i *lagen (2015:51) om register över tillträdesförbud vid idrottsarrangemang*.

Sekretessen enligt 4 a § hindrar inte att en uppgift lämnas ut till en idrottsorganisation enligt vad som föreskrivs i 2 kap. 14 § *polisens brottsdatalag (2010:361)*.

37 kap.

7 §⁶

Sekretessen enligt 6 § hindrar inte att uppgift lämnas ut enligt vad som föreskrivs i *lagen (2000:344) om Schengens informationssystem och polisdatalagen (2010:361)*.

Sekretessen enligt 6 § hindrar inte att uppgift lämnas ut enligt vad som föreskrivs i *lagen (2000:344) om Schengens informationssystem och polisens brottsdatalag (2010:361)*.

-
1. Denna lag träder i kraft den 1 maj 2018.
 2. Äldre bestämmelser gäller fortfarande för uppgifter i handlingar som har omhändertagits för arkivering före ikraftträdandet av denna lag.

⁵ Senaste lydelse 2015:53.

⁶ Senaste lydelse 2010:369.

1.16 Förslag till lag om ändring i polisdatalagen (2010:361)

Härigenom föreskrivs i fråga om polisdatalagen (2010:361)

dels att 1, 2, 4 och 6 kap. ska upphöra att gälla,

dels att 3 kap. 5 och 9–15 §§ och 5 kap. 4–6 §§, ska upphöra att gälla,

dels att rubrikerna före 3 kap. 8, 9 och 14 §§ och 5 kap. 4 och 5 §§ ska utgå,

dels att nuvarande 4 kap. ska betecknas 5 kap. och nuvarande 5 kap. ska betecknas 6 kap.,

dels att nuvarande 3 kap. 6 § ska betecknas 3 kap. 5 §, att nuvarande 3 kap. 7 § ska betecknas 3 kap. 6 §, att nuvarande 3 kap. 8 § ska betecknas 3 kap. 7 § och att rubriken före nuvarande 3 kap. 8 § ska placeras före nya 3 kap. 7 §, att nuvarande 5 kap. 7 § ska betecknas 6 kap. 6 § och att rubriken före nuvarande 5 kap. 6 § ska placeras före nya 6 kap. 6 §, att nuvarande 5 kap. 8 § ska betecknas 6 kap. 7 § och att rubriken före nuvarande 5 kap. 8 § ska placeras före nya 6 kap. 7 § och att nuvarande 5 kap. 9 § ska betecknas 6 kap. 9 §,

dels att 3 kap. 1–4 §§ och nya 3 kap. 5–7 §§ och 6 kap. 3 och 6–8 §§ ska ha följande lydelse,

dels att det ska införas sex nya paragrafer, 3 kap. 8 och 9 §§ och 6 kap. 4, 5, 8 och 10 §§, och nya rubriker före 3 kap. 1 § och före nya 3 kap. 8 §, 6 kap. 4 och 9 §§ av följande lydelse,

dels att det ska införas fem nya kapitel i lagen, 1, 2, 4, 5 och 7 kap., av följande lydelse,

dels att rubriken till lagen ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

Polisdatalag

Polisens brottsdatalag

1 kap. Allmänna bestämmelser

Lagens tillämpningsområde

1 § Denna lag gäller utöver brottsdatalagen (2018:000) när någon av följande myndigheter i egenskap av behörig myndighet behandlar personuppgifter.

1. Polismyndigheten, om uppgifterna behandlas i syfte att bekämpa eller lagföra brott eller upprätthålla allmän ordning och säkerhet.

2. Ekobrottsmyndigheten, om uppgifterna behandlas i syfte att utreda brott och det inte är fråga om åklagarverksamhet.

3. Säkerhetspolisen i frågor som inte rör nationell säkerhet, om uppgifterna behandlas i syfte att bekämpa och lagföra brott.

För Ekobrottsmyndigheten och Säkerhetspolisen gäller endast 1–4 och 7 kap.

2 § Denna lag gäller inte vid behandling av personuppgifter enligt

1. lagen (1998:620) om belastningsregister,
2. lagen (1998:621) om misstankeregister,
3. lagen (2000:344) om Schengens informationssystem,
4. lagen (2006:444) om passagerarregister, eller
5. lagen (2014:400) om Polismyndighetens elimineringsdatabas.

3 § I lagen (2017:496) om internationellt polisiärt samarbete och i föreskrifter som regeringen har meddelat i anslutning till den lagen, finns det särskilda bestämmelser om behandling av personuppgifter som följer av internationella överenskommelser. Om det i dessa författningar finns avvikande bestämmelser, ska de tillämpas i stället för bestämmelserna i denna lag.

Personuppgiftsansvar

4 § Polismyndigheten är personuppgiftsansvarig för den behandling av personuppgifter som utförs vid myndigheten och för den behandling som myndigheten utför vid Ekobrottsmyndigheten i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet.

Ekobrottsmyndigheten är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför i syfte att utreda brott.

Säkerhetspolisen är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför.

Uttryck i lagen

5 § I denna lag avses med

dna-analys: varje förfarande som kan användas för analys av deoxyribonukleinsyra i humant material,

dna-profil: resultatet av en dna-analys som presenteras i form av siffror eller bokstäver, och

fingeravtryck: avtryck av finger eller hand.

Lagens tillämpning på uppgifter om juridiska personer

6 § Bestämmelserna om personuppgifter i följande paragrafer gäller också vid behandling av uppgifter om juridiska personer:

1. 4 § om personuppgiftsansvar,

2. 2 kap. 1 § om tillåtna rättsliga grunder för behandling av personuppgifter,

3. 3 kap. 2 § om gemensamt tillgängliga uppgifter,

4. 4 kap. 1–4 och 6–10 §§ om längsta tid som personuppgifter får behandlas,

5. 5 kap. 18–20 §§ om behandling av personuppgifter i penningtvättsregister, och

6. 5 kap. 21 och 22 §§ om behandling av personuppgifter i det internationella registret.

Bestämmelserna om personuppgifter i följande paragrafer i brottsdatalagen (2018:000) gäller också vid sådan behandling:

1. 2 kap. 2 § om diarieföring och handläggning i vissa fall,

2. 2 kap. 3 § andra stycket om ändamålet med behandlingen,

3. 2 kap. 17 § om längsta tid som personuppgifter får behandlas,

4. 2 kap. 4 och 22 §§ om behandling för nya ändamål, och

5. 3 kap. 6 § om tillgången till personuppgifter.

Lagens uppbyggnad

7 § I detta kapitel och i 2 kap. finns allmänna bestämmelser om behandling av personuppgifter och i 4 kap. bestämmelser om längsta tid för behandling av personuppgifter. I 7 kap. finns bestämmelser om administrativa sanktionsavgifter och rättsmedel.

För personuppgifter som görs eller har gjorts gemensamt tillgängliga gäller även 3 kap.

För personuppgifter som behandlas i register över dna-profiler, fingeravtrycks- och signalementsregister, penningtvätsregister, det internationella registret och tillträdesförbudsregistret, gäller 5 kap. i stället för 3 och 4 kap.

I 6 kap. finns bestämmelser om Polismyndighetens behandling av personuppgifter för forensiska ändamål. Vid sådan behandling gäller 6 kap. i stället för 2–4 kap.

2 kap. Grundläggande bestämmelser om behandling

Tillåtna rättsliga grunder för behandling av personuppgifter

1 § Personuppgifter får behandlas om det är nödvändigt för att utföra en arbetsuppgift i syfte att

1. förebygga, förhindra eller upptäcka brottslig verksamhet,
2. utreda eller lagföra brott,
3. upprätthålla allmän ordning och säkerhet, eller
4. fullgöra förpliktelser som följer av internationella åtaganden.

Arbetsuppgiften ska framgå av en bindande unionsrättsakt eller av en lag, en förordning eller ett särskilt beslut i vilket regeringen uppdragit åt myndigheten att ansvara för en sådan uppgift.

2 § Förutsättningarna för att behandla personuppgifter, som behandlas med stöd av 1 §, för nya ändamål regleras i 2 kap. 4 och 22 §§ brottsdatalagen (2018:000).

Särskilda upplysningar

3 § Bestämmelserna i 2 kap. 3 § andra stycket, 9 och 10 §§ brottsdatalagen (2018:000) om särskild upplysning gäller endast vid behandling av personuppgifter som har gjorts gemensamt tillgängliga med stöd av 3 kap. 2 §.

Känsliga personuppgifter

4 § Polismyndigheten och Säkerhetspolisen får behandla biometrisk uppgifter enligt de förutsättningar som anges i 2 kap. 12 § brottsdatalagen (2018:000).

5 § Sökförbudet i 2 kap. 14 § brottsdatalagen (2018:000) hindrar inte att brottsrubriceringar, uppgifter om tillvägagångssätt vid brott, uppgifter om verkställighet av påföljd eller uppgifter som beskriver en persons utseende används vid sökning.

6 § Sökförbudet i 2 kap. 14 § brottsdatalagen (2018:000) hindrar inte sökningar i syfte att få fram ett personurval grundat på etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening eller uppgifter som rör hälsa, sexualliv eller sexuell läggning, om sökningen görs i personuppgifter som inte har gjorts gemensamt tillgängliga.

Utlämnande av personuppgifter

7 § Om det är förenligt med svenska intressen, får personuppgifter lämnas ut till

1. Interpol,
2. Europol, eller
3. en polismyndighet eller åklagarmyndighet i en stat som är ansluten till Interpol.

Personuppgifter får lämnas ut enligt första stycket endast om mottagaren behöver uppgifterna för något av de syften som anges i 1 §.

Personuppgifter får vidare lämnas ut till en utländsk myndighet eller mellanfolklig organisation, om utlämnandet följer av en internationell överenskommelse som Sverige har tillträtt efter riksdagens godkännande.

8 § Polismyndigheten, Säkerhetspolisen, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket har, trots sekretess enligt 21 kap. 3 § första stycket och 35 kap. 1 § offentlighets- och sekretesslagen (2009:400), rätt att ta del av personuppgifter som har gjorts gemensamt tillgängliga med stöd av

3 kap. 2 §, om den mottagande myndigheten behöver uppgifterna för något av de syften som anges i 1 kap. 2 § brottsdatalagen (2018:000).

Första stycket gäller inte uppgifter som behandlas i särskilda register enligt 5 kap.

9 § Säkerhetspolisen, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket och Kustbevakningen har, trots sekretess enligt 21 kap. 3 § första stycket och 35 kap. 1 § offentlighets- och sekretesslagen (2009:400), rätt att ta del av uppgifter om huruvida personer förekommer i register över dna-profiler som regleras i 5 kap., om den mottagande myndigheten behöver uppgifterna för något av de syften som anges i 1 kap. 2 § brottsdatalagen (2018:000).

10 § Säkerhetspolisen, Ekobrottsmyndigheten, Tullverket, Kustbevakningen och Skatteverket har, trots sekretess enligt 21 kap. 3 § första stycket och 35 kap. 1 § offentlighets- och sekretesslagen (2009:400), rätt att ta del av personuppgifter som behandlas i fingeravtrycks- och signalementsregister enligt 5 kap., om den mottagande myndigheten behöver uppgifterna för något av de syften som anges i 1 kap. 2 § brottsdatalagen (2018:000). Migrationsverket har motsvarande rätt att ta del av personuppgifter som behandlas i fingeravtrycks- och signalementsregister, om verket behöver uppgifterna för att kontrollera fingeravtryck som verket tagit.

11 § Trots sekretess enligt 35 kap. 4 a § offentlighets- och sekretesslagen (2009:400) har en idrottsorganisation rätt att ta del av personuppgifter som behandlas i tillträdesförbudsregistret enligt 5 kap., om organisationen behöver uppgifterna för de syften som anges i 5 § lagen (2015:51) om idrottsorganisationers behandling av uppgifter om tillträdesförbud.

12 § Personuppgifter får lämnas ut elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt.

Elektroniskt utlämnande genom direktåtkomst är tillåtet bara i den utsträckning som anges i 3 kap. 7 § och 5 kap. 10 och 17 §§.

Personuppgifter från transportföretag

13 § Personuppgifter som tillhandahålls av transportföretag enligt 25 § polislagen (1984:387) får behandlas för något av de syften som anges i 1 § första stycket 1 och 2.

Personuppgifter som avses i första stycket får endast i ett enskilt fall behandlas för nya ändamål enligt 2 kap. 4 eller 22 § brottsdatalagen (2018:000).

14 § Vid terminalåtkomst enligt 26 § polislagen (1984:387) får personuppgifterna inte ändras eller på annat sätt bearbetas.

15 § Vid sökning i personuppgifter som avses i 13 § första stycket får namn, personnummer, samordningsnummer och andra liknande identitetsbeteckningar användas som sökbegrepp endast om uppgifterna avser en person som

1. är eller har varit misstänkt för brott,
2. är misstänkt för att ha utövat eller komma att utöva sådan brottslig verksamhet som avses i 3 kap. 2 § första stycket 1, eller
3. övervakas under de förutsättningar som anges i 3 kap. 2 § första stycket 2.

Föreskrifter

16 § Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om

1. att personuppgifter får lämnas ut i andra fall än som anges i 7–11 §§, och
2. begränsning av möjligheten att lämna ut personuppgifter elektroniskt enligt 12 § första stycket.

3 kap.

Allmän bestämmelse

1 §

Detta kapitel innehåller särskilda bestämmelser för behandling av personuppgifter som görs eller har gjorts gemensamt

Detta kapitel innehåller särskilda bestämmelser för behandling av personuppgifter som görs eller har gjorts gemensamt

tillgängliga i polisens brottsbekämpande verksamhet. Uppgifter som endast ett fåtal personer har rätt att ta del av anses inte som gemensamt tillgängliga.

Detta kapitel gäller inte när personuppgifter behandlas med stöd av 2 kap. 9 §.

tillgängliga med stöd av 2 §. Uppgifter som endast ett fåtal personer har rätt att ta del av anses inte som gemensamt tillgängliga.

Detta kapitel gäller inte när personuppgifter behandlas med stöd av 2 kap. 2 § brottsdatalagen (2018:000).

2 §¹

Följande personuppgifter får göras gemensamt tillgängliga:

1. Uppgifter som kan antas ha samband med misstänkt brottslig verksamhet, om den misstänkta verksamheten

a) innefattar brott för vilket är föreskrivet fängelse i ett år eller däröver, eller

b) sker systematiskt.

2. Uppgifter som behövs för övervakningen av en person, om han eller hon

a) kan antas komma att begå brott för vilket är föreskrivet fängelse i två år eller däröver, och

b) är allvarligt kriminellt belastad eller kan antas utgöra ett hot mot andras personliga säkerhet.

3. Uppgifter som förekommer i ett ärende om utredning eller beivrande av brott.

4. Uppgifter som behövs för att fullgöra vad som följer av internationella åtaganden, om det krävs för att den aktuella förpliktelsen ska kunna fullgöras.

5. Uppgifter som har rapporterats till Polismyndighetens ledningscentraler.

a) innefattar brott för vilket det är föreskrivet fängelse i ett år eller däröver, eller

2. Uppgifter som behövs för övervakningen av en person som

a) kan antas komma att begå brott för vilket det är föreskrivet fängelse i två år eller däröver och

3. Uppgifter som förekommer i ett ärende om utredning av eller lagföring för brott.

4. Uppgifter som förekommer i ett ärende om kontaktförbud eller om personskydd.

¹ Senaste lydelse 2014:597.

6. Uppgifter som behandlas i syfte att upprätthålla allmän ordning och säkerhet.

7. Uppgifter som behandlas i syfte att fullgöra internationella åtaganden, om det krävs för att den aktuella förpliktelsen ska kunna fullgöras.

DNA-profiler får inte göras gemensamt tillgängliga. Att sådana uppgifter får behandlas i särskilda register följer av 4 kap.

Dna-profiler får inte göras gemensamt tillgängliga. Att sådana uppgifter får behandlas i särskilda register följer av 5 kap.

Tillgången till uppgifter som görs gemensamt tillgängliga med stöd av första stycket 2 ska begränsas till särskilt angivna tjänstemän som har till uppgift att arbeta med övervakningen. Information om att en person är föremål för övervakning får dock göras tillgänglig för andra.

3 §

Vid behandling enligt 1 § ska det genom en särskild upplysning eller på något annat sätt framgå för vilket närmare ändamål personuppgifterna behandlas. Har uppgifterna gjorts gemensamt tillgängliga med stöd av 2 § första stycket 2 eller 5, ska detta särskilt framgå.

Det ska framgå genom en särskild upplysning eller på något annat sätt om personuppgifter har gjorts gemensamt tillgängliga med stöd av 2 § första stycket 2 eller 5.

4 §

Om uppgifter, som behandlas enligt 1 §, direkt kan hänföras till en person som inte är misstänkt för brott eller för att ha utövat eller komma att utöva sådan brottslig verksamhet som avses i 2 § första stycket 1, ska det genom en särskild upplysning eller på något annat sätt framgå

Om uppgifter som är gemensamt tillgängliga direkt kan hänföras till en person som inte är misstänkt för att ha utövat eller komma att utöva sådan brottslig verksamhet som avses i 2 § första stycket 1, ska det genom en särskild upplysning eller på något annat sätt framgå

att personen inte är misstänkt.

Uppgifter om en person som kan antas ha samband med *misstänkt* brottslig verksamhet ska förse med en upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak, om inte *detta* på grund av *särskilda omständigheter* är onödigt. *Detsamma gäller uppgifter om personer som avses i 2 § första stycket 2.*

att personen inte är misstänkt.

Uppgifter om en person som kan antas ha *direkt* samband med *sådan* brottslig verksamhet som avses i 2 § första stycket 1 eller som övervakas med stöd av 2 § första stycket 2 ska förse med en upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak, om det inte på grund av *omständigheterna* är onödigt.

5 §

Vid sökning på namn, personnummer, samordningsnummer eller andra liknande identitetsbeteckningar i uppgifter som har gjorts gemensamt tillgängliga får sådana uppgifter tas fram som anger att den sökta personen

1. är anmäld för brott,
2. är eller har varit misstänkt för brott,
3. är misstänkt för att ha utövat eller komma att utöva sådan brottslig verksamhet som avses i 2 § första stycket 1,
4. övervakas enligt 2 § första stycket 2,
5. har anmält ett brott,
6. är målsägande i ett ärende som rör ansvar för brott,

7. förekommer i ett ärende som vittne eller annan som lämnar eller har lämnat uppgifter eller yttrande,

8. har gett in eller tillhandahållits en handling,

Vid sökning i *automatiserade behandlingssystem* på namn, personnummer, samordningsnummer eller andra liknande identitetsbeteckningar i uppgifter som har gjorts gemensamt tillgängliga får *endast* sådana uppgifter tas fram som anger att den sökta personen

7. berörs av ett *kontaktförbud* eller av *åtgärder i ett personskyddsärende*,

8. förekommer i ett ärende som vittne eller annan som lämnar eller har lämnat uppgifter eller yttrande,

9. har gett in eller tillhandahållits en handling,

9. är anmäld *såsom* försvunnen,
10. har bedömts kunna komma att möta ett polisingripande med grovt våld, eller

11. är efterlyst.

Regeringen eller den myndighet som regeringen bestämmer meddelar föreskrifter om begränsning av tillgången till sådana uppgifter som avses i första stycket.

10. är anmäld *som* försvunnen,
11. har bedömts kunna komma att möta ett polisingripande med grovt våld, eller

12. är efterlyst.

6 §

Bestämmelserna i 6 § gäller inte vid

1. sökning i en viss handling eller i ett visst ärende, *eller*

2. sökning i en uppgiftssamling som har skapats för att undersöka viss brottslighet eller vissa kriminella grupperingar och som enbart de som arbetar i undersökningen har åtkomst till.

Bestämmelserna i 6 § gäller inte heller vid sökning som utförs av särskilt angivna tjänstemän och som görs

1. för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott för vilket är föreskrivet fängelse i fyra år eller däröver eller för sådant ändamål som avses i 2 § första stycket 2, *eller*

2. för att utreda brott för vilket är föreskrivet fängelse i fyra

Bestämmelserna i 5 § gäller inte vid sökning i en viss handling eller i ett visst ärende.

Bestämmelserna i 5 § gäller inte heller vid sökning som görs av särskilt angivna tjänstemän

1. när de utför beredningsuppgifter i underrättelseverksamhet och arbetet befinner sig i ett inledande skede,

2. i syfte att i underrättelseverksamhet bearbeta och analysera personuppgifter som har gjorts gemensamt tillgängliga med stöd av 2 § första stycket 1 eller 2 och som enbart dessa tjänstemän har tillgång till,

3. i syfte att utreda brott för vilket det är föreskrivet fängelse

år eller däröver.

i fyra år eller däröver, eller

4. i syfte att samordna utredningar om brott som kan vara systematiska och för vilka det är föreskrivet fängelse i två år eller däröver.

Bestämmelserna i 5 § gäller inte heller vid sökning som en tjänsteman vid någon av Polismyndighetens ledningscentraler utför på begäran av en polisman som verkställer ett ingripande eller vidtar en åtgärd som rör en enskild.

Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om under vilka förutsättningar sökning får äga rum med stöd av första och andra styckena.

Regeringen meddelar föreskrifter om ytterligare undantag från 6 §.

7 §²

Säkerhetspolisen, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket får medges direktåtkomst till personuppgifter i polisens brottbekämpande verksamhet. Direktåtkomsten får endast avse personuppgifter som har gjorts gemensamt tillgängliga.

En myndighet som medgetts direktåtkomst ansvarar för att

Polismyndigheten, Säkerhetspolisen, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket får för något av de syften som anges i 1 kap. 2 § brottsdatalagen (2018:000) medges direktåtkomst till personuppgifter som har gjorts gemensamt tillgängliga med stöd av 2 §.

² Senaste lydelse 2014:597.

tillgången till personuppgifter begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter.

Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om omfattningen av direktåtkomsten samt om behörighet och säkerhet.

Föreskrifter

8 §

Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om ytterligare undantag från 5 §.

9 §

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om

1. begränsning av tillgången till sådana personuppgifter som avses i 5 §,

2. under vilka förutsättningar sökning får utföras med stöd av 6 §, och

3. omfattningen av direktåtkomst enligt 7 § och om behörighet och säkerhet vid sådan åtkomst.

4 kap. Längsta tid som personuppgifter får behandlas

Allmän bestämmelse

1 § Detta kapitel gäller bara för automatiserad behandling.

Av 2 kap. 17 § första stycket brottsdatalagen (2018:000) framgår att personuppgifter inte får behandlas under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen.

I följande bestämmelser anges hur länge uppgifter som behandlas i särskilda register och i forensisk verksamhet får behandlas:

1. 5 kap. 7 § om uppgifter i register över dna-profiler,
2. 5 kap. 15 och 16 §§ om uppgifter i fingeravtrycks- och signallementsregister,
3. 5 kap. 20 § om uppgifter i penningtvättsregister,
4. 5 kap. 22 § om uppgifter i det internationella registret,
5. 5 kap. 26 § om uppgifter i tillträdesförbudsregistret, och
6. 6 kap. 6 § om uppgifter om sådana uppslag som anges i 6 kap. 1 § första stycket 5.

Personuppgifter som inte har gjorts gemensamt tillgängliga

2 § Trots det som sägs i 2 kap. 17 § andra stycket brottsdatalagen (2018:000) får personuppgifter som varken har gjorts gemensamt tillgängliga eller behandlas med stöd av 5 kap. inte behandlas längre än

1. ett år efter det att ärendet avslutades, om de behandlas i ett ärende, eller
2. ett år efter det att de behandlades automatiserat första gången, om de inte kan hänföras till ett ärende.

Första stycket gäller inte personuppgifter i ärenden om utredning av eller lagföring för brott.

Gemensamt tillgängliga uppgifter i ärenden om utredning av eller lagföring för brott

3 § Om en brottsanmälan avskrivs på grund av att den påstådda gärningen inte utgör brott, får personuppgifterna i anmälan inte längre behandlas för ändamål inom denna lags tillämpningsområde. Om en brottsanmälan i annat fall inte har lett till förundersökning

eller annan motsvarande utredning, får personuppgifterna inte behandlas för ändamål inom denna lags tillämpningsområde när åtal inte längre får väckas för brottet.

4 § Om en förundersökning har lett till åtal eller annan domstolsprövning, får personuppgifterna i förundersökningen inte behandlas för ändamål inom denna lags tillämpningsområde längre än fem år efter utgången av det kalenderår då domstolens avgörande fick laga kraft.

Om en förundersökning har lagts ner eller avslutats på annat sätt än genom åtal, får personuppgifterna i förundersökningen inte behandlas för ändamål inom denna lags tillämpningsområde längre än fem år efter utgången av det kalenderår då åklagarens eller förundersökningsledarens beslut meddelades.

Första och andra styckena gäller även personuppgifter i andra utredningar som handläggs enligt bestämmelser i 23 kap. rättegångsbalken.

5 § Om en förundersökning mot en person har lagts ner, om ett åtal har lagts ner eller om en frikännande dom har fått laga kraft, får personen inte längre vara sökbar som misstänkt.

Övriga gemensamt tillgängliga uppgifter

6 § Trots det som sägs i 2 kap. 17 § andra stycket brottsdatalagen (2018:000) får personuppgifter som har gjorts gemensamt tillgängliga med stöd av 3 kap. 2 § första stycket 1, 2 eller 4–7 som längst behandlas under den tid som anges i 7–10 §§.

7 § Personuppgifter som kan antas ha samband med sådan brottslig verksamhet som anges i 3 kap. 2 § första stycket 1 får, om de behandlas i ett ärende, inte behandlas längre än ett år efter det att ärendet avslutades.

Om personuppgifterna inte behandlas i ett ärende får de inte behandlas längre än tre år efter utgången av det kalenderår då registreringen avseende personen gjordes. Personuppgifter som kan antas ha samband med brottslig verksamhet som innefattar brott för vilket det är föreskrivet fängelse i två år eller däröver får inte

behandlas längre än fem år efter utgången av det kalenderår då registreringen gjordes. Om en ny registrering beträffande personens anknytning till brottslig verksamhet görs före utgången av de tider, får de personuppgifter som finns om personen fortsätta att behandlas så länge någon av uppgifterna om honom eller henne får behandlas.

Den tid då en misstänkt person avtjänar ett fängelsestraff eller genomgår sluten ungdomsvård eller rättspsykiatrisk vård med särskild utskrivningsprövning ska inte räknas med vid beräkningen av de tider som anges i andra stycket.

8 § Personuppgifter som behandlas i samband med sådan övervakning som avses i 3 kap. 2 § första stycket 2 får inte behandlas längre än tio år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes.

Den tid då en övervakad person avtjänar ett fängelsestraff eller genomgår sluten ungdomsvård eller rättspsykiatrisk vård med särskild utskrivningsprövning ska inte räknas med vid beräkningen av den tid som anges i första stycket.

9 § Personuppgifter som behandlas med stöd av 3 kap. 2 § första stycket 4 får inte behandlas längre än ett år efter det att ärendet som uppgifterna behandlades i avslutades.

Personuppgifter som behandlas med stöd av 3 kap. 2 § första stycket 7 får inte behandlas längre än ett år efter utgången av det kalenderår då ärendet som uppgifterna behandlades i avslutades.

10 § Personuppgifter som behandlas med stöd av 3 kap. 2 § första stycket 5 eller 6 får inte behandlas längre än ett år efter utgången av det kalenderår då de behandlades automatiserat första gången.

Föreskrifter

11 § Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om att vissa kategorier av personuppgifter får fortsätta behandlas för ändamål inom denna lags tillämpningsområde under längre tid än vad som anges i 3, 4 och 7–10 §§.

12 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om

1. att personuppgifter, med avvikelse från 2 § första stycket och 7–10 §§, får behandlas under längre tid för arkivändamål av allmänt intresse och vetenskapliga, statistiska eller historiska ändamål, och

2. begränsning av behandlingen av personuppgifter för ändamål inom denna lags tillämpningsområde vid digital arkivering.

5 kap. Register

Register över dna-profiler

Rätten att föra register

1 § Polismyndigheten får föra register över dna-profiler (dna-registret, utredningsregistret och spårregistret) i syfte att

1. förebygga, förhindra eller upptäcka brottslig verksamhet,

2. utreda eller lagföra brott,

3. fullgöra förpliktelser som följer av internationella åtaganden, och

4. underlätta identifiering av avlidna personer.

I lagen (2014:400) om Polismyndighetens elimineringsdatabas finns bestämmelser om elimineringsdatabasen.

Dna-registret

2 § Dna-registret får innehålla dna-profiler från prov som har tagits med stöd av 28 kap. rättegångsbalken och som avser personer som

1. genom dom som fått laga kraft har dömts till annan påföljd än böter, eller

2. har godkänt strafföreläggande som avser villkorlig dom.

3 § En dna-profil som registreras får endast ge information om identitet och inte om personliga egenskaper.

Utöver dna-profiler får dna-registret innehålla uppgifter om vem analysen avser, i vilket ärende profilen har tagits fram och brottskod.

Utredningsregistret

4 § Utredningsregistret får innehålla dna-profiler från prov som har tagits med stöd av 28 kap. rättegångsbalken och som avser personer som är skäligen misstänkta för brott på vilket det kan följa fängelse.

Bestämmelserna i 3 § gäller också vid registrering i utredningsregistret.

Spårregistret

5 § Spårregistret får innehålla dna-profiler som har tagits fram under utredning av brott och som inte kan hänföras till en identifierbar person. Utöver dna-profiler får spårregistret innehålla upplysningar som visar i vilket ärende profilen har tagits fram och brottskod.

6 § Dna-profiler i spårregistret får jämföras med dna-profiler

1. som inte kan hänföras till en identifierbar person,
2. som finns i dna-registret, eller
3. som kan hänföras till en person som är skäligen misstänkt för brott.

Dna-profiler i spårregistret får också jämföras i andra fall om det är nödvändigt för att fullgöra en internationell överenskommelse som Sverige har tillträtt efter riksdagens godkännande eller om det följer av en unionsrättsakt.

Längsta tid som personuppgifter får behandlas

7 § Trots det som sägs i 2 kap. 17 § andra stycket brottsdatalagen (2018:000) får personuppgifter i dna-registren som längst behandlas under den tid som anges i andra–fjärde styckena.

Uppgifter får inte längre behandlas i dna-registret när uppgifterna om den registrerade tagits bort ur belastningsregistret enligt lagen (1998:620) om belastningsregister.

Uppgifter får inte längre behandlas i utredningsregistret när uppgifterna om den registrerade får föras in i dna-registret eller när förundersökning eller åtal läggs ner, åtal ogillas, åtal bifalls men på-

följden bestäms till enbart böter eller när den registrerade har godkänt ett strafföreläggande som avser enbart böter.

Uppgifter får inte behandlas i spårregistret längre än trettio år efter registreringen. Sådana uppgifter får dock behandlas sjuttio år efter registreringen om uppgifterna hänför sig till utredningar om brott som anges i 35 kap. 2 § första stycket brottsbalken.

Prover för dna-analys

8 § Om det i samband med utredning av ett brott har tagits ett prov för dna-analys, får provet inte användas för något annat ändamål än det som provet togs för.

9 § Ett prov för dna-analys som har tagits med stöd av 28 kap. rättegångsbalken, eller på begäran av en annan stat, ska förstöras senast sex månader efter det att provet togs.

Direktåtkomst

10 § Säkerhetspolisen, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket och Kustbevakningen får för något av de syften som anges i 1 kap. 2 § brottsdatalagen (2018:000) medges direktåtkomst till register över dna-profiler som regleras i detta kapitel.

Fingeravtrycks- och signalementsregister

Rätten att föra register

11 § Polismyndigheten får föra fingeravtrycks- och signalementsregister i syfte att

1. förebygga, förhindra eller upptäcka brottslig verksamhet,
2. utreda eller lagföra brott,
3. fullgöra förpliktelser som följer av internationella åtaganden,
4. underlätta identifiering av okända personer, och
5. kontrollera fingeravtryck som Migrationsverket har tagit enligt 9 kap. 8 § utlänningslagen (2005:716).

Innehåll

12 § I fingeravtrycks- och signalementsregister får uppgifter behandlas om en person som

1. är misstänkt eller dömd för brott och som har varit föremål för åtgärd enligt 28 kap. 14 § rättegångsbalken, eller

2. har lämnat fingeravtryck enligt 19 § lagen (1991:572) om särskild utlänningskontroll.

Uppgifter om fingeravtryck som inte kan hänföras till en identifierbar person får behandlas om uppgiften kommit fram i en utredning om brott.

I fingeravtrycks- och signalementsregister får inte personuppgifter behandlas som har inhämtats med stöd av 36 § första stycket 2 lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare.

13 § Utöver vad som anges i 12 § får i fingeravtrycks- och signalementsregister uppgifter behandlas om en person som har dömts för brott i en annan medlemsstat inom Europeiska unionen och vars fingeravtrycks- eller signalementsuppgifter har överförts hit med stöd av artikel 4.2 i rådets rambeslut 2009/315/RIF av den 26 februari 2009 om organisationen av medlemsstaternas utbyte av uppgifter ur kriminalregistret och uppgifternas innehåll. Sådana uppgifter får dock endast behandlas om det för motsvarande gärning i Sverige är föreskrivet fängelse i ett år eller däröver och den som uppgifterna avser vid tidpunkten för gärningen hade fyllt femton år.

14 § Fingeravtrycks- och signalementsregister får innehålla uppgifter om

1. fingeravtryck,
2. signalement,
3. fotografi,
4. videoupptagning,
5. identifieringsuppgifter,
6. ärendenummer, och
7. brottskod.

Längsta tid som personuppgifter får behandlas

15 § Trots det som sägs i 2 kap. 17 § andra stycket brottsdatalagen (2018:000) får uppgifter i fingeravtrycks- och signalementsregister om en misstänkt person inte behandlas längre än tre månader efter det att uppgifterna om den registrerade tagits bort ur misstankeregistret som förs enligt lagen (1998:621) om misstankeregister och ur belastningsregistret som förs enligt lagen (1998:620) om belastningsregister.

Uppgifter som inte kan hänföras till en identifierbar person får inte behandlas längre än trettio år efter registreringen. Sådana uppgifter får dock behandlas sjuttio år efter registreringen om uppgifterna hänför sig till utredningar om brott som anges i 35 kap. 2 § första stycket brottsbalken.

16 § Trots det som sägs i 2 kap. 17 § andra stycket brottsdatalagen (2018:000) får uppgifter i fingeravtrycks- och signalementsregister som behandlas för att fullgöra ett internationellt åtagande inte behandlas när de inte längre behövs för det ändamålet.

Uppgifter om personer som har lämnat fingeravtryck med stöd av lagen (1991:572) om särskild utlänningskontroll får inte behandlas längre än tio år efter registreringen.

Direktåtkomst

17 § Säkerhetspolisen, Ekobrottsmyndigheten, Tullverket, Kustbevakningen och Skatteverket får för något av de syften som anges i 1 kap. 2 § brottsdatalagen (2018:000) medges direktåtkomst till personuppgifter i fingeravtrycks- och signalementsregister.

Penningtvätsregister*Rätten att föra register*

18 § Polismyndigheten får föra penningtvätsregister. Personuppgifter får behandlas i penningtvätsregister om det behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet

1. där penningtvätt är ett led för att dölja vinning av brott eller brottslig verksamhet, eller

2. som innefattar finansiering av terrorism.

19 § I penningtvätsregister får personuppgifter behandlas som

1. kan antas ha samband med sådan brottslig verksamhet som avses i 18 §,
2. har rapporterats till Polismyndigheten med stöd av lag eller annan författning, eller
3. har lämnats av en utländsk myndighet som i sin stat ansvarar för arbetet med att förebygga, förhindra eller upptäcka sådan brottslig verksamhet som avses i 18 §.

Längsta tid som personuppgifter får behandlas

20 § Trots det som sägs i 2 kap. 17 § andra stycket brottsdatalagen (2018:000) får personuppgifter i penningtvätsregister inte behandlas längre än fem år efter utgången av det kalenderår då den senaste registreringen avseende personens anknytning till brottslig verksamhet gjordes.

Det internationella registret

Rätten att föra register

21 § Polismyndigheten får föra ett internationellt register. Personuppgifter i det internationella registret får behandlas om det behövs för handläggningen av ärenden som rör internationellt polisiärt samarbete eller internationellt straffrättsligt samarbete.

Uppgifter om dödsfall, olyckshändelser eller andra liknande händelser i utlandet får också behandlas i det internationella registret, om ärendet rör en fråga som ska handläggas av Polismyndigheten.

Längsta tid som personuppgifter får behandlas

22 § Trots det som sägs i 2 kap. 17 § andra stycket brottsdatalagen (2018:000) får personuppgifter i det internationella registret inte behandlas längre än tre år efter utgången av det kalenderår då ärendet som uppgifterna behandlades i avslutades.

Tillträdesförbudsregistret

Rätten att föra register

23 § Polismyndigheten får föra ett register med uppgifter om personer som meddelats tillträdesförbud enligt lagen (2005:321) om tillträdesförbud vid idrottsarrangemang (tillträdesförbudsregistret) i syfte att förebygga, förhindra eller upptäcka överträdelse av tillträdesförbud.

Innehåll

24 § Tillträdesförbudsregistret får innehålla följande uppgifter om en person som har meddelats tillträdesförbud.

1. Namn.
2. Personnummer eller samordningsnummer.
3. Folkbokföringsadress och annan stadigvarande adress.
4. Alias.
5. Fotografi.
6. Anknnytning till idrott och idrottsorganisation.
7. Omfattningen och giltighetstiden av beslut om tillträdesförbud.
8. Överträdelse av gällande tillträdesförbud.

25 § Polismyndigheten får behandla uppgifter i tillträdesförbudsregistret i syfte att tillhandahålla idrottsorganisationer den information som behövs för att upprätthålla gällande beslut om tillträdesförbud.

Längsta tid som personuppgifter får behandlas

26 § Trots det som sägs i 2 kap. 17 § andra stycket brottsdatalagen (2018:000) får uppgifter i tillträdesförbudsregistret endast behandlas så länge tillträdesförbudet gäller.

Föreskrifter

27 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om

1. omfattningen av direktåtkomst till dna-register och fingeravtrycks- och signalementsregister och om behörighet och säkerhet vid sådan åtkomst,

2. tillgången till personuppgifter i penningtvätsregister och det internationella registret,

3. att personuppgifter i fingeravtrycks- och signalementsregister, penningtvätsregister, det internationella registret och tillträdesförbudsregistret, med avvikelse från det som sägs i 15, 16, 20, 22 och 26 §§, får behandlas under längre tid för arkivändamål av allmänt intresse och vetenskapliga, statistiska eller historiska ändamål.

6 kap.

3 §³

Personuppgifter som behandlas enligt 1 § första stycket 2 eller 5 eller andra stycket 2 eller 2 § andra stycket får även behandlas när det är nödvändigt för att tillhandahålla information som behövs i annan brottsbekämpande verksamhet hos Polismyndigheten eller i brottsbekämpande verksamhet hos Säkerhetspolisen, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen eller Skatteverket.

I ett enskilt fall får personuppgifter som behandlas enligt 1 eller 2 § även behandlas för att tillhandahålla information för något annat ändamål än det som anges i första stycket, under förutsätt-

Förutsättningarna för att behandla personuppgifter, som behandlas med stöd av 1 eller 2 §, för nya ändamål regleras i 2 kap. 4 och 22 §§ brottsdatalagen (2018:000). Enbart personuppgifter som behandlas enligt 1 § första stycket 2 eller 5 eller andra stycket 2 eller 2 § andra stycket får i ett enskilt fall behandlas för nya ändamål utanför den forensiska verksamheten.

³ Senaste lydelse 2015:436.

ning att ändamålet inte är oförenligt med det ändamål som uppgifterna samlades in för.

Känsliga personuppgifter

4 §

Biometriska och genetiska uppgifter får behandlas enligt 1 § under de förutsättningar som anges i 2 kap. 12 § brottsdatalagen (2018:000).

5 §

Sökförbudet i 2 kap. 14 § brottsdatalagen (2018:000) hindrar inte sökningar i personuppgifter som behandlas i register enligt 5 kap. i syfte att få fram ett personurval grundat på uppgifter som rör hälsa eller biometriska eller genetiska uppgifter.

Bevarande

Längsta tid som personuppgifter får behandlas

6 §⁴

Nationellt forensiskt centrum får inte behandla personuppgifter för det ändamål som anges i 1 § första stycket 5 när det har förflutit fem år efter utgången av det kalenderår då ärendet där uppgifterna förekommer registrerades.

Nationellt forensiskt centrum får inte behandla personuppgifter för det ändamål som anges i 1 § första stycket 5 längre än fem år efter utgången av det kalenderår då ärendet där uppgifterna förekommer registrerades.

⁴ Senaste lydelse 2015:436.

7 §⁵

Säkerhetspolisen, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket har, trots sekretess enligt 21 kap. 3 § första stycket och 35 kap. 1 § offentlighets- och sekretesslagen (2009:400), rätt att ta del av personuppgifter som behandlas enligt 1 § första stycket 5, om den mottagande myndigheten behöver uppgifterna *i sin brottsbekämpande verksamhet*.

Första stycket gäller inte uppgifter som behandlas i särskilda register enligt 4 kap.

Säkerhetspolisen, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket har, trots sekretess enligt 21 kap. 3 § första stycket och 35 kap. 1 § offentlighets- och sekretesslagen (2009:400), rätt att ta del av personuppgifter som behandlas enligt 1 § första stycket 5, om den mottagande myndigheten behöver uppgifterna *för något av de syften som anges i 1 kap. 2 § brottsdatalogen (2018:000)*.

Första stycket gäller inte uppgifter som behandlas i särskilda register enligt 5 kap.

8 §

Personuppgifter får lämnas ut elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt.

Föreskrifter9 §⁶

Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om att personuppgifter får lämnas ut i andra fall än som anges i 8 §.

Bestämmelser om att uppgifter får lämnas ut finns även i offentlighets- och sekretesslagen (2009:400).

Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om begränsning av möjligheten att lämna ut personuppgifter elektroniskt enligt 8 §.

⁵ Senaste lydelse 2015:436.

⁶ Senaste lydelse 2015:436.

10 §

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om begränsning av behandlingen av personuppgifter enligt detta kapitel vid digital arkivering.

7 kap. Administrativa sanktionsavgifter och rättsmedel

Administrativa sanktionsavgifter

1 § Sanktionsavgift får tas ut av den personuppgiftsansvarige vid överträdelse av bestämmelserna i

1. 2 kap. 1 § om tillåtna rättsliga grunder för behandling av personuppgifter,

2. 3 kap. 3 och 4 §§ om särskilda upplysningar, eller

3. 4 kap. 2–4 eller 7–10 §, 5 kap. 7, 15, 16, 20, 22 eller 26 § eller 6 kap. 6 § om längsta tid som personuppgifter får behandlas.

Sanktionsavgiften ska vara minst 50 000 kronor och högst 20 000 000 kronor.

Skadestånd

2 § Vid behandling av personuppgifter enligt denna lag eller föreskrifter som har meddelats i anslutning till den ska bestämmelsen i 7 kap. 1 § brottsdatalagen (2018:000) om skadestånd tillämpas på motsvarande sätt.

Överklagande

3 § Bestämmelser om överklagande och om vilka beslut som får överklagas finns i 7 kap. brottsdatalagen (2018:000).

1. Denna lag träder i kraft den 1 maj 2018.

2. Sanktionsavgift enligt 7 kap. 1 § får beslutas endast för överträdelser som har begåtts efter ikraftträdandet.

3. Bestämmelsen om skadestånd i 48 § personuppgiftslagen (1998:204) gäller fortfarande för skada som har orsakats före ikraftträdandet vid behandling av personuppgifter enligt denna lag eller föreskrifter som har meddelats i anslutning till den.

1.17 Förslag till lag om ändring i kustbevakningsdatalagen (2012:145)

Häri genom föreskrivs i fråga om kustbevakningsdatalagen (2012:145)

dels att 1–3 och 5 kap. ska upphöra att gälla,

dels att 4 kap. 2, 4 och 8–14 §§ ska upphöra att gälla,

dels att rubrikerna före 4 kap. 8 och 13 §§ ska utgå,

dels att nuvarande 4 kap. ska betecknas 3 kap.,

dels att nuvarande 4 kap. 1 § ska betecknas 3 kap. 2 § och att rubriken före nuvarande 4 kap. 1 § ska placeras före nya 3 kap. 2 §, att nuvarande 4 kap. 3 § ska betecknas 3 kap. 3 § och att rubriken före nuvarande 4 kap. 2 § ska placeras före nya 3 kap. 3 §, att nuvarande 4 kap. 5 § ska betecknas 3 kap. 4 § och att rubriken före nuvarande 4 kap. 4 § ska placeras före nya 3 kap. 4 §, att nuvarande 4 kap. 6 § ska betecknas 3 kap. 5 §, att nuvarande 4 kap. 7 § ska betecknas 3 kap. 6 § och att rubriken före nuvarande 4 kap. 7 § ska placeras före nya 3 kap. 6 §,

dels att nya 3 kap. 2–6 §§ ska ha följande lydelse,

dels att det ska införas tre nya paragrafer, 3 kap. 1, 7 och 8 §§, och nya rubriker före nya 3 kap. 1 och 7 §§ av följande lydelse,

dels att det ska införas fyra nya kapitler, 1, 2, 4 och 5 kap., av följande lydelse,

dels att rubriken till lagen ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

Kustbevakningsdatalag

Kustbevakningens brottsdatalag

1 kap. Allmänna bestämmelser

Lagens tillämpningsområde

1 § Denna lag gäller utöver brottsdatalagen (2018:000) när Kustbevakningen i egenskap av behörig myndighet behandlar personuppgifter i syfte att bekämpa eller lagföra brott eller upprätthålla allmän ordning och säkerhet.

2 § I lagen (2017:496) om internationellt polisiärt samarbete och i föreskrifter som regeringen har meddelat i anslutning till den lagen, finns det särskilda bestämmelser om behandling av personuppgifter som följer av internationella överenskommelser. Om det i dessa författningar finns avvikande bestämmelser, ska de tillämpas i stället för bestämmelserna i denna lag.

Personuppgiftsansvar

3 § Kustbevakningen är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför.

Lagens tillämpning på uppgifter om juridiska personer

4 § Bestämmelserna om personuppgifter i följande paragrafer gäller också vid behandling av uppgifter om juridiska personer:

1. 3 § om personuppgiftsansvar,
2. 2 kap. 1 § om tillåtna rättsliga grunder för behandling av personuppgifter,
3. 3 kap. 2 § om gemensamt tillgängliga uppgifter, och
4. 4 kap. 1–4 och 6–9 §§ om längsta tid som personuppgifter får behandlas.

Bestämmelserna om personuppgifter i följande paragrafer i brottsdatalogen (2018:000) gäller också vid sådan behandling:

1. 2 kap. 2 § om diarieföring och handläggning i vissa fall,
2. 2 kap. 3 § andra stycket om ändamålet med behandlingen,
3. 2 kap. 17 § om längsta tid som personuppgifter får behandlas,
4. 2 kap. 4 och 22 §§ om behandling för nya ändamål, och
5. 3 kap. 6 § om tillgången till personuppgifter.

2 kap. Grundläggande bestämmelser om behandling

Tillåtna rättsliga grunder för behandling av personuppgifter

1 § Kustbevakningen får behandla personuppgifter om det är nödvändigt för att utföra en arbetsuppgift i syfte att

1. förebygga, förhindra eller upptäcka brottslig verksamhet,

2. utreda eller lagföra brott,
3. upprätthålla allmän ordning och säkerhet, eller
4. fullgöra förpliktelser som följer av internationella åtaganden.

Arbetsuppgiften ska framgå av en bindande unionsrättsakt eller av en lag, en förordning eller ett särskilt beslut i vilket regeringen uppdragit åt myndigheten att ansvara för en sådan uppgift.

2 § Förutsättningarna för att behandla personuppgifter, som behandlas med stöd av 1 §, för nya ändamål regleras i 2 kap. 4 och 22 §§ brottsdatalagen (2018:000).

Särskilda upplysningar

3 § Bestämmelserna i 2 kap. 3 § andra stycket, 9 och 10 §§ brottsdatalagen (2018:000) om särskild upplysning gäller endast vid behandling av personuppgifter som har gjorts gemensamt tillgängliga med stöd av 3 kap. 2 §.

Känsliga personuppgifter

4 § Sökförbudet i 2 kap. 14 § brottsdatalagen (2018:000) hindrar inte att brottsrubriceringar, uppgifter om tillvägagångssätt vid brott eller uppgifter som beskriver en persons utseende används vid sökning.

5 § Sökförbudet i 2 kap. 14 § brottsdatalagen (2018:000) hindrar inte sökningar i syfte att få fram ett personurval grundat på etniskt ursprung, religiös eller filosofisk övertygelse eller uppgifter som rör hälsa, om sökningen görs i personuppgifter som inte har gjorts gemensamt tillgängliga.

Utlämnande av personuppgifter

6 § Om det är förenligt med svenska intressen, får personuppgifter lämnas ut till

1. Interpol,
2. Europol,

3. en polismyndighet eller åklagarmyndighet i en stat som är ansluten till Interpol, eller

4. en kustbevakningsmyndighet eller tullmyndighet inom Europeiska ekonomiska samarbetsområdet (EES).

Personuppgifter får lämnas ut enligt första stycket endast om mottagaren behöver uppgifterna för något av de syften som anges i 1 §.

Personuppgifter får vidare lämnas ut till en utländsk myndighet eller mellanfolklig organisation, om utlämnandet följer av en internationell överenskommelse som Sverige har tillträtt efter riksdagens godkännande.

7 § Polismyndigheten, Säkerhetspolisen, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket och Skatteverket har, trots sekretess enligt 21 kap. 3 § första stycket och 35 kap. 1 § offentlighets- och sekretesslagen (2009:400), rätt att ta del av personuppgifter som har gjorts gemensamt tillgängliga med stöd av 3 kap. 2 §, om den mottagande myndigheten behöver uppgifterna för något av de syften som anges i 1 kap. 2 § brottsdatalagen (2018:000).

8 § Personuppgifter får lämnas ut elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt.

Elektroniskt utlämnande genom direktåtkomst är tillåtet bara i den utsträckning som anges i 3 kap. 6 §.

Föreskrifter

9 § Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om

1. att personuppgifter får lämnas ut i andra fall än som anges i 6 och 7 §§, och

2. begränsning av möjligheten att lämna ut personuppgifter elektroniskt enligt 8 § första stycket.

3 kap.

Allmän bestämmelse

1 §

Detta kapitel innehåller särskilda bestämmelser för behandling av personuppgifter som görs eller har gjorts gemensamt tillgängliga med stöd av 2 §. Uppgifter som endast ett fåtal personer har rätt att ta del av anses inte som gemensamt tillgängliga.

Detta kapitel gäller inte när personuppgifter behandlas med stöd av 2 kap. 2 § brottsdatalogen (2018:000).

2 §

Följande personuppgifter får göras gemensamt tillgängliga i *Kustbevakningens brottsbekämpande verksamhet*:

1. Uppgifter som kan antas ha samband med misstänkt brottslig verksamhet, om den misstänkta verksamheten

a) innefattar brott för vilket det är föreskrivet fängelse i ett år eller däröver, eller

b) sker systematiskt.

2. Uppgifter som förekommer i ett ärende om utredning eller *beivrande av brott*.

3. Uppgifter som *behövs för att fullgöra internationella åtaganden, om det krävs för att den aktuella förpliktelsen ska kunna fullgöras*.

4. Uppgifter som har rapporterats till Kustbevakningens ledningscentraler.

Följande personuppgifter får göras gemensamt tillgängliga:

2. Uppgifter som förekommer i ett ärende om utredning *av eller lagföring för brott*.

3. Uppgifter som *behandlas i syfte att upprätthålla allmän ordning och säkerhet*.

5. Uppgifter som *behandlas i syfte att fullgöra internationella*

åtaganden, om det krävs för att den aktuella förpliktelsen ska kunna fullgöras.

3 §

Om uppgifter som *behandlas enligt 1 §* direkt kan hänföras till en person som inte är misstänkt *för brott eller* för att ha utövat eller komma att utöva sådan brottslig verksamhet som avses i *1 § första stycket 1*, ska det genom en särskild upplysning eller på annat sätt framgå att personen inte är misstänkt.

Uppgifter om en person som kan antas ha samband med *miss-tänkt* brottslig verksamhet ska försees med en upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak, om inte *detta* är onödigt på grund av *särskilda omständigheter*.

Om uppgifter som är *gemensamt tillgängliga* direkt kan hänföras till en person som inte är misstänkt för att ha utövat eller komma att utöva sådan brottslig verksamhet som avses i *2 § 1*, ska det genom en särskild upplysning eller på *något* annat sätt framgå att personen inte är misstänkt.

Uppgifter om en person som kan antas ha *direkt* samband med *sådan* brottslig verksamhet som avses i *2 § 1* ska försees med en upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak, om *det* inte på grund av *omständigheterna* är onödigt.

4 §

Vid sökning på namn, personnummer, samordningsnummer eller andra liknande identitetsbeteckningar i uppgifter som har gjorts gemensamt tillgängliga får endast sådana uppgifter tas fram som anger att den sökta personen

1. är anmäld för brott,
2. är eller har varit misstänkt för brott,
3. är misstänkt för att ha utövat eller komma att utöva så-

Vid sökning i *automatiserade behandlingssystem* på namn, personnummer, samordningsnummer eller andra liknande identitetsbeteckningar i uppgifter som har gjorts gemensamt tillgängliga får endast sådana uppgifter tas fram som anger att den sökta personen

3. är misstänkt för att ha utövat eller komma att utöva så-

dan brottslig verksamhet som avses i 1 § första stycket 1,

4. har anmält ett brott,

5. är målsägande i ett ärende som rör ansvar för brott,

6. förekommer i ett ärende som vittne eller annan som lämnar eller har lämnat uppgifter eller yttrande,

7. har gett in eller tillhandahållits en handling,

8. är anmäld försvunnen,

8. är anmäld som försvunnen,

9. har bedömts kunna komma att möta ett ingripande med grovt våld, eller

10. är efterlyst.

Regeringen eller den myndighet som regeringen bestämmer meddelar föreskrifter om begränsning av tillgången till sådana uppgifter som avses i första stycket.

5 §

Begränsningarna i 5 § gäller inte vid

1. sökning i en viss handling eller i ett visst ärende, eller

2. sökning i en uppgiftssamling som har skapats för att undersöka viss brottslighet och som enbart de som arbetar i undersökningen har åtkomst till.

Regeringen eller den myndighet som regeringen bestämmer meddelar föreskrifter om under vilka förutsättningar sökning får äga rum med stöd av första stycket.

Regeringen meddelar ytterligare föreskrifter om begränsningarna i 5 §.

Bestämmelserna i 4 § gäller inte vid sökning i en viss handling eller i ett visst ärende.

Bestämmelserna i 4 § gäller inte heller vid sökning som utförs av särskilt angivna tjänstemän i syfte att i underrättelseverksamhet bearbeta och analysera personuppgifter som har gjorts gemensamt tillgängliga med stöd av 2 § 1 och som enbart dessa tjänstemän har tillgång till.

6 §¹

Polismyndigheten, Säkerhetspolisen, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket och Skatteverket får medges direktåtkomst till personuppgifter i *Kustbevakningens brottsbekämpande verksamhet. Direktåtkomsten får endast avse personuppgifter som har gjorts gemensamt tillgängliga.*

En myndighet som har medgetts direktåtkomst ansvarar för att tillgången till personuppgifter begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter.

Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om omfattningen av direktåtkomsten samt om behörighet och säkerhet.

Polismyndigheten, Säkerhetspolisen, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket och Skatteverket får för *något av de syften som anges i 1 kap. 2 § brottsdatalagen (2018:000)* medges direktåtkomst till personuppgifter som har gjorts gemensamt tillgängliga *med stöd av 2 §.*

Föreskrifter

7 §

Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om ytterligare undantag från 4 §.

8 §

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om

¹ Senaste lydelse 2014:693.

1. begränsning av tillgången till sådana personuppgifter som avses i 4 §,

2. under vilka förutsättningar sökning får utföras med stöd av 5 §, och

3. omfattningen av direktåtkomst enligt 6 § och om behörighet och säkerhet vid sådan åtkomst.

4 kap. Längsta tid som personuppgifter får behandlas

Allmän bestämmelse

1 § Detta kapitel gäller bara för automatiserad behandling.

Av 2 kap. 17 § första stycket brottsdatalagen (2018:000) framgår att personuppgifter inte får behandlas under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen.

Personuppgifter som inte har gjorts gemensamt tillgängliga

2 § Trots det som sägs i 2 kap. 17 § andra stycket brottsdatalagen (2018:000) får personuppgifter som inte har gjorts gemensamt tillgängliga inte behandlas längre än

1. ett år efter det att ärendet avslutades, om de behandlas i ett ärende, eller

2. ett år efter det att de behandlades automatiserat första gången, om de inte kan hänföras till ett ärende.

Första stycket gäller inte personuppgifter i ärenden om utredning av eller lagföring för brott.

Gemensamt tillgängliga uppgifter i ärenden om utredning av eller lagföring för brott

3 § Om en brottsanmälan avskrivs på grund av att den påstådda gärningen inte utgör brott, får personuppgifterna i anmälan inte längre behandlas för ändamål inom denna lags tillämpningsområde.

Om en brottsanmälan i annat fall inte har lett till förundersökning eller annan motsvarande utredning, får personuppgifterna inte behandlas för ändamål inom denna lags tillämpningsområde när åtal inte längre får väckas för brottet.

4 § Om en förundersökning har lett till åtal eller annan domstolsprövning, får personuppgifterna i förundersökningen inte behandlas för ändamål inom denna lags tillämpningsområde längre än fem år efter utgången av det kalenderår då domstolens avgörande fick laga kraft.

Om en förundersökning har lagts ner eller avslutats på annat sätt än genom åtal, får personuppgifterna i förundersökningen inte behandlas för ändamål inom denna lags tillämpningsområde längre än fem år efter utgången av det kalenderår då åklagarens eller förundersökningsledarens beslut meddelades.

Första och andra styckena gäller även personuppgifter i andra utredningar som handläggs enligt bestämmelser i 23 kap. rättegångsbalken.

5 § Om en förundersökning mot en person har lagts ner, om ett åtal har lagts ner eller om en frikännande dom har fått laga kraft, får personen inte längre vara sökbar som misstänkt.

Övriga gemensamt tillgängliga uppgifter

6 § Trots det som sägs i 2 kap. 17 § andra stycket brottsdatalagen (2018:000) får personuppgifter som har gjorts gemensamt tillgängliga med stöd av 3 kap. 2 § 1 eller 3–5 som längst behandlas under den tid som anges i 7–9 §§.

7 § Personuppgifter som kan antas ha samband med sådan brottslig verksamhet som anges i 3 kap. 2 § 1 får inte behandlas längre än tre år efter utgången av det kalenderår då registreringen avseende personen gjordes. Personuppgifter som kan antas ha samband med brottslig verksamhet som innefattar brott för vilket det är föreskrivet fängelse i två år eller däröver får inte behandlas längre än fem år efter utgången av det kalenderår då registreringen gjordes. Om en ny registrering beträffande personens anknytning till

brottslig verksamhet görs före utgången av de tiderna, får de personuppgifter som finns om personen fortsätta att behandlas så länge någon av uppgifterna om honom eller henne får behandlas.

8 § Personuppgifter som behandlas med stöd av 3 kap. 2 § 3 eller 4 får inte behandlas längre än ett år efter utgången av det kalenderår då de behandlades automatiserat första gången.

9 § Personuppgifter som behandlas med stöd av 3 kap. 2 § 5 får inte behandlas längre än ett år efter utgången av det kalenderår då ärendet som uppgifterna behandlades i avslutades.

Föreskrifter

10 § Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om

1. att vissa kategorier av personuppgifter får fortsätta behandlas för ändamål inom denna lags tillämpningsområde under längre tid än vad som anges i 3, 4 och 7–9 §§, och

2. begränsning av behandlingen av personuppgifter för ändamål inom denna lags tillämpningsområde vid digital arkivering.

11 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om att personuppgifter, med avvikelse från 2 § första stycket och 7–9 §§, får behandlas under längre tid för arkivändamål av allmänt intresse och vetenskapliga, statistiska eller historiska ändamål.

5 kap. Administrativa sanktionsavgifter och rättsmedel

Administrativa sanktionsavgifter

1 § Sanktionsavgift får tas ut av den personuppgiftsansvarige vid överträdelse av bestämmelserna i

1. 2 kap. 1 § om tillåtna rättsliga grunder för behandling av personuppgifter,

2. 3 kap. 3 § om särskild upplysning, eller

3. 4 kap. 2–4 eller 7–9 § om längsta tid som personuppgifter får behandlas.

Sanktionsavgiften ska vara minst 50 000 kronor och högst 20 000 000 kronor.

Skadestånd

2 § Vid behandling av personuppgifter enligt denna lag eller föreskrifter som har meddelats i anslutning till den ska bestämmelsen i 7 kap. 1 § brottsdatalagen (2018:000) om skadestånd tillämpas på motsvarande sätt.

Överklagande

3 § Bestämmelser om överklagande och om vilka beslut som får överklagas finns i 7 kap. brottsdatalagen (2018:000).

1. Denna lag träder i kraft den 1 maj 2018.

2. Sanktionsavgift enligt 5 kap. 1 § får beslutas endast för överträdelser som har begåtts efter ikraftträdandet.

3. Bestämmelsen om skadestånd i 48 § personuppgiftslagen (1998:204) gäller fortfarande för skada som har orsakats före ikraftträdandet vid behandling av personuppgifter enligt denna lag eller föreskrifter som har meddelats i anslutning till den.

1.18 Förslag till lag om ändring i lagen (2014:400) om Polismyndighetens elimineringsdatabas

Härigenom föreskrivs i fråga om lagen (2014:400) om Polismyndighetens elimineringsdatabas

dels att 6 och 7 §§ och rubriken före 7 § ska upphävas,¹

dels att i 3, 8–10, 13 och 14 §§ ”DNA” ska bytas ut mot ”dna”,

dels att 1, 2, 4, 11 och 12 §§ och rubrikerna före 2, 11 och 12 §§ ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

1 §²

Polismyndigheten får föra ett register över *DNA-profiler* i syfte att stärka kvaliteten i den forensiska verksamheten med *DNA-analyser* (elimineringssdatabasen) i enlighet med denna lag.

Uppgifter i elimineringsdatabasen får endast behandlas för att upptäcka och utreda kontamineringar vid *DNA-analyser* och hanteringen av *DNA-spår*.

Begreppen *DNA-profil* och *DNA-analys* som används i lagen har samma betydelse som i *polisdatalagen* (2010:361).

Polismyndigheten får föra ett register över *dna-profiler* i syfte att stärka kvaliteten i den forensiska verksamheten med *dna-analyser* (elimineringssdatabasen) i enlighet med denna lag.

Uppgifter i elimineringsdatabasen får endast behandlas för att upptäcka och utreda kontamineringar vid *dna-analyser* och hanteringen av *dna-spår*.

Begreppen *dna-profil* och *dna-analys* som används i lagen har samma betydelse som i *polisens brottsdatalog* (2010:361).

¹ Senaste lydelse av 6 § 2014:600.

² Senaste lydelse 2014:600.

Förhållandet till *personuppgifts-*
*lagen*Förhållandet till *annan person-*
uppgiftsreglering

2 §

Denna lag gäller utöver *per-*
sonuppgiftslagen (1998:204).

Denna lag gäller utöver
brottsdatalagen (2018:000).

4 §

En *DNA-profil* som har tagits fram under utredning av brott och som inte kan hänföras till en identifierbar person får vid ett tillfälle jämföras med *DNA-profiler* i elimineringsdatabasen. Jämförelsen ska göras innan jämförelse görs med andra *DNA-profiler* i de *DNA-register* som regleras i 4 kap. *polisdata-*
lagen (2010:361).

En *dna-profil* som har tagits fram under utredning av brott och som inte kan hänföras till en identifierbar person får vid ett tillfälle jämföras med *dna-profiler* i elimineringsdatabasen. Jämförelsen ska göras innan jämförelse görs med andra *dna-profiler* i de *dna-register* som regleras i 5 kap. *polisens brotts-*
datalag (2010:361).

En *DNA-profil* från prov som har tagits med stöd av 28 kap. rättegångsbalken får vid ett tillfälle jämföras med *DNA-profiler* i elimineringsdatabasen. Avser *DNA-profilen* en misstänkt ska jämförelsen göras innan profilen läggs in i det utredningsregister eller det *DNA-register* som regleras i 4 kap. *polisdata-*
lagen.

En *dna-profil* från prov som har tagits med stöd av 28 kap. rättegångsbalken får vid ett tillfälle jämföras med *dna-profiler* i elimineringsdatabasen. Avser *dna-profilen* en misstänkt ska jämförelsen göras innan profilen läggs in i det utredningsregister eller det *dna-register* som regleras i 5 kap. *polisens brotts-*
datalag.

En *DNA-profil* som har tagits fram för att kvalitetssäkra den forensiska verksamheten med *DNA-analyser* och som inte hänför sig till brottsutredande verksamhet får jämföras med *DNA-profiler* i elimineringsdatabasen.

En *dna-profil* som har tagits fram för att kvalitetssäkra den forensiska verksamheten med *dna-analyser* och som inte hänför sig till brottsutredande verksamhet får jämföras med *dna-profiler* i elimineringsdatabasen.

*Gallring**Längsta tid för behandling*11 §³

Trots det som sägs i 2 kap. 17 § andra stycket brottsdatalogen (2018:000) får personuppgifter som längst behandlas under den tid som anges i andra–femte styckena.

Uppgifter i elimineringsdatabasen *ska gallras* när de inte längre behövs för att utreda om en persons *DNA* kan ha kontaminerat material, prover eller lokaler.

Uppgifter som rör anställda vid Polismyndigheten *ska gallras senast* två år efter det att det förhållande som grundade skyldigheten att lämna prov upphörde.

Uppgifter som har registrerats med stöd av 9 § *ska gallras senast* ett år efter det att uppgifterna registrerades.

Uppgifter som rör andra än de som anges i andra och tredje styckena *ska gallras senast* ett år efter det att det förhållande som grundade skyldigheten upphörde.

Uppgifter i elimineringsdatabasen *får inte behandlas* när de inte längre behövs för att utreda om en persons *dna* kan ha kontaminerat material, prover eller lokaler.

Uppgifter som rör anställda vid Polismyndigheten *får inte behandlas längre än* två år efter det att det förhållande som grundade skyldigheten att lämna prov upphörde.

Uppgifter som har registrerats med stöd av 9 § *får inte behandlas längre än* ett år efter det att uppgifterna registrerades.

Uppgifter som rör andra än de som anges i andra och tredje styckena *får inte behandlas längre än* ett år efter det att det förhållande som grundade skyldigheten upphörde.

³ Senaste lydelse 2014:600.

*Rättelse och skadestånd**Skadestånd*

12 §

Bestämmelserna i personuppgiftslagen (1998:204) om rättelse och skadestånd tillämpas på motsvarande sätt vid behandling av personuppgifter enligt denna lag eller enligt föreskrifter som avses i 13 eller 14 §.

Vid behandling av personuppgifter enligt denna lag eller enligt föreskrifter som avses i 13 eller 14 § ska bestämmelsen i 7 kap. 1 § brottsdatalagen (2018:000) om skadestånd tillämpas på motsvarande sätt.

-
1. Denna lag träder i kraft den 1 maj 2018.
 2. Bestämmelsen om skadestånd i 48 § personuppgiftslagen (1998:204) gäller fortfarande för skada som före ikraftträdandet har orsakats vid behandling av personuppgifter enligt denna lag.

1.19 Förslag till lag om ändring i lagen (2015:51) om register över tillträdesförbud vid idrottsarrangemang

Härigenom föreskrivs i fråga om lagen (2015:51) om register över tillträdesförbud vid idrottsarrangemang

dels att 2, 4, 6, 8–10, 12 och 15 §§ ska upphöra att gälla,

dels att rubrikerna före 2, 4, 8–10, 12 och 15 §§ ska utgå,

dels att nuvarande 3 § ska betecknas 2 § och att rubriken före nuvarande 3 § ska placeras före nya 2 §, att nuvarande 5 § ska betecknas 4 §, att nuvarande 7 § ska betecknas 5 § och att rubriken före nuvarande 6 § ska placeras före nya 5 §, att nuvarande 11 § ska betecknas 6 § och att rubriken före nuvarande 11 § ska placeras före nya 6 §, att nuvarande 13 § ska betecknas 7 §, att nuvarande 14 § ska betecknas 8 § och att rubriken före nuvarande 14 § ska placeras före nya 8 §,

dels att rubriken före nya 4 § ska lyda Rätten att behandla personuppgifter,

dels att 1 och nya 2, 4, 6 och 7 §§ ska ha följande lydelse,

dels att det ska införas en ny paragraf, 3 §, och före nya 3 och 7 §§ nya rubriker med följande lydelse,

dels att rubriken till lagen ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

Lag om register över tillträdesförbud vid idrottsarrangemang

Lag om idrottsorganisationers behandling av uppgifter om tillträdesförbud

1 §

Syftet med denna lag är att göra det möjligt för *Polismyndigheten och* idrottsorganisationer som anordnar idrottsarrangemang att behandla personuppgifter för att på ett ändamålsenligt sätt kunna upprätthålla gäl-

Syftet med denna lag är att göra det möjligt för idrottsorganisationer som anordnar idrottsarrangemang att behandla personuppgifter för att på ett ändamålsenligt sätt kunna upprätthålla gällande beslut *enligt lagen*

lande beslut om tillträdesförbud vid idrottsarrangemang och att skydda människor mot att deras personliga integritet kränks vid sådan behandling.

(2005:321) om tillträdesförbud vid idrottsarrangemang och att skydda människor mot att deras personliga integritet kränks vid sådan behandling.

2 §

Denna lag gäller behandling av personuppgifter för att upprätthålla gällande beslut om tillträdesförbud. *Lagen gäller vid*

1. *Polismyndighetens behandling av personuppgifter i tillträdesförbudsregistret, och*

2. *idrottsorganisationers behandling av personuppgifter från tillträdesförbudsregistret.*

Lagen gäller behandling som är helt eller delvis automatiserad eller om personuppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier. Lagen gäller även för annan behandling i fall som avses i 14 §.

Denna lag gäller *vid idrottsorganisationers* behandling av personuppgifter *från det tillträdesförbudsregister som förs enligt polisens brottsdatalag (2010:361)* för att upprätthålla gällande beslut om tillträdesförbud.

Lagen gäller *för* behandling som är helt eller delvis automatiserad eller om personuppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier. Lagen gäller även för annan behandling i fall som avses i 8 §.

Förhållandet till annan reglering om personuppgiftsbehandling

3 §

Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter

och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) gäller vid behandling av personuppgifter enligt denna lag. Lagen (2018:000) med kompletterande bestämmelser till EU:s dataskyddsförordning gäller om inte annat följer av denna lag eller föreskrifter som har meddelats i anslutning till den.

4 §

Polismyndigheten är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför enligt denna lag.

Varje idrottsorganisation är personuppgiftsansvarig för den behandling av personuppgifter som organisationen utför.

6 §

Tillgången till personuppgifter ska begränsas till vad den som arbetar vid Polismyndigheten eller som arbetar eller utför uppdrag åt en idrottsorganisation behöver för att kunna fullgöra arbetsuppgifterna eller uppdraget.

Tillgången till personuppgifter ska begränsas till vad den som arbetar eller utför uppdrag åt en idrottsorganisation behöver för att kunna fullgöra arbetsuppgifterna eller uppdraget.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om tillgången till personuppgifter.

7 §

Längsta tid som personuppgifter får behandlas

En uppgift som en idrottsorganisation har fått tillgång till från tillträdesförbudsregistret ska

Behandlingen av personuppgifter som en idrottsorganisation har fått tillgång till från tillträ-

tas bort om uppgiften inte längre behövs för de ändamål som anges i 7 §, dock senast när tillträdesförbudets giltighetstid löper ut eller om tillträdesförbudet dessförinnan upphävs.

desförbudsregistret ska *upphöra* senast när tillträdesförbudets giltighetstid löper ut eller om tillträdesförbudet dessförinnan upphävs.

-
1. Denna lag träder i kraft den 1 maj 2018.
 2. Bestämmelserna i 4 och 15 §§ i deras nuvarande lydelse ska fortsätta att gälla för idrottsorganisationers personuppgiftsbehandling till den 25 maj 2018.
 3. Bestämmelsen i 3 § ska inte tillämpas förrän den 25 maj 2018.

1.20 Förslag till lag om ändring i åklagardatalagen (2015:433)

Härigenom föreskrivs i fråga om åklagardatalagen (2015:433)

dels att 1 och 2 kap. ska upphöra att gälla,
dels att 3 kap. 3, 4 och 7 §§ ska upphöra att gälla,
dels att rubriken före 3 kap. 3 § ska utgå,
dels att nuvarande 3 kap. 5 § ska betecknas 3 kap. 3 § och att rubriken före nuvarande 3 kap. 4 § ska placeras före nya 3 kap. 3 §, att nuvarande 3 kap. 6 § ska betecknas 3 kap. 4 §, att nuvarande 3 kap. 8 § ska betecknas 3 kap. 5 § och att rubriken före nuvarande 3 kap. 8 § ska placeras före nya 3 kap. 5 §,
dels att 3 kap. 1 och 2 §§ och nya 3–5 §§ ska ha följande lydelse,
dels att det ska införas två nya paragrafer, 3 kap. 6 och 7 §§, och nya rubriker före 3 kap. 1 § och nya 3 kap. 6 § av följande lydelse,
dels att det ska införas fyra nya kapitel, 1, 2, 4 och 5 kap., av följande lydelse,
dels att rubriken till lagen ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

Åklagardatalag

Åklagarväsendets brottsdatalag

1 kap. Allmänna bestämmelser

Lagens tillämpningsområde

1 § Denna lag gäller utöver brottsdatalagen (2018:000) när Åklagarmyndigheten eller Ekobrottsmyndigheten i egenskap av behörig myndighet behandlar personuppgifter i åklagarverksamhet i syfte att bekämpa eller lagföra brott eller handlägga frågor om ändring eller verkställighet av straffrättsliga påföljder eller upprätthållande av allmän ordning och säkerhet.

Bestämmelser om personuppgiftsbehandling vid Ekobrottsmyndigheten finns också i polisens brottsdatalag (2010:361).

Personuppgiftsansvar

2 § Åklagarmyndigheten och Ekobrottsmyndigheten är var och en personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför.

Lagens tillämpning på uppgifter om juridiska personer

3 § Bestämmelserna om personuppgifter i följande paragrafer gäller också vid behandling av uppgifter om juridiska personer:

1. 2 § om personuppgiftsansvar,
2. 2 kap. 1 § om tillåtna rättsliga grunder för behandling av personuppgifter,
3. 3 kap. 2 § om gemensamt tillgängliga uppgifter, och
4. 4 kap. 1, 2 och 4 §§ om längsta tid som personuppgifter får behandlas.

Bestämmelserna om personuppgifter i följande paragrafer i brottsdatalagen (2018:000) gäller också vid sådan behandling:

1. 2 kap. 2 § om diarieföring och handläggning i vissa fall,
2. 2 kap. 3 § andra stycket om ändamålet med behandlingen,
3. 2 kap. 17 § om längsta tid som personuppgifter får behandlas,
4. 2 kap. 4 och 22 §§ om behandling för nya ändamål, och
5. 3 kap. 6 § om tillgången till personuppgifter.

2 kap. Grundläggande bestämmelser om behandling

Tillåtna rättsliga grunder för behandling av personuppgifter

1 § Personuppgifter får behandlas om det är nödvändigt för att utföra en arbetsuppgift i syfte att

1. förebygga eller förhindra brottslig verksamhet,
2. utreda eller lagföra brott,
3. handlägga frågor om ändring eller verkställighet av straffrättsliga påföljder,
4. handlägga frågor som rör upprätthållande av allmän ordning och säkerhet, eller
5. fullgöra förpliktelser som följer av internationella åtaganden.

Arbetsuppgiften ska framgå av en bindande unionsrättsakt eller av en lag, en förordning eller ett särskilt beslut i vilket regeringen uppdragit åt myndigheten att ansvara för en sådan uppgift.

2 § Förutsättningarna för att behandla personuppgifter, som behandlas med stöd av 1 §, för nya ändamål regleras i 2 kap. 4 och 22 §§ brottsdatalagen (2018:000).

Särskilda upplysningar

3 § Bestämmelserna i 2 kap. 3 § andra stycket, 9 och 10 §§ brottsdatalagen (2018:000) om särskild upplysning gäller endast vid behandling av personuppgifter som har gjorts gemensamt tillgängliga med stöd av 3 kap. 2 §.

Känsliga personuppgifter

4 § Sökförbudet i 2 kap. 14 § brottsdatalagen (2018:000) hindrar inte att brottsrubriceringar eller uppgifter som beskriver en persons utseende används vid sökning.

Utlämnande av personuppgifter

5 § Om det är förenligt med svenska intressen, får personuppgifter lämnas ut till

1. Eurojust,
2. Interpol,
3. Europol, eller
4. en polismyndighet eller åklagarmyndighet i en stat som är ansluten till Interpol.

Personuppgifter får lämnas ut enligt första stycket endast om mottagaren behöver uppgifterna för något av de syften som anges i 1 §.

Personuppgifter får vidare lämnas ut till en utländsk myndighet eller mellanfolklig organisation, om utlämnandet följer av en internationell överenskommelse som Sverige har tillträtt efter riksdagens godkännande.

6 § Åklagarmyndigheten, Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Kustbevakningen och Skatteverket har, trots sekretess enligt 21 kap. 3 § första stycket och 35 kap. 1 § offentlighets- och sekretesslagen (2009:400), rätt att ta del av personuppgifter som har gjorts gemensamt tillgängliga med stöd av 3 kap. 2 §, om den mottagande myndigheten behöver uppgifterna för något av de syften som anges i 1 kap. 2 § brottsdatalogen (2018:000).

7 § Personuppgifter får lämnas ut elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt.

Elektroniskt utlämnande genom direktåtkomst är tillåtet bara i den utsträckning som anges i 3 kap. 5 §.

Föreskrifter

8 § Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om

1. att personuppgifter får lämnas ut i andra fall än som anges i 5 och 6 §§, och

2. begränsning av möjligheten att lämna ut personuppgifter elektroniskt enligt 7 § första stycket.

3 kap.

Allmän bestämmelse

1 §

Detta kapitel innehåller särskilda bestämmelser för behandling av personuppgifter som görs eller har gjorts gemensamt tillgängliga *i åklagarväsendets operativa verksamhet*. Uppgifter som endast ett fåtal personer har rätt att ta del av anses inte som gemensamt tillgängliga.

Detta kapitel gäller inte när personuppgifter behandlas med

Detta kapitel innehåller särskilda bestämmelser för behandling av personuppgifter som görs eller har gjorts gemensamt tillgängliga *med stöd av 2 §*. Uppgifter som endast ett fåtal personer har rätt att ta del av anses inte som gemensamt tillgängliga.

Detta kapitel gäller inte när personuppgifter behandlas med

stöd av 2 kap. 7 §.

stöd av 2 kap. 2 § brottsdatalogen (2018:000).

2 §

Personuppgifter i åklagarväsendets operativa verksamhet får göras gemensamt tillgängliga.

Alla personuppgifter som behandlas för syften som omfattas av denna lags tillämpningsområde får göras gemensamt tillgängliga.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela närmare föreskrifter om sådana uppgifter.

3 §

Vid sökning på namn, personnummer, samordningsnummer eller andra liknande identitetsbeteckningar i uppgifter som har gjorts gemensamt tillgängliga får sådana uppgifter tas fram som anger att den sökta personen

Vid sökning i automatiserade behandlingssystem på namn, personnummer, samordningsnummer eller andra liknande identitetsbeteckningar i uppgifter som har gjorts gemensamt tillgängliga får *endast* sådana uppgifter tas fram som anger att den sökta personen

1. är eller har varit misstänkt för brott,

2. är misstänkt för att ha utövat eller komma att utöva brottslig verksamhet,

3. har anmält ett brott,

4. är målsägande i ett ärende som rör ansvar för brott,

5. är sökande, motpart eller annan part eller kan jämföras med part i ett ärende,

6. förekommer i ett ärende som vittne eller *någon* annan

1. är anmäld för brott,

2. är eller har varit misstänkt för brott,

3. är misstänkt för att ha utövat eller komma att utöva brottslig verksamhet,

4. har anmält ett brott,

5. är målsägande i ett ärende som rör ansvar för brott,

6. är sökande, motpart eller annan part eller kan jämföras med part i ett ärende,

7. förekommer i ett ärende som vittne eller annan som läm-

som lämnar eller har lämnat uppgifter eller yttrande,

7. är eller har varit åklagare i ett ärende, eller är eller har varit offentlig försvarare eller målsägandebiträde eller kan jämföras med sådana, eller

8. har gett in eller tillhandahållits en handling.

nar eller har lämnat uppgifter eller yttrande,

8. är eller har varit åklagare i ett ärende, eller är eller har varit offentlig försvarare eller målsägandebiträde eller kan jämföras med sådana, eller

9. har gett in eller tillhandahållits en handling.

4 §

Bestämmelserna i 5 § gäller inte vid sökning i en viss handling eller i ett visst ärende.

Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om ytterligare undantag från 5 §.

Bestämmelserna i 3 § gäller inte vid sökning i en viss handling eller i ett visst ärende.

5 §

Åklagarmyndigheten, Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Kustbevakningen och Skatteverket får i den brottbekämpande verksamheten medges direktåtkomst till personuppgifter i åklagarväsendets operativa verksamhet. Direktåtkomsten får endast avse personuppgifter som har gjorts gemensamt tillgängliga.

En myndighet som har medgetts direktåtkomst ansvarar för att tillgången till personuppgifter begränsas till det som varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter.

Åklagarmyndigheten, Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Kustbevakningen och Skatteverket får för något av de syften som anges i 1 kap. 2 § brottsdatalagen (2018:000) medges direktåtkomst till personuppgifter som har gjorts gemensamt tillgängliga med stöd av 2 §.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela närmare föreskrifter om omfattningen av direktåtkomsten och om behörighet och säkerhet.

Föreskrifter

6 §

Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om ytterligare undantag från 3 §.

7 §

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om

- 1. gemensamt tillgängliga uppgifter, och*
- 2. omfattningen av direktåtkomst enligt 5 § och om behörighet och säkerhet vid sådan åtkomst.*

4 kap. Längsta tid som personuppgifter får behandlas

Allmän bestämmelse

1 § Detta kapitel gäller bara för automatiserad behandling.

Av 2 kap. 17 § första stycket brottsdatalagen (2018:000) framgår att personuppgifter inte får behandlas under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen.

Personuppgifter i ärenden

2 § Personuppgifter i ett ärende får inte behandlas för ändamål inom denna lags tillämpningsområde längre än fem år efter utgången av det kalenderår då ärendet avslutades av åklagaren, eller, om frågan prövats av domstol, från utgången av det kalenderår då domstolens avgörande fick laga kraft.

3 § Om en förundersökning mot en person inte har inletts eller har lagts ner, om ett åtal har lagts ner eller om en frikännande dom har fått laga kraft, får personen inte längre vara sökbar som misstänkt.

Övriga personuppgifter

4 § Trots det som sägs i 2 kap. 17 § andra stycket brottsdatalagen (2018:000) får personuppgifter som inte kan hänföras till ett ärende inte behandlas längre än ett år efter utgången av det kalenderår då de behandlades automatiserat första gången.

Föreskrifter

5 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om

1. att uppgifter i vissa ärendetyper eller vissa kategorier av personuppgifter får fortsätta att behandlas för ändamål inom denna lags tillämpningsområde under längre tid än vad som anges i 2 §,

2. att personuppgifter, med avvikelse från 4 §, får behandlas under längre tid för arkivändamål av allmänt intresse och vetenskapliga, statistiska eller historiska ändamål, och

3. begränsning av behandlingen av personuppgifter för ändamål inom denna lags tillämpningsområde vid digital arkivering.

5 kap. Administrativa sanktionsavgifter och rättsmedel

Administrativa sanktionsavgifter

1 § Sanktionsavgift får tas ut av den personuppgiftsansvarige vid överträdelse av bestämmelserna i

1. 2 kap. 1 § om tillåtna rättsliga grunder för behandling av personuppgifter, eller

2. 4 kap. 2 eller 4 § om längsta tid som personuppgifter får behandlas.

Sanktionsavgiften ska vara minst 50 000 kronor och högst 20 000 000 kronor.

Skadestånd

2 § Vid behandling av personuppgifter enligt denna lag eller föreskrifter som har meddelats i anslutning till den ska bestämmelsen i 7 kap. 1 § brottsdatalagen (2018:000) om skadestånd tillämpas på motsvarande sätt.

Överklagande

3 § Bestämmelser om överklagande och om vilka beslut som får överklagas finns i 7 kap. brottsdatalagen (2018:000).

1. Denna lag träder i kraft den 1 maj 2018.

2. Sanktionsavgift enligt 5 kap. 1 § får beslutas endast för överträdelser som har begåtts efter ikraftträdandet.

3. Bestämmelsen om skadestånd i 48 § personuppgiftslagen (1998:204) gäller fortfarande för skada som har orsakats före ikraftträdandet vid behandling av personuppgifter enligt denna lag eller föreskrifter som har meddelats i anslutning till den.

1.21 Förslag till lag om ändring i utlänningsdatalagen (2016:27)

Härigenom föreskrivs att 14 § utlänningsdatalagen (2016:27) ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

14 §

Migrationsverket får föra separata register över fingeravtryck och fotografier som tas med stöd av 9 kap. 8 § utlänningslagen (2005:716).

Med begränsning av de ändamål som annars gäller enligt 11 och 13 §§ får uppgifter om fingeravtryck eller fotografier i registren användas endast

1. vid prövning av ansökningar om uppehållstillstånd där skäl som anges i 4 kap. 1–2 a §§ utlänningslagen åberopas,

2. i ärenden om avvisning och utvisning,

3. i testverksamhet,

4. om det behövs för att kontrollera identiteten av en person på ett fotografi som kommit in till Migrationsverket, eller

5. om det behövs för att Migrationsverket ska kunna kontrollera ett fingeravtryck mot *det* fingeravtrycks- och signalementsregister som Polismyndigheten för enligt 4 kap. 11 § *polisdatalagen* (2010:361).

5. om det behövs för att Migrationsverket ska kunna kontrollera ett fingeravtryck mot fingeravtrycks- och signalementsregister som Polismyndigheten för enligt 5 kap. 11 § *polisens brottsdatalag* (2010:361).

Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela

1. ytterligare föreskrifter om vilka uppgifter som får behandlas i registren över fingeravtryck och fotografier, och

2. föreskrifter om gallring.

Denna lag träder i kraft den 1 maj 2018.

1.22 Förslag till lag om ändring i tullagen (2016:253)

Härigenom föreskrivs att 4 kap. 8 § tullagen (2016:253) ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

4 kap. 8 §

Ett transportföretag får lämna uppgifter enligt 6 § på så sätt att de görs läsbara för Tullverket genom terminalåtkomst.

Tullverket får ta del av uppgifter genom terminalåtkomst endast i den omfattning och under den tid som behövs för att kontrollera aktuella transporter. *Uppgifter som hålls tillgängliga på detta sätt får inte ändras eller på annat sätt bearbetas eller lagras av Tullverket.*

Uppgifter om enskilda personer som lämnats på annat sätt än genom terminalåtkomst ska omedelbart förstöras, om de visar sig sakna betydelse för utredning av eller lagföring för brott.

Tullverket får ta del av uppgifter genom terminalåtkomst endast i den omfattning och under den tid som behövs för att kontrollera aktuella transporter.

Denna lag träder i kraft den 1 maj 2018.

1.23 Förslag till lag om ändring i tullbrottsdatalagen (2017:447)

Härigenom föreskrivs i fråga om tullbrottsdatalagen (2017:447)

dels att 1 och 2 kap. ska upphöra att gälla,

dels att 3 kap. 5 § och 4 kap. 5 § ska upphöra att gälla,

dels att nuvarande 3 kap. 6 § ska betecknas 3 kap. 5 §, att nuvarande 3 kap. 7 § ska betecknas 3 kap. 6 §, att nuvarande 3 kap. 8 § ska betecknas 3 kap. 7 § och att rubriken före nuvarande 3 kap. 8 § ska placeras före nya 3 kap. 7 §, att nuvarande 4 kap. 2 § ska betecknas 4 kap. 12 §, att nuvarande 4 kap. 3 § ska betecknas 4 kap. 2 § och att rubriken före nuvarande 4 kap. 3 § ska placeras före nya 4 kap. 2 §, att nuvarande 4 kap. 4 § ska betecknas 4 kap. 3 §, att nuvarande 4 kap. 6 § ska betecknas 4 kap. 4 § och att rubriken före nuvarande 4 kap. 5 § ska placeras före nya 4 kap. 4 §, att nuvarande 4 kap. 7 § ska betecknas 4 kap. 5 §, att nuvarande 4 kap. 8 § ska betecknas 4 kap. 6 §, att nuvarande 4 kap. 9 § ska betecknas 4 kap. 8 § och att rubriken före nuvarande 4 kap. 9 § ska placeras före nya 4 kap. 7 §,

dels att 3 kap. 1–4 §§ och nya 3 kap. 5–7 §§, 4 kap. 1 § och nya 4 kap. 2–5, 8, 10 och 13 §§, rubriken till 4 kap. och rubriken före 4 kap. 1 § och nya 4 kap. 4 § ska ha följande lydelse,

dels att det ska införas sex nya paragrafer, 3 kap. 8 och 9 §§ och 4 kap. 7, 9, 11 och 12 §§ och nya rubriker före 3 kap. 1 §, nya 3 kap. 8 § och nya 4 kap. 12 §§ av följande lydelse,

dels att det ska införas tre nya kapitel, 1, 2 och 5 kap., av följande lydelse,

dels att rubriken till lagen ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

Tullbrottsdatalag

Tullverkets brottsdatalag

1 kap. Allmänna bestämmelser

Lagens tillämpningsområde

1 § Denna lag gäller utöver brottsdatalagen (2018:000) när Tullverket i egenskap av behörig myndighet behandlar personuppgifter i syfte att bekämpa eller lagföra brott.

2 § I lagen (2017:496) om internationellt polisiärt samarbete och i föreskrifter som regeringen har meddelat i anslutning till den lagen, finns det särskilda bestämmelser om behandling av personuppgifter som följer av internationella överenskommelser om polisiärt samarbete. Om det i dessa författningar finns avvikande bestämmelser, ska de tillämpas i stället för bestämmelserna i denna lag.

Personuppgiftsansvar

3 § Tullverket är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför.

Lagens tillämpning på uppgifter om juridiska personer

4 § Bestämmelserna om personuppgifter i följande paragrafer gäller också vid behandling av uppgifter om juridiska personer:

1. 3 § om personuppgiftsansvar,
2. 2 kap. 1 § om tillåtna rättsliga grunder för behandling av personuppgifter,
3. 3 kap. 2 § om gemensamt tillgängliga uppgifter, och
4. 4 kap. 1–5 och 8–11 §§ om längsta tid som personuppgifter får behandlas.

Bestämmelserna om personuppgifter i följande paragrafer i brottsdatalagen (2018:000) gäller också vid sådan behandling:

1. 2 kap. 2 § om diarieföring och handläggning i vissa fall,
2. 2 kap. 3 § andra stycket om ändamålet med behandlingen,

3. 2 kap. 17 § om längsta tid som personuppgifter får behandlas,
4. 2 kap. 4 och 22 §§ om behandling för nya ändamål, och
5. 3 kap. 6 § om tillgången till personuppgifter.

2 kap. Grundläggande bestämmelser om behandling

Tillåtna rättsliga grunder för behandling av personuppgifter

1 § Tullverket får behandla personuppgifter om det är nödvändigt för att utföra en arbetsuppgift i syfte att

1. förebygga, förhindra eller upptäcka brottslig verksamhet,
2. utreda eller lagföra brott, eller
3. fullgöra förpliktelser som följer av internationella åtaganden.

Arbetsuppgiften ska framgå av en bindande unionsrättsakt eller av en lag, en förordning eller ett särskilt beslut i vilket regeringen uppdragit åt myndigheten att ansvara för en sådan uppgift.

2 § Förutsättningarna för att behandla personuppgifter, som behandlas med stöd av 1 §, för nya ändamål regleras i 2 kap. 4 och 22 §§ brottsdatalagen (2018:000).

Särskilda upplysningar

3 § Bestämmelserna i 2 kap. 3 § andra stycket, 9 och 10 §§ brottsdatalagen (2018:000) om särskild upplysning gäller endast vid behandling av personuppgifter som har gjorts gemensamt tillgängliga med stöd av 3 kap. 2 §.

Känsliga personuppgifter

4 § Tullverket får behandla biometriska uppgifter enligt de förutsättningar som anges i 2 kap. 12 § brottsdatalagen (2018:000).

5 § Sökförbudet i 2 kap. 14 § brottsdatalagen (2018:000) hindrar inte att brottsrubriceringar, uppgifter om tillvägagångssätt vid brott eller uppgifter som beskriver en persons utseende används vid sökning.

6 § Sökförbudet i 2 kap. 14 § brottsdatalagen (2018:000) hindrar inte sökningar i syfte att få fram ett personurval grundat på etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller uppgifter som rör hälsa, sexualliv eller sexuell läggning om sökningen görs i personuppgifter som inte har gjorts gemensamt tillgängliga.

Utlämnande av personuppgifter

7 § Om det är förenligt med svenska intressen, får personuppgifter lämnas ut till

1. Interpol,
2. Europol,
3. en polismyndighet eller åklagarmyndighet i en stat som är ansluten till Interpol, eller
4. en tullmyndighet eller kustbevakningsmyndighet inom Europeiska ekonomiska samarbetsområdet (EES).

Personuppgifter får lämnas ut enligt första stycket endast om mottagaren behöver uppgifterna för något av de syften som anges i 1 §.

Personuppgifter får vidare lämnas ut till en utländsk myndighet eller mellanfolklig organisation, om utlämnandet följer av en internationell överenskommelse som Sverige har tillträtt efter riksdagens godkännande.

8 § Polismyndigheten, Säkerhetspolisen, Ekobrottsmyndigheten, Åklagarmyndigheten, Kustbevakningen och Skatteverket har, trots sekretess enligt 21 kap. 3 § första stycket och 35 kap. 1 § offentlighets- och sekretesslagen (2009:400), rätt att ta del av personuppgifter som har gjorts gemensamt tillgängliga med stöd av 3 kap. 2 §, om den mottagande myndigheten behöver uppgifterna för något av de syften som anges i 1 kap. 2 § brottsdatalagen (2018:000).

9 § Personuppgifter får lämnas ut elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt.

Utlämnande genom direktåtkomst är tillåtet bara i den utsträckning som anges i 3 kap. 7 §.

Personuppgifter från transportföretag

10 § Personuppgifter som tillhandahålls Tullverket enligt 15 § lagen (1996:701) om Tullverkets befogenheter vid Sveriges gräns mot ett annat land inom Europeiska unionen eller 4 kap. 6 § tulllagen (2016:253) får behandlas för att planera kontroller och välja ut kontrollobjekt för något av de syften som anges i 1 § första stycket 1 eller 2.

Personuppgifter som avses i första stycket får endast i ett enskilt fall behandlas för nya ändamål enligt 2 kap. 4 eller 22 § brottsdatalogen (2018:000).

11 § Vid terminalåtkomst enligt 16 § lagen (1996:701) om Tullverkets befogenheter vid Sveriges gräns mot ett annat land inom Europeiska unionen eller 4 kap. 8 § tulllagen (2016:253) får Tullverket inte ändra eller på annat sätt bearbeta personuppgifterna.

12 § Vid sökning i personuppgifter som avses i 10 § första stycket får namn, personnummer, samordningsnummer och andra liknande identitetsbeteckningar användas som sökbegrepp endast om uppgifterna avser en person som

1. är eller har varit misstänkt för brott,
2. är misstänkt för att ha utövat eller komma att utöva sådan brottslig verksamhet som avses i 3 kap. 2 § första stycket 1, eller
3. övervakas under de förutsättningar som anges i 3 kap. 2 § första stycket 2.

Föreskrifter

13 § Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om

1. att personuppgifter får lämnas ut i andra fall än som anges i 7 och 8 §§, och
2. begränsning av möjligheten att lämna ut personuppgifter elektroniskt enligt 9 § första stycket.

3 kap.

Allmän bestämmelse

1 §

Detta kapitel innehåller särskilda bestämmelser för behandling av personuppgifter som görs eller har gjorts gemensamt tillgängliga *i Tullverkets brottsbekämpande verksamhet*. Uppgifter som endast ett fåtal personer har rätt att ta del av anses inte som gemensamt tillgängliga.

Detta kapitel gäller inte när personuppgifter behandlas med stöd av 2 kap. 7 §.

Detta kapitel innehåller särskilda bestämmelser för behandling av personuppgifter som görs eller har gjorts gemensamt tillgängliga *med stöd av 2 §*. Uppgifter som endast ett fåtal personer har rätt att ta del av anses inte som gemensamt tillgängliga.

Detta kapitel gäller inte när personuppgifter behandlas med stöd av 2 kap. 2 § *brottsofflagen (2018:000)*.

2 §

Följande personuppgifter får göras gemensamt tillgängliga:

1. Uppgifter som kan antas ha samband med misstänkt brottslig verksamhet, om den misstänkta verksamheten

a) innefattar brott för vilket det är föreskrivet fängelse i ett år eller däröver, eller

b) sker systematiskt.

2. Uppgifter som behövs för övervakningen av en person, *om han eller hon*

a) kan antas komma att begå brott för vilket det är föreskrivet fängelse i två år eller däröver, och

b) är allvarligt kriminellt belastad.

3. Uppgifter som förekommer i ett ärende om utredning eller *beivrande av brott*.

4. Uppgifter som *behövs för att fullgöra internationella åtaganden, om det krävs för att den aktuella förpliktelsen ska kunna fullgöras*.

2. Uppgifter som behövs för övervakningen av en person *som*

3. Uppgifter som förekommer i ett ärende om utredning *av eller lagföring för brott*.

4. Uppgifter som *har rapporterats till Tullverkets ledningscentraler*.

5. Uppgifter som *har rapporterats till Tullverkets kommunikationscentral.*

5. Uppgifter som *behandlas i syfte att fullgöra internationella åtaganden, om det krävs för att den aktuella förpliktelsen ska kunna fullgöras.*

Personuppgifter från transportföretag som behandlas enligt 2 kap. 10 § första stycket får göras gemensamt tillgängliga endast om det behövs i ett enskilt fall.

Tillgången till uppgifter som görs gemensamt tillgängliga med stöd av första stycket 2 ska begränsas till särskilt angivna tjänstemän som har till uppgift att arbeta med övervakningen. Information om att en person är föremål för övervakning får dock göras tillgänglig för andra.

3 §

För gemensamt tillgängliga uppgifter ska det genom en särskild upplysning eller på något annat sätt framgå för vilket närmare ändamål personuppgifterna behandlas. Har personuppgifterna gjorts gemensamt tillgängliga med stöd av 2 § första stycket 2, ska detta särskilt framgå.

Det ska framgå genom en särskild upplysning eller på något annat sätt om personuppgifter har gjorts gemensamt tillgängliga med stöd av 2 § första stycket 2.

4 §

Om uppgifter som är gemensamt tillgängliga direkt kan hänföras till en person som inte är misstänkt *för brott eller* för att ha utövat eller komma att utöva sådan brottslig verksamhet som avses i 2 § första stycket 1, ska det genom en särskild upplysning eller på annat sätt framgå att personen inte är misstänkt.

Uppgifter om en person som

Om uppgifter som är gemensamt tillgängliga direkt kan hänföras till en person som inte är misstänkt för att ha utövat eller komma att utöva sådan brottslig verksamhet som avses i 2 § första stycket 1, ska det genom en särskild upplysning eller på något annat sätt framgå att personen inte är misstänkt.

Uppgifter om en person som

kan antas ha samband med *misstänkt* brottslig verksamhet ska försees med en upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak, om inte *detta* är onödigt *på grund av särskilda omständigheter*. *Detsamma gäller uppgifter om personer som avses i 2 § första stycket 2.*

kan antas ha *direkt* samband med *sådan* brottslig verksamhet som avses i 2 § första stycket 1 eller som övervakas med stöd av 2 § första stycket 2 ska försees med en upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak, om det inte *på grund av omständigheterna* är onödigt.

5 §

Vid sökning på namn, personnummer, samordningsnummer eller andra liknande identitetsbeteckningar i uppgifter som har gjorts gemensamt tillgängliga får endast sådana uppgifter tas fram som anger att den sökta personen

Vid sökning i *automatiserade behandlingssystem* på namn, personnummer, samordningsnummer eller andra liknande identitetsbeteckningar i uppgifter som har gjorts gemensamt tillgängliga får endast sådana uppgifter tas fram som anger att den sökta personen

1. är anmäld för brott,
2. är eller har varit misstänkt för brott,
3. är misstänkt för att ha utövat eller komma att utöva sådan brottslig verksamhet som avses i 2 § första stycket 1,
4. övervakas enligt 2 § första stycket 2,
5. har anmält ett brott,
6. är målsägande i ett ärende som rör ansvar för brott,
7. förekommer i ett ärende som vittne eller annan som lämnar eller har lämnat uppgifter eller yttrande,
8. har gett in eller tillhandahållits en handling,
9. har bedömts kunna komma att möta ett ingripande med grovt våld, eller
10. är efterlyst.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om begränsning av tillgången till

sådana uppgifter som avses i första stycket.

6 §

Bestämmelserna i 6 § gäller inte vid

1. sökning i en viss handling eller i ett visst ärende, eller

2. sökning i en uppgiftssamling som har skapats för att undersöka viss brottslighet eller vissa kriminella grupperingar och som enbart de som arbetar i undersökningen har åtkomst till.

Bestämmelserna i 6 § gäller inte heller vid sökning som utförs av särskilt angivna tjänstemän och som görs

1. för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott för vilket det är föreskrivet fängelse i fyra år eller däröver eller för sådant ändamål som avses i 2 § första stycket 2, eller

2. för att utreda brott för vilket det är föreskrivet fängelse i fyra år eller däröver.

Regeringen eller den myndighet som regeringen bestämmer

Bestämmelserna i 5 § gäller inte vid sökning i en viss handling eller i ett visst ärende.

Bestämmelserna i 5 § gäller inte heller vid sökning som görs av särskilt angivna tjänstemän

1. när de utför beredningsuppgifter i underrättelseverksamhet och arbetet befinner sig i ett inledande skede,

2. i syfte att i underrättelseverksamhet bearbeta och analysera personuppgifter som har gjorts gemensamt tillgängliga med stöd av 2 § första stycket 1 eller 2 och som enbart dessa tjänstemän har tillgång till,

3. i syfte att utreda brott för vilket det är föreskrivet fängelse i fyra år eller däröver, eller

4. i syfte att samordna utredningar om brott som kan vara systematiska och för vilka det är föreskrivet fängelse i två år eller däröver.

Bestämmelserna i 5 § gäller inte heller vid sökning som en

kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om under vilka förutsättningar sökning får äga rum med stöd av första och andra styckena. Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om ytterligare undantag från 6 §.

tjänsteman vid någon av Tullverkets ledningscentraler utför på begäran av en tulltjänsteman som verkställer ett ingripande eller vidtar en åtgärd som rör en enskild.

7 §

Polismyndigheten, Säkerhetspolisen, Ekobrottsmyndigheten, Åklagarmyndigheten, Kustbevakningen och Skatteverket får medges direktåtkomst till personuppgifter i Tullverkets brottsbekämpande verksamhet. Direktåtkomsten får endast avse personuppgifter som är gemensamt tillgängliga.

Polismyndigheten, Säkerhetspolisen, Ekobrottsmyndigheten, Åklagarmyndigheten, Kustbevakningen och Skatteverket får för något av de syften som anges i 1 kap. 2 § brottsdatalagen (2018:000) medges direktåtkomst till personuppgifter som har gjorts gemensamt tillgängliga med stöd av 2 §.

En myndighet som har medgetts direktåtkomst ansvarar för att tillgången till personuppgifter begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela närmare föreskrifter om omfattningen av direktåtkomsten samt om behörighet och säkerhet.

Föreskrifter

8 §

Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om ytterligare undantag från 5 §.

9 §

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om

1. begränsning av tillgången till sådana personuppgifter som avses i 5 §,

2. under vilka förutsättningar sökning får utföras med stöd av 6 §, och

3. omfattningen av direktåtkomst enligt 7 § och behörighet och säkerhet vid sådan åtkomst.

4 kap. Bevarande och gallring av personuppgifter

4 kap. Längsta tid som personuppgifter får behandlas

Generella bestämmelser

Allmän bestämmelse

1 §

Detta kapitel gäller, om inte annat sägs, bara för automatiserad behandling.

Personuppgifter får inte bevaras under längre tid än vad som behövs för något eller några av de ändamål som anges i lagen.

Av 2 kap. 17 § första stycket brottsdatalogen (2018:000) framgår att personuppgifter inte får behandlas under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen.

I följande paragrafer anges hur länge uppgifter som behandlas automatiserat längst får bevaras:

1. 3 och 4 §§ om uppgifter som inte har gjorts gemensamt tillgängliga,

2. 5–7 §§ om uppgifter i ärenden om utredning eller beivrande av brott som har gjorts gemensamt tillgängliga, och

3. 9 och 10 §§ om andra uppgifter som har gjorts gemensamt tillgängliga än som anges i 2.

2 §

Personuppgifter som behandlas automatiserat och som inte har gjorts gemensamt tillgängliga ska, om de behandlas i ett ärende, gallras senast ett år efter det att ärendet avslutades. Om de inte kan hänföras till ett ärende, ska uppgifterna gallras senast ett år efter det att de behandlades automatiserat första gången.

Första stycket gäller inte personuppgifter i ärenden om utredning eller *beivrande av brott*.

Trots det som sägs i 2 kap. 17 § andra stycket brottsdatalogen (2018:000) får personuppgifter som inte har gjorts gemensamt tillgängliga inte behandlas längre än

1. ett år efter det att ärendet avslutades, om de behandlas i ett ärende, eller

2. ett år efter det att de behandlades automatiserat första gången, om de inte kan hänföras till ett ärende.

Första stycket gäller inte personuppgifter i ärenden om utredning *av* eller *lagföring för brott*.

3 §

I 4 kap. 8 § tullagen (2016:253) och 16 § lagen (1996:701) om Tullverkets befogenheter vid Sveriges gräns mot ett annat land inom Europeiska unionen

Personuppgifter som med stöd av 15 § lagen (1996:701) om Tullverkets befogenheter vid Sveriges gräns mot ett annat land inom Europeiska unionen

finns bestämmelser om lagring och förstöring av vissa uppgifter från transportföretag.

eller 4 kap. 6 § tullagen (2016:253) tillhandahålls på annat sätt än genom terminalåtkomst ska omedelbart förstöras, om de visar sig sakna betydelse för något av de syften som anges i 2 kap. 1 § första stycket 1 eller 2.

Det som sägs i första stycket gäller också vid behandling av personuppgifter som ingår i en strukturerad samling personuppgifter.

Gemensamt tillgängliga uppgifter i ärenden om utredning eller beivrande av brott

Gemensamt tillgängliga uppgifter i ärenden om utredning av eller lagföring för brott

4 §

Om en brottsanmälan avskrivs på grund av att den påstådda gärningen inte utgör brott, får personuppgifterna i anmälan inte längre behandlas i *Tullverkets brottsbekämpande verksamhet*. Om en brottsanmälan i annat fall inte har lett till förundersökning eller annan motsvarande utredning, får personuppgifterna inte behandlas i *Tullverkets brottsbekämpande verksamhet* när åtal inte längre får väckas för brottet.

Om en brottsanmälan avskrivs på grund av att den påstådda gärningen inte utgör brott, får personuppgifterna i anmälan inte längre behandlas för ändamål inom denna lags tillämpningsområde. Om en brottsanmälan i annat fall inte har lett till förundersökning eller annan motsvarande utredning, får personuppgifterna inte behandlas för ändamål inom denna lags tillämpningsområde när åtal inte längre får väckas för brottet.

5 §

Om en förundersökning har lett till åtal eller annan domstolsprövning, får personupp-

Om en förundersökning har lett till åtal eller annan domstolsprövning, får personupp-

gifterna i förundersökningen inte behandlas *i Tullverkets brottbekämpande verksamhet när det har förflutit fem år efter utgången av det kalenderår då domen, eller det beslut som meddelades med anledning av talan,* fick laga kraft.

Om en förundersökning har lagts *ned* eller avslutats på annat sätt än genom åtal, får personuppgifterna i förundersökningen inte behandlas *i Tullverkets brottbekämpande verksamhet när det har förflutit fem år efter utgången av det kalenderår då åklagarens eller förundersökningsledarens beslut meddelades.*

Första och andra styckena gäller även personuppgifter i andra utredningar som handläggs enligt bestämmelser i 23 kap. rättegångsbalken.

gifterna i förundersökningen inte behandlas *för ändamål inom denna lags tillämpningsområde längre än fem år efter utgången av det kalenderår då domstolens avgörande* fick laga kraft.

Om en förundersökning har lagts *ner* eller avslutats på annat sätt än genom åtal, får personuppgifterna i förundersökningen inte behandlas *för ändamål inom denna lags tillämpningsområde längre än fem år efter utgången av det kalenderår då åklagarens eller förundersökningsledarens beslut meddelades.*

7 §

Trots det som sägs i 2 kap. 17 § andra stycket brottsdatalagen (2018:000) får personuppgifter som har gjorts gemensamt tillgängliga med stöd av 3 kap. 2 § första stycket 1, 2, 4 eller 5 som längst behandlas under den tid som anges i 8–11 §§.

8 §

Personuppgifter som har gjorts gemensamt tillgängliga enligt 3 kap. 2 § första stycket 1 eller 2 ska gallras enligt andra–fjärde styckena.

Personuppgifter som kan antas ha samband med sådan brottslig verksamhet som anges i 3 kap. 2 § första stycket 1 får, om de behandlas i ett ärende, inte behandlas längre än ett år efter det att ärendet avslutades.

Uppgifter som kan antas ha samband med sådan brottslig verksamhet som anges i 3 kap. 2 § första stycket 1 ska gallras senast tre år efter utgången av det kalenderår då registreringen avseende personen gjordes. Uppgifter som kan antas ha samband med brottslig verksamhet som innefattar brott för vilket det är föreskrivet fängelse i två år eller däröver ska dock gallras senast fem år efter utgången av det kalenderår då registreringen gjordes. Om en ny registrering beträffande personen görs före utgången av gallringsfristen, behöver de uppgifter som finns om personen inte gallras så länge någon av uppgifterna om honom eller henne får bevaras.

Uppgifter som har behandlats i samband med sådan övervakning som avses i 3 kap. 2 § första stycket 2 ska gallras senast tio år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes.

Den tid då en misstänkt eller övervakad person avtjänar ett fängelsestraff eller genomgår

Om personuppgifterna inte behandlas i ett ärende får de inte behandlas längre än tre år efter utgången av det kalenderår då registreringen avseende personen gjordes. Personuppgifter som kan antas ha samband med brottslig verksamhet som innefattar brott för vilket det är föreskrivet fängelse i två år eller däröver får inte behandlas längre än fem år efter utgången av det kalenderår då registreringen gjordes. Om en ny registrering beträffande personens anknytning till brottslig verksamhet görs före utgången av de tiderna, får de uppgifter som finns om personen fortsätta att behandlas så länge någon av uppgifterna om honom eller henne får behandlas.

Den tid då en misstänkt person avtjänar ett fängelsestraff eller genomgår sluten ungdoms-

sluten ungdomsvård eller rättspsykiatrisk vård med särskild utskrivningsprövning ska inte räknas med vid beräkningen av de *frister* som anges i *andra och tredje styckena*.

vård eller rättspsykiatrisk vård med särskild utskrivningsprövning ska inte räknas med vid beräkningen av de *tider* som anges i *andra stycket*.

9 §

Personuppgifter som behandlas i samband med sådan övervakning som avses i 3 kap. 2 § första stycket 2 får inte behandlas längre än tio år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes.

Den tid då en övervakad person avtjänar ett fängelsestraff eller genomgår sluten ungdomsvård eller rättspsykiatrisk vård med särskild utskrivningsprövning ska inte räknas med vid beräkningen av den tid som anges i första stycket.

10 §

Personuppgifter som har gjorts gemensamt tillgängliga enligt 3 kap. 2 § första stycket 4 eller 5 ska gallras enligt andra eller tredje stycket.

Uppgifter som har behandlats med stöd av 3 kap. 2 § första stycket 4 ska gallras senast ett år efter utgången av det kalenderår då ärendet som uppgifterna behandlades i avslutades.

Uppgifter som har behandlats med stöd av 3 kap. 2 § första

Personuppgifter som behandlas med stöd av 3 kap. 2 § första stycket 4 får inte behandlas längre än ett år efter utgången av det kalenderår då de behandlades automatiserat första gången.

stycket 5 ska gallras senast ett år efter utgången av det kalenderår då de behandlades automatiserat första gången.

11 §

Personuppgifter som behandlas med stöd av 3 kap. 2 § första stycket 5 får inte behandlas längre än ett år efter utgången av det kalenderår då ärendet som uppgifterna behandlades i avslutades.

Föreskrifter

12 §

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om

1. att vissa kategorier av personuppgifter får *bevaras i den brottsbekämpande verksamheten* under längre tid än vad som anges i 6, 7, 9 och 10 §§,

2. att personuppgifter, med avvikelse från 3 § första stycket, 9 och 10 §§, får *bevaras för historiska, statistiska eller vetenskapliga ändamål*, och

3. digital arkivering.

1. att vissa kategorier av personuppgifter får *fortsätta att behandlas för ändamål inom denna lags tillämpningsområde* under längre tid än vad som anges i 4, 5 och 8–11 §§,

2. att personuppgifter, med avvikelse från 2 § första stycket och 8–11 §§, får *behandlas under längre tid för arkivändamål av allmänt intresse och vetenskapliga, statistiska eller historiska ändamål* och

3. *begränsning av behandlingen av personuppgifter för ändamål inom denna lags tillämpningsområde vid digital arkivering.*

5 kap. Administrativa sanktionsavgifter och rättsmedel

Administrativa sanktionsavgifter

1 § Sanktionsavgift får tas ut av den personuppgiftsansvarige vid överträdelse av bestämmelserna i

1. 2 kap. 1 § om tillåtna rättsliga grunder för behandling av personuppgifter,

2. 3 kap. 3 och 4 §§ om särskilda upplysningar, eller

3. 4 kap. 2–5 eller 8–11 § om längsta tid som personuppgifter får behandlas.

Sanktionsavgiften ska vara minst 50 000 kronor och högst 20 000 000 kronor.

Skadestånd

2 § Vid behandling av personuppgifter enligt denna lag eller föreskrifter som har meddelats i anslutning till den ska bestämmelsen i 7 kap. 1 § brottsdatalagen (2018:000) om skadestånd tillämpas på motsvarande sätt.

Överklagande

3 § Bestämmelser om överklagande och om vilka beslut som får överklagas finns i 7 kap. brottsdatalagen (2018:000).

1. Denna lag träder i kraft den 1 maj 2018.

2. Sanktionsavgift enligt 5 kap. 1 § får beslutas endast för överträdelser som har begåtts efter ikraftträdandet.

3. Bestämmelsen om skadestånd i 48 § personuppgiftslagen (1998:204) gäller fortfarande för skada som har orsakats före ikraftträdandet vid behandling av personuppgifter enligt denna lag eller föreskrifter som har meddelats i anslutning till den.

1.24 Förslag till lag om ändring i skattebrottsdatalagen (2017:452)

Härigenom föreskrivs i fråga om skattebrottsdatalagen (2017:452)

dels att 1 och 2 kap. ska upphöra att gälla,

dels att 3 kap. 3 och 5 §§ och 4 kap. 4 § ska upphöra att gälla,

dels att nuvarande 3 kap. 4 § ska betecknas 3 kap. 3 §, att nuvarande 3 kap. 6 § ska betecknas 3 kap. 4 § och att rubriken före nuvarande 3 kap. 5 § ska placeras före nya 3 kap. 4 §, att nuvarande 3 kap. 7 § ska betecknas 3 kap. 5 §, att nuvarande 3 kap. 8 § ska betecknas 3 kap. 6 § och att rubriken före nuvarande 3 kap. 8 § ska placeras före nya 3 kap. 6 §, att nuvarande 4 kap. 2 § ska betecknas 4 kap. 9 §, att nuvarande 4 kap. 3 § ska betecknas 4 kap. 2 § och att rubriken före nuvarande 4 kap. 3 § ska placeras före nya 4 kap. 2 §, att nuvarande 4 kap. 5 § ska betecknas 4 kap. 3 § och att rubriken före nuvarande 4 kap. 4 ska placeras före nya 4 kap. 3 §, att nuvarande 4 kap. 6 § ska betecknas 4 kap. 4 §, att nuvarande 4 kap. 7 § ska betecknas 4 kap. 5 §, att nuvarande 4 kap. 8 § ska betecknas 4 kap. 7 § och att rubriken före nuvarande 4 kap. 8 § ska placeras före nya 4 kap. 6 §,

dels att 3 kap. 1 och 2 §§ och nya 3 kap. 3–6 §§, 4 kap. 1 § och nya 4 kap. 2–4, 7 och 9 §§, rubriken till 4 kap. och rubriken före 4 kap. 1 § ska ha följande lydelse,

dels att det ska införas fyra nya paragrafer, 3 kap. 7 och 8 §§ och 4 kap. 6 och 8 §§ och nya rubriker före 3 kap. 1 §, nya 3 kap. 7 § och nya 4 kap. 9 § av följande lydelse,

dels att det ska införas tre nya kapitel, 1, 2 och 5 kap., av följande lydelse,

dels att rubriken till lagen ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

Skattebrottsdatalag

Skatteverkets brottsdatalag

1 kap. Allmänna bestämmelser

Lagens tillämpningsområde

1 § Denna lag gäller utöver brottsdatalagen (2018:000) när Skatteverket i egenskap av behörig myndighet behandlar personuppgifter i syfte att bekämpa brott.

Personuppgiftsansvar

2 § Skatteverket är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför.

Lagens tillämpning på uppgifter om juridiska personer

3 § Bestämmelserna om personuppgifter i följande paragrafer gäller också vid behandling av uppgifter om juridiska personer:

1. 2 § om personuppgiftsansvar,
2. 2 kap. 1 § om tillåtna rättsliga grunder för behandling av personuppgifter,
3. 3 kap. 2 § om gemensamt tillgängliga uppgifter, och
4. 4 kap. 1–4 och 7 och 8 §§ om längsta tid som personuppgifter får behandlas.

Bestämmelserna om personuppgifter i följande paragrafer i brottsdatalagen (2018:000) gäller också vid sådan behandling:

1. 2 kap. 2 § om diarieföring och handläggning i vissa fall,
2. 2 kap. 3 § andra stycket om ändamålet med behandlingen,
3. 2 kap. 17 § om längsta tid som personuppgifter får behandlas,
4. 2 kap. 4 och 22 §§ om behandling för nya ändamål, och
5. 3 kap. 6 § om tillgången till personuppgifter.

2 kap. Grundläggande bestämmelser om behandling

Tillåtna rättsliga grunder för behandling av personuppgifter

1 § Skatteverket får behandla personuppgifter om det är nödvändigt för att utföra en arbetsuppgift i syfte att

1. förebygga, förhindra eller upptäcka brottslig verksamhet,
2. utreda brott, eller
3. fullgöra förpliktelser som följer av internationella åtaganden.

Arbetsuppgiften ska framgå av en bindande unionsrättsakt eller av en lag, en förordning eller ett särskilt beslut i vilket regeringen uppdragit åt myndigheten att ansvara för en sådan uppgift.

2 § Förutsättningarna för att behandla personuppgifter, som behandlas med stöd av 1 §, för nya ändamål regleras i 2 kap. 4 och 22 §§ brottsdatalagen (2018:000).

Särskilda upplysningar

3 § Bestämmelserna i 2 kap. 3 § andra stycket, 9 och 10 §§ brottsdatalagen (2018:000) om särskild upplysning gäller endast vid behandling av personuppgifter som har gjorts gemensamt tillgängliga med stöd av 3 kap. 2 §.

Sökning

Känsliga personuppgifter

4 § Sökförbudet i 2 kap. 14 § brottsdatalagen (2018:000) hindrar inte att uppgifter som beskriver en persons utseende används vid sökning.

5 § Sökförbudet i 2 kap. 14 § brottsdatalagen (2018:000) hindrar inte sökning i syfte att få fram ett personurval grundat på etniskt ursprung, om sökningen görs i personuppgifter som inte har gjorts gemensamt tillgängliga.

Beskattningsdatabasen

6 § I lagen (2001:181) om behandling av uppgifter i Skatteverkets beskattningsverksamhet finns bestämmelser om beskattningsdatabasen. Vid sökning i beskattningsdatabasen som görs för något av de syften som anges i 1 § får endast uppgift om namn, personnummer eller samordningsnummer användas.

Utlämnande av personuppgifter

7 § Personuppgifter får lämnas ut till en utländsk myndighet eller mellanfolklig organisation, om utlämnandet följer av en internationell överenskommelse som Sverige har tillträtt efter riksdagens godkännande.

8 § Polismyndigheten, Säkerhetspolisen, Ekobrottsmyndigheten, Åklagarmyndigheten, Kustbevakningen och Tullverket har, trots sekretess enligt 21 kap. 3 § första stycket och 35 kap. 1 § offentlighets- och sekretesslagen (2009:400), rätt att ta del av personuppgifter som har gjorts gemensamt tillgängliga med stöd av 3 kap. 2 §, om den mottagande myndigheten behöver uppgifterna för något av de syften som anges i 1 kap. 2 § brottsdatalagen (2018:000).

9 § Personuppgifter får lämnas ut elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt.

Utlämnande genom direktåtkomst är tillåtet bara i den utsträckning som anges i 3 kap. 6 §.

Föreskrifter

10 § Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om

1. att personuppgifter får lämnas ut i andra fall än som anges i 7 och 8 §§, och

2. begränsning av möjligheten att lämna ut personuppgifter elektroniskt enligt 9 § första stycket.

3 kap.

Allmän bestämmelse

1 §

Detta kapitel innehåller särskilda bestämmelser för behandling av personuppgifter som görs eller har gjorts gemensamt tillgängliga *i Skatteverkets brottsbekämpande verksamhet*. Uppgifter som endast ett fåtal personer har rätt att ta del av anses inte som gemensamt tillgängliga.

Detta kapitel gäller inte när personuppgifter behandlas med stöd av 2 kap. 7 §.

Detta kapitel innehåller särskilda bestämmelser för behandling av personuppgifter som görs eller har gjorts gemensamt tillgängliga *med stöd av 2 §*. Uppgifter som endast ett fåtal personer har rätt att ta del av anses inte som gemensamt tillgängliga.

Detta kapitel gäller inte när personuppgifter behandlas med stöd av 2 kap. 2 § *brottsdatalagen (2018:000)*.

2 §

Följande personuppgifter får göras gemensamt tillgängliga:

1. Uppgifter som kan antas ha samband med misstänkt brottslig verksamhet, om den misstänkta verksamheten

a) innefattar brott för vilket det är föreskrivet fängelse i ett år eller däröver, eller

b) sker systematiskt.

2. Uppgifter som förekommer i ett ärende om utredning av brott.

3. *Uppgifter som behövs för att fullgöra internationella åtaganden, om det krävs för att den aktuella förpliktelsen ska kunna fullgöras.*

3. *Uppgifter som behandlas i syfte att fullgöra internationella åtaganden, om det krävs för att den aktuella förpliktelsen ska kunna fullgöras.*

3 §

Om uppgifter som är gemensamt tillgängliga direkt kan hänföras till en person som inte är misstänkt *för brott eller* för att

Om uppgifter som är gemensamt tillgängliga direkt kan hänföras till en person som inte är misstänkt för att ha utövat

ha utövat eller komma att utöva sådan brottslig verksamhet som avses i 2 § första stycket 1, ska det genom en särskild upplysning eller på annat sätt framgå att personen inte är misstänkt.

Uppgifter om en person som kan antas ha samband med *misstänkt* brottslig verksamhet ska förses med en upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak, om inte *detta* är onödigt *på grund av särskilda omständigheter*.

eller komma att utöva sådan brottslig verksamhet som avses i 2 § 1, ska det genom en särskild upplysning eller på något annat sätt framgå att personen inte är misstänkt.

Uppgifter om en person som kan antas ha *direkt* samband med *sådan* brottslig verksamhet som avses i 2 § 1 ska förses med en upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak, om *det* inte *på grund av omständigheterna* är onödigt.

4 §

Vid sökning på namn, personnummer, samordningsnummer eller andra liknande identitetsbeteckningar i uppgifter som har gjorts gemensamt tillgängliga får endast sådana uppgifter tas fram som anger att den sökta personen

1. är anmäld för brott,
2. är eller har varit misstänkt för brott,
3. är misstänkt för att ha utövat eller komma att utöva sådan brottslig verksamhet som avses i 2 § första stycket 1,
4. har anmält ett brott,
5. är målsägande i ett ärende som rör ansvar för brott,
6. förekommer i ett ärende som vittne eller annan som lämnar eller har lämnat uppgifter eller yttrande,
7. har gett in eller tillhandahållits en handling,
8. har bedömts kunna komma att möta ett ingripande med grovt våld, eller

Vid sökning *i automatiserade behandlingssystem* på namn, personnummer, samordningsnummer eller andra liknande identitetsbeteckningar i uppgifter som har gjorts gemensamt tillgängliga får endast sådana uppgifter tas fram som anger att den sökta personen

3. är misstänkt för att ha utövat eller komma att utöva sådan brottslig verksamhet som avses i 2 § 1,

9. är eller har varit registrerad som funktionär i en eller flera juridiska personer vilka kan antas ha samband med brottslig verksamhet.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om begränsning av tillgången till sådana uppgifter som avses i första stycket.

5 §

Bestämmelserna i 6 § gäller inte vid

1. sökning i en viss handling eller i ett visst ärende, eller

2. sökning i en uppgiftssamling som har skapats för att undersöka viss brottslighet eller vissa kriminella grupperingar och som enbart de som arbetar i undersökningen har åtkomst till.

Bestämmelserna i 6 § gäller inte heller vid sökning som utförs av särskilt angivna tjänstemän och som görs

1. för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott för vilket det är föreskrivet fängelse i fyra år eller däröver, eller

2. för att utreda brott för vilket det är föreskrivet fängelse i

Bestämmelserna i 4 § gäller inte vid sökning i en viss handling eller i ett visst ärende.

Bestämmelserna i 4 § gäller inte heller vid sökning som görs av särskilt angivna tjänstemän

1. när de utför beredningsuppgifter i underrättelseverksamhet och arbetet befinner sig i ett inledande skede,

2. i syfte att i underrättelseverksamhet bearbeta och analysera personuppgifter som har gjorts gemensamt tillgängliga med stöd av 2 § 1 eller 2 och som enbart dessa tjänstemän har tillgång till, eller

3. i syfte att utreda brott för vilket det är föreskrivet fängelse

fyra år eller däröver.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om under vilka förutsättningar sökning får äga rum med stöd av första och andra styckena. Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om ytterligare undantag från 6 §.

i fyra år eller däröver.

6 §

Polismyndigheten, Säkerhetspolisen, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket och Kustbevakningen får medges direktåtkomst till personuppgifter i Skatteverkets brottsbekämpande verksamhet. Direktåtkomsten får endast avse personuppgifter som har gjorts gemensamt tillgängliga.

En myndighet som har medgetts direktåtkomst ansvarar för att tillgången till personuppgifter begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela närmare föreskrifter om omfattningen av direktåtkomsten samt om behörighet och säkerhet.

Polismyndigheten, Säkerhetspolisen, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket och Kustbevakningen får för något av de syften som anges i 1 kap. 2 § brottsdatalagen (2018:000) medges direktåtkomst till personuppgifter som har gjorts gemensamt tillgängliga med stöd av 2 §.

*Föreskrifter**7 §*

Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om ytterligare undantag från 4 §.

8 §

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om

1. begränsning av tillgången till sådana personuppgifter som avses i 4 §,

2. under vilka förutsättningar sökning får utföras med stöd av 5 §, och

3. omfattningen av direktåtkomst enligt 6 § och om behörighet och säkerhet vid sådan åtkomst.

4 kap. Bevarande och gallring av personuppgifter

4 kap. Längsta tid som personuppgifter får behandlas

Generella bestämmelser

Allmän bestämmelse

1 §

Detta kapitel gäller bara för automatiserad behandling.

Personuppgifter får inte bevaras under längre tid än vad som behövs för något eller några av de ändamål som anges i lagen.

Av 2 kap. 17 § första stycket brottsdatalogen (2018:000) framgår att personuppgifter inte får behandlas under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen.

I följande paragrafer anges hur länge uppgifter som behandlas automatiserat längst får bevaras:

1. 3 § om uppgifter som inte har gjorts gemensamt tillgängliga,

2. 4–6 §§ om uppgifter i ärenden om utredning av brott som har gjorts gemensamt tillgängliga, och

3. 8 § om andra uppgifter som har gjorts gemensamt tillgängliga än som anges i 2.

2 §

Personuppgifter som behandlas automatiserat och som inte har gjorts gemensamt tillgängliga ska, om de behandlas i ett ärende, gallras senast ett år efter det att ärendet avslutades. Om de inte kan hänföras till ett ärende, ska uppgifterna gallras senast ett år efter det att de behandlades automatiserat första gången.

Första stycket gäller inte personuppgifter i ärenden om utredning av brott.

Trots det som sägs i 2 kap. 17 § andra stycket brottsdatalagen (2018:000) får personuppgifter som inte har gjorts gemensamt tillgängliga inte behandlas längre än

1. ett år efter det att ärendet avslutades, om de behandlas i ett ärende, eller

2. ett år efter det att de behandlades automatiserat första gången, om de inte kan hänföras till ett ärende.

3 §

Om en brottsanmälan avskrivs på grund av att den påstådda gärningen inte utgör brott, får personuppgifterna i anmälan inte längre behandlas i Skatteverkets brottsbekämpande verksamhet. Om en brottsanmälan i annat fall inte har lett till

Om en brottsanmälan avskrivs på grund av att den påstådda gärningen inte utgör brott, får personuppgifterna i anmälan inte längre behandlas för ändamål inom denna lags tillämpningsområde. Om en brottsanmälan i annat fall inte

förundersökning eller annan motsvarande utredning, får personuppgifterna inte behandlas i *Skatteverkets brottsbekämpande verksamhet* när åtal inte längre får väckas för brottet.

har lett till förundersökning eller annan motsvarande utredning, får personuppgifterna inte behandlas för *ändamål inom denna lags tillämpningsområde* när åtal inte längre får väckas för brottet.

4 §

Om en förundersökning har lett till åtal eller annan domstolsprövning, får personuppgifterna i förundersökningen inte behandlas i *Skatteverkets brottsbekämpande verksamhet* när det har förflutit fem år efter utgången av det kalenderår då domen, eller det beslut som meddelades med anledning av talan, fick laga kraft.

Om en förundersökning har lett till åtal eller annan domstolsprövning, får personuppgifterna i förundersökningen inte behandlas för *ändamål inom denna lags tillämpningsområde* längre än fem år efter utgången av det kalenderår då domstolens avgörande fick laga kraft.

Om en förundersökning har lagts *ned* eller avslutats på annat sätt än genom åtal, får personuppgifterna i förundersökningen inte behandlas i *Skatteverkets brottsbekämpande verksamhet* när det har förflutit fem år efter utgången av det kalenderår då åklagarens eller förundersökningsledarens beslut meddelades.

Om en förundersökning har lagts *ner* eller avslutats på annat sätt än genom åtal, får personuppgifterna i förundersökningen inte behandlas för *ändamål inom denna lags tillämpningsområde* längre än fem år efter utgången av det kalenderår då åklagarens eller förundersökningsledarens beslut meddelades.

Första och andra styckena gäller även personuppgifter i andra utredningar som handläggs enligt bestämmelser i 23 kap. rättegångsbalken.

6 §

Trots det som sägs i 2 kap. 17 § andra stycket brottsdatalogen (2018:000) får personuppgifter som har gjorts gemensamt tillgängliga med stöd av 3 kap. 2 § 1 eller 3 som längst behandlas under den tid som anges i 7 och 8 §§.

7 §

Personuppgifter som har gjorts gemensamt tillgängliga enligt 3 kap. 2 § 1 eller 3 ska gallras enligt andra och tredje styckena.

Uppgifter som kan antas ha samband med sådan brottslig verksamhet som anges i 3 kap. 2 § 1 ska gallras senast tre år efter utgången av det kalenderår då registreringen avseende personen gjordes. Uppgifter som kan antas ha samband med brottslig verksamhet som innefattar brott för vilket är föreskrivet fängelse i två år eller däröver ska dock gallras senast fem år efter utgången av det kalenderår då registreringen gjordes. Om en ny registrering beträffande personen görs före utgången av gallringsfristen, behöver de uppgifter som finns om personen inte gallras så länge någon av uppgifterna om honom eller henne får bevaras.

Uppgifter som har behandlats med stöd av 3 kap. 2 § 3 ska

Personuppgifter som kan antas ha samband med sådan brottslig verksamhet som anges i 3 kap. 2 § 1 får inte behandlas längre än tre år efter utgången av det kalenderår då registreringen avseende personen gjordes. Personuppgifter som kan antas ha samband med brottslig verksamhet som innefattar brott för vilket är föreskrivet fängelse i två år eller däröver får inte behandlas längre än fem år efter utgången av det kalenderår då registreringen gjordes. Om en ny registrering beträffande personens anknytning till brottslig verksamhet görs före utgången av de tiderna, får de uppgifter som finns om personen fortsätta att behandlas så länge någon av uppgifterna om honom eller henne får behandlas.

gallras senast ett år efter utgången av det kalenderår då ärendet som uppgifterna behandlades i avslutades.

8 §

Personuppgifter som behandlas med stöd av 3 kap. 2 § 3 får inte behandlas längre än ett år efter utgången av det kalenderår då ärendet som uppgifterna behandlades i avslutades.

Föreskrifter

9 §

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om

1. att vissa kategorier av personuppgifter får *bevaras i den brottsbekämpande verksamheten* under längre tid än vad som anges i 5, 6 och 8 §§,

2. att personuppgifter, med avvikelse från 3 § första stycket och 8 §, får *bevaras för historiska, statistiska eller vetenskapliga ändamål*, och

3. digital arkivering.

1. att vissa kategorier av personuppgifter får *fortsätta behandlas för ändamål inom denna lags tillämpningsområde* under längre tid än vad som anges i 3, 4, 7 och 8 §§,

2. att personuppgifter, med avvikelse från 2 § första stycket, 7 och 8 §§, får *behandlas under längre tid för arkivändamål av allmänt intresse och vetenskapliga, statistiska eller historiska ändamål*, och

3. *begränsning av behandlingen av personuppgifter för ändamål inom denna lags tillämpningsområde vid digital arkivering.*

5 kap. Administrativa sanktionsavgifter och rättsmedel

Administrativa sanktionsavgifter

1 § Sanktionsavgift får tas ut av den personuppgiftsansvarige vid överträdelse av bestämmelserna i

1. 2 kap. 1 § om tillåtna rättsliga grunder för behandling av personuppgifter,

2. 3 kap. 3 § om särskild upplysning, eller

3. 4 kap. 2–4, 7 eller 8 § om längsta tid som personuppgifter får behandlas.

Sanktionsavgiften ska vara minst 50 000 kronor och högst 20 000 000 kronor.

Skadestånd

2 § Vid behandling av personuppgifter enligt denna lag eller föreskrifter som har meddelats i anslutning till den ska bestämmelsen i 7 kap. 1 § brottsdatalagen (2018:000) om skadestånd tillämpas på motsvarande sätt.

Överklagande

3 § Bestämmelser om överklagande och om vilka beslut som får överklagas finns i 7 kap. brottsdatalagen (2018:000).

1. Denna lag träder i kraft den 1 maj 2018.

2. Sanktionsavgift enligt 5 kap. 1 § får beslutas endast för överträdelser som har begåtts efter ikraftträdandet.

3. Bestämmelsen om skadestånd i 48 § personuppgiftslagen (1998:204) gäller fortfarande för skada som har orsakats före ikraftträdandet vid behandling av personuppgifter enligt denna lag eller föreskrifter som meddelats i anslutning till den.

1.25 Förslag till lag om ändring i lagen (2017:496) om internationellt polisiärt samarbete¹

Härigenom föreskrivs att 6 kap. 1 §, 7 kap. 1, 3, 4 och 7 §§, 8 kap. 3 §, 9 kap. 4 och 5 §§ och 10 kap. 1–3 §§ lagen (2017:496) om internationellt polisiärt samarbete ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

6 kap.

1 §

Om inte annat följer av denna lag eller föreskrifter som regeringen har meddelat i anslutning till lagen gäller

– polisdatalagen (2010:361) för polisens behandling av personuppgifter vid internationellt polisiärt samarbete,

– kustbevakningsdatalagen (2012:145) för Kustbevakningens behandling av personuppgifter vid internationellt polisiärt samarbete, och

– tullbrottsdatalagen (2017:447) för Tullverkets behandling av personuppgifter vid internationellt polisiärt samarbete.

Om inte annat följer av denna lag eller föreskrifter som regeringen har meddelat i anslutning till lagen gäller följande författningar för respektive myndighet för behandling av personuppgifter vid internationellt polisiärt samarbete

– brottsdatalagen (2018:000),
och

– polisens brottsdatalog (2010:361),

– Kustbevakningens brottsdatalog (2012:145),

– Tullverkets brottsdatalog (2017:447), eller

¹ Observera att hänsyn inte har tagits till de förslag som lämnas i SOU 2017:29 s. 76.

– Säkerhetspolisens datalag
(2018:000).

7 kap.

1 §

Vid samarbete enligt Prüm-rådsbeslutet får ett utländskt kontaktställe medges direktåtkomst till referensuppgifter i de svenska registren över dna-profiler.

Efter en överenskommelse mellan Sverige och en annan stat får kontaktstället i den andra staten göra en automatisk jämförelse mellan sina oidentifierade dna-profiler och referensuppgifter i de svenska registren över dna-profiler.

Första och andra styckena gäller endast de register över dna-profiler som regleras i *polis-datalagen* (2010:361). Första och andra styckena gäller endast de register över dna-profiler som regleras i *polisens brottsdatalag* (2010:361).

3 §

Vid samarbete enligt Prüm-rådsbeslutet får ett utländskt kontaktställe medges direktåtkomst till referensuppgifter i svenska fingeravtrycksregister som förs med stöd av *polis-datalagen* (2010:361).

Vid samarbete enligt Prüm-rådsbeslutet får ett utländskt kontaktställe medges direktåtkomst till referensuppgifter i svenska fingeravtrycksregister som förs med stöd av *polisens brottsdatalag* (2010:361).

4 §

I syfte att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda brott får det svenska kontaktstället i enskilda fall genom direktåtkomst söka uppgifter i en annan stats fingeravtrycksregister. Uppgifter får behandlas endast i den utsträckning den andra staten tillåter det och om behandlingen i motsvarande fall hade varit tillåten i svenska fingeravtrycks-

I syfte att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda brott får det svenska kontaktstället i enskilda fall genom direktåtkomst söka uppgifter i en annan stats fingeravtrycksregister. Uppgifter får behandlas endast i den utsträckning den andra staten tillåter det och om behandlingen i motsvarande fall hade varit tillåten i svenska fingeravtrycks-

register som förs med stöd av *polisdatalagen* (2010:361).

register som förs med stöd av *polisens brottsdatalag* (2010:361).

Det svenska kontaktstället ansvarar för att kontrollera om det mottagna fingeravtrycket stämmer överens med det fingeravtryck sökningen avsåg.

7 §

Bestämmelserna i personuppgiftslagen (1998:204) om rättelse och skadestånd gäller vid behandling av personuppgifter enligt detta kapitel eller enligt föreskrifter som har meddelats i anslutning till kapitlet.

Vid behandling av personuppgifter enligt detta kapitel eller enligt föreskrifter som har meddelats i anslutning till kapitlet ska bestämmelsen i 7 kap. 1 § brottsdatalagen (2018:000) om skadestånd tillämpas på motsvarande sätt.

8 kap.

3 §

Bestämmelserna i personuppgiftslagen (1998:204) om rättelse och skadestånd gäller vid behandling av personuppgifter enligt detta kapitel eller enligt föreskrifter som har meddelats i anslutning till kapitlet.

Vid behandling av personuppgifter enligt detta kapitel eller enligt föreskrifter som har meddelats i anslutning till kapitlet ska bestämmelsen i 7 kap. 1 § brottsdatalagen (2018:000) om skadestånd tillämpas på motsvarande sätt.

9 kap.

4 §

Det är förbjudet att till tredjeland eller en internationell organisation överföra eller göra tillgängliga sådana personuppgifter som har hämtats från VIS och som har lagts in i systemet av en annan stat.

Detta är dock tillåtet i brådskande fall om

1. de villkor för sökning som anges i 1 § andra stycket är uppfyllda,
2. det är förenligt med svenska intressen att uppgifterna lämnas ut,

3. den stat som har lagt in uppgifterna i systemet samtycker till det, och

4. förutsättningarna i 33 och 34 §§ *personuppgiftslagen* (1998:204) är uppfyllda.

4. förutsättningarna i 8 kap. 1 § *brottsdatalagen* (2018:000) är uppfyllda.

5 §

Bestämmelserna i personuppgiftslagen (1998:204) om rättelse och skadestånd gäller vid behandling av personuppgifter enligt detta kapitel eller enligt föreskrifter som har meddelats i anslutning till kapitlet.

Vid behandling av personuppgifter enligt detta kapitel eller enligt föreskrifter som har meddelats i anslutning till kapitlet *ska bestämmelsen i 7 kap. 1 § brottsdatalagen (2018:000) om skadestånd tillämpas på motsvarande sätt.*

10 kap.

1 §

Vid samarbete enligt avtalet med USA får ett amerikanskt kontaktställe *trots 33 § personuppgiftslagen (1998:204)* medges direktåtkomst till referensuppgifter i svenska fingeravtrycksregister som förs med stöd av *polisdatalagen* (2010:361).

Vid samarbete enligt avtalet med USA får ett amerikanskt kontaktställe medges direktåtkomst till referensuppgifter i svenska fingeravtrycksregister som förs med stöd av *polisens brottsdatalag* (2010:361).

2 §

På begäran av behöriga myndigheter får ett svenskt kontaktställe i enskilda fall genom direktåtkomst söka uppgifter i amerikanska fingeravtrycksregister i syfte att utreda ett brott för vilket det enligt svensk lag är föreskrivet fängelse i mer än ett år. Det samma gäller om sökningen görs i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar ett sådant brott.

Uppgifter får behandlas endast om behandlingen i motsvarande fall hade varit tillåten i svenska fingeravtrycksregister som förs med stöd av *polisdata-*

Uppgifter får behandlas endast om behandlingen i motsvarande fall hade varit tillåten i svenska fingeravtrycksregister som förs med stöd av *polisens*

lagen (2010:361).

brottsdatalag (2010:361).

Det svenska kontaktstället ansvarar för att kontrollera om det mottagna fingeravtrycket stämmer överens med det fingeravtryck sökningsen avsåg.

3 §

Bestämmelserna i personuppgiftslagen (1998:204) om rättelse och skadestånd gäller vid behandling av personuppgifter enligt detta kapitel eller enligt föreskrifter som har meddelats i anslutning till kapitlet.

Vid behandling av personuppgifter enligt detta kapitel eller enligt föreskrifter som har meddelats i anslutning till kapitlet ska bestämmelsen i 7 kap. 1 § brottsdatalagen (2018:000) om skadestånd tillämpas på motsvarande sätt.

1. Denna lag träder i kraft den 1 maj 2018.

2. Bestämmelsen om skadestånd i 48 § personuppgiftslagen (1998:204) gäller fortfarande för skada som har orsakats före ikraftträdandet vid behandling av personuppgifter enligt denna lag eller föreskrifter som har meddelats i anslutning till den.

1.26 Förslag till lag om ändring i brottsdatalagen (2018:000)

Härigenom föreskrivs i fråga om brottsdatalagen (2018:000) dels att nuvarande 2 kap. 21 § ska betecknas 2 kap. 22 § och att rubriken före nuvarande 2 kap. 21 § ska placeras före nya 2 kap. 22 §, nuvarande 2 kap. 22 § ska betecknas 2 kap. 23 § och att rubriken före nuvarande 2 kap. 22 § ska placeras före nya 2 kap. 23 §, dels att 2 kap. 4, 13 och 18 §§, 6 kap. 1 § och nya 2 kap. 22 § ska ha följande lydelse, dels att det ska införas två nya paragrafer, 2 kap. 21 § och 3 kap. 16 §, och en ny rubrik före 2 kap. 21 § av följande lydelse.

Lydelse enligt SOU 2017:29

Föreslagen lydelse

2 kap.

4 §

Innan personuppgifter får behandlas för ett nytt ändamål inom denna lags tillämpningsområde ska det säkerställas att

- | | |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| <p>1. det finns en tillåten rättslig grund enligt 1 § för den nya behandlingen, och</p> <p>2. behandlingen är nödvändig</p> | <p>1. det finns en tillåten rättslig grund enligt 1 § för den nya behandlingen och</p> <p>och proportionerlig för det nya ändamålet.</p> |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|

I den utsträckning skyldighet att lämna uppgifter följer av lag eller förordning behöver någon prövning enligt första stycket inte göras. Det gäller dock inte uppgiftslämnande med stöd av 6 kap. 5 § offentlighets- och sekretesslagen.

13 §

<p>Personuppgifter som avses i 11 och 12 §§ betecknas i denna lag som känsliga personupp-</p>	<p>Personuppgifter som avses i 11 och 12 §§ betecknas som känsliga personuppgifter. Känsliga</p>
-----------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------

gifter. Känsliga personuppgifter får behandlas med stöd av 2 §. lika personuppgifter får behandlas med stöd av 2 §.

18 §

Om det inte är föreskrivet i lag eller annan författning när en viss kategori av personuppgifter inte längre får behandlas för *andra ändamål än arkivändamål*, ska den personuppgiftsansvarige årligen se över behovet av att fortsatt behandla personuppgifterna.

Om det inte är föreskrivet i lag eller annan författning när en viss kategori av personuppgifter inte längre får behandlas för *ändamål inom denna lags tillämpningsområde*, ska den personuppgiftsansvarige årligen se över behovet av att fortsatt behandla personuppgifterna.

Utlämnande av personuppgifter

21 §

Personuppgifter som är nödvändiga för att framställa rättsstatistik ska lämnas till den myndighet som ansvarar för att framställa sådan statistik.

22 §

Av artikel 2.1 d i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), i den ursprungliga lydelsen, framgår att dataskyddsförordningen ska tillämpas när en behörig myndighet behandlar personuppgifter för ändamål utanför denna lags

Av artikel 2.2 d i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), i den ursprungliga lydelsen, framgår att dataskyddsförordningen ska tillämpas när en behörig myndighet behandlar personuppgifter för ändamål utanför denna lags

tillämpningsområde.

tillämpningsområde.

Innan personuppgifter som behandlas med stöd av denna lag behandlas för ett ändamål utanför lagens tillämpningsområde ska det säkerställas att behandlingen är nödvändig och proportionerlig för det ändamålet.

I den utsträckning skyldighet att lämna uppgifter följer av lag eller förordning behöver någon prövning enligt andra stycket inte göras. Det gäller dock inte uppgiftslämnande med stöd av 6 kap. 5 § offentlighets- och sekretesslagen.

3 kap.

16 §

Den som fullgör uppgift som dataskyddsombud får inte obehörigen röja eller utnyttja det som han eller hon då har fått veta om enskilds personliga eller ekonomiska förhållanden.

I det allmännas verksamhet tillämpas offentlighets- och sekretesslagen (2009:400) i stället för första stycket.

6 kap.

1 §

Sanktionsavgift får tas ut av en personuppgiftsansvarig vid överträdelse av bestämmelser i

1. 2 kap. 1–5, 7–12, 14–18 eller 19 § andra stycket,

2. 3 kap. 2–8 §§, eller

3. 8 kap. 1–6 eller 8 §.

1. 2 kap. 1–5, 7–12, 14–18 §, 19 § andra stycket eller 22 § andra stycket,

2. 3 kap. 2–8 §, eller

Sanktionsavgift får också tas ut om en personuppgiftsansvarig inte anmäler en personuppgiftsincident enligt 3 kap. 9 § första stycket, inte dokumenterar sådana incidenter eller underlåter att bistå tillsynsmyndigheten enligt 5 kap. 5 § eller att följa tillsynsmyndighetens beslut enligt 5 kap. 7 § första stycket 2 eller 3.

Denna lag träder i kraft den 1 maj 2018.

1.27 Förslag till Säkerhetspolisens dataförordning (2018:000)

Härigenom föreskrivs följande.

1 kap. Allmänna bestämmelser

1 § I denna förordning finns kompletterande föreskrifter till Säkerhetspolisens datalag (2018:000).

2 § Uttryck som används i denna förordning har samma innebörd som i Säkerhetspolisens datalag (2018:000).

2 kap. Behandling av personuppgifter

Underrättelseskyldighet

1 § Om det visar sig att sådana personuppgifter som anges i 2 kap. 13 § eller 14 § första stycket Säkerhetspolisens datalag (2018:000) har lämnats ut ska mottagaren omedelbart underrättas om det. Detsamma gäller så långt möjligt den som har tagit del av sådana personuppgifter som har gjorts tillgängliga.

2 § En underrättelse enligt 3 kap. 7 § andra stycket Säkerhetspolisens datalag (2018:000) ska göras innan Säkerhetspolisen första gången medger en utländsk underrättelse- eller säkerhetstjänst direktåtkomst. Av underrättelsen ska omfattningen av direktåtkomsten framgå.

Utlämnande av personuppgifter

3 § Säkerhetspolisen får meddela närmare föreskrifter om vad som krävs i fråga om behörighet och säkerhet för att myndigheten ska kunna medge direktåtkomst för de myndigheter som anges i 3 kap. 5 och 6 §§ Säkerhetspolisens datalag (2018:000).

Direktåtkomst till uppgifterna får inte medges innan Säkerhetspolisen har försäkrat sig om att den mottagande myndigheten uppfyller kraven på behörighet och säkerhet.

3 kap. Längsta tid för behandling m.m.

Rutiner för att säkerställa tidsfristerna

1 § Säkerhetspolisen ska se till att det finns rutiner för att säkerställa att de som behandlar personuppgifter respekterar fristerna för när personuppgifter inte längre får behandlas.

Digital arkivering

2 § När Säkerhetspolisen arkiverar uppgifter och handlingar digitalt ska de arkiverade uppgifterna och handlingarna avskiljas så att de inte kan behandlas för något av de syften som anges i 2 kap. 1 eller 2 § Säkerhetspolisens datalag (2018:000). Åtkomsten till arkiverade uppgifter och handlingar ska begränsas till särskilt angivna tjänstemän.

Säkerhetspolisen får, efter att ha gett Riksarkivet tillfälle att yttra sig, meddela närmare föreskrifter om digital arkivering.

Fortsatt behandling av vissa personuppgifter

3 § I 4–6 §§ föreskrivs att vissa kategorier av personuppgifter i brottanmälningar och avslutade förundersökningar får behandlas för syften som anges i 2 kap. 1 § första stycket 2 Säkerhetspolisens datalag (2018:000), trots att den tid som anges i 4 kap. 3 eller 4 § samma lag har löpt ut. Detsamma gäller personuppgifter i andra utredningar som handläggs enligt bestämmelser i 23 kap. rättegångsbalken.

När personuppgifter får behandlas enligt 4–6 §§ får, utöver vad som sägs i de bestämmelserna, följande uppgifter behandlas:

1. ärendenummer eller liknande referensuppgifter,
2. brottskoder, och
3. uppgifter om omständigheterna kring brottet.

4 § Uppgifter om den dömd i en förundersökning som lett till fällande dom får behandlas trots att den tid som anges i 4 kap. 4 § första stycket Säkerhetspolisens datalag (2018:000) har löpt ut, om behandlingen av särskilda skäl är nödvändig för att finna samband mellan olika brott eller mellan tänkbara gärningsmän.

Behandlingen ska dock upphöra senast i samband med att uppgifterna om den dömd tas bort ur belastningsregistret enligt lagen (1998:620) om belastningsregister.

5 § Uppgifter om en person som har varit misstänkt i en förundersökning som har lagts ner eller har avslutats på annat sätt än genom åtal, får i ett enskilt fall behandlas trots att den tid som anges i 4 kap. 4 § andra stycket Säkerhetspolisens datalag (2018:000) har löpt ut, om behandlingen är nödvändig för att trots detta kunna lagföra personen.

Behandlingen ska dock upphöra senast då åtal inte längre får väckas för brottet eller, i fall som avses i 35 kap. 2 § första stycket brottsbalken, senast sjuttio år från den dag då brottet begicks.

6 § Uppgifter om personer som har dömts för, eller har varit misstänkta för, brott där det finns en betydande risk för återfall i samma eller likartad brottslighet, får behandlas trots att den tid som anges i 4 kap. 3 eller 4 § Säkerhetspolisens datalag (2018:000) har löpt ut, om behandlingen av särskilda skäl är nödvändig för att förebygga, förhindra eller upptäcka brott för vilket fängelse i fyra år eller däröver är föreskrivet.

Behandlingen ska dock upphöra, i fråga om brott som har lett till fällande dom, senast i samband med att uppgifterna tas bort ur belastningsregistret enligt lagen (1998:620) om belastningsregister och i övriga fall senast femton år efter det att förundersökningen lades ner eller avslutades på annat sätt.

Behandling för arkivändamål av allmänt intresse m.m.

7 § Riksarkivet får, efter att ha gett Säkerhetspolisen tillfälle att yttra sig, meddela föreskrifter om att personuppgifter som avses i 4 kap. 2 och 7–11 §§ Säkerhetspolisens datalag (2018:000) får be-

handlas under längre tid för arkivändamål av allmänt intresse och vetenskapliga, statistiska eller historiska ändamål.

4 kap. Skyldigheter som personuppgiftsansvarig

Tekniska och organisatoriska åtgärder

1 § De åtgärder som Säkerhetspolisen ska vidta enligt 5 kap. 1 och 2 §§ Säkerhetspolisens datalag (2018:000) ska vara rimliga med beaktande av behandlingens art, omfattning, sammanhang och ändamål och de särskilda riskerna med behandlingen. När Säkerhetspolisen vidtar åtgärder enligt 5 kap. 2 § samma lag ska även de tekniska möjligheterna och kostnaderna för åtgärderna beaktas.

Behörigheter

2 § För tilldelning av behörighet för åtkomst till personuppgifter ska det särskilt beaktas att det, utöver behovet av uppgifterna, ställs krav på utbildning och erfarenhet.

Säkerhetspolisen ansvarar för att det inom myndigheten finns rutiner för tilldelning, förändring, borttagning och regelbunden uppföljning av behörigheter för åtkomst till personuppgifter.

Dokumentationsskyldighet

Interna strategier

3 § De åtgärder som avses i 5 kap. 1 § Säkerhetspolisens datalag (2018:000) ska, om det inte är obehövt med hänsyn till verksamhetens begränsade omfattning, innefatta antagande och dokumentation av interna strategier för dataskydd.

Register över behandlingar

4 § Säkerhetspolisen ska förteckna kategorier av behandlingar av personuppgifter som myndigheten ansvarar för. Registret ska, förutom namnet på och kontaktuppgifter till myndigheten, gemen-

samt personuppgiftsansvariga och dataskyddsbud, för varje kategori av behandling innehålla följande uppgifter.

1. Den rättsliga grunden för behandlingen.
2. Ändamålen med behandlingen.
3. Kategorier av tjänstemän som har tillgång till de personuppgifter som behandlas.
4. Kategorier av mottagare till vilka uppgifterna kan komma att lämnas ut, även i tredjeland eller internationella organisationer.
5. Kategorier av registrerade som berörs av behandlingen.
6. Kategorier av personuppgifter som kan komma att behandlas.
7. Överföringar av personuppgifter till tredjeland eller internationella organisationer.

Loggning

5 § Skyldigheten att föra loggar i automatiserade behandlingssystem enligt 5 kap. 4 § Säkerhetspolisens datalag (2018:000) ska omfatta behandlingar som innebär insamling, ändring, läsning, utlämning, överföring till tredjeland eller internationella organisationer, sammanföring och radering av personuppgifter. Loggarna över läsning och utlämning ska visa datum och tidpunkt för behandlingen och, så långt möjligt, vem som har läst eller lämnat ut personuppgifterna och vem som har fått ta del av personuppgifterna.

Konsekvensbedömning och samråd

6 § Konsekvensbedömningar som avses i 5 kap. 6 § första stycket Säkerhetspolisens datalag (2018:000) ska dokumenteras och innehålla följande uppgifter.

1. En allmän beskrivning av den planerade behandlingen.
2. En bedömning av riskerna för intrång i registrerades personliga integritet.
3. Vilka åtgärder som planeras för att hantera riskerna.
4. Åtgärder och rutiner för att säkerställa skyddet av personuppgifterna.
5. Rutiner för att visa att tillämpliga dataskyddsregler följs.

7 § Vid förhandssamråd enligt 5 kap. 6 § andra stycket Säkerhetspolisens datalag (2018:000) ska Säkerhetspolisen ge in konsekvensbedömningen till tillsynsmyndigheten och tillhandahålla den övriga information som begärs av myndigheten.

Vid bedömningen av om typen av behandling innebär sådan risk för intrång i registrerades personliga integritet att förhandssamråd ska äga rum ska ny teknik, nya rutiner eller nya förfaranden särskilt beaktas.

Anmälan av överträdelser

8 § Säkerhetspolisen ska ha interna rutiner för anmälan av överträdelser av bestämmelser om personuppgiftsbehandling som garanterar att anmälares identitet skyddas.

Säkerheten vid behandling av personuppgifter

9 § Skyddsåtgärder enligt 5 kap. 7 § Säkerhetspolisens datalag (2018:000) ska åstadkomma en skyddsnivå som är lämplig med beaktande av

1. de tekniska möjligheterna,
2. kostnaderna för åtgärderna,
3. behandlingens art, omfattning, sammanhang och ändamål,
4. de särskilda riskerna med behandlingen,
5. om känsliga personuppgifter behandlas, och
6. hur integritetskänsliga övriga personuppgifter som behandlas är.

Dataskyddsombud

10 § Säkerhetspolisen ska säkerställa att dataskyddsombud ges möjlighet att delta i de frågor som rör skyddet av personuppgifter.

Säkerhetspolisen ska se till att dataskyddsombud kan utföra de uppgifter som anges i 5 kap. 10 och 11 §§ Säkerhetspolisens datalag (2018:000) genom att tillhandahålla nödvändiga resurser, ge tillgång till dokumentation om behandling av personuppgifter och vid behov medge åtkomst till personuppgifter som behandlas. Säker-

hetspolisen ska också se till att dataskyddsombud ges möjlighet att upprätthålla sin sakkunskap.

Personuppgiftsbiträden

Avtalets eller överenskommelsens innehåll

11 § Ett avtal eller en annan överenskommelse enligt 5 kap. 13 § Säkerhetspolisens datalag (2018:000) ska åtminstone ange vad behandlingen ska avse, hur länge behandlingen ska pågå, dess art och ändamål, typen av personuppgifter, kategorier av registrerade och Säkerhetspolisens skyldigheter och rättigheter. I avtalet eller överenskommelsen ska det särskilt föreskrivas att personuppgiftsbiträdet ska

1. behandla personuppgifter bara enligt instruktioner från Säkerhetspolisen,

2. säkerställa att personer som har tillstånd att behandla personuppgifter har förbundit sig att iaktta regler om tystnadsplikt eller omfattas av lagstadgad tystnadsplikt,

3. hjälpa Säkerhetspolisen att säkerställa att bestämmelserna om registrerades rättigheter följs,

4. radera eller återlämna alla personuppgifter till Säkerhetspolisen när uppdraget har slutförts och, om inte annat följer av lag eller förordning, radera befintliga kopior,

5. ge Säkerhetspolisen tillgång till den information som krävs för att visa att det som sägs i denna paragraf, 13 § och 5 kap. 12–14 §§ Säkerhetspolisens datalag följs, och

6. respektera de villkor som framgår av denna paragraf, 12 § och 5 kap. 13 § Säkerhetspolisens datalag vid anlitan av ett annat personuppgiftsbiträde.

Underbiträden

12 § Har Säkerhetspolisen lämnat ett generellt tillstånd enligt 5 kap. 13 § andra stycket Säkerhetspolisens datalag (2018:000), ska personuppgiftsbiträdet informera Säkerhetspolisen innan nya personuppgiftsbiträden anlitas.

Register över behandlingar

13 § Varje personuppgiftsbiträde ska förteckna kategorier av behandlingar av personuppgifter som utförs för Säkerhetspolisens räkning. Registret ska innehålla namnet på och kontaktuppgifter till personuppgiftsbiträdet och Säkerhetspolisen och för varje kategori av behandling följande uppgifter.

1. Namnet på och kontaktuppgifter till eventuella underbiträden.

2. Om överföringar av personuppgifter har gjorts till ett tredjeland eller en internationell organisation, vilka uppgifter som har överförts och till vem.

3. Om möjligt, en allmän beskrivning av de säkerhetsåtgärder som har vidtagits.

Övriga skyldigheter

14 § Det som sägs om Säkerhetspolisens skyldigheter i 5 och 9 §§ gäller även för personuppgiftsbiträden som Säkerhetspolisen anlitar.

Gemensamt personuppgiftsansvariga

15 § När Säkerhetspolisen är gemensamt personuppgiftsansvarig med annan ska Säkerhetspolisen säkerställa att myndigheterna i en skriftlig överenskommelse reglerar sina respektive förpliktelser i egenskap av personuppgiftsansvariga. Överenskommelsen får inte innebära att Säkerhetspolisens författningensliga skyldigheter inte fullgörs.

Den registrerade får, trots en sådan överenskommelse som avses i första stycket, utöva sina rättigheter gentemot var och en av de personuppgiftsansvariga.

Övriga bestämmelser

16 § Innan Säkerhetspolisen meddelar föreskrifter med stöd av denna förordning i frågor som berör särskilda risker för intrång i den personliga integriteten ska myndigheten samråda med tillsynsmyndigheten.

Föreskrifter

17 § Tillsynsmyndigheten får meddela närmare föreskrifter om

1. sådana åtgärder som avses i 5 kap. 1–3 och 7 §§ Säkerhetspolisens datalag (2018:000),
2. krav och rutiner för loggning enligt 5 kap. 4 § Säkerhetspolisens datalag, och
3. vilka typer av behandlingar som ska omfattas av förhandssamråd enligt 5 kap. 6 § andra stycket Säkerhetspolisens datalag.

5 kap. Enskildas rättigheter

Krav på utformningen av information

1 § Information enligt 6 kap. 1 och 2 §§ Säkerhetspolisens datalag (2018:000) ska vara lättillgänglig och lättbegriplig och lämnas i lämplig form. Detsamma gäller information enligt 3–7 §§ denna förordning.

Enskilds begäran

2 § Begäran enligt 6 kap. 2, 6 eller 7 § Säkerhetspolisens datalag (2018:000) ska göras skriftligen hos Säkerhetspolisen.

Säkerhetspolisen ska säkerställa att begäran görs av en behörig person.

Beslut

3 § Beslut enligt 6 kap. 3 § första stycket, 5 § första stycket, 6 och 7 §§ och 9 § andra stycket Säkerhetspolisens datalag (2018:000) ska vara skriftliga. Beslut som går den registrerade emot ska motiveras.

Av 6 kap. 3 § andra stycket Säkerhetspolisens datalag framgår att skälen för vissa beslut inte behöver lämnas ut.

Underrättelser

Underrättelser till enskilda

4 § Sökanden ska underrättas om beslut enligt 6 kap. 3 § första stycket Säkerhetspolisens datalag (2018:000). Någon underrättelse behöver inte lämnas om det skulle skada det intresse som föranleder att information inte lämnas.

5 § Sökanden ska underrättas om beslut enligt 6 kap. 5 § första stycket eller 9 § andra stycket Säkerhetspolisens datalag (2018:000).

6 § Den registrerade ska underrättas om följande beslut enligt Säkerhetspolisens datalag (2018:000).

1. Beslut enligt 6 kap. 6 eller 7 §.
2. Beslut om att en begränsning enligt 6 kap. 6 § andra stycket upphör.

Underrättelser till andra

7 § Den myndighet från vilken personuppgifter kommer ska underrättas om beslut enligt 6 kap. 6 § första stycket Säkerhetspolisens datalag (2018:000).

Den som har tagit emot personuppgifter ska underrättas om beslut enligt 6 kap. 6 eller 7 § Säkerhetspolisens datalag.

6 kap. Tillsyn

Anmälningsskyldighet

1 § Om tillsynsmyndigheten i sin tillsyn uppmärksammar förhållanden som kan utgöra brott, ska myndigheten anmäla det till Åklagarmyndigheten.

Tillsynsmyndigheten ska samråda med Åklagarmyndigheten innan en sådan anmälan görs. Till anmälan ska inspektionen föga

det underlag som finns och även i övrigt lämna det bistånd som behövs i anledning av anmälan.

Förhandssamråd

2 § Om tillsynsmyndigheten anser att sådan planerad behandling som avses i 5 kap. 6 § andra stycket Säkerhetspolisens datalag (2018:000) kan komma att stå i strid med lag eller annan författning, ska myndigheten senast inom tre månader efter att en begäran om samråd mottogs skriftligen lämna råd enligt 7 kap. 4 § första stycket samma lag. Om det finns skäl för det får tiden förlängas.

3 § Tillsynsmyndigheten ska informera Säkerhets- och integritetsskyddsnämnden om att samråd enligt 5 kap. 6 § andra stycket Säkerhetspolisens datalag (2018:000) har begärts. Om det är lämpligt ska nämnden ges tillfälle att yttra sig till tillsynsmyndigheten inom ramen för samrådet. Säkerhets- och integritetsskyddsnämnden har rätt att få tillgång till underlaget för samrådet och tillsynsmyndighetens yttrande.

7 kap. Överföring av personuppgifter till tredjeland och internationella organisationer

1 § Överföringar av personuppgifter enligt 9 kap. 4 § 2 och 5 § Säkerhetspolisens datalag (2018:000) ska dokumenteras. Av dokumentationen ska framgå vilka personuppgifter som överförts, datum och tidpunkt för överföringen, ändamålet med och grunden för överföringen och till vem personuppgifterna överfördes.

2 § Överföringar av personuppgifter enligt 9 kap. 6 § Säkerhetspolisens datalag (2018:000) ska dokumenteras.

-
1. Denna förordning träder i kraft den 1 maj 2018.
 2. Bestämmelserna i 3 kap. 6 § om loggning behöver inte tillämpas på automatiserade behandlingssystem som inrättats före ikraftträdandet förrän den 1 maj 2023.

1.28 Förslag till domstolarnas brottsdataförordning (2018:000)

Härigenom föreskrivs följande.

Allmän bestämmelse

1 § I denna förordning finns kompletterande föreskrifter till domstolarnas brottsdatalag (2018:000).

Direktåtkomst

När direktåtkomst är tillåten

2 § Direktåtkomst enligt 2 kap. 12 § domstolarnas brottsdatalag (2018:000) får medges endast i de fall som anges i 3–7 §§ och med de ytterligare begränsningar som enligt 8 § gäller för direktåtkomst till personuppgifter i mål och ärenden som har avgjorts slutligt.

Direktåtkomst vid överklagande

3 § När ett mål eller ärende överklagas får den lägre domstolsinstans som har prövat målet eller ärendet medge högre domstolsinstanser direktåtkomst till personuppgifterna i målet eller ärendet och till personuppgifterna i andra mål och ärenden som har samband med det överklagade målet eller ärendet.

4 § När ett mål eller ärende överklagas får en högre domstolsinstans medge de lägre domstolsinstanser som har prövat målet eller ärendet direktåtkomst till personuppgifterna i målet eller ärendet och till personuppgifterna i andra mål och ärenden som har samband med det överklagade målet eller ärendet.

5 § Vid tillämpningen av 3 och 4 §§ ska en ansökan om resning eller om återställande av försutten tid eller en klagan över domvillan jämföras med ett överklagande.

Direktåtkomst till rättspraxis

6 § Högsta domstolen och hovrätterna får medge en allmän domstol direktåtkomst till domar och beslut. Högsta förvaltningsdomstolen och kammarrätterna får medge en allmän förvaltningsdomstol direktåtkomst till domar och beslut. Direktåtkomsten får även avse

1. uppgifter om parterna och deras ombud, biträden eller försvarare,
2. uppgifter om expediering, delgivning, överklagande och laga kraft,
3. uppgift om saken,
4. ärendemening,
5. uppgift om samband med andra mål,
6. en sammanfattning av domen eller beslutet,
7. uppgifter om domare, handläggare och andra tjänstemän vid domstolen, och
8. andra uppgifter med direkt anknytning till en dom eller ett beslut.

Direktåtkomst i samband med beredskapsverksamhet

7 § Domstolar som tillsammans deltar i beredskap får medge varandra direktåtkomst till personuppgifter som behövs för handläggningen av de mål och ärenden som omfattas av beredskapsverksamheten.

Direktåtkomst till slutligt avgjorda mål och ärenden

8 § När ett mål eller ärende har avgjorts slutligt genom en dom eller ett beslut som har fått laga kraft får direktåtkomst till personuppgifterna i målet eller ärendet medges endast under

1. sex månader efter det att domen eller beslutet fick laga kraft vid direktåtkomst enligt 3–5 §§, och
2. tjugo år efter det att domen eller beslutet fick laga kraft vid direktåtkomst enligt 6 §.

Bemyndigande

9 § Domstolsverket får meddela föreskrifter om tillgången till personuppgifter. För tilldelning av behörighet för åtkomst till personuppgifter ska det särskilt beaktas att det, utöver behovet av uppgifterna, ställs krav på utbildning och erfarenhet.

10 § Domstolsverket får meddela föreskrifter om begränsning av

1. möjligheten att lämna ut personuppgifter elektroniskt på annat sätt än genom direktåtkomst,
2. möjligheten att lämna ut personuppgifter genom direktåtkomst och om behörighet och säkerhet vid sådan åtkomst, och
3. behandling av personuppgifter som hänför sig till mål eller ärenden som har avgjorts slutligt genom dom eller beslut som har fått laga kraft.

11 § Domstolsverket får meddela de ytterligare föreskrifter som behövs för verkställighet av domstolarnas brottsdatalog (2018:000) och denna förordning.

Innan Domstolsverket meddelar föreskrifter med stöd av denna förordning, ska myndigheten samråda med Datainspektionen i frågor som berör särskilda risker för intrång i den personliga integriteten.

-
1. Denna förordning träder i kraft den 1 maj 2018.
 2. Bestämmelserna i 8 § om begränsning av direktåtkomst i fråga om slutligt avgjorda mål och ärenden behöver inte tillämpas förrän den 1 januari 2019.

1.29 Förslag till förordning (2018:000) om underrättelseskyldighet för Kriminalvården

Härigenom föreskrivs följande.

1 § Kriminalvården ska lämna underrättelse till nedan angivna myndigheter i följande fall.

Uppgift lämnas till	Uppgift lämnas om
1. Totalförsvarets rekryteringsmyndighet	<p>Intagning i eller avgång från kriminalvårdsanstalt av svenska medborgare som under kalenderåret fyller 18–47 år.</p> <p>Beslut om förlängning av verkställighetstid med minst en månad för intagen om vilken underrättelse har lämnats tidigare.</p> <p>Verkställighetens början vid verkställighet utanför anstalt i form av intensivövervakning med elektronisk kontroll och tidpunkt för verkställighetens slut för svenska medborgare som under kalenderåret fyller 18–47 år.</p>
2. Försäkringskassan	<p>Tidpunkt för frihetsberövande på grund av häktning eller hävande av häktningsbeslut.</p> <p>Tidpunkt för intagning i eller avgång från kriminalvårdsanstalt eller tidpunkt då verkställighet av fängelsestraff på</p>

annat sätt påbörjades och avslutad tidpunkt för avgång från kriminalvårdsanstalt.

Tidpunkt för påbörjad eller avslutad vårdvistelse eller utökad frigång enligt fängelselagen (2010:610).

Tidpunkt för avvikelse från kriminalvårdsanstalt eller från vistelse utanför anstalt i form av vårdvistelse eller utökad frigång enligt fängelselagen och tidpunkt för återupptagande av sådan verkställighet efter avvikelse.

Tidpunkt för påbörjad eller avslutad vistelse på statens bekostnad i ett sådant familjehem eller hem för vård eller boende som avses i socialtjänstlagen (2001:453) till följd av dom på skyddstillsyn med särskild behandlingsplan.

3. Polismyndigheten

Intagning i eller avgång från kriminalvårdsanstalt eller förflyttning till annan anstalt.

Verkställighetens början vid verkställighet utanför anstalt i form av intensivövervakning med elektronisk kontroll och tidpunkt för verkställighetens slut och vistelse utanför anstalt i form av vårdvistelse, vistelse i halvvägshus eller utökad frigång enligt fängelselagen.

Verkställighetens början i kriminalvårdsanstalt när den sammanlagda tiden att avtjäna är fängelse i minst ett år.

Permission eller avgång från kriminalvårdsanstalt, om underrättelsen kan antas vara av betydelse för myndighetens verksamhet.

4. Säkerhetspolisen

Intagning i eller avgång från kriminalvårdsanstalt och permission eller förflyttning till annan anstalt, om underrättelsen kan antas vara av betydelse för Säkerhetspolisens verksamhet.

Vistelse utanför anstalt i form av vårdvistelse, vistelse i halvvägshus eller utökad frigång enligt fängelselagen, om underrättelsen kan antas vara av betydelse för Säkerhetspolisens verksamhet.

5. Pensionsmyndigheten

Tidpunkt för frihetsberövande på grund av häktning eller hävande av häktningsbeslut.

Tidpunkt för intagning i eller avgång från kriminalvårdsanstalt eller tidpunkt då verkställighet av fängelsestraff på annat sätt påbörjades och beslutad tidpunkt för avgång från kriminalvårdsanstalt.

Tidpunkt för påbörjad eller avslutad vårdvistelse eller utökad frigång enligt fängelselagen.

Tidpunkt för avvikelser från kriminalvårdsanstalt eller från vistelse utanför anstalt i form av vårdvistelse eller utökad frigång enligt fängelselagen och tidpunkt för återupptagande av sådan verkställighet efter avvikelse.

Tidpunkt för påbörjad eller avslutad vistelse på statens bekostnad i ett sådant familjehem eller hem för vård eller boende som avses i socialtjänstlagen till följd av dom på skyddstillsyn med särskild behandlingsplan.

2 § Kriminalvården ska på Tullverkets begäran underrätta verket om var en person vistas som är häktad, intagen i kriminalvårdsanstalt eller vistas utanför kriminalvårdsanstalt i form av vårdvistelse.

3 § Bestämmelser om skyldighet för Kriminalvården att i andra fall lämna uppgifter till Polismyndigheten finns i 30 § förordningen (1999:1134) om belastningsregister.

Denna förordning träder i kraft den 1 maj 2018.

1.30 Förslag till förordning om ändring i förordningen (1970:517) om rättsväsendets informationssystem

Härigenom föreskrivs att 1 § förordningen (1970:517) om rättsväsendets informationssystem ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

1 §¹

För att samla in, lagra, bearbeta och lämna uppgifter som har samband med verksamhet inom polisen och domstolsväsendet ska personuppgifter behandlas automatiserat i rättsväsendets informationssystem. Informationssystemet ska bestå av delsystem.

Frågor om väsentlig förändring av informationssystemet och om standarder i systemet bereds av den personuppgiftsansvarige i samråd med berörda centrala myndigheter.

Bestämmelser om skyldighet för rättsväsendets myndigheter att lämna uppgifter inom kriminalvården. *I kriminalvårdens brottsdataförordning (2001:682) finns det bestämmelser om skyldighet för rättsväsendets myndigheter att lämna uppgifter.*

Denna förordning träder i kraft den 1 maj 2018.

¹ Senaste lydelse 2014:1119.

1.31 Förslag till förordning om ändring i förordningen (1977:937) om allmänna förvaltningsdomstolars behörighet m.m.

Härigenom föreskrivs att 7 d § förordningen (1977:937) om allmänna förvaltningsdomstolars behörighet m.m. ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

7 d §¹

Beslut av Kriminalvården som överklagas till en förvaltningsrätt ska tas upp av Förvaltningsrätten i Linköping om beslutet gäller en person som inte är inskriven vid en kriminalvårdsanstalt, ett häkte eller ett frivårdskontor i landet och beslutet avser ärenden enligt

1. lagen (1963:193) om samarbete med Danmark, Finland, Island och Norge angående verkställighet av straff m.m., eller

2. lagen (2001:617) om be- 2. kriminalvårdens brottsdata-
handling av personuppgifter inom lag (2001:617).
kriminalvården.

Denna förordning träder i kraft den 1 maj 2018.

¹ Senaste lydelse 2009:872.

1.32 Förslag till förordning om ändring i folkbokföringsförordningen (1991:749)

Härigenom föreskrivs att 5 a § folkbokföringsförordningen (1991:749) ska ha följande lydelse.

5 a §¹

Samordningsnummer får tilldelas en person om det inte råder osäkerhet om hans eller hennes identitet.

Även om det råder osäkerhet om en persons identitet, får samordningsnummer tilldelas för

1. registrering i register som förs enligt lagen (1998:620) om belastningsregister, lagen (1998:621) om misstankeregister, *lagen (2010:362) om polisens allmänna spaningsregister* och *polisdatalagen* (2010:361),

2. annan behandling av uppgifter enligt *polisdatalagen*, eller i övrigt inom rättsväsendets informationssystem,

3. Migrationsverkets behandling av personuppgifter med stöd av utlänningsdatalagen (2016:27) när det gäller personer som omfattas av lagen (1994:137) om mottagande av asylsökande m.fl., eller

4. registrering i beskattningsdatabasen.

1. registrering i register som förs enligt lagen (1998:620) om belastningsregister, lagen (1998:621) om misstankeregister och *polisens brottsdatalag* (2010:361),

2. annan behandling av uppgifter enligt *polisens brottsdatalag* eller *Säkerhetspolisens datalag* (2018:000), eller i övrigt inom rättsväsendets informationssystem,

Denna förordning träder i kraft den 1 maj 2018.

¹ Senaste lydelse 2016:31.

1.33 Förslag till förordning om ändring i förordningen (1995:238) om totalförsvarsplikt

Härigenom föreskrivs att 3 kap. 7 § förordningen (1995:238) om totalförsvarsplikt ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

3 kap.

7 §¹

Bestämmelser om skyldighet för Kriminalvården att till Totalförsvarets rekryteringsmyndighet lämna uppgifter finns i förordningen (2001:682) om behandling av personuppgifter inom kriminalvården.

I förordningen (2018:000) om Kriminalvårdens underrättelse-skyldighet finns det bestämmelser om Kriminalvårdens skyldighet att lämna uppgifter till Totalförsvarets rekryteringsmyndighet.

Denna förordning träder i kraft den 1 maj 2018.

¹ Senaste lydelse 2010:1473.

1.34 Förslag till förordning om ändring i förordningen (1995:1301) om handläggning av skadeståndsanspråk mot staten

Härigenom föreskrivs att 3 § förordningen (1995:1301) om handläggning av skadeståndsanspråk mot staten ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

3 §¹

Justitiekanslern handlägger anspråk på ersättning med stöd av
– 36 kap. 17 § andra stycket brottsbalken,
– 2 kap. 1 § eller 3 kap. 1 eller 2 § skadeståndslagen (1972:207),
om anspråket grundas på ett påstående om felaktigt beslut eller
underlåtenhet att meddela beslut,

– 23 § datalagen (1973:289),

– 48 § personuppgiftslagen
(1998:204), 2 kap. 6 § lagen
(2007:258) om behandling av
personuppgifter i Försvarsmak-
tens försvarsunderrättelseverk-
samhet och militära säkerhets-
tjänst och 2 kap. 5 § lagen
(2007:259) om behandling av
personuppgifter i Försvarets
radioanstalts försvarsunderrät-
telse- och utvecklingsverksamhet,

– 48 § personuppgiftslagen
(1998:204), 2 kap. 6 § lagen
(2007:258) om behandling av
personuppgifter i Försvarsmak-
tens försvarsunderrättelseverk-
samhet och militära säkerhets-
tjänst, 2 kap. 5 § lagen (2007:259)
om behandling av person-
uppgifter i Försvarets radio-
anstalts försvarsunderrättelse-
och utvecklingsverksamhet,
7 kap. 1 § brottsdatalagen
(2018:000) och bestämmelser
som hänvisar till den bestäm-
melsen och 8 kap. 1 § Säkerhets-
polisens datalag (2018:000).

¹ Senaste lydelse 2017:508.

– lagen (1998:714) om ersättning vid frihetsberövanden och andra tvångsåtgärder, dock inte anspråk som avses i 8 § i den lagen,
– 5 kap. 3 § lagen (2017:496) om internationellt polisiärt samarbete, om anspråket grundas på ett påstående om felaktigt beslut eller underlåtenhet att meddela beslut,

– 26 § lagen (2011:111) om förstörande av vissa hälsofarliga missbrukssubstanser,

– 46 kap. 20 § skatteförfarandelagen (2011:1244), eller

– 44 § kameraövervakningslagen (2013:460).

Justitiekanslern handlägger också anspråk på ersättning som grundas på ett påstående om överträdelse av gemenskapsrätten.

Av 4 § följer att vissa anspråk på ersättning med stöd av 3 kap. 1 eller 2 § skadeståndslagen handläggs av Kammarkollegiet.

Denna förordning träder i kraft den 1 maj 2018.

1.35 Förslag till förordning om ändring i vapenförordningen (1996:70)

Härigenom föreskrivs att 1 kap. 4 § vapenförordningen (1996:70) ska ha följande lydelse.

1 kap.

4 §¹

Följande kategorier av anställda vid Polismyndigheten får ges tillgång till uppgifter i vapenregister som regleras i 1 a kap. vapenlagen (1996:67):

1. anställda som handlägger vapenärenden,
2. anställda som arbetar vid myndighetens ledningscentraler, och
3. de särskilt angivna tjänstemän vid myndigheten som utför uppgifter enligt 3 kap. 7 § andra stycket *polisdatalagen* (2010:361).
3. de särskilt angivna tjänstemän vid myndigheten som utför uppgifter enligt 3 kap. 6 § andra stycket *polisens brottsdatalag* (2010:361).

Anställda vid Polismyndigheten som upprätthåller allmän ordning och säkerhet, bistår med handräckning eller utreder brott får ges tillgång till uppgift om huruvida någon har tillstånd att inneha vapen.

Denna förordning träder i kraft den 1 maj 2018.

¹ Senaste lydelse 2014:1149.

1.36 Förslag till förordning om ändring i förordningen (2001:682) om behandling av personuppgifter inom kriminalvården

Härigenom föreskrivs i fråga om förordningen (2001:682) om behandling av personuppgifter inom kriminalvården

dels att 2, 4, 7, 12, 14, 18, 20, 23, 25, 27, 29–33, 39, 43, 45–48 och 50 §§ ska upphöra att gälla,

dels att rubrikerna före 2, 4, 7, 12, 14, 18, 20, 23, 25, 27, 29–33, 45–48, 52, 54 och 55 §§ och rubrikerna efter 37, 45 och 48 §§ ska utgå,

dels att nuvarande 3 § ska betecknas 2 §, att rubriken efter nuvarande 2 § ska placeras efter 1 § och att rubriken före nuvarande 3 § ska placeras före nya 2 §, att nuvarande 5 § ska betecknas 3 §, att rubriken efter nuvarande 4 § ska placeras efter nya 2 § och att rubriken före nuvarande 5 § ska placeras före nya 3 §, att nuvarande 8 § ska betecknas 4 § och att rubriken före nuvarande 8 § ska placeras före nya 4 §, att nuvarande 9 § ska betecknas 4 §, att rubriken efter nuvarande 8 § ska placeras efter nya 4 § och att rubriken före nuvarande 9 § ska placeras före nya 5 §, att nuvarande 13 § ska betecknas 7 § och att rubriken före nuvarande 13 § ska placeras före nya 7 §, att nuvarande 15 § ska betecknas 8 §, att rubriken efter nuvarande 14 § ska placeras efter nya 7 § och att rubriken före nuvarande 15 § ska placeras före nya 8 §, att nuvarande 16 § ska betecknas 9 § och att rubriken före nuvarande 16 § ska placeras före nya 9 §, att nuvarande 19 § ska betecknas 10 § och att rubriken före nuvarande 19 § ska placeras före nya 10 §, att nuvarande 21 § ska betecknas 11 §, att rubriken efter nuvarande 20 § ska placeras efter nya 10 § och att rubriken före nuvarande 21 § ska placeras före nya 11 §, att nuvarande 22 § ska betecknas 12 § och att rubriken före nuvarande 22 § ska placeras före nya 12 §, att nuvarande 24 § ska betecknas 13 § och att rubriken före nuvarande 24 § ska placeras före nya 13 §, att nuvarande 26 § ska betecknas 14 §, att rubriken efter nuvarande 25 § ska placeras efter nya 13 § och att rubriken före nuvarande 26 § ska placeras före nya 14 §, att nuvarande 28 § ska betecknas 15 § och att rubriken före nuvarande 28 § ska

placeras före nya 15 §, att nuvarande 34 § ska betecknas 16 §, att rubriken efter nuvarande 33 § ska placeras efter nya 15 § och att rubriken före nuvarande 34 § ska placeras före nya 16 §, att nuvarande 35 § ska betecknas 17 §, att nuvarande 36 § ska betecknas 18 § och att rubriken före nuvarande 36 § ska placeras före nya 18 §, att nuvarande 37 § ska betecknas 19 § och att rubriken före nuvarande 37 § ska placeras före nya 19 §, att nuvarande 40 § ska betecknas 21 §, att rubriken efter nuvarande 37 § ska placeras efter nya 20 § och att rubriken före nuvarande 39 § ska placeras före nya 21 §, att nuvarande 41 § ska betecknas 22 §, att nuvarande 44 § ska betecknas 23 § och att rubriken före nuvarande 44 § ska placeras före nya 23 §, att nuvarande 49 § ska betecknas 25 § och att rubriken före nuvarande 49 § ska placeras före nya 25 §, att nuvarande 51 § ska betecknas 26 § och att rubriken före nuvarande 51 § ska placeras före nya 26 §, att nuvarande 52 § ska betecknas 27 §, att nuvarande 54 § ska betecknas 28 § och att nuvarande 55 § ska betecknas 29 §,

dels att 1 § och nya 2–17, 19, 21–23 och 25, 27–30 §§ och rubrikerna före 1 §, nya 4, 7, 10, 13, 15, 19, 21, 23 och 25 §, ska ha följande lydelse,

dels att rubriken efter nya 4 § ska lyda *Behandling av uppgifter om häktade* och rubriken före nya 26 § ska lyda *Underrättelse-skyldighet*,

dels att det ska införas två nya paragrafer, 20 och 24 §§, och nya rubriker före 20 och 27 §§ av följande lydelse,

dels att rubriken till förordningen ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

Förordning om behandling av personuppgifter inom kriminalvården

Kriminalvårdens brottsdataförordning

Inledande bestämmelser

Allmän bestämmelse

1 §

I denna förordning ges kompletterande föreskrifter om sådan behandling av personupp-

I denna förordning finns kompletterande föreskrifter till kriminalvårdens brottsdatalog

gifter som omfattas av lagen (2001:617) om behandling av personuppgifter inom kriminalvården.

Av 34 och 39 §§ framgår att det inom kriminalvården skall föras ett centralt kriminalvårdsregister och ett säkerhetsregister. I 36 § finns bestämmelser om skyldighet för myndigheter att lämna uppgifter som behövs för det centrala kriminalvårdsregistret.

Av 16 § framgår att Kriminalvården ska föra ett centralt kriminalvårdsregister. I 18 § finns bestämmelser om skyldighet för myndigheter att lämna uppgifter som behövs för registret.

2 §¹

I fråga om personer som avses i 1 § första stycket 1–9 lagen (2001:617) om behandling av personuppgifter inom kriminalvården får, i den utsträckning det är nödvändigt för det ändamål för vilket behandlingen utförs, följande personuppgifter behandlas:

Om det är nödvändigt för att utföra en arbetsuppgift för något av de syften som anges i 2 kap. 1 § kriminalvårdens brottsdatalag (2001:617) får uppgifter om följande behandlas:

1. namn, personnummer eller annan identifieringsuppgift, fotografi, adress, telefonnummer, yrke och utbildning, kön, medborgarskap och språk,
2. kommun där den registrerade är folkbokförd *och socialdistriktet,*
3. namn, adress, telefonnummer, telefaxnummer och e-postadress som rör
 - a) ombud eller ställföreträdare för den registrerade,
 - b) arbetsgivare, utbildningsanstalt eller liknande och kontaktperson,
 - c) statlig eller kommunal befattningshavare som i tjänsten tar befattning med den registrerade, och
 - d) *tolk som anlitas av kriminalvården,*
2. kommun där den registrerade är folkbokförd,
- d) tolk,

¹ Senaste lydelse 2006:1126.

4. närståendes namn, adress och telefonnummer samt relation till den registrerade,

5. uppgifter om genomförd personutredning och rättspsykiatrisk undersökning, läkarintyg enligt 7 § lagen (1991:2041) om särskild personutredning i brottmål, m.m. samt utredning med ett utlåtande om risk för återfall i brottslighet enligt 10 § lagen (2006:45) om omvandling av fängelse på livstid,

6. uppgifter om domstols dom eller slutliga beslut som avser fängelse, skyddstillsyn, villkorlig dom med föreskrift om samhällstjänst eller förvandlingsstraff för böter eller vite, samt beslut i häktningsfråga,

7. uppgifter om domstols avräkningsunderlag,

8. brott för vilket den registrerade är skäligen misstänkt,

9. uppgifter om ansökan om nåd samt regeringens beslut om nåd,

10. annat beslut av regeringen som avser den registrerade och som har betydelse för verkställigheten av påföljd,

11. uppgifter om ansökan och beslut enligt lagen (2006:45) om omvandling av fängelse på livstid,

12. uppgifter om dom, beslut eller föreläggande av allmän förvaltningsdomstol eller av myndighet inom eller utom kriminalvården som avser den registrerade och som har betydelse för

4. närståendes namn, adress, telefonnummer och relation till den registrerade,

5. genomförd personutredning och rättspsykiatrisk undersökning, läkarintyg enligt 7 § lagen (1991:2041) om särskild personutredning i brottmål, m.m. och utredning med utlåtande om risk för återfall i brottslighet enligt 10 § lagen (2006:45) om omvandling av fängelse på livstid,

6. domstols dom eller slutliga beslut som avser fängelse, skyddstillsyn, villkorlig dom med föreskrift om samhällstjänst eller förvandlingsstraff för böter eller vite och beslut i häktningsfrågor,

7. domstols avräkningsunderlag,

8. brott för vilket den registrerade är skäligen misstänkt,

9. ansökan om nåd och regeringens beslut i sådana frågor,

10. annat beslut av regeringen som avser den registrerade och som har betydelse för verkställigheten av påföljd,

11. ansökan och beslut enligt lagen om omvandling av fängelse på livstid,

12. dom, beslut eller föreläggande av allmän förvaltningsdomstol eller beslut av en myndighet som avser den registrerade och som har betydelse för verkställigheten av påföljd,

verkställigheten av påföljd,

13. *uppgifter om* överklagande av domstols dom eller beslut, regeringens beslut eller myndighets beslut,

14. tidpunkt för verkställighetens början, provotid och övervakningstid,

15. tidpunkt för frigivning från kriminalvårdsanstalt *samt* återstående strafftid vid villkorlig frigivning,

16. *uppgifter om* verkställighet av samhällstjänst och intensivövervakning med elektronisk kontroll,

17. beslut av myndighet i *Sverige eller* annan stat om verkställighet av påföljd som avser den registrerade,

18. *uppgifter i övrigt angående* verkställighet av påföljd,

19. tidpunkten för bortfallande av fängelse enligt 35 kap. 8 och 9 §§ brottsbalken eller förvandlingsstraff för böter eller vite enligt 18 och 21 §§ bötesverkställighetslagen (1979:189), *och*

20. *grunden för intagning i häkte eller kriminalvårdsanstalt i fall som avses i 1 § första stycket 8 lagen om behandling av personuppgifter inom kriminalvården (2001:617) eller anledning till transport inom kriminalvårdens transporttjänst.*

13. överklagande av domstols dom eller beslut, regeringens beslut eller myndighets beslut,

15. tidpunkt för frigivning från kriminalvårdsanstalt *och* återstående strafftid vid villkorlig frigivning,

16. verkställighet av samhällstjänst och intensivövervakning med elektronisk kontroll,

17. beslut av myndighet i annan stat om verkställighet av påföljd som avser den registrerade,

18. *andra* uppgifter om verkställighet av påföljd, *och*

19. tidpunkten för bortfallande av fängelse enligt 35 kap. 8 och 9 §§ brottsbalken eller förvandlingsstraff för böter eller vite enligt 18 och 21 §§ bötesverkställighetslagen (1979:189).

3 §²

I fråga om personer som är föremål för personutredning får utöver vad som anges i 3 och 4 §§ följande *personuppgifter* behandlas:

1. *uppgift om* att den registrerade är intagen i häkte eller kriminalvårdsanstalt med angivande av häktet eller anstalten,

2. *uppgifter om domstols* begäran om personutredning *samt uppgifter om* begäran om hjälp med yttrande från annan enhet inom Kriminalvården,

3. *uppgifter om* tidigare domar, brott den registrerade tidigare har begått, tidigare ådömd påföljd och uppgifter om verkställigheten *av denna*,

4. datum då personutredning har lämnats till domstolen,

5. datum för huvudförhandling och domstols dom,

6. *uppgift om* den påföljd som den registrerade har dömts till eller uppgift om att åtalet har ogillats, och

7. *uppgifter om* den misstänktes personliga förhållanden *som* behövs för att utreda vilka åtgärder som kan antas förebygga framtida brottslighet.

I fråga om personer som är föremål för personutredning får utöver vad som anges i 2 § *uppgifter om* följande behandlas:

1. att den registrerade är intagen i häkte eller kriminalvårdsanstalt med angivande av häktet eller anstalten,

2. begäran om personutredning *och* begäran om hjälp med yttrande från annan enhet inom Kriminalvården,

3. tidigare domar, brott den registrerade tidigare har begått, tidigare ådömd påföljd och uppgifter om verkställigheten,

6. den påföljd som den registrerade har dömts till eller uppgift om att åtalet har ogillats, och

7. den misstänktes personliga förhållanden *om det* behövs för att utreda vilka åtgärder som kan antas förebygga framtida brottslighet.

² Senaste lydelse 2005:1025.

*Gallring**Längsta tid som personuppgifter får behandlas*

Uppgifter som avses i 5–7 §§ skall *gallras* senast två år efter det att det mål i vilket personutredningen har begärts slutligt har avgjorts. *Om den som personutredningen avser har dömts till fängelse, skyddstillsyn eller villkorlig dom med föreskrift om samhällstjänst, skall dock uppgifterna gallras senast tio år efter det att den senaste påföljden helt har verkställts.*

4 §³

Trots det som sägs i 2 kap. 17 § andra stycket brottsdatalogen (2018:000) får uppgifter som avses i 3 § inte behandlas längre än

1. två år efter det att det mål i vilket personutredningen har begärts slutligt har avgjorts, eller
2. tio år efter det att den senaste påföljden helt har verkställts, *om den som personutredningen avser har dömts till fängelse, skyddstillsyn eller villkorlig dom med föreskrift om samhällstjänst.*

I fråga om personer som är häktade får utöver vad som anges i 3 och 4 §§ följande *personuppgifter* behandlas:

1. uppgifter om den häktades ankomst till häktet och om tilldelat inskrivningsnummer,
2. datum och tidpunkt för anhållande och häktning,
3. restriktioner som avses i 24 kap. 5 a § rättegångsbalken,
4. anknytning till annan häktad eller anhållen med anledning av att denne är misstänkt för delaktighet i samma brott som den häktade,
5. medgivande från den häktade om granskning av försändelse enligt 3 kap. 8 § häkteslagen (2010:611),
6. uppgifter om tid, plats, bevakning och villkor vid besök,

5 §⁴

I fråga om personer som är häktade får utöver vad som anges i 2 § *uppgifter om* följande behandlas:

³ Senaste lydelse 2005:10.

⁴ Senaste lydelse 2011:148.

7. tjänsteutövande besökares namn, adress, telefonnummer och titel,

8. namn, personnummer, adress, telefonnummer och uppgift om språk och relation till den häktade samt sådana uppgifter som avses i 3 kap. 11 § häkteslagen om annan besökare än som avses i 7 och om person som en häktad tillåts att ha elektronisk kommunikation med,

9. tilldelat rum och specialkost samt uppgifter om förvaring av den häktades tillhörigheter,

10. behov av hälso- och sjukvård,

11. behov av vård eller behandling relaterad till missbruk eller till den häktades brottslighet,

12. behov av utbildning och uppgifter om sysselsättning,

13. plats utanför förvaringslokalen där den häktade vistas under permission eller med anledning av sjukdom, undersökning, förhör, förhandling eller liknande,

14. uppgifter om omständigheter som Kriminalvården måste beakta vid frigivning,

15. uppgifter om att den häktade har svensk pension och om underrättelse till Försäkringskassan och Pensionsmyndigheten med anledning av frihetsberövandet,

16. uppgifter om transport,

17. uppgifter om tidigare inträffad fritagning eller avvikelse eller försök eller förberedelse till det samt risk för fritagning eller avvikelse,

18. uppgifter om att den häktade tidigare i häkte eller under verkställigheten av fängelsestraff har gjort sig skyldig till våld eller hot om våld mot personal inom kriminalvården eller mot andra intagna i häkte eller anstalt eller uppgift om framtida risk för sådant våld eller hot,

19. uppgifter om att den häktade tidigare i häkte eller under verkställigheten av fängelsestraff allvarligt stört ordningen inom häktet eller anstalten eller uppgift om framtida risk för sådant handlande,

20. uppgifter om att den häktade tidigare i häkte eller under verkställigheten av fängelsestraff befattat sig med sådana medel som avses i 4 kap. 8 § häkteslagen eller 8 kap. 8 § fängelselagen (2010:610) eller uppgift om framtida risk för befattning med sådana medel,

21. uppgifter om annan misskötsamhet,
 22. uppgifter om sådan kontroll som avses i 4 kap. 5 § häkteslagen,
23. *underrättelse till häktades beskickning,*
 24. tidpunkt då den häktade har delgetts domstols dom och uppgifter om nöjdförklaring,
 25. uppgifter om utskrivning, *och*
 26. uppgifter som är nödvändiga för handläggningen av ett ärende som enligt lag eller förordning ska prövas av Kriminalvården.
23. tidpunkt då den häktade har delgetts domstols dom och uppgifter om nöjdförklaring,
 24. uppgifter om utskrivning,
 25. uppgifter som är nödvändiga för handläggningen av ett ärende som enligt lag eller förordning ska prövas av Kriminalvården.

6 §⁵

Kriminalvården får i fråga om den som är häktad utöver vad som anges i 3, 4 och 9 §§ behandla personuppgifter i en sådan journal som avses i 5 § häktesförordningen (2010:2011) och 6 § andra stycket förordningen (2007:1172) med instruktion för Kriminalvården. En sådan journal får innehålla uppgifter om alla beslut som har fattats, viktiga händelser under vistelsen i häkte och väsentliga uppgifter om vidtagna eller planerade åtgärder som gäller den häktade. Den får även innehålla uppgifter om omständigheter i övrigt som är av betydelse under vistelsen i häkte.

Kriminalvården får i fråga om den som är häktad utöver vad som anges i 2 och 5 §§ behandla personuppgifter i en sådan journal som avses i 5 § häktesförordningen (2010:2011) och 6 § andra stycket förordningen (2007:1172) med instruktion för Kriminalvården. En sådan journal får innehålla uppgifter om alla beslut som har fattats, viktiga händelser under vistelsen i häkte och väsentliga uppgifter om vidtagna eller planerade åtgärder som gäller den häktade. Den får även innehålla uppgifter om omständigheter i övrigt som är av betydelse under vistelsen i häkte.

⁵ Senaste lydelse 2011:148.

*Gallring**Längsta tid som personuppgifter får behandlas*

7 §

Uppgifter om en häktad skall gallras senast två år efter det att den häktade har frigivits från häktet.

Trots det som sägs i 2 kap. 17 § andra stycket brottsdatalagen (2018:000) får uppgifter om en häktad inte behandlas längre än

1. två år efter det att den häktade frigavs från häktet eller

2. tio år efter det att påföljden helt har verkställts, om den häktade efter att ha frigetts från häkte har dömts till fängelse, skyddstillsyn eller villkorlig dom med föreskrift om samhällstjänst.

8 §⁶

I fråga om personer som är dömda till fängelse får utöver vad som anges i 3 och 4 §§ följande personuppgifter behandlas:

I fråga om personer som är dömda till fängelse, är ålagda fängelse som förvandlingsstraff för böter eller vite eller på grund av en utländsk dom ska verkställa fängelsepåföljd i Sverige får utöver det som anges i 2 § uppgifter om följande behandlas:

1. sådana uppgifter som avses i 5 § 7 samt 9 § 1, 6–12, 15–21 och 24 och som när det gäller den som är häktad respektive misstänkt i stället ska avse den som är intagen i kriminalvårdsanstalt,

1. sådana uppgifter som avses i 3 § 7 och 5 § 1, 6–12, 15–21 och 25 och som när det gäller den som är häktad respektive misstänkt i stället ska avse den som är intagen i kriminalvårdsanstalt,

2. anknytning till annan intagen som är dömd för delaktighet i samma brott som den dömda,

⁶ Senaste lydelse 2015:649.

3. uppgifter om placering i avskildhet och undersökning enligt 6 kap. fängeslagen (2010:610) och om användande av fängsel och undersökning enligt 8 kap. 10 § samma lag,

4. uppgifter om placering på säkerhetsavdelning,

5. uppgift om att målsägande i enlighet med 35 § fängesförelagningen (2010:2010) ska underrättas,

6. uppgifter om permissioner och vistelser utanför anstalt enligt 9 kap. 1 §, 10 kap. 1, 2 och 4 §§ samt 11 kap. 1 § fängeslagen,

7. uppgifter om sådan kontroll som avses i 8 kap. 6 § fängeslagen,

8. beslut om att den dömd ska inställa sig i anstalt eller påbörja intensivövervakning med elektronisk kontroll, beslut om uppskov med verkställighet och begäran om förpassning genom Polismyndighetens försorg,

9. övervakarens namn, adress och telefonnummer,

10. uppgift om att den dömd har ålagts näringsförbud, kontaktförbud, förbud enligt 3 kap. 5 § lagen (2015:642) om europeisk skyddsorder eller tillträdesförbud,

11. uppgifter om beslut enligt 26 kap. 18 och 19 §§, 27 kap. 6 § 1 och 2 och 28 kap. 7 § brottbalken, och

12. uppgifter som är nödvändiga för handläggningen av ett ärende som enligt lag eller förordning ska prövas av Kriminalvården.

I fråga om den som verkställer fängelsestraffet genom intensivövervakning med elektronisk kontroll tillämpas bestämmelserna i första stycket 1 när det gäller hänvisningen till 5 § 7 och första stycket 8–12.

I fråga om den som verkställer fängelsestraffet genom intensivövervakning med elektronisk kontroll tillämpas bestämmelserna i första stycket 1 när det gäller hänvisningen till 3 § 7 och första stycket 8–12.

9 §⁷

Kriminalvården får i fråga om den som *är dömd till fängelse* utöver vad som anges i 3, 4 och 15 §§ behandla personuppgifter i en sådan journal som avses

Kriminalvården får i fråga om den som *avses i 8 §* utöver vad som anges i 2 och 8 §§ behandla personuppgifter i en sådan journal som avses i 5 § fängesförelagningen

⁷ Senaste lydelse 2011:148.

i 5 § fängelseförordningen (2010:2010), 12 § förordningen (1994:1060) om intensivövervakning med elektronisk kontroll, 4 kap. 6 a § förordningen (1998:642) om verkställighet av frivårdspåföljder och 6 § andra stycket förordningen (2007:1172) med instruktion för Kriminalvården. En sådan journal får innehålla uppgifter om alla beslut som har fattats, viktiga händelser under verkställigheten och väsentliga uppgifter om vidtagna eller planerade åtgärder om den intagne, den som står under övervakning efter villkorlig frigivning och den som transporteras av *kriminalvårdens* transporttjänst. Journalen får även innehålla uppgifter om omständigheter i övrigt som är av betydelse för verkställigheten.

ordningen (2010:2010), 12 § förordningen (1994:1060) om intensivövervakning med elektronisk kontroll, 4 kap. 6 a § förordningen (1998:642) om verkställighet av frivårdspåföljder och 6 § andra stycket förordningen (2007:1172) med instruktion för Kriminalvården. En sådan journal får innehålla uppgifter om alla beslut som har fattats, viktiga händelser under verkställigheten och väsentliga uppgifter om vidtagna eller planerade åtgärder rörande den intagne, den som står under övervakning efter villkorlig frigivning och den som transporteras av *Kriminalvårdens* transporttjänst. Journalen får även innehålla uppgifter om omständigheter i övrigt som är av betydelse för verkställigheten.

Gallring

Längsta tid som personuppgifter får behandlas

10 §⁸

Uppgifter i en sådan journal som avses i 16 § skall gallras senast tio år efter det att det senaste straffet avseende den registrerade helt har verkställts. I övrigt skall uppgifter om en person som är dömd till fängelse gallras senast två år efter det att villkorlig frigivning har skett

Trots det som sägs i 2 kap. 17 § andra stycket brottsdatalogen (2018:000) får uppgifter i en sådan journal som avses i 9 § inte behandlas längre än tio år efter det att det senaste straffet avseende den registrerade helt har verkställts. I övrigt får uppgifter om en person som avses i

⁸ Senaste lydelse 2005:10.

eller intensivövervakning med elektronisk kontroll har upphört.

I fråga om uppgifter om personer som avses i 1 § första stycket 8 lagen (2001:617) om behandling av personuppgifter inom kriminalvården skall dock gallring ske senast två år efter det att den registrerade har lämnat anstalten.

8 § inte behandlas längre än två år efter det att villkorlig frigivning har skett eller intensivövervakning med elektronisk kontroll har upphört.

11 §⁹

I fråga om personer som är dömda till skyddstillsyn får utöver vad som anges i 3 och 4 §§ följande *personuppgifter* behandlas:

1. sådana uppgifter som avses i 5 § 7 samt 15 § 10 och 11,
2. uppgifter om sysselsättning,
3. övervakarens namn, adress och telefonnummer,
4. uppgifter som är nödvändiga för handläggningen av ett ärende som enligt lag eller förordning ska prövas av Kriminalvården.

I fråga om personer som är dömda till skyddstillsyn *eller som på grund av en utländsk dom ska undergå skyddstillsyn eller motsvarande påföljd i Sverige* får utöver vad som anges i 2 § uppgifter om följande behandlas:

1. sådana uppgifter som avses i 3 § 7 och 8 § 9–12, och
2. sysselsättning.

⁹ Senaste lydelse 2011:148.

12 §¹⁰

Kriminalvården får i fråga om den som *är dömd till skyddstillsyn* utöver vad som anges i 3, 4 och 21 §§ behandla personuppgifter i en sådan journal som avses i 2 kap. 10 § och 3 kap. 5 § förordningen (1998:642) om verkställighet av frivårdspåföljder och 6 § andra stycket förordningen (2007:1172) med instruktion för Kriminalvården. En sådan journal får innehålla uppgifter om alla beslut som har fattats, viktiga händelser under verkställigheten och väsentliga uppgifter om vidtagna eller planerade åtgärder som gäller den dömd. Den får även innehålla uppgifter om omständigheter i övrigt som är av betydelse för verkställigheten.

Gallring

Uppgifter i en sådan journal som avses i 22 § *skall gallras senast* tio år efter det att den senaste påföljden avseende den registrerade helt har verkställts. I övrigt *skall* uppgifter om en person som *är dömd till skydds-tillsyn gallras senast* två år efter det att övervakningen har upp-

Kriminalvården får i fråga om den som *avses i 11 §* utöver vad som anges i 2 och 11 §§ behandla personuppgifter i en sådan journal som avses i 2 kap. 10 § och 3 kap. 5 § förordningen (1998:642) om verkställighet av frivårdspåföljder och 6 § andra stycket förordningen (2007:1172) med instruktion för Kriminalvården. En sådan journal får innehålla uppgifter om alla beslut som har fattats, viktiga händelser under verkställigheten och väsentliga uppgifter om vidtagna eller planerade åtgärder som gäller den dömd. Den får även innehålla uppgifter om omständigheter i övrigt som är av betydelse för verkställigheten.

*Längsta tid som personuppgifter får behandlas*13 §¹¹

Trots det som sägs i 2 kap. 17 § andra stycket brottsdatalogen (2018:000) får uppgifter i en sådan journal som avses i 12 § *inte behandlas längre än* tio år efter det att den senaste påföljden avseende den registrerade helt har verkställts. I övrigt får uppgifter om en person som

¹⁰ Senaste lydelse 2011:148.

¹¹ Senaste lydelse 2005:10.

hört.

avses i 11 § inte behandlas längre än två år efter det att övervakningen har upphört.

14 §¹²

Kriminalvården får i fråga om den som är dömd till villkorlig dom med föreskrift om samhällstjänst utöver vad som anges i 3 och 4 §§ behandla personuppgifter i en sådan journal som avses i 3 kap. 5 § förordningen (1998:642) om verkställighet av frivårdspåföljder. En sådan journal får innehålla uppgifter om samtliga beslut som har fattats, viktiga händelser under verkställigheten och väsentliga uppgifter om vidtagna eller planerade åtgärder som gäller den dömda. Den får även innehålla uppgifter om omständigheter i övrigt som är av betydelse för verkställigheten.

Kriminalvården får i fråga om den som är dömd till villkorlig dom med föreskrift om samhällstjänst, *eller som på grund av en utländsk dom ska undergå villkorlig dom med föreskrift om samhällstjänst eller motsvarande påföljd i Sverige*, utöver vad som anges i 2 § behandla personuppgifter i en sådan journal som avses i 3 kap. 5 § förordningen (1998:642) om verkställighet av frivårdspåföljder. En sådan journal får innehålla uppgifter om samtliga beslut som har fattats, viktiga händelser under verkställigheten och väsentliga uppgifter om vidtagna eller planerade åtgärder som gäller den dömda. Den får även innehålla uppgifter om omständigheter i övrigt som är av betydelse för verkställigheten.

Gallring

Längsta tid som personuppgifter får behandlas

15 §¹³

Uppgifter i en sådan journal som avses i 26 § *skall gallras senast* tio år efter det att den

Trots det som sägs i 2 kap. 17 § andra stycket brottsdatalogen (2018:000) får uppgifter i en

¹² Senaste lydelse 2005:1025.

¹³ Senaste lydelse 2005:10.

senaste påföljden avseende den registrerade helt har verkställts. I övrigt skall uppgifter om en person som är dömd till villkorlig dom med föreskrift om samhällstjänst gallras senast två år efter det att föreskriften om samhällstjänst helt har verkställts.

sådan journal som avses i 14 § inte behandlas längre än tio år efter det att den senaste påföljden avseende den registrerade helt har verkställts. I övrigt får uppgifter om en person som avses i 14 § inte behandlas längre än två år efter det att föreskriften om samhällstjänst helt har verkställts.

16 §¹⁴

För de ändamål som anges i 3 § första stycket 1 och 2 lagen (2001:617) om behandling av personuppgifter inom kriminalvården skall Kriminalvården föra ett register (centrala kriminalvårdsregistret) över personer som

Kriminalvården ska föra ett register (centrala kriminalvårdsregistret) över personer som

1. har dömts till fängelse, skyddstillsyn eller villkorlig dom med föreskrift om samhällstjänst,
2. har ålagts förvandlingsstraff för böter eller vite,
3. eller på grund av en utländsk brottmålsdom skall verkställa en sådan påföljd som avses i 1 och 2 i Sverige.

1. är häktade,
2. har dömts till fängelse, skyddstillsyn eller villkorlig dom med föreskrift om samhällstjänst,
3. har ålagts förvandlingsstraff för böter eller vite, eller
4. på grund av en utländsk brottmålsdom ska verkställa en sådan påföljd som avses i 2 eller 3 i Sverige.

17 §¹⁵

Det centrala kriminalvårdsregistret får innehålla sådana uppgifter som avses i 3 § 1, 5–7,

Det centrala kriminalvårdsregistret får innehålla sådana uppgifter som avses i 2 § 1, 5–7,

¹⁴ Senaste lydelse 2005:1025.

¹⁵ Senaste lydelse 2011:148.

9–11 och 13–19, i 15 § 1 när det gäller hänvisningen till 9 § 16, i 15 § 6 och 9 och i 21 § 2. 9–11 och 13–19, 5 § 16, 8 § 6 och 9 och i 11 § 2.

Utlämnande av uppgifter m.m. *Utlämnande av uppgifter*

19 §¹⁶

Uppgifter i det centrala kriminalvårdsregistret ska på begäran lämnas ut till Regeringskansliet, en domstol, Åklagarmyndigheten, Ekobrottsmyndigheten, Justitiekanslern, Riksdagens ombudsmän, Polismyndigheten, Säkerhetspolisen, Datainspektionen eller en myndighet som får besluta om frihetsberövande åtgärd enligt lagen (1957:668) om utlämning för brott, lagen (2003:1156) om överlämnande från Sverige enligt en europeisk arresteringsorder, utlämningslagen (2005:716) eller lagen (2011:1165) om överlämnande från Sverige enligt en nordisk arresteringsorder.

Dessutom får Regeringskansliet, Polismyndigheten och Säkerhetspolisen ha direktåtkomst till registret. För Regeringskansliet får dock endast sådana uppgifter göras tillgängliga som behövs i ärenden om nåd i brottmål.

Uppgifter i centrala kriminalvårdsregistret ska på begäran lämnas ut till Regeringskansliet, en domstol, Åklagarmyndigheten, Ekobrottsmyndigheten, Justitiekanslern, Riksdagens ombudsmän, Polismyndigheten, Säkerhetspolisen och Datainspektionen.

¹⁶ Senaste lydelse 2014:1162.

Direktåtkomst

20 §

Regeringskansliet, Polismyndigheten och Säkerhetspolisen får medges direktåtkomst till registret. För Regeringskansliet får endast sådana uppgifter göras tillgängliga som behövs i ärenden om nåd.

Registrets ändamål och Registrets innehåll21 §¹⁷

Säkerhetsregistret får utöver vad som anges i 39 § omfatta häktade eller intagna om det finns särskild anledning att anta att de under den tid som häktningen eller verkställigheten av fängelsestraffet pågår tillsammans med andra kan komma att

1. utöva allvarlig brottslig verksamhet,

2. göra sig skyldiga till hets mot folkgrupp enligt 16 kap. 8 § brottsbalken eller sådant brott mot allmän verksamhet som avses i 17 kap. 1, 2 och 10 §§ samma balk,

3. allvarligt störa ordningen inom häktet eller anstalten,

4. delta i nätverk som bidrar till allvarliga ordningsstörningar eller brottslig verksamhet, eller

5. förbereda rymning eller fri-tagning.

¹⁷ Senaste lydelse 2011:148.

Om regeringen med stöd av 7 kap. 11 § fängelselagen (2010:610) *har* beslutat om avvikelser från bestämmelserna i 7 kap. samma lag i fråga om en intagen, ska registret *omfatta en sådan intagen*, om det inte är uppenbart obehövt.

Har regeringen med stöd av 7 kap. 11 § fängelselagen (2010:610) beslutat om avvikelser från bestämmelserna i 7 kap. samma lag i fråga om en intagen, ska *uppgifter om honom eller henne föras in i säkerhetsregistret*, om det inte är uppenbart obehövt.

22 §

Säkerhetsregistret får föras för att samla, bearbeta och analysera information som ger underlag för åtgärder för att upprätthålla säkerheten eller förebygga brott och får innehålla de uppgifter som behövs för detta ändamål.

Registret *skall innehålla*

1. skälen för registrering, *med särskilt angivande av de omständigheter som ger anledning till ett sådant antagande som avses i 40 §*, och

2. upplysning om varifrån *uppgifter i registret* kommer och, om det inte är obehövt, en bedömning av uppgiftslämnarens trovärdighet.

Säkerhetsregistret får om det är oundgängligen nödvändigt innehålla känsliga uppgifter. För sökning i säkerhetsregistret får känsliga uppgifter användas som sökbegrepp.

Av registret ska framgå

1. skälen för registrering *och de omständigheter som föranlett registreringen*, och

2. upplysning om varifrån *uppgifterna* kommer och, om det inte är obehövt, en bedömning av uppgiftslämnarens trovärdighet.

Direktåtkomst och utlämnande av uppgifter inom kriminalvården Utlämnande av uppgifter

23 §¹⁸

Rikspolischefen, säkerhetspolischefen och de personer som respektive chef utser får ha direktåtkomst till uppgifter om huruvida en person är registrerad i säkerhetsregistret. Polismyndigheten och Säkerhetspolisen får lämna ut en sådan uppgift till Åklagarmyndigheten och Ekobrottsmyndigheten, om uppgiften kan antas ha särskild betydelse för en pågående undersökning i myndighetens brottsutredande verksamhet eller för andra brottsbekämpande åtgärder.

Uppgifter i säkerhetsregistret får, efter prövning av chefen för Kriminalvården eller av de personer som han eller hon utser, lämnas ut till Polismyndigheten eller Säkerhetspolisen. Utlämnandet får endast avse uppgifter som kan antas ha särskild betydelse för

1. en pågående undersökning i Polismyndighetens eller Säkerhetspolisens brottsutredande verksamhet,

2. andra brottsbekämpande åtgärder, eller

3. att upprätthålla ordningen och säkerheten i Kriminalvårdens verksamhet.

Uppgifter i säkerhetsregistret ska lämnas ut till Polismyndigheten, Säkerhetspolisen, Ekobrottsmyndigheten och Åklagarmyndigheten, om uppgiften kan antas ha särskild betydelse för

1. en förundersökning,

¹⁸ Senaste lydelse 2014:1162.

Uppgifter i säkerhetsregistret får, efter prövning av chefen för Kriminalvården eller av de personer som han eller hon utser, även lämnas ut till Regeringskansliet om uppgiften kan antas ha betydelse i ärenden

1. om nåd i brottmål,
2. enligt lagen (1991:572) om särskild utlänningskontroll, eller
3. enligt 7 kap. 11 § eller 13 kap. 6 § fängelselagen (2010:610).

Uppgifter i säkerhetsregistret får, efter prövning av chefen för Kriminalvården eller av de personer som han eller hon utser, även lämnas ut till allmän domstol om uppgiften kan antas ha betydelse i ärenden som handläggs enligt lagen (2006:45) om omvandling av fängelse på livstid.

Uppgifter i säkerhetsregistret ska lämnas ut till Regeringskansliet om uppgiften kan antas ha betydelse i ärenden

Uppgifter i säkerhetsregistret får lämnas ut till en allmän domstol om uppgiften kan antas ha betydelse i ärenden enligt lagen (2006:45) om omvandling av fängelse på livstid.

Direktåtkomst

24 §

Direktåtkomst till säkerhetsregistret ska begränsas till uppgifter om huruvida någon som har registrerats med stöd av 3 kap. 2 § andra stycket 1–4 kriminalvårdens brottsdatalog (2001:617) förekommer i registret.

Skyldighet att anmäla oriktighet i register, *m.m.*

Skyldighet att anmäla oriktighet i register

25 §¹⁹

Den som i tjänsten tar del av uppgifter ur det centrala kriminalvårdsregistret eller säkerhetsregistret och misstänker att registrets innehåll är oriktigt skall genast anmäla det till Kriminalvården.

Den som i tjänsten tar del av uppgifter i centrala kriminalvårdsregistret eller säkerhetsregistret och misstänker att registrets innehåll är oriktigt ska genast anmäla det till Kriminalvården.

Föreskrifter

26 §²⁰

Riksarkivet får, efter samråd med Kriminalvården, meddela föreskrifter om att uppgifter som skall gallras enligt bestämmelser i denna förordning får bevaras för historiska, statistiska och vetenskapliga ändamål.

Riksarkivet får, efter att ha gett Kriminalvården tillfälle att yttra sig, meddela föreskrifter om att personuppgifter som inte längre får behandlas enligt denna förordning får behandlas under längre tid för arkivändamål av allmänt intresse och vetenskapliga, statistiska eller historiska ändamål.

27 §²¹

Kriminalvården meddelar närmare föreskrifter om omfattningen av uppgiftsskyldigheten i 36 och 46 §§ samt om tiden och sättet för att fullgöra den efter samråd med berörd myndighet.

Kriminalvården får, efter att ha gett berörd myndighet tillfälle att yttra sig, meddela föreskrifter om omfattningen av uppgiftsskyldigheten i 18 och 26 §§ och om tiden och sättet för att fullgöra den.

¹⁹ Senaste lydelse 2005:1025.

²⁰ Senaste lydelse 2005:1025.

²¹ Senaste lydelse 2014:1162.

28 §²²

Kriminalvården får meddela föreskrifter om *begränsningar* av de uppgifter som behandlas för ett visst ändamål.

Kriminalvården får meddela föreskrifter om *begränsning* av de personuppgifter som behandlas enligt 2 kap. 1 § *kriminalvårdens brottsdatalag* (2001:617).

29 §²³

Kriminalvården får efter samråd med *Datainspektionen* meddela de ytterligare föreskrifter som behövs för verkställighet av *lagen* (2001:617) om *behandling av personuppgifter inom kriminalvården* och denna förordning.

Kriminalvården får meddela de ytterligare föreskrifter som behövs för verkställighet av *kriminalvårdens brottsdatalag* (2001:617) och denna förordning.

Innan Kriminalvården meddelar föreskrifter med stöd av denna förordning, ska myndigheten samråda med Datainspektionen i frågor som berör särskilda risker för intrång i den personliga integriteten.

1. Denna förordning träder i kraft den 1 maj 2018.

2. Äldre bestämmelser gäller fortfarande för uppgifter i handlingar som omhändertagits för arkivering före ikraftträdandet av denna förordning.

²² Senaste lydelse 2005:1025.

²³ Senaste lydelse 2005:1025.

1.37 Förslag till förordning om ändring i förordningen (2005:323) om tillträdesförbud vid idrottsarrangemang

Härigenom förskrivs att 2 § förordningen (2005:323) om tillträdesförbud vid idrottsarrangemang ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

2 §¹

Om en domstol eller åklagare beslutar om tillträdesförbud eller häver eller ändrar ett sådant förbud, ska Polismyndigheten underrättas om beslutet. Åklagarmyndigheten ska, i fråga om den som är föremål för registrering *enligt lagen (2015:51) om register över tillträdesförbud vid idrottsarrangemang*, till Polismyndigheten även lämna sådana uppgifter som anges i 8 § *samma lag* och som myndigheten har tillgång till i ett ärende som rör tillträdesförbud.

Bestämmelser om registrering av beslut om tillträdesförbud finns i lagen (1998:620) om belastningsregister och förordningen (1999:1134) om belastningsregister *samt i lagen (2015:51) om register över tillträdesförbud vid idrottsarrangemang* och förordningen (2015:54)

Om en domstol eller *en* åklagare beslutar om tillträdesförbud eller häver eller ändrar ett sådant förbud, ska Polismyndigheten underrättas om beslutet. Åklagarmyndigheten ska, i fråga om den som är föremål för registrering *i tillträdesförbudsregistret*, till Polismyndigheten även lämna sådana uppgifter som anges i 5 kap. 24 § *polisens brottsdatalag (2010:361)* och som myndigheten har tillgång till i ett ärende som rör tillträdesförbud.

Bestämmelser om registrering av beslut om tillträdesförbud finns i

1. lagen (1998:620) om belastningsregister,

2. förordningen (1999:1134) om belastningsregister,

3. *polisens brottsdatalag (2010:361)*, och

¹ Senaste lydelse 2015:56.

om register över tillträdesförbud vid idrottsarrangemang. 4. förordningen (2015:54) om register över tillträdesförbud vid idrottsarrangemang.

Denna förordning träder i kraft den 1 maj 2018.

1.38 Förslag till förordning om ändring i förordningen (2007:1141) med instruktion för Säkerhets- och integritetsskyddsmyndigheten

Härigenom föreskrivs att 2 och 20 §§ förordningen (2007:1141) med instruktion för Säkerhets- och integritetsskyddsmyndigheten ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

2 §¹

Myndigheten har till uppgift att i ärenden om registerkontroll enligt säkerhetsskyddslagen (1996:627) pröva frågor om utlämnande av uppgifter

1. från register som omfattas av lagen (1998:620) om belastningsregister,

2. från register som omfattas av lagen (1998:621) om misstankeregister,

3. från register som omfattas av lagen (2010:362) om polisens allmänna spaningsregister, och

4. som behandlas med stöd av polisdatalagen (2010:361).

2. från register som omfattas av lagen (1998:621) om misstankeregister, och

3. som Polismyndigheten eller Säkerhetspolisen behandlar med stöd av brottsdatalagen (2018:000), polisens brottsdatalag (2010:361) eller Säkerhetspolisens datalag (2018:000).

Myndigheten ska pröva frågor om utlämnande av uppgifter även i sådana fall som avses i 10 § förordningen (1989:149) om bevakningsföretag m.m. och 7 § skyddsförordningen (2010:523).

¹ Senaste lydelse 2010:1158.

20 §²

Om nämnden i sin verksamhet uppmärksammar förhållanden som kan utgöra brott, ska nämnden anmäla det till Åklagarmyndigheten (Riksåklagarens kansli) eller annan behörig myndighet.

Om nämnden uppmärksammar felaktigheter som kan medföra skadeståndsansvar för staten gentemot en fysisk eller en juridisk person, ska nämnden anmäla det till Justitiekanslern.

Om nämnden finner omständigheter som *Datainspektionen* bör uppmärksammas på, ska nämnden anmäla det till inspektionen.

Nämnden ska samråda med den berörda myndigheten innan en sådan anmälan som avses i första–tredje styckena lämnas. *Till anmälan ska nämnden foga sin utredning.* Efter det att anmälan har gjorts ska nämnden lämna myndigheten det biträde som behövs.

Om nämnden när den utför kontroll enligt 3 § lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet uppmärksammar felaktigheter som kan medföra skadeståndsansvar för staten gentemot en fysisk eller en juridisk person, ska nämnden anmäla det till Justitiekanslern.

Om nämnden bedömer att *Säkerhetspolisen* brister i sina skyldigheter vid behandling av personuppgifter på sådant sätt att *Datainspektionens* korrigerande befogenheter kan behöva användas, ska nämnden anmäla det till inspektionen.

Nämnden ska samråda med den berörda myndigheten innan en sådan anmälan som avses i första–tredje styckena ges in. När anmälan har gjorts ska nämnden lämna myndigheten det biträde som behövs. *Myndigheten har rätt att ta del av nämndens underlag i den utsträckning som behövs.*

Denna förordning träder i kraft den 1 maj 2018.

² Senaste lydelse 2009:1516.

1.39 Förslag till förordning om ändring i offentlighets- och sekretessförordningen (2009:641)

Härigenom föreskrivs att 2 § offentlighets- och sekretessförordningen (2009:641) ska ha följande lydelse.

Nuvarande lydelse

2 §¹

Följande myndigheter är i den utsträckning som framgår nedan undantagna från registreringskyldigheten enligt 5 kap. 1 § offentlighets- och sekretesslagen (2009:400).

Myndighet	Handlingar som innehåller sekretessreglerade uppgifter och som inte behöver registreras
Pensionsmyndigheten	– handlingar i försäkringsärenden, och
Polismyndigheten	– statistiskt primärmaterial – anteckningar om det löpande polisarbetet, – sådana protokoll enligt 27 och 28 §§ polislagen (1984:387) eller enligt lagen (1976:511) om omhändertagande av berusade personer m.m. som avser avvísningar, avlägsnanden, omhändertaganden, gripanden eller fängselanvändning och som inte registreras i särskilda ärenden, – underrättelser från Kriminalvården om permissioner, – handlingar som utgör

¹ Senaste lydelse 2016:864.

		underlag för belastningsregistret, misstankeregistret, register enligt 4 kap. <i>polisdatalagen</i> (2010:361) eller för på motsvarande sätt strukturerade uppgiftssamlingar som avser brottslig verksamhet och som förs med stöd av <i>polisdatalagen</i> ,
		– framställningar om fingeravtrycksundersökning, och
		– statistiskt primärmaterial
		– statistiskt primärmaterial
Riksbanken		

Statistiska centralbyrån		– statistiskt primärmaterial
Säkerhetspolisen		– anteckningar om det löpande polisarbetet,
		– underrättelser från Kriminalvården om permissioner,
		– handlingar som utgör underlag för strukturerade uppgiftssamlingar som avser brottslig verksamhet och som förs med stöd av <i>polisdatalagen</i> ,
Totalförsvarets myndighet	rekryterings-	– patientjournaler som rör totalförsvarspliktiga
Tullverket		– handlingar som rör klarering av varor och transportmedel,
		– handlingar som innehåller bokningsuppgifter inhämtade från transportföretag, och
		– handlingar som ingår i informationssystemet om transporter av sprit och cigaretter
åklagarmyndigheter		– utdrag ur folkbokföringsdatabasen,
		– utdrag ur belastningsregistret, misstankeregistret och register enligt <i>polisdatalagen</i> (2010:361),

- utdrag ur vägtrafikregistret,
och
- rekvisitioner av sådana utdrag

Föreslagen lydelse

2 §

Följande myndigheter är i den utsträckning som framgår nedan undantagna från registreringskyldigheten enligt 5 kap. 1 § offentlighets- och sekretesslagen (2009:400).

Myndighet	Handlingar som innehåller sekretessreglerade uppgifter och som inte behöver registreras
Pensionsmyndigheten	<ul style="list-style-type: none"> – handlingar i försäkringsärenden, och – statistiskt primärmaterial
Polismyndigheten	<ul style="list-style-type: none"> – anteckningar om det löpande polisarbetet, – sådana protokoll enligt 27 och 28 §§ polislagen (1984:387) eller enligt lagen (1976:511) om omhändertagande av berusade personer m.m. som avser avvisningar, avlägsnanden, omhändertaganden, gripanden eller fängselanvändning och som inte registreras i särskilda ärenden, – underrättelser från Kriminalvården om permissioner, – handlingar som utgör underlag för belastningsregistret, misstankeregistret, register enligt 5 kap. polisens brottsdatalag (2010:361) eller för på motsvarande sätt strukturerade uppgiftssamlingar som avser

	<p>brottslig verksamhet och som förs med stöd av <i>polisens brottsdatalag</i>,</p> <ul style="list-style-type: none"> – framställningar om fingeravtrycksundersökning, och – statistiskt primärmaterial – statistiskt primärmaterial
Riksbanken	

Statistiska centralbyrån	– statistiskt primärmaterial
Säkerhetspolisen	<ul style="list-style-type: none"> – anteckningar om det löpande polisarbetet, – underrättelser från Kriminalvården om permissioner, – handlingar som utgör underlag för strukturerade uppgiftssamlingar som avser brottslig verksamhet och som förs med stöd av <i>Säkerhetspolisens datalag (2018:000)</i>, – patientjournaler som rör totalförsvarspliktiga – handlingar som rör klarering av varor och transportmedel, – handlingar som innehåller bokningsuppgifter inhämtade från transportföretag, och – handlingar som ingår i informationssystemet om transporter av sprit och cigaretter
Totalförsvarets rekryteringsmyndighet	– utdrag ur folkbokföringsdatabasen,
Tullverket	<ul style="list-style-type: none"> – utdrag ur belastningsregistret, misstankeregistret och register enligt <i>polisens brottsdatalag (2010:361)</i>, – utdrag ur vägtrafikregistret, och – rekvisitioner av sådana utdrag
åklagarmyndigheter	

Denna förordning träder i kraft den 1 maj 2018.

1.40 Förslag till förordning om ändring i polisdataförordningen (2010:1155)

Härigenom föreskrivs i fråga om polisdataförordningen (2010:1155)

dels att 2–4, 6, 8, 10, 12, 17 och 18 §§ ska upphöra att gälla,

dels att rubrikerna före 2, 3 och 14 § ska utgå,

dels att nuvarande 4 a § ska betecknas 2 § och att rubriken efter nuvarande 2 a § ska placeras före nya 2 §, att nuvarande 5 § ska betecknas 3 § och att rubriken före nuvarande 5 § ska placeras före nya 3 §, att nuvarande 7 § ska betecknas 4 §, att nuvarande 11 § ska betecknas 5 § och att rubriken före nuvarande 10 § ska placeras före nya 5 §, att nuvarande 13 § ska betecknas 6 §, att nuvarande 14 § ska betecknas 7 §, att nuvarande 15 § ska betecknas 8 §, att nuvarande 16 § ska betecknas 9 §, att nuvarande 18 a § ska betecknas 10 §, att nuvarande 18 b § ska betecknas 11 §, att nuvarande 19 § ska betecknas 12 § och att rubriken före nuvarande 19 § ska placeras före nya 12 §, att nuvarande 20 § ska betecknas 13 § och att rubriken före nuvarande 20 § ska placeras före nya 13 §, att nuvarande 21 § ska betecknas 14 §, att nuvarande 22 § ska betecknas 15 §, att nuvarande 23 § ska betecknas 16 §, att nuvarande 24 § ska betecknas 17 §, att nuvarande 25 § ska betecknas 18 §, att nuvarande 26 § ska betecknas 19 §, att nuvarande 27 § ska betecknas 20 § och att rubriken före nuvarande 27 § ska placeras före nya 20 §, att nuvarande 28 § ska betecknas 21 § och att rubriken före nuvarande 28 § ska placeras före nya 21 § och att nuvarande 29 § ska betecknas 22 §,

dels att rubriken efter nuvarande 18 b § ska placeras efter nya 11 § och lyda Längsta tid för behandling m.m.,

dels att 1 §, nya 2–9 och 12–22 §§ och rubrikerna före nya 5, 13 och 20 §§, ska ha följande lydelse,

dels att rubriken till förordningen ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

Polisdataförordning

Polisens brottsdataförordning

1 §

I denna förordning finns kompletterande föreskrifter *om sådan behandling av personuppgifter som omfattas av polisdatalagen* (2010:361). *Begrepp och uttryck som används i denna förordning har samma innebörd och tillämpningsområde som i lagen.*

I denna förordning finns kompletterande föreskrifter *till polisens brottsdatalag* (2010:361).

2 §¹

Endast tjänstemän vid den finansunderrättelseenhet vid Polismyndigheten som anges i 35 § förordningen (2014:1102) med instruktion för Polismyndigheten får ha tillgång till uppgifter i penningtvätsregister som förs med stöd av 4 kap. 18 § *polisdatalagen* (2010:361).

Endast tjänstemän vid den finansunderrättelseenhet vid Polismyndigheten som anges i 35 § förordningen (2014:1102) med instruktion för Polismyndigheten får ha tillgång till uppgifter i penningtvätsregister som förs med stöd av 5 kap. 18 § *polisens brottsdatalag* (2010:361).

Endast tjänstemän vid den nationella funktion för internationella uppgifter vid Polismyndigheten som anges i 35 § förordningen med instruktion för Polismyndigheten får ha tillgång till uppgifter i det internationella registret som förs med stöd av 4 kap. 21 § *polisdatalagen*.

Endast tjänstemän *som fullgör arbetsuppgifter* vid den nationella funktion för internationella uppgifter vid Polismyndigheten som anges i 35 § förordningen med instruktion för Polismyndigheten får ha tillgång till uppgifter i det internationella registret som förs med stöd av 5 kap. 21 § *polisens brottsdatalag*.

¹ Senaste lydelse 2014:1181.

Vid Polismyndigheten ska det löpande föras en förteckning över de tjänstemän vid myndigheten som behandlar uppgifter enligt första och andra styckena.

3 §²

Vid sökning enligt 3 kap. 6 § *polisdatalagen* (2010:361) får *uppgift* som visar att den sökta personen tidigare varit misstänkt för ett visst brott inte tas fram om en domstol, genom avgörande som har *vunnit* laga kraft, har ogillat åtalet, meddelat frikännande dom eller avskrivit målet sedan åtalet lagts *ned*.

Polismyndigheten får meddela föreskrifter om begränsning av tillgången till sådana uppgifter som avses i 3 kap. 6 § första stycket polisdatalagen. Särskild hänsyn ska då tas till den enskildes rätt till skydd mot intrång i den personliga integriteten. Tillgången till personuppgifter om tidigare misstankar om brott ska särskilt begränsas.

Vid sökning enligt 3 kap. 5 § *polisens brottsdatalag* (2010:361) får *uppgifter* som visar att den sökta personen tidigare *har* varit misstänkt för ett visst brott inte tas fram om en domstol, genom ett avgörande som har *fått* laga kraft, har ogillat åtalet, meddelat frikännande dom eller avskrivit målet sedan åtalet lagts *ner*.

4 §³

Vid Polismyndigheten ska det löpande föras en förteckning över de tjänstemän vid *myndigheten* som utför uppgifter enligt 3 kap. 7 § andra stycket *polisdatalagen* (2010:361).

Polismyndigheten *och Eko-brottsmyndigheten* ska löpande *föra* förteckning över de tjänstemän vid *respektive myndighet* som utför uppgifter enligt 3 kap. 6 § andra stycket *polisens brottsdatalag* (2010:361).

² Senaste lydelse 2014:1181.

³ Senaste lydelse 2014:1181.

Ändamål för behandling och Utlämnande av personuppgifter utlämnande av vissa uppgifter

5 §

Om en uppgift i en förundersökning kan antas ha betydelse för en konkursutredning, *får uppgiften lämnas ut till konkursförvaltaren.*

Om en uppgift i en förundersökning kan antas ha betydelse för en konkursutredning, *har konkursförvaltaren rätt att ta del av uppgiften.*

6 §

Uppgifter som behandlas enligt 2 kap. 7 § *polisdatalagen* (2010:361) får, om det är förenligt med svenska intressen, lämnas ut till en utländsk myndighet som ansvarar för bekämpning av penningtvätt eller finansiering av särskilt allvarlig brottslighet, om det behövs för att den utländska myndigheten ska kunna förebygga, förhindra, upptäcka, utreda eller *beivra* brott.

Personuppgifter som behandlas enligt 2 kap. 1 § *polisens brottsdatalag* (2010:361) får, om det är förenligt med svenska intressen, lämnas ut till en utländsk myndighet som ansvarar för bekämpning av penningtvätt eller finansiering av särskilt allvarlig brottslighet, om det behövs för att den utländska myndigheten ska kunna förebygga, förhindra, upptäcka, utreda eller *lagföra* brott.

7 §⁴

Polismyndigheten får meddela närmare *föreskrifter om vad som krävs* i fråga om behörighet och säkerhet för att myndigheten ska *kunna* medge direktåtkomst *till uppgifter för de myndigheter som anges i* 3 kap. 8 § *polisdatalagen* (2010:361).

Direktåtkomst *till uppgifterna* får inte medges innan Polismyndigheten har försäkrat sig

Polismyndigheten får *ställa villkor* i fråga om behörighet och säkerhet för att myndigheten ska medge direktåtkomst enligt 3 kap. 7 § *polisens brottsdatalag* (2010:361). *Detsamma gäller Ekobrottsmyndigheten.*

Direktåtkomst får inte medges innan Polismyndigheten *respektive Ekobrottsmyndigheten*

⁴ Senaste lydelse 2014:1181.

om att den mottagande myndigheten uppfyller kraven på behörighet och säkerhet.

har försäkrat sig om att den mottagande myndigheten uppfyller kraven på behörighet och säkerhet.

8 §⁵

Säkerhetspolisens, Ekobrottsmyndighetens, Åklagarmyndighetens, Tullverkets och Kustbevakningens direktåtkomst enligt 4 kap. 10 § *polisdatalagen* (2010:361) till register över DNA-profiler ska begränsas till uppgifter om huruvida någon förekommer i sådana register.

Säkerhetspolisens, Ekobrottsmyndighetens, Åklagarmyndighetens, Tullverkets och Kustbevakningens direktåtkomst enligt 5 kap. 10 § *polisens brottsdatalag* (2010:361) till register över dna-profiler ska begränsas till uppgifter om huruvida någon förekommer i sådana register.

9 §⁶

Säkerhetspolisens, Ekobrottsmyndighetens, Tullverkets, Kustbevakningens och Skatteverkets direktåtkomst enligt 4 kap. 17 § *polisdatalagen* (2010:361) till personuppgifter om fingeravtryck ska begränsas till uppgifter om huruvida någon förekommer i fingeravtrycksregister.

Säkerhetspolisens, Ekobrottsmyndighetens, Tullverkets, Kustbevakningens och Skatteverkets direktåtkomst enligt 5 kap. 17 § *polisens brottsdatalag* (2010:361) till fingeravtrycks- och signalementsregister ska begränsas till uppgifter om huruvida någon förekommer i fingeravtrycksregister.

12 §⁷

När *Polismyndigheten* eller *Säkerhetspolisen* arkiverar uppgifter och handlingar digitalt ska de arkiverade uppgifterna och handlingarna avskiljas från myndighetens brottbekämpande

När uppgifter och handlingar arkiveras digitalt ska uppgifterna och handlingarna avskiljas så att de inte kan behandlas för något av de syften som anges i 2 kap. 1 § *polisens brottsdatalag*

⁵ Senaste lydelse 2014:1181.

⁶ Senaste lydelse 2014:1181.

⁷ Senaste lydelse 2014:1181.

verksamhet. Åtkomsten till arkiverade uppgifter och handlingar ska begränsas till särskilt angivna tjänstemän.

Polismyndigheten *respektive Säkerhetspolisen* får, efter samråd med Riksarkivet, meddela närmare föreskrifter om digital arkivering.

Bevarande av uppgifter

I 21–26 §§ föreskrivs att vissa kategorier av *uppgifter* i brottsanmälningar och avslutade förundersökningar får behandlas i *polisens brottsbekämpande verksamhet efter utgången av den tid som anges i 3 kap. 10 och 11 §§ polisdatalagen* (2010:361). Detsamma gäller *uppgifter* i andra utredningar som handläggs enligt bestämmelser i 23 kap. rättegångsbalken.

När *uppgifter* får behandlas enligt 21–26 §§ får, utöver vad som sägs i de bestämmelserna, följande *uppgifter* behandlas:

1. ärendenummer eller liknande *referensuppgift*,
2. *brottskod*, och
3. uppgifter om omständigheterna kring brottet.

(2010:361). Åtkomsten till arkiverade uppgifter och handlingar ska begränsas till särskilt angivna tjänstemän.

Polismyndigheten får, efter att ha gett Riksarkivet tillfälle att yttra sig, meddela närmare föreskrifter om digital arkivering.

Fortsatt behandling av vissa personuppgifter

13 §

I 14–19 §§ föreskrivs att vissa kategorier av *personuppgifter* i brottsanmälningar och avslutade förundersökningar får behandlas för ändamål som omfattas av tillämpningsområdet för *polisens brottsdatalag* (2010:361), trots att den tid som anges i 4 kap. 3 och 4 §§ samma lag har löpt ut. Detsamma gäller *personuppgifter* i andra utredningar som handläggs enligt bestämmelser i 23 kap. rättegångsbalken.

När *personuppgifter* får behandlas enligt 14–19 §§ får, utöver vad som sägs i de bestämmelserna, följande *uppgifter* behandlas:

1. ärendenummer eller liknande *referensuppgifter*,
2. *brottskoder*, och

14 §

Uppgifter om den dömde i en förundersökning som lett till fällande dom får behandlas *efter utgången av den tid som anges i 3 kap. 11 § första stycket polisdatalagen* (2010:361), om behandlingen av särskilda skäl är nödvändig för att finna samband mellan olika brott eller mellan tänkbara gärningsmän.

Uppgifterna ska dock *gallras* senast i samband med att uppgifterna om den dömde *gallras* ur belastningsregistret enligt lagen (1998:620) om belastningsregister.

Uppgifter om den dömde i en förundersökning som *har* lett till fällande dom får behandlas *trots att den tid som anges i 4 kap. 4 § första stycket polisens brottsdatalag* (2010:361) *har löpt ut*, om behandlingen av särskilda skäl är nödvändig för att finna samband mellan olika brott eller mellan tänkbara gärningsmän.

Behandlingen ska dock *upphöra* senast i samband med att uppgifterna om den dömde *tas bort* ur belastningsregistret enligt lagen (1998:620) om belastningsregister.

15 §

Uppgifter om en person som har varit misstänkt i en förundersökning som har lagts *ned* eller har avslutats på annat sätt än genom åtal, får i ett enskilt fall behandlas *efter utgången av den tid som anges i 3 kap. 11 § andra stycket polisdatalagen* (2010:361), om behandlingen är nödvändig för att *trots detta kunna lagföra personen*.

Uppgifterna ska dock *gallras* senast då åtal inte längre får väckas för brottet eller, i fall som avses i 35 kap. 2 § första stycket brottsbalken, senast sjuttio år från den dag då brottet begicks.

Uppgifter om en person som har varit misstänkt i en förundersökning som har lagts *ner* eller har avslutats på annat sätt än genom åtal, får i ett enskilt fall behandlas *om det är nödvändigt för att kunna lagföra personen trots att den tid som anges i 4 kap. 4 § andra stycket polisens brottsdatalag* (2010:361) *har löpt ut*.

Behandlingen ska dock *upphöra* senast då åtal inte längre får väckas för brottet eller, i fall som avses i 35 kap. 2 § första stycket brottsbalken, senast sjuttio år från den dag då brottet begicks.

16 §⁸

Uppgifter om personer som har dömts för, eller har varit misstänkta för, brott där det finns en betydande risk för återfall i samma eller likartad brottslighet, får behandlas *efter utgången av den tid som anges i 3 kap. 10 och 11 §§ polisdatalagen* (2010:361), om behandlingen av särskilda skäl är nödvändig för att förebygga, förhindra eller upptäcka brott för vilket fängelse i fyra år eller däröver är föreskrivet.

Uppgifterna ska dock gallras, i fråga om brott som har lett till fällande dom, senast i samband med att uppgifterna *gallras* ur belastningsregistret enligt lagen (1998:620) om belastningsregister och i övriga fall senast femton år efter det att förundersökningen lades ner eller avslutades på annat sätt.

Polismyndigheten får i samråd med Säkerhetspolisen meddela närmare föreskrifter om vid vilka typer av brott det får anses finnas en sådan risk för återfall som anges i första stycket.

Uppgifter om personer som har dömts för, eller har varit misstänkta för, brott där det finns en betydande risk för återfall i samma eller likartad brottslighet, får behandlas *trots att den tid som anges i 4 kap. 3 och 4 §§ polisens brottsdatalag* (2010:361) *har löpt ut*, om behandlingen av särskilda skäl är nödvändig för att förebygga, förhindra eller upptäcka brott för vilket *det är föreskrivet* fängelse i fyra år eller däröver.

Behandlingen ska dock upphöra, i fråga om brott som har lett till fällande dom, senast i samband med att uppgifterna *tas bort* ur belastningsregistret enligt lagen (1998:620) om belastningsregister och i övriga fall senast femton år efter det att förundersökningen lades ner eller avslutades på annat sätt.

17 §

Om uppgifter om egendom som har varit föremål för brott finns i en förundersökning eller i en brottsanmälan, får uppgif-

Om uppgifter om egendom som har varit föremål för brott finns i en förundersökning eller i en brottsanmälan, får uppgif-

⁸ Senaste lydelse 2014:1181.

terna behandlas *efter utgången av* den tid som anges i 3 kap. 10 och 11 §§ *polisdatalagen* (2010:361), om behandlingen av särskilda skäl är nödvändig för att kunna återställa egendomen till rätt ägare eller för att kunna spåra föremålets användning vid annat brott eller brottslig verksamhet.

Personuppgifter *knutna till* sådan egendom ska dock *gallras* när *behandlingen* inte längre är nödvändig för något av de ändamål som anges i första stycket.

terna behandlas *trots att* den tid som anges i 4 kap. 3 och 4 §§ *polisens brottsdatalag* (2010:361) *har löpt ut*, om behandlingen av särskilda skäl är nödvändig för att kunna återställa egendomen till rätt ägare eller för att kunna spåra föremålets användning vid annat brott eller brottslig verksamhet.

Behandlingen av personuppgifter *som avser* sådan egendom ska dock *upphöra* när *den* inte längre är nödvändig för något av de ändamål som anges i första stycket.

18 §

Uppgifter om en person som är eftersökt *såsom* försvunnen får behandlas *så länge* uppgiften *behövs för ändamålet med behandlingen*.

Uppgifterna ska dock gallras senast tre månader efter det att personen har anträffats.

Uppgifter om *att* en person *varit* eftersökt *som* försvunnen får *inte* behandlas *för ändamålet att återfinna personen längre än tre månader efter det att personen har anträffats.*

19 §

Skildringar av barn i det digitala referensbiblioteket över barnpornografiska framställningar får behandlas *efter utgången av* den tid som anges i 3 kap. 10 och 11 §§ *polisdatalagen* (2010:361), om behandlingen är nödvändig för att förebygga, förhindra eller upptäcka följande brott mot barn: brott

Skildringar av barn i det digitala referensbiblioteket över barnpornografiska framställningar får behandlas *efter utgången av* den tid som anges i 4 kap. 3 och 4 §§ *polisens brottsdatalag* (2010:361), om behandlingen är nödvändig för att förebygga, förhindra eller upptäcka följande brott mot barn: brott

mot 4 kap. 1 a §, 6 kap. eller 16 kap. 10 a § brottsbalken.

Uppgifterna ska dock *gallras* senast fyrtio år efter det att de infördes i referensbiblioteket.

Undantag från gallring

mot 4 kap. 1 a §, 6 kap. eller 16 kap. 10 a § brottsbalken.

Behandlingen ska dock *upphöra* senast fyrtio år efter det att skildringarna infördes i referensbiblioteket.

Behandling för arkivändamål av allmänt intresse m.m.

20 §⁹

Riksarkivet får, *efter samråd med Polismyndigheten respektive Säkerhetspolisen*, meddela föreskrifter om att *uppgifter som ska gallras enligt 2 kap. 13 §, 3 kap. 14 §, 4 kap. 14, 15, 20 och 22 §§ eller 6 kap. 7 och 12 §§ polisdatalagen (2010:361)* får *bevaras för historiska, statistiska eller vetenskapliga ändamål*.

Riksarkivet får, *efter att ha gett berörd myndighet tillfälle att yttra sig*, meddela föreskrifter om att *personuppgifter som avses i 4 kap. 2 och 7–10 §§ och 5 kap. 15, 16, 20 och 22 §§ polisens brottsdatalag (2010:361)* får *behandlas under längre tid för arkivändamål av allmänt intresse och vetenskapliga, statistiska eller historiska ändamål*.

21 §¹⁰

Polismyndigheten och *Säkerhetspolisen* får *för sina respektive verksamhetsområden* meddela de ytterligare föreskrifter som behövs för verkställighet av *polisdatalagen (2010:361)* och denna förordning.

Polismyndigheten får, *efter att ha gett berörd myndighet tillfälle att yttra sig*, meddela de ytterligare föreskrifter som behövs för verkställighet av *polisens brottsdatalag (2010:361)* och denna förordning.

22 §¹¹

Innan Polismyndigheten eller *Säkerhetspolisen* meddelar föreskrifter med stöd av denna för-

Innan Polismyndigheten meddelar föreskrifter med stöd av denna förordning, ska myn-

⁹ Senaste lydelse 2015:450.

¹⁰ Senaste lydelse 2014:1181.

¹¹ Senaste lydelse 2014:1181.

ordning i frågor som berör särskilda risker för intrång i den personliga integriteten ska myndigheten samråda med Datainspektionen och Säkerhets- och integritetsskyddsnämnden.

digheten samråda med Datainspektionen i frågor som berör särskilda risker för intrång i den personliga integriteten.

Denna förordning träder i kraft den 1 maj 2018.

1.41 Förslag till förordning om ändring i kustbevakningsdataförordningen (2012:146)

Härigenom föreskrivs i fråga om kustbevakningsdataförordningen (2012:146)

dels att 2–5, 7–9, 11, 19 och 20 §§ ska upphöra att gälla,

dels att rubriken efter 2 § och rubrikerna före 3 och 19 §§ ska utgå,

dels att nuvarande 6 § ska betecknas 2 § och att rubriken före nuvarande 5 § ska placeras före nya 2 §, att nuvarande 10 § ska betecknas 4 § och att rubriken före nuvarande 8 § ska placeras före nya 4 §, att rubriken efter nuvarande 11 § ska placeras efter nya 4 §, att nuvarande 12 § ska betecknas 5 § och att rubriken före nuvarande 12 § ska placeras före nya 5 §, att nuvarande 13 § ska betecknas 11 §, att nuvarande 14 § ska betecknas 6 § och att rubriken före nuvarande 14 § ska placeras före nya 6 §, att nuvarande 15 § ska betecknas 7 §, att nuvarande 16 § ska betecknas 8 §, att nuvarande 17 § ska betecknas 9 § och att nuvarande 18 § ska betecknas 10 §,

dels att 1 §, nya 2–11 §§ och rubrikerna före 1 § och nya 4–6 §§ och efter nya 4 § ska ha följande lydelse,

dels att det ska införas en ny paragraf, 3 §, och en ny rubrik före nya 11 § av följande lydelse,

dels att rubriken till förordningen ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

Kustbevakningsdataförordning

Kustbevakningens brottsdataförordning

Inledande bestämmelser

Allmän bestämmelse

1 §

I denna förordning finns kompletterande föreskrifter om sådan behandling av personupp-

I denna förordning finns kompletterande föreskrifter till Kustbevakningens brottsdatalog

gifter som omfattas av kustbevakningsdatalagen (2012:145). De uttryck som används i denna förordning har samma innebörd och tillämpningsområde som i lagen.

2 §

Vid sökning enligt 4 kap. 5 § *kustbevakningsdatalagen* (2012:145) får *uppgifter* som visar att den sökta personen tidigare har varit misstänkt för ett visst brott inte tas fram om en domstol, genom ett avgörande som har *vunnit* laga kraft, har ogillat åtalet, meddelat frikännande dom eller skrivit av målet sedan åtalet lagts *ned*.

Kustbevakningen får meddela föreskrifter om begränsning av tillgången till sådana uppgifter som avses i 4 kap. 5 § första stycket kustbevakningsdatalagen. Särskild hänsyn ska då tas till den enskildes rätt till skydd mot intrång i den personliga integriteten. Tillgången till personuppgifter om tidigare mistankar om brott ska särskilt begränsas.

Vid sökning enligt 3 kap. 4 § *Kustbevakningens brottsdatalag* (2012:145) får *uppgift* som visar att den sökta personen tidigare har varit misstänkt för ett visst brott inte tas fram om en domstol, genom avgörande som har *fått* laga kraft, har ogillat åtalet, meddelat frikännande dom eller skrivit av målet sedan åtalet lagts *ner*.

3 §

Kustbevakningen ska löpande föra förteckning över de tjänstemän som utför uppgifter enligt 3 kap. 5 § andra stycket kustbevakningens brottsdatalag (2012:145).

Elektroniskt utlämnande av Direktåtkomst personuppgifter

4 §

Kustbevakningen får *meddela närmare föreskrifter om vad som krävs* i fråga om behörighet och säkerhet för att myndigheten ska *kunna* medge direktåtkomst till personuppgifter för de myndigheter som anges i 9 § denna förordning och i 4 kap. 7 § kustbevakningsdatalagen (2012:145).

Direktåtkomst till uppgifterna får inte medges innan Kustbevakningen har försäkrat sig om att den mottagande myndigheten uppfyller kraven på behörighet och säkerhet.

Kustbevakningen får *ställa villkor* i fråga om behörighet och säkerhet för att myndigheten ska medge direktåtkomst enligt 3 kap. 6 § Kustbevakningens brottsdatalag (2012:145).

Direktåtkomst får inte medges innan Kustbevakningen har försäkrat sig om att den mottagande myndigheten uppfyller kraven på behörighet och säkerhet.

Bevarande och gallring

Längsta tid för behandling m.m.

Allmänna bestämmelser om arkivering och gallring

Digital arkivering

5 §

När Kustbevakningen arkiverar uppgifter och handlingar digitalt ska de arkiverade uppgifterna och handlingarna avskiljas från myndighetens brottbekämpande verksamhet. Åtkomsten till arkiverade uppgifter och handlingar ska begränsas till särskilt angivna tjänstemän.

När uppgifter och handlingar arkiveras digitalt ska uppgifterna och handlingarna avskiljas så att de inte kan behandlas för något av de syften som anges i 2 kap. 1 § Kustbevakningens brottsdatalag (2012:145). Åtkomsten till arkiverade uppgifter och handlingar ska begränsas till särskilt angivna tjänstemän.

Bevarande av personuppgifter som behandlas i den brottsbekämpande verksamheten

Fortsatt behandling av vissa personuppgifter

6 §

I 15–18 §§ föreskrivs att vissa kategorier av *uppgifter* i brottsanmälningar och avslutade förundersökningar får behandlas i *Kustbevakningens brottsbekämpande verksamhet efter utgången av den tid som anges i 4 kap. 9 och 10 §§ kustbevakningsdatalagen* (2012:145). Detsamma gäller *uppgifter* i andra utredningar som handläggs enligt bestämmelser i 23 kap. rättegångsbalken.

Vid behandlingen av *uppgifter* enligt 15–18 §§ får, utöver vad som sägs där, även följande *uppgifter* behandlas:

1. ärendenummer och liknande referensuppgifter,
2. brottskoder, och
3. uppgifter om omständigheterna kring brottet.

I 7–10 §§ föreskrivs att vissa kategorier av *personuppgifter* i brottsanmälningar och avslutade förundersökningar får behandlas för ändamål som omfattas av *tillämpningsområdet för Kustbevakningens brottsdatalag* (2012:145), trots att den tid som anges i 4 kap. 3 och 4 §§ *samma lag har löpt ut*. Detsamma gäller *personuppgifter* i andra utredningar som handläggs enligt bestämmelser i 23 kap. rättegångsbalken.

När *personuppgifter* får behandlas enligt 7–10 §§ får, utöver vad som sägs i de bestämmelserna, följande *uppgifter* behandlas:

1. ärendenummer eller liknande referensuppgifter,

7 §

Uppgifter om *en dömd person* i en förundersökning som har lett till *en* fällande dom får behandlas *efter utgången av den tid som anges i 4 kap. 10 § första stycket kustbevakningsdatalagen* (2012:145), om behandlingen av särskilda skäl är nödvändig för att finna samband

Uppgifter om *den dömd*e i en förundersökning som har lett till fällande dom får behandlas *trots att den tid som anges i 4 kap. 4 § första stycket Kustbevakningens brottsdatalag* (2012:145) *har löpt ut*, om behandlingen av särskilda skäl är nödvändig för att finna samband

mellan olika brott eller mellan tänkbara gärningsmän.

Uppgifterna ska dock gallras senast när uppgifterna om den dömde gallras ur belastningsregistret enligt lagen (1998:620) om belastningsregister.

mellan olika brott eller mellan tänkbara gärningsmän.

Behandlingen ska dock upphöra senast i samband med att uppgifterna om den dömde tas bort ur belastningsregistret enligt lagen (1998:620) om belastningsregister.

8 §

Uppgifter om en person som har varit misstänkt i en förundersökning som lagts *ned* eller avslutats på annat sätt än genom åtal får i ett enskilt fall behandlas *efter utgången av* den tid som anges i 4 kap. 10 § andra stycket kustbevakningsdatalagen (2012:145), *om behandlingen är nödvändig för att kunna lagföra personen.*

Uppgifterna ska dock gallras senast då åtal inte längre får väckas för brottet eller senast sjuttio år från den dag då brottet begicks i fall som avses i 35 kap. 2 § första stycket brottsbalken.

Uppgifter om en person som har varit misstänkt i en förundersökning som *har* lagts *ner* eller *har* avslutats på annat sätt än genom åtal, får i ett enskilt fall behandlas *om det är nödvändigt för att kunna lagföra personen trots att* den tid som anges i 4 kap. 4 § andra stycket Kustbevakningens brottsdatalag (2012:145) *har löpt ut.*

Behandlingen ska dock upphöra senast då åtal inte längre får väckas för brottet.

9 §

Om uppgifter om egendom som har varit föremål för brott finns i en förundersökning eller i en brottsanmälan, får uppgifterna behandlas *efter utgången av* den tid som anges i 4 kap. 9 och 10 §§ kustbevakningsdatalagen (2012:145). *Detta gäller dock under förutsättning att behandlingen av särskilda skäl är nöd-*

Om uppgifter om egendom som har varit föremål för brott finns i en förundersökning eller i en brottsanmälan, får uppgifterna behandlas *trots att* den tid som anges i 4 kap. 3 och 4 §§ Kustbevakningens brottsdatalag (2012:145) *har löpt ut, om behandlingen av särskilda skäl är nödvändig för att kunna åter-*

vändig för att kunna återställa egendomen till rätt ägare eller spåra föremålets användning vid annat brott eller brottslig verksamhet.

Personuppgifter som gäller sådan egendom ska dock *gallras* när *behandlingen* inte längre är nödvändig för något av de ändamål som anges i första stycket.

ställa egendomen till rätt ägare eller *för att kunna* spåra föremålets användning vid annat brott eller brottslig verksamhet.

Behandlingen av personuppgifter som gäller sådan egendom ska dock *upphöra* när *den* inte längre är nödvändig för något av de ändamål som anges i första stycket.

10 §

Uppgifter om en person som är eftersökt som försvunnen får behandlas *så länge uppgiften behövs för ändamålet med behandlingen*.

Uppgifterna ska dock gallras senast tre månader efter det att personen har anträffats.

Uppgifter om *att* en person varit eftersökt som försvunnen får *inte* behandlas *längre än tre månader efter det att personen har anträffats*.

Behandling för arkivändamål av allmänt intresse m.m.

11 §

Riksarkivet får, efter *samråd med Kustbevakningen*, meddela föreskrifter om att uppgifter som ska *gallras enligt 3 kap. 5 §, 4 kap. 13 § eller 5 kap. 7 § kustbevakningsdatalagen (2012:145)* får *bevaras för historiska, statistiska eller vetenskapliga ändamål*.

Riksarkivet får, efter *att ha gett Kustbevakningen tillfälle att yttra sig*, meddela föreskrifter om att *personuppgifter som avses i 4 kap. 2 § första stycket och 7–9 §§ Kustbevakningens brottsdatalag (2012:145)* får *behandlas under längre tid för arkivändamål av allmänt intresse och vetenskapliga, statistiska eller historiska ändamål*.

Denna förordning träder i kraft den 1 maj 2018.

1.42 Förslag till förordning om ändring i förordningen (2014:405) om Polismyndighetens elimineringsdatabas

Härigenom föreskrivs i fråga om förordningen (2014:405) om Polismyndighetens elimineringsdatabas

dels att i 2–7 §§ ”DNA” ska bytas ut mot ”dna”,

dels att 5 § ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

Sökning i elimineringsdatabasen får endast göras av särskilt angivna tjänstemän vid Nationellt forensiskt centrum som är behöriga att göra sökningar i de register över *DNA-profiler* som regleras i 4 kap. *polisdatalagen* (2010:361).

5 §¹

Sökning i elimineringsdatabasen får endast göras av särskilt angivna tjänstemän vid Nationellt forensiskt centrum som är behöriga att göra sökningar i de register över *dna-profiler* som regleras i 5 kap. *polisens brottsdatalag* (2010:361).

Denna förordning träder i kraft den 1 maj 2018.

¹ Senaste lydelse 2014:1189.

1.43 Förslag till förordning om ändring i förordningen (2014:1103) med instruktion för Säkerhetspolisen

Härigenom föreskrivs att 10 § förordningen (2014:1103) med instruktion för Säkerhetspolisen ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

10 §

I 6 § polislagen (1984:387) finns grundläggande bestämmelser om Säkerhetspolisens samarbete med andra myndigheter och organ.

Säkerhetspolisen ska lämna lämna tekniskt biträde till Ekobrottsmyndigheten, Åklagarmyndigheten och Tullverket i den utsträckning som myndigheterna kommer överens om.

Denna förordning träder i kraft den 1 maj 2018.

1.44 Förslag till förordning om ändring i förordningen (2015:54) om register över tillträdesförbud vid idrottsarrangemang

Härigenom förskrivs i fråga om förordningen (2015:54) om register över tillträdesförbud vid idrottsarrangemang

dels att 2–4 §§ ska upphävas,

dels att rubriken före 2 § ska utgå,

dels att 5–9 §§ ska betecknas 2–6 §§,

dels att rubriken före 3 § ska placeras före nya 2 §, rubriken före 7 § ska placeras före nya 4 § och rubriken före 8 § ska placeras före nya 5 §,

dels att nya 4 och 5 §§ ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

4 §

Bestämmelser om skyldighet att lämna sådana uppgifter som anges i 8 § *lagen (2015:51) om register över tillträdesförbud vid idrottsarrangemang* finns i 2 § förordningen (2005:323) om tillträdesförbud vid idrottsarrangemang.

Bestämmelser om skyldighet att lämna sådana uppgifter som anges i 5 kap. 24 § *polisens brottsdatalog (2010:361)* finns i 2 § förordningen (2005:323) om tillträdesförbud vid idrottsarrangemang.

5 §

Polismyndigheten får meddela de ytterligare föreskrifter som behövs för verkställighet av *lagen (2015:51) om register över tillträdesförbud vid idrottsarrangemang* och denna förordning.

Polismyndigheten får meddela de ytterligare föreskrifter som behövs för verkställighet av *lagen (2015:51) om idrottsorganisationers behandling av uppgifter om tillträdesförbud* och denna förordning.

Denna förordning träder i kraft den 1 maj 2018.

1.45 Förslag till förordning om ändring i förordningen (2015:476) om behandling av personuppgifter i Nationellt forensiskt centrum's uppdragsverksamhet

Härigenom föreskrivs att 1 § förordningen (2015:476) om behandling av personuppgifter i Nationellt forensiskt centrum's uppdragsverksamhet ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

Denna förordning gäller vid helt eller delvis automatiserad behandling av personuppgifter vid undersökningar som Nationellt forensiskt centrum i Polismyndigheten utför på uppdrag av andra än de myndigheter eller organ som anges i 5 kap. 1 § *polisdatalagen* (2010:361).

1 §

Denna förordning gäller vid helt eller delvis automatiserad behandling av personuppgifter vid undersökningar som Nationellt forensiskt centrum i Polismyndigheten utför på uppdrag av andra än de myndigheter eller organ som anges i 6 kap. 1 § *polisens brottsdatalag* (2010:361).

Denna förordning träder i kraft den 1 maj 2018.

1.46 Förslag till förordning om ändring i åklagardataförordningen (2015:575)

Härigenom föreskrivs i fråga om åklagardataförordningen (2015:575)

dels att 2, 3, 7 och 8 §§ ska upphöra att gälla,

dels att rubrikerna före 2 och 6 §§ ska utgå,

dels att nuvarande 4 § ska betecknas 2 § och att rubriken före nuvarande 4 § ska placeras före nya 2 §, att nuvarande 5 § ska betecknas 3 §, att nuvarande 6 § ska betecknas 4 §, att rubriken efter nuvarande 8 § ska placeras efter nya 4 §, att nuvarande 9 § ska betecknas 5 § och att rubriken före nuvarande 9 § ska placeras före nya 5 §, att nuvarande 10 § ska betecknas 6 § och att rubriken före nuvarande 10 § ska placeras före nya 6 §, att nuvarande 11 § ska betecknas 7 § och att rubriken före nuvarande 11 § ska placeras före nya 7 § och att nuvarande 12 § ska betecknas 8 §,

dels att 1 § och nya 2–8 §§ och rubriken före nya 6 § ska ha följande lydelse,

dels att rubriken efter nya 4 § ska lyda Längsta tid för behandling m.m.,

dels att det ska införas en ny rubrik före 1 § av följande lydelse,

dels att rubriken till förordningen ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

Åklagardataförordning

Åklagarväsendets brottsdataförordning

Allmän bestämmelse

1 §

I denna förordning finns kompletterande föreskrifter om sådan behandling av personuppgifter som omfattas av åklagardatalagen (2015:433). Begrepp och

I denna förordning finns kompletterande föreskrifter till åklagarväsendets brottsdatalag (2015:433).

uttryck som används i denna förordning har samma innebörd och tillämpningsområde som i lagen.

2 §

Åklagarmyndigheten och Ekobrottsmyndigheten får lämna uppgifter om juridiska personer till Skatteverket om uppgifterna behövs där för brottsbekämpande verksamhet.

Åklagarmyndigheten och Ekobrottsmyndigheten får lämna uppgifter om juridiska personer till Skatteverket *om myndigheten behöver uppgifterna i syfte att bekämpa brott.*

3 §

Åklagarmyndigheten och Ekobrottsmyndigheten får, om det är förenligt med svenska intressen, lämna personuppgifter som behandlas enligt 2 kap. 5 § åklagardatalagen (2015:433) till en utländsk myndighet, ett EU-organ eller en mellanfolklig organisation, om det behövs för att *mottagaren av uppgifterna ska kunna förebygga, förhindra, upptäcka, utreda eller beivra brott.*

Åklagarmyndigheten och Ekobrottsmyndigheten får, om det är förenligt med svenska intressen, lämna personuppgifter som behandlas enligt 2 kap. 1 § åklagarväsendets brottsdatalag (2015:433) till en utländsk myndighet, ett EU-organ eller en mellanfolklig organisation, om det behövs för att *den utländska myndigheten eller organisationen ska kunna förebygga, förhindra, upptäcka, utreda eller lagföra brott.*

4 §

Åklagarmyndigheten får, efter att ha gett Ekobrottsmyndigheten tillfälle att yttra sig, meddela närmare föreskrifter om omfattningen av direktåtkomst och om vad som krävs i fråga om behörighet och säkerhet för att direktåtkomst till uppgifter ska kunna medges de myndigheter som anges i 3 kap. 8 § åklagar-

Åklagarmyndigheten *respektive* Ekobrottsmyndigheten får ställa villkor i fråga om behörighet och säkerhet för att myndigheten ska medge direktåtkomst enligt 3 kap. 5 § åklagarväsendets brottsdatalag (2015:433).

datalagen (2015:433).

Direktåtkomst till uppgifterna får inte medges innan den myndighet som beslutar om direktåtkomst har försäkrat sig om att den mottagande myndigheten uppfyller *uppställda krav* på behörighet och säkerhet.

Direktåtkomst får inte medges innan den myndighet som beslutar om direktåtkomst har försäkrat sig om att den mottagande myndigheten uppfyller *kraven* på behörighet och säkerhet.

5 §

När *Åklagarmyndigheten eller Ekobrottsmyndigheten arkiverar uppgifter och handlingar* digitalt ska de arkiverade uppgifterna och handlingarna avskiljas från myndighetens operativa verksamhet. Åtkomsten till arkiverade uppgifter och handlingar ska begränsas till särskilt angivna tjänstemän.

När *uppgifter och handlingar arkiveras* digitalt ska uppgifterna och handlingarna avskiljas så att de inte kan behandlas för något av de syften som anges i 2 kap. 1 § åklagarväsendets brottsdatalag (2015:433). Åtkomsten till arkiverade uppgifter och handlingar ska begränsas till särskilt angivna tjänstemän.

Åklagarmyndigheten får, efter att ha gett Ekobrottsmyndigheten och Riksarkivet tillfälle att yttra sig, meddela närmare föreskrifter om digital arkivering.

Undantag från gallring

Behandling för arkivändamål av allmänt intresse m.m.

6 §

Riksarkivet får, efter att ha gett Åklagarmyndigheten och Ekobrottsmyndigheten tillfälle att yttra sig, meddela föreskrifter om att *uppgifter som ska gallras enligt 2 kap. 10 § tredje stycket åklagardatalagen (2015:433)* får bevaras för historiska, statistiska eller vetenskapliga ändamål.

Riksarkivet får, efter att ha gett Åklagarmyndigheten och Ekobrottsmyndigheten tillfälle att yttra sig, meddela föreskrifter om att *personuppgifter som avses i 4 kap. 4 § åklagarväsendets brottsdatalag (2015:433)* får behandlas under längre tid för arkivändamål av allmänt intresse och vetenskapliga, statistiska eller historiska ändamål.

7 §

Åklagarmyndigheten får, efter att ha gett Ekobrottsmyndigheten tillfälle att yttra sig, meddela de ytterligare föreskrifter som behövs för verkställighet av *åklagardatalagen* (2015:433) och denna förordning.

Åklagarmyndigheten får, efter att ha gett Ekobrottsmyndigheten tillfälle att yttra sig, meddela de ytterligare föreskrifter som behövs för verkställighet av *åklagarväsendets brottsdatalag* (2015:433) och denna förordning.

8 §

Innan Åklagarmyndigheten meddelar föreskrifter med stöd av denna förordning *i frågor som berör särskilda risker för intrång i den personliga integriteten* ska myndigheten ge Datainspektionen tillfälle att yttra sig.

Innan Åklagarmyndigheten meddelar föreskrifter med stöd av denna förordning, ska myndigheten *samråda med Datainspektionen i frågor som berör särskilda risker för intrång i den personliga integriteten.*

Denna förordning träder i kraft den 1 maj 2018.

1.47 Förslag till förordning om ändring i tullbrottsdataförordningen (2017:450)

Härigenom föreskrivs i fråga om tullbrottsdataförordningen (2017:450)

dels att 2–4, 7–9 och 18 §§ ska upphöra att gälla,

dels att rubriken efter 2 § och rubriken före 3 § ska utgå,

dels att nuvarande 5 § ska betecknas 2 § och att rubriken före nuvarande 5 § ska placeras före nya 2 §, att nuvarande 6 § ska betecknas 3 §, att nuvarande 10 § ska betecknas 4 § och att rubriken före nuvarande 8 § ska placeras före nya 4 §, att rubriken efter nuvarande 10 § ska placeras efter nya 4 §, att nuvarande 11 § ska betecknas 5 § och att rubriken före nuvarande 11 § ska placeras före nya 5 §, att nuvarande 12 § ska betecknas 6 § och att rubriken före nuvarande 12 § ska placeras före nya 6 §, att nuvarande 13 § ska betecknas 7 §, att nuvarande 14 § ska betecknas 8 §, att nuvarande 15 § ska betecknas 9 §, att nuvarande 16 § ska betecknas 10 §, att nuvarande 17 § ska betecknas 11 § och rubriken före nuvarande 17 § ska placeras före nya 11 §, att nuvarande 19 § ska betecknas 12 § och att rubriken före nuvarande 18 § ska placeras före nya 12 §,

dels att rubriken efter nya 4 § ska lyda Längsta tid för behandling m.m.,

dels att 1 §, nya 2–12 §§ och rubrikerna före 1 § och nya 4, 6 och 11 §§ ska ha följande lydelse,

dels att rubriken till förordningen ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

Tullbrottsdataförordning

Tullverkets brottsdataförordning

Inledande bestämmelser

Allmän bestämmelse

1 §

I denna förordning finns kompletterande föreskrifter om sådan behandling av personupp-

I denna förordning finns kompletterande föreskrifter till Tullverkets brottsdatalag

gifter som omfattas av tullbrottsdatalogen (2017:447). De uttryck som används i denna förordning har samma innebörd och tillämpningsområde som i lagen.

2 §

Vid sökning enligt 3 kap. 6 § *Tullbrottsdatalogen* (2017:447) får *uppgifter* som visar att den sökta personen tidigare har varit misstänkt för ett visst brott inte tas fram om en domstol, genom ett avgörande som har fått laga kraft, har ogillat åtalet, meddelat frikännande dom eller avskrivit målet sedan åtalet lagts *ned*.

Tullverket får meddela föreskrifter om begränsning av tillgången till sådana uppgifter som avses i 3 kap. 6 § första stycket tullbrottsdatalogen. Särskild hänsyn ska då tas till den enskildes rätt till skydd mot intrång i den personliga integriteten. Tillgången till personuppgifter om tidigare misstankar om brott ska särskilt begränsas.

Vid sökning enligt 3 kap. 5 § *Tullverkets brottsdatalog* (2017:447) får *uppgift* som visar att den sökta personen tidigare har varit misstänkt för ett visst brott inte tas fram om en domstol, genom ett avgörande som har fått laga kraft, har ogillat åtalet, meddelat frikännande dom eller avskrivit målet sedan åtalet lagts *ner*.

3 §

Tullverket ska löpande föra en förteckning över de tjänstemän vid myndigheten som utför uppgifter enligt 3 kap. 7 § andra stycket *tullbrottsdatalogen* (2017:447).

Tullverket ska löpande föra förteckning över de tjänstemän vid myndigheten som utför uppgifter enligt 3 kap. 6 § andra stycket *Tullverkets brottsdatalog* (2017:447).

*Elektroniskt utlämnande av Direktåtkomst
personuppgifter*

4 §

Tullverket får *meddela närmare föreskrifter om vad som krävs* i fråga om behörighet och säkerhet för att myndigheten ska *kunna* medge direktåtkomst till uppgifter för de myndigheter som anges i 3 kap. 8 § tullbrottsdatalagen (2017:447).

Direktåtkomst till uppgifterna får inte medges innan Tullverket har försäkrat sig om att den mottagande myndigheten uppfyller kraven på behörighet och säkerhet.

Tullverket får *ställa villkor* i fråga om behörighet och säkerhet för att myndigheten ska medge direktåtkomst enligt 3 kap. 7 § Tullverkets brottsdatalag (2017:447).

Direktåtkomst får inte medges innan Tullverket har försäkrat sig om att den mottagande myndigheten uppfyller kraven på behörighet och säkerhet.

5 §

När Tullverket arkiverar uppgifter och handlingar digitalt ska *de arkiverade* uppgifterna och handlingarna avskiljas från myndighetens brottsbekämpande verksamhet. Åtkomsten till arkiverade uppgifter och handlingar ska begränsas till särskilt angivna tjänstemän.

Tullverket får, efter att ha gett Riksarkivet tillfälle att yttra sig, meddela närmare föreskrifter om digital arkivering.

När Tullverket arkiverar uppgifter och handlingar digitalt ska uppgifterna och handlingarna avskiljas så att *de inte kan behandlas för något av de syften* som anges i 2 kap. 1 § Tullverkets brottsdatalag (2017:447). Åtkomsten till arkiverade uppgifter och handlingar ska begränsas till särskilt angivna tjänstemän.

Bevarande och gallring av Fortsatt behandling av vissa uppgifter personuppgifter

6 §

I 13–15 §§ föreskrivs att vissa kategorier av *uppgifter* i brottsanmälningar och avslutade förundersökningar får behandlas i *Tullverkets brottsbekämpande verksamhet efter utgången av* den tid som anges i 4 kap. 6 och 7 §§ *tullbrottsdatalagen* (2017:447). Detsamma gäller *uppgifter* i andra utredningar som handläggs enligt bestämmelser i 23 kap. rättegångsbalken.

När *uppgifter* behandlas enligt 13–15 §§ får, utöver vad som sägs i de bestämmelserna, följande uppgifter behandlas:

1. ärendenummer och liknande referensuppgifter,
2. brottskoder, och
3. uppgifter om omständigheterna kring brottet.

I 7–9 §§ föreskrivs att vissa kategorier av *personuppgifter* i brottsanmälningar och avslutade förundersökningar får behandlas *för ändamål som omfattas av tillämpningsområdet för Tullverkets brottsdatalag* (2017:447), trots att den tid som anges i 4 kap. 4 och 5 §§ *samma lag har löpt ut*. Detsamma gäller *personuppgifter* i andra utredningar som handläggs enligt bestämmelser i 23 kap. rättegångsbalken.

När *personuppgifter* behandlas enligt 7–9 §§ får, utöver vad som sägs i de bestämmelserna, följande uppgifter behandlas:

1. ärendenummer eller liknande referensuppgifter,

7 §

Uppgifter om *en dömd person* i en förundersökning som har lett till fällande dom får behandlas *efter utgången av* den tid som anges i 4 kap. 7 § första stycket *tullbrottsdatalagen* (2017:447), om behandlingen av särskilda skäl är nödvändig för att finna samband mellan olika brott eller mellan tänkbara gärningsmän.

Uppgifterna ska dock gallras

Uppgifter om *den dömd* i en förundersökning som har lett till fällande dom får behandlas *trots att* den tid som anges i 4 kap. 5 § första stycket *Tullverkets brottsdatalag* (2017:447) *har löpt ut*, om behandlingen av särskilda skäl är nödvändig för att finna samband mellan olika brott eller mellan tänkbara gärningsmän.

Behandlingen ska dock upp-

senast i samband med att uppgifterna om den dömda *gallras* ur belastningsregistret enligt lagen (1998:620) om belastningsregister.

höra senast i samband med att uppgifterna om den dömda *tas bort* ur belastningsregistret enligt lagen (1998:620) om belastningsregister.

8 §

Uppgifter om en person som har varit misstänkt i en förundersökning som har lagts *ned* eller avslutats på annat sätt än genom åtal får i ett enskilt fall behandlas *efter utgången av* den tid som anges i 4 kap. 7 § andra stycket *tullbrottsdatalagen* (2017:447), *om behandlingen är nödvändig för att personen ska kunna lagföras.*

Uppgifterna ska dock gallras senast då åtal inte längre får väckas för brottet *eller senast sjuttio år från den dag då brottet begicks i fall som avses i 35 kap. 2 § första stycket brottsbalken.*

Uppgifter om en person som har varit misstänkt i en förundersökning som har lagts *ner* eller avslutats på annat sätt än genom åtal får i ett enskilt fall behandlas *om det är nödvändigt för att personen ska kunna lagföras trots att* den tid som anges i 4 kap. 5 § andra stycket *Tullverkets brottsdatalag* (2017:447) *har löpt ut.*

Behandlingen ska dock upphöra senast då åtal inte längre får väckas för brottet.

9 §

Uppgifter om personer som har dömts för, eller har varit misstänkta för, brott där det finns en betydande risk för återfall i samma eller likartad brottslighet, får behandlas *efter utgången av* den tid som anges i 4 kap. 6 och 7 §§ *tullbrottsdatalagen* (2017:447), om behandlingen av särskilda skäl är nödvändig för att förebygga, förhindra eller upptäcka brott för vilket det är föreskrivet fängelse

Uppgifter om personer som har dömts för, eller har varit misstänkta för, brott där det finns en betydande risk för återfall i samma eller likartad brottslighet, får behandlas *trots att* den tid som anges i 4 kap. 4 och 5 §§ *Tullverkets brottsdatalag* (2017:447) *har löpt ut*, om behandlingen av särskilda skäl är nödvändig för att förebygga, förhindra eller upptäcka brott för vilket det är föreskrivet

i fyra år eller däröver.

Uppgifterna ska dock gallras, i fråga om brott som har lett till fällande dom, senast i samband med att uppgifterna gallras ur belastningsregistret enligt lagen (1998:620) om belastningsregister och i övriga fall senast femton år efter det att förundersökningen lades ner eller avslutades på annat sätt.

fängelse i fyra år eller däröver.

Behandlingen ska dock upphöra, i fråga om brott som har lett till fällande dom, senast i samband med att uppgifterna tas bort ur belastningsregistret enligt lagen (1998:620) om belastningsregister och i övriga fall senast femton år efter det att förundersökningen lades ner eller avslutades på annat sätt.

10 §

Personuppgifter som behövs för handläggning av ärenden i det internationella samarbetet ska, om behandlingen av särskilda skäl är nödvändig efter utgången av den tid som anges i 4 kap. 10 § andra stycket tullbrottsdatalagen (2017:447) för att fullgöra internationella åtaganden, gallras senast tre år efter utgången av det kalenderår då ärendet som uppgifterna behandlades i avslutades.

Personuppgifter som behövs för handläggning av ärenden i det internationella samarbetet får behandlas trots att den tid som anges i 4 kap. 11 § Tullverkets brottsdatalag (2017:447) har löpt ut, om behandling av särskilda skäl är nödvändig för att fullgöra internationella åtaganden.

Behandlingen ska dock upphöra senast tre år efter utgången av det kalenderår då ärendet som uppgifterna behandlades i avslutades.

Undantag från gallring

Behandling för arkivändamål av allmänt intresse m.m.

11 §

Riksarkivet får, efter att ha gett Tullverket tillfälle att yttra sig, meddela föreskrifter om att

Riksarkivet får, efter att ha gett Tullverket tillfälle att yttra sig, meddela föreskrifter om att

uppgifter som ska gallras enligt 4 kap. 3 § första stycket och 4 kap. 9 och 10 §§ tullbrottsdatalogen (2017:447) samt 16 § denna förordning får bevaras för historiska, statistiska eller vetenskapliga ändamål.

personuppgifter som avses i 4 kap. 2 § första stycket och 8–11 §§ Tullverkets brottsdatalog (2017:447) och 10 § denna förordning får behandlas under längre tid för arkivändamål av allmänt intresse och vetenskapliga, statistiska eller historiska ändamål.

12 §

Innan Tullverket meddelar föreskrifter med stöd av denna förordning, ska myndigheten ge Datainspektionen *tillfälle att yttra sig* i frågor som berör särskilda risker för intrång i den personliga integriteten.

Innan Tullverket meddelar föreskrifter med stöd av denna förordning, ska myndigheten *samråda med* Datainspektionen i frågor som berör särskilda risker för intrång i den personliga integriteten.

Denna förordning träder i kraft den 1 maj 2018.

1.48 Förslag till förordning om ändring i skattebrottsdataförordningen (2017:458)

Härigenom föreskrivs i fråga om skattebrottsdataförordningen (2017:458)

dels att 2–4, 7, 9, 10 och 17 §§ ska upphöra att gälla,

dels att rubriken efter 2 § och rubrikerna före 3 och 9 §§ ska utgå,

dels att nuvarande 5 § ska betecknas 2 § och att rubriken före nuvarande 5 § ska placeras före nya 2 §, att nuvarande 6 § ska betecknas 3 §, att nuvarande 8 § ska betecknas 4 § och rubriken före nuvarande 8 § ska placeras före nya 4 §, att nuvarande 11 § ska betecknas 5 § och att rubriken efter nuvarande 11 § ska placeras efter nya 5 §, att nuvarande 12 § ska betecknas 6 § och rubriken före nuvarande 12 § ska placeras före nya 6 §, att nuvarande 13 § ska betecknas 7 § och rubriken före nuvarande 13 § ska placeras före nya 7 §, att nuvarande 14 § ska betecknas 8 §, att nuvarande 15 § ska betecknas 9 §, att nuvarande 16 § ska betecknas 10 § och att rubriken före nuvarande 16 § ska placeras före nya 10 §, att nuvarande 18 § ska betecknas 11 § och rubriken före nuvarande 17 § ska placeras före nya 11 §,

dels att rubriken efter nya 5 § ska lyda Längsta tid för behandling m.m.,

dels att 1 § och nya 2–11 och rubrikerna före 1 § och nya 4, 7 och 10 §§ ska ha följande lydelse,

dels att rubriken till förordningen ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

Skattebrottsdataförordning

Skatteverkets brottsdataförordning

Inledande bestämmelser

Allmän bestämmelse

1 §

I denna förordning finns kompletterande bestämmelser om sådan behandling av person-

I denna förordning finns kompletterande bestämmelser till Skatteverkets brottsdatalog

uppgifter som omfattas av skattebrottsdatalagen (2017:452). De uttryck som används i denna förordning har samma innebörd och tillämpningsområde som i lagen.

2 §

Vid sökning enligt 3 kap. 6 § *skattebrottsdatalagen* (2017:452) får uppgifter som visar att den sökta personen tidigare har varit misstänkt för ett visst brott inte tas fram om en domstol, genom ett avgörande som har fått laga kraft, har ogillat åtalet, meddelat frikännande dom eller avskrivit målet sedan åtalet lagts *ned*.

Skatteverket får meddela föreskrifter om begränsning av tillgången till sådana uppgifter som avses i 3 kap. 6 § första stycket skattebrottsdatalagen. Särskild hänsyn ska då tas till den enskildes rätt till skydd mot intrång i den personliga integriteten. Tillgången till personuppgifter om tidigare misstankar om brott ska särskilt begränsas.

3 §

Skatteverket ska löpande föra en förteckning över de tjänstemän vid myndigheten som utför uppgifter enligt 3 kap. 7 § andra stycket *skattebrottsdatalagen* (2017:452).

Vid sökning enligt 3 kap. 4 § *Skatteverkets brottsdatalag* (2017:452) får uppgifter som visar att den sökta personen tidigare har varit misstänkt för ett visst brott inte tas fram om en domstol, genom ett avgörande som har fått laga kraft, har ogillat åtalet, meddelat frikännande dom eller avskrivit målet sedan åtalet lagts *ner*.

Skatteverket ska löpande föra förteckning över de tjänstemän vid myndigheten som utför uppgifter enligt 3 kap. 5 § andra stycket *Skatteverkets brottsdatalag* (2017:452).

Utlämnande av *uppgifter*

Om en uppgift i en förundersökning kan antas ha betydelse för en konkursutredning, *får uppgiften lämnas till* konkursförvaltaren.

Skatteverket får *meddela närmare föreskrifter om vad som krävs* i fråga om behörighet och säkerhet för att myndigheten ska *kunna* medge direktåtkomst till uppgifter för de myndigheter som anges i 3 kap. 8 § *skattebrottsdatalagen* (2017:452).

Direktåtkomst till uppgifterna får inte medges innan Skatteverket har försäkrat sig om att den mottagande myndigheten uppfyller kraven på behörighet och säkerhet.

När Skatteverket arkiverar uppgifter och handlingar digitalt ska *de arkiverade* uppgifterna och handlingarna avskiljas från myndighetens brottsbekämpande verksamhet. Åtkomsten till arkiverade uppgifter och handlingar ska begränsas till särskilt angivna tjänstemän.

Skatteverket får, efter att ha gett Riksarkivet tillfälle att yttra sig, meddela närmare föreskrifter om digital arkivering.

Utlämnande av *personuppgifter*

4 §

Om en uppgift i en förundersökning kan antas ha betydelse för en konkursutredning, *har* konkursförvaltaren rätt att ta del av uppgiften.

5 §

Skatteverket får *ställa villkor* i fråga om behörighet och säkerhet för att myndigheten ska medge direktåtkomst enligt 3 kap. 6 § *Skatteverkets brottsdatalag* (2017:452).

Direktåtkomst får inte medges innan Skatteverket har försäkrat sig om att den mottagande myndigheten uppfyller kraven på behörighet och säkerhet.

6 §

När Skatteverket arkiverar uppgifter och handlingar digitalt ska uppgifterna och handlingarna avskiljas så att *de inte kan behandlas för något av de syften som anges i 2 kap. 1 § Skatteverkets brottsdatalag* (2017:452). Åtkomsten till arkiverade uppgifter och handlingar ska begränsas till särskilt angivna tjänstemän.

*Bevarande och gallring av uppgifter**Fortsatt behandling av vissa personuppgifter*

7 §

I 14 och 15 §§ föreskrivs att vissa kategorier av *uppgifter* i avslutade förundersökningar får behandlas i *Skatteverkets brottsbekämpande verksamhet efter utgången av* den tid som anges i 4 kap. 6 § *skattebrottsdatalagen* (2017:452). Detsamma gäller *uppgifter* i andra utredningar som handläggs enligt bestämmelser i 23 kap. rättegångsbalken.

När *uppgifter* behandlas enligt 14 och 15 §§ får, utöver vad som sägs i de bestämmelserna, följande uppgifter behandlas:

1. ärendenummer och liknande referensuppgifter,
2. brottskoder, och
3. uppgifter om omständigheterna kring brottet.

7 §

I 8 och 9 §§ föreskrivs att vissa kategorier av *personuppgifter* i avslutade förundersökningar får behandlas för *ändamål som omfattas av tillämpningsområdet för Skatteverkets brottsdatalag* (2017:452), trots att den tid som anges i 4 kap. 4 § *samma lag har löpt ut*. Detsamma gäller *personuppgifter* i andra utredningar som handläggs enligt bestämmelser i 23 kap. rättegångsbalken.

När *personuppgifter* behandlas enligt 8 och 9 §§ får, utöver vad som sägs i de bestämmelserna, följande uppgifter behandlas:

1. ärendenummer eller liknande referensuppgifter,

8 §

Uppgifter om *en dömd person* i en förundersökning som har lett till fällande dom får behandlas *efter utgången av* den tid som anges i 4 kap. 6 § första stycket *skattebrottsdatalagen* (2017:452), om behandlingen av särskilda skäl är nödvändig för att finna samband mellan olika brott eller mellan tänkbara gärningsmän.

Uppgifter om *den dömd* i en förundersökning som har lett till fällande dom får behandlas trots att den tid som anges i 4 kap. 4 § första stycket *Skatteverkets brottsdatalag* (2017:452) *har löpt ut*, om behandlingen av särskilda skäl är nödvändig för att finna samband mellan olika brott eller mellan tänkbara gärningsmän.

Uppgifterna ska dock gallras senast i samband med att uppgifterna om den dömda gallras ur belastningsregistret enligt lagen (1998:620) om belastningsregister.

Behandlingen ska dock upphöra senast i samband med att uppgifterna om den dömda tas bort ur belastningsregistret enligt lagen (1998:620) om belastningsregister.

9 §

Uppgifter om en person som har varit misstänkt i en förundersökning som har lagts *ned* eller avslutats på annat sätt än genom åtal får i ett enskilt fall behandlas *efter utgången av* den tid som anges i 4 kap. 6 § andra stycket *skattebrottsdatalagen* (2017:452), *om behandlingen är nödvändig för att personen ska kunna lagföras.*

Uppgifter om en person som har varit misstänkt i en förundersökning som har lagts *ner* eller avslutats på annat sätt än genom åtal får i ett enskilt fall behandlas *om det är nödvändigt för att kunna lagföra personen trots att* den tid som anges i 4 kap. 4 § andra stycket *Skatteverkets brottsdatalag* (2017:452) *har löpt ut.*

Uppgifterna ska dock gallras senast då åtal inte längre får väckas för brottet eller senast sjuttio år från den dag då brottet begicks i fall som avses i 35 kap. 2 § första stycket brottsbalken.

Behandlingen ska dock upphöra senast då åtal inte längre får väckas för brottet.

*Undantag från gallring**Behandling för arkivändamål av allmänt intresse m.m.*

10 §

Riksarkivet får, efter att ha gett Skatteverket tillfälle att yttra sig, meddela föreskrifter om att *uppgifter som ska gallras enligt* 4 kap. 3 § första stycket eller 4 kap. 8 § *skattebrottsdatalagen* (2017:452), *får bevaras för historiska, statistiska eller vetenskapliga ändamål.*

Riksarkivet får, efter att ha gett Skatteverket tillfälle att yttra sig, meddela föreskrifter om att *personuppgifter som anges i* 4 kap. 2 § första stycket eller 4 kap. 6–8 §§ *Skatteverkets brottsdatalag* (2017:452), *får behandlas under längre tid för arkivändamål av allmänt intresse*

och *vetenskapliga*, statistiska
eller *historiska* ändamål.

11 §

Innan Skatteverket meddelar föreskrifter med stöd av denna förordning, ska myndigheten ge Datainspektionen *tillfälle att yttra sig* i frågor som berör särskilda risker för intrång i den personliga integriteten.

Innan Skatteverket meddelar föreskrifter med stöd av denna förordning, ska myndigheten *samråda med* Datainspektionen i frågor som berör särskilda risker för intrång i den personliga integriteten.

Denna förordning träder i kraft den 1 maj 2018.

1.49 Förslag till förordning om ändring i förordningen (2017:504) om internationellt polisiärt samarbete

Härigenom föreskrivs att 5 kap. 3, 11, 12 och 14 §§, 6 kap. 6, 7 och 9 §§, 7 kap. 10 och 11 §§ och 8 kap. 2, 4 och 8–10 §§ och rubrikerna före 5 kap. 11 §, 6 kap. 6 §, 7 kap. 10 § och 8 kap. 8 § förordningen (2017:504) om internationellt polisiärt samarbete ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

5 kap.

3 §

Det svenska kontaktstället ska bistå den egna myndigheten och de myndigheter som anges i andra stycket med att söka uppgifter i utländska dna-register, fingeravtrycksregister och fordonsregister enligt de förutsättningar som anges i 7 kap. 2 § första stycket samt 7 kap. 4 eller 6 § lagen (2017:496) om internationellt polisiärt samarbete.

Myndigheter som får begära sökningar är

- | | |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>1. de som anges i bestämmelsen om direktåtkomst i 4 kap. 10 § <i>polisdatalagen</i> (2010:361) när det gäller dna-register,</p> <p>2. de som anges i bestämmelsen om direktåtkomst i 4 kap. 17 § <i>polisdatalagen</i> när det gäller fingeravtrycksregister, och</p> <p>3. Säkerhetspolisen, Åklagarmyndigheten, Ekobrottsmyndigheten och Tullverket när det gäller fordonsregister.</p> | <p>1. de som anges i bestämmelsen om direktåtkomst i 5 kap. 10 § <i>polisens brottsdatalag</i> (2010:361) när det gäller dna-register,</p> <p>2. de som anges i bestämmelsen om direktåtkomst i 5 kap. 17 § <i>polisens brottsdatalag</i> när det gäller fingeravtrycksregister, och</p> |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Polismyndigheten är svenskt kontaktställe vid utbyte av dna-profiler, fingeravtryck och fordonsuppgifter enligt Prümrådsbeslutet.

Gallring, spärrning och särskild upplysning

Längsta tid för behandling, spärrning och särskild upplysning

11 §

Personuppgifter som har översänts från en annan stat enligt Prömrådsbeslutet ska *gallras* om uppgifterna är felaktiga eller inte borde ha översänts eller tagits emot. Felaktiga uppgifter får i stället rättas.

Personuppgifter enligt första stycket som har översänts och tagits emot korrekt ska *gallras* när syftet med översändandet har uppnåtts eller inte längre kan uppnås. Uppgifter som har översänts från en annan stat i samband med ett större evenemang med gränsöverskridande verkningar ska *gallras* senast ett år från det att uppgifterna togs emot.

Personuppgifter som har översänts från en annan stat enligt Prömrådsbeslutet ska *raderas* om uppgifterna är felaktiga eller inte borde ha översänts eller tagits emot. Felaktiga uppgifter får i stället rättas.

Behandlingen av personuppgifter enligt första stycket som har översänts och tagits emot korrekt ska *upphöra* när syftet med översändandet har uppnåtts eller inte längre kan uppnås. *Behandlingen av* uppgifter som har översänts från en annan stat i samband med ett större evenemang med gränsöverskridande verkningar ska *upphöra* senast ett år från det att uppgifterna togs emot.

12 §

I stället för att *gallra* personuppgifter enligt 11 § ska *uppgifterna spärras*, om det finns skäl att anta att *gallring* skulle innebära skada för den person som uppgifterna rör. Att uppgifterna är spärrade innebär att de endast får behandlas för att tillgodose det syfte som förhindrade *gallring*.

I stället för att *radera eller upphöra med behandlingen av* personuppgifter enligt 11 § ska, om det finns skäl att anta att *en sådan åtgärd* skulle innebära skada för den person som uppgifterna rör, *uppgifterna spärras*. Att uppgifterna är spärrade innebär att de endast får behandlas för att tillgodose det syfte som *förhindrade att uppgifterna raderades eller att behandlingen av dem upphörde*.

14 §

Uppgifter som har registrerats enligt 9 eller 10 § ska *gallras* två år efter registreringen.

Behandlingen av uppgifter som har registrerats enligt 9 eller 10 § ska *upphöra* två år efter registreringen.

6 kap.

Gallring, spärrning och särskild upplysning

Längsta tid för behandling, spärrning och särskild upplysning

6 §

Personuppgifter som har översänts från en annan stat enligt CBE-direktivet ska *gallras* om uppgifterna är felaktiga eller inte borde ha översänts eller tagits emot. Felaktiga uppgifter får i stället rättas.

Personuppgifter som har översänts från en annan stat enligt CBE-direktivet ska *raderas* om uppgifterna är felaktiga eller inte borde ha översänts eller tagits emot. Felaktiga uppgifter får i stället rättas.

Personuppgifter enligt första stycket som har översänts och tagits emot korrekt ska *gallras* när syftet med översändandet har uppnåtts eller inte längre kan uppnås.

Behandlingen av personuppgifter enligt första stycket som har översänts och tagits emot korrekt ska *upphöra* när syftet med översändandet har uppnåtts eller inte längre kan uppnås.

7 §

I stället för att *gallra* personuppgifter enligt 6 § ska *uppgifterna spärras*, om det finns skäl att anta att *gallring* skulle innebära skada för den person som uppgifterna rör. Att uppgifterna är spärrade innebär att de endast får behandlas för att tillgodose det syfte som förhindrade *gallring*.

I stället för att *radera eller upphöra med behandlingen av* personuppgifter enligt 6 § ska, om det finns skäl att anta att *en sådan åtgärd* skulle innebära skada för den person som uppgifterna rör, *uppgifterna spärras*. Att uppgifterna är spärrade innebär att de endast får behandlas för att tillgodose det syfte som förhindrade att *uppgifterna raderas eller att behandlingen av dem upphörde*.

9 §

Uppgifter som har registrerats enligt 5 § ska *gallras* två år efter registreringen.

Behandlingen av uppgifter som har registrerats enligt 5 § ska *upphöra* två år efter registreringen

7 kap.

*Gallring**Längsta tid för behandling*

10 §

Uppgifter som har hämtats från VIS och som har lagts in i systemet av en annan stat ska *gallras* när uppgifterna inte längre behövs för något av de ändamål som anges i 9 kap. 3 § lagen (2017:496) om internationellt polisiärt samarbete.

Behandlingen av uppgifter som har hämtats från VIS och som har lagts in i systemet av en annan stat ska *upphöra* när uppgifterna inte längre behövs för något av de ändamål som anges i 9 kap. 3 § lagen (2017:496) om internationellt polisiärt samarbete.

11 §

Uppgifter som har registrerats enligt 5 eller 9 § ska *gallras* ett år efter registreringen.

Behandlingen av uppgifter som har registrerats enligt 5 eller 9 § ska *upphöra* ett år efter registreringen.

8 kap.

2 §

Om ett amerikanskt kontaktställe efter en sökning enligt 10 kap. 1 § lagen (2017:496) om internationellt polisiärt samarbete ansöker hos det svenska kontaktstället om att få ut övriga tillgängliga personuppgifter och ytterligare information med anknytning till fingeravtrycket, får det svenska kontaktstället lämna ut uppgifter till det

Om ett amerikanskt kontaktställe efter en sökning enligt 10 kap. 1 § lagen (2017:496) om internationellt polisiärt samarbete ansöker hos det svenska kontaktstället om att få ut övriga tillgängliga personuppgifter och ytterligare information med anknytning till fingeravtrycket, får det svenska kontaktstället lämna ut uppgifter till det

amerikanska kontaktstället endast om det finns förutsättningar enligt 2 kap. 15 § första stycket *polisdatalagen* (2010:361) och 33–35 §§ *personuppgiftslagen* (1998:204).

amerikanska kontaktstället endast om det finns förutsättningar enligt 2 kap. 10 § första stycket och 8 kap. 1 § *brottsdatalagen* (2018:000).

4 §

Polismyndigheten, Säkerhetspolisen, Ekobrottsmyndigheten i den polisverksamhet som bedrivs vid myndigheten, Tullverket och Kustbevakningen får i enskilda fall, utan särskild begäran, lämna ut personuppgifter till ett amerikanskt kontaktställe enligt avtalet med USA, om särskilda omständigheter ger anledning att anta att den person som uppgifterna rör kommer att begå eller har begått brott för vilket det enligt svensk lag är föreskrivet fängelse i mer än ett år. Om det bedöms vara nödvändigt för att förebygga, förhindra eller upptäcka sådan brottslig verksamhet eller utreda ett sådant brott, får även andra uppgifter än personuppgifter lämnas ut.

Uppgifter enligt första stycket får endast lämnas ut om det finns förutsättningar enligt 2 kap. 15 § första stycket *polisdatalagen* (2010:361) och 33–35 §§ *personuppgiftslagen* (1998:204).

Uppgifter enligt första stycket får endast lämnas ut om det finns förutsättningar enligt 2 kap. 10 § första stycket *polisens brottsdatalag* (2010:361) och 8 kap. 1 § *brottsdatalagen* (2018:000).

Det svenska kontaktstället ska översända uppgifterna till ett amerikanskt kontaktställe.

Gallring och spärrning

Längsta tid för behandling och spärrning

8 §

Personuppgifter som har översänts från ett amerikanskt kontaktställe enligt avtalet med USA ska *gallras* om uppgifterna är felaktiga eller inte borde ha översänts eller tagits emot. Felaktiga uppgifter får i stället rättas.

Personuppgifter som har översänts från ett amerikanskt kontaktställe enligt avtalet med USA ska *raderas* om uppgifterna är felaktiga eller inte borde ha översänts eller tagits emot. Felaktiga uppgifter får i stället rättas.

I stället för att *gallra* personuppgifter enligt första stycket ska uppgifterna spärras, om det finns skäl att anta att *gallring* skulle innebära skada för den person som uppgifterna rör. Att uppgifterna är spärrade innebär att de endast får behandlas för att tillgodose det syfte som förhindrade *gallring*.

I stället för att *radera* personuppgifter enligt första stycket ska uppgifterna spärras, om det finns skäl att anta att *radering* skulle innebära skada för den person som uppgifterna rör. Att uppgifterna är spärrade innebär att de endast får behandlas för att tillgodose det syfte som förhindrade *radering*.

9 §

Personuppgifter som har översänts och tagits emot korrekt ska *gallras* när syftet med översändandet eller vidarebehandlingen har uppnåtts eller inte längre kan uppnås.

Behandlingen av personuppgifter som har översänts och tagits emot korrekt ska *upphöra* när syftet med översändandet eller vidarebehandlingen har uppnåtts eller inte längre kan uppnås.

10 §

Uppgifter som har registrerats enligt 7 § ska *gallras* två år efter registreringen.

Behandlingen av uppgifter som har registrerats enligt 7 § ska *upphöra* två år efter registreringen.

Denna förordning träder i kraft den 1 maj 2018.

1.50 Förslag till förordning om ändring i brottsdataförordningen (2018:000)

Härigenom föreskrivs att det i brottsdataförordningen (2018:000) ska införas tre nya paragrafer, 3 kap. 4 a, 4 b och 4 c §§, och en ny rubrik före 3 kap. 4 a § med följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

3 kap.

Tillgången till personuppgifter

4 a §

För tilldelning av behörighet för åtkomst till personuppgifter ska, utöver behovet av uppgifterna, utbildning och erfarenhet särskilt beaktas.

4 b §

I en behörig myndighet ska det finnas rutiner för tilldelning av, förändring, borttagning och regelbunden uppföljning av behörigheter för åtkomst till personuppgifter.

4 c §

Tillgången till uppgifter om tidigare brottsmisstankar ska särskilt begränsas.

Denna förordning träder i kraft den 1 maj 2018.

2 Utredningens uppdrag och arbete

2.1 Utredningsuppdraget

Utredningsuppdraget består i att föreslå hur man i svensk rätt ska genomföra Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF. Direktiven för utredningsarbetet finns i *bilaga 1*.

I utredningens uppdrag ingår bl.a. att

- lämna förslag till en ny ramlagstiftning med bestämmelser om skydd av personuppgifter inom direktivets tillämpningsområde,
- analysera och bedöma behovet av författningsändringar i vissa centrala författningar om rättsväsendets behandling av personuppgifter,
- lämna de förslag till ändringar som krävs för att anpassa dessa författningar till de nya förutsättningarna för regleringen,
- bedöma om direktivet ger anledning till ny eller ändrad reglering om tillsyn och vid behov lämna författningsförslag, och
- bedöma om det finns anledning att reglera Säkerhetspolisens personuppgiftsbehandling separat från den lagstiftning som gäller för Polismyndigheten och vid behov lämna författningsförslag.

Utredningen har även åtagit sig att göra de anpassningar som kan krävas i lagen (2014:400) om Polismyndighetens elimineringsdatabas, lagen (2015:51) om register över tillträdesförbud vid idrottsarrangemang och lagen (2017:496) om internationellt polisiärt samarbete, alla med tillhörande förordningar.

2.2 Genomförandet av uppdraget

Förslag till ny ramlagstiftning och tillsyn inom direktivets tillämpningsområde redovisades den 5 april 2017 i delbetänkandet Brottsdatalog (SOU 2017:29).

Utredningens arbete påbörjades i slutet av april 2016 och har bedrivits på sedvanligt sätt med regelbundna sammanträden med gruppen av sakkunniga och experter. Utredningen har sammanträtt vid sammanlagt fem tillfällen för att ta fram detta betänkande.

Utredaren och sekretariatet har i denna del av utredningsuppdraget samrått med andra utredningar enligt följande.

Utredaren och huvudsekreteraren samrådde med Utredningen om stärkt integritet i Rättsmedicinalverkets verksamhet (Ju 2016:18) den 11 oktober 2016 och den 30 juni 2017.

Utredaren och huvudsekreteraren samrådde den 8 februari och den 19 maj 2017 med Eva Lönkvist som fått i uppdrag att biträda Justitiedepartementet med att anpassa viss lagstiftning på området för allmän ordning och säkerhet till EU:s dataskyddsreform.

Utredaren och huvudsekreteraren samrådde med Socialdataskyddsutredningen (S 2016:05) den 7 november 2016.

Den 7 november och 21 december 2016 och den 23 augusti 2017 samrådde utredaren och delar av sekretariatet med Peder Liljeqvist som fått i uppdrag att biträda Justitiedepartementet med att anpassa domstolsdatalagen, kriminalvårdens registerlagstiftning och utlänningsdatalagen till dataskyddsförordningen.

Utredaren och delar av sekretariatet har haft möte med företrädare för

- Kriminalvården den 14 oktober 2016 och 25 april 2017,
- Kustbevakningen den 8 februari 2017,
- Säkerhetspolisen den 15 februari och 16 maj 2017,
- Socialstyrelsen den 12 april 2017,

- Domstolsverket den 19 april 2017,
- Ekobrottsmyndigheten den 15 november 2016 och 7 juni 2017,
och
- Polismyndigheten den 25 april och 7 juni 2017.

3 Brottsdatalagens innehåll

3.1 Ny reglering av dataskyddet

3.1.1 Dataskyddsreformen

Europeiska unionens (EU) nya dataskyddsreglering består av två rättsliga instrument. Det ena är Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (EUT L 119, 4.5.2016, s. 1, i fortsättningen dataskyddsförordningen). Det andra är Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF (EUT L 119, 4.5.2016, s. 89, i fortsättningen direktivet). Reformen innebär att reglerna om personuppgiftsbehandling i framtiden finns dels i dataskyddsförordningen, som är direkt tillämplig i svensk rätt, och den lagstiftning som kompletterar förordningen, dels i de författningar som genomför direktivet.

Dataskyddsförordningen gäller inte när direktivet är tillämpligt. Hur direktivet genomförs får därigenom avgörande betydelse för vilket regelverk som är tillämpligt.

Dataskyddsutredningen, som haft i uppdrag att utreda bl.a. behovet av kompletterande lagstiftning till dataskyddsförordningen och vissa generella frågor med anknytning till dataskyddsreformen, har avgett betänkandet Ny dataskyddslag (SOU 2017:39). I betänkandet föreslås bl.a. att personuppgiftslagen (1998:204) ska upphöra att gälla den 25 maj 2018, då förordningen börjar gälla.

3.1.2 Genomförandet av dataskyddsdirektivet

I delbetänkandet Brottsdatalag beskrivs dataskyddsreformen närmare (se SOU 2017:29 s. 119 f.). Utredningen lämnar där förslag till en ny ramlag, brottsdatalagen, och en ny förordning till den, brottsdataförordningen. Lagen och förordningen, som tillsammans genomför dataskyddsdirektivet, ska gälla generellt inom direktivets tillämpningsområde. Direktivet ska vara genomfört senast den 6 maj 2018.

Brottsdatalagen drar upp gränsen mellan å ena sidan den särskilda regleringen av behandling av personuppgifter vid brottsbekämpning, lagföring, straffverkställighet och upprätthållande av allmän ordning och säkerhet och å andra sidan dataskyddsförordningens tillämpningsområde. Lagen är kapitelindeldad. I 1 kap. finns allmänna bestämmelser om lagens tillämpningsområde och där definieras också de uttryck som används i lagen. I 2 kap. regleras behandlingen av personuppgifter och i 3 kap. de personuppgiftsansvarigas skyldigheter. Enskildas rättigheter regleras i 4 kap. Tillsynen över personuppgiftsbehandling behandlas i 5 kap. och administrativa sanktionsavgifter i 6 kap. I 7 kap. behandlas skadestånd och rättsmedel och i 8 kap. överföring av personuppgifter till tredjeland och internationella organisationer.

Brottsdatalagen anger ramen för vilken personuppgiftsbehandling som är tillåten för de syften som anges i lagen och vilka som ska tillämpa lagen, vilket är de som är behöriga myndigheter enligt lagen. Där regleras frågor som är gemensamma för alla behöriga myndigheter. Brottsdatalagen kommer därigenom att för sitt tillämpningsområde fylla i stort sett samma funktion som personuppgiftslagen gör i dag. På samma sätt som nu kommer det dessutom att finnas särskilda registerförfattningar för flertalet av de myndigheter som kommer att tillämpa brottsdatalagen. De kommer dock inte att vara lika omfattande som i dag, eftersom de i vissa delar ersätts av den nya generella regleringen. I registerförfattningarna kommer bara de regler som är specifika för just den myndigheten att finnas. Det kommer vidare även fortsättningsvis att finnas särskilda författningar som reglerar enskilda register inom brottsdatalagens tillämpningsområde.

3.2 Innehållet i brottsdatalagen

3.2.1 Regler om behandlingen av personuppgifter

Lagens tillämpningsområde

Brottsdatalagen gäller för behandling av personuppgifter som utförs av en behörig myndighet i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller verkställa straffrättsliga påföljder. Den gäller också för behandling av personuppgifter som en behörig myndighet utför i syfte att upprätthålla allmän ordning och säkerhet. Med behörig myndighet avses en myndighet som har till arbetsuppgift att bedriva sådan verksamhet eller en annan aktör som utövar myndighet för något av dessa syften. Vilka myndigheter som är behöriga räknas inte upp, men lagen kommer framför allt att tillämpas av Polismyndigheten, Tullverket, Kustbevakningen, Skatteverket, Ekobrottsmyndigheten, Åklagarmyndigheten, domstolarna och Kriminalvården.

En behörig myndighet ska dock bara tillämpa brottsdatalagen vid behandling av personuppgifter för brottsbekämpning, lagföring, straffverkställighet eller upprätthållande av allmän ordning och säkerhet. Syftet med behandlingen av personuppgifter i det enskilda fallet blir därmed av avgörande betydelse för när lagen ska tillämpas, inte verksamheten som sådan. Om en behörig myndighet även har andra arbetsuppgifter, ska lagen inte tillämpas vid den personuppgiftsbehandling som utförs för de syftena.

Även andra än myndigheter som har fått till uppgift att utöva myndighet inom lagens tillämpningsområde är behöriga myndigheter i lagens mening.

Lagen gäller enbart för sådan behandling av personuppgifter som är helt eller delvis automatiserad och för annan behandling som ingår i eller är avsedd att ingå i en strukturerad samling av personuppgifter som är tillgänglig för sökning eller sammanställning enligt särskilda kriterier.

Lagen gäller inte vid Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet eller om Polismyndigheten har övertagit en arbetsuppgift som rör nationell säkerhet från Säkerhetspolisen.

Brottsdatalagen är subsidiär till annan lagstiftning. Det innebär att det kan finnas avvikande bestämmelser i registerförfattningarna

för de behöriga myndigheterna. En behörig myndighet som saknar registerförfattning ska tillämpa brottsdatalogen för sådan personuppgiftsbehandling som ligger inom lagens tillämpningsområde.

Rättslig grund för behandlingen av personuppgifter

All behandling av personuppgifter ska ha en rättslig grund. I brottsdatalogen finns det två bestämmelser om rättslig grund. Enligt 2 kap. 1 § får personuppgifter behandlas om det är nödvändigt för att en behörig myndighet ska kunna utföra en arbetsuppgift i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa en straffrättslig påföljd eller upprätthålla allmän ordning och säkerhet. Arbetsuppgiften ska framgå av en bindande unionsrättsakt eller av en lag, en förordning eller ett särskilt beslut av regeringen. Enligt 2 kap. 2 § får personuppgifter även behandlas om det är nödvändigt för diarieföring eller om uppgifterna har lämnats till en behörig myndighet i en anmälan, ansökan eller liknande och behandlingen är nödvändig för myndighetens handläggning.

Ändamål för behandlingen av personuppgifter

Personuppgifter får enligt 2 kap. 3 § bara behandlas för särskilda, uttryckligt angivna och berättigade ändamål. Om det inte framgår av sammanhanget eller på annat sätt för vilket ändamål personuppgifterna behandlas, ska det tydliggöras genom en särskild upplysning. Det som åsyftas är ändamålet i det enskilda fallet, t.ex. att personuppgifterna behandlas i en viss förundersökning eller för handläggningen av ett visst brottmål.

Innan personuppgifter får behandlas för ett nytt ändamål som ligger inom brottsdatalogens tillämpningsområde ska det enligt 2 kap. 4 § säkerställas att det finns en rättslig grund för den nya behandlingen och att behandlingen är nödvändig och proportionerlig för det nya ändamålet.

De behöriga myndigheterna får även enligt 2 kap. 5 § behandla personuppgifter för vetenskapliga, statistiska eller historiska ändamål inom lagens tillämpningsområde.

Krav på behandlingen av personuppgifter

Personuppgifter ska enligt 2 kap. 6 § behandlas författningsenligt och på ett korrekt sätt och enligt 2 kap. 8 § vara adekvata och relevanta i förhållande till ändamålen med behandlingen. Fler personuppgifter får inte behandlas än vad som är nödvändigt med hänsyn till ändamålen med behandlingen. Personuppgifterna ska dessutom enligt 2 kap. 7 § vara korrekta och, om det är nödvändigt, uppdaterade. Uppgifter som beskriver en persons utseende ska utformas på ett objektivt sätt med respekt för människovärdet.

Vidare ska det så långt möjligt göras åtskillnad mellan olika typer av personuppgifter. Kategorier av registrerade ska enligt 2 kap. 9 § kunna skiljas från varandra, t.ex. misstänkta och brottsoffer. Om det inte framgår av sammanhanget eller på annat sätt, ska det tydliggöras genom en särskild upplysning. Likaså ska enligt 2 kap. 10 § personuppgifter som grundar sig på fakta skiljas från uppgifter som grundar sig på personliga bedömningar. Om grunden inte framgår av sammanhanget eller på annat sätt ska den tydliggöras genom en särskild upplysning.

Behandling av känsliga personuppgifter

Personuppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening eller som rör hälsa, sexualliv eller sexuell läggning benämns känsliga personuppgifter och får enligt huvudregeln i 2 kap. 11 § inte behandlas. I de fall där uppgifter om en person redan behandlas får de dock kompletteras med känsliga personuppgifter när det är absolut nödvändigt för ändamålet med behandlingen.

Även biometriska uppgifter som används för att identifiera en person och genetiska uppgifter är enligt 2 kap. 12 § känsliga personuppgifter. De får behandlas endast om det är särskilt föreskrivet och absolut nödvändigt för ändamålet med behandlingen.

Det är enligt 2 kap. 14 § förbjudet att göra sökningar i syfte att få fram ett personurval grundat på känsliga personuppgifter. Även sökningar som är tillåtna kan ibland resultera i ett sådant urval, men frågan om de uppgifter som tas fram får fortsätta att behandlas ska bedömas med utgångspunkt i de allmänna reglerna om behandling

av personuppgifter. För sådana sammanställningar av personuppgifter ska gälla absolut sekretess.

Rättelse, komplettering och radering av personuppgifter

Alla rimliga åtgärder ska enligt 2 kap. 15 § vidtas för att personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålet med behandlingen utan onödigt dröjsmål rättas och för att hindra att sådana uppgifter lämnas ut eller görs tillgängliga. Personuppgifter som är inaktuella ska uppdateras om det är nödvändigt.

Alla rimliga åtgärder ska också enligt 2 kap. 16 § vidtas för att personuppgifter som behandlas i strid med grundläggande bestämmelser om behandling utan onödigt dröjsmål raderas och för att förhindra att sådana uppgifter lämnas ut eller görs tillgängliga. Om personuppgifterna behöver finnas kvar som bevisning ska i stället behandlingen av uppgifterna utan onödigt dröjsmål begränsas.

Längsta tid som personuppgifter får behandlas

Personuppgifter får enligt huvudregeln i 2 kap. 17 § inte behandlas längre än vad som är nödvändigt med hänsyn till ändamålet med behandlingen. Det hindrar inte att en behörig myndighet arkiverar och bevarar allmänna handlingar eller att arkivmaterial lämnas till en arkivmyndighet. Om det inte finns en författningsbestämmelse om när en viss kategori av personuppgifter inte längre får behandlas för andra ändamål än arkivändamål, ska den personuppgiftsansvarige enligt 2 kap. 18 § årligen se över behovet av att fortsätta att behandla personuppgifterna.

Automatiserade beslut

Om ett beslut, som har rättsliga följder för en fysisk person eller annars i betydande grad påverkar honom eller henne, enbart grundas på automatiserad behandling av sådana personuppgifter som är avsedda att bedöma hans eller hennes egenskaper, ska personen enligt 2 kap. 19 § ha möjlighet att på begäran få beslutet omprövat

av någon person. Automatiserade beslut som grundas enbart på känsliga personuppgifter förbjuds.

Behandling för ändamål utanför brottsdatalogens tillämpningsområde

I 2 kap. 21 § erinras om att dataskyddsförordningen ska tillämpas när en behörig myndighet behandlar personuppgifter för ändamål utanför brottsdatalogens tillämpningsområde. Det innebär att förordningen ska tillämpas bl.a. när personuppgifter behandlas för att eventuellt lämnas ut till någon annan än en behörig myndighet för den myndighetens behov eller när en brottsbekämpande myndighet överväger att lämna ut personuppgifter för att användas i annan verksamhet som myndigheten bedriver.

3.2.2 Personuppgiftsansvarigas skyldigheter

Personuppgiftsansvarets omfattning

I 3 kap. 1 § slås fast att den personuppgiftsansvarige är ansvarig för all behandling av personuppgifter som utförs under dennes ledning eller på dennes vägnar. Vem som är personuppgiftsansvarig framgår som regel av myndigheternas registerförfattningar.

Åtgärder för att säkerställa författningsenlig behandling

I 3 kap. 2–5 §§ anges vilka tekniska och organisatoriska åtgärder en personuppgiftsansvarig är skyldig att vidta för att säkerställa och kunna visa att personuppgiftsbehandlingen är författningsenlig och att registrerades rättigheter skyddas. Det rör sig både om inbyggt dataskydd, dataskydd som standard och krav på loggning i automatiserade behandlingssystem.

Den personuppgiftsansvarige ska också enligt 3 kap. 6 § se till att tillgången till personuppgifter begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter.

I 3 kap. 7 § regleras den personuppgiftsansvariges skyldighet att både inför en ny typ av behandling och vid betydande förändringar av redan pågående behandling, som antas medföra särskild risk för intrång i registrerades personliga integritet, göra en s.k. konse-

kvensbedömning. Om den visar att det finns särskild risk för intrång i registrerades integritet, eller om typen av behandling innebär särskild risk för intrång, ska den personuppgiftsansvarige samråda med tillsynsmyndigheten innan behandlingen påbörjas eller förändringen genomförs, s.k. förhandssamråd.

Säkerheten för personuppgifter

Den personuppgiftsansvarige är enligt 3 kap. 8 § skyldig att vidta lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifterna, särskilt mot obehörig eller otillåten behandling och mot förlust, förstöring eller annan oavsiktlig skada.

Om det inträffar en personuppgiftsincident ska den personuppgiftsansvarige enligt 3 kap. 9 § anmäla det till tillsynsmyndigheten inom 72 timmar från det att den personuppgiftsansvarige fick kännedom om incidenten. Anmälningsskyldigheten gäller dock inte om incidenten rör nationell säkerhet. Någon anmälan behöver inte heller göras bl.a. om det kan antas att incidenten inte har medfört eller kommer att medföra någon risk för otillbörligt intrång i registrerades personliga integritet.

Den personuppgiftsansvarige ska enligt 3 kap. 10 § underrätta den registrerade om sådana personuppgiftsincidenter som ska anmälas till tillsynsmyndigheten. Någon underrättelse behöver dock inte lämnas om det gäller sekretess eller tystnadsplikt, vilket framgår av 3 kap. 11 §. Det finns även vissa andra undantag från anmälningskyldigheten.

Samarbete med tillsynsmyndigheten

Enligt 3 kap. 12 § ska den personuppgiftsansvarige samarbeta med tillsynsmyndigheten när den utför uppgifter enligt brottsdatalogen med tillhörande förordning. Skyldigheten, som är mer långtgående än kraven i förvaltningslagen, gäller generellt.

Dataskyddsbud

Den personuppgiftsansvarige ska enligt 3 kap. 13 § utse dataskyddsbud och anmäla till tillsynsmyndigheten när sådana utses och entledigas. Dataskyddsbudens uppgifter anges i 3 kap. 14 §. Ombuden ska bl.a. självständigt kontrollera att den personuppgiftsansvarige behandlar personuppgifter författningsenligt och på ett korrekt sätt och i övrigt fullgör sina skyldigheter. Om den personuppgiftsansvarige bryter mot bestämmelser om behandling av personuppgifter och inte vidtar rättelse, ska dataskyddsbudet enligt 3 kap. 15 § anmäla det till tillsynsmyndigheten.

Personuppgiftsbiträden

Enligt 3 kap. 17 § får den personuppgiftsansvarige få anlita personuppgiftsbiträden om det är lämpligt. Den personuppgiftsansvarige ska försäkra sig om att biträdet vidtar lämpliga tekniska och organisatoriska åtgärder för att behandlingen av personuppgifter ska vara författningsenlig och för att skydda registrerades rättigheter. Det ska enligt 3 kap. 18 § upprättas ett skriftligt avtal eller en annan skriftlig överenskommelse om personuppgiftsbitrådets behandling av personuppgifter för den personuppgiftsansvariges räkning.

Ett personuppgiftsbiträde och de som arbetar under bitrådets ledning får enligt 3 kap. 19 § bara behandla personuppgifter i enlighet med instruktioner från den personuppgiftsansvarige.

Gemensamt personuppgiftsansvar

Två eller flera myndigheter får enligt 3 kap. 21 § vara gemensamt personuppgiftsansvariga endast i den utsträckning det följer av lag eller förordning eller regeringen i ett enskilt fall beslutar om det.

3.2.3 Enskildas rättigheter

Rätten till information

Den personuppgiftsansvarige ska enligt 4 kap. 1 § göra viss allmän information tillgänglig för registrerade, exempelvis på myndighetens webbplats. Det gäller den personuppgiftsansvariges identitet och kontaktuppgifter, dataskyddsombudets kontaktuppgifter, ändamålen med behandlingen, rätten att få information och att begära rättelse, radering eller begränsning av behandlingen och möjligheten att lämna in klagomål till tillsynsmyndigheten och kontaktuppgifterna till den.

I specifika fall ska den personuppgiftsansvarige enligt 4 kap. 2 § på eget initiativ lämna viss ytterligare information till den registrerade, om det behövs för att han eller hon ska kunna ta tillvara sina rättigheter. Det rör sig om bl.a. information om den rättsliga grunden för behandlingen, kategorier av mottagare av uppgifterna, hur länge uppgifterna får behandlas och övrig nödvändig information.

Den personuppgiftsansvarige ska vidare enligt 4 kap. 3 § till den som begär det utan onödigt dröjsmål lämna skriftligt besked om personuppgifter som rör honom eller henne behandlas. Om så är fallet ska sökanden få del av dem och få viss information om behandlingen. Informationen avser bl.a. vilka personuppgifter om sökanden som behandlas, varifrån de kommer, den rättsliga grunden för behandlingen, ändamålen med behandlingen och hur länge personuppgifterna får behandlas.

Den som har varit föremål för ett automatiserat beslut får enligt 4 kap. 4 § begära närmare information om beslutet.

Information enligt 4 kap. 1, 2 och 4 §§ ska enligt 4 kap. 12 § lämnas utan avgift. Information enligt 4 kap. 3 § ska lämnas utan avgift en gång per år.

Begränsning av rätten till information

Rätten till information enligt 4 kap. 2 eller 3 § får enligt 4 kap. 5 § begränsas i den utsträckning det är författningsreglerat eller framgår av beslut som har meddelats med stöd av författning att uppgifter inte får lämnas ut. Begränsning får dock bara göras av hänsyn till vissa i paragrafen uppräknade intressen, bl.a. intresset av att

förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet och intresset av att nationell säkerhet skyddas.

Om det finns grund för att begränsa informationen är den personuppgiftsansvarige inte skyldig att lämna ut skälen för beslutet eller för beslut i fråga om rättelse, radering eller begränsning av behandlingen.

Motsvarande undantag från informationsskyldigheten gäller för en behörig myndighet som inte tillämpar offentlighets- och sekretesslagen.

Rätten till rättelse, radering och begränsning av behandlingen

På begäran av den registrerade ska den personuppgiftsansvarige enligt 4 kap. 9 § utan onödigt dröjsmål rätta eller komplettera personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålet med behandlingen. Om den personuppgiftsansvarige inte kan fastställa att personuppgifterna är korrekta ska behandlingen av dem i stället utan onödigt dröjsmål begränsas.

På begäran av den registrerade ska den personuppgiftsansvarige enligt 4 kap. 10 § utan onödigt dröjsmål radera personuppgifter om de behandlas på otillåtet sätt. Detsamma gäller om radering krävs för att den personuppgiftsansvarige ska fullgöra en rättslig förpliktelse. Om uppgifterna behöver sparas som bevisning ska behandlingen av dem i stället utan onödigt dröjsmål begränsas.

Den personuppgiftsansvarige avgör enligt 4 kap. 11 § vilken åtgärd som ska vidtas med anledning av en begäran om rättelse, radering eller begränsning av behandlingen.

3.2.4 Tillsyn

Tillsynsmyndighetens uppdrag och arbetsuppgifter

I 5 kap. 1 § anges de dubbla perspektiv som tillsynsmyndigheten ska ha. Myndigheten ska verka både för att fysiska personers grundläggande fri- och rättigheter skyddas i samband med behand-

ling av personuppgifter och för att underlätta det fria flödet av personuppgifter inom brottsdatalogens tillämpningsområde.

I 5 kap. 2–4 §§ anges vilka arbetsuppgifter tillsynsmyndigheten ska ha. Tillsynsmyndigheten ska utöva allmän tillsyn över personuppgiftsbehandling, handlägga klagomål från registrerade, på begäran kontrollera om personuppgifter behandlas författningenligt, ge råd och stöd till personuppgiftsansvariga och personuppgiftsbiträden och på begäran bistå tillsynsmyndigheter i andra medlemsstater.

Tillsynsmyndighetens befogenheter

Tillsynsmyndighetens befogenheter regleras i 5 kap. 5–7 §§. Befogenheterna bildar en trappa, där successivt mer ingripande befogenheter kan användas.

Tillsynsmyndigheten har enligt 5 kap. 5 §, som reglerar myndighetens undersökande befogenheter, rätt att av personuppgiftsansvariga på begäran få bl.a. tillgång till de personuppgifter som behandlas, upplysningar om och dokumentation av behandlingen av personuppgifter och säkerhets- och skyddsåtgärder, tillträde till lokaler som den personuppgiftsansvarige disponerar och det biträde som behövs för att utöva tillsynen.

Om tillsynsmyndigheten bedömer att det finns risk för att personuppgifter kan komma att behandlas i strid med lag eller annan författning ska myndigheten enligt 5 kap. 6 §, som reglerar de förebyggande befogenheterna, genom råd, rekommendationer eller påpekanden försöka förmå den personuppgiftsansvarige eller personuppgiftsbiträdet att vidta åtgärder för att minska den risken. Myndigheten får utfärda en skriftlig varning för att planerad behandling riskerar att stå i strid med lag eller annan författning. Varning får även utfärdas om det finns risk för att pågående behandling kan komma att strida mot lag eller annan författning.

Om tillsynsmyndigheten konstaterar att personuppgifter behandlas i strid med lag eller annan författning, eller att den personuppgiftsansvarige eller personuppgiftsbiträdet annars inte fullgör sina skyldigheter, får myndigheten använda sina korrigerande befogenheter. De regleras i 5 kap. 7 §. Tillsynsmyndigheten får förelägga den personuppgiftsansvarige eller personuppgiftsbiträdet att

vidta åtgärder för att behandlingen ska bli författningssenlig eller för att uppfylla andra skyldigheter. Om bristen är allvarlig får myndigheten förbjuda fortsatt behandling och myndigheten får även besluta om sanktionsavgift. Myndigheten får också använda sina förebyggande befogenheter, med undantag för varning.

Innan tillsynsmyndigheten fattar ett bindande beslut ska enligt 5 kap. 8 § den som beslutet gäller ges tillfälle att yttra sig.

Besked angående handläggningen av klagomål

Om tillsynsmyndigheten inte inom tre månader från det att ett klagomål kom in har tagit ställning till om tillsyn ska utövas i anledning av klagomålet, ska myndigheten enligt 5 kap. 9 § på skriftlig begäran av den registrerade antingen lämna besked i frågan eller i ett särskilt beslut avslå begäran. Besked eller beslut ska meddelas inom två veckor från det att begäran kom in till myndigheten. Om tillsynsmyndigheten har avslagit en sådan begäran om besked får den registrerade enligt 5 kap. 10 § återkomma med en ny begäran om besked först efter tre månader.

Samarbete med tillsynsmyndigheter i andra medlemsstater

På begäran av en tillsynsmyndighet i en annan medlemsstat ska den svenska tillsynsmyndigheten bistå den utländska myndigheten. Tillsynsmyndigheten får då enligt 5 kap. 12 § använda sina vanliga befogenheter. En begäran om bistånd får enligt 5 kap. 11 § bara vägras om det skulle strida mot en bindande unionsrättsakt, en lag eller en förordning att tillmötesgå den.

Tillsynsmyndigheten får enligt 5 kap. 13 §, om det är förenligt med svenska intressen, lämna ut en sekretessbelagd uppgift till en behörig tillsynsmyndighet i en annan medlemsstat.

Information som tillsynsmyndigheten efter begäran har fått från en tillsynsmyndighet i en annan medlemsstat får enligt 5 kap. 14 § inte användas för något annat ändamål än det för vilket informationen begärdes.

Förfarandet när det finns anledning att ifrågasätta en unionsrättsakt

Om tillsynsmyndigheten vid handläggningen av ett ärende bedömer att det finns särskilda skäl att ifrågasätta giltigheten av en unionsrättsakt som påverkar tillämpningen av brottsdatalogen, får myndigheten enligt 5 kap. 15 § hos allmän förvaltningsdomstol ansöka om att en korrigerande åtgärd ska vidtas. Genom att föra talan vid domstol öppnas möjlighet för domstolen att begära ett förhandsavgörande av EU-domstolen.

3.2.5 Sanktioner, skadestånd och rättsmedel*Sanktionsavgift*

Ett nytt sanktionssystem med administrativa sanktionsavgifter införs. Regleringen innebär att den personuppgiftsansvarige ska betala sanktionsavgift om regelsystemet överträds. I vissa fall kan även personuppgiftsbiträden bli skyldiga att betala sanktionsavgift.

De överträdelser som kan föranleda att sanktionsavgift tas ut av den personuppgiftsansvarige räknas uttömmande upp i 6 kap. 1 §. Det gäller först och främst överträdelser som innebär att personuppgifter behandlas på otillåtet sätt. Sanktionsavgift kan också tas ut om den personuppgiftsansvarige har underlåtit att anmäla en personuppgiftsincident till tillsynsmyndigheten, inte har dokumenterat sådana incidenter, inte har bistått tillsynsmyndigheten på det sätt som krävs enligt lagen eller har underlåtit att följa bindande beslut som tillsynsmyndigheten har meddelat. I 6 kap. 2 § regleras i vilka fall sanktionsavgift får tas ut av personuppgiftsbiträden.

I 6 kap. 3 § anges hur stor sanktionsavgift som får tas ut. Sanktionsavgiften är lägst 25 000 kronor och högst 10 miljoner kronor vid mindre allvarliga överträdelser. Vilka överträdelser som räknas som mindre allvarliga anges i paragrafen. Vid andra överträdelser är sanktionsavgiften lägst 50 000 kronor och högst 20 miljoner kronor. Om flera bestämmelser har överträtts genom samma personuppgiftsbehandling eller genom sammankopplade behandlingar ska sanktionsavgiften bestämmas med hänsyn till samtliga överträdelser. Avgiften får dock aldrig överstiga maximibeloppet för den allvarligaste överträdelser.

I 6 kap. 4 § anges hur sanktionsavgiften ska bestämmas i det enskilda fallet. Både vid bedömningen av om sanktionsavgift ska tas ut och när storleken på avgiften bestäms ska särskild hänsyn tas till bl.a. om överträdelsen varit uppsåtlig eller berott på oaktsamhet, den skada, fara eller kränkning som överträdelsen inneburit, överträdelsens karaktär, svårhetsgrad och varaktighet och vad den personuppgiftsansvarige gjort för att begränsa skadan.

Sanktionsavgift får enligt 6 kap. 5 § sättas ned helt eller delvis om överträdelsen är ursäktlig eller om det annars skulle vara oskäligt att ta ut avgift.

Skadestånd

Den personuppgiftsansvarige ska enligt 7 kap. 1 § ersätta den registrerade för den skada och kränkning av den personliga integriteten som behandling av personuppgifter i strid med lagen har orsakat. Någon möjlighet till jämkning av skadeståndet finns inte, t.ex. om någon annan har vidarebefordrat felaktiga personuppgifter som den personuppgiftsansvarige sedan har behandlat.

Överklagande av beslut som en myndighet fattat i egenskap av personuppgiftsansvarig

Beslut i fråga om bl.a. rättelse, komplettering, radering eller begränsning av behandlingen, som en myndighet har fattat i egenskap av personuppgiftsansvarig, får enligt 7 kap. 2 § överklagas till allmän förvaltningsdomstol. Uppräkningen av vilka beslut som får överklagas är uttömmande. Prövningstillstånd krävs vid överklagande till kammarrätten.

Överklagande av tillsynsmyndighetens beslut

Om den som har lämnat in ett klagomål till tillsynsmyndigheten inte inom tre månader har fått besked av myndigheten om klagomålet kommer att leda till tillsyn, får klaganden begära ett skriftligt besked i frågan och kan därefter, om myndigheten avslår begäran, enligt 7 kap. 3 § föra s.k. dröjsmålstalan i allmän förvaltningsdom-

stol. En sådan talan innebär att domstolen bara tar ställning till om tillsynsmyndigheten borde ha lämnat klaganden besked, inte om tillsyn ska utövas eller inte. Domstolen kan förelägga tillsynsmyndigheten att inom viss tid ge klaganden besked i fråga om tillsyn kommer att utövas.

Andra beslut som tillsynsmyndigheten har meddelat får enligt 7 kap. 4 § överklagas till allmän förvaltningsdomstol. Vid överklagande till kammarrätten krävs prövningstillstånd.

Några andra beslut än de som nu har angetts får enligt 7 kap. 5 § inte överklagas.

3.2.6 Överföring av personuppgifter till tredjeland och internationella organisationer

Förutsättningar för att överföring ska vara tillåten

I 8 kap. 1–5 §§ anges förutsättningarna för att personuppgifter ska få överföras till ett tredjeland eller en internationell organisation. Personuppgifter får endast överföras om överföringen görs av en behörig myndighet och är nödvändig för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet och överföringen riktas till en behörig myndighet i ett tredjeland eller till en internationell organisation som är en behörig myndighet. Dessutom ska det finnas en adekvat skyddsnivå för behandlingen av personuppgifter i det tredjelandet eller hos den internationella organisationen. Beslut om adekvat skyddsnivå meddelas av Europeiska kommissionen. Om det inte finns ett sådant beslut får personuppgifterna ändå överföras om tillräckliga skyddsåtgärder har fastställts i ett avtal eller garanteras på annat sätt. I sista hand får personuppgifter överföras om överföringen är nödvändig i någon av de i lagen angivna undantagssituationerna.

Enligt 8 kap. 2 § får personuppgifter som en svensk myndighet har fått från en annan medlemsstat inte överföras till ett tredjeland eller en internationell organisation utan förhandsmedgivande av den medlemsstaten. Om medgivande inte hinner inhämtas får dock uppgifterna ändå överföras om det är nödvändigt för att avvärja en omedelbar och allvarlig fara för allmän säkerhet.

Vidareöverföring

S.k. vidareöverföring regleras i 8 kap. 6 §. Med det avses överföring av personuppgifter som har lämnats av en medlemstat till en annan och som sedan har överförts till antingen ett tredjeland eller en internationell organisation som i sin tur vill överföra uppgifterna till antingen ett tredjeland eller en internationell organisation. En svensk myndighet får inte ge tillstånd till sådan vidareöverföring om personuppgifterna har kommit från en annan medlemsstat och den staten inte har medgett vidareöverföring. När en svensk behörig myndighet ska ta ställning till om personuppgifter ska få vidareöverföras ska enligt 8 kap. 7 § särskild vikt läggas vid bl.a. brottets allvar, allvaret i faran för allmän säkerhet och det ändamål för vilket personuppgifterna ursprungligen lämnades till den andra medlemsstaten.

Överföring till någon annan än en behörig myndighet

I vissa fall kan personuppgifter behöva överföras till någon som inte är en behörig myndighet i ett tredjeland, t.ex. direkt till en målsägande som är etablerad där. Det får enligt 8 kap. 8 § göras endast om det är absolut nödvändigt för att den svenska myndigheten ska kunna utföra en sådan arbetsuppgift som gör lagen tillämplig och myndigheten underrättar mottagaren om för vilket eller vilka ändamål personuppgifterna får behandlas. Dessutom krävs att det skulle vara ineffektivt eller olämpligt att överföra personuppgifterna till en behörig myndighet i det tredjelandet.

Villkor om användningsbegränsning

Om en svensk behörig myndighet har fått personuppgifter från ett tredjeland eller en internationell organisation och det på grund av en överenskommelse med det tredjelandet eller den internationella organisationen gäller villkor som begränsar möjligheten att använda uppgifterna, ska enligt 8 kap. 9 § svenska myndigheter följa villkoren oavsett vad som är föreskrivet i lag eller annan författning.

En svensk behörig myndighet får, vid överföring av personuppgifter till ett tredjeland eller en internationell organisation, enligt

8 kap. 10 § i ett enskilt fall ställa upp villkor som begränsar mottagarens möjlighet att använda uppgifterna om det krävs med hänsyn till enskilds rätt eller från allmän synpunkt.

3.2.7 Ikraftträdande och övergångsbestämmelser

Utredningen föreslår i delbetänkandet att den nya lagstiftningen ska träda i kraft den 1 maj 2018. Det nya sanktionssystemet kräver särskilda övergångsbestämmelser. Det krävs också särskilda övergångsbestämmelser för hur pågående mål och ärenden om bl.a. tillsyn och skadestånd ska hanteras. Bestämmelserna om loggning i automatiserade behandlingssystem som inrättats före den 6 maj 2018 behöver inte tillämpas förrän den 1 maj 2023.

4 Framtida utformning av registerförfattningarna

4.1 Utgångspunkter

I utredningens uppdrag ingår att se över vissa författningar som reglerar personuppgiftsbehandling inom direktivets tillämpningsområde. Det gäller lagen (2001:617) om behandling av personuppgifter inom kriminalvården, polisdatalagen (2010:361), kustbevakningsdatalagen (2012:145), åklagardatalagen (2015:433), domstolsdatalagen (2015:728), tullbrottsdatalagen (2017:447) och skattebrottsdatalagen (2017:452), alla med tillhörande förordningar. I det följande benämns de registerförfattningarna.

Uppdraget omfattar dels att analysera i vilken utsträckning författningarna står i överensstämmelse med bestämmelserna i direktivet, dels att anpassa dem till de krav som ställs där och till förslagen i delbetänkandet. Utredningen ska enligt direktiven så långt det är lämpligt och möjligt sträva efter lösningar som är förenliga med gällande författningar och systematik (dir. 2016:21 s. 6).

Som redovisas i kapitel 3 föreslår utredningen i delbetänkandet en ny lag, brottsdatalagen, som kommer att fylla ungefär samma funktion som personuppgiftslagen gör i dag i verksamhet som rör brottsbekämpning, lagföring, straffverkställighet och upprätthållande av allmän ordning och säkerhet. I delbetänkandet konstaterar utredningen att det, vid sidan av brottsdatalagen, alltjämt kommer att behövas bestämmelser som tar hänsyn till de särskilda behov en viss behörig myndighet har av att kunna behandla personuppgifter för att utföra sina arbetsuppgifter. Sådan särreglering bör finnas i myndigheternas registerförfattningar (se SOU 2017:29 s. 140 f.).

4.2 Det krävs anpassningar till den nya dataskyddsregleringen

Regleringen i registerförfattningarna utgår i dag från personuppgiftslagen, antingen genom att registerförfattningen gäller i stället för personuppgiftslagen men hänvisar till ett antal bestämmelser i den lagen eller genom att registerförfattningen gäller utöver personuppgiftslagen.

Personuppgiftslagen, som är tillämplig vid personuppgiftsbehandling i hela samhället, är allmänt hållen och tar i mycket begränsad utsträckning hänsyn till de särskilda behov som vissa samhällssektorer har. I och med att brottsdatalagen innehåller bestämmelser som är skraddarsydda för brottsbekämpning, lagföring, straffverkställighet och upprätthållande av allmän ordning och säkerhet minskar behovet av att ha särregler i registerförfattningarna. Att den nya regleringen leder till större enhetlighet underlättar informationsflödet, vilket är ett övergripande syfte med direktivet.

Utredningens utgångspunkt är att de generella bestämmelserna i brottsdatalagen ska ersätta motsvarande bestämmelser i registerförfattningarna. Om det inte finns några sakliga skäl för särlösningar bör regleringarna så långt det är möjligt vara likadana för att underlätta informationsutbytet. Det innebär att registerförfattningarna enligt utredningens mening ibland bör anpassas till varandra, även om det inte krävs för genomförandet av direktivet.

I detta kapitel tar utredningen upp några övergripande frågor som rör den framtida utformningen av myndigheternas registerförfattningar, medan behovet av ändringar i var och en av dem behandlas i de följande kapitlen. Vissa ändringar är desamma för flertalet av författningarna, medan det i andra fall krävs särskilda lösningar. Utredningen behandlar behovet av generella ändringar i kapitel 5 och 6, medan ändringar som är specifika för en viss myndighets registerförfattning behandlas i kapitel 7–13. Säkerhetspolisens personuppgiftsbehandling, som i dag regleras i polisdatalagen men ligger utanför brottsdatalagens tillämpningsområde, behandlas i kapitel 14 och 15.

4.3 Merparten av bestämmelserna är förenliga med dataskyddsdirektivet

Utredningens bedömning: Merparten av bestämmelserna i registerförfattningarna är förenliga med direktivet och behöver inte ändras av det skälet. Många bestämmelser behöver dock ändras av andra skäl, bl.a. för att få en enhetlig terminologi. Det krävs också omfattande redaktionella ändringar.

Skälen för utredningens bedömning: Med undantag för kriminalvårdens lagstiftning har alla registerförfattningar som uppdraget omfattar tillkommit under de senaste åren. Det innebär att de uppfyller kraven som ställs i dataskyddsrambeslutet. Mot bakgrund av att direktivet i stor utsträckning bygger vidare på regleringen i dataskyddsrambeslutet är registerförfattningarna redan till stor del anpassade till de krav som ställs i direktivet. Det utesluter inte att det även i de nya registerförfattningarna kan finnas enskilda bestämmelser som behöver ändras för att stå i överensstämmelse med hur brottsdatalagen genomför direktivet, eftersom det tillkommit vissa krav. Utredningen har vid en genomgång av de enskilda bestämmelserna funnit att flertalet av dem inte behöver ändras för att uppfylla kraven i direktivet.

När det gäller Kriminalvårdens lagstiftning avviker den i många avseenden från den modernare lagstiftning som gäller för flertalet behöriga myndigheter. I motsats till de flesta andra registerförfattningarna gäller Kriminalvårdens dessutom utöver personuppgiftslagen och skiljer sig på så sätt från de övriga även strukturmässigt. Den regleringen kräver därför särskilda överväganden.

Skillnaderna i fråga om registerförfattningarnas tillämpningsområden får betydelse för hur de bör anpassas till brottsdatalagen. Eftersom vissa författningar gäller för personuppgiftsbehandling både inom och utanför brottsdatalagens tillämpningsområde går det inte att använda samma mall för hur alla registerförfattningar bör anpassas till brottsdatalagen.

Eftersom det finns fler bestämmelser av generell karaktär i brottsdatalagen än i personuppgiftslagen behövs, som nyss nämnts, inte motsvarande bestämmelser i registerförfattningarna. När många bestämmelser i registerförfattningarna blir överflödiga be-

höver de omarbetas. Det krävs redaktionella ändringar även av andra skäl, exempelvis på grund av att vissa bestämmelser samlas eller på grund av ändrade hänvisningar. Vissa bestämmelser bör ändras för att få till stånd en mer enhetlig utformning eller terminologi, anpassad till brottsdatalagen.

De bestämmelser i registerförfattningarna som utredningen anser inte kräver någon saklig ändring kommer inte att kommenteras när respektive författning behandlas. Utredningen kommer inte heller att särskilt kommentera sådana bestämmelser som enbart blir föremål för mindre ändringar av språklig eller redaktionell karaktär.

4.4 Lagarnas tillämpningsområden

4.4.1 Tillämpningsområdet ska regleras

Utredningens bedömning: Registerlagarna bör även i fortsättningen innehålla bestämmelser om tillämpningsområdet. Regleringen bör i likhet med tillämpningsområdet för brottsdatalagen utgå från syftet med personuppgiftsbehandlingen i stället för i vilken verksamhet den utförs.

Skälen för utredningens bedömning

Bestämmelser om tillämpningsområdet bör finnas kvar men anpassas

I dag anges det vilket tillämpningsområde respektive registerförfattning har t.ex. genom att det föreskrivs att lagen gäller i en viss myndighets brottsbekämpande eller operativa verksamhet. I vissa registerförfattningar fyller bestämmelsen om tillämpningsområdet den funktionen att den anger att författningen gäller för flera myndigheter (se t.ex. 1 kap. 2 § polisdatalagen). I andra fall har bestämmelserna till syfte att avgränsa tillämpningsområdet till någon eller några delar av en myndighets verksamhet (se t.ex. 1 kap. 2 § tullbrottsdatalagen och 1 kap. 2 § skattebrottsdatalagen).

Uppdelningen mellan brottsdatalagen och dataskyddsförordningen innebär att alla registerförfattningar behöver en tydlig avgränsning. Det är därför nödvändigt att även i fortsättningen ha bestämmelser om tillämpningsområdet i registerförfattningarna.

Utredningen återkommer i kapitel 7–14 till hur tillämpningsområdet bör utformas för de olika myndigheterna.

Från verksamhet till syfte

Syftet med personuppgiftsbehandlingen är avgörande för om brottsdatalagen är tillämplig, medan regleringen i registerlagarna i dag bygger på i vilken verksamhet behandlingen utförs, t.ex. brottsbekämpande verksamhet. Regleringen i brottsdatalagen har sin grund i att direktivet utgår från syftet med behandlingen, inte i vilken verksamhet den utförs. Det är därför inte möjligt att behålla bestämmelser som författningstekniskt knyts till den verksamhet där behandlingen utförs. Utredningen redovisar i delbetänkandet ingående vad det innebär för tillämpningen att fokus flyttas från verksamheten som sådan till syftet med den enskilda behandlingen (se SOU 2017:29 s. 181 f.).

Utredningen har, i enlighet med direktiven för arbetet, strävat efter att behålla inarbetade begrepp. Mot bakgrund av regleringen i direktivet är det dock inte alltid möjligt. Ett sådant exempel är uttrycket brottsbekämpande verksamhet, som i dag används i ett flertal av registerförfattningarna. Eftersom regleringen ska utgå från syftet med behandlingen av personuppgifter bör uttrycket brottsbekämpande verksamhet utmönstras ur registerförfattningarna. I stället bör tillämpningsområdet utgå från utformningen av 1 kap. 2 § brottsdatalagen. Det innebär att tillämpningsområdet i varierande utsträckning bör knytas till att personuppgifter behandlas i något av de syften som anges i brottsdatalagen, dvs. att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet (se SOU 2017:29 s. 159 f.).

Myndigheten ska agera i egenskap av behörig myndighet

Det är inte enbart syftet med personuppgiftsbehandlingen som avgör om brottsdatalagen är tillämplig. Det krävs också att myndigheten agerar i egenskap av behörig myndighet enligt den lagen. I 1 kap. 6 § brottsdatalagen definieras behörig myndighet som en myndighet som har till uppgift att förebygga, förhindra eller upp-

täcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet. Det bör av tillämpningsområdet i respektive registerförfattning framgå att författningen endast är tillämplig när myndigheten agerar i egenskap av behörig myndighet.

Hur förhåller sig regleringarna till varandra?

En särskild fråga är hur man ska se på det förhållandet att tillämpningsområdet i en myndighets registerförfattning inte är lika brett som brottsdatalagens tillämpningsområde. Som exempel kan nämnas att tillämpningsområdet för flertalet registerförfattningar inte omfattar straffverkställighet och inte heller upprätthållande av allmän ordning och säkerhet. Utredningens utgångspunkt är att brottsdatalagen, som ska tillämpas i hela rättskedjan, bildar den yttre ramen och att tillämpningsområdena i registerförfattningarna inskränker rätten att behandla personuppgifter till vad som gäller för en viss myndighet eller till behandling av personuppgifter för vissa syften i en del av dess verksamhet.

En annan viktig fråga är hur brottsdatalagens tillämpningsområde och registerförfattningarnas tillämpningsområden förhåller sig till varandra. En utgångspunkt bör vara att en myndighets registerförfattning ska reglera all myndighetens personuppgiftsbehandling inom brottsdatalagens tillämpningsområde. I dag regleras dock framför allt Polismyndighetens personuppgiftsbehandling inom brottsdatalagens tillämpningsområde i flera olika författningar. Det framgår av 1 kap. 3 § polisdatalagen. Det är mot den bakgrunden inte möjligt att reglera all myndighetens personuppgiftsbehandling inom brottsdatalagens tillämpningsområde i registerförfattningen. Det bör enligt utredningens mening i så stor utsträckning som möjligt framgå av respektive registerförfattning om det finns annan reglering inom brottsdatalagens tillämpningsområde som helt ersätter regleringen i registerförfattningen. Om det i någon författning finns avvikande bestämmelser som till viss del ersätter regleringen i registerförfattningen bör det också framgå på samma sätt som i dag. Det är fallet med särregleringen i lagen (2017:496) om internationellt polisiärt samarbete och föreskrifter som har meddelats i anslutning till den lagen.

4.4.2 Vad innebär det ändrade tillämpningsområdet?

Som framgått kommer de justeringar som görs beträffande tillämpningsområdet att träffa alla myndigheter i rättskedjan. Det som framför allt får betydelse är att endast den personuppgiftsbehandling som utförs i vissa angivna syften kommer att omfattas av registerförfattningarnas tillämpningsområde. I dag reglerar registerförfattningarna personuppgiftsbehandling såväl i myndigheternas kärnverksamhet som för att lämna uppgifter till andra – oavsett för vilket ändamål det görs. Efter anpassningen kommer registerförfattningarna att i fråga om uppgiftslämnande enbart reglera den personuppgiftsbehandling som ligger inom brottsdatalogens tillämpningsområde. Det är en direkt effekt av att olika regelverk gäller för personuppgiftsbehandling inom brottsdatalogens respektive dataskyddsförordningens tillämpningsområden. Exempel på något som i många fall kommer att ligga utanför tillämpningsområdet kan vara när Tullverkets brottsbekämpande verksamhet lämnar uppgifter till verksamheten under Effektiv handel. Utlämnande av allmänna handlingar enligt tryckfrihetsförordningen ligger alltid utanför tillämpningsområdet.

Tillämpningsområdet för alla registerförfattningar blir därmed smalare än i dag, eftersom inte all personuppgiftsbehandling som utförs när en myndighet ägnar sig åt brottsbekämpning, lagföring, straffverkställighet eller upprätthållande av allmän ordning och säkerhet har ett sådant syfte att registerförfattningen är tillämplig.

Det förhållandet att tillämpningsområdet enbart omfattar den som agerar som behörig myndighet har däremot mindre betydelse, eftersom syftet med behandlingen och begreppet behörig myndighet är så intimt förbundna med varandra och båda förutsättningarna ska vara uppfyllda för att personuppgiftsbehandlingen ska ligga inom tillämpningsområdet.

4.5 Ska registerförfattningarna reglera frågor som inte rör dataskydd?

Utredningens bedömning: Registerförfattningarna bör även i fortsättningen innehålla sekretessbrytande bestämmelser. De bör också reglera på vilket sätt personuppgifter får tillhandahållas och viss föreskriftsrätt som inte direkt rör tillämpningsområdet.

Skälen för utredningens bedömning

Registerförfattningarna ska även i fortsättningen innehålla annat än bara dataskyddsbestämmelser

Registerförfattningarna innehåller i dag inte bara dataskyddsbestämmelser utan också vissa andra bestämmelser som har direkt anknytning till dataskyddsregleringen. En kategori är de sekretessbrytande bestämmelser som finns i flertalet registerförfattningar. Det finns två typer av sådana bestämmelser. Den ena är de som gör det möjligt att medge direktåtkomst till vissa personuppgifter. Den andra är de som har till syfte att bryta sekretessen för visst informationsutbyte som till stor del sker elektroniskt, t.ex. de brottsbekämpande myndigheternas informationsutbyte med Interpol och Europol. Enligt utredningens mening har de sekretessbrytande bestämmelserna så nära samband med personuppgiftsbehandlingen att de hör hemma i registerförfattningarna. Det är också svårt att se att de har en naturlig plats i någon annan befintlig författning. De bör därför finnas kvar i registerförfattningarna.

En annan kategori är de bestämmelser som reglerar på vilket sätt personuppgifter får tillhandahållas. Hit hör naturligtvis reglerna om direktåtkomst. I flertalet registerförfattningar finns det också en bestämmelse som föreskriver att endast enstaka personuppgifter får lämnas ut på medium för automatiserad behandling. Även dessa bestämmelser har enligt utredningens mening sin naturliga plats i registerförfattningarna. De medverkar dessutom indirekt till dataskyddet, eftersom de begränsar möjligheten att tillhandahålla personuppgifter elektroniskt.

Den tredje kategorin är sådana bestämmelser som upplyser om att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter om att personuppgifter får behandlas för historiska, statistiska och vetenskapliga ändamål och om digital arkivering. Som utredningen utvecklar i avsnitt 5.5.2 och 5.5.3 bör även sådana bestämmelser finnas kvar i registerförfattningarna.

Ställningstagandet att registerförfattningarna även i fortsättningen bör reglera dessa frågor ligger i linje med att det i direktiven för utredningen framhålls att den nuvarande strukturen så långt möjligt bör behållas.

Ingen uttömmande reglering av uppgiftslämnande och sekretessgenombrott

Det kan anmärkas att sekretessbrytande bestämmelser finns både i offentlighets- och sekretesslagen (2009:400) och i andra författningar som också ska tillämpas av de myndigheter vilkas registerförfattningar ligger inom brottsdatalagens tillämpningsområde. Bestämmelserna i registerförfattningarna reglerar därmed inte uttömmande när sekretessen bryts.

Vissa bestämmelser som är sekretessbrytande syftar också till att ange till vem uppgifter får lämnas. Bestämmelser av det slaget finns även i andra författningar, både sådana som reglerar personuppgiftsbehandling inom brottsdatalagens tillämpningsområde och sådana som helt eller delvis ligger utanför tillämpningsområdet. I exempelvis förordningen (1999:1134) om belastningsregister finns det bestämmelser om uppgiftslämnande både för ändamål inom brottsdatalagens tillämpningsområde och utanför. Registerförfattningarna reglerar alltså inte uttömmande vilket uppgiftslämnande som är tillåtet.

5 Generella ändringar

5.1 Registerförfattningarna har likartat innehåll

De brottsbekämpande myndigheternas registerförfattningar är uppbyggda på samma sätt och har framför allt i de inledande kapitlen till stor del ett likartat innehåll. Det beror på att polisdatalagen har använts som mönster när nyare registerförfattningar har utformats. Eftersom registerförfattningarna har betydande likheter är behovet av ändringar i dem i stor utsträckning detsamma. Det finns därför anledning att i detta kapitel behandla de ändringar som är desamma för alla eller ett flertal av registerförfattningarna.

Kriminalvårdens registerlagstiftning skiljer sig visserligen till stora delar från övriga registerförfattningar, men även den innehåller vissa bestämmelser som liknar dem som finns i de övriga registerförfattningarna. När så är fallet behandlas även kriminalvårdens bestämmelser i detta kapitel.

Däremot behandlas domstolarnas registerlagstiftning inte här utan i kapitel 12. Utredningen föreslår där att en ny lag införs för domstolarnas personuppgiftsbehandling inom brottsdatalagens tillämpningsområde.

Säkerhetspolisens registerlagstiftning diskuteras inte heller i detta avsnitt. Utredningen återkommer till den i avsnitt 14 och 15.

En närmare beskrivning av registerförfattningarna finns i kapitel 3 i delbetänkandet (se SOU 2017:29 s. 91 f.).

5.2 En ny lagteknisk struktur

Utredningens förslag: Registerförfattningarna ska gälla utöver brottsdatalagen.

Skälen för utredningens förslag: Polisdatalagen, kustbevakningsdatalagen, åklagardatalagen, tullbrottsdatalagen och skattebrottsdatalagen gäller i stället för personuppgiftslagen (se exempelvis 2 kap. 1 § polisdatalagen). Lagen om behandling av personuppgifter inom kriminalvården har en annan struktur. I 2 § föreskrivs att om inte annat följer av lagen eller föreskrifter som har meddelats med stöd av den tillämpas personuppgiftslagen.

Enligt delbetänkandet bör registerförfattningarna gälla utöver brottsdatalagen (se SOU 2017:29 s. 141 f.). De registerförfattningar som i dag gäller i stället för personuppgiftslagen bör därför anpassas så att de gäller utöver brottsdatalagen. En bestämmelse som anger det bör tas in i respektive registerförfattning. Även Kriminalvårdens registerlagstiftning bör anpassas så att den gäller utöver brottsdatalagen i stället för utöver personuppgiftslagen.

I brottsdatalagen finns alla grundläggande bestämmelser om hur personuppgifter får behandlas. Där regleras också den personuppgiftsansvariges skyldigheter, enskildas rättigheter och tillsynen över personuppgiftsbehandling. Brottsdatalagen innehåller vidare bestämmelser om administrativa sanktionsavgifter, skadestånd och rättsmedel. Där anges också vad som gäller för överföring av personuppgifter till tredjeland. Att registerförfattningarna föreslås gälla utöver brottsdatalagen innebär att de framför allt bör innehålla bestämmelser som innebär preciseringar, undantag eller avvikelser från bestämmelserna i brottsdatalagen. Det innebär vidare att de bestämmelser som finns i registerförfattningarna ska läsas tillsammans med regleringen i brottsdatalagen. Det kan vara fråga om bestämmelser som t.ex. preciserar vilka särskilda krav som gäller vid behandling av en viss typ av personuppgifter eller hur länge en viss typ av personuppgifter får behandlas. Det kan även finnas bestämmelser som inskränker möjligheten att behandla vissa personuppgifter.

En konsekvens av att en registerförfattning gäller utöver brottsdatalagen är att tillämparen inte kan nöja sig med att ta del av registerförfattningens reglering utan också måste tolka bestämmelserna

i registerförfattningen i ljuset av regleringen i brottsdatalagen. Om formuleringen av en bestämmelse i en registerförfattning t.ex. medger två olika tolkningar, men bara den ena av dem är förenlig med regleringen i brottsdatalagen, är det den tolkningen som gäller.

I en författning som gäller utöver en annan upprepas inte bestämmelserna i den överordnade författningen, utom i de fall där det är nödvändigt för förståelsen av en bestämmelse i den förstnämnda författningen. Inte heller görs det hänvisningar till bestämmelserna i den överordnade författningen om det inte är absolut nödvändigt för sammanhanget. En författning som gäller utöver en annan ställer därför särskilda krav på tillämparen.

5.3 Bestämmelser som inte längre behövs

5.3.1 Hänvisningar till personuppgiftslagen

Utredningens förslag: Alla hänvisningar till personuppgiftslagen i registerförfattningarna ska upphävas.

Skälen för utredningens förslag

Några hänvisningar till personuppgiftslagen ska inte finnas

Dataskyddsutredningen föreslår att personuppgiftslagen ska upphöra att gälla den 25 maj 2018, då dataskyddsförordningen ska börja tillämpas (se SOU 2017:39 s. 78 f.). I 2 kap. 2 § polisdatalagen, 2 kap. 2 § kustbevakningsdatalagen, 2 kap. 2 § åklagardatalagen, 2 kap. 2 § tullbrottsdatalagen och 2 kap. 2 § skattebrottsdatalagen räknas det upp vilka paragrafer i personuppgiftslagen som ska tillämpas när personuppgifter behandlas enligt respektive lag. I lagen om behandling av personuppgifter inom kriminalvården finns det inte någon motsvarande uppräkningslista. Däremot föreskrivs i 8 § att bestämmelserna i personuppgiftslagen om rättelse och skadestånd gäller även vid behandling av personuppgifter enligt kriminalvårdens registerförfattning. Det finns även andra bestämmelser i den lagen som hänvisar till personuppgiftslagen.

Brottsdatalagen innehåller en för de behöriga myndigheterna gemensam reglering av all personuppgiftsbehandling som utförs i

syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet. När brottsdatalagen införs och personuppgiftslagen upphör att gälla bör det inte längre finnas några hänvisningar till personuppgiftslagen i registerförfattningarna. Sådana bestämmelser bör därför upphävas.

Vissa hänvisningar ska inte ersättas

Alla de hänvisningar till personuppgiftslagen som räknas upp i nyss nämnda bestämmelser har inte någon motsvarighet i brottsdatalagen. Hit hör bestämmelsen i 8 § första stycket personuppgiftslagen om förhållandet till offentlighetsprincipen. Som framgår av delbetänkandet regleras den frågan fortsättningsvis i dataskyddsförordningen, varför det inte bör finnas några bestämmelser om förhållandet till offentlighetsprincipen vare sig i brottsdatalagen eller i registerförfattningarna (se SOU 2017:29 s. 179 f.).

Det gäller också kravet i 42 § personuppgiftslagen på upplysningar till allmänheten om sådana behandlingar som inte ska anmälas till tillsynsmyndigheten. Det finns inte längre något behov av en sådan bestämmelse, eftersom varken direktivet eller brottsdatalagen föreskriver någon motsvarande anmälningsskyldighet.

Användningen av personnummer

I 22 § personuppgiftslagen, som registerförfattningarna hänvisar till, föreskrivs det att personnummer och samordningsnummer bara får behandlas utan samtycke när det är klart motiverat bl.a. med hänsyn till ändamålet med behandlingen och vikten av en säker identifiering. Bestämmelsen om behandling av personnummer och liknande identifieringsuppgifter har ingen motsvarighet i direktivet. Myndigheter som behöver behandla personnummer och liknande identifieringsuppgifter som ett led i sin verksamhet kan göra det i dag i syfte att fastställa en säker identitet. Utredningen ser inte något behov av att införa en generell bestämmelse som motsvarar 22 § personuppgiftslagen, eftersom kraven på en säker identifiering väger särskilt tungt i verksamhet inom brottsdatalagens tillämpningsområde och användningen av personnummer och

liknande identitetsuppgifter därmed nära nog alltid är motiverad. En sådan bestämmelse skulle därför inte fylla någon praktisk funktion för att skydda enskildas integritet. I viss verksamhet kan dock en sådan reglering vara motiverad (se avsnitt 12.4.4).

Undantaget från informationsskyldighet vid ljud och bild

Enligt 23 § personuppgiftslagen ska den personuppgiftsansvarige självant informera den registrerade om behandling av personuppgifter som samlas in från den registrerade själv. I 2 kap. 2 § tredje stycket polisdatalagen, 2 kap. 2 § tredje stycket kustbevakningsdatalagen och 2 kap. 2 § tredje stycket tullbrottsdatalagen görs undantag från den informationsskyldigheten vid behandling av personuppgifter genom bilder eller ljud och i samband med larm, om det med hänsyn till omständigheterna inte finns tid att informera. Motsvarande undantag för behandling genom bilder eller ljud görs i 2 kap. 2 § tredje stycket skattebrottsdatalagen.

I brottsdatalagen finns det ingen motsvarighet till informationsskyldigheten i 23 § personuppgiftslagen. I 4 kap. 2 § brottsdatalagen föreskrivs däremot att den registrerade ska informeras i specifika fall om det behövs för att han eller hon ska kunna ta tillvara sina rättigheter (se SOU 2017:29 s. 378 f.).

Enligt utredningens uppfattning fråntas den registrerade inte möjligheten att ta tillvara sina rättigheter om han eller hon inte informeras om att han eller hon förekommer i en bild- eller ljudupptagning som har tillkommit i annat syfte än att samla in personuppgifter om den registrerade (jfr Integritet och effektivitet i polisens brottsbekämpande verksamhet, prop. 2009/10:85, s. 86 och 314). Det kan t.ex. vara fråga om bilder från en brottsplats eller från en demonstration med våldsinslag eller en filmsekvens från ett oljeutsläpp. Värdet av att informera den enskilde i sådana situationer kan ifrågasättas (jfr Kustbevakningsdatalag, prop. 2011/12:45, s. 81). Detsamma gäller information i samband med larm. De som larmar får anses känna till att deras personuppgifter registreras. Det innebär att det inte behövs någon information för att den registrerade ska kunna ta tillvara sina rättigheter.

Utredningen anser att det i dessa båda fall inte rör sig om sådana specifika fall som avses i 4 kap. 2 § brottsdatalagen. Myndigheten är

då enligt direktivet inte skyldig att informera den registrerade. Det innebär att det nuvarande undantaget från informationsskyldigheten inte längre fyller någon funktion och därför bör tas bort.

5.3.2 Hänvisningar till 2013 års lag

Utredningens förslag: Bestämmelser som hänvisar till 2013 års lag ska upphävas.

Skälen för utredningens förslag: Utredningen föreslår i delbetänkandet att lagen (2013:329) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen (2013 års lag) ska upphävas när brottsdatalagen träder i kraft (se SOU 2017:29 s. 145 f.). I 2 a § lagen om behandling av personuppgifter inom kriminalvården, 1 kap. 5 § polisdatalagen, 1 kap. 2 a § kustbevakningsdatalagen, 1 kap. 3 § åklagardatalagen, 1 kap. 3 § andra stycket tullbrottsdatalagen och 1 kap. 3 § skattebrottsdatalagen hänvisas till att bestämmelserna i 2013 års lag, och i föreskrifter som har meddelats i anslutning till den lagen, ska tillämpas i stället för bestämmelserna i respektive författning. Som en konsekvens av att 2013 års lag upphävs bör alla hänvisningar till den lagen upphävas. Utredningen återkommer till frågan i avsnitt 17.5, eftersom det finns hänvisningar till 2013 års lag i ytterligare några författningar.

5.3.3 Syftet med lagarna

Utredningens förslag: Bestämmelser som beskriver syftet med respektive registerförfattning ska upphävas.

Skälen för utredningens förslag: Enligt 1 kap. 1 § första stycket brottsdatalagen är syftet med lagen dels att skydda fysiska personers grundläggande fri- och rättigheter i samband med behandling av personuppgifter, dels att säkerställa att behöriga myndigheter kan behandla och utbyta personuppgifter med varandra på ett ändamålsenligt sätt (se SOU 2017:29 s. 144).

I 1 kap. 1 § polisdatalagen, 1 kap. 1 § kustbevakningsdatalagen, 1 kap. 1 § åklagardatalagen, 1 kap. 1 § tullbrottsdatalagen och 1 kap. 1 § skattebrottsdatalagen anges det övergripande syftet med respektive lag. Exempelvis anges i 1 kap. 1 § polisdatalagen att syftet med lagen är att ge polisen möjlighet att behandla personuppgifter på ett ändamålsenligt sätt i sin brottsbekämpande verksamhet och skydda människor mot att deras personliga integritet kränks vid sådan behandling. Brottsdatalagen kommer att tillämpas av alla myndigheter som behandlar personuppgifter inom lagens tillämpningsområde. Den dubbla målsättningen med lagen – att stärka integritetsskyddet och att samtidigt värna om att behöriga myndigheter kan behandla personuppgifter på ett ändamålsenligt sätt – gäller således oavsett om det är t.ex. Polismyndigheten eller Kustbevakningen som behandlar personuppgifter. Det finns då inte skäl att i registerförfattningarna behålla bestämmelser som anger att syftet med lagen i stort sett är detsamma som det övergripande syftet med brottsdatalagen. De bör därför upphävas. Som framgår av avsnitt 5.2 ska registerförfattningarna läsas tillsammans med brottsdatalagen. Att syftet inte framgår direkt av var och en av registerförfattningarna innebär därför inte att integritetsskyddet försvagas.

5.3.4 Automatiserad behandling

Utredningens förslag: Bestämmelser om att registerförfattningarna endast gäller vid behandling av personuppgifter som är automatiserad eller på annat sätt strukturerad ska upphävas.

Skälen för utredningens förslag: Enligt 1 kap. 3 § brottsdatalagen gäller lagen för sådan behandling av personuppgifter som är helt eller delvis automatiserad och för annan behandling av personuppgifter som ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier (se SOU 2017:29 s. 173 f.).

I 1 § andra stycket lagen om behandling av personuppgifter inom kriminalvården, 1 kap. 2 § andra stycket polisdatalagen, 1 kap. 2 § andra stycket kustbevakningsdatalagen, 1 kap. 2 § första stycket åklagardatalagen, 1 kap. 2 § tullbrottsdatalagen och 1 kap. 2 § skat-

tebrottsdatalagen finns det bestämmelser med motsvarande innehåll. Det finns inte något behov av att i registerförfattningarna upprepa att de i huvudsak gäller för automatiserad behandling. Sådana bestämmelser bör därför upphävas.

5.3.5 Bestämmelser om lagarnas uppbyggnad

Utredningens förslag: Bestämmelser om hur registerförfattningarna är uppbyggda eller var en viss typ av bestämmelser finns ska som huvudregel upphävas.

Skälen för utredningens förslag: I 1 kap. 7 § polisdatalagen, 1 kap. 5 § kustbevakningsdatalagen, 1 kap. 5 § tullbrottsdatalagen och 1 kap. 5 § skattebrottsdatalagen anges hur respektive lag är uppbyggd. När polisdatalagen infördes såg lagstiftaren ett behov av att tydliggöra hur lagens olika kapitel förhöll sig till varandra, hur de skulle tillämpas och av vem. Den regleringen har senare använts som mönster för de övriga registerförfattningarna. Genom att brottsdatalagen innehåller den generella regleringen för de behöriga myndigheterna kommer åtskilliga bestämmelser i registerförfattningarna inte längre att behövas. Tillämpningsområdet för flera av lagarna ändras också på det sättet att bestämmelser om behandling av personuppgifter för andra syften än de som anges i brottsdatalagen rensas bort. Behovet av bestämmelser om lagarnas uppbyggnad minskar till följd av dessa ändringar. Det bör därför inte finnas bestämmelser om hur lagarna är uppbyggda, om det inte finns särskilda skäl för det (se avsnitt 7.2.3).

I polisdatalagen och kustbevakningsdatalagen finns det bestämmelser om bevarande och gallring i olika kapitel. Lagarna innehåller därför – för att skapa en överblick – bestämmelser som anger var i lagen bevarande och gallring regleras (se 2 kap. 12 § och 3 kap. 9 § polisdatalagen och 3 kap. 4 § kustbevakningsdatalagen). En annan lagstiftningsteknik används i tullbrottsdatalagen och skattebrottsdatalagen, där alla bestämmelser om bevarande och gallring är samlade i ett särskilt kapitel. Där inleds i stället kapitlet med en bestämmelse som presenterar innehållet.

Utredningen anser som utvecklas i avsnitt 5.5.1 att bestämmelser om bevarande och gallring som huvudregel bör hållas samman.

Därmed finns det inte längre behov av bestämmelser som tydliggör var i lagen sådana frågor regleras, varför de bör upphävas.

5.3.6 Personuppgiftsombud

Utredningens förslag: Bestämmelser i registerförfattningarna om att de personuppgiftsansvariga ska utse personuppgiftsombud ska upphävas.

Skälen för utredningens förslag: Enligt 3 kap. 13 § brottsdatalagen ska personuppgiftsansvariga utse ett eller flera dataskyddsombud. Den personuppgiftsansvarige ska anmäla till tillsynsmyndigheten både när ett dataskyddsombud utses och när ombudet entledigas (se SOU 2017:29 s. 340 f.).

I 2 kap. 5 § polisdatalagen, 2 kap. 5 § kustbevakningsdatalagen, 2 kap. 4 § åklagardatalagen, 2 kap. 4 § tullbrottsdatalagen och 2 kap. 4 § skattebrottsdatalagen föreskrivs skyldighet att utse ett eller flera personuppgiftsombud och att anmäla till tillsynsmyndigheten när ett sådant ombud utses eller entledigas. I och med att det i brottsdatalagen finns en generell bestämmelse om skyldighet att utse dataskyddsombud (som är den benämning som används i stället för personuppgiftsombud) behövs inga sådana bestämmelser i registerförfattningarna. Bestämmelserna om att personuppgiftsombud ska utses bör därför upphävas.

5.3.7 Behandling för diarietföring

Utredningens förslag: Bestämmelser i registerförfattningarna om att personuppgifter får behandlas om det är nödvändigt för diarietföring eller för att utföra andra nödvändiga handläggningsåtgärder ska upphävas.

Skälen för utredningens förslag: Enligt 2 kap. 2 § brottsdatalagen får personuppgifter alltid behandlas om det är nödvändigt för diarietföring. Personuppgifter får också behandlas om uppgifterna har lämnats till en behörig myndighet i en anmälan, ansökan eller lik-

nande och behandlingen är nödvändig för myndighetens handläggning (se SOU 2017:29 s. 239 f.).

I 2 kap. 9 § polisdatalagen, 2 kap. 6 § kustbevakningsdatalagen, 2 kap. 7 § åklagardatalagen, 2 kap. 7 § tullbrottsdatalagen och 2 kap. 7 § skattebrottsdatalagen föreskrivs att personuppgifter får behandlas om det är nödvändigt för diarieföring eller om uppgifterna har lämnats till myndigheten i en anmälan eller liknande och behandlingen är nödvändig för handläggningen. Eftersom brottsdatalagen innehåller en motsvarande bestämmelse finns det inte något skäl att behålla bestämmelserna i registerförfattningarna. De bör därför upphävas.

5.3.8 Behandling av känsliga personuppgifter

Utredningens förslag: Bestämmelser i registerförfattningarna om behandling av känsliga personuppgifter och användning av känsliga personuppgifter som sökbegrepp ska upphävas. Det gäller även bestämmelser om att uppgifter som beskriver en persons utseende ska utformas på ett objektivt sätt med respekt för människovärdet.

Skälen för utredningens förslag

Känsliga personuppgifter

I 2 kap. 11 och 12 §§ brottsdatalagen finns det bestämmelser om känsliga personuppgifter. I 2 kap. 11 § föreskrivs att personuppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening eller som rör hälsa, sexualliv eller sexuell läggning inte får behandlas. Om uppgifter om en person behandlas får de dock kompletteras med känsliga personuppgifter när det är absolut nödvändigt för ändamålet med behandlingen. Enligt 2 kap. 12 § brottsdatalagen får biometriska uppgifter som används för att identifiera en person och genetiska uppgifter behandlas endast om det är särskilt föreskrivet och det är absolut nödvändigt för ändamålet med behandlingen. Att biometriska uppgifter som används för att identifiera en person och genetiska uppgifter ingår i uppräkningslistan av känsliga person-

uppgifter har sin grund i direktivet. Detsamma gäller uppgifter om sexuell läggning, även om de redan tidigare som regel har betraktats som känsliga personuppgifter (se SOU 2017:29 s. 264 f.).

I 5 § lagen om behandling av personuppgifter inom kriminalvården, 2 kap. 10 § polisdatalagen, 2 kap. 8 § åklagardatalagen, 2 kap. 7 § kustbevakningsdatalagen, 2 kap. 10 § tullbrottsdatalagen och 2 kap. 8 § skattebrottsdatalagen finns det bestämmelser om behandling av känsliga personuppgifter. Eftersom behandling av känsliga personuppgifter regleras i brottsdatalagen, finns det inte skäl att behålla motsvarande generella regler i registerförfattningarna. De bör därför upphävas.

I avsnitt 5.3.7 föreslår utredningen att de allmänna bestämmelserna i registerförfattningarna om behandling för diarieföring ska upphävas. Enligt 2 kap. 13 § brottsdatalagen, som hänvisar till 2 kap. 2 §, får även känsliga personuppgifter behandlas om det är nödvändigt för diarieföring. Detsamma gäller om uppgifterna har lämnats till en behörig myndighet i en anmälan, ansökan eller liknande och behandlingen är nödvändig för myndighetens handläggning (se SOU 2017:29 s. 271 f.).

I 2 kap. 10 § andra stycket polisdatalagen, 2 kap. 7 § andra stycket kustbevakningsdatalagen, 2 kap. 8 § andra stycket åklagardatalagen, 2 kap. 10 § andra stycket tullbrottsdatalagen och 2 kap. 8 § andra stycket skattebrottsdatalagen finns det motsvarande bestämmelser om att känsliga personuppgifter får behandlas för diarieföring eller andra nödvändiga handläggningsuppgifter. Det finns inte anledning att behålla dessa bestämmelser, eftersom det finns en motsvarande reglering i brottsdatalagen. Bestämmelserna i registerförfattningarna bör därför upphävas.

Uppgifter som beskriver en persons utseende

I 2 kap. 7 § andra stycket brottsdatalagen föreskrivs att uppgifter som beskriver en persons utseende ska utformas på ett objektivt sätt med respekt för människovärdet (se SOU 2017:29 s. 259). Bestämmelsen har placerats tillsammans med reglerna om personuppgifters kvalitet i stället för i anslutning till bestämmelserna om behandling av känsliga personuppgifter, eftersom den gäller obero-

ende av om uppgifterna om utseende är känsliga personuppgifter eller inte.

I 2 kap. 10 § tredje stycket polisdatalagen, 2 kap. 7 § tredje stycket kustbevakningsdatalagen, 2 kap. 8 § tredje stycket åklagardatalagen, 2 kap. 10 § tredje stycket tullbrottsdatalagen och 2 kap. 8 § tredje stycket skattebrottsdatalagen finns det bestämmelser med motsvarande innehåll. Eftersom det i brottsdatalagen finns en bestämmelse om hur uppgifter om personers utseende ska utformas behöver det inte regleras i registerförfattningarna. Bestämmelser om det bör således upphävas.

Registerförfattningarna ska inte längre innehålla sökförbud

I 2 kap. 14 § brottsdatalagen föreskrivs ett generellt förbud mot att utföra sökningar i syfte att få fram ett personurval grundat på känsliga personuppgifter.

Enligt 3 kap. 5 § polisdatalagen, 4 kap. 4 § kustbevakningsdatalagen, 3 kap. 4 § åklagardatalagen, 3 kap. 5 § tullbrottsdatalagen och 3 kap. 5 § skattebrottsdatalagen får känsliga personuppgifter inte användas som sökbegrepp vid sökning i personuppgifter som gjorts gemensamt tillgängliga. Något motsvarande sökförbud finns inte för uppgifter som endast ett fåtal har tillgång till. Enligt 5 § tredje stycket lagen om behandling av personuppgifter inom kriminalvården får känsliga personuppgifter inte användas som sökbegrepp om inte regeringen har föreskrivit det.

Mot bakgrund av att brottsdatalagen innehåller ett generellt sökförbud behövs inte längre bestämmelserna i registerförfattningarna om användning av känsliga personuppgifter som sökbegrepp. De bör därför upphävas. Detsamma bör gälla 5 § tredje stycket lagen om behandling av personuppgifter inom kriminalvården och de bestämmelser om användning av känsliga personuppgifter som sökbegrepp som finns i tillhörande förordning.

Utredningen återkommer i kapitlen om de olika registerförfattningarna till frågan om det behövs undantag från sökförbudet i brottsdatalagen.

5.3.9 Tillgången till personuppgifter

Utredningens förslag: Bestämmelser i registerförfattningarna om tillgången till personuppgifter ska upphävas. Det gäller även bestämmelser om att regeringen eller den myndighet som regeringen bestämmer har rätt att meddela föreskrifter om det.

Generella bestämmelser om vad den personuppgiftsansvarige ska beakta när tillgång ges till personuppgifter och om att det ska finnas rutiner för tilldelning, förändring, borttagning och regelbunden uppföljning av behörighet för åtkomst till personuppgifter ska tas in i brottsdataförordningen. De ska ersätta motsvarande bestämmelser i registerförordningarna.

Skälen för utredningens förslag

Tillgången till personuppgifter bör enbart regleras i brottsdatalagen

Enligt 3 kap. 6 § brottsdatalagen ska den personuppgiftsansvarige se till att tillgången till personuppgifter begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter (se SOU 2017:29 s. 311 f.). Enligt 3 kap. 23 § 2 brottsdatalagen kan regeringen eller den myndighet som regeringen bestämmer meddela föreskrifter om tillgången till personuppgifter.

I 2 kap. 11 § polisdatalagen, 2 kap. 3 § kustbevakningsdatalagen, 2 kap. 9 § åklagardatalagen, 2 kap. 11 § tullbrottsdatalagen och 2 kap. 10 § skattebrottsdatalagen föreskrivs att tillgången till personuppgifter ska begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter. Bestämmelserna kompletteras av en möjlighet för regeringen, eller den myndighet som regeringen bestämmer, att meddela närmare föreskrifter om tillgången till personuppgifter. I bestämmelser om direktåtkomst i nämnda lagar föreskrivs det att den mottagande myndigheten ansvarar för att tillgången till personuppgifter begränsas på motsvarande sätt (se t.ex. 3 kap. 8 § andra stycket polisdatalagen). Likartade bestämmelser finns i 6 och 10 §§ lagen om behandling av personuppgifter inom kriminalvården.

Eftersom det finns en generellt tillämplig bestämmelse i brottsdatalagen som föreskriver att tillgången till personuppgifter ska begränsas, finns det inte något behov av att behålla motsvarande be-

stämmelser i registerförfattningarna. Det gäller även bestämmelser om begränsning av tillgången till personuppgifter vid direktåtkomst. I registerförfattningarna bör det inte heller finnas några bestämmelser om föreskriftsrätt om tillgången till personuppgifter, eftersom det är fråga om interna förhållanden i myndigheterna (se avsnitt 5.7).

Nya generella bestämmelser i brottsdataförordningen

I 3 § polisdataförordningen (2010:1155) föreskrivs att Polismyndigheten och Säkerhetspolisen får meddela närmare föreskrifter om tillgången till personuppgifter för sina respektive verksamhetsområden. För tilldelning av behörighet för åtkomst till personuppgifter ska det särskilt beaktas att det, utöver behovet av uppgifterna, ställs krav på utbildning och erfarenhet. I 3 § kustbevakningsdataförordningen (2012:146), 2 § åklagardataförordningen (2015:575), 3 § tullbrottsdataförordningen (2017:450) och 3 § skattebrottsdataförordningen (2017:458) finns motsvarande bestämmelser.

Enligt 4 § polisdataförordningen ansvarar Polismyndigheten och Säkerhetspolisen för att det inom respektive myndighet finns rutiner för tilldelning, förändring, borttagning och regelbunden uppföljning av behörigheter för åtkomst till personuppgifter. Motsvarande bestämmelser finns i 4 § kustbevakningsdataförordningen, 3 § åklagardataförordningen, 4 § tullbrottsdataförordningen och 4 § skattebrottsdataförordningen.

De nu aktuella bestämmelserna är av den arten att de enligt utredningens mening bör gälla generellt inom brottsdatalagens tillämpningsområde. Bestämmelser med den innebörden bör därför tas in i brottsdataförordningen och bestämmelserna i registerförfattningarna bör upphävas. Myndigheterna bör dock inte ha någon föreskriftsrätt på området, eftersom det enbart rör sig om interna förhållanden som kan regleras på annat sätt än i föreskrifter (se avsnitt 5.7).

5.3.10 Särskilda upplysningar

Utredningens förslag: Registerförfattningarna ska inte innehålla bestämmelser som motsvarar brottsdatalagens bestämmelser om särskilda upplysningar. Bestämmelser om att vissa personuppgifter ska förse med särskilda upplysningar ska dock finnas kvar för uppgifter som behandlas i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet.

Bestämmelserna om särskilda upplysningar ska liksom i dag enbart gälla vid behandling av personuppgifter som har gjorts gemensamt tillgängliga.

Skälen för utredningens förslag

Bestämmelser om särskilda upplysningar

Enligt 2 kap. 3 § andra stycket brottsdatalagen ska det ändamål som personuppgifter behandlas för tydliggöras genom en särskild upplysning, om det inte framgår av sammanhanget eller på annat sätt. I 2 kap. 9 § brottsdatalagen föreskrivs att personuppgifter som rör olika kategorier av registrerade så långt det är möjligt ska särskiljas, t.ex. personer som är misstänkta eller dömda för brott, brottsoffer eller andra som berörs av ett brott. Om det inte framgår av sammanhanget eller på annat sätt vilken kategori personen tillhör, ska det tydliggöras genom en särskild upplysning. Enligt 2 kap. 10 § brottsdatalagen ska vidare personuppgifter som grundar sig på fakta så långt det är möjligt skiljas från personuppgifter som grundar sig på personliga bedömningar. Om grunden inte framgår av sammanhanget eller på något annat sätt ska den tydliggöras genom en särskild upplysning (se SOU 2017:29 s. 260 f.).

I flera av registerförfattningarna föreskrivs att det i vissa fall ska lämnas särskilda upplysningar. Bestämmelser om särskilda upplysningar, med något olika innehåll, finns i 3 kap. 3 och 4 §§ polisdatalagen, 4 kap. 2 och 3 §§ kustbevakningsdatalagen, 3 kap. 3 § åklagardatalagen, 3 kap. 3 och 4 §§ tullbrottsdatalagen och 3 kap. 3 och 4 §§ skattebrottsdatalagen. De särskilda upplysningarna ska avse att personen i fråga inte är misstänkt vare sig för brott eller för att utöva brottslig verksamhet. I fråga om den som är misstänkt för att utöva eller att komma att utöva brottslig verksamhet ska de sär-

skilda upplysningarna belysa uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak. Det ska också finnas en särskild upplysning om ändamålet med behandlingen, om det inte framgår på annat sätt. Bestämmelserna om särskilda upplysningar gäller endast för personuppgifter som har gjorts gemensamt tillgängliga.

Upplysningar om ändamålet med behandlingen

Registerförfattningarna bör inte innehålla bestämmelser som motsvarar brottsdatalagens krav på att ändamålet med behandlingen ska framgå. Bestämmelser som ställer upp sådana krav bör därför upphävas.

Särskilda upplysningar bara om uppgifterna är gemensamt tillgängliga

I delbetänkandet konstaterar utredningen att det kan finnas skäl att i registerförfattningarna fortsatt göra undantag från bestämmelserna om särskilda upplysningar för personuppgifter som inte har gjorts gemensamt tillgängliga (se SOU 2017:29 s. 262).

Behovet av särskilda upplysningar gör sig framför allt gällande om personuppgifter behandlas utanför sitt ursprungliga sammanhang. I förarbetena till polisdatalagen diskuteras ingående skälen för att ha sådana bestämmelser och när särskilda upplysningar inte behövs (se prop. 2009/10:85 s. 145 f.). Utredningen anser att det inte finns behov av särskilda upplysningar när det integritetsskydd som de särskilda upplysningarna syftar till att skapa tillgodoses på annat sätt, t.ex. genom att det fåtal personer som behandlar uppgifterna är införstådda med varför det görs. Det finns också anledning att erinra om att direktivets krav på särskilda upplysningar beträffande vilken kategori en person tillhör och beträffande att fakta ska skiljas från personliga bedömningar bara gäller så långt det är möjligt att lämna sådan information. Det innebär att man varit väl införstådd med att sådana upplysningar inte alltid kommer att finnas. Det finns därför möjlighet att göra undantag från de kraven.

Kravet i 2 kap. 3 § andra stycket brottsdatalagen att ändamålet med behandlingen ska framgå följer inte av direktivet utan skapar ett sådant extra skydd för enskildas integritet som direktivet med-

ger att nationell rätt får innehålla. Det finns därför även möjlighet att göra undantag från det kravet.

Bestämmelserna om särskilda upplysningar bör mot den bakgrunden på samma sätt som i dag enbart gälla vid behandling av personuppgifter som har gjorts gemensamt tillgängliga.

För de behöriga myndigheter som inte har en reglering som gör skillnad mellan uppgifter som har gjorts gemensamt tillgängliga och andra uppgifter kommer bestämmelserna i brottsdatalagen om särskilda upplysningar att gälla utan undantag. Det kan förefalla som om det därmed ställs högre krav på de myndigheter som i dag överhuvudtaget inte behöver förse personuppgifter med särskilda upplysningar, medan de myndigheter som har en sådan reglering får undantag från kraven i brottsdatalagen. Enligt brottsdatalagen ska personuppgifter förse med särskilda upplysningar bara om det förhållande som upplysningen skulle avse inte framgår av sammanhanget eller på något annat sätt. Som utredningen konstaterar i delbetänkandet är det framför allt i det inledande skedet av en förundersökning och i underrättelseverksamhet som det kan vara otvetydigt vilken roll en person har och varför uppgifter om honom eller henne behandlas (se SOU 2017:29 s. 261). När det gäller andra myndigheter än de brottsbekämpande kommer det därför normalt inte att krävas några särskilda upplysningar och då finns det inte heller skäl att ha något undantag.

Upplysningar om vilken kategori en person tillhör

I brottsdatalagen ställs det delvis andra krav på särskilda upplysningar än i registerförfattningarna. Sådana bestämmelser i registerförfattningarna som innebär att det genom en särskild upplysning ska framgå att en viss person inte är misstänkt täcks, såvitt gäller brottsutredande och lagförande verksamhet, av regleringen i 2 kap. 9 § brottsdatalagen. Det finns därför inte skäl att i registerförfattningarna behålla bestämmelser som föreskriver att det ska framgå att en person inte är misstänkt för brott.

Det väcker frågan hur man ska se på det förhållandet att begreppet misstänkt används i registerförfattningarna även om personer vilkas uppgifter behandlas i underrättelseverksamhet, trots att regelverket i övrigt förutsätter att ett konkret brott har begåtts för

att någon ska kunna betecknas som misstänkt. Misstänkt används i detta sammanhang för att skilja ut personer som kan ha direkt samband med den brottsliga verksamheten från andra (se t.ex. 3 kap. 4 § polisdatalagen och 3 kap. 4 § tullbrottsdatalagen). Författningsregleringen av underrättelseverksamhet är mycket begränsad och har inte en sådan tydlig uppdelning mellan olika kategorier av personer som regleringen i rättegångsbalken. Utredningen anser att det är minst lika viktigt ur integritetssynpunkt att det i underrättelseverksamheten görs tydlig skillnad mellan personer som har ett direkt samband med den brottsliga verksamheten och andra personer som i annan verksamhet. Mot den bakgrunden bör det nuvarande kravet i registerförfattningarna på särskilda upplysningar i fråga om nu aktuella kategorier behållas.

Användningen av begreppet misstänkt i det sammanhanget kritiserades av Lagrådet när polisdatalagen infördes. Regeringen valde ändå att behålla det under hänvisning till tidigare lagstiftning på området (se prop. 2009/10:85 s. 150 och 522). Även om det kan diskuteras om det är lämpligt att använda uttrycket misstänkt avseende brottslighet som inte är så konkret att brotten kan individualiseras anser utredningen att det är så inarbetat att det inte bör ändras.

Särskilda upplysningar om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak

När det gäller bestämmelsen i 2 kap. 10 § brottsdatalagen, som föreskriver att fakta ska skiljas från personliga bedömningar och att det ska anges genom en särskild upplysning om det inte framgår på annat sätt, kan det ifrågasättas om det går att dra en parallell med de bestämmelser som i dag finns i registerförfattningarna. Det är framför allt beträffande uppgifter som behandlas i underrättelseverksamhet som det enligt 3 kap. 4 § polisdatalagen, 4 kap. 3 § kustbevakningsdatalagen, 3 kap. 4 § tullbrottsdatalagen och 3 kap. 4 § skattebrottsdatalagen krävs särskilda upplysningar om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak. Sådana bestämmelser preciserar enligt utredningens mening vilka upplysningar som krävs i fråga om personuppgifter som behandlas i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet. Utredningen anser därför att de bestämmelser i registerförfattning-

arna som föreskriver att uppgifter om en person som kan antas ha samband med misstänkt brottslig verksamhet ska förse med en upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet bör behållas.

Det bör understrykas att upplysningar om en uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak inte bara är en fråga om dataskydd utan i minst lika stor utsträckning har betydelse för brottsbekämpningen. Utan sådana upplysningar ökar risken att felaktiga slutsatser dras om personers anknytning till brottslighet, vilket i sin tur kan leda till beslut och ingripanden riktade mot fel personer. Det ligger därför i myndigheternas eget intresse att det av uppgifter som görs gemensamt tillgängliga i underrättelseverksamhet framgår vilket värde som kan tillmätas dem. Det har emellertid framkommit att bestämmelserna i fråga anses vara svårtolkade och därför kan kräva förtydliganden.

En första fråga är om kravet på särskild upplysning bara gäller den person som har direkt samband med den misstänkta brottsliga verksamheten eller om det även gäller uppgifter om andra personer. Förarbetena är inte tydliga på den punkten och det finns omständigheter som kan anföras för båda tolkningarna. Enligt utredningens mening bör kravet på upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak endast avse uppgifter om den som antas utöva eller komma att utöva den brottsliga verksamheten. Eftersom det krav som gäller för anknytningen till den brottsliga verksamheten är mycket lågt ställt kan regleringen träffa betydligt fler personer än vad misstanke om ett konkret brott kan göra. Så snart det finns något som stöder ett antagande om att en person har direkt samband med brottslig verksamhet och det är fråga om uppgifter som görs gemensamt tillgängliga bör således enligt utredningens mening uppgifterna om personen förse med en särskild upplysning.

En andra fråga är vilka uppgifter om sådana personer som behöver förse med en särskild upplysning, eftersom det inte bör gälla alla upplysningar om personen i fråga. Enligt utredningens mening är det endast sådana uppgifter som belyser på vilket sätt personen är knuten till brottsligheten som bör förse med upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak. Det kan, förutom till anknytningen till den brottsliga verksamheten, t.ex. röra sig om uppgifter om brottslighetens art och omfatt-

ning. Uppgifter av det slaget kan behöva förses med särskilda upplysningar för att personens anknytning till brottsligheten ska kunna bedömas.

På samma sätt som i dag bör det göras undantag från kravet på särskild upplysning om det inte finns något behov av en sådan, därför att det framgår av sammanhanget vem som är uppgiftslämnare och hur trovärdig uppgiften är eller det av annat skäl är onödigt med en sådan upplysning. Om det t.ex. är fråga om uppgifter som hämtas från förundersökningar eller domar är en särskild upplysning som regel onödigt om källan framgår. Enligt förarbetena till polisdatalagen anses det vara onödigt att bedöma trovärdigheten om uppgiftslämnaren är en polisman. Detsamma bör gälla andra tjänstemän med brottsbekämpande uppgifter. Däremot kan det även i ett sådant fall behövas en upplysning om uppgiftens riktighet i sak, eftersom förutsättningarna för att göra en viss iakttagelse kan behöva belysas (se prop. 2009/10:85 s. 341).

Den nuvarande formuleringen av bestämmelserna innebär att det krävs särskild upplysning om det inte på grund av särskilda omständigheter är onödigt. Regleringen tolkas i dag, på grund av uttalanden i förarbetena, så att det nästan undantagslöst krävs särskilda upplysningar, eftersom det är oklart vilka särskilda omständigheter som kan föranleda avsteg från huvudregeln. Det kan ifrågasättas om en så restriktiv tillämpning har varit avsedd. Det kan därför finnas anledning att ändra regleringen något.

Enligt utredningens mening bör det ställas krav på särskilda upplysningar om det inte på grund av omständigheterna är onödigt. Med en sådan formulering undviker man den osäkerhet som kan finnas om vilken typ av omständigheter som kan göra behovet av särskilda upplysningar överflödigt. Om de samlade omständigheterna gör att trovärdigheten och riktigheten kan bedömas bör det vara tillräckligt.

5.3.11 Längsta tid för behandling

Utredningens förslag: Bestämmelser i registerförfattningarna om att personuppgifter inte får bevaras under längre tid än vad som behövs för något eller några av de ändamål som anges i respektive författning ska upphävas.

Skälen för utredningens förslag: Enligt 2 kap. 17 § första stycket brottsdatalagen får personuppgifter inte behandlas under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen (se SOU 2017:29 s. 284 f.).

I 7 § lagen om behandling av personuppgifter inom kriminalvården, 2 kap. 12 § polisdatalagen, 3 kap. 4 § kustbevakningsdatalagen, 2 kap. 10 § åklagardatalagen, 4 kap. 1 § tullbrottsdatalagen och 4 kap. 1 § skattebrottsdatalagen föreskrivs att personuppgifter inte får bevaras under längre tid än vad som behövs för något eller några av de ändamål som anges i respektive lag.

Generella bestämmelser om att personuppgifter inte får behandlas under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen bör upphävas, eftersom det finns en motsvarande reglering i brottsdatalagen. Utredningen återkommer till bestämmelserna om längsta tid för behandling i avsnitt 5.5.

5.3.12 Upplysning om regleringen i offentlighets- och sekretesslagen

Utredningens förslag: Hänvisningar i registerförfattningarna till att det finns bestämmelser om utlämnande i offentlighets- och sekretesslagen ska upphävas.

Skälen för utredningens förslag: I 2 kap. 19 § andra stycket och 5 kap. 9 § andra stycket polisdatalagen, 3 kap. 8 § andra stycket kustbevakningsdatalagen, 2 kap. 15 § andra stycket åklagardatalagen, 2 kap. 14 § andra stycket tullbrottsdatalagen och 2 kap. 13 § andra stycket skattebrottsdatalagen, som alla reglerar viss föreskriftsrätt, finns det hänvisningar till regleringen om utlämnande i offentlighets- och sekretesslagen. Bestämmelserna erinrar om att det även i offentlighets- och sekretesslagen finns bestämmelser om utlämnande. Syftet med bestämmelserna är enbart att klargöra att det i den lagen finns bestämmelser om utlämnande. Eftersom det finns bestämmelser om utlämnande också i andra författningar, exempelvis i tryckfrihetsförordningen, och hänvisningen är så generellt utformad fyller bestämmelserna i registerförfattningarna inte någon funktion. Bestämmelserna innehåller inte heller någon materiell reglering. De bör därför upphävas.

5.4 Behov av nya bestämmelser och anpassningar

5.4.1 Uppgifter om juridiska personer

Utredningens bedömning: Det är möjligt att i registerförfattningarna behålla bestämmelser som rör behandling av uppgifter om juridiska personer.

Utredningens förslag: Hänvisningar ska också göras till de bestämmelser i brottsdatalagen som motsvarar dem som i dag finns i registerförfattningarna och som är tillämpliga vid behandling av uppgifter om juridiska personer.

Skälen för utredningens bedömning och förslag: I 1 kap. 6 § polisdatalagen, 1 kap. 3 § kustbevakningsdatalagen, 1 kap. 4 § åklagardatalagen, 1 kap. 4 § tullbrottsdatalagen och 1 kap. 4 § skattebrottsdatalagen föreskrivs att vissa bestämmelser i författningarna även ska tillämpas på uppgifter om juridiska personer. Som anges i delbetänkandet gäller direktivet enbart till skydd för fysiska personer och tillämpningsområdet för brottsdatalagen har utformats med det som grund (se SOU 2017:29 s. 665).

En första fråga är om dataskyddsreformen bör leda till att bestämmelserna i registerförfattningarna om att de i vissa delar ska tillämpas på uppgifter om juridiska personer bör tas bort. Utredningen anser att det inte är nödvändigt. Det är visserligen allmänt sett inte lika angeläget att skydda uppgifter om juridiska personer som uppgifter om fysiska personer. Eftersom uppgifter om juridiska personer i många fall samtidigt är indirekta personuppgifter kan behovet av särskilda skyddsregler för uppgifter om juridiska personer diskuteras. I de fall där lagstiftaren har ansett att det finns goda skäl att ge visst skydd även för uppgifter om juridiska personer finns det enligt utredningens mening inte skäl att ta bort det skyddet. Bestämmelser om skydd för uppgifter om juridiska personer bör därför behållas.

Frågan är då om bestämmelserna enbart bör ta sikte på frågor som regleras i respektive registerförfattning, trots att vissa frågor som i dag regleras i registerförfattningarna och som ska tillämpas även på uppgifter om juridiska personer regleras i brottsdatalagen. Eftersom utredningen anser att dagens reglering bör behållas bör

en hänvisning göras till de bestämmelser i brottsdatalagen som motsvarar dem som i dag finns i registerförfattningarna och som är tillämpliga vid behandling av uppgifter om juridiska personer.

5.4.2 Administrativa sanktionsavgifter

Utredningens förslag: Sanktionsavgift ska få tas ut av den personuppgiftsansvarige vid överträdelse av vissa bestämmelser i registerförfattningarna. Det gäller överträdelse av bestämmelser om tillåtna rättsliga grunder för behandling av personuppgifter, särskilda upplysningar och längsta tid för behandling av personuppgifter.

Sanktionsavgiften ska vara minst 50 000 kronor och högst 20 000 000 kronor.

Skälen för utredningens förslag

Vilka överträdelser ska kunna föranleda sanktionsavgift?

Utredningen gör i delbetänkandet bedömningen att överträdelser av regler om personuppgiftsbehandling inte bör vara straffsanktionerade, utöver vad som redan följer av brottsbalkens regler (se SOU 2017:29 s. 492 f.). I stället föreslår utredningen att det införs möjlighet att ta ut administrativa sanktionsavgifter. Bestämmelser om det har tagits in i 6 kap. brottsdatalagen.

Sanktionsavgift kan enligt brottsdatalagen tas ut vid överträdelse av bestämmelser i den lagen. Om en bestämmelse i en registerförfattning ersätter, preciserar eller på annat sätt kompletterar en bestämmelse i brottsdatalagen som kan föranleda sanktionsavgift, bör även överträdelse av bestämmelsen i registerförfattningen kunna föranleda sanktionsavgift.

Av de skäl som redovisas i delbetänkandet bör emellertid inte alla överträdelser kunna leda till sanktionsavgift (se SOU 2017:29 s. 509 f.). De principer som utredningen anger där bör tillämpas även när det gäller överträdelser av bestämmelser i registerförfattningarna. Utredningen anser således att sanktionsavgift inte bör kunna tas ut vid överträdelse av bestämmelser som inte är dataskyddsbestämmelser, t.ex. sekretessbrytande bestämmelser.

Med dessa utgångspunkter bedömer utredningen att överträdelse av bestämmelser i de brottsbekämpande myndigheternas och kriminalvårdens registerförfattningar om tillåtna rättsliga grunder för behandling av personuppgifter och om längsta tid för behandling av personuppgifter bör kunna föranleda sanktionsavgift. Det samma bör gälla bestämmelser om särskilda upplysningar. Bestämmelser om när personuppgifter får göras gemensamt tillgängliga är visserligen mycket viktiga ur integritetssynpunkt, men enligt utredningens mening bör överträdelse av sådana bestämmelser inte kunna föranleda sanktionsavgift. Det beror på att det är fråga om tillämpning av bestämmelser som kräver bedömningar.

Det bör i respektive registerförfattning anges vilka överträdelser som kan föranleda sanktionsavgift.

Vad ska gälla för behandling av uppgifter om juridiska personer?

Utredningen gör i avsnitt 5.4.1 bedömningen att det är möjligt att i registerförfattningarna behålla bestämmelser om behandling av uppgifter om juridiska personer. Utredningen föreslår också att vissa bestämmelser i brottsdatalagen ska gälla vid sådan behandling. Överträdelse av vissa av de bestämmelser som föreslås vara tillämpliga på uppgifter om juridiska personer kan föranleda sanktionsavgift. Frågan är om det bör leda till att sanktionsavgift bör kunna tas ut även vid behandling av uppgifter om juridiska personer.

Bestämmelser som utvidgar tillämpningen av vissa bestämmelser till att gälla vid behandling av uppgifter om juridiska personer förstärker indirekt skyddet för fysiska personer, eftersom det kan vara svårt att skilja uppgifter om fysiska personer som är ägare av eller ställföreträdare för en juridisk person från uppgifter som enbart rör den juridiska personen. Det kan tala för att även överträdelser vid behandling av uppgifter om juridiska personer bör kunna föranleda sanktionsavgift. Å andra sidan är det inte lika angeläget att skydda uppgifter om juridiska personer som uppgifter om fysiska personer (jfr Domstolsdatalag, Ds 2013:10, s. 49 f.).

Sanktionsavgift är främst tänkt att utgöra en reaktion på sådan otillåten behandling av personuppgifter som riskerar att kränka den personliga integriteten, vilket talar för att inskränka tillämpningen till uppgifter om fysiska personer. Eftersom direktivet enbart skyd-

dar uppgifter om fysiska personer och bestämmelserna om sanktionsavgift har införts som en konsekvens av kravet på sanktioner i direktivet anser utredningen att det inte finns skäl att utsträcka möjligheten att ta ut sanktionsavgift till överträdelser som gäller behandling av uppgifter om juridiska personer. Omfattar behandlingen även uppgifter om fysiska personer kan sanktionsavgift tas ut för den överträdelsen om förutsättningarna för det är uppfyllda.

Hur hög bör sanktionsavgiften vara?

Enligt 6 kap. 3 § första och andra styckena brottsdatalagen ska sanktionsavgift tas ut med ett lägre belopp vid mindre allvarliga överträdelser och med ett högre belopp vid allvarligare överträdelser. Det framgår av paragrafen vilka överträdelser som är mindre allvarliga respektive allvarliga. Överträdelse av brottsdatalagens bestämmelser om tillåtna rättsliga grunder för behandling, särskilda upplysningar och längsta tid för behandling av personuppgifter är enligt paragrafen allvarliga överträdelser. Det bör gälla även vid överträdelse av motsvarande bestämmelser i registerförfattningarna. För att motsvara regleringen i brottsdatalagen bör sanktionsavgiften vara minst 50 000 kronor och högst 20 000 000 kronor. En bestämmelse som anger sanktionsavgiftens storlek bör finnas i var och en av registerförfattningarna.

Vem ska betala sanktionsavgift?

Den som är personuppgiftsansvarig ansvarar även för den behandling som ett personuppgiftsbiträde utför. I delbetänkandet konstaterar utredningen att sanktionsavgift bara ska kunna tas ut av personuppgiftsbiträden i de fall där biträdet brutit mot uttryckliga skyldigheter enligt brottsdatalagen (se SOU 2017:29 s. 504 f.). Eftersom registerförfattningarna inte innehåller några sådana skyldigheter för personuppgiftsbiträden bör sanktionsavgift för överträdelser av bestämmelser i registerförfattningarna endast kunna tas ut av personuppgiftsansvariga. Om ett personuppgiftsbiträde i strid med brottsdatalagen har bestämt ändamålen med och medlen för behandlingen är biträdet att anse som personuppgiftsansvarig för den behandlingen och sanktionsavgift kan då tas ut i samma ut-

sträckning som av en personuppgiftsansvarig (se 3 kap. 19 § andra stycket brottsdatalagen). Det kommer då att gälla även vid överträdelse av bestämmelser i en registerförfattning.

Brottsdatalagens handläggningsbestämmelser gäller

I brottsdatalagen finns det bestämmelser i 6 kap. 3 § tredje stycket, 4 och 5 §§ om hur sanktionsavgiften ska bestämmas och i 6 kap. 6 och 7 §§ om vad som gäller i fråga om beslut om sanktionsavgift. Registerförfattningarna föreslås i avsnitt 5.2 gälla utöver brottsdatalagen. Det innebär enligt utredningens mening att de handläggnings- och verkställighetsregler som finns i brottsdatalagen gäller även i de fall där sanktionsavgift tas ut för överträdelser av bestämmelser i registerförfattningarna. Några bestämmelser om handläggningen behövs därför inte i registerförfattningarna.

5.4.3 Skadestånd

Utredningens förslag: I registerförfattningarna ska det anges att bestämmelsen om skadestånd i brottsdatalagen ska tillämpas på motsvarande sätt när personuppgifter behandlas i strid med registerförfattningarna.

Skälen för utredningens förslag: Enligt 7 kap. 1 § brottsdatalagen ska den personuppgiftsansvarige ersätta den registrerade för den skada och kränkning av den personliga integriteten som personuppgiftsbehandling i strid med brottsdatalagen, eller föreskrifter som har meddelats i anslutning till den, har orsakat (SOU 2017:29 s. 532 f.).

I registerförfattningarna finns det inte några bestämmelser om skadestånd. I stället hänvisas det i 2 kap. 2 § första stycket 12 polisdatalagen, 2 kap. 2 § första stycket 12 kustbevakningsdatalagen, 2 kap. 2 § första stycket 12 åklagardatalagen, 2 kap. 2 § första stycket 12 tullbrottsdatalagen och 2 kap. 2 § första stycket 12 skattebrottsdatalagen till 48 § personuppgiftslagen när det gäller skadestånd. Enligt 8 § lagen om behandling av personuppgifter inom kriminalvården gäller personuppgiftslagens bestämmelser om

skadestånd vid behandling av personuppgifter enligt den lagen eller föreskrifter som har meddelats i anslutning till den.

Rätten till skadestånd vid skada och kränkning bör vara densamma när personuppgifter behandlas i strid med bestämmelser i registerförfattningarna som vid behandling i strid med brottsdatalagen. Det bör framgå genom att det i registerförfattningarna föreskrivs att 7 kap. 1 § brottsdatalagen ska tillämpas på motsvarande sätt vid behandling av personuppgifter enligt respektive registerlag eller föreskrifter som har meddelats i anslutning till den.

I dag prövar Justitiekanslern frågor om skadeståndsskyldighet enligt 48 § personuppgiftslagen. Det bör därför vara Justitiekanslern som prövar frågor om staten är skadeståndsskyldig enligt 7 kap. 1 § brottsdatalagen och enligt bestämmelser i registerförfattningarna som hänvisar till den paragrafen. Ett tillägg bör därför göras i 3 § förordningen (1995:1301) om handläggning av skadeståndsanspråk mot staten.

5.4.4 Överklagande

Utredningens förslag: I registerförfattningarna ska framgå att det finns bestämmelser om överklagande i brottsdatalagen.

Skälen för utredningens förslag: Brottsdatalagen innehåller generella bestämmelser om överklagande. I 7 kap. 2 § brottsdatalagen föreskrivs att beslut i fråga om rättelse eller komplettering, radering eller begränsning av behandlingen av personuppgifter, som har meddelats av en myndighet i egenskap av personuppgiftsansvarig, får överklagas till allmän förvaltningsdomstol. Detsamma gäller beslut att inte lämna information på begäran av en registrerad, att ta ut avgift för att lämna information eller att inte medge omprövning av ett automatiserat beslut. I 7 kap. 3 § finns en särskild bestämmelse om dröjsmålstalan. Även beslut med stöd av den paragrafen får överklagas. Enligt 7 kap. 4 § får tillsynsmyndighetens beslut enligt lagen eller enligt föreskrifter som har meddelats i anslutning till den överklagas till allmän förvaltningsdomstol. I 7 kap. 5 § föreskrivs att andra beslut enligt lagen än de nu nämnda inte får överklagas (se SOU 2017:29 s. 537 f.).

I 2 kap. 2 § första stycket 13 polisdatalagen, 2 kap. 2 § första stycket 13 kustbevakningsdatalagen, 2 kap. 2 § första stycket 13 åklagardatalagen, 2 kap. 2 § första stycket 13 tullbrottsdatalagen och 2 kap. 2 § första stycket 13 skattebrottsdatalagen hänvisas det till överklagandereglerna i 51 § första stycket, 52 § första stycket och 53 § personuppgiftslagen. I 51 § första stycket regleras rätten att överklaga tillsynsmyndighetens beslut om annat än föreskrifter. Enligt 52 § första stycket får en myndighets beslut i fråga om information efter ansökan, om rättelse och underrättelse till tredje man, om information vid automatiserade beslut och om upplysningar till allmänheten om personuppgiftsbehandlingar som inte har anmälts till tillsynsmyndigheten överklagas. Enligt 53 § personuppgiftslagen får andra beslut inte överklagas. I 12–16 §§ lagen om behandling av personuppgifter inom kriminalvården finns det särskilda överklagandebestämmelser.

I brottsdatalagen anges uttömmande vilka beslut av behöriga myndigheter som får överklagas. Rätten att överklaga omfattar enbart sådana beslut som en myndighet har fattat i egenskap av personuppgiftsansvarig och som berör den enskilde och går honom eller henne emot. Några andra beslut av en behörig myndighet får inte överklagas. Myndigheterna kommer att fatta beslut om exempelvis rättelse, radering eller begränsning av behandlingen med stöd av brottsdatalagen. Det blir alltså inte aktuellt att med stöd av någon av registerförfattningarna fatta sådana beslut som rör enskilda som de bör ha rätt att överklaga. Det bör därför framgå av registerförfattningarna att överklagande regleras i brottsdatalagen.

5.4.5 Uppgifter till rättsstatistiken

Utredningens förslag: I brottsdatalagen ska föreskrivas att personuppgifter som är nödvändiga för att framställa rättsstatistik ska lämnas till den myndighet som ansvarar för att framställa sådan statistik. Motsvarande bestämmelser i registerförfattningarna ska upphävas.

Skälen för utredningens förslag: I 9 § lagen om behandling av personuppgifter inom kriminalvården, 2 kap. 14 § polisdatalagen, 2 kap. 12 § åklagardatalagen, 2 kap. 15 § tullbrottsdatalagen och

2 kap. 14 § skattebrottsdatalagen föreskrivs att personuppgifter som är nödvändiga för att framställa rättsstatistik ska lämnas till den myndighet som ansvarar för att framställa sådan statistik. Eftersom regleringen är av generell natur bör det införas en bestämmelse om det i brottsdatalagen. Bestämmelserna i registerförfattningarna bör därmed upphävas.

Kustbevakningen har i dag ingen skyldighet att lämna sådan statistik och det finns därför ingen bestämmelse om uppgiftslämnande till rättsstatistiken i kustbevakningsdatalagen. Det hindrar inte att regleringen placeras i brottsdatalagen.

5.4.6 Terminologin anpassas

Utredningens förslag: Terminologin i registerförfattningarna ska anpassas till brottsdatalagen och i viss utsträckning till data-skyddsförordningen.

Skälen för utredningens förslag

Uttrycket brottsbekämpning

Som framgår av avsnitt 4.4.1 bör uttrycket brottsbekämpande verksamhet utmönstras ur registerförfattningarna. I stället bör som i brottsdatalagen utgångspunkten vara att personuppgifter behandlas i syfte att bekämpa eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet.

Brottsbekämpande verksamhet anses i dag omfatta både att förebygga, förhindra och upptäcka brottslig verksamhet och att utreda och beivra brott. I brottsdatalagen görs dock, i linje med hur direktivet är utformat, skillnad mellan brottsbekämpning och lagföring. Uppgiften att beivra brott hänförs till lagföring. Uttrycket brottsbekämpning kommer därmed att ha en snävare innebörd än i dag. Det blir emellertid ingen saklig skillnad för de myndigheter som har till uppgift att både utreda och beivra brott, eftersom både brottsbekämpning och lagföring omfattas av registerförfattningens tillämpningsområde. För Skatteverket, som i motsats till övriga myndigheter inte har några lagförande uppgifter, innebär det inte heller någon ändring i sak att terminologin ändras på detta sätt.

Uttrycket beivra brott

Brottsdatalagen gäller för behandling av personuppgifter som utförs i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet. Utredningen framhåller i delbetänkandet att det modernare uttrycket lagföra brott bör användas i brottsdatalagen i stället för beivra brott (se SOU 2017:29 s. 162 f.).

I flera av registerförfattningarna används i dag uttrycket beivra brott. Det förekommer bl.a. i 2 kap. 7 § polisdatalagen, 3 kap. 2 § kustbevakningsdatalagen, 2 kap. 5 § åklagardatalagen och 2 kap. 5 § tullbrottsdatalagen. Registerförfattningarna bör anpassas så att terminologin stämmer överens med hur tillämpningsområdet anges i 1 kap. 2 § brottsdatalagen. Det innebär att uttrycket beivra brott bör ersättas av lagföra brott i registerförfattningarna.

Uttrycken bevarande och gallring

Att bestämmelserna om bevarande och gallring bör formuleras om och i stället utgå från hur länge personuppgifter får behandlas diskuteras i avsnitt 5.5.

5.5 Särskilt om längsta tid för behandling

5.5.1 Regleringen samlas

Utredningens bedömning: Bestämmelserna om bevarande och gallring i registerförfattningarna syftar till att skydda den personliga integriteten och reglerar inte bevarande och gallring i arkivlagens mening. Bestämmelserna bör formuleras om så att det framgår att det är fråga om dataskyddsbestämmelser.

Utredningens förslag: Regler om hur länge uppgifter får behandlas ska som huvudregel samlas i särskilda kapitel i registerförfattningarna.

Skälen för utredningens bedömning och förslag

Olika typer av bestämmelser

I registerförfattningarna finns det bestämmelser om bevarande och gallring av personuppgifter. Regleringen gäller enbart personuppgifter som behandlas automatiserat. Den styr således inte hur länge uppgifter som behandlas på papper får bevaras, varken i den brottsbekämpande verksamheten eller för arkivändamål. När det i detta avsnitt talas om hur länge personuppgifter får behandlas eller i vilken utsträckning behandling för arkivändamål är tillåten avses enbart automatiserad behandling.

Enligt de brottsbekämpande myndigheternas registerförfattningar gäller som huvudregel att personuppgifter inte får behandlas längre än vad som behövs för något av de ändamål som omfattas av respektive lags tillämpningsområde. I avsnitt 5.3.11 föreslår utredningen att de bestämmelserna ska upphävas, eftersom motsvarande reglering finns i brottsdatalagen. Därutöver finns det två olika typer av bestämmelser om bevarande och gallring av personuppgifter. Tullbrottsdatalagen kan tas som exempel, men motsvarande bestämmelser finns i de övriga brottsbekämpande myndigheternas registerförfattningarna.

Den ena typen är bestämmelser om gallring (se 4 kap. 3, 9 och 10 §§ tullbrottsdatalagen). De gäller för personuppgifter som inte förekommer i ärenden om utredning av eller lagföring för brott. Regleringen innebär att personuppgifterna inte får behandlas automatiserat efter vissa i lagen angivna tidsfrister. De får alltså inte heller arkiveras digitalt. Det följer av att det i 2 kap. 2 § andra stycket tullbrottsdatalagen görs undantag från 8 § andra stycket personuppgiftslagen, som föreskriver att arkivlagstiftningen har företräde framför personuppgiftslagstiftningen. Behandling för arkivändamål är dock tillåten om det med stöd av 4 kap. 2 § 2 har meddelats föreskrifter om att personuppgifterna får bevaras för historiska, statistiska eller vetenskapliga ändamål.

Den andra typen av bestämmelser begränsar möjligheten att behandla personuppgifter i myndighetens brottsbekämpande verksamhet. Bestämmelserna gäller för personuppgifter som har gjorts gemensamt tillgängliga och som rör ärenden om utredning av eller lagföring för brott (se 4 kap. 6 och 7 §§ tullbrottsdatalagen). De föreskriver hur länge personuppgifter får behandlas i den brottsbe-

kämpande verksamheten, men det hindrar inte att uppgifterna behandlas för bl.a. arkivändamål. Regeringen eller den myndighet som regeringen bestämmer kan enligt 4 kap. 2 § 1 och 3 tullbrottsdatalagen meddela föreskrifter om att vissa kategorier av personuppgifter får behandlas i den brottsbekämpande verksamheten under längre tid än vad som annars är föreskrivet och om digital arkivering.

Bestämmelser om bevarande och gallring är inte arkivrättsliga regler

Utgångspunkten i det arkivrättsliga regelverket är att uppgifter ska bevaras, medan presumptionen i regelverk som skyddar personuppgifter är den omvända (se SOU 2017:29 s. 283). Gallring enligt det arkivrättsliga regelverket syftar till att begränsa arkivens omfattning, medan gallring enligt registerförfattningarna syftar till att skydda enskildas personliga integritet.

Bestämmelserna om bevarande och gallring i registerförfattningarna har alltså till syfte att skydda den personliga integriteten vid automatiserad behandling av personuppgifter (se exempelvis prop. 2009/10:85 s. 207 f. och prop. 2016/17:91 s. 169). Som utredningen konstaterar i delbetänkandet bör orden bevarande och gallring enbart användas i den betydelse de har i arkivlagstiftningen, för att tydligt skilja mellan arkivrättsliga regler och regler om dataskydd. När syftet med bestämmelserna som i detta fall är att skydda den personliga integriteten bör regleringen därför i stället ange den yttersta gränsen för hur länge personuppgifterna får behandlas (se SOU 2017:29 s. 282 f.). Det gäller både gallringsbestämmelserna och bestämmelserna som begränsar möjligheten att behandla personuppgifter i den brottsbekämpande verksamheten. Bestämmelserna bör därför formuleras om så att det framgår att de är dataskyddsregler (se avsnitt 5.5.2 och 5.5.3).

En samlad reglering

I tullbrottsdatalagen och skattebrottsdatalagen, som båda nyligen har trätt i kraft, har bestämmelserna om bevarande och gallring samlats i ett särskilt kapitel. Den lösningen ger tillämparen en bättre överblick över hur länge personuppgifter får behandlas enligt

lagen och bör så långt möjligt väljas i de övriga registerförfattningarna. I de fall där behandling av personuppgifter i särskilda register eller viss specifik verksamhet regleras särskilt bör dock bestämmelser som reglerar hur länge personuppgifter får behandlas i registret eller verksamheten hållas samman med regleringen i övrigt.

5.5.2 Bestämmelser om längsta tid för behandling oavsett ändamål

Utredningens förslag: De bestämmelser som i dag reglerar gallring ska formuleras om så att de i stället anger den längsta tid som personuppgifterna får behandlas.

Det ska alltså finnas bestämmelser om föreskriftsrätt avseende behandling av personuppgifter för vetenskapliga, statistiska eller historiska ändamål.

Skälen för utredningens förslag

Gallringsbestämmelserna ska finnas kvar men formuleras om

I delbetänkandet konstaterar utredningen att behandling av personuppgifter för arkivändamål omfattas av dataskyddsförordningens tillämpningsområde (se SOU 2017:29 s. 287). Det kan mot den bakgrunden ifrågasättas om bestämmelser om gallring bör finnas i registerförfattningar som reglerar personuppgiftsbehandling inom brottsdatalagens tillämpningsområde. Som nyss konstaterats är gallringsbestämmelserna i registerförfattningarna emellertid inte gallringsbestämmelser i arkivrättslig mening, utan dataskyddsbestämmelser. Syftet är att skydda enskildas personliga integritet genom att det föreskrivs när den automatiserade behandlingen av personuppgifter ska upphöra. Om informationen överförs från elektronisk form till pappersform och därefter inte finns kvar elektroniskt, anses detta skydd ha tillgodosetts (se t.ex. Tullbrottsdatalag, prop. 2016/17:91, s. 171). Bestämmelserna reglerar således inte i vilken utsträckning det är tillåtet att behandla personuppgifterna för arkivändamål, utan styr endast i vilken form det får göras genom att ange att automatiserad behandling för arkivändamål inte är tillåten. De hindrar således inte arkivering på papper.

Om det inte längre skulle finns några bestämmelser i registerförfattningarna som föreskriver när den automatiserade behandlingen av personuppgifter ska upphöra, skulle arkivlagens huvudregel om bevarande behöva tillämpas på om uppgifterna finns i allmänna handlingar. En del av dagens integritetsskydd går då förlorat. Bestämmelser som reglerar hur länge personuppgifter får behandlas automatiserat och vara digitalt tillgängliga är därför enligt utredningens mening nödvändiga för att tillgodose skyddet för enskildas personliga integritet. Sådana bestämmelser bör därför även fortsättningsvis finnas i registerförfattningarna.

Bestämmelserna om gallring bör emellertid formuleras om så att det framgår att de är dataskyddsbestämmelser. De bör utgå från hur länge personuppgifterna får behandlas automatiserat. Det gäller 7 § första stycket lagen om behandling av personuppgifter inom kriminalvården och de gallringsbestämmelser som finns i tillhörande förordning, 2 kap. 13 §, 3 kap. 14 §, 4 kap. 7, 14, 15, 20 och 22 §§ polisdatalagen, 3 kap. 5 § och 4 kap. 13 § kustbevakningsdatalagen, 2 kap. 10 § tredje stycket åklagardatalagen, 4 kap. 3, 9 och 10 §§ tullbrottsdatalagen och 4 kap. 3 och 8 §§ skattebrottsdatalagen. Någon ändring av hur länge personuppgifterna får behandlas bör som huvudregel inte göras (se dock avsnitt 7.6 och 8.6).

Arkivlagstiftningen ska inte ha företrädare

Enligt 2 kap. 17 § första stycket brottsdatalagen får personuppgifter inte behandlas under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen. Det hindrar enligt andra stycket inte att en myndighet arkiverar och bevarar allmänna handlingar eller att arkivmaterial lämnas till en arkivmyndighet. Av registerförfattningarna följer att arkivlagstiftningen inte har företrädare när gallringsbestämmelser är tillämpliga (se t.ex. 2 kap. 2 § andra stycket polisdatalagen). Syftet med regleringen är som nyss nämnts att förtydliga att personuppgifter i dessa fall inte får behandlas automatiserat för arkivändamål, det vill säga att uppgifterna inte får arkiveras digitalt. Uppgifterna får dock behandlas för arkivändamål om de överförs till pappersform. För att tydliggöra att ingen förändring i det avseendet är avsedd, trots den ändrade termi-

nologin, bör det i registerförfattningarna göras undantag från 2 kap. 17 § andra stycket brottsdatalagen i ovan nämnda paragrafer.

Föreskrifträtten ska finnas kvar

I flertalet av registerförfattningarna upplyses om att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter om att personuppgifter får bevaras för historiska, statistiska eller vetenskapliga ändamål. Sådana bestämmelser finns bl.a. i 2 kap. 13 § tredje stycket polisdatalagen, 3 kap. 5 § tredje stycket och 4 kap. 14 § andra stycket kustbevakningsdatalagen, 2 kap. 11 § 2 åklagardatalagen, 4 kap. 2 § 2 tullbrottsdatalagen och 4 kap. 2 § 2 skattebrottsdatalagen.

Det finns även i framtiden behov av att kunna meddela föreskrifter om att personuppgifter som behandlas med stöd av registerförfattningarna får fortsätta att behandlas automatiserat för sådana ändamål när den längsta tillåtna tiden för behandling som anges i registerförfattningen löper ut. Sådana föreskrifter ger möjlighet att tillgodose dels rätten att ta del av allmänna handlingar, dels rättskipningens, förvaltningens och forskningens behov. Bestämmelserna bör dock formuleras om så att föreskrifträtten avser hur länge personuppgifterna får behandlas. Utredningen återkommer till att de även bör formuleras om för att motsvara dataskyddsförordningens och dataskyddsdirektivets terminologi.

Enligt 7 § andra stycket lagen om behandling av personuppgifter inom kriminalvården får, trots vad som föreskrivs om gallring i första stycket, personuppgifter bevaras för historiska, statistiska eller vetenskapliga ändamål. Kriminalvården har även i fortsättningen behov av att kunna behandla personuppgifter för statistik- och forskningsändamål. I likhet med vad som föreslås beträffande övriga registerförfattningar bör det därför upplysas om att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter om att personuppgifter får behandlas för historiska, statistiska eller vetenskapliga ändamål. Föreskrifträtten bör ersätta den nuvarande regleringen.

Det kan även här ifrågasättas om bestämmelser om föreskrifträtt som möjliggör fortsatt behandling av personuppgifter för historiska, statistiska eller vetenskapliga ändamål bör finnas i register-

författningar som endast reglerar personuppgiftsbehandling inom brottsdatalagens tillämpningsområde. Eftersom föreskriftsrätten gäller personuppgifter som behandlas för ändamål som omfattas av registerförfattningens tillämpningsområde och inte för arkivändamål kan föreskriftsrätten inte överföras till arkivlagstiftningen. Det finns inte heller någon annan naturlig plats för sådana bestämmelser. Utredningen anser därför att föreskriftsrätten även fortsättningsvis bör regleras i registerförfattningarna.

Behandling för historiska, statistiska och vetenskapliga ändamål

Som nyss nämnts kan enligt bestämmelser i polisdatalagen, kustbevakningsdatalagen, åklagardatalagen, tullbrottsdatalagen och skattebrottsdatalagen regeringen eller den myndighet som regeringen bestämmer meddela föreskrifter om att personuppgifter får bevaras för historiska, statistiska eller vetenskapliga ändamål.

I 9 § tredje stycket personuppgiftslagen används samma uttryck. I dataskyddsförordningen används i stället uttrycken arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål. Historiska ändamål delas alltså upp i arkivändamål av allmänt intresse och historiska forskningsändamål. Avsikten med uppdelningen är att förtydliga vad som avses med historiska ändamål. Även i direktivet görs i artikel 4.3 skillnad mellan behandling för arkivändamål av allmänt intresse och vetenskaplig, statistisk och historisk användning för ändamål som omfattas av direktivets tillämpningsområde.

Som nyss nämnts finns det även i framtiden behov av att kunna meddela föreskrifter om att personuppgifter som behandlas med stöd av en viss registerförfattning får fortsätta att behandlas för vetenskapliga, statistiska och historiska ändamål när den längsta tiden för behandling enligt registerförfattningen löper ut. För att terminologin ska motsvara dataskyddsförordningens och dataskyddsdirektivets bör det framgå att föreskriftsrätten även omfattar behandling för arkivändamål av allmänt intresse.

5.5.3 Bestämmelser om längsta tid för behandling för ändamål inom tillämpningsområdet

Utredningens förslag: Bestämmelser som i dag reglerar hur länge personuppgifter får behandlas i den brottsbekämpande verksamheten ska formuleras om så att det framgår att de bara begränsar behandling för ändamål inom registerförfattningens tillämpningsområde.

Bestämmelser om föreskriftsrätt avseende digital arkivering ska finnas kvar i registerförfattningarna, men det ska förtydligas att de endast omfattar behandling av personuppgifter för ändamål inom tillämpningsområdet.

Skälen för utredningens förslag

Endast begränsning av behandlingen för ändamål inom registerförfattningens tillämpningsområde

I 3 kap. 10 och 11 §§ polisdatalagen, 4 kap. 9 och 10 §§ kustbevakningsdatalagen, 4 kap. 6 och 7 §§ tullbrottsdatalagen och 4 kap. 5 och 6 §§ skattebrottsdatalagen anges hur länge vissa personuppgifter får behandlas automatiserat i den brottsbekämpande verksamheten. Enligt 2 kap. 10 § andra stycket åklagardatalagen gäller motsvarande vid behandling för ändamål i den operativa verksamheten. Bestämmelserna hindrar inte att uppgifterna fortsätter att behandlas automatiserat för andra ändamål under längre tid än vad som anges i dem, vilket innebär att personuppgifterna bl.a. får behandlas automatiserat för arkivändamål. Bestämmelserna begränsar alltså enbart möjligheten till fortsatt behandling i den verksamhet som regleras i respektive registerförfattning. För att tydliggöra det bör det framgå att bestämmelserna enbart reglerar hur länge personuppgifter får behandlas för ändamål inom respektive registerförfattningens tillämpningsområde.

Den ändrade terminologin bör även medföra att 2 kap. 18 § brottsdatalagen ändras så att det tydliggörs att skyldigheten enligt den paragrafen att ompröva behovet av att behandla personuppgifter gäller om det inte finns en föreskrift i lag eller annan författning som anger när en viss kategori av personuppgifter inte längre får behandlas för ändamål inom brottsdatalagens tillämpningsområde.

Konsekvenserna av att uppgifter har arkiverats

Att uppgifter har arkiverats, oavsett om det görs digitalt eller i pappersform, innebär naturligtvis inte att det är förbjudet att på nytt behandla personuppgifterna för något av de ändamål som anges i en registerförfattning. Det förutsätter dock att det finns en tillåten rättslig grund för att göra det och att regleringen i övrigt tillåter den nya behandlingen. Ett typiskt exempel kan vara att det kommer fram uppgifter som gör att en nedlagd förundersökning som har arkiverats bör återupptas eller att fråga om resning eller annat extraordinärt rättsmedel aktualiseras beträffande en dom eller ett beslut som har fått laga kraft. Ny behandling av de arkiverade uppgifterna kan då påbörjas för det ändamålet.

I de brottsbekämpande myndigheternas registerförfordningar föreskrivs det att personuppgifterna ska avskiljas från myndighetens brottsbekämpande eller operativa verksamhet vid digital arkivering. Syftet är att uppgifterna inte ska vara digitalt åtkomliga i den verksamheten. Det ska alltså inte vara möjligt för vem som helst att enkelt söka fram de digitalt arkiverade personuppgifterna. Normalt bör det bara vara arkivarier som förfogar över uppgifterna och kan göra sökningar i dem.

Med hänsyn till att arkivlagen inte hindrar eller ställer upp några begränsningar för fortsatt automatiserad behandling av arkiverade uppgifter finns det även i fortsättningen behov av att kunna meddela föreskrifter till skydd för den personliga integriteten vid digital arkivering.

Det kan ifrågasättas om föreskrifter avseende arkiverade uppgifter, som behandlas med stöd av dataskyddsförordningen, bör finnas i en registerförfattning som endast reglerar personuppgiftsbehandling inom brottsdatalogens tillämpningsområde. Syftet med föreskrifterna är att reglera hur digitalt arkiverade uppgifter får behandlas för ändamål inom respektive lags tillämpningsområde och att därigenom skydda enskildas integritet, t.ex. genom att ange vem som ska få ha tillgång till uppgifterna eller vilka sökningar som ska få göras. Mot den bakgrunden hör regleringen enligt utredningens mening hemma i personuppgiftslagstiftningen och inte i arkivlagstiftningen.

5.5.4 Omständigheter som påverkar längsta tid för behandling i underrättelseverksamhet

Utredningens förslag: Endast uppgifter om en persons anknytning till brottslig verksamhet ska påverka längsta tid för behandling av personuppgifter i underrättelseverksamhet.

Skälen för utredningens förslag: I dag föreskrivs det i vissa bestämmelser att den tid som personuppgifter får behandlas i underrättelseverksamhet kan förlängas om en ny registrering avseende personen i fråga görs. Sådana bestämmelser finns bl.a. i 3 kap. 14 §, 4 kap. 20 § och 6 kap. 12 § polisdatalagen, 4 kap. 13 § kustbevakningsdatalagen och 4 kap. 9 § tullbrottsdatalagen. Det framgår emellertid inte av bestämmelserna vad den registrering som kan föranleda att personuppgifter får fortsätta att behandlas ska avse. Det kan knappast ha varit lagstiftarens avsikt att tiden för hur länge personuppgifter får behandlas ska kunna påverkas av vilka uppgifter som helst. Normalt saknar t.ex. ny folkbokföringsadress, nytt registreringsnummer på fordon som personen disponerar eller någon annan sådan uppgift betydelse för frågan om personen utövar eller kan komma att utöva brottslig verksamhet. Enligt utredningens mening bör det tydliggöras att endast sådana omständigheter som har betydelse för personens anknytning till brottslig verksamhet bör påverka hur länge personuppgifterna får behandlas. En sådan omständighet kan vara att personen har begått brott, men det bör då vara fråga om ett brott som har någon anknytning till den brottsliga verksamheten. Att en person t.ex. gör sig skyldig till skadegörelse eller misshandel av en anhörig kan sällan ha betydelse för om personen kan antas vara inblandad i narkotikabrottslighet.

Säkerhets- och integritetsskyddsnämnden har väckt ytterligare en fråga om hur bestämmelserna bör tolkas (nämndens uttalande den 4 maj 2017, dnr 223-2016). Det gäller frågan om huruvida en ny registrering avseende en person förlänger tiden för behandling enbart avseende den personen, eller om den registreringen även påverkar tiden för behandling avseende personer som har anknytning till samma brottsliga verksamhet. Utredningen har inte haft utrymme att behandla den frågan.

5.6 Särskilt om elektroniskt utlämnande

5.6.1 Olika former av elektroniskt utlämnande

Direktåtkomst

Det finns inte någon legaldefinition av uttrycket direktåtkomst. Det som vanligtvis avses med direktåtkomst är att någon har direkt tillgång till någon annans register eller databas och på egen hand kan söka efter information, dock utan att kunna påverka innehållet i registret eller databasen. Enligt Informationshanteringsutredningen bör direktåtkomst anses föreligga om en myndighet hos en annan myndighet har sådan teknisk tillgång till upptagningar som avses i 2 kap. 3 § andra stycket tryckfrihetsförordningen, dvs. om upptagningen är tillgänglig för myndigheten med tekniskt hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att den kan läsas, avlyssnas eller på annat sätt uppfattas (se Myndighetsdatalag, SOU 2015:39, s. 390 f.). Högsta förvaltningsdomstolen använde i rättsfallet HFD 2015 ref. 61 samma definition av direktåtkomst. I begreppet direktåtkomst ligger också att den som är personuppgiftsansvarig för registret eller databasen saknar kontroll över vilka uppgifter som den som har direktåtkomst vid ett visst tillfälle tar del av. Från integritetssynpunkt har det därför ansetts viktigt att frågor om tillgång till uppgifter genom direktåtkomst regleras särskilt i registerlagstiftningarna (se Ökat informationsutbyte mellan arbetslöshetsförsäkringen, socialförsäkringen och studiestödet, prop. 2000/01:129, s. 74, Lag om behandling av personuppgifter i den arbetsmarknadspolitiska verksamheten, prop. 2001/02:144, s. 35 f. och Elektronisk informationsöverföring hos arbetslöshetskassorna och inom Arbetsmarknadsverket, prop. 2005/06:52, s. 8).

Vid direktåtkomst fattas beslutet om överföring i varje enskilt fall av mottagaren. Den faktiska begränsningen av direktåtkomsten görs med hjälp av olika tekniska lösningar, beroende på hur omfattningen av direktåtkomsten har begränsats i det enskilda fallet. Det kan göras exempelvis genom olika behörighetsnivåer. Direktåtkomst anses således föreligga inte bara när tillgång ges utan begränsning, utan även vid mer eller mindre förfinade avgränsningar av åtkomst till enstaka eller ett flertal uppgifter (se E-delegationens rapport Direktåtkomst och utlämnande på medium för automatis-

rad behandling, s. 8). Den personuppgiftsansvarige ska se till att åtkomsten rent faktiskt begränsas på det sätt som föreskrivs.

Utlämnande på medium för automatiserad behandling

I princip anses allt elektroniskt utlämnande som inte görs genom direktåtkomst göras genom utlämnande på medium för automatiserad behandling. Sådant utlämnande kan göras på många olika sätt. Det kan vara fråga om att personuppgifter lämnas t.ex. via e-post eller dvd-skiva eller genom direkt överföring från ett datasystem till ett annat via elektroniska kommunikationsnät. Begreppet utlämnande på medium för automatiserad behandling har dock i takt med att tekniken utvecklats ibland getts en vidare innebörd. Det används numera för överlämnande av elektroniskt lagrade uppgifter via alla slags medium för lagring och överföring (se Överskottsinformation vid direktåtkomst, SOU 2012:90, s. 198). I förarbetsuttalanden har som exempel på sådant utlämnande bl.a. nämnts s.k. batchkörningar. Med det avses visst automatiskt utlämnande efter sökningar och sammanställningar där svar lämnas med viss tidsfördröjning (se prop. 2000/01:129 s. 76 och Utökad elektroniskt informationsutbyte, prop. 2007/08:160, s. 60).

5.6.2 Behovet av att kommunicera elektroniskt

Dagens kommunikationsbehov

Myndigheter som sysslar med brottsbekämpning, lagföring och straffverkställighet har stora behov av att kommunicera med såväl andra myndigheter som enskilda. Det kan röra sig om att begära eller utbyta information, att begära eller lämna yttranden, att ge insyn i en förundersökning, att delge handlingar under förundersökningsförfarandet eller brottmålsprocessen eller att expediera strafförelägganden och andra beslut. Tyngdpunkten ligger på kommunikation mellan behöriga myndigheter, men det rör sig också om kommunikation med andra. När det gäller andra myndigheter kan det exempelvis vara fråga om kontakter med Transportstyrelsen (trafikutredningar, expediering av strafförelägganden och beslut), Arbetsförmedlingen (brottsutredningar, personutredning

och straffverkställighet) eller Försäkringskassan (brottsutredningar, personutredning, straffverkställighet). När det gäller kommunikation med enskilda kan som exempel nämnas att Polismyndigheten i sin brottsbekämpande verksamhet har stort behov av att kunna kommunicera med bl.a. banker och försäkringsbolag och att Ekobrottsmyndigheten ofta har kontakt med finansiella aktörer.

Det finns också skäl att framhålla att behovet av kommunikation utanför ordinarie kontorstid är betydande, eftersom brottsbekämpande verksamhet pågår även på annan tid. Det kan då vara nödvändigt att t.ex. kunna förse offentliga försvarare med handlingar elektroniskt.

Under lång tid sköttes kommunikationsbehovet i huvudsak på papper, bl.a. därför att regelverket i rättegångsbalken förutsatte sådan hantering. Framför allt det senaste decenniet har dock inneburit att kommunikationen i allt större utsträckning kan skötas i elektronisk form.

Elektroniskt utlämnande ger effektivitetsvinster

Informationshanteringsutredningen, som hade i uppdrag att generellt se över frågor om elektroniskt utlämnande, framhåller att frågan om hur den bästa effektiviteten kan uppnås för närvarande inte synes handla så mycket om vilken elektronisk utlämnandeform som bör väljas utan mer om myndigheternas möjlighet att överhuvudtaget åstadkomma det informationsutbyte som regeringen eller de själva vill ska förekomma. Problemen med att uppnå önskad effektivisering förefaller enligt den utredningen till viss del handla om legala förutsättningar för ett visst informationsutbyte (se SOU 2015:39 s. 148).

Både i Sverige och inom EU uppmuntras myndigheter att i så stor utsträckning som möjligt dra nytta av de effektivitetsvinster som modern teknik kan ge. Det pågår sedan länge ett utvecklingsarbete under ledning av Regeringskansliet, det s.k. RIF-arbetet, som syftar till att myndigheterna i rättskedjan i ökande utsträckning ska kunna dra nytta av personuppgifter som har lagrats elektroniskt av de myndigheter som ligger tidigare i kedjan. Genom registerförfattningarna har myndigheterna i rättskedjan lagstöd för att kunna utbyta personuppgifter elektroniskt med varandra och att

medge övriga myndigheter tillgång till vissa uppgifter genom direktåtkomst. Av effektivitetsskäl kan de emellertid behöva lämna ut personuppgifter i elektronisk form även till andra. Den möjligheten begränsas i dag genom reglerna om utlämnande på medium för automatiserad behandling.

Risker med elektroniskt utlämnande

När det gäller elektroniskt utlämnande brukar utlämnande genom direktåtkomst förknippas med särskilda risker. Ett skäl till det är att de upptagningar som direktåtkomsten avser blir allmänna handlingar hos den mottagande myndigheten (se SOU 2012:90 s. 64 f. och 123 f. och SOU 2015:39 s. 134 f.). Sammanställningar av uppgifter som i samband med direktåtkomst görs tekniskt tillgängliga för den mottagande myndigheten anses enligt 2 kap. 3 § andra stycket tryckfrihetsförordningen förvarade hos den mottagande myndigheten och utgör således allmänna handlingar där. Ju fler myndigheter som har direktåtkomst till uppgifter i ett datasystem, desto större blir allmänhetens möjlighet att få tillgång till uppgifterna (se Utlänningsdatalag, SOU 2003:40, s. 201 och Personuppgiftsbehandling på utlännings- och medborgarskapsområdet, SOU 2015:73, s. 304). Ett annat skäl till att direktåtkomst anses innebära särskilda risker är att den typiskt sett innebär att uppgifter blir tillgängliga för fler personer och att den utlämnande myndighetens möjligheter att kontrollera användningen av uppgifterna minskar (se Utlänningsdatalag, prop. 2015/16:65, s. 89 f.).

Det förhållandet att en myndighet får tillgång till uppgifter genom direktåtkomst ger dock inte mottagaren rätt att behandla personuppgifterna. Mottagaren måste ha rättsligt stöd i sin egen registerlagstiftning för personuppgiftsbehandlingen och även i övrigt uppfylla alla skyldigheter som är förenade med den.

Inte bara direktåtkomst utan även utlämnande av personuppgifter på medium för automatiserad behandling anses medföra risker från integritetssynpunkt. Sådant utlämnande innebär nämligen som regel att mottagaren kan bearbeta informationen, t.ex. genom att samköra den mot elektroniska uppgifter som har hämtats från andra informationskällor. Det ökar risken för att uppgifterna behandlas i strid med de grundläggande kraven på dataskydd.

För att minska de risker som ökat elektroniskt utlämnande anses medföra har det bl.a. införts en ny sekretessbestämmelse. Enligt 21 kap. 7 § offentlighets- och sekretesslagen gäller sekretess för personuppgift, om det kan antas att utlämnande skulle medföra att uppgiften behandlas i strid med personuppgiftslagen. Syftet med bestämmelsen är att det ska vara möjligt att hindra s.k. massuttag, om det finns skäl att anta att uppgifterna skulle missbrukas.

5.6.3 Utlämnande genom direktåtkomst

Utredningens bedömning: Möjligheterna att tillhandahålla personuppgifter genom direktåtkomst behöver inte ändras.

Skälen för utredningens bedömning

Nuvarande reglering

Av 2 kap. 21 § polisdatalagen framgår att utlämnande genom direktåtkomst bara är tillåtet i den utsträckning som följer av lagen. Sådana bestämmelser finns bl.a. i 4 kap., där vissa register särregleras. I 3 kap. 8 § polisdatalagen anges vilka myndigheter som får medges direktåtkomst till andra personuppgifter än de som behandlas i särskilda register. Där föreskrivs också att direktåtkomst endast får avse personuppgifter som gjorts gemensamt tillgängliga. Liknande bestämmelser finns i 2 kap. 9 § kustbevakningsdatalagen, 2 kap. 17 § åklagardatalagen, 2 kap. 17 § och 3 kap. 8 § tullbrottsdatalagen och 2 kap. 16 § och 3 kap. 8 § skattebrottsdatalagen.

Även i kriminalvårdens registerlagstiftning finns det bestämmelser om direktåtkomst, men de finns i huvudsak i förordning (se 37, 43 och 44 §§ förordningen om behandling av personuppgifter inom kriminalvården).

Reglerna om direktåtkomst behöver inte ändras

Informationshanteringsutredningen anser att det även i fortsättningen bör göras skillnad mellan direktåtkomst och annat elektroniskt utlämnande, eftersom konsekvenserna av direktåtkomst till

personuppgifter skiljer sig från annat elektroniskt utlämnande (se SOU 2015:39 s. 136 f.).

Direktåtkomst kräver i dag lagstöd enligt samtliga registerförfattningar med undantag av kriminalvårdens. Enligt 10 § första stycket 2 lagen om behandling av personuppgifter inom kriminalvården meddelar regeringen föreskrifter om vilka myndigheter som får ha direktåtkomst. Riksdagen ska således i de flesta fall ta ställning till om en viss myndighet kan tillåtas att få direktåtkomst.

Med något enstaka undantag är det endast myndigheter som tillämpar brottsdatalagen som enligt registerförfattningarna får medges direktåtkomst. Enligt utredningens mening ger de nuvarande bestämmelserna om direktåtkomst ett tillräckligt skydd för den personliga integriteten och är även i övrigt förenliga med direktivet. Möjligheterna att tillhandahålla personuppgifter genom direktåtkomst behöver därför inte ändras.

5.6.4 Annat elektroniskt utlämnande tillåts i större utsträckning

Utredningens förslag: Personuppgifter ska få lämnas ut elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt. Regeringen ska genom föreskrifter kunna begränsa möjligheten att tillhandahålla personuppgifter på det sättet.

Skälen för utredningens förslag

Nuvarande reglering

Registerförfattningarna för de brottsbekämpande myndigheterna innehåller bestämmelser om elektroniskt utlämnande. I 2 kap. 20 § polisdatalagen, 2 kap. 8 § kustbevakningsdatalagen, 2 kap. 16 § åklagardatalagen, 2 kap. 16 § tullbrottsdatalagen och 2 kap. 15 § skattebrottsdatalagen föreskrivs att enstaka personuppgifter får lämnas ut på medium för automatiserad behandling. Registerförfattningarna innehåller dessutom bestämmelser om att regeringen kan meddela föreskrifter om att uppgifter får lämnas ut på medium för automatiserad behandling även i andra fall. I de förordningar som kompletterar registerlagarna finns det i varierande utsträck-

ning bestämmelser om att uppgifter får lämnas ut på medium för automatiserad behandling i större utsträckning än vad som anges i respektive lag. Begränsningen till enstaka personuppgifter gäller t.ex. inte i förhållande till de myndigheter som får medges direktåtkomst. Det innebär att begränsningen inte gäller i förhållande till andra brottsbekämpande myndigheter.

I domstolsdatalagen har en delvis annan reglering valts. Enligt 16 § domstolsdatalagen får personuppgifter lämnas ut på medium för automatiserad behandling om det inte är olämpligt.

Dataskyddsdirektivet reglerar inte hur personuppgifter tillhandahålls

Varken dataskyddsdirektivet eller dataskyddsförordningen innehåller några bestämmelser om elektroniskt utlämnande av personuppgifter. Det gör inte heller det nu gällande dataskyddsdirektivet. Att lämna ut personuppgifter elektroniskt innebär behandling av personuppgifter och utlämnande förutsätter därmed att reglerna om behandling av personuppgifter följs och att inte annan lagstiftning hindrar utlämnandet.

Eftersom dataskyddsdirektivet inte reglerar på vilket sätt personuppgifter får lämnas ut, finns det inget som hindrar att de nuvarande reglerna om elektroniskt utlämnande behålls.

Kritik mot reglerna om utlämnande av enstaka personuppgifter

Bestämmelserna om att bara enstaka personuppgifter får lämnas ut på medium för automatiserad behandling har kritiserats. Redan när de infördes framförde vissa remissinstanser invändningar mot att begränsa det elektroniska utlämnandet till enstaka uppgifter. Det ansågs otidsenligt och i alltför hög grad begränsa myndigheternas möjlighet att utnyttja de fördelar som elektronisk kommunikation kan ge (se bl.a. prop. 2009/10:85 s. 184 f.). Det var också omfattande kritik mot begränsningen till enstaka uppgifter som ledde till att en annan lösning valdes i domstolsdatalagen (se Domstolsdatalag, prop. 2014/15:148, s. 75 f.)

Till kritikerna hör Informationshanteringsutredningen, som föreslår att det i myndighetsdatalagen tas in en bestämmelse som medger elektroniskt utlämnande till enskilda om det inte är olämpligt.

ligt. Däremot bör det enligt den utredningen inte gälla några lagliga begränsningar för att tillhandahålla myndigheter personuppgifter i elektronisk form (se SOU 2015:39 s. 447).

De myndigheter som har en reglering som föreskriver att endast enstaka personuppgifter får tillhandahållas på medium för automatiserad behandling har instämt i kritiken och under utredningsarbetet framfört önskemål om en reglering som motsvarar den som finns i domstolsdatalagen. Mot det har Datainspektionen anfört att det av integritetsskäl alltså bör vara lagstiftaren som avgör om utlämnande i viss form är lämpligt.

Även uttrycket ”utlämnande på medium för automatiserad behandling” har kritiserats, bl.a. på den grunden att det är otydligt (se SOU 2012:90 s. 198 f. och SOU 2015:39 s. 442).

Bör regleringen ändras?

Numera förväntar sig både myndigheter och enskilda att handlingar i stor utsträckning kan förmedlas elektroniskt. Frågan är om den utvecklingen bör mötas med bestämmelser som förenklar för myndigheterna i rättskedjan att kunna kommunicera elektroniskt.

I avsnitt 5.6.2 framhålls att de brottsbekämpande myndigheterna behöver kommunicera elektroniskt med andra myndigheter och med enskilda. Det är en utveckling som kan antas fortsätta. Elektronisk kommunikation är som regel kostnadseffektiv om man jämför med postbefordran. I vissa avseenden är elektronisk kommunikation säkrare än traditionell befordran, eftersom spårbarheten är större. Elektronisk kommunikation gör det också enkelt att sända större informationsmängder. För mottagaren är skillnaden mellan att få uppgifter på papper och i elektronisk form inte heller så stor i dag. Med modern teknik kan nämligen text på papper enkelt omvandlas till elektroniska uppgifter.

I förarbetena till bl.a. polisdatalagen och kustbevakningsdatalagen framhålls att när ordet enstaka används i bestämmelsen om utlämnande av uppgifter på medium för automatiserad behandling har ordet en annan innebörd än i vanligt språkbruk. När personuppgifter förekommer i en eller ett fåtal handlingar är bestämmelsen inte avsedd att utgöra ett hinder mot att handlingen lämnas ut t.ex. via e-post. Det förhållandet att en handling, t.ex. en lista över

telefonnummer, innehåller ett stort antal personuppgifter hindrar inte att handlingen lämnas ut med stöd av bestämmelsen. Bestämmelsen ger också stöd för utlämnande av t.ex. ett ärende eller delar av ett ärende där personuppgifter förekommer. Ett förundersökningsprotokoll kan således ofta lämnas ut elektroniskt. Däremot får inte en större mängd uppgifter, t.ex. ett helt register eller delar av ett register, lämnas ut med stöd av en sådan bestämmelse (se prop. 2009/10:85 s. 333 och prop. 2011/12:45 s. 98).

Det finns uppenbara nackdelar med en reglering som gång på gång föranleder samma kritik. Det finns enligt utredningens mening risk att bestämmelser – som enligt sin ordalydelse talar för en mer restriktiv tillämpning av elektroniskt utlämnade än vad som förefaller vara avsedd – kan motverka statsmakternas strävanden att myndigheterna ska dra nytta av effektivitetsvinsterna med ny teknik. Det är också olyckligt om förarbetena ger uttryck för att lagregler ska tolkas annorlunda än sin ordalydelse. Det riskerar att undergräva förtroendet för lagstiftningen. En annan risk med hur bestämmelserna är formulerade i dag är att de ger sken av att ge ett starkare integritetsskydd än vad som i praktiken är fallet.

Mot den nu angivna bakgrunden anser utredningen att bestämmelserna om utlämnande av personuppgifter på medium för automatiserad behandling i registerförfattningarna bör ses över, trots att riksdagen nyligen har godkänt sådana bestämmelser i tullbrottsdatalagen och skattebrottsdatalagen.

Samma reglering som för domstolarna

Utredningen delar uppfattningen att tiden nu är mogen att lämna större utrymme för utlämnande i elektronisk form för de brottsbekämpande myndigheterna. Även om det i relativt stor utsträckning förekommer integritetskänsliga personuppgifter i framför allt brottsbekämpande verksamhet och vid straffverkställighet måste riskerna med att överföra sådana uppgifter elektroniskt vägas mot behovet av snabb och effektiv kommunikation. Sekretessbestämmelserna tillsammans med regleringen av personuppgiftsbehandling skyddar enskilda mot att möjligheten att lämna ut personuppgifter elektroniskt missbrukas. Den som överväger att lämna ut personuppgifter, oavsett i vilken form det görs, måste alltid över-

väga om sekretessregleringen lägger hinder i vägen och, om så inte är fallet, om regelverket för personuppgiftsbehandling gör det möjligt att lämna uppgifterna i elektronisk form.

För polisen, Kustbevakningen, åklagarväsendet, Tullverket och Skatteverket har regeringen redan i förordning öppnat för elektroniskt uppgiftslämnande på annat sätt än genom direktåtkomst om det inte är olämpligt. Det gäller dock enbart i förhållande till vissa i förordningarna uppräknade kategorier av mottagare, framför allt sådana till vilka det förekommer frekvent uppgiftslämnande.

Mot den bakgrunden bör enligt utredningens mening samma lagtekniska lösning som i domstolsdatalagen väljas i de brottsbekämpande myndigheternas registerförfattningar. Utredningen föreslår således att bestämmelserna ändras på det sättet att personuppgifter ska få lämnas ut elektroniskt om det inte är olämpligt.

Informationshanteringsutredningen anser att uttrycket ”utlämnande på medium för automatiserad behandling” bör utmönstras och föreslår att uttrycket ”utlämnande i elektronisk form” ska användas i stället (se SOU 2015:39 s. 442).

Ett modernare uttryckssätt är enligt utredningens mening att föredra. Eftersom registerförfattningarna ses över är det lämpligt att göra den förändringen nu. Även fortsättningsvis bör det i registerförfattningarna göras tydlig skillnad mellan elektroniskt utlämnande i form av direktåtkomst och elektroniskt utlämnande på annat sätt.

När kan elektroniskt utlämnande komma i fråga?

I fråga om elektroniskt utlämnande på annat sätt än genom direktåtkomst bör enligt utredningens mening skillnad göras mellan utlämnande till myndigheter och utlämnande till enskilda. Det bör normalt inte anses olämpligt att lämna personuppgifter elektroniskt till myndigheter (jfr SOU 2015:39 s. 447 f.). Om det i ett enskilt fall skulle bedömas vara olämpligt bör emellertid personuppgifterna lämnas på annat sätt.

Även när det gäller utlämnande till enskilda har lagstiftaren redan tagit ställning till att sådant utlämnande är godtagbart till vissa kategorier av mottagare, om det inte är olämpligt. Det gäller t.ex. uppgifter som lämnas till konkursförvaltare i vissa fall. Person-

uppgifter bör kunna lämnas ut elektroniskt till sådana kategorier i samma utsträckning som i dag.

När det gäller andra enskilda än de som i dag pekas ut i förordning kan det krävas närmare överväganden bl.a. med hänsyn till vem mottagaren är och vilken säkerhet mottagaren har för sin personuppgiftsbehandling. I de fallen är det svårare att göra en generell bedömning av om elektroniskt utlämnande kan vara lämpligt. Utredningen anser att regeringen bör kunna meddela föreskrifter som begränsar möjligheten att lämna ut personuppgifter elektroniskt på annat sätt än genom direktåtkomst.

5.7 Frågor om föreskriftsrätt m.m.

Utredningens bedömning: Bestämmelserna om föreskriftsrätt bör samlas i registerförfattningarna.

Utredningens förslag: Sådan föreskriftsrätt som inte längre fyller någon funktion ska tas bort.

Innan en myndighet utfärdar föreskrifter i frågor som berör särskilda risker för intrång i den personliga integriteten ska den samråda med Datainspektionen. Det ska regleras i förordning.

Skälen för utredningens bedömning och förslag

Föreskriftsrätt

I registerförfattningarna finns det ett flertal bestämmelser där det upplyses att regeringen själv kan meddela föreskrifter i en viss fråga, eller delegera den uppgiften till en myndighet. I dag är dessa bestämmelser utspridda i registerförfattningarna. Utredningen anser att regleringen blir lättare att överblicka och enklare att tillämpa om bestämmelserna om föreskriftsrätt samlas i slutet av varje kapitel i registerförfattningarna.

En annan fråga som aktualiserats vid genomgången av registerförfattningarna är om alla bestämmelser om föreskriftsrätt fyller någon praktisk funktion. I en del fall rör det sig om föreskriftsrätt som är knuten till bestämmelser som inte längre ska finnas kvar i registerförfattningarna. Sådana bestämmelser bör upphävas. Det

finns också vissa bestämmelser om vidaredelegation av föreskriftsrätt som inte bör behållas därför att det som regleringen avser enbart rör myndighetsinterna frågor eller därför att det är uppgifter som följer med rollen som personuppgiftsansvarig. Myndigheterna bör alltså inte ha någon föreskriftsrätt om det är fråga om interna förhållanden som kan regleras på annat sätt än i föreskrifter. Det gäller exempelvis föreskriftsrätten i 3 § polisdataförordningen om tillgången till personuppgifter, i 5 § andra stycket om begränsning av tillgången till vissa uppgifter och 8 § om sökning. Motsvarande bestämmelser i övriga registerförordningar bör också upphävas.

Samråd inför utfärdande av föreskrifter

I 29 § polisdataförordningen föreskrivs att innan Polismyndigheten eller Säkerhetspolisen meddelar föreskrifter i frågor som berör särskilda risker för intrång i den personliga integriteten, ska myndigheten samråda med Datainspektionen och Säkerhets- och integritetsskyddsnämnden. Motsvarande bestämmelser, som föreskriver samrådsskyldighet med enbart Datainspektionen, finns i 20 § kustbevakningsdataförordningen, 12 § åklagardataförordningen, 19 § tullbrottsdataförordningen och 18 § skattebrottsdataförordningen. Bestämmelserna är lite olika utformade. I vissa av paragraferna talas det om samråd och i andra om att Datainspektionen ska ges tillfälle att yttra sig.

Enligt utredningens mening är samarbetet mellan de personuppgiftsansvariga och tillsynsmyndigheten av stor betydelse. Reglerna om samrådsskyldighet bör vara likalydande, för att det inte ska råda någon tvekan om omfattningen av skyldigheten. I 3 kap. 7 § brottsdatalagen regleras samarbetet mellan personuppgiftsansvariga och tillsynsmyndigheten vid s.k. förhandssamråd. Utredningen anser att även det samarbete som bör föregå att föreskrifter utfärdas bör ha formen av samråd med tillsynsmyndigheten.

I 6 och 7 §§ kustbevakningsdataförordningen finns det bestämmelser om att Kustbevakningen får meddela föreskrifter. Enligt utredningens förslag tas föreskriftsrätten bort. Någon samrådsskyldighet med Datainspektionen bör då inte heller finnas.

6 Tillåtna rättsliga grunder och behandling för nya ändamål

6.1 Ändamål eller tillåtna rättsliga grunder?

6.1.1 Dagens ändamålsbestämmelser

Primära och sekundära ändamål

En grundläggande princip för all personuppgiftsbehandling är att personuppgifter får samlas in bara för särskilda, uttryckligt angivna och berättigade ändamål. De får inte heller behandlas för något ändamål som är oförenligt med det ändamål för vilket de samlades in. I registerförfattningar finns det därför normalt bestämmelser om för vilka ändamål personuppgifter får behandlas. Syftet är att ange ramen för vilken behandling som är tillåten. På så sätt kan användning och spridning av personuppgifter begränsas.

I de brottsbekämpande myndigheternas registerförfattningar delas ändamålen upp i primära och sekundära (se 2 kap. 7 och 8 §§ polisdatlagen, 3 kap. 2 och 3 §§ kustbevakningsdatlagen, 2 kap. 5 och 6 §§ åklagardatalagen, 2 kap. 5 och 6 §§ tullbrottsdatlagen och 2 kap. 5 och 6 §§ skattebrottsdatlagen). Bestämmelserna har samma utformning och liknande innehåll. När ändamålsbestämmelser diskuteras i detta kapitel avses dessa bestämmelser.

De primära ändamålen i de brottsbekämpande myndigheternas registerförfattningar reglerar behandlingen av de personuppgifter som behövs i den berörda myndighetens egen brottsbekämpande verksamhet. De sekundära ändamålen reglerar i vilken utsträckning personuppgifter som behandlas för något av de primära ändamålen får behandlas för att lämnas ut till andra myndigheter eller till enskilda för att tillgodose deras behov. Det kan också vara fråga om att personuppgifter i den brottsbekämpande verksamheten behöver

lämnas till verksamhet i samma myndighet som inte är brottsbekämpande för den verksamhetens behov.

Syftet med uppdelningen i primära och sekundära ändamål är att göra det tydligt både hur personuppgifter får användas i den brottsbekämpande verksamheten och för vilka ändamål och till vem uppgifterna får lämnas ut.

Även de ändamålsbestämmelser som gäller för Säkerhetspolisen och domstolarna är uppdelade i primära och sekundära. De har dock en annan utformning och ett annat innehåll och behandlas därför inte i detta kapitel. Ändamålsbestämmelserna i kriminalvårdens registerlagstiftning är också annorlunda utformade och behandlas inte heller i detta kapitel.

Informationshanteringsutredningens slutsatser

Informationshanteringsutredningen anser att det har skett en sammanblandning mellan vad som i dataskyddsrättslig mening är särskilda bestämda ändamål respektive tillåtna rättsliga grunder för behandling. Det finns enligt den utredningen risk att tillämparen blandar samman ändamål med rättslig grund och godtar ett i författning bestämt allmänt ändamål som ett särskilt och tillräckligt preciserat ändamål och drar den felaktiga slutsatsen att kravet på att det ska finnas särskilda, uttryckligt angivna och berättigade ändamål för behandlingen därmed är uppfyllt. Informationshanteringsutredningen anser att det skulle ge ett bättre integritetsskydd om personuppgiftsansvariga enbart vore hänvisade till att, utifrån de grundläggande kraven i 9 § första stycket c personuppgiftslagen, på eget ansvar formulera ändamål som är tillräckligt specifika för att ge ledning för vilka personuppgifter som är adekvata och inte för många för den aktuella behandlingen. Därför innehåller förslaget till myndighetsdatalag inga ändamålsbestämmelser och förutsätter inte heller att sådana ska finnas. I förslaget anges endast att personuppgifter får behandlas om det är nödvändigt för att en myndighet ska kunna utföra sin verksamhet (se SOU 2015:39 s. 277 f.).

Förslaget har fått ett blandat mottagande. Vissa remissinstanser anser att ändamålsbestämmelser har betydelse för att göra det tydligt för enskilda inom vilka ramar myndigheter får samla in och behandla personuppgifter och menar att den föreslagna bestämmel-

sen är alltför vag. Andra är positiva till förslaget och framhåller att det förenklar bedömningen av vilken personuppgiftsbehandling som är tillåten.

6.1.2 Bestämmelser om rättslig grund

Det måste alltid finnas en rättslig grund för behandling

Både dataskyddsdirektivet och dataskyddsförordningen utgår från att varje behandling av personuppgifter måste vila på en rättslig grund för att vara laglig. Det är alltså endast om det finns en rättslig grund som personuppgifter överhuvudtaget får behandlas.

Kravet på att det alltid ska finnas en rättslig grund för behandlingen av personuppgifter är inte nytt. Det framgår av artikel 7 i det nu gällande dataskyddsdirektivet och kommer till uttryck i bl.a. 10 § personuppgiftslagen. Det förs dock inga resonemang kring kravet på rättslig grund i förarbetena till de brottsbekämpande myndigheternas registerförfattningar. Det finns därför skäl att nu lyfta fram den frågan och diskutera hur kravet på rättslig grund förhåller sig till de primära och sekundära ändamålen i registerförfattningarna.

I artikel 6.1 i dataskyddsförordningen finns det en uttömmande uppräkningslista av de rättsliga grunderna för behandling av personuppgifter enligt förordningen. Utredningen återkommer till dem i avsnitt 6.4.1. Någon motsvarande uppräkningslista finns inte i direktivet. Däremot anges förutsättningarna för att en behandling ska vara laglig i artikel 8.1.

Regleringen i brottsdatalagen

Brottsdatalagen innehåller bestämmelser om tillåtna rättsliga grunder för behandlingen. Enligt 2 kap. 1 §, som genomför artikel 8.1 i direktivet, får personuppgifter behandlas om det är nödvändigt för att en behörig myndighet ska kunna utföra en arbetsuppgift i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa en straffrättslig påföljd eller upprätthålla allmän ordning och säkerhet. Arbetsuppgiften ska framgå av en bindande unionsrättsakt eller av en lag, en förordning eller ett

särskilt beslut i vilket regeringen uppdragit åt den behöriga myndigheten att ansvara för en sådan uppgift.

Grunden för att behandla personuppgifter finns alltså i regleringen av den behöriga myndighetens arbetsuppgifter. Som exempel kan nämnas att det i 2 § polislagen (1984:387) anges att en av Polismyndighetens huvuduppgifter är att utreda och beivra brott. Den arbetsuppgiften preciseras av bestämmelser i framför allt rättegångsbalken som reglerar hur förundersökning ska bedrivas och i vilka fall en polisman får utfärda föreläggande om ordningsbot. Ytterligare bestämmelser finns i bl.a. lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare och olika lagar om användningen av straffprocessuella tvångsmedel. På motsvarande sätt anges det i 3 § förordningen (2007:853) med instruktion för Kustbevakningen att myndigheten bl.a. ska bedriva övervakning för att förebygga och ingripa mot störningar i sjötrafiken, förhindra och upptäcka brottslig verksamhet, ingripa vid misstanke om brott och utreda och beivra eller bistå med utredningen av brott. Vilka brott Kustbevakningen har till uppgift att ingripa mot framgår bl.a. av lagen (1982:395) om Kustbevakningens medverkan vid polisiär övervakning och lagen (2000:1225) om straff för smuggling. Hur det ska göras regleras framför allt i rättegångsbalken och nyss nämnda lagar. Regleringar av motsvarande slag finns för övriga behöriga myndigheter.

Grunden för att behandla personuppgifter kan även finnas i regler som primärt gäller för andra myndigheter. Skyldigheten enligt 23 kap. 3 § andra stycket rättegångsbalken att biträda åklagare vid brottsutredning utgör den rättsliga grunden för att polisen ska kunna överlämna personuppgifter till åklagare i det brottsbekämpande arbetet. Motsvarande bestämmelser finns för Tullverket, Skatteverket och Kustbevakningen.

Regleringen i 2 kap. 1 § brottsdatalagen är således en del av den rättsliga grunden genom att de behöriga myndigheterna där ges rättsligt stöd för att behandla personuppgifter automatiserat för att utföra sina arbetsuppgifter. Ett sådant stöd krävs, eftersom regleringen av arbetsuppgiften i sig (t.ex. att hålla vittnesförhör) inte ger någon rätt att behandla personuppgifter. Det behöver dock inte finnas uttryckliga bestämmelser om att personuppgifter får behandlas automatiserat för att utföra en viss arbetsuppgift. Det är tillräckligt att behandlingen är ett nödvändigt led för att kunna

utföra arbetsuppgiften, om arbetsuppgiften ligger inom brottsdatalagens tillämpningsområde och täcks av myndighetens registerförfattning. Regleringen av personuppgiftsbehandling är i sig inte tillräcklig, om det saknas författningsstöd för själva arbetsuppgiften (se SOU 2017:29 s. 238 f.). Att behandlingen av personuppgifter är rättsligt grundad innebär alltså att det finns både en reglerad arbetsuppgift och bestämmelser om att personuppgifter får behandlas för att utföra arbetsuppgiften.

Skyldigheten att diarieföra inkomna handlingar regleras i 5 kap. offentlighets- och sekretesslagen (2009:400). I 2 kap. 2 § brottsdatalagen föreskrivs att personuppgifter får behandlas om det är nödvändigt för diarieföring eller om uppgifterna lämnats till en behörig myndighet i en anmälan, ansökan eller liknande och behandlingen är nödvändig för handläggningen.

Att behandlingen är rättsligt grundad räcker inte

Den omständigheten att viss behandling är rättsligt grundad innebär inte att vilka personuppgifter som helst får behandlas eller att det får göras på valfritt sätt. Den personuppgiftsansvarige måste också iaktta de krav som föreskrivs i övriga bestämmelser i brottsdatalagen. Personuppgifter får enbart behandlas för särskilda, uttryckligt angivna och berättigade ändamål. Bara de personuppgifter som är adekvata och relevanta för ändamålet med behandlingen får behandlas. För behandling av känsliga personuppgifter gäller särskilda krav. Dessutom ska den personuppgiftsansvarige iaktta eventuella särregler och andra bestämmelser i registerförfattningar som också gäller för personuppgiftsbehandlingen i fråga.

6.1.3 Primära och sekundära ändamålsbestämmelser är bestämmelser om rättslig grund

Utredningens bedömning: De bestämmelser i polisdatalagen, kustbevakningsdatalagen, åklagardatalagen, tullbrottsdatalagen och skattebrottsdatalagen som kallas primära och sekundära ändamålsbestämmelser är en del av den rättsliga grunden för behandling av personuppgifter.

Skälen för utredningens bedömning

De primära ändamålsbestämmelserna

Utredningen anser att det finns fog för Informationshanteringsutredningens uppfattning att vad som i dataskyddsrättslig mening är tillåtna rättsliga grunder för behandling och vad som är renodlade ändamålsbestämmelser ibland har blandats samman. Det kan leda till att tillämparen förväxlar ändamål med rättslig grund och godtar ett i författning angivet allmänt ändamål som ett särskilt och tillräckligt preciserat ändamål i det enskilda fallet. Ett exempel är uppgiftssamlingen benämnd ”Kringresande” som fördes av Polismyndigheten i Skåne. Säkerhets- och integritetsskyddsnämnden kritiserade vid sin granskning bl.a. att ändamålet med personuppgiftsbehandlingen var alldeles för vitt. Personuppgifterna hade samlats in för specifika ändamål men lagrades och behandlades sedan i uppgiftssamlingen för ändamålet länsövergripande brottslighet. Ändamålet låg visserligen inom ramen för sådan underrättelseverksamhet som avses i 2 kap. 7 § 1 polisdatalagen. Det uppfyllde dock inte det grundläggande kravet på att behandling bara ska utföras för särskilda, uttryckligt angivna och berättigade ändamål (uttalande den 15 november 2013, dnr 173-2013).

Enligt 2 kap. 3 § brottsdatalagen ska all behandling av personuppgifter utföras för särskilda, uttryckligt angivna och berättigade ändamål. Det är i förhållande till ändamålen som det ska prövas vilka personuppgifter som är adekvata och relevanta för behandlingen, att inte för många personuppgifter behandlas och att de inte behandlas under längre tid än nödvändigt. Ändamålen måste därmed vara tillräckligt specifika för att ge ledning för den bedömningen.

Författningsbestämmelser som anger för vilket eller vilka ändamål personuppgifter får behandlas i en viss verksamhet måste vara generellt utformade, eftersom de ska kunna tåla utvecklingen av ny teknik och vissa förändringar i myndighetens sätt att arbeta. En ändamålsbestämmelse bör dock enligt utredningens mening ge någon ledning för prövningen av vilka personuppgifter som är adekvata och relevanta för behandlingen.

De primära ändamålsbestämmelserna i registerförfattningarna ger enligt utredningens mening inte någon egentlig ledning för prövningen av vilka personuppgifter som får behandlas. I exem-

pelvis 2 kap. 7 § polisdatalagen anges endast att Polismyndigheten får behandla personuppgifter för att utföra vissa av sina huvudsakliga arbetsuppgifter, bl.a. utreda och beivra brott. Syftet med bestämmelsen är att precisera när personuppgifter alls får behandlas i myndighetens brottsbekämpande verksamhet. Den utgör den yttre ramen inom vilken de särskilda, uttryckliga och berättigade ändamålen med behandlingen i enskilda fall ska bestämmas. Utredningen anser därför att de bestämmelser i myndigheternas registerförfattningar som i dag kallas primära ändamålsbestämmelser inte är ändamålsbestämmelser i egentlig mening. De är däremot på samma sätt som 2 kap. 1 § brottsdatalagen en del av den rättsliga grunden och tydliggör att personuppgiftsbehandling är tillåten när arbetsuppgifterna fullgörs. I avsnitt 6.3.1 diskuteras om innehållet i de primära ändamålsbestämmelserna bör behållas.

De sekundära ändamålsbestämmelserna

De sekundära ändamålsbestämmelserna reglerar i vilken utsträckning personuppgifter som behandlas för något primärt ändamål även får behandlas för att lämnas till andra för att tillgodose deras behov. De reglerar alltså behandling för nya ändamål. Enligt bestämmelserna får personuppgifter behandlas framför allt för att ge andra myndigheter information som behövs i viss typ av verksamhet där eller för att lämna information till andra verksamheter inom den egna myndigheten för att de ska kunna utföra en viss arbetsuppgift.

På samma sätt som de primära ändamålsbestämmelserna är de sekundära i stor utsträckning allmänt hållna och ger inte någon egentlig ledning för prövningen av vilka personuppgifter som får behandlas. I 2 kap. 8 § polisdatalagen anges i punkten 1 att personuppgifter får lämnas ut om de behövs i brottsbekämpande verksamhet hos Säkerhetspolisen, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket. Det motsvarar de primära ändamålsbestämmelserna i de mottagande myndigheternas registerförfattningar. Enligt punkten 2 får personuppgifter också lämnas ut om uppgifterna behövs i brottsbekämpande verksamhet hos utländska myndigheter eller mellanfolkliga organisationer. Personuppgifter får alltså lämnas ut till andra

brottsbekämpande myndigheter för att tillgodose behov i deras motsvarande verksamhet. Punkterna 3, 4, 5 och 7 anger att personuppgifter som Polismyndigheten behandlar i den brottsbekämpande verksamheten under vissa förutsättningar får behandlas för att lämnas till andra verksamheter inom myndigheten och till andra myndigheter för att tillgodose informationsbehov där. Samtliga nu nämnda punkter, som endast anger att personuppgifter får behandlas om det behövs för någon annans verksamhet, är enligt utredningens mening bestämmelser om rättslig grund. Det är endast punkten 6, där det anges att personuppgifter får lämnas till Migrationsverket för att verket ska kunna kontrollera fingeravtryck som tagits med stöd av 9 kap. 8 § utlänningslagen (2005:716) mot Polismyndighetens fingeravtrycks- och signalementsregister, som enligt utredningens mening är så konkret att den är en ändamålsbestämmelse. Den bestämmelsen behandlas i avsnitt 7.7.2. I avsnitt 6.3.2 och 6.4.2 diskuteras om de övriga punkterna kan och bör behållas.

Regleringen i 2 kap. 8 § polisdatalagen har utgjort mönster för övriga brottsbekämpande myndigheters sekundära ändamålsbestämmelser. Motsvarande bedömning som har gjorts i fråga om den paragrafen görs beträffande de sekundära ändamålsbestämmelserna i de övriga registerförfattningarna.

6.2 Ny utgångspunkt i brottsdatalagen

Som framgår av avsnitt 6.1 skiljer regleringen i registerförfattningarna mellan behandling för den egna brottsbekämpande verksamhetens behov och behandling för att tillhandahålla information för andras behov. När personuppgifter lämnas ut som ett led i myndighetens egen brottsbekämpande verksamhet, inte i syfte att tillgodose någon annans behov, anses utlämnandet omfattas av de primära ändamålen.

Enligt 2 kap. 3 § brottsdatalagen får som nyss nämnts personuppgifter behandlas bara för särskilda, uttryckligt angivna och berättigade ändamål. Innan personuppgifter behandlas för ett nytt ändamål inom lagens tillämpningsområde ska det enligt 2 kap. 4 § säkerställas dels att det finns en tillåten rättslig grund för den nya behandlingen, dels att behandlingen är både nödvändig och proportionerlig för det nya ändamålet. Som utredningen konstaterar i

delbetänkandet saknar det betydelse om det är den personuppgiftsansvarige som ursprungligen har samlat in personuppgifterna som utför behandlingen för det nya ändamålet eller om det är en annan personuppgiftsansvarig, så länge de båda är behöriga myndigheter och ändamålet med behandlingen ligger inom lagens tillämpningsområde. Även behandling för att lämna ut personuppgifter till någon som inte är en behörig myndighet kan omfattas av lagen, om ändamålet med behandlingen ligger inom tillämpningsområdet (se SOU 2017:29 s. 247 f.). Det saknar således betydelse om behandlingen för det nya ändamålet utförs för behov i myndighetens egen brottsbekämpande verksamhet eller för att tillgodose en annan myndighets behov av information, så länge ändamålet med behandlingen ligger inom lagens tillämpningsområde. Det centrala är i stället den prövning som alltid ska göras innan personuppgifter får behandlas för ett nytt ändamål.

Regleringen i 2 kap. 4 § brottsdatalagen gäller dock bara vid behandling för nya ändamål inom lagens tillämpningsområde. Av 2 kap. 21 § framgår att dataskyddsförordningen ska tillämpas vid behandling för ändamål utanför brottsdatalagens tillämpningsområde. I utredningens uppdrag ingår att analysera om det finns utrymme för och behov av att inom dataskyddsförordningens tillämpningsområde införa eller behålla specifik reglering i svensk rätt om behandling av personuppgifter för att tillhandahålla information (dir. 2016:21 s. 10 f.). I avsnitt 6.3.2 diskuteras behandling för nya ändamål inom brottsdatalagens tillämpningsområde. Behandling för ändamål utanför tillämpningsområdet tas upp i avsnitt 6.4.

6.3 Behandling för ändamål inom brottsdatalagens tillämpningsområde

6.3.1 Tillåtna rättsliga grunder för behandling

Utredningens förslag: Det ska finnas bestämmelser i registerförfattningarna om vad som utgör tillåtna rättsliga grunder för behandling.

Skälen för utredningens förslag

Bestämmelser om tillåtna rättsliga grunder för behandling

Som konstateras i avsnitt 6.1.3 bör dagens primära ändamålsbestämmelser ses som en del av den rättsliga grunden som ger stöd för att behandla personuppgifter för att utföra vissa arbetsuppgifter. Frågan är om det alltså finns behov av sådana bestämmelser i registerförfattningarna när 2 kap. 1 § brottsdatalagen innehåller en generell bestämmelse om tillåtna rättsliga grunder för behandling av personuppgifter.

Ingen av de behöriga myndigheterna har i dag en registerförfattning som gäller för hela brottsdatalagens tillämpningsområde. Även om det finns bestämmelser som avgränsar tillämpningsområdet för de olika registerförfattningarna fyller bestämmelser som tydliggör inom vilka ramar var och en av myndigheterna får behandla personuppgifter en viktig funktion både för tillämpare och för enskilda. Bestämmelser som sätter ramar för personuppgiftsbehandlingen innebär också att lagstiftaren tvingas överväga behovet av ändrad reglering av personuppgiftsbehandlingen om myndigheten tillförs nya arbetsuppgifter. Det är enligt utredningens mening till fördel från integritetsskyddssynpunkt (jfr SOU 2015:39 s. 281). Innehållet i de bestämmelser som i dag kallas primära ändamålsbestämmelser bör därför behållas.

Det bör dock tydliggöras att bestämmelserna i fråga är en del av den rättsliga grunden. För att det inte ska uppstå någon tvekan om hur regleringarna förhåller sig till varandra bör bestämmelserna därför ersätta 2 kap. 1 § brottsdatalagen inom respektive registerförfattnings tillämpningsområde. I vilken utsträckning bestämmelserna i registerförfattningarna behöver anpassas till terminologin i brottsdatalagen behandlas i kapitlet om de särskilda registerförfattningarna.

Det kan tillfogas att den närmare innebörden av de tillåtna rättsliga grunderna i respektive myndighets registerförfattning måste uttolkas tillsammans med regleringen av arbetsuppgifterna. Polismyndighetens uppgift att utreda brott är generell, medan Tullverket, Kustbevakningen och Skatteverket bara har till uppgift att utreda vissa typer av brott. På motsvarande sätt har Polismyndigheten ett generellt uppdrag att förebygga, förhindra och upptäcka

brottslig verksamhet, medan de andra myndigheterna endast har den uppgiften när det gäller vissa typer av brottslighet.

För åklagarväsendets del innefattar lagföra brott både beslut om åtalsunderlåtelse, åtalsbeslut och beslut om strafföreläggande. För Tullverket, som har vissa åklagarfunktioner, innebär begreppet i huvudsak detsamma men bara såvitt avser sådana brott som myndigheten får lagföra. Till det kommer att utfärda förelägganden av ordningsbot för sådana brott. För Polismyndigheten och Kustbevakningen är tillämpningsområdet smalare. Där innefattar lagföra brott enbart utfärdande av förelägganden av ordningsbot. Polismyndighetens rätt att utfärda ordningsbot är generell, men för Kustbevakningen är rätten begränsad till vissa brottstyper.

Även när det gäller straffverkställighet och ordningshållning finns det vissa skillnader i fråga om arbetsuppgifterna som påverkar vilken personuppgiftsbehandling som är tillåten.

Behandling i registervårdande syfte behöver inte regleras

Både Säkerhets- och integritetsskyddsnämnden och Datainspektionen har påtalat att myndigheter behöver rättsligt stöd för att kunna behandla personuppgifter i registervårdande syfte. Det gäller framför allt möjligheterna att använda känsliga personuppgifter som sökbegrepp (se nämndens uttalande den 14 juni 2016, dnr 112-2015, och inspektionens samrådsyttrande den 1 juli 2016, dnr 1047-2016).

Det är givetvis viktigt att personuppgiftsansvariga kan göra sökningar och på annat sätt behandla personuppgifter om det behövs för att kunna se till att bestämmelserna om personuppgiftsbehandling efterlevs. Det kan exempelvis krävas för att kontrollera att personuppgifter inte behandlas för länge eller att sökningar med användande av känsliga personuppgifter inte utförs i strid med regelverket. I kontrollarbetet kan sökningar eller annan personuppgiftsbehandling som hade varit förbjuden i den operativa verksamheten vara nödvändig. Enligt utredningens mening måste sådan registervård anses vara en integrerad del av den personuppgiftsansvariges skyldigheter enligt brottsdatalagen och registerförfattningarna. Det bör också noteras att det är få personer som arbetar med registervård och att de behandlar personuppgifterna enbart i

syfte att kontrollera att regelverket efterlevs, vilket knappast påverkar enskildas integritet negativt.

Lagrådet har vid granskning av registerlagstiftning uttalat att planering, uppföljning och utvärdering av verksamheten är en integrerad del av själva verksamheten och inte någon fristående aktivitet som behöver regleras särskilt. Det har därför ansetts att det inte behövs någon särskild ändamålsbestämmelse som ger stöd för behandling av personuppgifter för bl.a. planering och uppföljning av verksamheten (se t.ex. Tullverkets brottsbekämpning – Effektivare uppgiftsbehandling, prop. 2004/05:164, s. 179 och Åklagardatalag, 2014/15:63, s. 63). Motsvarande bedömning bör enligt utredningens mening göras när det gäller registervård. Det behöver således inte regleras särskilt att personuppgiftsbehandling för registervård är tillåten.

6.3.2 Behandling för nya ändamål

Utredningens bedömning: Enligt brottsdatalagen ska det, innan personuppgifter behandlas för nya ändamål, säkerställas att det finns en rättslig grund för behandlingen och att den är nödvändig och proportionerlig för det nya ändamålet. Någon annan begränsning av utlämnande av personuppgifter bör inte införas.

Utredningens förslag: De sekundära ändamålsbestämmelserna i polisdatalagen, kustbevakningsdatalagen, åklagardatalagen, tullbrottsdatalagen och skattebrottsdatalagen ska upphävas i de delar de avser behandling för ändamål inom brottsdatalagens tillämpningsområde.

Skälen för utredningens bedömning och förslag

Nuvarande reglering av behandling för nya ändamål

I 9 § första stycket d personuppgiftslagen finns en generell bestämmelse om vidarebehandling. Där regleras finalitetsprincipen, enligt vilken personuppgifter inte får behandlas för något ändamål som är

oförenligt med det ändamål för vilket uppgifterna samlades in. Bestämmelsen gäller för alla myndigheter i rättskedjan.

De sekundära ändamålsbestämmelserna i de brottsbekämpande myndigheternas registerförfattningar innehåller särskilda regler om vidarebehandling. De reglerar när det är tillåtet att behandla personuppgifter som behandlas för något av de primära ändamålen för att tillhandahålla information till andra myndigheter eller till andra verksamheter inom den egna myndigheten för deras behov. Det handlar alltså alltid om behandling av redan insamlade uppgifter för nya ändamål. De sekundära ändamålen omfattar behandling för ändamål som ligger både inom och utanför brottsdatalagens tillämpningsområde. I detta avsnitt behandlar utredningen de delar av bestämmelserna som avser ändamål inom brottsdatalagens tillämpningsområde. Behandling för ändamål utanför tillämpningsområdet behandlas i avsnitt 6.4.2.

Enligt de sekundära ändamålsbestämmelserna får de brottsbekämpande myndigheterna för det första lämna ut personuppgifter som redan behandlas, om uppgifterna behövs i brottsbekämpande verksamhet hos övriga brottsbekämpande myndigheter och hos utländsk myndighet eller mellanfolklig organisation. Polismyndigheten och Tullverket får dessutom tillhandahålla information till Kriminalvården för att den myndigheten ska kunna förebygga brott och upprätthålla säkerheten i sin verksamhet. Polismyndigheten får även lämna personuppgifter ur en förundersökning till konkursförvaltare.

I kapitel 8 i delbetänkandet behandlar utredningen olika gränsdragningsfrågor (se SOU 2017:29 s. 181 f.). Där framgår att det på vissa områden inte går att säga att all behandling omfattas av brottsdatalagens tillämpningsområde eller ligger utanför det, utan att syftet med behandlingen i det enskilda fallet blir avgörande för vilket regelverk som ska tillämpas. Det innebär att vissa punkter i en sekundär ändamålsbestämmelse kan omfatta ändamål som ligger både inom och utanför tillämpningsområdet för brottsdatalagen. Det gäller t.ex. rätten att behandla personuppgifter för att fullgöra författningsreglerade uppgiftsskyldigheter. Exempel på sådan uppgiftsskyldighet som ligger inom brottsdatalagens tillämpningsområde är Polismyndighetens omfattande skyldighet att lämna personuppgifter enligt 36 § förordningen (2001:682) om behandling av personuppgifter inom kriminalvården. Även rätten att behandla

personuppgifter för att tillhandahålla information som behövs i en annan myndighets verksamhet, om det åligger den brottsbekämpande myndigheten att bistå den andra myndigheten med viss uppgift, kan avse ändamål både inom och utanför brottsdatalagens tillämpningsområde. Detsamma gäller information som tillhandahålls inom ramen för myndighetsöverskridande samverkan mot brott och Polismyndighetens tillhandahållande av information till sådan verksamhet hos myndigheten som avser handräckning.

Kan nuvarande reglering av utlämnande behållas?

Innan personuppgifter behandlas för ett nytt ändamål inom brottsdatalagens tillämpningsområde ska det enligt 2 kap. 4 § säkerställas dels att det finns en tillåten rättslig grund för behandlingen, dels att behandlingen är nödvändig och proportionerlig för det nya ändamålet. Frågan är om det vid sidan av den regeln kan finnas bestämmelser som motsvarar de sekundära ändamålsbestämmelserna.

Behandling för nya ändamål kan leda till ökad spridning av personuppgifter genom att fler får tillgång till dem. Det kan också leda till att uppgifterna behandlas under längre tid än vad som var avsett från början. Behandling för nya ändamål kan därmed medföra ökat intrång i enskildas personliga integritet. Som utredningen framhåller i delbetänkandet är det därför viktigt att en noggrann prövning görs innan personuppgifter behandlas för ett nytt ändamål (se SOU 2017:29 s. 249). Om den nuvarande utformningen av de sekundära ändamålsbestämmelserna skulle behållas, där utlämnande av personuppgifter i de flesta fall är tillåtet utan någon annan prövning än om det är nödvändigt att tillhandahålla informationen, skulle prövningen enligt 2 kap. 4 § brottsdatalagen sättas ur spel. En sådan prövning krävs enligt artikel 4.2 i direktivet. Det är därför inte förenligt med direktivet att behålla de sekundära ändamålsbestämmelserna med den utformning de har i dag.

Bör möjligheterna att lämna ut personuppgifter begränsas på annat sätt?

Utredningen konstaterar i delbetänkandet att direktivet inte hindrar att man i nationell rätt sätter gränser för i vilken utsträckning personuppgifter får lämnas mellan myndigheter. Sådana begränsningar kan bidra till att skydda enskildas personliga integritet och göra det tydligt och förutsebart i vilken utsträckning behöriga myndigheter får lämna personuppgifter till andra (se SOU 2017:29 s. 253). I förarbetena till flera av registerförfattningarna framhåller regeringen emellertid att det från brottsbekämpande synpunkt är angeläget att samhällets samlade resurser används på ett så rationellt och effektivt sätt som möjligt. Brottsligheten känner inga geografiska gränser eller myndighetsgränser och det framstår därför som självklart att brottsbekämpande myndigheter ska samverka med varandra. Sådan samverkan förutsätter möjligheter till effektivt utbyte av information (se bl.a. prop. 2009/10:85 s. 166 f. och prop. 2016/17:91 s. 96 f.).

Ett av syftena med brottsdatalagen är att säkerställa att behöriga myndigheter kan behandla och utbyta personuppgifter med varandra på ett ändamålsenligt sätt. Den prövning som enligt 2 kap. 4 § brottsdatalagen ska göras innan personuppgifter behandlas för ett nytt ändamål ska alltid göras innan en behörig myndighet får lämna ut information. Enligt utredningens mening är den prövningen tillräcklig för att skydda enskildas integritet. Det finns därför inte skäl att föreslå någon annan begränsning i möjligheten att tillhandahålla information för ändamål inom brottsdatalagens tillämpningsområde. Det innebär att de sekundära ändamålsbestämmelserna i polisdatalagen, kustbevakningsdatalagen, åklagardatalagen, tullbrottsdatalagen och skattebrottsdatalagen bör upphävas i de delar de avser behandling för ändamål inom brottsdatalagens tillämpningsområde. Utredningen återkommer i avsnitt 6.5 till vad som bör gälla vid författningsreglerad uppgiftsskyldighet.

6.4 Behandling för ändamål utanför brottsdatalagens tillämpningsområde

6.4.1 Tillämpningen av dataskyddsförordningen

Nuvarande reglering av behandling för nya ändamål

Som anges i avsnitt 6.3.2 regleras vidarebehandling av personuppgifter dels i 9 § första stycket i personuppgiftslagen, dels i de sekundära ändamålsbestämmelserna i registerförfattningarna. De sekundära ändamålsbestämmelserna reglerar behandling för ändamål som både ligger inom och utanför brottsdatalagens tillämpningsområde. I detta avsnitt behandlas de delar som reglerar ändamål utanför tillämpningsområdet.

Polismyndigheten och Tullverket får behandla personuppgifter för att tillhandahålla information som behövs i annan verksamhet som respektive myndighet ansvarar för, om det finns särskilda skäl för det. Motsvarande bestämmelser finns för Kustbevakningen och Skatteverket, men de är mer preciserade.

Flera av punkterna i de sekundära ändamålsbestämmelserna omfattar som nyss nämnts ändamål som ligger både inom och utanför brottsdatalagens tillämpningsområde. Det gäller bl.a. rätten att behandla personuppgifter för att fullgöra författningsreglerade uppgiftsskyldigheter. Utanför tillämpningsområdet ligger exempelvis Polismyndighetens skyldighet att lämna personuppgifter enligt 14 kap. 1 § socialtjänstlagen (2001:453) och 6 kap. 12 § smittskyddslagen (2004:168). Även rätten att behandla personuppgifter för att tillhandahålla information som behövs i en annan myndighets verksamhet, om det åligger den brottsbekämpande myndigheten att bistå den andra myndigheten med viss uppgift, kan avse ändamål utanför brottsdatalagens tillämpningsområde. Som exempel kan nämnas skyldigheten att bistå Riksdagens ombudsmän vid granskning av andra myndigheter, t.ex. socialförvaltningen. Det gäller också information som tillhandahålls inom ramen för myndighetsöverskridande samverkan mot brott, om syftet med utlämnandet t.ex. är att bidrag eller andra utbetalningar ska kunna dras in. Även Polismyndighetens tillhandahållande av information till sådan verksamhet hos myndigheten som avser handräckning kan avse ändamål utanför brottsdatalagens tillämpningsområde, exem-

pelvis om handräckning lämnas åt någon som bedriver hälso- och sjukvård.

Dataskyddsförordningen ska tillämpas redan vid utlämnandet

I 2 kap. 21 § brottsdatalagen upplyses om att dataskyddsförordningen ska tillämpas när en behörig myndighet behandlar personuppgifter för ändamål utanför lagens tillämpningsområde. Som anges i delbetänkandet ska förordningen tillämpas redan när en behörig myndighet tillhandahåller personuppgifter till andra, om ändamålet ligger utanför brottsdatalagens tillämpningsområde (se SOU 2017:29 s. 292). Det gäller när personuppgifter ska lämnas ut till myndigheter och andra aktörer som inte är behöriga myndigheter för deras behov. Som exempel kan nämnas när Kustbevakningen lämnar personuppgifter till Sjöfartsverket eller Transportstyrelsen efter en fartygskollision. Personuppgifter som en behörig myndighet behandlar enligt brottsdatalagen kan också behöva lämnas till en enhet inom samma myndighet som bedriver verksamhet utanför lagens tillämpningsområde. Personuppgifter som behandlas i Polismyndighetens brottsbekämpande verksamhet kan t.ex. behöva lämnas till den verksamhet inom myndigheten där frågor om pass eller olika typer av tillstånd behandlas.

Regleringen i dataskyddsförordningen

Dataskyddsförordningen utgår, på samma sätt som direktivet, från att varje behandling av personuppgifter måste vila på en rättslig grund. De rättsliga grunderna räknas uttömmande upp i artikel 6.1 i förordningen. Om ingen av dem är tillämplig är behandlingen inte laglig och får därmed inte utföras. De rättsliga grunder som räknas upp i artikel 6.1 är bl.a. följande:

- a) Den registrerade har lämnat sitt samtycke till behandlingen.
- b) Behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås.
- c) Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som den personuppgiftsansvarige har.

- d) Behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller en annan fysisk person.
- e) Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.

Hur de olika punkterna ska tolkas utvecklas av Dataskyddsutredningen. Den utredningen uttalar bl.a. att det är rimligt att anta att alla uppgifter som utförs av statliga myndigheter i syfte att uppfylla ett uttryckligt uppdrag av riksdag eller regering är av allmänt intresse (se SOU 2017:39 s. 124). Det är därför framför allt artikel 6.1 e som kan bli relevant när behöriga myndigheter lämnar ut personuppgifter för ändamål utanför brottsdatalogens tillämpningsområde. Även artikel 6.1 c och d bör kunna aktualiseras.

Enligt artikel 6.2 får medlemsstaterna i vissa fall behålla eller införa mer specifika bestämmelser för att anpassa tillämpningen av bestämmelserna i förordningen med hänsyn till behandling av personuppgifter för att efterleva artiklarna 6.1 c eller e. I artikel 6.3 anges att den rättsliga grunden för behandling som avses i punkterna i fråga ska fastställas i enlighet med unionsrätten eller en medlemsstats nationella rätt. Artikel 6.3 ger också ett visst utrymme för medlemsstaterna att specificera villkoren för när personuppgifter får behandlas och hur det ska gå till. I artikeln anges att den rättsliga grund som fastställer en rättslig förpliktelse, myndighetsutövning eller en uppgift av allmänt intresse kan innehålla särskilda bestämmelser för att anpassa tillämpningen av bestämmelserna i förordningen. Som exempel nämns bl.a. de allmänna villkor som ska gälla för behandlingen, vilken typ av personuppgifter som ska behandlas, vilka registrerade som berörs, de enheter till vilka personuppgifterna får lämnas ut och för vilka ändamål. Av skäl 10 framgår att förordningen inte utesluter att det i medlemsstaternas nationella rätt fastställs närmare omständigheter för specifika situationer där personuppgifter behandlas, inbegripet mer exakta villkor för laglig behandling. Bestämmelser som specificerar villkoren för laglig behandling måste dock uppfylla ett mål av allmänt intresse och vara proportionerliga mot det legitima mål som eftersträvas. Det innebär enligt Dataskyddsutredningen att lagstiftaren måste göra en avvägning mellan å ena sidan behovet av att uppgiften kan

utföras på ett effektivt och rättssäkert sätt och å andra sidan den enskildes rätt till skydd för sina personuppgifter (SOU 2017:39 s. 134).

6.4.2 En prövning ska göras innan personuppgifter lämnas ut

Utredningens förslag: Det ska inte längre anges i vilka situationer personuppgifter som behandlas med stöd av registerförfattningarna får lämnas ut. Regleringen ska i stället bygga på att det ska göras en prövning innan uppgifterna lämnas ut.

De sekundära ändamålsbestämmelserna i polisdatalagen, kustbevakningsdatalagen, åklagardatalagen, tullbrottsdatalagen och skattebrottsdatalagen ska upphävas även i de delar de avser behandling för ändamål utanför brottsdatalagens tillämpningsområde.

Skälen för utredningens förslag

Kan den nuvarande regleringen behållas?

Det råder enligt utredningens mening ingen tvekan om att det är tillåtet att i registerförfattningar reglera utlämnandefrågor på data-skyddsförordningens tillämpningsområde. Till skillnad från vad som gäller vid behandling för nya ändamål inom brottsdatalagens tillämpningsområde skulle det därmed vara möjligt att behålla innehållet i de sekundära ändamålsbestämmelserna när det är fråga om behandling för nya ändamål utanför tillämpningsområdet.

I förarbetena till de brottsbekämpande myndigheternas registerförfattningar har regeringen gjort bedömningen att det inte är möjligt att uttömmande reglera alla de situationer där vidarebehandling av personuppgifter kan komma att aktualiseras. De sekundära ändamålen har därför uttryckts så preciserat och fullständigt som möjligt, men kompletteras av en möjlighet att i enskilda fall tillhandahålla personuppgifter för andra ändamål än de angivna, om det nya ändamålet inte kan anses oförenligt med insamlingsändamålet (se t.ex. prop. 2009/10:85 s. 98 f. och prop. 2016/17:91 s. 89). Målsättningen är enligt förarbetena att de sekundära ändamålen ska omfatta merparten av myndigheternas uppgiftslämnande.

Det är inte heller nu möjligt att reglera alla de situationer där personuppgifter kan behöva behandlas för nya ändamål för att tillhandahållas annan verksamhet inom myndigheten eller lämnas till andra myndigheter eller enskilda. Om regleringen ska behållas måste den således kompletteras med en bestämmelse som ger möjlighet att tillhandahålla personuppgifter även i andra fall än de som räknas upp i de sekundära ändamålsbestämmelserna. Som anges i delbetänkandet bedömer utredningen att den behandling som görs då blir en ursprungsbehandling enligt dataskyddsförordningen, vilket gör att finalitetsprincipen inte ska tillämpas på den behandlingen (se SOU 2017:29 s. 292 f.). Även om det är möjligt att behålla innehållet i de sekundära ändamålsbestämmelserna kan de alltså inte ha samma utformning som i dag.

Bör regleringen behållas?

Ett syfte med dagens sekundära ändamålsbestämmelser är att underlätta bedömningen av om kraven enligt finalitetsprincipen är uppfyllda. Lagstiftaren har bedömt att det är förenligt med det ursprungliga ändamålet med behandlingen att vidarebehandla personuppgifterna i de angivna situationerna (se bl.a. prop. 2009/10:85 s. 99 och prop. 2016/17:91 s. 102). Tillämparen behöver därför i de flesta fall bara pröva om det är nödvändigt att tillhandahålla informationen som någon annan har behov av. För Polismyndigheten och Tullverket gäller en ytterligare begränsning i de fall där personuppgifter behövs i annan verksamhet som respektive myndighet ansvarar för. Då får personuppgifter tillhandahållas endast om det finns särskilda skäl för det (se 2 kap. 8 § första stycket 4 polisdatalagen och 2 kap. 6 § första stycket 4 tullbrottsdatalagen).

Om behandling för ändamål utanför brottsdatalagens tillämpningsområde skulle regleras ungefär på samma sätt som i dag, dvs. att de situationer där det är tillåtet att tillhandahålla information räknas upp så fullständigt som möjligt så att merparten av uppgiftslämnandet omfattas, skulle det innebära att tillämparen i de flesta fall inte behöver göra någon annan prövning än om det är nödvändigt att lämna uppgifterna. I 2 kap. 4 § brottsdatalagen föreskrivs att det innan personuppgifter behandlas för ett nytt ändamål inom lagens tillämpningsområde ska säkerställas att det finns en

tillåten rättslig grund för den nya behandlingen och att behandlingen är nödvändig och proportionerlig för det nya ändamålet. Det skulle enligt utredningens mening skapa en omotiverad skillnad att kräva en noggrannare prövning för behandling för nya ändamål inom brottsdatalagens tillämpningsområde än utanför det. Det borde snarare ställas högre krav för att få behandla personuppgifter som förekommer i den brottsbekämpande verksamheten för nya ändamål utanför brottsdatalagens tillämpningsområde.

Det kan tilläggas att personuppgifter som behandlas med stöd av dataskyddsförordningen får behandlas för nya ändamål endast om behandlingen är förenlig med finalitetsprincipen. Det måste således göras en prövning av om det nya ändamålet är förenligt med det ändamål som uppgifterna samlades in för när personuppgifter vidarebehandlas enligt förordningen.

Även om det är olika prövningar som ska göras så krävs det alltså en prövning innan personuppgifter behandlas för nya ändamål både inom brottsdatalagens och inom dataskyddsförordningens tillämpningsområde. Mot den bakgrunden anser utredningen att är rimligt att kräva en prövning även när personuppgifter som behandlas med stöd av brottsdatalagen ska behandlas för ändamål utanför lagens tillämpningsområde. De situationer där personuppgifter som redan behandlas bör få behandlas för att tillhandahållas andra bör därför inte längre räknas upp. Regleringen bör i stället utgå från att det alltid ska göras en prövning innan uppgifter behandlas för nya ändamål. De sekundära ändamålsbestämmelserna i polisdatalagen, kustbevakningsdatalagen, åklagardatalagen, tullbrottsdatalagen och skattebrottsdatalagen bör därför upphävas även i de delar de avser behandling för ändamål utanför brottsdatalagens tillämpningsområde.

6.4.3 Utformningen av regleringen

Utredningens förslag: Innan personuppgifter, som behandlas med stöd av brottsdatalagen, behandlas för ändamål utanför lagens tillämpningsområde ska det säkerställas att behandlingen är nödvändig och proportionerlig för det nya ändamålet.

Överträdelse av bestämmelsen om behandling för nya ändamål utanför brottsdatalagens tillämpningsområde ska kunna föranleda sanktionsavgift.

Skälen för utredningens förslag

En prövning av nödvändighet och proportionalitet ska alltid göras

Frågan är då vad som bör krävas för att personuppgifter, som behandlas för ändamål inom brottsdatalagens tillämpningsområde, ska få behandlas för ändamål utanför det. Redan dagens reglering innebär att det ska prövas om det är nödvändigt att tillhandahålla personuppgifterna i de situationer som räknas upp i de sekundära ändamålsbestämmelserna. För att Polismyndigheten och Tullverket ska få lämna information till andra verksamheter inom respektive myndighet krävs det också särskilda skäl (se 2 kap. 8 § första stycket 4 polisdatalagen och 2 kap. 6 § första stycket 4 tullbrottsdatalagen). I förarbetena framhålls att kravet på särskilda skäl innebär att information inte får tillhandahållas rutinmässigt utan att det i det enskilda fallet måste finnas särskilda skäl som talar för att informationen bör tillhandahållas den andra verksamheten (prop. 2009/10:85 s. 322 och prop. 2016/17:91 s. 102). Det krävs alltså en individuell prövning.

Som nyss nämnts ska det enligt 2 kap. 4 § brottsdatalagen prövas om behandlingen är nödvändig och proportionerlig innan personuppgifter får behandlas för ett nytt ändamål inom lagens tillämpningsområde. I delbetänkandet anges att syftet med kravet på proportionalitet är att det ska göras en bedömning i det enskilda fallet av behovet av den nya behandlingen ställt i relation till inkränket i den personliga integriteten (se SOU 2017:29 s. 252).

Oavsett om man ställer krav på särskilda skäl eller nödvändighet och proportionalitet är det centrala enligt både polisdatalagen, tullbrottsdatalagen och brottsdatalagen att det görs en noggrann pröv-

ning av skälen för den nya behandlingen innan personuppgifter behandlas för ett nytt ändamål. Det skulle skapa en enhetlig tillämpning och underlätta för myndigheterna om den prövning som ska göras innan personuppgifter behandlas för nya ändamål är densamma oavsett om det nya ändamålet ligger inom eller utanför brottsdatalagens tillämpningsområde.

Den prövning som bör krävas innan personuppgifter behandlas för nya ändamål utanför brottsdatalagens tillämpningsområde bör därför enligt utredningens mening avse om den nya behandlingen är nödvändig och proportionerlig. En sådan prövning utgör en lämplig avvägning mellan mottagarens behov av personuppgifterna och skyddet för enskildas personliga integritet. Ett krav på sådan prövning är också förenligt med regleringen i dataskyddsförordningen.

I de flesta fall som räknas upp i dagens sekundära ändamålsbestämmelser ställs det inte krav på särskilda skäl för att personuppgifter ska få tillhandahållas. En proportionalitetsprövning kommer därmed att ställa ökade krav. Som regel måste det dock anses proportionerligt att behandla personuppgifter för att tillhandahålla information i de situationer som i dag räknas upp i de sekundära ändamålsbestämmelserna. Den nya regleringen kommer därmed enligt utredningens bedömning inte att påverka omfattningen av uppgiftslämnandet i de fallen.

Utformningen av regleringen

Utgångspunkten för regleringen är alltså att samma prövning bör göras oavsett om personuppgifterna ska behandlas för nya ändamål inom eller utanför brottsdatalagens tillämpningsområde. Innan personuppgifter behandlas för ett nytt ändamål inom lagens tillämpningsområde ska det enligt 2 kap. 4 § brottsdatalagen säkerställas dels att det finns en tillåten rättslig grund för den nya behandlingen, dels att behandlingen är nödvändig och proportionerlig för det nya ändamålet. Att det ska finnas en rättslig grund för behandlingen när personuppgifter behandlas för ändamål utanför brottsdatalagens tillämpningsområde regleras i artikel 6 i dataskyddsförordningen och bör inte upprepas i den nationella regleringen. Det bör därför framgå att det innan behandling påbörjas för ett nytt

ändamål utanför brottsdatalagens tillämpningsområde – utöver de krav som gäller enligt förordningen – ska säkerställas att behandlingen är nödvändig och proportionerlig för det nya ändamålet.

I kravet på proportionalitet ligger att skälen för den nya behandlingen ska väga tyngre än det intrång som behandlingen innebär för den enskilde. Det som står att vinna med behandlingen ska alltså vägas mot intrånget i enskildas integritet (jfr SOU 2017:29 s. 251 f.). Det kan exempelvis finnas information i Polismyndighetens brottsbekämpande verksamhet om att en person har sådana kontakter i kriminella kretsar att han eller hon vid en helhetsbedömning t.ex. ter sig olämplig för att få en viss befattning eller tillstånd att bedriva viss verksamhet. Det kan då anses vara proportionerligt att informationen tillhandahålls för att användas vid prövningen av anställnings- eller tillståndsärendet. Det kan på motsvarande sätt vara proportionerligt att lämna information om det i Tullverkets brottsbekämpande verksamhet kommer fram uppgifter om hur personer kringgår regelverket som har betydelse för hur verksamheten under Effektiv handel bör inrikta sina kontroller.

Det är också av betydelse vilken typ av personuppgifter det är fråga om och i vilken verksamhet de ska användas. Att en uppgift om var någon uppehåller sig lämnas från Polismyndighetens brottsbekämpande verksamhet till delgivningsverksamheten är generellt sett harmlöst. Däremot kan det finnas andra uppgifter som det inte är proportionerligt att lämna för tillgodose någon annans behov. Det krävs starkare skäl för att tillhandahålla exempelvis känsliga personuppgifter, men även det kan vara motiverat om det motstående intresset är tillräckligt starkt.

Regleringen bör vara densamma för alla brottsbekämpande myndigheter. Den bör därför placeras i brottsdatalagen och inte i respektive myndighets registerförfattning. Om den även bör gälla i domstolarnas och Kriminalvårdens verksamhet återkommer utredningen till i avsnitt 12.4.2 och 13.3.1.

Annat skydd för den personliga integriteten

Det är dock inte enbart prövningen av om det är nödvändigt och proportionerligt att behandla personuppgifterna för det nya ändamålet som sätter gränser för när uppgifterna får tillhandahållas

andra. Mottagaren måste självfallet också ha rätt att behandla dem. Det måste finnas en tillåten rättslig grund för behandlingen enligt dataskyddsförordningen och alla principer för behandling av personuppgifter ska iakttas för att den nya behandlingen ska vara tillåten, t.ex. att personuppgifterna är adekvata och relevanta för ändamålet med behandlingen och att de inte behandlas längre än nödvändigt med hänsyn till ändamålet med behandlingen. Den prövningen kan endast göras av mottagaren och är inget som den som tillhandahåller information behöver beakta vid överväganden av om informationen kan tillhandahållas.

Dessutom sätter sekretessregleringen gränser för i vilken utsträckning uppgifter får lämnas ut. Det gäller framför allt när uppgifter lämnas mellan myndigheter. Enligt 8 kap. 2 § offentlighets- och sekretesslagen kan sekretess emellertid gälla även mellan olika verksamhetsgrenar inom en myndighet, om de är att anse som självständiga i förhållande till varandra. Så är fallet i t.ex. Skatteverket, där bl.a. den brottsbekämpande verksamheten utgör en självständig verksamhetsgren i förhållande till andra verksamheter.

Överträdelse ska kunna föranleda sanktionsavgift

I 6 kap. 1 och 2 §§ brottsdatalogen föreskrivs vilka överträdelser som kan föranleda sanktionsavgift. Enligt 6 kap. 1 § 1 får sanktionsavgift tas ut bl.a. vid överträdelse av bestämmelsen i 2 kap. 4 § om behandling för nya ändamål inom lagens tillämpningsområde. Med hänsyn till att utredningen nu föreslår att samma prövning ska göras innan personuppgifter behandlas för ett nytt ändamål – oavsett om det ligger inom eller utanför lagens tillämpningsområde – bör även överträdelse av bestämmelsen om behandling för nytt ändamål utanför tillämpningsområdet kunna föranleda sanktionsavgift.

6.5 Uppgiftsskyldighet ersätter prövningen

Utredningens förslag: I den utsträckning skyldighet att lämna uppgifter följer av lag eller förordning behöver någon prövning av om behandlingen är nödvändig och proportionerlig för det nya ändamålet inte göras. En prövning ska dock göras innan uppgifter lämnas med stöd av 6 kap. 5 § offentlighets- och sekretesslagen.

Skälen för utredningens förslag

Författningsreglerad uppgiftsskyldighet

Enligt de sekundära ändamålsbestämmelserna är det i dag tillåtet att lämna uppgifter i den utsträckning det finns skyldighet att göra det enligt lag eller förordning. Som nyss nämnts kan sådana skyldigheter avse ändamål både inom och utanför brottsdatalogens tillämpningsområde.

Både i förundersöknings- och brottmålsförfarandet finns det omfattande skyldigheter att informera myndigheter och andra. I förundersökningskungörelsen (1947:948) finns ingående bestämmelser om uppgiftsskyldighet. Sådana skyldigheter föreskrivs också i bl.a. 12 § strafföreläggandekungörelsen (1970:60), där det regleras till vilka fysiska eller juridiska personer domar, beslut och underrettelser i brottmål ska expedieras. Liknande skyldigheter finns även på andra områden. Enligt 36 § förordningen om behandling av personuppgifter inom kriminalvården har Polismyndigheten en vidsträckt skyldighet att lämna underrättelser till Kriminalvården.

Även i andra fall är behöriga myndigheter skyldiga att lämna viss information. Ett exempel är 14 kap. 1 § 2 socialtjänstlagen enligt vilken rättspsykiatrisk undersökningsverksamhet, Kriminalvården, Polismyndigheten och Säkerhetspolisen är skyldiga att genast anmäla till socialnämnden om de i sin verksamhet får kännedom om eller misstänker att barn far illa.

När det i lag eller förordning föreskrivs att uppgifter ska lämnas har lagstiftaren tagit ställning till att det dels är så viktigt att det ska införas en skyldighet att lämna information, dels att eventuell sekretess ska brytas. Lagstiftaren får då också anses ha tagit ställning

till att uppgiftslämnandet är nödvändigt och proportionerligt. Enligt utredningens mening bör sådan uppgiftsskyldighet ersätta den föreslagna prövningen av om behandlingen är nödvändig och proportionerlig för det nya ändamålet, oavsett om det gäller ändamål inom eller utanför brottsdatalagens tillämpningsområde. Det bör tydliggöras i bestämmelserna.

Om det i lag eller förordning bara föreskrivs en möjlighet, men ingen skyldighet, att lämna uppgifter ska myndigheten däremot pröva om det är nödvändigt och proportionerligt att lämna dem, eftersom lagstiftaren då inte har gjort den prövningen.

Uppgiftslämnande enligt 6 kap. 5 § offentlighets- och sekretesslagen

En särskild fråga är hur man ska se på uppgiftslämnande med stöd av 6 kap. 5 § offentlighets- och sekretesslagen. Enligt den paragrafen ska en myndighet på begäran av en annan myndighet lämna uppgift som den förfogar över, i den mån hinder inte möter på grund av bestämmelse om sekretess eller av hänsyn till arbetets behöriga gång. Bestämmelsen anses innebära en skyldighet att lämna uppgifter (se t.ex. *Behandling av personuppgifter inom studiestödsområdet*, prop. 2008/09:96, s. 80 och prop. 2009/10:85 s. 120 f.). Bestämmelser om sekretess har ett annat syfte än bestämmelser om skydd av personuppgifter. Sekretess kan skydda enskildas integritet, men det är långt ifrån alltid det primära syftet med lagstiftningen. Att det konstateras att sekretess inte gäller för en uppgift och att den därmed kan lämnas till en myndighet med stöd av 6 kap. 5 § offentlighets- och sekretesslagen innebär inte att lagstiftaren har tagit ställning till att tillhandahållandet är nödvändigt och proportionerligt i brottsdatalagens mening. Trots att uppgiftslämnande enligt paragrafen betraktas som en uppgiftsskyldighet gör den inte prövningen av nödvändighet och proportionalitet enligt brottsdatalagen obehövlig. Det bör framgå av regleringen att uppgiftslämnande med stöd av 6 kap. 5 § offentlighets- och sekretesslagen inte ersätter prövningen av om den nya behandlingen är nödvändig och proportionerlig.

7 Polisdatalagen

7.1 Polisdatalagen behöver anpassas

7.1.1 Nuvarande reglering

Polisdatalagen gäller enligt 1 kap. 2 § vid behandling av personuppgifter i brottsbekämpande verksamhet vid Polismyndigheten och Säkerhetspolisen och i polisiär verksamhet vid Ekobrottsmyndigheten. Den gäller enligt 1 kap. 3 § däremot inte vid behandling av personuppgifter enligt vapenlagen (1996:67), lagen (1998:620) om belastningsregister, lagen (1998:621) om misstankeregister, lagen (2000:344) om Schengens informationssystem, lagen (2006:444) om passagerarregister, lagen (2010:362) om polisens allmänna spaningsregister och lagen (2015:51) om register över tillträdesförbud vid idrottsarrangemang. I 2 kap. finns allmänna bestämmelser om behandling av personuppgifter. För personuppgifter som har gjorts gemensamt tillgängliga gäller 2 och 3 kap. medan 4 kap. gäller i stället för 3 kap. vid behandling av personuppgifter i särskilda register. Behandling för forensiska ändamål regleras i 5 kap. och behandling av personuppgifter i Säkerhetspolisens verksamhet i 6 kap.

Som anges i avsnitt 4.2 måste registerförfattningarna ändras i vissa avseenden med anledning av dataskyddsdirektivet och anpassas till brottsdatalagen. Många bestämmelser behöver överhuvudtaget inte anpassas eller endast ändras redaktionellt. Utredningen behandlar de anpassningar och ändringar som är gemensamma för registerförfattningarna i kapitel 5 och 6. De övriga anpassningar som krävs i polisdatalagen behandlas i detta kapitel. Regleringen av Säkerhetspolisens personuppgiftsbehandling i frågor som rör nationell säkerhet behandlas i kapitel 14 och 15.

7.1.2 Polisdatalagen ges ett nytt namn

Utredningens förslag: Polisdatalagen med tillhörande förordning ska benämnas polisens brottsdatalag och polisens brottsdataförordning.

Skälen för utredningens förslag: Som framgår av avsnitt 9.1.2 föreslår utredningen att Kustbevakningens personuppgiftsbehandling i den operativa verksamheten ska regleras i två olika registerförfattningar. Detsamma föreslås för åklagarväsendets och domstolarnas personuppgiftsreglering (se avsnitt 11.1.2 och 12.1.3). För att tydliggöra vilka registerförfattningar som ska gälla utöver brottsdatalagen finns det skäl att i så stor utsträckning som möjligt ha enhetliga benämningar på dem. Ett namnbyte får också till effekt att det tydligare framgår att det har gjorts genomgripande förändringar av lagstiftningens struktur med anledning av att brottsdatalagen införs. Polisdatalagen bör därför ges ett nytt namn.

Namnet bör knyta an till hur brottsdatalagen benämns. Det bör vara kort och ange för vem författningen gäller och vad den handlar om. Det är enligt utredningens mening inte lämpligt att använda myndighetsbenämningar i namnet på lagen, eftersom den på samma sätt som i dag ska tillämpas av flera myndigheter och namnet blir för långt om alla myndigheter skulle anges. Gemensamt för de myndigheter som ska tillämpa lagen är att lagen ska gälla i deras polisiära verksamhet. Utredningen föreslår därför att lagen ska benämnas polisens brottsdatalag. Polisdataförordningen bör i konsekvens med det benämnas polisens brottsdataförordning.

Som en konsekvens av att lagens namn ändras måste alla hänvisningar till den ändras.

7.2 Allmänna bestämmelser

7.2.1 Tillämpningsområdet

Utredningens förslag: Polisens brottsdatalag ska gälla utöver brottsdatalagen när

1. Polismyndigheten i egenskap av behörig myndighet behandlar personuppgifter i syfte att bekämpa eller lagföra brott eller upprätthålla allmän ordning och säkerhet,
2. Ekobrottsmyndigheten i egenskap av behörig myndighet behandlar personuppgifter i syfte att utreda brott och det inte är fråga om åklagarverksamhet, och
3. Säkerhetspolisen i egenskap av behörig myndighet behandlar personuppgifter i frågor som inte rör nationell säkerhet om uppgifterna behandlas i syfte att bekämpa eller lagföra brott.

Lagen ska inte gälla vid personuppgiftsbehandling enligt lagen om belastningsregister, lagen om misstankeregister, lagen om Schengens informationssystem, lagen om passagerarregister eller lagen om Polismyndighetens elimineringsdatabas.

Skälen för utredningens förslag

Den nuvarande regleringen behöver anpassas

I avsnitt 4.4.1 tar utredningen ställning till att registerförfattningarna även i fortsättningen ska innehålla bestämmelser om tillämpningsområdet och anger övergripande vad som bör gälla för den regleringen. Vidare föreslår utredningen i avsnitt 5.2 att registerförfattningarna ska gälla utöver brottsdatalagen.

Polisdatlagen gäller enligt 1 kap. 2 § för behandling av personuppgifter i brottsbekämpande verksamhet vid Polismyndigheten och Säkerhetspolisen och i polisiär verksamhet vid Ekobrottsmyndigheten. Tillämpningsområdet måste dock anpassas till brottsdatalagens tillämpningsområde, så att det dels utgår från syftet med behandlingen, dels omfattar den personuppgiftsbehandling som myndigheterna utför inom brottsdatalagens tillämpningsområde

och som inte regleras i någon annan lag. Det bör också framgå att lagen endast gäller när myndigheterna agerar i egenskap av behöriga myndigheter, eftersom det är en viktig avgränsning för tillämpningsområdet (se SOU 2017:29 s. 159 f.).

Polisdatalagen gäller i dag även i Säkerhetspolisens brottsbekämpande verksamhet. Som framgår av avsnitt 14.2.2 anser utredningen att Säkerhetspolisens personuppgiftsbehandling som rör nationell säkerhet bör regleras i en särskild lag. I detta avsnitt diskuteras därför enbart i vilken utsträckning Säkerhetspolisen bör tillämpa polisens brottsdatalag.

Tillämpningsområdet för Polismyndigheten

Polisdatalagen gäller vid behandling av personuppgifter i Polismyndighetens brottsbekämpande verksamhet. Som framgår av avsnitt 5.4.6 anses lagföring av brott i dag ingå i begreppet brottsbekämpning, medan det i brottsdatalagen görs skillnad mellan brottsbekämpning och lagföring. För att tillämpningsområdet ska täcka det som i dag omfattas av regleringen bör det därför inkludera personuppgiftsbehandling i syfte att bekämpa och lagföra brott.

Brottsdatalagens tillämpningsområde omfattar även personuppgiftsbehandling i syfte att upprätthålla allmän ordning och säkerhet. Polismyndigheten har enligt 2 § polislagen i uppdrag att förebygga, förhindra och upptäcka brottslig verksamhet och andra störningar av den allmänna ordningen eller säkerheten och att övervaka den allmänna ordningen och säkerheten och ingripa när störningar har inträffat. Som anges i delbetänkandet anser utredningen att det normalt krävs fysisk närvaro på platsen där oordning förekommer eller riskerar att göra det för att det ska vara fråga om upprätthållande av allmän ordning och säkerhet (se SOU 2017:29 s. 166 f.). För att polisens brottsdatalag så långt möjligt ska täcka all Polismyndighetens behandling av personuppgifter som omfattas av brottsdatalagens tillämpningsområde bör myndighetens behandling av personuppgifter vid upprätthållande av allmän ordning och säkerhet omfattas av tillämpningsområdet. Var gränsen för tillämpningsområdet bör gå diskuteras närmare i delbetänkandet (se SOU 2017:29 s. 227 f.).

Brottsdatalagens tillämpningsområde omfattar även personuppgiftsbehandling i syfte att verkställa straffrättsliga påföljder. Enligt 3 § bötesverkställighetsförordningen (1979:197) är Polismyndigheten central uppbördsmyndighet och ansvarar för uppbörd av böter oavsett vilken myndighet som har utfärdat ett föreläggande av ordningsbot eller ett strafföreläggande. Polismyndigheten ansvarar även för uppbörd av böter som utdömts av allmän domstol. I departementspromemorian Uppbörd av böter (Ds 2015:5) föreslås att Polismyndighetens behandling av personuppgifter i verksamheten för verkställighet av bötesstraff ska regleras i en särskild lag – lagen om register över uppbörd av böter. Personuppgiftsbehandlingen ska enligt förslaget undantas från polisdatalagens tillämpningsområde. Promemorian har remitterats och bereds för närvarande i Regeringskansliet. Mot den bakgrunden lämnar utredningen inget förslag till hur Polismyndighetens personuppgiftsbehandling i syfte att verkställa straff bör regleras.

Tillämpningsområdet för Ekobrottsmyndigheten

Ekobrottsmyndigheten är en åklagarmyndighet med ett utökat uppdrag. I myndigheten integreras åklagarverksamheten med den polisiära verksamhet som krävs för att utreda de brott som Ekobrottsmyndigheten har i uppdrag att bekämpa (se prop. 2014/15:63 s. 21 f.). Den operativa verksamheten kan delas in i tre verksamhetsområden: underrättelseverksamhet, utrednings- och lagföringsverksamhet och brottsförebyggande verksamhet. Huvuddelen av Ekobrottsmyndighetens verksamhet består i att utreda brott. Åklagare är alltid förundersökningsledare i förundersökningar vid myndigheten och fattar beslut om lagföring.

Personuppgiftsbehandlingen vid Ekobrottsmyndigheten regleras i dag i både åklagardatalagen och polisdatalagen. Polisdatalagen gäller i den polisiära verksamheten medan åklagardatalagen gäller i den övriga operativa verksamheten. Det har framkommit att det finns osäkerhet om vilket regelverk som ska tillämpas.

Enligt utredningens mening bör utgångspunkten för vilket regelverk som ska tillämpas vara densamma när det gäller Ekobrottsmyndigheten som när det gäller Åklagarmyndigheten och Polismyndigheten. Den personuppgiftsbehandling som utförs för

att fullgöra åklagaruppgifter i utredningsverksamheten bör därför styras av den registerförfattning som gäller för åklagarväsendet. På samma sätt som gäller för förundersökningar som utförs av Polismyndigheten, oavsett vem som leder förundersökningen, bör den personuppgiftsbehandling som utförs i den övriga utredningsverksamheten vid Ekobrottsmyndigheten regleras i polisens brottsdatalag.

I dag används uttrycket polisiär verksamhet för att avgränsa tillämpningsområdet för polisdatalagen. Det finns ingen definition av vad som är polisiär verksamhet. Sådan verksamhet är vittomfattande och berör många sektorer av samhället. Det är därför enligt utredningens mening bättre att regleringen utgår från åklagarverksamheten vid avgränsningen av tillämpningsområdet, eftersom det är tydligare vad som ingår i åklagarverksamhet än i polisiär verksamhet.

Åklagarverksamhet består av två huvuddelar, brottsutredning och lagföring, men åklagare har även vissa andra författningsreglerade uppgifter inom brottsdatalagens tillämpningsområde. Brottsutredning avser först och främst att åklagare fattar beslut i fråga om huruvida förundersökning ska inledas eller begränsas, läggas ned eller avslutas på annat sätt. Det innefattar också alla beslut som åklagare fattar om åtgärder under en förundersökning, exempelvis om straffprocessuella tvångsmedel eller framställningar till domstol. Beslut i samband med att förundersökningar läggs ned eller avslutas på annat sätt, t.ex. genom åtalsunderlåtelse, och uppgifter i samband med besluten ingår således i åklagarverksamheten. Åklagare är enligt 22 kap. rättegångsbalken skyldiga att biträda målsägande. Åklagarverksamhet inkluderar även att förbereda och föra olika former av talan som kan föras i ett brottmål i samband med ansvarstalan, t.ex. talan om enskilt anspråk, näringsförbud, rådgivningsförbud eller skattetillägg. Lagföring avser huvudsakligen att utfärda strafförelägganden och besluta om åtal, att föra ansvarstalan och att företräda staten i andra frågor i brottmål. På samma sätt som domstol har åklagare omfattande skyldigheter att expediera beslut när en förundersökning inte inleds, läggs ned eller åtalsfrågan avgörs av åklagaren på annat sätt än genom åtal och i samband med beslut i fråga om tvångsmedel.

Det är dock inte längre möjligt att låta regleringen bygga endast på den verksamhet som personuppgifterna behandlas i. Som nyss

nämnts är syftet med personuppgiftsbehandlingen avgörande för lagens tillämpningsområde. Polisens brottsdatalag bör därför gälla vid personuppgiftsbehandling i syfte att utreda brott, om det inte är fråga om åklagarverksamhet. Vid Ekobrottsmyndigheten är det enbart åklagare som fattar beslut om lagföring. Därför bör myndighetens personuppgiftsbehandling i det syftet inte regleras i polisens brottsdatalag (jfr avsnitt 11.2).

Det bedrivs även underrättelseverksamhet vid Ekobrottsmyndigheten. Den verksamheten leds och utförs dock av Polismyndigheten. Polisens brottsdatalag ska tillämpas på den behandlingen, på samma sätt som vid annan personuppgiftsbehandling som Polismyndigheten utför.

Tillämpningsområdet för Säkerhetspolisen

Säkerhetspolisen ska enligt 13 § förordningen (2014:1103) med instruktion för Säkerhetspolisen bistå vid polisverksamhet som leds av Polismyndigheten om myndigheten i ett enskilt fall begär det och det inte finns särskilda skäl mot det. Säkerhetspolisen ska också lämna tekniskt biträde och annan hjälp till Polismyndigheten i den utsträckning som myndigheterna kommer överens om. När Säkerhetspolisen lämnar sådant biträde omfattas personuppgiftsbehandlingen av brottsdatalagens tillämpningsområde, om det inte rör nationell säkerhet (se SOU 2017:29 s. 177).

Enligt 30 § förordningen (2014:1102) med instruktion för Polismyndigheten får chefen för Nationella operativa avdelningen i samråd med biträdande säkerhetspolischefen i ett enskilt fall bestämma att en förundersökning eller annan liknande uppgift i den brottsbekämpande verksamheten ska lämnas över till Säkerhetspolisen för fortsatt handläggning. Syftet med bestämmelsen är bl.a. att jävssituationer ska kunna undvikas (se prop. 2013/14:110 s. 400). När Säkerhetspolisen med stöd av ett beslut enligt den paragrafen genomför en förundersökning eller utför någon annan uppgift som normalt skulle utföras av Polismyndigheten och som omfattas av brottsdatalagens tillämpningsområde bör Säkerhetspolisen tillämpa den lagen (se SOU 2017:29 s. 177).

För Polismyndighetens del kompletteras brottsdatalagen av polisens brottsdatalag och polisens brottsdataförordning. När

Säkerhetspolisen biträder eller övertar en arbetsuppgift från Polismyndigheten bör Säkerhetspolisen därför tillämpa samma reglering. Säkerhetspolisen bör således tillämpa polisens brottsdatalag i frågor som inte rör nationell säkerhet, om personuppgifterna behandlas i syfte att bekämpa eller lagföra brott.

Frågan är då vad som bör gälla när Säkerhetspolisen biträder andra myndigheter i deras brottsbekämpning. I dag föreskrivs det i 6 kap. 1 § 6 polisdatalagen att personuppgifter får behandlas om det behövs för att Säkerhetspolisen ska lämna tekniskt biträde till Polismyndigheten, Ekobrottsmyndigheten, Åklagarmyndigheten eller Tullverket. Den personuppgiftsbehandling som avses rör i huvudsak tekniskt biträde avseende verkställighet av vissa hemliga tvångsmedel (se SOU 2012:44 s. 146 f.). Säkerhetspolisens roll vid sådant biträde kan närmast liknas vid att vara personuppgiftsbiträde. Det är den myndighet som fått tillstånd till att använda tvångsmedlet som anger vilka personuppgifter som ska behandlas och hur de får användas. Det är då också logiskt att det är den myndighetens registerlagstiftning som ska tillämpas. För att det ska vara tydligt att Säkerhetspolisen även i fortsättningen ska lämna tekniskt biträde till de angivna myndigheterna bör det införas en bestämmelse om det i myndighetens instruktion.

Lagen ska inte gälla vid behandling i vissa register

Enligt 1 kap. 3 § polisdatalagen gäller lagen inte vid behandling enligt vapenlagen, lagen om belastningsregister, lagen om miss-tankeregister, lagen om Schengens informationssystem, lagen om passagerarregister, lagen om polisens allmänna spaningsregister och lagen om register över tillträdesförbud vid idrottsarrangemang.

Som konstateras i avsnitt 4.4.1 är det inte möjligt att reglera all Polismyndighetens personuppgiftsbehandling inom brottsdatalagens tillämpningsområde i polisens brottsdatalag. Den bör därför på samma sätt som i dag inte gälla vid behandling av personuppgifter som regleras särskilt i andra författningar. Undantag bör dock endast göras för personuppgiftsbehandling som skulle ha omfattats av lagens tillämpningsområde om någon särreglering inte fanns. Vid samråd med den utredare som har i uppdrag att anpassa författningar på området för allmän ordning och säkerhet har det

framkommit att utredaren anser att bestämmelserna om personuppgiftsbehandling i vapenlagen kompletterar dataskyddsförordningen. Utredningen gör ingen annan bedömning. Personuppgiftsbehandling enligt vapenlagen bör därför inte längre anges bland undantagen. Eftersom lagen (2010:362) om polisens allmänna spaningsregister har upphört att gälla bör hänvisningen till den tas bort. Som framgår av avsnitt 16.2 anser utredningen att Polismyndighetens behandling av personuppgifter i tillträdesförbudsregistret bör regleras i polisens brottsdatalag. Hänvisningen till den lagen bör därför också tas bort.

Enligt lagen om Polismyndighetens elimineringsdatabas får Polismyndigheten föra ett register över dna-profiler i syfte att stärka kvaliteten i den forensiska verksamheten med dna-analyser. Både dna-profiler som inte kan hänföras till en identifierbar person och dna-profiler från prov som har tagits med stöd av 28 kap. rättegångsbalken från en misstänkt jämförs med dna-profilerna i elimineringsdatabasen innan de läggs in i spårregistret respektive utredningsregistret eller dna-registret. Syftet med det är att säkerställa att sökningar i registren inte ger felaktiga resultat på grund av att kontaminerade dna-profiler har registrerats.

I delbetänkandet konstaterar utredningen att behandling av dna-profiler i elimineringsdatabasen är en verksamhet som är ouppslösligt förbunden med Polismyndighetens hantering av de övriga dna-registren. Den regleringen bör därför omfattas av brottsdatalagens tillämpningsområde (se SOU 2017:29 s. 190 f.).

Med hänsyn till att elimineringsdatabasen inte får användas för att utreda brott ansåg regeringen att regleringen av den inte passade in i polisdatalagen, eftersom den lagen gäller i den brottsbekämpande verksamheten (se prop. 2013/14:110 s. 456). Utredningen anser att det alltjämt finns goda skäl att reglera databasen särskilt, dels för att regleringen av både provtagning och personuppgiftsbehandling ska vara samlad i en författning, dels för att markera att personuppgifterna i databasen rör andra än personer med anknytning till brott och brottslig verksamhet och inte får användas i brottsbekämpningen. Behandling som utförs enligt lagen om Polismyndighetens elimineringsdatabas bör därför undantas från polisens brottsdatalags tillämpningsområde.

7.2.2 Personuppgiftsansvar

Utredningens förslag: Polismyndigheten ska vara personuppgiftsansvarig för den behandling av personuppgifter som utförs vid myndigheten och för den behandling som myndigheten utför vid Ekobrottsmyndigheten i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet.

Ekobrottsmyndigheten ska vara personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför i syfte att utreda brott.

Säkerhetspolisen ska vara personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför.

Skälen för utredningens förslag: Polismyndigheten är i dag enligt 2 kap. 4 § polisdatalagen personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför och den behandling som utförs i polisiär verksamhet vid Ekobrottsmyndigheten.

Att Polismyndigheten även fortsättningsvis bör vara personuppgiftsansvarig för den behandling av personuppgifter som utförs vid den egna myndigheten är självklart, liksom att Säkerhetspolisen bör vara personuppgiftsansvarig för den behandling som myndigheten utför enligt lagen. Vem som bör vara personuppgiftsansvarig för den behandling som utförs vid Ekobrottsmyndigheten är däremot inte lika självklart.

Frågan har länge varit föremål för diskussion. Ekobrottsmyndigheten har i olika lagstiftningsärenden framfört att myndigheten bör vara personuppgiftsansvarig för all den behandling av personuppgifter som utförs vid myndigheten, eftersom det inte är möjligt att dela upp personuppgiftsansvaret beroende på vem som hanterar personuppgifterna eller vilket it-system som används (se prop. 2009/10:85 s. 92 f. och prop. 2013/14:110 s. 447 f.).

Ekobrottsmyndigheten är enligt 2 kap. 3 § åklagardatalagen personuppgiftsansvarig för den personuppgiftsbehandling som utförs vid myndigheten enligt åklagardatalagen. När Ekobrottsmyndigheten inrättades var myndigheten även personuppgiftsansvarig för personuppgiftsbehandlingen i den polisverksamhet som bedrevs vid myndigheten. Myndigheten omfattades däremot inte av den tidigare gällande polisdatalagens (1998:622) tillämpningsområde, eftersom den är en åklagarmyndighet. Myndighetens personupp-

giftsbehandling reglerades, förutom i förordningen (2006:937) om behandling av personuppgifter inom åklagarväsendet, i personuppgiftslagen. För att Ekobrottsmyndigheten skulle kunna bedriva kriminalunderrättelseverksamhet ändrades den tidigare gällande polisdatalagen (1998:622) och gjordes från den 1 januari 2004 tillämplig på polisverksamheten i myndigheten (Övergångsbestämmelserna till polisdatalagen m.m., prop. 2002/03:144, s. 15 f.). Däravande Rikspolisstyrelsen blev personuppgiftsansvarig för den personuppgiftsbehandling vid Ekobrottsmyndigheten som utfördes med stöd av polisdatalagen.

Personuppgiftsansvarig definieras i 1 kap. 6 § brottsdatalagen som den behöriga myndighet som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter. Enligt förarbetena till den nu gällande polisdatalagen bör huvudregeln vara att den myndighet som utför själva behandlingen också ska ha personuppgiftsansvaret för den. Regeringen ansåg dock att någon förändring av personuppgiftsansvaret vid Ekobrottsmyndigheten inte var motiverad när polisdatalagen infördes (se prop. 2009/10:85 s. 93). Inte heller när åklagardatalagen infördes gjordes någon ändring (se prop. 2014/15:63 s. 45).

Polismyndigheten leder underrättelse- och spaningsverksamheten vid de polisoperativa enheterna vid Ekobrottsmyndigheten. Även om personuppgiftsbehandlingen utförs vid Ekobrottsmyndigheten är det Polismyndigheten som leder den verksamheten och som därigenom bestämmer ändamålen med och medlen för behandlingen. Polismyndigheten bör därför även i fortsättningen vara personuppgiftsansvarig för den personuppgiftsbehandling som utförs i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet vid Ekobrottsmyndigheten. Däremot är det Ekobrottsmyndigheten som genomför brottsutredningarna och som därigenom bestämmer ändamålen med och medlen för behandlingen. Polismyndigheten har ingen praktisk möjlighet att fullgöra personuppgiftsansvaret i den verksamheten. Så som personuppgiftsansvarig definieras i brottsdatalagen bör Ekobrottsmyndigheten därför pekas ut som personuppgiftsansvarig för den behandling som myndigheten utför i syfte att utreda brott enligt polisens brottsdatalog (se avsnitt 7.2.1 och 11.2).

7.2.3 En bestämmelse om hur lagen är uppbyggd

Utredningens förslag: Polisens brottsdatalag ska innehålla en bestämmelse om hur lagen är uppbyggd.

Skälen för utredningens förslag: I avsnitt 5.3.5 föreslår utredningen att registerförfattningarna inte längre ska innehålla bestämmelser om hur lagarna är uppbyggda, om det inte finns särskilda skäl för det.

Alla kapitel i polisdatalagen gäller inte för all personuppgiftsbehandling inom tillämpningsområdet. Personuppgiftsbehandling i vissa register och i den forensiska verksamheten kommer även i fortsättningen att regleras i särskilda kapitel på grund av att bara delar av lagen ska vara tillämpliga. Vidare är det bara vissa kapitel som gäller för Ekobrottsmyndigheten och Säkerhetspolisen. Det behöver därför tydliggöras vad som gäller för dem och hur lagens kapitel förhåller sig till varandra. Bestämmelsen om lagens uppbyggnad bör således behållas men anpassas till hur Säkerhetspolisens personuppgiftsbehandling regleras (se avsnitt 14.2.2) och de strukturella förändringar som föreslås i kapitel 5.

7.3 Grundläggande bestämmelser om behandling

7.3.1 Tillåtna rättsliga grunder och behandling för nya ändamål

Utredningens förslag: Personuppgifter ska få behandlas om det är nödvändigt för att utföra en arbetsuppgift i syfte att

1. förebygga, förhindra eller upptäcka brottslig verksamhet,
2. utreda eller lagföra brott,
3. upprätthålla allmän ordning och säkerhet, eller
4. fullgöra förpliktelser som följer av internationella åtaganden.

Arbetsuppgiften ska framgå av en bindande unionsrättsakt eller av en lag, en förordning eller ett särskilt beslut i vilket rege-

ringen uppdragit åt myndigheten att ansvara för en sådan uppgift.

Det ska framgå genom en hänvisning att personuppgifter som behandlas med stöd av lagen ska få behandlas för nya ändamål enligt de förutsättningar som anges i brottsdatalagen.

Skälen för utredningens förslag

En bestämmelse som ersätter brottsdatalagens bestämmelse om tillåtna rättsliga grunder för behandling

Som anges i avsnitt 6.3.1 bör registerförfattningarna innehålla bestämmelser om tillåtna rättsliga grunder för behandling av personuppgifter. Regleringen i 2 kap. 7 § polisdatlagen bör således behållas, men det ska framgå att det inte är en ändamålsbestämmelse i egentlig mening. Bestämmelsen är på samma sätt som 2 kap. 1 § brottsdatalagen en del av den rättsliga grunden och ger Polismyndigheten, Ekobrottsmyndigheten och Säkerhetspolisen rättsligt stöd för att behandla personuppgifter automatiserat för att utföra sina arbetsuppgifter (se avsnitt 6.1.2).

Polismyndigheten får i dag behandla personuppgifter om det behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller beivra brott eller fullgöra de förpliktelser som följer av internationella åtaganden. Polismyndigheten bör givetvis få fortsätta att behandla personuppgifter om det är nödvändigt för att fullgöra sådana arbetsuppgifter, men regleringen bör anpassas till brottsdatalagens terminologi. Det bör i tillämpliga delar gälla även för övriga myndigheter som tillämpar polisens brottsdatalag.

Som framgår av avsnitt 7.2.1 föreslår utredningen att polisens brottsdatalag ska tillämpas på Polismyndighetens personuppgiftsbehandling vid upprätthållande av allmän ordning och säkerhet. Upprätthållande av allmän ordning och säkerhet bör därför också vara en tillåten rättslig grund.

Polisens brottsdatalag föreslås gälla utöver brottsdatalagen. För att det inte ska råda någon osäkerhet om hur bestämmelsen i 2 kap. 1 § brottsdatalagen förhåller sig till bestämmelsen om tillåtna rättsliga grunder i registerförfattningen bör den senare helt ersätta bestämmelsen i brottsdatalagen. Det bör därför på samma sätt som i brottsdatalagen i polisens brottsdatalag föreskrivas att den arbets-

uppgift som ska utföras ska framgå av en bindande unionsrättsakt eller en lag, en förordning eller ett särskilt beslut i vilket regeringen uppdragit åt myndigheten att ansvara för en sådan uppgift. Vad det innebär utvecklas i delbetänkandet (se SOU 2017:29 s. 238 f.).

Behandling för nya ändamål

I dag regleras behandling för nya ändamål till viss del i den sekundära ändamålsbestämmelsen i 2 kap. 8 § polisdatalagen. Utredningen anser som framgår av avsnitt 6.3.2 och 6.4.2 att de sekundära ändamålsbestämmelserna bör upphävas. Förutsättningarna för behandling för nya ändamål bör i stället regleras i brottsdatalagen. Innan personuppgifter får behandlas för nya ändamål inom brottsdatalagens tillämpningsområde ska det enligt 2 kap. 4 § brottsdatalagen säkerställas att behandlingen är nödvändig och proportionerlig för det nya ändamålet. Utredningen föreslår att samma prövning ska göras när de brottsbekämpande myndigheterna behandlar personuppgifter för nya ändamål utanför tillämpningsområdet. Det bör införas en bestämmelse i polisens brottsdatalag som tydliggör att förutsättningarna för att behandla personuppgifter, som behandlas med stöd av den lagen, för nya ändamål regleras i brottsdatalagen.

7.3.2 Behandling av biometriska och genetiska uppgifter

Utredningens förslag: Polismyndigheten och Säkerhetspolisen ska få behandla biometriska uppgifter enligt de förutsättningar som anges i brottsdatalagen.

Utredningens bedömning: Säkerhetspolisen och Ekobrottsmyndigheten bör inte få behandla genetiska uppgifter. Polismyndigheten bör endast få behandla genetiska uppgifter i den forensiska verksamheten.

Skälen för utredningens förslag och bedömning

Förutsättningarna för att behandla biometriska och genetiska uppgifter

Biometriska uppgifter är enligt 1 kap. 6 § brottsdatalagen personuppgifter som rör en persons fysiska, fysiologiska eller beteendemässiga kännetecken, som tagits fram genom särskild teknisk behandling och som möjliggör eller bekräftar unik identifiering av personen i fråga. Vanliga fotografier och filmer omfattas inte av definitionen om de inte bearbetas tekniskt på något sätt så att identifiering blir möjlig, t.ex. i ett ansiktsigenkänningsprogram (se SOU 2017:29 s. 148 f.).

Genetiska uppgifter är enligt 1 kap. 6 § brottsdatalagen personuppgifter som rör en persons nedärvda eller förvärvade genetiska kännetecken och som härrör från analys av ett spår eller ett prov av personen i fråga. Det är framför allt information som kan tas fram vid dna-analyser, men även motsvarande information som tas fram vid andra analyser omfattas (se SOU 2017:29 s. 149 f. och 265.).

Enligt 2 kap. 12 och 13 §§ brottsdatalagen utgör biometriska uppgifter som används för att identifiera en person och genetiska uppgifter känsliga personuppgifter. Sådana uppgifter får endast behandlas om det är särskilt föreskrivet och det är absolut nödvändigt för ändamålet med behandlingen. Det finns därför skäl att överväga myndigheternas behov av att behandla sådana uppgifter.

Biometriska uppgifter

Biometri är ett samlingsnamn för sådan automatiserad teknik som syftar till att identifiera en person eller avgöra om en påstådd identitet är riktig. Den baseras på mätning av fysiska karaktärsdrag hos den som ska identifieras. Fingeravtryck, ansiktsgeometri, ögats iris eller nät- eller regnbågshinna, röst, hand, blodkärl, dna eller rörelsemönster kan användas.

Fingeravtryck och dna har använts länge i den polisiära verksamheten, men den tekniska utvecklingen har förändrat förutsättningarna för att använda framför allt biometri. Det har under de senaste åren utvecklats helt nya möjligheter att använda exempelvis ansikts- och röstigenkänning. Utvecklingen går fort och det är svårt att förutse vad som kommer att vara möjligt inom några år.

Polisen bör även i fortsättningen ha möjlighet att behandla biometriska uppgifter i brottsbekämpningen. Det är viktigt att den rättsliga regleringen inte hämmar eller hindrar utvecklingen och användningen av ny teknik. Enligt 2 kap. 12 § brottsdatalagen får biometriska uppgifter som används för att identifiera en person behandlas bara om det är absolut nödvändigt för ändamålet med behandlingen. Utredningen bedömer att det för närvarande inte finns skäl att begränsa möjligheterna att använda biometriska uppgifter ytterligare.

Polismyndigheten och Säkerhetspolisen har behov av att behandla biometriska uppgifter medan det är svårt att se att Ekobrottsmyndigheten har ett sådant behov (jfr avsnitt 11.3.2). Det bör därför införas en bestämmelse i polisens brottsdatalag som medger att Polismyndigheten och Säkerhetspolisen får behandla biometriska uppgifter enligt de förutsättningar som anges i brottsdatalagen.

Det bör anmärkas att de personuppgifter som förekommer i ett utlåtande som baseras på en teknisk bearbetning av biometriska eller genetiska uppgifter inte i sig utgör sådana uppgifter. Det kommer alltså att vara möjligt att behandla personuppgifter i sådana utlåtanden i samma utsträckning som i dag.

Utredningen återkommer till frågan om behandling av biometriska uppgifter i den forensiska verksamheten i avsnitt 7.8.4.

Genetiska uppgifter

Genetiska uppgifter behandlas vid dna-analyser för att ta fram dna-profiler eller forensiska uppslag. Själva dna-profilen, som behandlas i Polismyndighetens dna-register, är endast en sifferkombination och är därmed ingen genetisk uppgift. Den är i stället en biometrisk uppgift, eftersom den tas fram genom en särskild teknisk behandling av en persons arvs massa för att möjliggöra unik identifiering av personen i fråga (se SOU 2017:29 s. 265)

Av avsnitt 7.8.4 framgår i vilken utsträckning Polismyndigheten bör få behandla genetiska uppgifter i den forensiska verksamheten. Det har i övrigt inte framkommit att någon av de andra myndigheter som tillämpar polisens brottsdatalag har behov av att behandla genetiska uppgifter och utredningen anser därför att de inte

bör få behandla sådana uppgifter. Någon bestämmelse som medger sådan behandling bör därför inte finnas i lagen.

7.3.3 Sökning på känsliga personuppgifter

Utredningens förslag: Sökförbudet i brottsdatalagen ska inte hindra att brottsrubriceringar, uppgifter om tillvägagångssätt vid brott, uppgifter om verkställighet av påföljd eller uppgifter som beskriver en persons utseende används vid sökning.

Det ska inte heller hindra sökning i syfte att få fram ett personurval grundat på etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening eller uppgifter som rör hälsa, sexualliv eller sexuell läggning, om sökningen görs i personuppgifter som inte har gjorts gemensamt tillgängliga.

Skälen för utredningens förslag

Undantag från sökförbudet i brottsdatalagen vid sökning i alla slags personuppgifter

I avsnitt 5.3.8 föreslår utredningen att förbudet i 3 kap. 5 § polisdatalagen att använda känsliga personuppgifter som sökbegrepp ska upphävas, eftersom det i 2 kap. 14 § brottsdatalagen finns ett generellt sökförbud. Det förbudet utgår till skillnad från dagens reglering från syftet med sökningen. Om syftet inte är att få fram ett personurval grundat på känsliga personuppgifter är sökningen tillåten, även om känsliga personuppgifter används vid sökningen (se SOU 2017:29 s. 272 f.).

Eftersom sökförbudet har en ny utformning är det nödvändigt att se över bestämmelserna om sökning. Enligt 3 kap. 5 § andra stycket polisdatalagen är det tillåtet att använda brottsrubriceringar och uppgifter som beskriver en persons utseende som sökbegrepp vid sökning i uppgifter som har gjorts gemensamt tillgängliga. Det finns även i fortsättningen behov av att kunna använda sådana uppgifter vid sökning, även om det leder till att man får fram ett personurval grundat på känsliga personuppgifter. Det bör därför enligt utredningens mening göras undantag från brottsdatalagens sökför-

bud i polisens brottsdatalag för sådana sökningar. För att möjligheterna till sökning ska vara desamma som i dag bör undantaget omfatta sökningar i alla slags personuppgifter, dvs. oberoende av om uppgifterna har gjorts gemensamt tillgängliga eller inte.

Polisen har även behov av att kunna göra sökningar på tillvägagångssätt vid brott. Sådana sökningar kan i vissa fall leda till ett personurval grundat på känsliga personuppgifter. Som exempel kan nämnas att tillvägagångssätt vid sexualbrott kan avslöja uppgifter om sexualliv eller sexuell läggning. Tillvägagångssätt vid både sexualbrott och andra brott kan avslöja skador som gärningsmannen ådragit sig, dvs. avslöja uppgifter om hälsa. Undantaget från sökförbudet bör därför omfatta tillvägagångssätt vid brott.

Även sökning på verkställighet av påföljd kan ibland vara nödvändig. Det är framför allt vårdpåföljder som polisen har intresse av att få fram vid sökning och som kan leda till ett personurval grundat på känsliga personuppgifter. Det kan vara fallet exempelvis om det har begåtts brott som bär tydliga tecken av att gärningsmannen lider av en psykisk störning. Polisen har då intresse av att kartlägga om personer som undergår rättspsykiatrisk vård haft frigång eller permission. Att någon är föremål för rättspsykiatrisk vård avslöjar en uppgift om hälsa. Kriminalvården är enligt 46 § förordningen om behandling av personuppgifter inom kriminalvården skyldig att underrätta Polismyndigheten och Säkerhetspolisen bl.a. om permissioner och vårdvistelser inom ramen för fängelsestraff. Även sådan information, t.ex. om att någon vistas på en viss typ av behandlingshem, kan avslöja uppgifter om bl.a. hälsa. Undantaget från sökförbudet i brottsdatalagen bör därför även omfatta sökning på uppgifter om verkställighet av påföljd.

Undantag vid sökning i personuppgifter som inte har gjorts gemensamt tillgängliga

Det nuvarande förbudet i polisdatalagen mot att använda känsliga personuppgifter som sökbegrepp gäller endast vid sökning i uppgifter som har gjorts gemensamt tillgängliga. Det innebär att känsliga personuppgifter får användas vid sökning i uppgifter som enbart ett fåtal har tillgång till. Den enda begränsningen i dag är att behandling av känsliga personuppgifter ska vara absolut nödvändig.

Utredningens utgångspunkt är att de behöriga myndigheternas möjlighet att använda känsliga personuppgifter vid sökning inte ska försämrats. För att effektivt kunna bekämpa brott kan polisen ha behov av att göra sammanställningar i syfte att få fram ett personurval grundat på känsliga personuppgifter vid sökning i uppgifter som inte har gjorts gemensamt tillgängliga. Det finns därför skäl att göra vissa undantag från sökförbudet i brottsdatalagen när det gäller sökning i uppgifter som enbart ett fåtal har tillgång till.

Framför allt i underrättelseverksamheten kan det finnas behov av sökningar som innebär att sammanställningar grundade på känsliga personuppgifter skapas. Organiserad brottslighet av olika slag kräver inte sällan kartläggning av misstänkta kontakter och vanor. Då kan olika typer av känsliga personuppgifter avslöjas. Det kan t.ex. visa sig att en övervakad person regelbundet besöker en lokal där det förekommer religiösa ceremonier (uppgift om religiös övertygelse) eller politisk eller facklig verksamhet (uppgift om politisk åsikt eller medlemskap i fackförening) eller umgås huvudsakligen med personer som har visst ursprung (uppgift om etniskt ursprung). Polisen måste kunna göra sökningar i sådana underrättelseuppgifter för att förebygga, förhindra eller upptäcka brottslig verksamhet som begås av flera personer som förenas genom sitt etniska ursprung, sin religiösa eller filosofiska övertygelse eller sina politiska åsikter. Likaså måste polisen kunna göra sökningar i syfte förebygga, förhindra och upptäcka brott som riktar sig mot personer av visst etniskt ursprung eller med viss religiös övertygelse. I utredningsverksamheten finns motsvarande behov av att kunna söka på känsliga personuppgifter.

Polisen har dock inte behov av att kunna ta fram personurval grundade på alla kategorier av känsliga personuppgifter. Det kan aldrig finnas behov av att göra sammanställningar grundade på ras, eftersom det inte finns någon vetenskaplig grund för att dela in människor i skilda raser (se SOU 2017:29 s. 267). Behovet av att göra sammanställningar grundade på genetiska och biometriska uppgifter i den forensiska verksamheten vid Polismyndigheten behandlas i avsnitt 7.8.4. Av avsnitt 14.7.3 framgår att utredningen inte anser att behandling av biometriska uppgifter i ansiktsgenkänningsprogram är att anse som sökning. Det finns därför inte något behov av undantag för sökning när det gäller biometriska uppgifter utanför den forensiska verksamheten.

Undantaget från sökförbudet i brottsdatalagen bör därför utformas så att sökning möjliggörs när det gäller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening eller uppgifter som rör hälsa, sexualliv eller sexuell läggning. Det innebär att möjligheterna att använda känsliga personuppgifter vid sökning i uppgifter som inte har gjorts gemensamt tillgängliga begränsas i förhållande till vad som gäller i dag. Eftersom det inte finns behov av ett generellt undantag bedömer utredningen att förslaget inte innebär någon försämring.

Hur förhåller sig sökmöjligheterna till sekretessbestämmelsen?

Som anges i delbetänkandet kan det ifrågasättas om sökförbudet i 2 kap. 14 § brottsdatalagen uppfyller kraven för att omfattas av begränsningsregeln i 2 kap. 3 § tredje stycket tryckfrihetsförordningen. För att säkerställa att allmänheten inte med stöd av offentlighetsprincipen ska kunna få ut sammanställningar grundade på känsliga personuppgifter som myndigheten själv inte får ta fram föreslår utredningen en bestämmelse om absolut sekretess (se SOU 2017:29 s. 274 f. och 643 f.). Sekretessen gäller hos behöriga myndigheter till skydd för enskild för uppgifter i ett sådant personurval som avses i 2 kap. 14 § brottsdatalagen.

Sekretessbestämmelsen är enbart tänkt att träffa sökning som är förbjuden. Syftet är att allmänheten inte ska ha större möjligheter än myndigheterna själva att få fram sammanställningar grundade på känsliga personuppgifter. Allmänheten bör ha samma möjlighet som myndigheterna själva att begära ut sådana sammanställningar. När det nu föreslås undantag från sökförbudet får det prövas om uppgifterna i sammanställningen omfattas av någon annan sekretessbestämmelse, t.ex. sekretess som skyddar förundersökning eller sekretess i underrättelseverksamhet enligt 18 kap. 1 eller 2 § offentlighets- och sekretesslagen. Även sekretess till skydd för enskilda personliga förhållanden enligt 35 kap. offentlighets- och sekretesslagen skyddar normalt uppgifter av det här slaget.

Den föreslagna sekretessbestämmelsen skyddar sammanställningar som tas fram i strid med förbudet i brottsdatalagen. Den behöver enligt utredningens mening inte ändras med anledning av de föreslagna undantagen från sökförbudet.

7.4 Personuppgifter från transportföretag

7.4.1 Personuppgiftsbehandlingen bör regleras i polisens brottsdatalag

Utredningens förslag: Bestämmelserna om hur Polismyndigheten och Säkerhetspolisen får behandla personuppgifter som transportföretag på begäran tillhandahåller myndigheterna enligt polislagen ska tas in i polisens brottsdatalag. Sådana personuppgifter ska få behandlas i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott.

Skälen för utredningens förslag

Nuvarande reglering

Enligt 25 § polislagen är transportföretag skyldiga att på begäran skyndsamt lämna vissa personuppgifter till Polismyndigheten och Säkerhetspolisen. Det rör sig bl.a. om uppgifter om resenärers namn, medresenärers namn och transportmedel. Uppgifterna får endast begäras om de kan ha betydelse för myndighetens brottsbekämpande verksamhet. Regleringen har sitt ursprung i de lagändringar som krävdes med anledning av att Sverige blev medlem i EU (se avsnitt 8.4.1).

Personuppgifterna får tillhandahållas genom terminalåtkomst till transportföretagens bokningssystem där polisen endast får läsa uppgifterna men inte bearbeta eller lagra dem. Terminalåtkomst tillåts enligt 26 § bara i den omfattning och under den tid som behövs för att kontrollera aktuella transporter. Uppgifterna får även lämnas på annat sätt om transportföretaget anser att det är bättre. Uppgifterna lämnas ofta elektroniskt, men det förekommer även att de tillhandahålls på papper. Utredningen utgår från att personuppgifterna, oavsett på vilket sätt de tillhandahålls, normalt är strukturerade på ett sådant sätt att polisens brottsdatalag är tillämplig på behandlingen.

Uppgifter om enskilda som lämnas på annat sätt än genom terminalåtkomst ska enligt 26 § tredje stycket polislagen omedelbart förstöras, om de visar sig sakna betydelse för utredning av eller lagföring för brott. Syftet med bestämmelsen är att hindra att uppgif-

terna sprids, eftersom det till allra största delen är fråga om information om enskilda personer som inte är misstänkta för vare sig brott eller brottslig verksamhet.

Personuppgiftsbehandlingen bör regleras i registerförfattningen

I polislagen regleras alltså inte bara transportföretagens uppgiftsskyldighet, utan även på vilket sätt och hur länge polisen får behandla personuppgifterna. Tullverket har motsvarande tillgång till uppgifter från transportföretag enligt bestämmelser i lagen (1996:701) om Tullverkets befogenheter vid Sveriges gräns mot ett annat land inom Europeiska unionen (inregränslagen) och tullagen (2016:253).

För polisens del finns det i dag ingen reglering av behandlingen av personuppgifter från transportföretag i polisdatalagen. Tullverkets behandling av personuppgifter från transportföretag regleras däremot både i inregränslagen och tullagen och i 2 kap. 8 och 9 §§ tullbrottsdatalagen. I avsnitt 8.4.1 behandlas frågan om regleringen av Tullverkets behandling av uppgifter från transportföretag bör samlas i tullbrottsdatalagen.

Utredningens utgångspunkt är att myndigheternas personuppgiftsbehandling inom brottsdatalagens tillämpningsområde i så stor utsträckning som möjligt ska regleras i deras registerförfattningar (se avsnitt 4.4.1). Enstaka bestämmelser om personuppgiftsbehandling i annan lagstiftning än myndigheternas registerförfattningar riskerar därför att komma i skymundan. För enskilda blir regleringen mycket svåröverskådlig. Det är i detta fall särskilt olyckligt med tanke på att de flesta uppgifterna rör personer som inte kan misstänkas för brott. Det är också mindre lämpligt att ha enstaka bestämmelser om personuppgiftsbehandling i lagar som i övrigt reglerar polisens verksamhet och befogenheter. Utredningen anser därför att det finns skäl att föra över bestämmelserna om hur polisen får behandla personuppgifter från transportföretag till polisens brottsdatalag. Transportföretagens skyldigheter bör alltså regleras i polislagen.

Hur får uppgifterna behandlas?

Enligt 26 § polislagen får transportföretagen tillhandahålla Polismyndigheten och Säkerhetspolisen passageraruppgifter genom att göra dem läsbara via terminalåtkomst. Uppgifter som hålls tillgängliga på det sättet får inte ändras eller på annat sätt bearbetas eller lagras av myndigheterna. Bestämmelsen kan uppfattas på det sättet att myndigheterna inte får hantera personuppgifterna på annat sätt än att läsa dem på en terminal. Det kan dock inte ha varit avsikten att regleringen ska tolkas så snävt, eftersom tillgången till sådana uppgifter skulle vara helt meningslös om uppgifter av betydelse för brottsbekämpningen inte skulle få tillföras den brottsbekämpande verksamheten. Av förarbetena till Tullverkets motsvarande bestämmelse framgår att uppgifterna kan behöva bevaras så länge de har betydelse för vidare åtgärder, vilket antogs vara i undantagsfall (se Tullens befogenheter vid den inre gränsen, prop. 1995/96:166, s. 84).

Det bör förtydligas att den nu aktuella bestämmelsen endast hindrar ändring eller bearbetning av uppgifterna i transportbolagens it-system. Om personuppgifter i ett enskilt fall ger upphov till ett underrättelseuppslag eller behövs i en brottsutredning kan de som regel behandlas enligt de generella bestämmelserna i brottsdatalagen och polisens brottsdatalag.

Polismyndigheten har framför allt behov av att kunna behandla bokningsuppgifter för att kontrollera en viss persons resande eller vilka som vid ett visst tillfälle reser till en viss destination. Polismyndigheten kan ha behov av sådana uppgifter både i sin underrättelseverksamhet och för brottsutredning. I underrättelseverksamheten kan det t.ex. vara viktigt att kartlägga hur vissa varor förs in i landet. Vid s.k. kontrollerade leveranser av narkotika kan bokningsuppgifter vara av stor betydelse. Vid utredning av brott kan det t.ex. vara av värde att kunna kartlägga möjliga vägar att föra stöldgods ut ur landet eller att följa narkotikans väg till Sverige. Polismyndigheten bör därför i enskilda fall kunna dra nytta av uppgifter från transportföretagen både i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet och i syfte att utreda eller lagföra brott.

I avsnitt 7.4.4 behandlas frågan om det i polisens brottsdatalag bör finnas en särskild bestämmelse om att personuppgifter från

transportföretag ska förstöras om de visar sig sakna betydelse för brottsbekämpningen.

PNR-utredningens förslag

Den 27 april 2016 antogs Europaparlamentets och rådets direktiv (EU) 2016/681 om användning av passageraruppgiftssamlingar (PNR-uppgifter) för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet. Direktivet reglerar skyldigheten för flygbolag att överföra passageraruppgiftssamlingar till särskilda enheter för passagerarinformation i medlemsstaterna, för vilka ändamål personuppgifterna får behandlas, hur länge de får lagras och under vilka förutsättningar de får lämnas ut. PNR-utredningen har haft i uppdrag att föreslå hur direktivet ska genomföras. I betänkandet Lag om flygpassageraruppgifter i brottsbekämpningen (SOU 2017:57) föreslår PNR-utredningen en ny lag som reglerar användningen av flygpassageraruppgifter i brottsbekämpningen. Lagen föreslås ha företräde framför bestämmelserna i polisdatalagen och polislagen. Förslagen bereds i Regeringskansliet. Utredningen har inte beaktat PNR-utredningens förslag.

7.4.2 Begränsningar i möjligheterna att behandla personuppgifter

Utredningens förslag: Vid sökning i personuppgifter från transportföretag får namn, personnummer, samordningsnummer och andra liknande identitetsbegrepp användas som sökbegrepp endast om uppgifterna avser en person som är eller har varit misstänkt för brott eller viss brottslig verksamhet eller som övervakas på visst sätt.

Personuppgifter som transportföretag tillhandahåller ska endast i enskilda fall få behandlas för nya ändamål enligt brottsdatalagen.

Skälen för utredningens förslag

Det bör regleras vilka sökbegrepp som får användas

I dag gäller inga begränsningar i polisens möjligheter att söka i uppgifter från transportföretag. Det gör det däremot om motsvarande uppgifter lämnas till Tullverket. Enligt 2 kap. 9 § tullbrottsdatalagen får vid sökning i uppgifter från transportföretag direkta personuppgifter som namn, personnummer och samordningsnummer användas som sökbegrepp bara om uppgifterna avser en person som är eller har varit misstänkt för brott eller viss brottslig verksamhet eller som övervakas på visst sätt.

I förarbetena till bestämmelserna om hur Tullverket får behandla uppgifter från transportföretag framhåller regeringen att sökning på resenärens namn i uppgifter från transportföretag är förenade med särskilda integritetsrisker mot bakgrund av dels att transportföretagen är skyldiga att lämna ut uppgifterna, dels att de flesta uppgifterna avser personer som inte kan misstänkas för någon brottslighet (se prop. 1995/96:166 s. 79 f.). Även om det vore effektivt för brottsbekämpningen om Tullverket kunde samköra uppgifter som kommit in från transportföretag med andra uppgifter från den brottsbekämpande verksamheten och på så sätt få fram vilka som redan övervakas eller kan misstänkas ha samband med brottslig verksamhet slås det fast i förarbetena till tullbrottsdatalagen att det inte bör tillåtas. Det är tillräckligt att Tullverket har möjlighet att söka efter personer som redan är eller har varit misstänkta för brott eller kan antas ha samband med brottslig verksamhet eller personer som är föremål för viss övervakning (se prop. 2016/17:91 s. 107).

Det gäller alltså helt olika regler för samma typ av personuppgifter beroende på vilken myndighet som tar emot dem. Det är enligt utredningens mening otillfredsställande ur integritetsynpunkt att regelverken skiljer sig åt, särskilt mot bakgrund av att det till största delen är fråga om överskottsinformation. Även om uppgifter från transportföretag används på olika sätt av Tullverket och polisen anser utredningen att polisen inte bör ha vidare möjligheter att söka i uppgifter från transportföretag än vad Tullverket har. En motsvarande bestämmelse om sökbegränsning bör därför tas in i polisens brottsdatalag.

Behandling för nya ändamål

I dag finns det inga bestämmelser om vidarebehandling av personuppgifter som transportföretag tillhandahåller. Det gör det däremot om motsvarande uppgifter lämnas till Tullverket. Enligt 2 kap. 8 § tullbrottsdatalagen får Tullverket endast om det behövs i ett enskilt fall behandla personuppgifter från transportföretag för något annat primärt ändamål. Det innebär att uppgifterna exempelvis får användas för att utreda brott.

Behandling för nya ändamål inom brottsdatalagens tillämpningsområde regleras i 2 kap. 4 § brottsdatalagen. För att sådan behandling ska vara tillåten krävs dels att det finns en tillåten rättslig grund för behandlingen, dels att behandlingen är nödvändig och proportionerlig för det nya ändamålet. Utredningen föreslår i avsnitt 6.4.3 att samma prövning ska göras när personuppgifter behandlas för nya ändamål utanför brottsdatalagens tillämpningsområde.

Riksdagen har nyligen ställt sig bakom att Tullverket ska få behandla personuppgifter av nu aktuellt slag för nya ändamål endast om det behövs i enskilda fall (se prop. 2016/17:91 s. 107). Mot den bakgrunden bör polisens rätt att behandla personuppgifter som tillhandahålls av transportföretag för nya ändamål begränsas på motsvarande sätt. Behandling för nya ändamål bör därför vara tillåten endast i enskilda fall.

7.4.3 Uppgifter från transportföretag får göras gemensamt tillgängliga

Utredningens bedömning: Personuppgifter från transportföretag får göras gemensamt tillgängliga. Det kräver ingen särskild reglering.

Skälen för utredningens bedömning: Uppgifterna från transportföretagen är till allra största delen information om personer som inte är intressanta ur ett brottsbekämpningsperspektiv. Utgångspunkten är därför att uppgifterna ska ges så liten spridning som möjligt.

När bestämmelserna om Tullverkets tillgång till uppgifter från transportföretag infördes konstaterade regeringen att uppgifternas karaktär krävde begränsningar av hur uppgifterna fick användas (se prop. 1995/96:166 s. 83 f.). Enligt 2 kap. 8 § andra stycket tullbrottsdatalagen får personuppgifter från transportföretag bara göras gemensamt tillgängliga i enskilda fall. Av förarbetena framgår att det skulle strida mot intentionerna bakom bestämmelserna om tillgång till uppgifter från transportföretag att generellt tillåta att sådana uppgifter görs gemensamt tillgängliga. Om uppgifterna, t.ex. efter en kontroll, visar sig vara nödvändiga för att utreda brott eller ha samband med allvarlig misstänkt brottslig verksamhet bör de dock få behandlas inom ramen för den utredningen eller det underrättelseärendet och göras gemensamt tillgängliga (se prop. 2016/17:91 s. 107).

Även polisen bör få göra nu aktuella personuppgifter gemensamt tillgängliga. Det kan dock inte bli fråga om att göra större mängder information gemensamt tillgänglig, eftersom den till största delen rör personer som inte är intressanta för brottsbekämpningen. I stället kommer det att vara uppgifter om någon eller några personer eller transporter som är av betydelse i underrättelseverksamheten eller i en brottsutredning som görs gemensamt tillgängliga. Vilka uppgifter som får göras gemensamt tillgängliga framgår av 3 kap. 2 § första stycket polisdatalagen. Enligt punkten 1 får uppgifter som kan antas ha samband med viss misstänkt brottslig verksamhet göras gemensamt tillgängliga. Detsamma gäller enligt punkten 3 uppgifter som förekommer i ett ärende om utredning eller beivrande av brott. Utredningen kan inte se att det skulle finnas andra fall i vilka uppgifter från transportföretag skulle behöva göras gemensamt tillgängliga. Någon särskild reglering behövs därför inte.

7.4.4 Hur länge personuppgifterna får behandlas

Utredningens förslag: Det ska inte finnas någon särskild bestämmelse om att uppgifter från transportföretag ska förstöras om de visar sig sakna betydelse för utredning av eller lagföring för brott.

Skälen för utredningens förslag: Enligt 26 § tredje stycket polislagen ska uppgifter om enskilda personer som ett transportföretag lämnat på annat sätt än genom terminalåtkomst omedelbart förstöras om de visar sig sakna betydelse för utredning av eller lagföring för brott.

Polismyndigheten har inte samma behov som Tullverket att i sin brottsbekämpande verksamhet fortlöpande ta del av alla uppgifter från transportföretag inför att transporterna ankommer. Behovet av uppgifter är mera relaterat till att i vissa fall kunna kontrollera vilka som förväntas komma med en viss transport eller att i efterhand kunna granska vilka personer som åkt med en viss transport. Mot den bakgrunden finns det inte samma behov av en särregel om förstörande. Enligt 2 kap. 17 § första stycket brottsdatalagen får personuppgifter inte behandlas under längre tid än nödvändigt med hänsyn till ändamålet med behandlingen. Bestämmelsen ger enligt utredningens mening tillräckligt skydd för uppgifterna. Det finns därför inte något behov av att införa en bestämmelse motsvarande 26 § tredje stycket polislagen när regleringen flyttas till polisens brottsdatalag (jfr avsnitt 5.3.11).

7.5 Gemensamt tillgängliga uppgifter

7.5.1 Nya kategorier av personuppgifter får göras gemensamt tillgängliga

Utredningens förslag: Personuppgifter som förekommer i ärenden om kontaktförbud eller om personskydd ska få göras gemensamt tillgängliga. Uppgifterna ska inte få behandlas längre än ett år efter det att ärendet som de behandlades i avslutades.

Personuppgifter som behandlas i syfte att upprätthålla allmän ordning och säkerhet ska också få göras gemensamt tillgängliga. De ska inte få behandlas längre än ett år efter utgången av det kalenderår då de behandlades automatiserat första gången.

Skälen för utredningens förslag

Personuppgifter i ärenden om kontaktförbud eller personskydd

I 3 kap. 2 § första stycket polisdatalagen anges vilka personuppgifter som får göras gemensamt tillgängliga. Det är bl.a. uppgifter som kan antas ha samband med misstänkt brottslig verksamhet, om den innefattar brott för vilket är föreskrivet fängelse i ett år eller däröver eller sker systematiskt, och uppgifter som förekommer i ärenden om utredning eller beivrande av brott som får göras gemensamt tillgängliga.

Om någon utsätts för hot eller våld är det viktigt att polisen så snabbt som möjligt får kännedom om huruvida han eller hon tidigare har varit utsatt för brott eller är föremål för skyddsåtgärder av något slag. Det finns då bättre förutsättningar att snabbt hitta gärningsmannen. När det gäller personer som skyddas av exempelvis kontaktförbud eller personsäkerhetsåtgärder är det dock inte alltid som personuppgifterna kan knytas till misstanke om brottslig verksamhet eller en utredning om brott så att uppgifterna av det skälet får göras gemensamt tillgängliga. Det finns därför behov av att kunna göra uppgifter om personer med någon form av skyddsbehov gemensamt tillgängliga. Det kan vara personer som skyddas av ett kontaktförbud, är föremål för vittnesskydd eller annat personsäkerhetsarbete.

Det är dock inte bara uppgifter om den person som har ett sådant skyddsbehov som bör få göras gemensamt tillgängliga. Det bör även gälla uppgifter om närstående till sådana personer, eftersom hot eller våld kan riktas mot dem för att komma åt den person som har det egentliga skyddsbehovet. Bestämmelsen kan lämpligen formuleras så att personuppgifter som förekommer i ärenden om kontaktförbud eller om personskydd får göras gemensamt tillgängliga. Med hänsyn till att personuppgifterna förekommer i ärenden bör de inte få behandlas längre än ett år efter det att ärendet som uppgifterna behandlades i avslutades. Regleringen av hur länge uppgifterna får behandlas behöver inte på samma sätt som i 3 kap. 14 § fjärde stycket polisdatalagen knytas till kalenderår, eftersom det enligt uppgift numera är tekniskt möjligt att ta bort uppgifterna oberoende av när under året tidsfristen löper ut.

Personuppgifter som behandlas i syfte att upprätthålla allmän ordning och säkerhet

Som framgår av avsnitt 7.2.1 föreslår utredningen att polisens brottsdatalag ska tillämpas på Polismyndighetens personuppgiftsbehandling i syfte att upprätthålla allmän ordning och säkerhet. I förarbetena till polisdatalagen framhålls att det är svårt att dra en tydlig gräns mellan polisens ordningshållning och brottsbekämpning, vilket beror på att övervakning och ordningshållande verksamhet även kan syfta till att förebygga och ingripa mot brott. Sådan verksamhet kan också ofta övergå i brottsbekämpning (se prop. 2009/10:85 s. 75). Inför kommenderingar vid särskilda händelser där ordningsstörningar befaras, t.ex. en fotbollsmatch eller en demonstration, kan det finnas behov av att göra uppgifter om tillträdesförbud eller uppgifter om personer som tidigare orsakat ordningsstörningar gemensamt tillgängliga. Även om sådana uppgifter i vissa fall skulle kunna göras gemensamt tillgängliga med stöd av 3 kap. 2 § första stycket 1 polisdatalagen är det inte givet att så alltid är fallet. Därför bör det tydliggöras att personuppgifter som behandlas i syfte att upprätthålla allmän ordning och säkerhet får göras gemensamt tillgängliga.

Personuppgifter som görs gemensamt tillgängliga i syfte att upprätthålla allmän ordning och säkerhet bör inte få behandlas längre än ett år efter utgången av det kalenderår då de behandlades automatiserat första gången.

7.5.2 Sökning i gemensamt tillgängliga uppgifter

Utredningens förslag: Bestämmelsen som begränsar resultatet vid sökning i gemensamt tillgängliga uppgifter med hjälp av namn, personnummer, samordningsnummer eller liknande identitetsbeteckningar ska enbart gälla i automatiserade behandlingssystem. Vid sådan sökning får uppgifter om personer som berörs av ett kontaktförbud eller av åtgärder i ett personskyddsärendet tas fram.

Begränsningarna ska inte gälla vid sökning i en viss handling eller i ett visst ärende. De ska inte heller gälla vid sökning som görs av särskilt angivna tjänstemän

1. när de utför beredningsuppgifter inom underrättelseverksamhet och arbetet befinner sig i ett inledande skede,
2. i syfte att i underrättelseverksamhet bearbeta och analysera personuppgifter som har gjorts gemensamt tillgängliga enligt vissa bestämmelser och som enbart dessa tjänstemän har tillgång till,
3. i syfte att utreda brott för vilket det är föreskrivet fängelse i fyra år eller däröver, eller
4. i syfte att samordna utredningar om brott som kan vara systematiska och för vilka det är föreskrivet fängelse i två år eller däröver.

Det ska också göras undantag för sökning som en tjänsteman vid någon av Polismyndighetens ledningscentraler utför på begäran av en polisman som verkställer ett ingripande eller vidtar en åtgärd som rör en enskild.

Skälen för utredningens förslag

Begränsning endast i automatiserade behandlingssystem

Från integritetssynpunkt är en av de viktigaste aspekterna med behandling av personuppgifter i vilken utsträckning uppgifter kan sökas och sammanställas. Ett av syftena med polisdatalagen är att polisen på ett bättre sätt ska kunna dra nytta av redan insamlad information. Lagen ger utrymme för att samla in och behandla en mängd olika personuppgifter, vilket gör att det kan finnas uppgifter om samma person i olika system och uppgiftssamlingar. De möjligheter till behandling som lagen ger och mängden information skulle – om det inte fanns några begränsningar – skapa utrymme för kvalificerade kartläggningar av enskildas personliga förhållanden, vilket kan utgöra ett intrång i den personliga integriteten (se prop. 2009/10:85 s. 153). För att värna den personliga integriteten har det därför i polisdatalagen införts särskilda begränsningar vid sökning i gemensamt tillgängliga uppgifter.

Eftersom sökning med hjälp av personnummer är ett viktigt inslag i polisens verksamhet och sådana identitetsbeteckningar är av

stor betydelse för att säkerställa identiteten och undvika personförväxlingar, ansågs det nödvändigt att medge sådan sökning i gemensamt tillgängliga uppgifter. I 3 kap. 6 § polisdatalagen regleras därför vilka uppgifter som får tas fram vid sökning på namn, personnummer, samordningsnummer eller andra liknande identitetsuppgifter. I 3 kap. 7 § görs vissa undantag från bestämmelserna i 3 kap. 6 §. I förarbetena diskuteras ingående vilka sökningar som bör vara tillåtna och vilka begränsningar som bör gälla (se prop. 2009/10:85 s. 159 f.). Syftet med begränsningsregeln är att det vid en initial allmän sökning bara ska vara möjligt att få fram vissa typer av uppgifter som ansetts vara polisiärt intressanta. Om det finns förutsättningar för att gå vidare och söka efter andra uppgifter beror på syftet med sökningen i det enskilda fallet och vilken behörighet den som söker informationen har tilldelats. Bestämmelsen ska alltså inte förstås så att den hindrar vidare sökning för den som har behov av det för att fullgöra sina arbetsuppgifter och som har tilldelats den behörighet som fortsatt sökning kräver.

Begränsningen gäller bara för uppgifter som behandlas med stöd av polisdatalagen. Den hindrar inte att det vid sökning även tas fram andra uppgifter som polisen har tillgång till, exempelvis genom direktåtkomst till folkbokföringen eller körkorts-, fordons- eller fastighetsregister. Vilken sökning som är tillåten i andra register regleras i de författningar som gäller för dem.

Regleringen är inte heller tänkt att träffa alla uppgifter som görs gemensamt tillgängliga. Det är varken tekniskt eller praktiskt möjligt att vid en allmän sökning inom rimlig tid ge tillgång till så stora mängder information. Genom att det numera är möjligt att göra fritextsökning i stora mängder information skulle det ställas orimliga krav på att information i vanliga textdokument skulle kategoriseras och göras sökbara respektive icke sökbara beroende på vad uppgiften gäller enbart för att uppfylla kraven på att begränsa resultatet vid sökning. För att tydliggöra att bestämmelsen inte är avsedd att träffa sådana sökningar bör det framgå att den enbart gäller i automatiserade behandlingssystem. Genom ett sådant förtydligande kan vissa missförstånd om hur bestämmelsen är tänkt att tillämpas undanröjas.

Bör ytterligare uppgifter få tas fram vid sökning?

Övergångsbestämmelserna till polisdatlagen innebär att bestämmelserna i 3 kap. 6 och 7 §§ ännu inte har börjat tillämpas. Det saknas därför erfarenheter av hur begränsningarna kommer att fungera i praktiken. Det kan också noteras att regeringen enligt 3 kap. 7 § fjärde stycket har möjlighet att göra ytterligare undantag från bestämmelserna i 3 kap. 6 §.

Mot bakgrund av de noggranna överväganden som gjordes när reglerna infördes finns det nu främst anledning att överväga om lagens delvis ändrade tillämpningsområde bör föranleda någon ändring. För Polismyndighetens del omfattar polisens brottsdatalog även behandling av personuppgifter för att upprätthålla allmän ordning och säkerhet. De uppgifter som då främst kan vara av intresse är uppgifter om att någon har straffats för eller är misstänkt för brott mot allmän ordning. Sådana uppgifter är redan i dag tillgängliga vid sökning. Detsamma gäller uppgifter om att någon kan antas komma att möta ett polisingripande med grovt våld. Det som i vissa sammanhang kan vara av intresse är uppgift om att någon har meddelats tillträdesförbud enligt lagen om tillträdesförbud vid idrottsarrangemang. Uppgifter om att någon har meddelats tillträdesförbud registreras i belastningsregistret och är på det sättet tillgängliga.

I avsnitt 7.5.1 föreslår utredningen att personuppgifter i ärenden om kontaktförbud eller om personskydd ska få göras gemensamt tillgängliga. För att den bestämmelsen ska få avsedd effekt, bör det vid sökning i gemensamt tillgängliga uppgifter få tas fram uppgifter som visar att den sökta personen berörs av ett kontaktförbud eller av åtgärder i ett personskyddsärende. Genom användningen av ordet berörs täcks även närstående. Det kan vara svårt att avgöra vilka uppgifter om en sådan person som bör göras sökbara, eftersom personen i fråga kan ha skyddade adressuppgifter eller annat skydd. Som regel torde det räcka att uppgifter om att personen har särskilt skyddsbehov görs sökbara.

I övrigt finns det inte anledning att utöka de nu gällande möjligheterna att få fram uppgifter vid en allmän sökning.

Behövs det fler eller andra undantag från begränsningsregeln?

Det som däremot bör övervägas är om det kan finnas skäl att göra någon ändring i undantagen från bestämmelserna i 3 kap. 6 § polisdatlagen om vad som får tas fram vid sökning. Enligt uppgift har undantaget i 3 kap. 7 § första stycket punkten 2 ibland tolkats på det sättet att man kan kringgå begränsningarna i 3 kap. 6 § genom att skapa en särskild uppgiftssamling, eftersom det gäller ett generellt undantag för personuppgifter som behandlas i sådana uppgiftssamlingar. Att bestämmelsen kan missbrukas är givetvis olyckligt och den bör mot den bakgrunden ändras.

Ändringen kan lämpligen göras på det sättet att undantaget knyts till att uppgifter behandlas i underrättelseverksamhet i syfte att bearbeta och analysera information som dels har gjorts gemensamt tillgänglig enligt 3 kap. 2 § första stycket 1 eller 2, dels endast särskilt angivna tjänstemän har tillgång till. I den regleringen täcks både 3 kap. 7 § första stycket punkten 2 och andra stycket punkten 1. Dessa båda punkter ersätts således av den nya, mer generellt utformade, punkten. Den ger ökade möjligheter till sökning, men begränsar samtidigt sökmöjligheterna på det sättet att endast särskilt angivna tjänstemän får utföra sådana sökningar. Utredningen anser att det är en rimlig avvägning mellan brottsbekämpningens behov och skyddet för personlig integritet.

Mot bakgrund av ökande problem med organiserad brottslighet i form av bl.a. kringresande ligor och annan seriebrottslighet kan det också finnas skäl att göra undantag vid sökning som utförs som ett led i att utreda brott som kan vara systematiska och för vilka det är föreskrivet fängelse i två år eller däröver, om sökningen görs av särskilt utpekade tjänstemän som sysslar med brottsamordning.

Den polispersonal som arbetar i yttre tjänst har ofta behov av att kunna få hjälp av personal vid Polismyndighetens ledningscentraler med sökning i syfte att klarlägga t.ex. en gripen eller omhändertagen persons identitet. Det kan också finnas behov av att söka fram uppgifter om minderårigas adress och vårdnadshavare eller att söka efter anhöriga till någon som har skadats i samband med ett brott. Vid sökningar av det slaget kan det vara nödvändigt att ta fram andra typer av information, samtidigt som den ingripande polismannen inte alltid har tillgång till nödvändiga sökmöjligheter i sin utrustning. Det bör därför även göras undantag

från begränsningsregeln för sökning som görs i Polismyndighetens ledningscentraler på begäran av en polisman i yttre tjänst.

I 6 § polisdataförordningen görs undantag från 3 kap. 6 § första stycket polisdatalagen för sökning som görs av särskilt angivna tjänstemän för att utföra beredningsuppgifter inom underrättelseverksamhet. Syftet med bestämmelsen är att möjliggöra att fler uppgifter kan tas fram i det inledande skedet av underrättelsearbete. Bestämmelsen bör i likhet med övriga undantag från begränsningsregeln finnas i lag. Det bör också tydliggöras att undantaget endast avser sökning i ett inledande skede.

7.6 Längsta tid för behandling

Utredningens förslag: Personuppgifter som kan antas ha samband med viss brottslig verksamhet ska, om de behandlas i ett ärende, inte få behandlas längre än ett år efter det att ärendet avslutades.

Skälen för utredningens förslag: I 3 kap. 14 § andra stycket polisdatalagen regleras hur länge personuppgifter som behandlas i viss underrättelseverksamhet får behandlas.

I underrättelseverksamhet behandlas personuppgifter som huvudregel inte i ärenden och regleringen av när behandlingen ska upphöra utgår därför från när den senaste registreringen avseende personen gjordes. I t.ex. samarbetet mot grov organiserad brottslighet görs vissa personuppgifter gemensamt tillgängliga i underrättelseverksamheten för att andra myndigheter ska kunna ta del av dem, trots att de endast behandlas av ett fåtal personer vid Polismyndigheten. Sådan information behandlas då i särskilda ärenden. Detsamma kan vara fallet i anslutning till en särskild händelse eller om myndigheterna får i uppdrag att samarbeta på visst sätt inom underrättelseverksamheten. När personuppgifter behandlas i ärenden i underrättelseverksamhet bör uppgifterna, på samma sätt som vid behandling av personuppgifter i andra ärenden, inte få behandlas längre än ett år efter det att ärendet avslutades. Hur bestämmelsen bör formuleras behandlas i avsnitt 5.5.2 och 7.5.1.

7.7 Personuppgiftsbehandling i särskilda register

7.7.1 Dna-register

Utredningens förslag: I polisens brottsdatalog ska det anges för vilka syften Polismyndigheten får föra dna-register.

Skälen för utredningens förslag: Enligt 4 kap. 1 § första stycket polisdatalagen får Polismyndigheten i den brottsbekämpande verksamheten föra register över dna-profiler. Av 1 kap. 7 § framgår att 2 kap. gäller vid behandling av personuppgifter i register enligt 4 kap. Det innebär att dna-registren får föras för de ändamål som anges i 2 kap. 7 § (se prop. 2009/10:85 s. 351). Registren får även föras för att underlätta identifiering av avlidna personer.

På samma sätt som när det gäller bestämmelserna om tillämpningsområde och tillåtna rättsliga grunder för behandling bör regleringen av dna-registren inte längre utgå från i vilken verksamhet personuppgiftsbehandlingen utförs, utan från syftet med behandlingen. Utredningen anser att det blir tydligare att räkna upp för vilka syften registren får föras i stället för att det ska läsas ut genom en hänvisning till bestämmelser i ett annat kapitel. Dna-registren bör på samma sätt som i dag få föras i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, fullgöra förpliktelser som följer av internationella åtaganden och underlätta identifiering av avlidna personer.

Hur 4 kap. 7 § polisdatalagen som reglerar gallring i dna-registren bör formuleras behandlas i avsnitt 5.5.2.

7.7.2 Fingeravtrycks- och signalementsregister

Utredningens förslag: I polisens brottsdatalog ska det anges för vilka syften Polismyndigheten får föra fingeravtrycks- och signalementsregister.

Skälen för utredningens förslag: Enligt 4 kap. 11 § polisdatalagen får Polismyndigheten föra fingeravtrycks- och signalementsregister. Av 1 kap. 7 § framgår att 2 kap. gäller vid behandling av personuppgifter i register enligt 4 kap. Det innebär att fingeravtrycks-

och signalementsregister får föras för de ändamål som anges i 2 kap. 7 § (se prop. 2009/10:85 s. 355). Registren får även föras för att underlätta identifiering av okända personer.

På samma sätt som när det gäller dna-registren bör det tydliggöras för vilka syften fingeravtrycks- och signalementsregister får föras i stället för att det ska läsas ut genom en hänvisning till bestämmelser i ett annat kapitel. Fingeravtrycks- och signalementsregister bör på samma sätt som i dag få föras i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, fullgöra förpliktelser som följer av internationella åtaganden och underlätta identifiering av okända personer.

Registren bör även i likhet med i dag få föras för att kontrollera fingeravtryck som Migrationsverket tagit enligt 9 kap. 8 § utlänningslagen, vilket motsvarar regleringen i 2 kap. 8 § första stycket 6 polisdatlagen.

I avsnitt 5.5.2 behandlar utredningen frågan om hur 4 kap. 14 och 15 §§ som reglerar gallring i fingeravtrycks- och signalementsregister bör formuleras.

7.8 Personuppgiftsbehandling för forensiska ändamål

7.8.1 Vad är forensiska ändamål?

Personuppgiftsbehandling vid Polismyndigheten för forensiska ändamål regleras i 5 kap. polisdatlagen. Forensik är ett sammanfattande begrepp för utveckling och tillämpning av metoder från olika vetenskapliga ämnesområden – t.ex. biologi, kemi eller teknologi – på frågeställningar om framför allt olika typer av fysiska spår som undersöks i anledning av misstanke om brott. Särskilda krav ställs på oberoende och vetenskaplig grund. Det är alltså bara de åtgärder som vilar på denna forensiska grund som kan sägas vara forensiska åtgärder. I kravet på oberoende ligger också att forensiska undersökningar, analyser och jämförelser hanteras helt separat från annat utredningsarbete under en förundersökning. Vad som görs och hur det dokumenteras är enbart beroende av vilket behov som finns i det enskilda ärendet av att forensiskt undersöka och analysera visst material. För frågan om ett visst föremål eller material hanteras för forensiska ändamål eller inte saknar det betydelse

om det har tagits i beslag. Att en undersökning äger rum inom ramen för en förundersökning är inte heller avgörande för frågan om bevismaterial hanteras för forensiska ändamål eller inte. Gränsdragningen mellan forensiska ändamål och brottsbekämpande ändamål diskuteras utförligt i förarbetena till 5 kap. (se Den nya polisorganisationen – några frågor om personuppgiftsbehandling m.m., prop. 2014/15:94, s. 56 f.).

Behandling för forensiska ändamål vid Polismyndigheten utförs huvudsakligen av Nationellt forensiskt centrum, men även andra enheter inom myndigheten utför viss sådan behandling. I delbetänkandet bedömer utredningen att den behandling för forensiska ändamål som Nationellt forensiskt centrum utför åt den egna myndigheten och åt andra behöriga myndigheter omfattas av brottsdatalagens tillämpningsområde (se SOU 2017:29 s. 189 f.). Det gäller även motsvarande behandling för forensiska ändamål av personuppgifter vid en annan enhet inom Polismyndigheten.

I förarbetena till 5 kap. anges att syftet med regleringen är att skapa en sammanhållen reglering av den forensiska processen inom Polismyndigheten (se prop. 2014/15:94 s. 56). De särskilda reglerna för personuppgiftsbehandling för forensiska ändamål är således inte tillämpliga i Ekobrottsmyndighetens och Säkerhetspolisens verksamhet.

7.8.2 Regleringen av forensiska ändamål behålls

Utredningens bedömning: Bestämmelserna om för vilka ändamål personuppgifter får behandlas i den forensiska verksamheten bör behållas.

Skälen för utredningens bedömning: I 5 kap. 1–3 §§ polisdatalagen anges för vilka ändamål personuppgifter får behandlas i den forensiska verksamheten vid Polismyndigheten. Ändamålen delas upp i primära och sekundära på samma sätt som i 2 kap. 7 och 8 §§ polisdatalagen. De primära ändamålen anger den behandling som utförs för forensiska ändamål vid Polismyndigheten, medan de sekundära ändamålen anger när uppgifter som behandlas för forensiska ändamål får användas i andra delar av myndighetens verksamhet.

het eller lämnas ut till andra myndigheter eller organisationer för deras behov.

I avsnitt 6.1.3 konstaterar utredningen att vad som i dataskyddsrättslig mening är tillåtna rättsliga grunder för behandling och vad som är renodlade ändamålsbestämmelser ibland har blandats samman. En ändamålsbestämmelse bör enligt utredningens mening ge ledning för prövningen av vilka personuppgifter som är adekvata och relevanta för behandlingen. Utredningen anser att 2 kap. 7 § polisdatlagen inte är en ändamålsbestämmelse i egentlig mening utan att den är en del av den rättsliga grunden och anger ramen för när personuppgifter får behandlas. Bestämmelserna i 5 kap. 1 och 2 §§ polisdatlagen om för vilka ändamål personuppgifter får behandlas i den forensiska verksamheten är betydligt mer konkreta och ger tydlig ledning för vilka personuppgifter som är adekvata och relevanta för behandlingen. De är således enligt utredningens mening ändamålsbestämmelser. De behöver inte anpassas till regleringen i brottsdatlagen utan bör behållas oförändrade.

7.8.3 Behandling för nya ändamål

Utredningens förslag: Det ska framgå genom en hänvisning att personuppgifter som behandlas för forensiska ändamål ska få behandlas för nya ändamål enligt de förutsättningar som anges i brottsdatlagen. Enbart personuppgifter som behandlas för vissa forensiska ändamål ska få behandlas för nya ändamål utanför den forensiska verksamheten.

Skälen för utredningens förslag

Kan den nuvarande regleringen av utlämnande behållas?

Den sekundära ändamålsbestämmelsen i 5 kap. 3 § polisdatlagen reglerar som nyss nämnts i vilken utsträckning personuppgifter som behandlas för något primärt forensiskt ändamål även får behandlas för att lämnas ut till andra för att tillgodose deras behov. Den reglerar alltså behandling för nya ändamål. Enligt paragrafen får personuppgifter som behandlas för vissa av de primära ändamålen även behandlas när det är nödvändigt för att tillhandahålla

information som behövs i annan brottsbekämpande verksamhet hos Polismyndigheten eller i brottsbekämpande verksamhet hos Säkerhetspolisen, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen eller Skatteverket. I ett enskilt fall får personuppgifter som behandlas för forensiska ändamål även behandlas för att tillhandahålla information för något annat ändamål, under förutsättning att ändamålet inte är oförenligt med det ändamål som uppgifterna samlades in för.

Innan personuppgifter behandlas för ett nytt ändamål inom brottsdatalagens tillämpningsområde ska det enligt 2 kap. 4 § brottsdatalagen säkerställas dels att det finns en tillåten rättslig grund för behandlingen, dels att behandlingen är nödvändig och proportionerlig för det nya ändamålet. Det innebär att en prövning alltid måste göras innan personuppgifter behandlas för nya ändamål, oavsett om det är för forensiska ändamål eller för andra ändamål inom brottsdatalagens tillämpningsområde. Om den sekundära ändamålsbestämmelsen skulle behållas, där utlämnande av personuppgifter i de flesta fall är tillåtet utan någon annan prövning än om det är nödvändigt att tillhandahålla informationen, skulle prövningen enligt brottsdatalagen sättas ur spel. En sådan prövning krävs enligt artikel 4.2 i direktivet. Det är således inte förenligt med direktivet att behålla den sekundära ändamålsbestämmelsen med den utformning den har i dag.

Bör möjligheterna att lämna ut personuppgifter begränsas på annat sätt?

I dag är det som huvudregel bara personuppgifter som behandlas för vissa forensiska ändamål som får behandlas utanför den forensiska verksamheten för att tillhandahållas de brottsbekämpande myndigheterna. Personuppgifter som behandlas när Nationellt forensiskt centrum begär eller utför forensiska åtgärder åt Rättsmedicinalverket, utländska laboratorier, utländska brottsbekämpande myndigheter, mellanfolkliga organisationer eller EU-organ med brottsbekämpande uppgifter, när centrumet begär åtgärder av ett annat expertorgan eller när uppgifter behandlas för forskning och statistik får som huvudregel inte behandlas utanför den forensiska verksamheten. Skälet till det är enligt förarbetena att det då inte finns skäl att redovisa resultaten för någon annan än uppdrags-

givaren (se prop. 2014/15:94 s. 67). Samma begränsningar bör gälla även i fortsättningen. Med hänsyn till kraven på nödvändighet och proportionalitet innan personuppgifter behandlas för nya ändamål finns det dock inte längre skäl att räkna upp till vilka myndigheter uppgifterna får lämnas ut.

I ett enskilt fall får också personuppgifter som behandlas för något forensiskt ändamål behandlas för andra ändamål, om det inte är oförenligt med insamlingsändamålet. Det kan avse ändamål både inom och utanför brottsdatalagens tillämpningsområde. Som anges i delbetänkandet bedömer utredningen att finalitetsprincipen inte ska tillämpas vare sig vid behandling inom tillämpningsområdet eller utanför det (se SOU 2017:29 s. 247 f. och 292 f.) Bestämmelsen kan därför inte behållas.

Utredningen föreslår i avsnitt 6.4.3 att en prövning av att behandlingen är nödvändig och proportionerlig ska göras även när de brottsbekämpande myndigheterna behandlar personuppgifter för nya ändamål utanför brottsdatalagens tillämpningsområde. En sådan prövning utgör enligt utredningens mening en lämplig avvägning mellan mottagarens behov av personuppgifterna och skyddet för enskildas personliga integritet även när det gäller personuppgifter som behandlas för forensiska ändamål. Den föreslagna bestämmelsen i brottsdatalagen bör därför gälla även vid behandling för forensiska ändamål.

7.8.4 Behandling av känsliga personuppgifter

Utredningens förslag: Biometriska uppgifter och genetiska uppgifter ska få behandlas för forensiska ändamål enligt de förutsättningar som anges i brottsdatalagen.

Sökförbudet i brottsdatalagen ska inte hindra sökningar i register som regleras särskilt i 5 kap. polisens brottsdatalag i syfte att få fram ett personurval grundat på uppgifter som rör hälsa eller biometriska eller genetiska uppgifter.

Skälen för utredningens förslag

Behandling av biometriska och genetiska uppgifter

I avsnitt 7.3.2 beskrivs vad som avses med biometriska och genetiska uppgifter. Enligt 2 kap. 12 och 13 §§ brottsdatalagen utgör biometriska uppgifter som används för att identifiera en person och genetiska uppgifter känsliga personuppgifter. Sådana uppgifter får endast behandlas om det är särskilt föreskrivet och det är absolut nödvändigt för ändamålet med behandlingen. Behandling av sådana uppgifter är en viktig del i den forensiska verksamheten, inte minst vid dna-analyser och behandling av personuppgifter i dna-registren och fingeravtrycks- och signalementsregistret. Den tekniska utvecklingen ger också nya möjligheter att använda framför allt biometri. Det kommer därför sannolikt att finnas ett ökande behov av att kunna behandla biometriska uppgifter för forensiska ändamål. Det bör därför föreskrivas att biometriska och genetiska uppgifter får behandlas för sådana ändamål.

Med hänsyn till att sådana uppgifter enligt brottsdatalagen endast får behandlas om det är absolut nödvändigt för ändamålet med behandlingen bedömer utredningen att det för närvarande inte finns skäl att begränsa möjligheterna att behandla biometriska och genetiska uppgifter ytterligare.

Undantag från sökförbudet i brottsdatalagen

Sökförbudet i 2 kap. 14 § brottsdatalagen utgår till skillnad från dagens reglering från syftet med sökningen. Om syftet inte är att få fram ett personurval grundat på känsliga personuppgifter är sökningen tillåten, även om känsliga personuppgifter används vid sökningen.

Det är Nationellt forensiskt centrum vid Polismyndigheten som administrerar dna-registren och fingeravtrycks- och signalementsregister. Vid sökning i registren används dna-profiler respektive fingeravtryck, vilket är biometriska uppgifter (se SOU 2017:29 s. 265 f.). Sökning på fingeravtryck resulterar alltid i en träfflista, vilket då blir ett personurval grundat på biometriska uppgifter. Det bör därför vara tillåtet att göra sökningar i syfte att få fram ett

personurval grundat på biometriska uppgifter i den forensiska verksamheten.

Information i forensiska databaser kan användas för att ge övriga delar av Polismyndigheten spaningsuppslag, s.k. forensiska uppslag. Tanken med det är att de iakttagelser som görs vid forensiska undersökningar i olika ärenden ska kunna komma till nytta i polisverksamheten som helhet eller i annan brottsbekämpande verksamhet (se prop. 2014/15:94 s. 62 f.). Det går exempelvis att genomföra s.k. familjesökning, vilket innebär att man jämför dna-profiler för att finna släktingar till en viss person, exempelvis en oidentifierad misstänkt. Familjesökning baserar sig på att nära släktingar till viss del har överensstämmande arvs massa och sökningar görs då mellan en dna-profil och registrerade dna-profiler med en längre grad av matchning mellan profilernas str-markörer. Sådana sökningar kan resultera i ett personurval grundat på biometriska uppgifter. Det finns därför skäl att göra undantag från sökförbudet när det gäller behandling av biometriska uppgifter i den forensiska verksamheten.

Möjligheterna att ta fram information ur dna-prover utvecklas hela tiden. Det går redan i dag att få fram olika personliga egenskaper som ögonfärg, ärftliga sjukdomar eller en persons biogenetiska ursprung. Det bör vara tillåtet att göra sökningar i syfte att få fram ett personurval grundat på genetiska uppgifter eller uppgifter som rör hälsa i den forensiska verksamheten.

8 Tullbrottsdatalagen

8.1 Tullbrottsdatalagen behöver anpassas

8.1.1 Nuvarande reglering

Tullbrottsdatalagen gäller enligt 1 kap. 2 § vid behandling av personuppgifter i Tullverkets brottsbekämpande verksamhet. Lagen trädde i kraft den 1 juli 2017. Vissa bestämmelser behöver dock inte tillämpas före den 1 januari 2019.

Vid myndighetens personuppgiftsbehandling i annan operativ verksamhet gäller lagen (2001:185) om behandling av uppgifter i Tullverkets verksamhet.

Som anges i avsnitt 4.2 måste registerförfattningarna ändras i vissa avseenden med anledning av dataskyddsdirektivet och anpassas till brottsdatalagen. Många bestämmelser behöver överhuvudtaget inte anpassas eller endast ändras redaktionellt. Utredningen behandlar de anpassningar och ändringar som är gemensamma för registerförfattningarna i kapitel 5 och 6. De ytterligare anpassningar som krävs i tullbrottsdatalagen behandlas i detta kapitel.

8.1.2 Tullbrottsdatalagen ges ett nytt namn

<p>Utredningens förslag: Tullbrottsdatalagen med tillhörande förordning ska benämnas Tullverkets brottsdatalag och Tullverkets brottsdataförordning.</p>

Skälen för utredningens förslag: Av de skäl som anges i avsnitt 7.1.2 finns det skäl att byta namn på registerförfattningarna inom brottsdatalagens tillämpningsområde. Trots att tullbrottsdatalagen nyligen fått sitt namn bör lagen därför enligt utredning-

ens mening ges ett nytt namn. Namnet bör knyta an till hur brottsdatalagen benämns. Det bör vara kort och tydligt ange för vem författningen gäller och vad den handlar om. Utredningen föreslår därför att lagen ska benämnas Tullverkets brottsdatalag. Tullbrottsdataförordningen bör i konsekvens med det benämnas Tullverkets brottsdataförordning. Som en konsekvens av att lagens namn ändras måste alla hänvisningar till den ändras.

8.2 Tillämpningsområdet

Utredningens förslag: Lagen ska gälla utöver brottsdatalagen när Tullverket i egenskap av behörig myndighet behandlar personuppgifter i syfte att bekämpa eller lagföra brott.

Skälen för utredningens förslag: I avsnitt 4.4.1 tar utredningen ställning till att registerförfattningarna även i fortsättningen ska innehålla bestämmelser om tillämpningsområdet. Vidare föreslår utredningen i avsnitt 5.2 att registerförfattningarna ska gälla utöver brottsdatalagen.

Enligt 1 kap. 2 § tullbrottsdatalagen gäller lagen i Tullverkets brottsbekämpande verksamhet. Tillämpningsområdet måste dock anpassas till brottsdatalagens tillämpningsområde så att det utgår från syftet med behandlingen i stället för i vilken verksamhet behandlingen utförs. Det bör också framgå att lagen endast gäller när Tullverket agerar i egenskap av behörig myndighet, eftersom det är en viktig avgränsning för tillämpningsområdet (se SOU 2017:29 s. 159 f.).

Som framgår av avsnitt 5.4.6 anses lagföring av brott i dag ingå i begreppet brottsbekämpning, medan det i brottsdatalagen görs skillnad mellan brottsbekämpning och lagföring. Det bör därför klargöras att tillämpningsområdet omfattar personuppgiftsbehandling i syfte att bekämpa och lagföra brott.

I avsnitt 4.4.2 diskuterar utredningen vad det ändrade tillämpningsområdet innebär.

8.3 Grundläggande bestämmelser om behandling

8.3.1 Tillåtna rättsliga grunder och behandling för nya ändamål

Utredningens förslag: Tullverket ska få behandla personuppgifter om det är nödvändigt för att utföra en arbetsuppgift i syfte att

1. förebygga, förhindra eller upptäcka brottslig verksamhet,
2. utreda eller lagföra brott, eller
3. fullgöra förpliktelser som följer av internationella åtaganden.

Arbetsuppgiften ska framgå av en bindande unionsrättsakt eller av en lag, en förordning eller ett särskilt beslut i vilket regeringen uppdragit åt myndigheten att ansvara för en sådan uppgift.

Det ska framgå genom en hänvisning att personuppgifter som behandlas med stöd av lagen ska få behandlas för nya ändamål enligt de förutsättningar som anges i brottsdatalagen.

Skälen för utredningens förslag

En bestämmelse som ersätter brottsdatalagens bestämmelse om tillåtna rättsliga grunder för behandling

Som anges i avsnitt 6.3.1 bör registerförfattningarna innehålla bestämmelser om tillåtna rättsliga grunder för behandling av personuppgifter. Regleringen i 2 kap. 5 § tullbrottsdatalagen bör således behållas, men det ska framgå att det inte är en ändamålsbestämelse i egentlig mening. Bestämmelsen är på samma sätt som 2 kap. 1 § brottsdatalagen en del av den rättsliga grunden och ger Tullverket rättsligt stöd för att behandla personuppgifter automatiserat för att utföra sina arbetsuppgifter (se avsnitt 6.1.2).

Tullverket får i dag behandla personuppgifter om det behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller beivra brott eller fullgöra de förpliktelser som följer av internationella åtaganden. Tullverket bör givetvis även i fortsättningen få behandla personuppgifter om det är nödvändigt för att fullgöra

sådana arbetsuppgifter, men regleringen bör anpassas till brottsdatalagens terminologi.

Tullverkets brottsdatalag föreslås gälla utöver brottsdatalagen. För att det inte ska råda någon osäkerhet om hur bestämmelsen i 2 kap. 1 § brottsdatalagen förhåller sig till bestämmelsen om tillåtna rättsliga grunder i registerförfattningen bör den senare helt ersätta bestämmelsen i brottsdatalagen. Det bör därför på samma sätt som i brottsdatalagen i Tullverkets brottsdatalag föreskrivas att den arbetsuppgift som ska utföras ska framgå av en bindande unionsrättsakt eller en lag, en förordning eller ett särskilt beslut i vilket regeringen uppdragit åt Tullverket att ansvara för en sådan uppgift. Vad det innebär utvecklas i delbetänkandet (se SOU 2017:29 s. 238 f.).

Gränsdragningen mot kontrollverksamhet

I delbetänkandet behandlar utredningen frågor om hur gränsen ska dras mellan brottsbekämpning och sådan kontrollverksamhet som ligger utanför brottsdatalagens tillämpningsområde. Som utredningen påpekar där kan gränsdragningen vara svår när det gäller Tullverkets verksamhet (se SOU 2017:29 s. 198 f.). Det gäller framför allt Tullverkets underrättelseverksamhet, som i stor utsträckning ger underlag till de selektiva kontroller av varor och resande som utgör en viktig bas i myndighetens brottsbekämpning, särskilt när det gäller organiserad brottslighet. Den kunskap som uppbyggs i underrättelseverksamheten om bl.a. resrutter, metoder för att dölja otillåtna varor och typiska kännetecken för någon som kan vara smugglare läggs sedan till grund för att bedöma vilka kategorier av personer som bör underkastas kontroll. Underrättelseverksamheten hämtar bl.a. information från andra delar av myndighetens verksamhet, t.ex. upplysningar om iakttagelser som har gjorts vid kontroller och i samband med att personer har ertappats för smugglingsbrott. Det krävs därför ett nära samarbete mellan dem som bedriver underrättelseverksamhet inom Tullverket och dem som utför fysiska tullkontroller i syfte att bekämpa brott. En förutsättning för att Tullverkets brottsbekämpning ska vara framgångsrik är att personuppgifter kan utbytas mellan underrättelseverksamheten och dem som utför kontroller i syfte att bekämpa

brott. De tillåtna rättsliga grunderna ger samma förutsättningar som i dag för sådant informationsutbyte.

Behandling för nya ändamål

I dag regleras behandling för nya ändamål till viss del i den sekundära ändamålsbestämmelsen i 2 kap. 6 § tullbrottsdatalagen. Utredningen anser som framgår av avsnitt 6.3.2 och 6.4.2 att de sekundära ändamålsbestämmelserna bör upphävas. Förutsättningarna för behandling för nya ändamål bör i stället regleras i brottsdatalagen. Innan personuppgifter får behandlas för nya ändamål inom brottsdatalagens tillämpningsområde ska det enligt 2 kap. 4 § brottsdatalagen säkerställas att behandlingen är nödvändig och proportionerlig för det nya ändamålet. Utredningen föreslår att samma prövning ska göras när de brottsbekämpande myndigheterna behandlar personuppgifter för nya ändamål utanför tillämpningsområdet. Det bör införas en bestämmelse i Tullverkets brottsdatalag som tydliggör att förutsättningarna för att behandla personuppgifter, som behandlas med stöd av den lagen, för nya ändamål regleras i brottsdatalagen.

8.3.2 Behandling av biometriska och genetiska uppgifter

Utredningens förslag: Tullverket ska få behandla biometriska uppgifter enligt de förutsättningar som anges i brottsdatalagen.

Utredningens bedömning: Tullverket bör inte få behandla genetiska uppgifter.

Skälen för utredningens förslag och bedömning: I avsnitt 7.3.2 anges vad som avses med biometriska och genetiska uppgifter och vilken betydelse sådana uppgifter har i brottsbekämpningen. Tullverket bör på samma sätt som polisen ha möjlighet att använda biometriska uppgifter i brottsbekämpningen. Enligt 2 kap. 12 § brottsdatalagen får biometriska uppgifter som används för att identifiera en person behandlas bara om det är absolut nödvändigt för ändamålet med behandlingen. Utredningen bedömer att det för

närvarande inte finns skäl att begränsa möjligheterna att använda biometriska uppgifter ytterligare. Det bör därför införas en bestämmelse i Tullverkets brottsdatalag som medger behandling av biometriska uppgifter enligt de förutsättningar som anges i brottsdatalagen.

Det har inte framkommit att Tullverket har behov av att behandla genetiska uppgifter. Utredningen anser därför att myndigheten inte bör få behandla sådana uppgifter. Någon bestämmelse som medger sådan behandling bör därför inte finnas i Tullverkets brottsdatalag.

8.3.3 Sökning på känsliga personuppgifter

Utredningens förslag: Sökförbudet i brottsdatalagen ska inte hindra att brottsrubriceringar, uppgifter om tillvägagångssätt vid brott eller uppgifter som beskriver en persons utseende används vid sökning.

Det ska inte heller hindra sökning i syfte att få fram ett personurval grundat på etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller uppgifter som rör hälsa, sexualliv eller sexuell läggning, om sökningen görs i personuppgifter som inte har gjorts gemensamt tillgängliga.

Skälen för utredningens förslag

Undantag från sökförbudet i brottsdatalagen vid sökning i alla slags personuppgifter

I avsnitt 5.3.8 föreslår utredningen att förbudet i 3 kap. 5 § tullbrottsdatalagen att använda känsliga personuppgifter som sökbegrepp ska upphävas, eftersom det i 2 kap. 14 § brottsdatalagen finns ett generellt förbud. Det förbudet utgår till skillnad från dagens reglering från syftet med sökningen. Om syftet inte är att få fram ett personurval grundat på känsliga personuppgifter är sökningen tillåten, även om känsliga personuppgifter används vid sökningen (se SOU 2017:29 s. 272 f.).

Eftersom sökförbudet har en ny utformning är det nödvändigt att se över bestämmelserna om sökning. Enligt 3 kap. 5 § andra

stycket tullbrottsdatalagen är det tillåtet att använda uppgifter som beskriver en persons utseende som sökbegrepp vid sökning i uppgifter som har gjorts gemensamt tillgängliga. På samma sätt som Polismyndigheten har Tullverket även i fortsättningen behov av att kunna använda sådana uppgifter som sökbegrepp, även om syftet är att få fram ett personurval grundat på känsliga personuppgifter (se avsnitt 7.3.3). Det bör därför enligt utredningens mening göras undantag från brottsdatalagens sökförbud i Tullverkets brottsdatalag. För att möjligheterna till sökning ska vara samma som i dag bör undantaget omfatta sökning i alla slags personuppgifter, dvs. oberoende av om uppgifterna har gjorts gemensamt tillgängliga eller inte.

Tullverket har i likhet med Polismyndigheten behov av att kunna göra sökningar på tillvägagångssätt vid brott och brottsrubriceringar. Sådana sökningar kan i vissa fall leda till ett personurval grundat på känsliga personuppgifter. Som exempel kan nämnas att smugglingsmetoder eller föremål som smugglas kan avslöja religiös övertygelse eller politiska åsikter. Ett annat exempel är att Tullverket vid kontroll av förbudet mot införsel och utförsel av barnpornografi kan behöva söka på brottsrubriceringar som kan avslöja en persons sexualliv eller sexuella läggning. Undantaget från sökförbudet i brottsdatalagen bör därför även omfatta sökning på uppgifter om tillvägagångssätt vid brott och brottsrubriceringar.

I samband med att beslag hävs behöver Tullverket få kännedom om huruvida ägaren verkställer en straffrättslig påföljd och var han eller hon i så fall befinner sig. Om personen verkställer påföljden genom vårdvistelse kan en sådan sökning avslöja uppgifter om hälsa. Behovet av sådan sökning kan enligt utredningens mening tillgodoses på annat sätt än genom ett undantag från sökförbudet. Det kan lämpligen göras genom att Kriminalvården ges skyldighet att på begäran underrätta Tullverket om var en häktad eller intagen är placerad (se avsnitt 13.7.3). Tullverket behöver därför i motsats till Polismyndigheten inget undantag från sökförbudet när det gäller uppgifter om verkställighet av påföljd.

Undantag vid sökning i personuppgifter som inte har gjorts gemensamt tillgängliga

Det nuvarande förbudet i tullbrottsdatalagen mot att använda känsliga personuppgifter som sökbegrepp gäller endast vid sökning i uppgifter som har gjorts gemensamt tillgängliga. Det innebär att känsliga personuppgifter får användas vid sökning i uppgifter som enbart ett fåtal har tillgång till. Den enda begränsningen i dag är att behandling av känsliga personuppgifter ska vara absolut nödvändig.

Utredningens utgångspunkt är att de behöriga myndigheternas möjlighet att använda känsliga personuppgifter vid sökning inte ska försämras. För att effektivt kunna bekämpa brott kan Tullverket ha behov av att kunna göra sammanställningar i syfte att få fram ett personurval grundat på känsliga personuppgifter vid sökningar i uppgifter som inte har gjorts gemensamt tillgängliga. Det finns därför skäl att göra vissa undantag från sökförbudet i brottsdatalagen när det gäller sökning i uppgifter som inte har gjorts gemensamt tillgängliga.

Framför allt i underrättelseverksamheten kan Tullverket behöva göra sökningar som innebär att sammanställningar grundade på etniskt ursprung, religiös övertygelse eller politiska åsikter skapas. Det kan t.ex. vara fallet om det är känt att en viss narkotikasort används av en grupp med visst etniskt ursprung eller religiös övertygelse. Smuggling av drogen kat, som endast odlas utomlands, hör hit. Vid hanteringen av frihetsberövade behöver Tullverket även kunna sammanställa uppgifter om personer som är självmordsbenägna eller s.k. sväljare, vilket innebär att uppgifter om hälsa kan avslöjas. Det är vidare sedan länge känt att det finns politiska eller andra ideologiskt motiverade grupperingar i utlandet som finansierar sin verksamhet genom organiserad brottslighet, t.ex. smuggling av cigaretter eller narkotika. De kan vara aktiva även i Sverige (se Lägesbild organiserad brottslighet 2011, Tullverket). Organiserad brottslighet av olika slag kräver inte sällan kartläggning av misstänkta kontakter och vanor som innebär att olika typer av känsliga personuppgifter kan avslöjas (jfr avsnitt 7.3.3). I kampen mot smuggling av barnpornografiska bilder kan Tullverket även ha behov av att söka på uppgifter som kan avslöja en persons sexualliv eller sexuella läggning, t.ex. på ordet pedofil eller vissa typer av sexleksaker. I utredningsverksamheten finns motsvarande behov av att

kunna söka på känsliga personuppgifter vid brott med okänd gärningsman.

Tullverket har dock inte behov av att kunna ta fram personurval grundade på alla kategorier av personuppgifter. Det kan aldrig finnas behov av att göra sammanställningar grundade på ras, eftersom det inte finns någon vetenskaplig grund för att dela in människor i skilda raser (se SOU 2017:29 s. 267). Det finns inte heller behov av att kunna göra sammanställningar grundade på medlemskap i fackförening eller på genetiska uppgifter. Av avsnitt 14.7.3 framgår att utredningen inte anser att behandling av biometriska uppgifter i ansiktsgenkänningsprogram är att anse som sökning. Det finns därför inte heller något behov av undantag för sökning när det gäller biometriska uppgifter.

Undantaget bör därför utformas så att sökning möjliggörs när det gäller uppgifter som kan avslöja etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse och uppgifter om hälsa, sexualliv eller sexuell läggning. Det innebär att möjligheterna att använda känsliga personuppgifter vid sökning i uppgifter som inte har gjorts gemensamt tillgängliga begränsas i förhållande till vad som gäller i dag. Eftersom Tullverket inte har behov av ett generellt undantag innebär undantaget ingen försämring.

Hur förhåller sig sökmöjligheterna till sekretessbestämmelsen?

I avsnitt 7.3.3 redogörs för hur bestämmelserna om sökning på känsliga personuppgifter förhåller sig till bestämmelser om sekretess. Som framgår där kommer utredningens tidigare förslag om att absolut sekretess ska gälla för sökningar som utförs i strid med det generella sökförbudet i 2 kap. 14 § brottdatalagen inte att gälla för sökningar som görs med stöd av de nu föreslagna undantagen. Utlämnande av känsliga personuppgifter i en sådan sammanställning får i stället prövas mot andra bestämmelser om sekretess.

8.4 Personuppgifter från transportföretag

8.4.1 Reglerna om personuppgiftsbehandling samlas

Utredningens förslag: Bestämmelserna om hur personuppgifter som transportföretag tillhandahåller Tullverket enligt bestämmelser i inregränslagen och tullagen får behandlas ska samlas i Tullverkets brottsdatalag.

Skälen för utredningens förslag

Transportföretagens uppgiftsskyldighet

Enligt 15 § lagen om Tullverkets befogenheter vid Sveriges gräns mot ett annat land inom Europeiska unionen (inregränslagen) och 4 kap. 6 och 7 §§ tullagen är transportföretag skyldiga att på begäran skyndsamt lämna vissa personuppgifter till Tullverket. Det rör sig bl.a. om resenärers namn, medresenärers namn och transportmedel. Av bestämmelserna framgår att Tullverket endast får begära sådana uppgifter om de kan antas ha betydelse för Tullverkets brottsbekämpande verksamhet.

Personuppgifterna får tillhandahållas genom terminalåtkomst till transportföretagens bokningssystem, där Tullverket endast får läsa uppgifterna men inte bearbeta eller lagra dem. Terminalåtkomst tillåts enligt 16 § inregränslagen och 4 kap. 8 § tullagen bara i den omfattning och under den tid som behövs för att kontrollera aktuella transporter. Uppgifterna kan även lämnas på annat sätt, om transportföretaget anser att det är bättre. De lämnas ofta elektroniskt, men det förekommer även att de tillhandahålls på papper. Utredningen utgår från att personuppgifterna, oavsett på vilket sätt de tillhandahålls, normalt är strukturerade på ett sådant sätt att tullbrottsdatalagen är tillämplig på behandlingen.

Uppgifter om enskilda personer som lämnats på annat sätt än genom terminalåtkomst ska enligt 16 § inregränslagen och 4 kap. 8 § tullagen omedelbart förstöras, om de visar sig sakna betydelse för utredning av eller lagföring för brott. Syftet med bestämmelserna är att hindra att uppgifterna sprids, eftersom det till allra största delen är fråga om information om enskilda personer som inte är misstänkta för brott eller har samband med brottslig verk-

samhet. I inregränslagen och tullagen regleras således inte bara transportföretagens uppgiftsskyldighet utan även på vilket sätt och hur länge personuppgifterna får behandlas.

Uppgifter från transportföretag behandlas och analyseras i Tullverkets underrättelseverksamhet av ett fåtal särskilt utpekade tjänstemän. Eftersom Tullverkets möjlighet att utföra fysiska kontroller i princip är knuten till gränspassage är intresset av bokningsuppgifter bara kortvarigt. När en transport har anlänt har myndigheten normalt inte längre något behov av samtliga uppgifter. Bestämmelserna om Tullverkets tillgång till uppgifter är utformade med särskild hänsyn till det (se prop. 1995/96:166 s. 83 f.).

Bestämmelserna om transportföretagens skyldighet tillkom i samband med Sveriges anslutning till EU, som en kompensatorisk åtgärd för att minska risken för negativa konsekvenser av den fria rörligheten för personer och varor. För att skapa bättre förutsättningar för kontroller vid den inre gränsen i kampen mot narkotikabrottslighet och annan internationell brottslighet gavs Tullverket möjlighet att i den brottsbekämpande verksamheten inhämta vissa uppgifter om varor, passagerare och fordon. Avsikten var att uppgifterna från transportföretagen skulle användas för att med ökad träffsäkerhet rikta kontroller mot varusändningar och mot personer som skulle kunna misstänkas för brottslighet inom Tullverkets verksamhetsområde (se prop. 1995/96:166 s. 72 f.). Metoden att med hjälp av uppgifter från transportföretag göra profilsökningar och kunna identifiera riskbeteenden redan innan en transport har nått Sverige ansågs dock vara lika viktig vid den yttre som den inre gränsen. Uppgiftsskyldigheten reglerades därför i både inregränslagen och tullagen (se prop. 1995/96:166 s. 80 f.).

Regleringen i tullbrottsdatalagen

Enligt 2 kap. 8 § tullbrottsdatalagen får personuppgifter, som har lämnats av transportföretag enligt nyssnämnda bestämmelser i inregränslagen och tullagen, behandlas av Tullverket om det är tillåtet enligt dessa lagar, men enbart i den utsträckning det behövs för planering av kontrollverksamheten och urval av kontrollobjekt. Om det behövs i ett enskilt fall får sådana personuppgifter behandlas även för något annat ändamål enligt 2 kap. 5 § tullbrottsdatala-

gen och göras gemensamt tillgängliga. Enligt 2 kap. 9 § är det endast tillåtet att söka på namn, personnummer eller annan identitetsbeteckning om uppgifterna avser en person som är eller har varit misstänkt för brott, är misstänkt för att ha utövat eller komma att utöva viss brottslig verksamhet eller är föremål för övervakning enligt lagen.

Kan den nuvarande regleringen behållas?

EU:s dataskyddsreform innebär att det behövs en tydligare gränsdragning mellan sådan behandling av personuppgifter som regleras i brottsdatalagen respektive dataskyddsförordningen med kompletterande lagstiftning, eftersom antingen det ena eller det andra regelverket gäller (se SOU 2017:29 s. 159 f.). Regleringen i 2 kap. 8 § tullbrottsdatalagen aktualiserar frågor dels om regleringen hör hemma där, dels om regleringen av vilken personuppgiftsbehandling som är tillåten bör delas upp på det sätt som görs i dag.

I delbetänkandet framhåller utredningen att kontrollverksamhet normalt ligger utanför brottsdatalagens tillämpningsområde. Utgångspunkten är att verksamheten övergår till att vara brottsbekämpande först när det i kontrollverksamheten finns anledning att anta att ett visst konkret brott begåtts, eller viss brottslig verksamhet utövas, (se SOU 2017:29 s. 198 f.). Det kan konstateras att de syften som i dag anges i 2 kap. 8 § tullbrottsdatalagen – planering av kontrollverksamheten och urval av kontrollobjekt – åtminstone vid första påseendet inte verkar vara förenliga med brottsdatalagens tillämpningsområde. Samtidigt tillåter regleringen i inregränslagen och tullagen bara att uppgifterna hämtas in i den brottsbekämpande verksamheten.

Tullverkets underrättelseverksamhet går i stor utsträckning ut på att förebygga, förhindra och upptäcka smuggling av framför allt narkotika och andra farliga föremål genom att studera resmönster, betalningssätt, vilka som reser i sällskap och liknande. Det framgår också tydligt av förarbetena att syftet med att ge Tullverket tillgång till personuppgifter i transportföretagens bokningssystem var att förhindra olaglig införsel av varor till Sverige och att därigenom förhindra narkotikabrottslighet och annan allvarlig brottslighet (se prop. 1995/96:166 s. 72 f.). I inregränslagen och tullagen föreskrivs

som nyss nämnts att uppgifter från transportföretag enbart får inhämtas om de kan ha betydelse för Tullverkets brottsbekämpande verksamhet. I förarbetena till tullbrottsdatalagen understryks att det endast är kontroller som utförs i brottsbekämpande syfte som åsyftas i 2 kap. 8 § (se prop. 2016/17:91 s. 108). Tillgången till uppgifter från transportföretag är av stor betydelse för Tullverkets möjligheter att förebygga och förhindra brottslig verksamhet och att upptäcka brott i samband med gränspassage. Utredningen anser därför att regleringen bör finnas i Tullverkets brottsdatalag, men att den behöver renodlas och anpassas till de nya förutsättningar som gäller för behandling av personuppgifter till följd av EU:s dataskyddsreform.

Ett samlat regelverk

Som framgått innehåller inregränslagen och tullagen inte bara bestämmelser om transportföretagens uppgiftsskyldighet utan även regler som dels begränsar tillgången till personuppgifter i transportföretagens bokningssystem, dels anger hur uppgifterna får behandlas av Tullverket. Där finns bestämmelser om vilken sökning som är tillåten och hur länge uppgifter som härrör från transportföretag får behandlas i den brottsbekämpande verksamheten. Samtidigt finns stödet för att behandla personuppgifterna automatiserat i tullbrottsdatalagen.

Bestämmelserna om transportföretags uppgiftsskyldighet infördes som nyss nämnts i samband med att Sverige blev medlem i EU. I förarbetena till Tullverkets registerförfattningar har frågan om de delar av bestämmelserna som avser Tullverkets behandling av personuppgifter borde samlas i en författning inte tagits upp.

Av de skäl som anges i avsnitt 7.4.1 bör bestämmelserna om hur personuppgifter från transportföretag får behandlas och hur länge de får behandlas flyttas från inregränslagen och tullagen till Tullverkets brottsdatalag. Med en sådan lösning blir regleringen mer överskådlig och lättillämpad. Transportföretagens uppgiftsskyldighet bör däremot alltså regleras i inregränslagen och tullagen.

8.4.2 En i huvudsak oförändrad reglering

Utredningens förslag: Tullverket ska få behandla personuppgifter som transportföretag på Tullverkets begäran tillhandahåller enligt bestämmelser i inregränslagen och tullagen för att planera kontroller och välja ut kontrollobjekt i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott. Sådana personuppgifter ska endast i enskilda fall få behandlas för nya ändamål.

Skälen för utredningens förslag

Syftena med regleringen

Av förarbetena till tullbrottsdatalagen framgår att den enda remissinstans som yttrade sig över 2 kap. 8 § ifrågasatte om användning för planering av kontrollverksamheten och urval av kontrollobjekt stämde överens med lagens övergripande syften. Regeringen bemötte det bl.a. genom att peka på att lagens tillämpningsområde är Tullverkets brottsbekämpande verksamhet (se prop. 2016/17:91 s. 108). Utredningen anser att det med den nya regleringen i brottsdatalagen är nödvändigt att klargöra att syftet med bestämmelsen inte är att planera Tullverkets allmänna kontrollverksamhet.

Vid inre gräns är det inte tillåtet att göra slumpmässiga kontroller, t.ex. att ta ut var tionde eller tjugonde person som passerar gränsen för kontroll. Däremot är det tillåtet att göra selektiva kontroller. Med det avses kontroller som bygger på att den som passerar gränsen uppfyller särskilda kriterier som pekar på förhöjd risk för att personen begår brott genom att t.ex. medföra otillåtna varor. Arbetet med att ta fram sådana kriterier som kan motivera att en viss person tas ut för kontroll och att identifiera riskprofiler görs av Tullverkets underrättelseverksamhet. Genom att med hjälp av transportföretagens uppgifter kartlägga bl.a. resmönster, betalningssätt, ålder och vilka som reser i sällskap ökar möjligheterna att kunna avslöja brott och att upptäcka nya smugglingsmetoder (se avsnitt 8.4.1).

Utredningen anser att det inte råder någon tvekan om att den kontrollverksamhet som avses i 2 kap. 8 § tullbrottsdatalagen är

sådan som avser att förebygga, förhindra eller upptäcka brottslig verksamhet.

Bestämmelserna ska i huvudsak vara desamma

Enligt utredningens mening bör de bestämmelser som flyttas över från inregränslagen och tullagen till Tullverkets brottsdatalag i huvudsak ha samma innehåll som i dag. De behöver dock anpassas till den lagens tillämpningsområde. Att personuppgifterna endast får behandlas för att planera kontroller och välja ut kontrollobjekt i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet bör framgå av bestämmelsen.

I avsnitt 7.4.1 föreslår utredningen att polisen ska få behandla uppgifter från transportföretag inte bara i syfte att förebygga, förhindra och upptäcka brottslig verksamhet utan även för att utreda eller lagföra brott.

Även om Tullverket främst har intresse av att behandla uppgifter från transportföretag för att effektivt kunna förebygga brott och för att bygga upp kunskap om smugglingsvägar och smugglingsmetoder, har myndigheten i likhet med polisen även behov av sådana uppgifter i sin utredningsverksamhet. Vid s.k. kontrollerade leveranser av narkotika kan bokningsuppgifter vara av stor praktisk betydelse. Vid utredning av smugglingsbrott är det viktigt att kunna kontrollera uppgifter om om resväg, resällskap och liknande. Tullverket bör därför kunna dra nytta av uppgifter från transportföretagen både i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet och i syfte att utreda eller lagföra brott.

I 2 kap. 8 § tullbrottsdatalagen anges att sådana uppgifter bara får behandlas i den utsträckning det är tillåtet enligt inregränslagen respektive tullagen. Någon motsvarande bestämmelse behövs inte i Tullverkets brottsdatalag, eftersom det alltid ska finnas en rättslig grund för behandlingen.

På samma sätt som i polisens brottsdatalag bör det förtydligas att bestämmelserna om terminalåtkomst endast hindrar ändring eller bearbetning av uppgifterna i transportbolagens it-system (se avsnitt 7.4.2). Finner Tullverket att personuppgifter i ett enskilt fall föranleder ett underrättelseuppslag eller behövs för en brottsutred-

ning kan de som regel behandlas enligt de generella bestämmelserna i brottsdatalagen och Tullverkets brottsdatalag.

Uppgifter om enskilda personer som lämnats på annat sätt än genom terminalåtkomst bör omedelbart förstöras, om de saknar betydelse för brottsbekämpning eller lagföring. Regleringen om förstörande i inregränslagen och tullagen gäller inte bara personuppgifter som behandlas automatiserat utan även annan behandling. Den nya regleringen bör därför täcka all behandling som omfattas av Tullverkets brottsdatalags tillämpningsområde. Kravet på förstörande bör dock inte omfatta de personuppgifter som myndigheten i ett enskilt fall behandlar i syfte att bekämpa eller lagföra brott.

Utredningen återkommer i avsnitt 8.5.2 till frågan om uppgifter från transportföretag får göras gemensamt tillgängliga.

Behandling för nya ändamål

I 2 kap. 8 § tullbrottsdatalagen föreskrivs att personuppgifter från transportföretag också får behandlas för något annat ändamål som anges i 2 kap. 5 § om det behövs i ett enskilt fall. Det innebär att sådana uppgifter t.ex. får användas för att utreda brott.

Behandling för nya ändamål inom brottsdatalagens tillämpningsområde regleras i 2 kap. 4 § brottsdatalagen. För att sådan behandling ska vara tillåten krävs det dels att det finns en tillåten rättslig grund för behandling för det nya ändamålet, dels att behandlingen är nödvändig och proportionerlig för det nya ändamålet. Utredningen föreslår i avsnitt 6.4.3 att samma prövning ska göras när personuppgifter behandlas för nya ändamål utanför brottsdatalagens tillämpningsområde.

Riksdagen har nyligen ställt sig bakom att Tullverket i ett enskilt fall får behandla personuppgifter av nu aktuellt slag för något annat ändamål som anges i 2 kap. 5 § tullbrottsdatalagen. Enligt direktivet är det inte möjligt att göra undantag från den prövning som kommer till uttryck i 2 kap. 4 § brottsdatalagen. Det innebär att en sådan prövning alltid krävs när uppgifter från transportföretag i ett enskilt fall ska behandlas för ett nytt ändamål. Även om uppgifter från transportföretag bara får hämtas in och behandlas för ändamål inom lagens tillämpningsområde kan det inte uteslutas

att det därefter uppkommer en situation där frågan om behandling för ändamål utanför tillämpningsområdet aktualiseras, t.ex. genom en begäran om att få del av en allmän handling. Det bör därför vara tillåtet att behandla uppgifterna för ändamål utanför tillämpningsområdet, men prövningen av nödvändighet och proportionalitet måste då göras (se avsnitt 6.4.3).

PNR-utredningens förslag

Som redovisas i avsnitt 7.4.1 har PNR-utredningen lämnat förslag till en ny lag om flygpassageraruppgifter i brottsbekämpningen som gäller för uppgifter som samlas in från flygbolag. Lagen föreslås ha företräde framför inregränslagen, tullagen och tullbrottsdatalagen. Utredningen har inte beaktat PNR-utredningens förslag.

8.5 Gemensamt tillgängliga uppgifter

8.5.1 Sökning i gemensamt tillgängliga uppgifter

Utredningens förslag: Bestämmelsen som begränsar resultatet vid sökning i gemensamt tillgängliga uppgifter med hjälp av namn, personnummer, samordningsnummer eller liknande identitetsbeteckningar ska enbart gälla i automatiserade behandlingssystem.

Begränsningarna ska inte gälla vid sökning i en viss handling eller i ett visst ärende. De ska inte heller gälla vid sökning som görs av särskilt angivna tjänstemän

1. när de utför beredningsuppgifter i underrättelseverksamhet, om arbetet befinner sig i ett inledande skede,
2. i syfte att i underrättelseverksamhet bearbeta och analysera personuppgifter som har gjorts gemensamt tillgängliga enligt vissa bestämmelser och som enbart dessa tjänstemän har tillgång till,
3. i syfte att utreda brott för vilket det är föreskrivet fängelse i fyra år eller däröver, eller

4. i syfte att samordna utredningar om brott som kan vara systematiska och för vilka det är föreskrivet fängelse i två år eller däröver.

Det ska också göras undantag för sökning som en tjänsteman vid någon av Tullverkets ledningscentraler utför på begäran av en tjänsteman som verkställer ett ingripande eller vidtar en åtgärd som rör en enskild.

Skälen för utredningens förslag

Begränsning endast i automatiserade behandlingssystem

Eftersom sökning med hjälp av namn, personnummer och samordningsnummer är ett viktigt inslag i Tullverkets verksamhet och sådana identitetsbeteckningar är av stor betydelse för att säkerställa identiteten och undvika personförväxlingar, ansågs det nödvändigt att medge sådan sökning i gemensamt tillgängliga uppgifter (jfr avsnitt 7.5.2). I 3 kap. 6 § tullbrottsdatalagen regleras därför vilka uppgifter som får tas fram vid sökning på namn, personnummer, samordningsnummer eller andra liknande identitetsbeteckningar. I 3 kap. 7 § görs vissa undantag från bestämmelserna i 3 kap. 6 §. I förarbetena diskuteras ingående vilka typer av sökning som bör vara tillåtna och vilka begränsningar som bör gälla (se prop. 2016/17:91 s. 138 f.). Paragraferna är utformade efter mönster av polisdatalagen.

Tullbrottsdatalagen har nyligen trätt i kraft och de aktuella bestämmelserna behöver inte tillämpas förrän år 2019. Liknande övergångsbestämmelser gäller även för polisen, som därför ännu inte heller har erfarenhet av att tillämpa bestämmelserna. Av de skäl som anges i avsnitt 7.5.2 bör det tydliggöras att regleringen enbart gäller vid sökning i automatiserade behandlingssystem. Där görs också vissa uttalanden om hur regleringen bör tolkas som är giltiga även för Tullverket.

Behövs det fler eller andra undantag från begränsningsregeln?

Undantagen i 3 kap. 7 § tullbrottsdatalagen från begränsningarna av vilka uppgifter som får tas fram vid sökning är utformade efter mönster av polisdatalagen. Av de skäl som anges i avsnitt 7.5.2 bör undantagen ändras även i Tullverkets brottsdatalag. Det gäller undantagen för att bearbeta och analysera information i underrättelseverksamhet. Vidare bör även Tullverket kunna göra sökningar i syfte att samordna brottsutredningar som avser brott som kan vara systematiska och för vilka det är föreskrivet fängelse i två år eller däröver. Regleringen bör utformas på samma sätt som för Polismyndigheten.

De tulltjänstemän som arbetar i yttre tjänst har ofta behov av att kunna få hjälp av personal vid Tullverkets ledningscentraler, t.ex. vakthavande befäl eller rikssambandscentralen, med sökning i syfte att klarlägga t.ex. en gripens persons identitet. Vid sökningar av det slaget kan det vara nödvändigt att få fram andra typer av information, samtidigt som den ingripande tulltjänstemannen inte alltid har tillgång till nödvändiga sökmöjligheter i sin utrustning. Det bör därför även göras undantag från begränsningsregeln för sådana sökningar som görs i Tullverkets ledningscentraler på begäran av en tulltjänsteman i yttre tjänst.

8.5.2 Uppgifter från transportföretag får göras gemensamt tillgängliga

Utredningens förslag: Bestämmelsen om i vilka fall personuppgifter från transportföretag får göras gemensamt tillgängliga ska arbetas in i regleringen om gemensamt tillgängliga uppgifter.

Skälen för utredningens förslag: I avsnitt 8.4.2 föreslår utredningen att regleringen av Tullverkets behandling av personuppgifter från transportföretag i huvudsak ska vara densamma som i dag. Utgångspunkten är att uppgifter från transportföretagen till allra största delen är information om personer som inte är intressanta för brottsbekämpningen och att sådana personuppgifter därför ska ges så liten spridning som möjligt. När bestämmelserna i inregränslagen och tullagen infördes konstaterade regeringen att uppgifter-

nas karaktär krävde begränsningar av hur de fick användas (se prop. 1995/96:166 s. 83 f.). Uppgifterna får därför som utgångspunkt inte göras gemensamt tillgängliga.

Enligt 2 kap. 8 § andra stycket tullbrottsdatalagen får personuppgifter från transportföretag bara göras gemensamt tillgängliga i enskilda fall. Av förarbetena framgår att det skulle strida mot intentionerna bakom bestämmelserna att generellt tillåta att sådana uppgifter görs gemensamt tillgängliga. Om personuppgifterna, t.ex. efter en kontroll, behövs för en brottsutredning eller ha samband med misstänkt brottslig verksamhet bör de dock få behandlas inom ramen för den utredningen eller det underrättelseärendet och göras gemensamt tillgängliga (se prop. 2016/17:91 s. 107).

I 3 kap. 2 § tullbrottsdatalagen anges under vilka förutsättningar som personuppgifter får göras gemensamt tillgängliga. Genom särregleringen i 2 kap. 8 § andra stycket av i vilka fall uppgifter från transportföretag får göras gemensamt tillgängliga skapas det enligt utredningens mening en otydlighet som kan leda till motsatsslut när det gäller andra slag av personuppgifter. Utredningen föreslår därför att den bestämmelsen utan någon ändring i sak flyttas till 3 kap. 2 §. På samma sätt som i dag bör alltså sådana uppgifter få göras gemensamt tillgängliga om det behövs i ett enskilt fall.

8.6 Längsta tid för behandling

Utredningens förslag: Personuppgifter som kan antas ha samband med viss brottslig verksamhet ska, om de behandlas i ett ärende, inte få behandlas längre än ett år efter det att ärendet avslutades.

Skälen för utredningens förslag: I 4 kap. 9 § andra stycket tullbrottsdatalagen regleras hur länge personuppgifter som behandlas i viss underrättelseverksamhet får behandlas.

I underrättelseverksamhet behandlas personuppgifter som huvudregel inte i ärenden och regleringen av när behandlingen ska upphöra utgår därför från när registreringen avseende personen gjordes. Som anges i avsnitt 7.6 behandlas personuppgifter i underrättelseverksamheten ibland i ärenden, exempelvis i samarbetet mot grov organiserad brottslighet eller i samband med en särskild hän-

delse. När personuppgifter i underrättelseverksamhet behandlas i ärenden bör uppgifterna, på samma sätt som vid behandling av personuppgifter i andra ärenden, inte få behandlas längre än ett år efter det att ärendet avslutades. Hur bestämmelsen bör formuleras behandlas i avsnitt 5.5.2 och 7.5.1.

8.7 Övergångsbestämmelser till tullbrottsdatalagen

Utredningens bedömning: Övergångsbestämmelserna till tullbrottsdatalagen behöver inte ändras.

Skälen för utredningens bedömning: Det finns övergångsbestämmelser till tullbrottsdatalagen. I punkten 3 b föreskrivs att bestämmelserna i 4 kap. 6 och 7 §§ tullbrottsdatalagen om hur länge vissa personuppgifter får behandlas inte behöver tillämpas förrän den 1 januari 2019. Den bestämmelsen står inte i strid med brottsdatalagens reglering om hur länge personuppgifter får behandlas och kan därmed behållas. Det bör dock framhållas att Tullverket måste iaktta skyldigheten i 2 kap. 18 § brottsdatalagen att återkommande se över behovet av att behandla uppgifterna fram till dess att bestämmelserna börjar tillämpas.

Övergångsbestämmelserna i punkterna 3 a och c som avser vissa bestämmelser om sökning kan också behållas, eftersom direktivet inte ställer några krav på sök begränsningar.

Utredningens förslag till anpassningar av tullbrottsdatalagen innebär att de bestämmelser som övergångsbestämmelserna tar sikte på får ny placering eller numrering. Övergångsbestämmelser behöver i sådana fall inte ändras utan ska fortsätta att tillämpas på samma sätt som tidigare.

I 18 kap. behandlas behovet av nya övergångsbestämmelser.

9 Kustbevakningsdatalagen

9.1 Kustbevakningsdatalagen behöver anpassas

9.1.1 Nuvarande reglering

Kustbevakningsdatalagen gäller enligt 1 kap. 2 § vid behandling av personuppgifter i Kustbevakningens brottsbekämpande verksamhet och i annan operativ verksamhet, t.ex. sjöövervakning och räddningstjänst. Bestämmelserna i 3 och 4 kap. gäller vid behandling av personuppgifter i den brottsbekämpande verksamheten, medan bestämmelserna i 5 kap. gäller vid personuppgiftsbehandling i annan operativ verksamhet.

Som anges i avsnitt 4.2 måste registerförfattningarna ändras i vissa avseenden med anledning av dataskyddsdirektivet och anpassas till brottsdatalagen. Många bestämmelser behöver överhuvudtaget inte anpassas eller endast ändras redaktionellt. Utredningen behandlar de anpassningar och ändringar som är gemensamma för registerförfattningarna i kapitel 5 och 6. De ytterligare ändringar som krävs i kustbevakningsdatalagen behandlas i detta kapitel.

En annan utredare har fått i uppdrag att anpassa den del av kustbevakningsdatalagen som ligger utanför brottsdatalagens tillämpningsområde till dataskyddsförordningen (Ju 2016:H).

9.1.2 Kustbevakningsdatalagen delas upp

Utredningens förslag: Kustbevakningsdatalagen med tillhörande förordning ska bara innehålla bestämmelser om personuppgiftsbehandling inom brottsdatalagens tillämpningsområde och ges nya namn. De ska benämnas Kustbevakningens brottsdatalag och Kustbevakningens brottsdataförordning.

Skälen för utredningens förslag

Den nuvarande regleringen renodlas

Vid kustbevakningsdatalagens tillkomst övervägde regeringen om Kustbevakningens personuppgiftsbehandling skulle regleras i två lagar, mot bakgrund av att myndigheten har arbetsuppgifter inom flera olika verksamhetsområden. Eftersom Kustbevakningens operativa verksamhet är integrerad och inte organisatoriskt indelad i självständiga verksamhetsgrenar ansåg regeringen att övervägande skäl talade för att myndighetens personuppgiftsbehandling skulle regleras i en lag (se prop. 2011/12:45 s. 63). Med hänsyn till hur den nya dataskyddsregleringen är utformad finns det emellertid skäl att på nytt överväga frågan.

Kustbevakningsdatalagen reglerar i dag personuppgiftsbehandling inom både brottsdatalagens och dataskyddsförordningens tillämpningsområden. Om man skulle behålla en samlad reglering för Kustbevakningens personuppgiftsbehandling skulle den därför behöva dels gälla utöver brottsdatalagen, dels komplettera dataskyddsförordningen.

Den nya dataskyddsregleringen gör det nödvändigt att dela upp regleringen av Kustbevakningens personuppgiftsbehandling på ett annat sätt än i dag. Det skulle i och för sig vara möjligt att göra alla nödvändiga ändringar i den befintliga lagen. Ett annat alternativ är att dela upp regleringen i två separata regelverk – ett för brottsdatalagens tillämpningsområde och ett för dataskyddsförordningens. Att ha separata registerförfattningar för en myndighets olika verksamheter är inget nytt. Skatteverket och Tullverket har i dag olika regleringar för personuppgiftsbehandlingen beroende på i vilken verksamhet uppgifterna behandlas, där regleringen för den brottsbekämpande verksamheten finns i en särskild lag. Lösningen med två separata regleringar är enligt utredningens mening tydlig och lätt att tillämpa. Att Kustbevakningen inte på samma sätt som de myndigheterna har en organisatorisk uppdelning i olika verksamhetsgrenar hindrar enligt utredningens mening inte en sådan lösning, eftersom syftet med personuppgiftsbehandlingen är avgörande för vilket regelverk som ska tillämpas.

Trots de skäl som anges i förarbetena till kustbevakningsdatalagen bör därför Kustbevakningens personuppgiftsbehandling fortsättningsvis regleras i två olika registerförfattningar. Den del av

Kustbevakningens personuppgiftsbehandling som ligger inom brottsdatalagens tillämpningsområde bör regleras i den befintliga lagen med hänsyn till att den i dag till största delen rör brottsbekämpande verksamhet. Utredningen har samrått om den lösningen med den utredare som har i uppdrag att anpassa Kustbevakningens registerförfattningar till dataskyddsförordningen.

Mot den bakgrunden bör de bestämmelser i kustbevakningsdatalagen som tar sikte på frågor som ligger utanför brottsdatalagens tillämpningsområde upphävas. Även 2 kap. 10 §, som ställer krav på att det ska framgå i vilken operativ verksamhet personuppgifter behandlas, bör upphävas.

Kustbevakningsdatalagen ges ett nytt namn

Eftersom endast den del av Kustbevakningens personuppgiftsbehandling som ligger inom brottsdatalagens tillämpningsområde ska regleras i kustbevakningsdatalagen, bör det övervägas om lagens namn ska bytas. Av de skäl som anges i avsnitt 7.1.2 finns det anledning att byta namn på registerförfattningarna inom brottsdatalagens tillämpningsområde. Namnet bör knyta an till hur brottsdatalagen benämns. Det bör vara kort och ange vem författningen gäller för och vad den handlar om. Utredningen föreslår därför att lagen ska benämnas Kustbevakningens brottsdatalag. Kustbevakningsdataförordningen bör i konsekvens med det benämnas Kustbevakningens brottsdataförordning. Som en konsekvens av att lagens namn ändras måste alla hänvisningar till den ändras.

9.2 Tillämpningsområdet

Utredningens förslag: Lagen ska gälla utöver brottsdatalagen när Kustbevakningen i egenskap av behörig myndighet behandlar personuppgifter i syfte att bekämpa eller lagföra brott eller upprätthålla allmän ordning och säkerhet.

Skälen för utredningens förslag

Den nuvarande regleringen behöver anpassas

I avsnitt 4.4.1 tar utredningen ställning till att registerförfattningarna även i fortsättningen ska innehålla bestämmelser om tillämpningsområdet och anger övergripande vad som bör gälla för den regleringen. Vidare föreslår utredningen i avsnitt 5.2 att registerförfattningarna ska gälla utöver brottsdatalagen.

Kustbevakningsdatalagen gäller enligt 1 kap. 2 § vid behandling av personuppgifter i Kustbevakningens operativa verksamhet som rör bl.a. brottsbekämpning, sjöövervakning och räddningstjänst. Tillämpningsområdet måste anpassas till brottsdatalagens tillämpningsområde så att det dels utgår från syftet med behandlingen, dels bara omfattar den personuppgiftsbehandling som Kustbevakningen utför inom brottsdatalagens tillämpningsområde. Det bör också framgå att lagen endast gäller när Kustbevakningen agerar i egenskap av behörig myndighet, eftersom det är en viktig avgränsning för tillämpningsområdet (se SOU 2017:29 s. 159 f.).

Närmare om tillämpningsområdet

Kustbevakningsdatalagen gäller för behandling av personuppgifter som rör bl.a. brottsbekämpning. Som framgår av avsnitt 5.4.6 anses lagföring av brott i dag ingå i begreppet brottsbekämpning, medan det i brottsdatalagen görs skillnad mellan brottsbekämpning och lagföring. För att tillämpningsområdet ska täcka det som i dag omfattas av regleringen bör det därför inkludera personuppgiftsbehandling i syfte att bekämpa eller lagföra brott.

Brottsdatalagens tillämpningsområde omfattar även personuppgiftsbehandling i syfte att upprätthålla allmän ordning och säkerhet. Kustbevakningen har vissa ordningshållande uppgifter.

En av Kustbevakningens arbetsuppgifter är att genom sjöövervakning förebygga och ingripa mot störningar av ordningen i sjötrafiken (3 § förordningen [2007:853] med instruktion för Kustbevakningen). I 5 kap. 1 § första stycket 1 kustbevakningsdatalagen regleras behandling av personuppgifter för ändamålet att övervaka den allmänna ordningen och säkerheten till sjöss. Sådan sjöövervakning syftar enligt förarbetena till att öka respekten för lagar och

föreskrifter och till att öka säkerheten till sjöss. Verksamheten omfattar allmän övervakningsverksamhet i form av patrullering och sjösäkerhetsövervakning. Till denna verksamhet räknas inte aktiviteter som föranleds av misstanke om brott eller brottslig verksamhet (se prop. 2011/12:45 s. 157).

Inom ramen för sjöövervakningen har Kustbevakningens tjänstemän rätt att ingripa vid ordningsstörningar i trafiken till sjöss eller när det behövs för att avvärja brott mot föreskrifter om trafikregler och säkerhetsanordningar för sjötrafiken, åtgärder mot vattenföroreningar från fartyg och dumpning av avfall i vatten. Vid ett sådant ingripande har en kustbevakningstjänsteman enligt 3 § lagen om Kustbevakningens medverkan vid polisiär övervakning samma befogenhet som en polisman har enligt 13 § polislagen att avvisa, avlägsna eller omhänderta den som genom sitt uppträdande stör ordningen eller utgör omedelbar fara för den. Det gäller dock bara vid ordningsstörningar till sjöss som utgör en omedelbar fara och i samband med att Kustbevakningen ingriper mot vissa brott enligt lagen om Kustbevakningens medverkan vid polisiär övervakning. Kustbevakningen har också ordningshållande uppgifter enligt dels lagen (2006:1209) om hamnskydd, dels lagen (2004:487) om sjöfartsskydd.

För att Kustbevakningens brottsdatalag ska täcka all Kustbevakningens behandling av personuppgifter som omfattas av brottsdatalagens tillämpningsområde bör myndighetens behandling av personuppgifter vid upprätthållande av allmän ordning och säkerhet omfattas av tillämpningsområdet.

Gränsdragningen för tillämpningsområdet

Utredningen konstaterar i delbetänkandet att det är personuppgiftsbehandling i syfte att upprätthålla allmän ordning och säkerhet som omfattas av brottsdatalagens tillämpningsområde. Utgångspunkten är att det krävs fysisk närvaro på den plats där oordning förekommer eller riskerar att uppstå för att det ska vara fråga om upprätthållande av allmän ordning och säkerhet (se SOU 2017:29 s. 164 f. och 167).

När en kustbevakningstjänsteman ingriper eller är beredd att ingripa vid en konkret ordningsstörning, eller en potentiell sådan

störning vid en specifik händelse, är det fråga om upprätthållande av allmän ordning och säkerhet. Personuppgiftsbehandling vid sådan verksamhet bör följaktligen omfattas av tillämpningsområdet för Kustbevakningens brottsdatalag. Detsamma bör gälla vid ingripanden och andra åtgärder för att avvärja konkreta brott.

Den verksamhet som består av allmän övervakning i trygghets-skapande syfte och att genom närvaro se till att allmän ordning och säkerhet inte störs, ligger däremot utanför tillämpningsområdet. Sådan övervakning kan utföras t.ex. genom rutinmässig patrullering till sjöss eller flygövervakning eller övervakning med hjälp av kameror eller annan digital utrustning i en ledningscentral. Denna typ av övervakning görs utan att den är inriktad mot en konkret störning eller konkret risk för störning. Allmän övervakning av sådant slag kan emellertid övergå till att ha ett ordningshållande syfte och därmed omfattas av tillämpningsområdet. Så är fallet om ledningscentralen tar radiokontakt med ett övervakat fartyg för att ge anvisningar om t.ex. vilken kurs fartyget ska hålla för att undvika ett avlyst vattenområde. I dessa fall upprätthålls allmän ordning och säkerhet utan någon fysisk närvaro på platsen där oordning förekommer eller riskerar att uppstå.

Även vid rutinmässig patrullering till sjöss kan det upptäckas ordningsstörningar som kräver ingripande. Det är oftast först vid ingripanden som det blir fråga om att behandla personuppgifter. Gränsdragningen avseende vilket regelverk som gäller i enskilda fall blir ytterst en fråga för tillämpningen.

9.3 Grundläggande bestämmelser om behandling

9.3.1 Tillåtna rättsliga grunder och behandling för nya ändamål

Utredningens förslag: Kustbevakningen ska få behandla personuppgifter om det är nödvändigt för att utföra en arbetsuppgift i syfte att

1. förebygga, förhindra eller upptäcka brottslig verksamhet,
2. utreda eller lagföra brott,
3. upprätthålla allmän ordning och säkerhet, eller

4. fullgöra förpliktelser som följer av internationella åtaganden.

Arbetsuppgiften ska framgå av en bindande unionsrättsakt eller av en lag, en förordning eller ett särskilt beslut i vilket regeringen uppdragit åt myndigheten att ansvara för en sådan uppgift.

Det ska framgå genom en hänvisning att personuppgifter som behandlas med stöd av lagen ska få behandlas för nya ändamål enligt de förutsättningar som anges i brottsdatalagen.

Skälen för utredningens förslag

En bestämmelse som ersätter brottsdatalagens bestämmelse om tillåtna rättsliga grunder för behandling

Som anges i avsnitt 6.3.1 bör registerförfattningarna innehålla bestämmelser om tillåtna rättsliga grunder för behandling av personuppgifter. Regleringen i 3 kap. 2 § kustbevakningsdatalagen bör således behållas, men det ska framgå att det inte är en ändamålsbestämmelse i egentlig mening. Bestämmelsen är på samma sätt som 2 kap. 1 § brottsdatalagen en del av den rättsliga grunden och ger Kustbevakningen rättsligt stöd för att behandla personuppgifter automatiserat för att utföra sina arbetsuppgifter (se avsnitt 6.1.2).

Kustbevakningen får i dag behandla personuppgifter i den brottsbekämpande verksamheten om det behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller beivra brott eller fullgöra de förpliktelser som följer av internationella åtaganden. Kustbevakningen bör givetvis även i fortsättningen få behandla personuppgifter om det är nödvändigt för att fullgöra sådana arbetsuppgifter, men regleringen bör anpassas till brottsdatalagens terminologi.

I avsnitt 9.2 föreslår utredningen att tillämpningsområdet för Kustbevakningens brottsdatalag ska omfatta personuppgiftsbehandling vid upprätthållande av allmän ordning och säkerhet. Det bör därför också vara en tillåten rättslig grund för myndighetens personuppgiftsbehandling.

Kustbevakningens brottsdatalag föreslås gälla utöver brottsdatalagen. För att det inte ska råda någon osäkerhet om hur bestämmelsen i 2 kap. 1 § brottsdatalagen förhåller sig till bestämmelsen om

tillåtna rättsliga grunder i registerförfattningen bör den senare ersätta bestämmelsen i brottsdatalagen. Det bör därför föreskrivas i Kustbevakningens brottsdatalag, på samma sätt som i brottsdatalagen, att den arbetsuppgift som Kustbevakningen ska utföra ska framgå av en bindande unionsrättsakt eller en lag, en förordning eller ett särskilt beslut i vilket regeringen uppdragit åt myndigheten att ansvara för en sådan uppgift. Vad det innebär utvecklas i delbetänkandet (se SOU 2017:29 s. 238 f.).

Behandling för nya ändamål

I dag regleras behandling för nya ändamål till viss del i den sekundära ändamålsbestämmelsen i 3 kap. 3 § kustbevakningsdatalagen. Utredningen anser som framgår av avsnitt 6.3.2 och 6.4.2 att de sekundära ändamålsbestämmelserna bör upphävas. Förutsättningarna för behandling för nya ändamål bör i stället regleras i brottsdatalagen. Innan personuppgifter får behandlas för nya ändamål inom brottsdatalagens tillämpningsområde ska det enligt 2 kap. 4 § brottsdatalagen säkerställas att behandlingen är nödvändig och proportionerlig för det nya ändamålet. Utredningen föreslår att samma prövning ska göras när de brottsbekämpande myndigheterna behandlar personuppgifter för nya ändamål utanför tillämpningsområdet. I lagen bör det införas en bestämmelse som tydliggör att förutsättningarna för att behandla personuppgifter, som behandlas med stöd av den lagen, för nya ändamål regleras i brottsdatalagen.

9.3.2 Behandling av biometriska och genetiska uppgifter

Utredningens bedömning: Kustbevakningen bör inte få behandla biometriska och genetiska uppgifter.

Skälen för utredningens bedömning: I avsnitt 7.3.2 redovisas vad som avses med biometriska och genetiska uppgifter och vilken betydelse sådana uppgifter har vid brottsbekämpning.

Enligt 2 kap. 12 och 13 §§ brottsdatalagen utgör biometriska uppgifter som används för att identifiera en person och genetiska uppgifter känsliga personuppgifter. Sådana uppgifter får endast be-

handlas om det är särskilt föreskrivet och det är absolut nödvändigt för ändamålet med behandlingen.

Det är svårt att se att Kustbevakningen har något behov av att behandla biometriska och genetiska uppgifter och utredningen anser därför att det inte bör finnas någon bestämmelse som medger sådan behandling i Kustbevakningens brottsdatalag.

9.3.3 Sökning på känsliga personuppgifter

Utredningens förslag: Sökförbudet i brottsdatalagen ska inte hindra att brottsrubriceringar, uppgifter om tillvägagångssätt vid brott eller uppgifter som beskriver en persons utseende används vid sökning.

Det ska inte heller hindra sökning i syfte att få fram ett personurval grundat på etniskt ursprung, religiös eller filosofisk övertygelse eller uppgifter som rör hälsa, om sökningen görs i personuppgifter som inte har gjorts gemensamt tillgängliga.

Skälen för utredningens förslag

Undantag från sökförbudet i brottsdatalagen vid sökning i alla slags personuppgifter

I avsnitt 5.3.8 föreslår utredningen att förbudet i 4 kap. 4 § första stycket kustbevakningsdatalagen att använda känsliga personuppgifter som sökbegrepp ska upphävas, eftersom det finns ett generellt sökförbud i 2 kap. 14 § brottsdatalagen. Det förbudet utgår till skillnad från dagens reglering från syftet med sökningen. Om syftet inte är att få fram ett personurval grundat på känsliga personuppgifter är sökningen tillåten, även om känsliga personuppgifter används vid sökningen (se SOU 2017:29 s. 272 f.).

Eftersom sökförbudet har en ny utformning är det nödvändigt att se över bestämmelserna om sökning. Enligt 4 kap. 4 § andra stycket kustbevakningsdatalagen är det tillåtet att använda brottsrubriceringar eller uppgifter som beskriver en persons utseende som sökbegrepp vid sökning i uppgifter som har gjorts gemensamt tillgängliga. Kustbevakningen har alltså behov av att kunna använda sådana uppgifter vid sökning, även om det leder till att man

får fram ett personurval grundat på känsliga personuppgifter. Det bör därför enligt utredningens mening göras undantag från brottsdatalagens sökförbud i Kustbevakningens brottsdatalag för sådana sökningar. För att möjligheterna till sökning ska vara desamma som i dag bör undantaget omfatta sökning i alla slags personuppgifter, dvs. oberoende av om de har gjorts gemensamt tillgängliga eller inte.

Kustbevakningen behöver i likhet med Polismyndigheten och Tullverket kunna göra sökningar på tillvägagångssätt vid brott (se avsnitt 7.3.3 och 8.3.3). Sådana sökningar kan i vissa fall leda till ett personurval grundat på känsliga personuppgifter. Som exempel kan nämnas att smugglingsmetoder kan avslöja uppgifter om såväl religiös övertygelse och politiska åsikter som uppgifter om gärningsmannens hälsa.

Undantag vid sökning i personuppgifter som inte har gjorts gemensamt tillgängliga

Det nuvarande förbudet i kustbevakningsdatalagen mot att använda känsliga personuppgifter som sökbegrepp gäller endast vid sökning i uppgifter som har gjorts gemensamt tillgängliga. Det innebär att känsliga personuppgifter får användas vid sökning i uppgifter som enbart ett fåtal har tillgång till. Den enda begränsningen i dag är att behandling av känsliga personuppgifter ska vara absolut nödvändig.

Utredningens utgångspunkt är att de behöriga myndigheternas möjlighet att använda känsliga personuppgifter vid sökning inte ska försämrats. Kustbevakningen kan behöva göra sammanställningar i syfte att få fram ett personurval grundat på känsliga personuppgifter vid sökning i uppgifter som inte har gjorts gemensamt tillgängliga. Framför allt Kustbevakningens underrättelseverksamhet kan behöva göra sökningar som innebär att sammanställningar grundade på etniskt ursprung eller religiös eller filosofisk övertygelse skapas. Organiserad brottslighet av olika slag kräver inte sällan kartläggning av misstänkta kontakter och vanor. Då kan olika typer av känsliga personuppgifter avslöjas (jfr avsnitt 7.3.3 och 8.3.3). Kustbevakningen måste kunna göra sökningar för att förebygga, förhindra eller upptäcka brottslig verksamhet som begås av flera personer som förenas genom sitt etniska ursprung eller sin religiösa eller filosofiska övertygelse. I utredningsverksamheten

finns motsvarande behov av att kunna söka på känsliga personuppgifter vid brott med okänd gärningsman. Det finns därför skäl att göra undantag från sökförbudet i brottsdatalagen när det gäller sökning i uppgifter som inte har gjorts gemensamt tillgängliga.

Kustbevakningen har dock inte behov av att kunna ta fram personurval grundade på alla kategorier av känsliga personuppgifter. Det kan aldrig finnas behov av att göra sammanställningar grundade på ras, eftersom det inte finns någon vetenskaplig grund för att dela in människor i skilda raser (se SOU 2017:29 s. 267). Utredningen ser inte heller något behov av att kunna göra sammanställningar grundade på genetiska eller biometriska uppgifter, uppgifter om medlemskap i fackförening eller politiska åsikter eller uppgifter som rör sexualliv eller sexuell läggning. Undantaget från sökförbudet i brottsdatalagen bör därför utformas så att sökning i personuppgifter som inte har gjorts gemensamt tillgängliga möjliggörs när det gäller uppgifter som kan avslöja etniskt ursprung, religiös eller filosofisk övertygelse eller uppgifter som rör hälsa. Det innebär att möjligheterna att använda känsliga personuppgifter vid sökning i uppgifter som inte har gjorts gemensamt tillgängliga begränsas i förhållande till vad som gäller i dag. Eftersom det inte finns behov av ett generellt undantag bedömer utredningen att förslaget inte innebär någon försämring.

Hur förhåller sig sökmöjligheterna till sekretessbestämmelsen?

I avsnitt 7.3.3 redovisas hur de nu föreslagna bestämmelserna om undantag från sökförbudet förhåller sig till bestämmelser om sekretess. Som framgår där kommer utredningens förslag om att absolut sekretess ska gälla hos behöriga myndigheter till skydd för enskild för uppgifter i ett sådant personurval som avses i 2 kap. 14 § brottsdatalagen inte att gälla för sökningar som görs med stöd av ett undantag från sökförbudet. Utlämnande av känsliga personuppgifter i en sådan sammanställning får i stället prövas mot andra bestämmelser om sekretess.

9.4 Gemensamt tillgängliga uppgifter

9.4.1 Behandling för diarieföring ska undantas

Utredningens förslag: Det som föreskrivs om gemensamt tillgängliga uppgifter ska inte gälla när personuppgifter behandlas med stöd av den särskilda bestämmelsen i brottsdatalagen om behandling av personuppgifter för diarieföring eller för att utföra andra nödvändiga handläggningsuppgifter.

Skälen för utredningens förslag: I polisdatalagen, åklagardatalagen, tullbrottsdatalagen och skattebrottsdatalagen föreskrivs att reglerna om gemensamt tillgängliga personuppgifter inte är tillämpliga när personuppgifter behandlas med stöd av den särskilda bestämmelsen om behandling av personuppgifter för diarieföring eller för att utföra andra nödvändiga handläggningsuppgifter. Någon sådan bestämmelse finns inte i kustbevakningsdatalagen.

Bestämmelsen om personuppgiftsbehandling vid diarieföring syftar inte till att möjliggöra behandling av personuppgifter i den operativa verksamheten, utan enbart till att inkomna handlingar ska kunna hanteras enligt offentlighets- och sekretesslagen och att tillgodose rätten till tillgång till allmänna handlingar enligt tryckfrihetsförordningen. Flera av de bestämmelser som gäller vid behandling av gemensamt tillgängliga personuppgifter är inte lämpade att reglera behandling av personuppgifter i diaries (se bl.a. Skattebrottsdatalag, prop. 2016/17:89, s. 87 f.). Det har giltighet även för Kustbevakningen. Det bör därför föreskrivas att reglerna om gemensamt tillgängliga personuppgifter inte gäller när personuppgifter behandlas med stöd av 2 kap. 2 § brottsdatalagen.

9.4.2 En ny kategori av personuppgifter får göras gemensamt tillgängliga

Utredningens förslag: Personuppgifter som behandlas i syfte att upprätthålla allmän ordning och säkerhet ska få göras gemensamt tillgängliga. De ska inte få behandlas längre än ett år efter utgången av det kalenderår då de behandlades automatiserat första gången.

Skälen för utredningens förslag: De personuppgifter som Kustbevakningen behandlar i annan operativ verksamhet än den brottsbekämpande och som behövs för att övervaka den allmänna ordningen och säkerheten till sjöss får i dag göras gemensamt tillgängliga enligt 5 kap. 1 § kustbevakningsdatalagen. Som framgår av avsnitt 9.2 föreslår utredningen att Kustbevakningens brottsdatalag ska tillämpas vid personuppgiftsbehandling i syfte att upprätthålla allmän ordning och säkerhet. Inför kommenderingar vid särskilda händelser där ordningsstörningar befaras kan det finnas behov av att göra uppgifter om personer som tidigare orsakat ordningsstörningar gemensamt tillgängliga. Utredningen anser därför att Kustbevakningen av de skäl som anges i avsnitt 7.5.1 bör kunna göra personuppgifter som behandlas i syfte att upprätthålla allmän ordning och säkerhet gemensamt tillgängliga.

Personuppgifter som görs gemensamt tillgängliga i syfte att upprätthålla allmän ordning och säkerhet bör inte få behandlas längre än ett år efter utgången av det kalenderår då de behandlades automatiserat första gången. Det motsvarar vad som föreslås gälla för Polismyndigheten.

9.4.3 Sökning i gemensamt tillgängliga uppgifter

Utredningens förslag: Bestämmelsen som begränsar resultatet vid sökning i gemensamt tillgängliga uppgifter med hjälp av namn, personnummer, samordningsnummer eller liknande identitetsbeteckningar ska enbart gälla i automatiserade behandlingssystem.

Begränsningarna ska inte gälla vid sökning som utförs av särskilt angivna tjänstemän i syfte att i underrättelseverksamhet bearbeta och analysera personuppgifter som har gjorts gemensamt tillgängliga enligt vissa bestämmelser och som enbart dessa tjänstemän har tillgång till.

Skälen för utredningens förslag

Begränsning endast i automatiserade behandlingssystem

Eftersom sökning med hjälp av namn, personnummer och samordningsnummer är ett viktigt inslag i Kustbevakningens verksamhet och sådana identitetsbeteckningar är av stor betydelse för att säkerställa identiteten och undvika personförväxlingar, ansågs det nödvändigt att medge sådan sökning i gemensamt tillgängliga uppgifter (se prop. 2011/12:45 s. 126 och avsnitt 7.5.2). I 4 kap. 5 § kustbevakningsdatalagen regleras därför vilka uppgifter som får tas fram vid sökning på namn, personnummer, samordningsnummer eller andra liknande identitetsbeteckningar. I 4 kap. 6 § görs vissa undantag från bestämmelserna i 4 kap. 5 §. I förarbetena diskuteras ingående vilka typer av sökning som bör vara tillåtna och vilka begränsningar som bör gälla (se prop. 2011/12:45 s. 126 f.). Paragraferna är utformade efter mönster av polisdatalagen.

Av de skäl som anges i avsnitt 7.5.2 bör det tydliggöras att regleringen enbart gäller vid sökning i automatiserade behandlingssystem. Där görs också vissa uttalanden om hur regleringen bör tolkas som är giltiga även för Kustbevakningen.

Sökning i gemensamt tillgängliga uppgifter

Det bör övervägas om det för Kustbevakningen delvis ändrade tillämpningsområdet för lagen bör föranleda någon ändring av begränsningsregeln i 4 kap. 5 § kustbevakningsdatalagen. Kustbevakningens brottsdatalag omfattar även behandling av personuppgifter i syfte att upprätthålla allmän ordning och säkerhet. De uppgifter som då främst kan vara av intresse är uppgifter om att någon är eller har varit misstänkt för brott mot allmän ordning. Sådana uppgifter är redan i dag tillgängliga vid en sökning. Detsamma gäller uppgifter om att någon kan antas komma att möta ett ingripande med grovt våld. Det finns därför inte anledning att utöka de nu gällande möjligheterna att få fram uppgifter vid en allmän sökning.

Det bör även övervägas om det kan finnas skäl att göra någon ändring i undantagen från begränsningarna. Av de skäl som anges i avsnitt 7.5.2 bör undantaget för sökning i underrättelseverksamhet

ändras på motsvarande sätt i Kustbevakningens brottsdatalag för att motverka att regleringen misstolkas.

10 Skattebrottsdatalagen

10.1 Skattebrottsdatalagen behöver anpassas

10.1.1 Nuvarande reglering

Skattebrottsdatalagen gäller enligt 1 kap. 2 § vid behandling av personuppgifter i Skatteverkets brottsbekämpande verksamhet. Det är dock bara en mycket begränsad del av myndighetens verksamhet. Lagen är ny och trädde i kraft den 1 juli 2017. Vissa av bestämmelserna i lagen behöver inte tillämpas före den 1 januari 2019.

Som anges i avsnitt 4.2 måste registerförfattningarna ändras i vissa avseenden med anledning av dataskyddsdirektivet och anpassas till brottsdatalagen. Många bestämmelser behöver överhuvudtaget inte anpassas eller endast ändras redaktionellt. Utredningen behandlar de anpassningar och ändringar som är gemensamma för registerförfattningarna i kapitel 5 och 6. De ytterligare anpassningar som krävs i skattebrottsdatalagen behandlas i detta kapitel.

10.1.2 Skattebrottsdatalagen ges ett nytt namn

Utredningens förslag: Skattebrottsdatalagen med tillhörande förordning ska benämnas Skatteverkets brottsdatalag och Skatteverkets brottsdataförordning.

Skälen för utredningens förslag: Av de skäl som anges i avsnitt 7.1.2 finns det anledning att byta namn på registerförfattningarna inom brottsdatalagens tillämpningsområde. Det gäller även skattebrottsdatalagen, trots att den nyligen fått sitt nuvarande namn. Namnet bör knyta an till hur brottsdatalagen benämns. Det bör vara kort och ange för vem författningen gäller och vad den

handlar om. Utredningen föreslår därför att lagen ska benämnas Skatteverkets brottsdatalag. Skattebrottsdataförordningen bör i konsekvens med det benämnas Skatteverkets brottsdataförordning. Som en konsekvens av att lagens namn ändras måste alla hänvisningar till den ändras.

10.2 Tillämpningsområdet

Utredningens förslag: Lagen ska gälla utöver brottsdatalagen när Skatteverket i egenskap av behörig myndighet behandlar personuppgifter i syfte att bekämpa brott.

Skälen för utredningens förslag: I avsnitt 4.4.1 tar utredningen ställning till att registerförfattningarna även i fortsättningen ska innehålla bestämmelser om tillämpningsområdet och anger övergripande hur regleringen bör utformas. Vidare föreslår utredningen i avsnitt 5.2 att registerförfattningarna ska gälla utöver brottsdatalagen.

Skattebrottsdatalagen gäller enligt 1 kap. 2 § för behandling av personuppgifter i Skatteverkets brottsbekämpande verksamhet. Tillämpningsområdet måste anpassas till brottsdatalagens tillämpningsområde så att det utgår från syftet med behandlingen i stället för i vilken verksamhet behandlingen utförs. Det bör också framgå att Skatteverkets brottsdatalag endast gäller när myndigheten agerar i egenskap av behörig myndighet, eftersom det är en viktig avgränsning för tillämpningsområdet (se SOU 2017:29 s. 159 f.).

Som framgår av avsnitt 5.4.6 anses lagföring av brott i dag ingå i begreppet brottsbekämpning. I brottsdatalagen görs det däremot skillnad mellan brottsbekämpning och lagföring. Skatteverket har dock inga lagförande uppgifter, vilket framgår av 2 kap. 5 § skattebrottsdatalagen. Tillämpningsområdet bör därför endast omfatta personuppgiftsbehandling i syfte att bekämpa brott.

I avsnitt 4.4.2 diskuterar utredningen vad det ändrade tillämpningsområdet innebär.

10.3 Grundläggande bestämmelser om behandling

10.3.1 Tillåtna rättsliga grunder och behandling för nya ändamål

Utredningens förslag: Skatteverket ska få behandla personuppgifter om det är nödvändigt för att utföra en arbetsuppgift i syfte att

1. förebygga, förhindra eller upptäcka brottslig verksamhet,
2. utreda brott, eller
3. fullgöra förpliktelser som följer av internationella åtaganden.

Arbetsuppgiften ska framgå av en bindande unionsrättsakt eller av en lag, en förordning eller ett särskilt beslut i vilket regeringen uppdragit åt myndigheten att ansvara för en sådan uppgift.

Det ska framgå genom en hänvisning att personuppgifter som behandlas med stöd av lagen ska få behandlas för nya ändamål enligt de förutsättningar som anges i brottsdatalagen.

Skälen för utredningens förslag

En bestämmelse som ersätter brottsdatalagens bestämmelse om tillåtna rättsliga grunder för behandling

Som anges i avsnitt 6.3.1 bör registerförfattningarna innehålla bestämmelser om tillåtna rättsliga grunder för behandling av personuppgifter. Regleringen i 2 kap. 5 § skattebrottsdatalagen bör således behållas, men det ska framgå att det inte är en ändamålsbestämelse i egentlig mening. Bestämmelsen är på samma sätt som 2 kap. 1 § brottsdatalagen en del av den rättsliga grunden och ger Skatteverket rättsligt stöd för att behandla personuppgifter automatiserat för att utföra sina arbetsuppgifter (se avsnitt 6.1.2).

Skatteverket får i dag behandla personuppgifter om det behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda brott eller fullgöra de förpliktelser som följer av internationella åtaganden. Myndigheten bör givetvis även i fortsättningen få behandla personuppgifter om det är nödvändigt för att fullgöra

sådana arbetsuppgifter, men regleringen bör anpassas till brottsdatalagens terminologi.

Skatteverkets brottsdatalog föreslås gälla utöver brottsdatalagen. För att det inte ska råda någon osäkerhet om hur bestämmelsen i 2 kap. 1 § brottsdatalagen förhåller sig till bestämmelsen om tillåtna rättsliga grunder i registerförfattningen bör den senare helt ersätta bestämmelsen i brottsdatalagen. I Skatteverkets brottsdatalog bör det därför på samma sätt som i brottsdatalagen föreskrivas att den arbetsuppgift som ska utföras ska framgå av en bindande unionsrättsakt eller en lag, en förordning eller ett särskilt beslut i vilket regeringen uppdragit åt myndigheten att ansvara för en sådan uppgift. Vad det innebär utvecklas i delbetänkandet (se SOU 2017:29 s. 238 f.).

Behandling för nya ändamål

I dag regleras behandling för nya ändamål till viss del i den sekundära ändamålsbestämmelsen i 2 kap. 6 § skattebrottsdatalagen. Utredningen anser som framgår av avsnitt 6.3.2 och 6.4.2 att de sekundära ändamålsbestämmelserna bör upphävas. Förutsättningarna för behandling för nya ändamål bör i stället regleras i brottsdatalagen. Innan personuppgifter får behandlas för nya ändamål inom brottsdatalagens tillämpningsområde ska det enligt 2 kap. 4 § brottsdatalagen säkerställas att behandlingen är nödvändig och proportionerlig för det nya ändamålet. Utredningen föreslår att samma prövning ska göras när de brottsbekämpande myndigheterna behandlar personuppgifter för nya ändamål utanför tillämpningsområdet. Det bör införas en bestämmelse i Skatteverkets brottsdatalog som tydliggör att förutsättningarna för att behandla personuppgifter, som behandlas med stöd av den lagen, för nya ändamål regleras i brottsdatalagen.

10.3.2 Behandling av biometriska och genetiska uppgifter

<p>Utredningens bedömning: Skatteverket bör inte få behandla biometriska och genetiska uppgifter.</p>

Skälen för utredningens bedömning: I avsnitt 7.3.2 redovisas vad som avses med biometriska och genetiska uppgifter och vilken betydelse de har vid brottsbekämpning.

Enligt 2 kap. 12 och 13 §§ brottsdatalagen utgör biometriska uppgifter som används för att identifiera en person och genetiska uppgifter känsliga personuppgifter. Sådana uppgifter får endast behandlas om det är särskilt föreskrivet och det är absolut nödvändigt för ändamålet med behandlingen.

Det är svårt att se att Skatteverket har något behov av att behandla biometriska och genetiska uppgifter och utredningen anser därför att det inte bör finnas någon bestämmelse som medger sådan behandling i Skatteverkets brottsdatalag.

10.3.3 Sökning på känsliga personuppgifter

Utredningens förslag: Sökförbudet i brottsdatalagen ska inte hindra att uppgifter som beskriver en persons utseende används vid sökning.

Det ska inte heller hindra sökning i syfte att få fram ett personurval grundat på etniskt ursprung, om sökningen görs i personuppgifter som inte har gjorts gemensamt tillgängliga.

Skälen för utredningens förslag

Undantag från sökförbudet i brottsdatalagen vid sökning i alla slags personuppgifter

I avsnitt 5.3.8 föreslår utredningen att förbudet i 3 kap. 5 § skattebrottsdatalagen att använda känsliga personuppgifter som sökbegrepp ska upphävas, eftersom det finns ett generellt sökförbud i 2 kap. 14 § brottsdatalagen. Det förbudet utgår till skillnad från dagens reglering från syftet med sökningen. Om syftet inte är att få fram ett personurval grundat på känsliga personuppgifter är sökningen tillåten, även om känsliga personuppgifter används vid sökningen (se SOU 2017:29 s. 272 f.).

Eftersom sökförbudet har en ny utformning är det nödvändigt att se över bestämmelserna om sökning. Enligt 3 kap. 5 § andra stycket skattebrottsdatalagen är det tillåtet att använda uppgifter

som beskriver en persons utseende som sökbegrepp vid sökning i uppgifter som gjorts gemensamt tillgängliga. Det finns även i fortsättningen behov att kunna använda sådana uppgifter vid sökning, även om det leder till att man får fram ett personurval grundat på känsliga personuppgifter. Det bör därför enligt utredningens mening göras undantag från brottsdatalagens sökförbud i Skatteverkets brottsdatalag. För att möjligheterna till sökning ska vara desamma som i dag bör undantaget omfatta sökningar i alla slags personuppgifter, dvs. oberoende av om uppgifterna har gjorts gemensamt tillgängliga eller inte.

Undantag vid sökning i personuppgifter som inte har gjorts gemensamt tillgängliga

Det nuvarande förbudet i skattebrottsdatalagen mot att använda känsliga personuppgifter som sökbegrepp gäller endast vid sökning i uppgifter som har gjorts gemensamt tillgängliga. Det innebär att känsliga personuppgifter kan användas vid sökning i uppgifter som endast ett fåtal har tillgång till. Den enda begränsningen i dag är att behandling av känsliga personuppgifter ska vara absolut nödvändig.

Utredningens utgångspunkt är att de behöriga myndigheternas möjlighet att använda känsliga personuppgifter vid sökning inte ska försämrats. För att effektivt kunna bekämpa brott behöver Skatteverket kunna göra sammanställningar i syfte att få fram ett personurval grundat på vissa känsliga personuppgifter vid sökning i uppgifter som inte har gjorts gemensamt tillgängliga. Det finns därför skäl att göra undantag från sökförbudet i brottsdatalagen vid sökning i uppgifter som inte har gjorts gemensamt tillgängliga.

Framför allt i underrättelseverksamheten kan det finnas behov av sökning som innebär att sammanställningar grundade på etniskt ursprung skapas. I t.ex. ärenden om falska identitetshandlingar eller gränsöverskridande ekonomisk brottslighet kan etniskt ursprung vara en gemensam faktor som knyter samman personer i ett nätverk. I utredningsverksamheten finns motsvarande behov av att kunna söka på sådana känsliga personuppgifter. Skatteverket har i övrigt inget behov av att kunna ta fram personurval grundade på känsliga personuppgifter.

Undantaget från sökförbudet i brottsdatalagen bör utformas så att sökning möjliggörs endast när det gäller etniskt ursprung. Det

innebär att möjligheterna att använda känsliga personuppgifter vid sökning i uppgifter som inte har gjorts gemensamt tillgängliga begränsas i förhållande till vad som gäller i dag. Eftersom det inte finns behov av ett generellt undantag bedömer utredningen att förslaget inte innebär någon försämring.

Hur förhåller sig sökmöjligheterna till sekretessbestämmelsen?

I avsnitt 7.3.3 redogörs för hur bestämmelserna om sökning på känsliga personuppgifter förhåller sig till bestämmelser om sekretess. Som framgår där kommer utredningens tidigare förslag om att absolut sekretess ska gälla för sökning som utförs i strid med det generella sökförbudet i 2 kap. 14 § brottdatalagen inte att gälla för sökningar som görs med stöd av de nu föreslagna undantagen. Utlämnande av känsliga personuppgifter i en sådan sammanställning får i stället prövas mot andra bestämmelser om sekretess.

10.4 Gemensamt tillgängliga uppgifter

Utredningens förslag: Bestämmelsen som begränsar resultatet vid sökning i gemensamt tillgängliga uppgifter med hjälp av namn, personnummer, samordningsnummer eller liknande identitetsbeteckningar ska enbart gälla i automatiserade behandlingssystem.

Begränsningarna ska inte gälla vid sökning i en viss handling eller i ett visst ärende. De ska inte heller gälla vid sökning som görs av särskilt angivna tjänstemän

1. när de utför beredningsuppgifter i underrättelseverksamhet, om arbetet befinner sig i ett inledande skede,
2. i syfte att i underrättelseverksamhet bearbeta och analysera personuppgifter som har gjorts gemensamt tillgängliga enligt vissa bestämmelser och som enbart dessa tjänstemän har tillgång till, eller
3. i syfte att utreda brott för vilket är föreskrivet fängelse i fyra år eller däröver.

Skälen för utredningens förslag

Begränsning endast i automatiserade behandlingssystem

Eftersom sökning med hjälp av namn, personnummer och samordningsnummer är ett viktigt inslag i Skatteverkets verksamhet och sådana identitetsbeteckningar är av stor betydelse för att säkerställa identiteten och undvika personförväxlingar, ansågs det nödvändigt att medge sådan sökning i gemensamt tillgängliga uppgifter (jfr avsnitt 7.5.2). I 3 kap. 6 § skattebrottsdatalagen regleras därför vilka uppgifter som får tas fram vid sökning på namn, personnummer, samordningsnummer eller andra liknande identitetsbeteckningar. I 3 kap. 7 § görs vissa undantag från bestämmelserna i 3 kap. 6 §. I förarbetena diskuteras ingående vilka typer av sökning som bör vara tillåtna och vilka begränsningar som bör gälla (se prop. 2016/17:89 s. 96 f.). Paragraferna är utformade efter mönster av polisdatalagen.

Skattebrottsdatalagen har nyligen trätt i kraft och de aktuella bestämmelserna behöver inte tillämpas förrän år 2019. Liknande övergångsbestämmelser gäller även för polisen, som därför ännu inte heller har erfarenhet av att tillämpa bestämmelserna. Av de skäl som anges i avsnitt 7.5.2 bör det tydliggöras att regleringen enbart gäller vid sökning i automatiserade behandlingssystem. Där görs också vissa uttalanden om hur regleringen bör tolkas som är giltiga även för Skatteverket.

Sökning i gemensamt tillgängliga uppgifter

Undantagen i 3 kap. 7 § skattebrottsdatalagen från begränsningarna av vilka uppgifter som får tas fram vid sökning är utformade efter mönster av polisdatalagen. Av de skäl som anges i avsnitt 7.5.2 bör undantagen ändras även i Skatteverkets brottsdatalag. Det gäller undantagen för att bearbeta och analysera information i underrättelseverksamhet. Regleringen bör utformas på samma sätt som för Polismyndigheten.

10.5 Övergångsbestämmelser till skattebrottsdatalagen

Utredningens bedömning: Övergångsbestämmelserna till skattebrottsdatalagen behöver inte ändras.

Skälen för utredningens bedömning: Utredningen föreslår i avsnitt 5.3.10 att vissa bestämmelser om särskilda upplysningar ska finnas kvar. I 3 kap. 4 § första stycket skattebrottsdatalagen föreskrivs att om uppgifter som är gemensamt tillgängliga direkt kan hänföras till en person som inte är misstänkt för brott eller för att ha utövat eller komma att utöva viss brottslig verksamhet, ska det genom en särskild upplysning eller på annat sätt framgå att personen inte är misstänkt. Vidare krävs det enligt andra stycket särskilda upplysningar i vissa fall om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak. Till paragrafen finns det övergångsbestämmelser i punkterna 3 och 4 a. Punkten 3 innebär att bestämmelsen om särskilda upplysningar inte behöver tillämpas på uppgifter som har samlats in före lagens ikraftträdande och punkten 4 a att den inte behöver tillämpas förrän den 1 januari 2019 när det gäller annat än underrättelseverksamhet.

Enligt 2 kap. 9 § brottsdatalagen ska uppgifter om olika kategorier av personer så långt möjligt särskiljas. Om det inte framgår av sammanhanget eller på annat sätt till vilken kategori en person hör ska det framgå genom en särskild upplysning. I delbetänkandet bedömer utredningen att det inte är nödvändigt att förse alla äldre personuppgifter med sådana upplysningar om de saknar det (se SOU 2017:29 s. 262). Det bör därför vara möjligt att behålla punkten 3 i övergångsbestämmelserna. Det kan däremot ifrågasättas om det är möjligt att ha kvar punkten 4 a med hänsyn till kraven i artikel 6 i direktivet på att det ska göras tydlig åtskillnad mellan olika kategorier av registrerade. Eftersom Skatteverket har anpassat sig till övergångsbestämmelsen i fråga och tiden mellan brottsdatalagens ikraftträdande och när övergångsbestämmelsen upphör att gälla är så kort anser utredningen att det inte finns skäl att upphäva övergångsbestämmelsen.

I punkten 4 c i övergångsbestämmelserna föreskrivs att 4 kap. 5 och 6 §§ om hur länge vissa personuppgifter får behandlas inte be-

höver tillämpas förrän den 1 januari 2019. En sådan övergångsbestämmelse står inte i strid med brottsdatalagens reglering om hur länge personuppgifter får behandlas och kan därmed behållas. Det bör dock framhållas att Skatteverket måste iaktta skyldigheten i 2 kap. 18 § brottsdatalagen att återkommande se över behovet av att behandla uppgifterna fram till dess att den nu aktuella bestämmelsen i Skatteverkets brottsdatalag börjar tillämpas.

Övergångsbestämmelserna till bestämmelserna om sökning kan behållas då direktivet inte ställer några krav på sökbegränsningar.

Utredningens förslag till anpassningar av skattebrottsdatalagen innebär att de bestämmelser som övergångsbestämmelserna tar sikte på får ny placering eller numrering. Övergångsbestämmelser behöver i sådana fall inte ändras utan ska fortsätta att tillämpas på samma sätt som tidigare.

I kapitel 18 behandlas behovet av nya övergångsbestämmelser.

11 Åklagardatalagen

11.1 Åklagardatalagen behöver anpassas

11.1.1 Nuvarande reglering

Åklagardatalagen gäller enligt 1 kap. 2 § första stycket vid behandling av personuppgifter i Åklagarmyndighetens och Ekobrottsmyndighetens (åklagarväsendets) operativa verksamhet. Med operativ verksamhet avses dels brottsbekämpande verksamhet, dels fullgörandet av andra åklagaruppgifter enligt lag eller förordning. Det senare kan t.ex. vara att föra talan om hävande av registrering av varumärkesrätt, att företräda staten i mål om vattenföreningensavgift eller att fatta beslut om förstörande av vissa hälsofarliga missbrukssubstanser (se prop. 2014/15:63 s. 43 f. och 68 f.). Lagen gäller enligt 1 kap. 2 § andra stycket inte vid behandling av personuppgifter i den polisiära verksamheten vid Ekobrottsmyndigheten. Vid sådan behandling gäller i stället polisdatalagen och andra författningar som reglerar polisens personuppgiftsbehandling.

Som anges i avsnitt 4.2 måste registerförfattningarna ändras i vissa avseenden med anledning av dataskyddsdirektivet och anpassas till brottsdatalagen. Många bestämmelser behöver överhuvudtaget inte anpassas eller endast ändras redaktionellt. Utredningen behandlar de anpassningar och ändringar som är gemensamma för registerförfattningarna i kapitel 5 och 6. De ytterligare anpassningar som krävs i åklagardatalagen behandlas i detta kapitel.

Frågan om anpassning av den del av åklagardatalagen som ligger utanför brottsdatalagens tillämpningsområde bereds för närvarande i Regeringskansliet.

11.1.2 Åklagardatalagen delas upp

Utredningens förslag: Åklagardatalagen med tillhörande förordning ska bara innehålla bestämmelser om personuppgiftsbehandling inom brottsdatalagens tillämpningsområde och ges nya namn. De ska benämnas åklagarväsendets brottsdatalag och åklagarväsendets brottsdataförordning.

Skälen för utredningens förslag

Den nuvarande regleringen renodlas

Vid åklagardatalagens tillkomst övervägde regeringen om åklagardatalagen endast skulle omfatta personuppgiftsbehandling i den brottsbekämpande verksamheten. Eftersom arbetsuppgifter utanför den brottsbekämpande verksamheten utgör en mycket liten del av åklagarverksamheten ansåg regeringen dock att det inte behövdes någon särskild författning för annan operativ verksamhet. Eftersom personuppgiftslagens allmänna bestämmelser inte heller var ändamålsenliga för sådan integritetskänslig verksamhet ansåg regeringen att åklagardatalagen borde omfatta all personuppgiftsbehandling som rör åklagaruppgifter (se prop. 2014/15:63 s. 43 f.). Med hänsyn till hur den nya dataskyddsregleringen är utformad finns det emellertid skäl att på nytt överväga den frågan.

Åklagardatalagen reglerar alltså huvudsakligen personuppgiftsbehandling inom brottsdatalagens tillämpningsområde, men även till viss del inom dataskyddsförordningens. Om man skulle behålla en samlad reglering för åklagarväsendets personuppgiftsbehandling skulle den därför till största delen gälla utöver brottsdatalagen, men skulle i övrigt komplettera dataskyddsförordningen.

Ett alternativ är att dela upp regleringen i två separata regelverk – ett för brottsdatalagens tillämpningsområde och ett för dataskyddsförordningens. Som anges i avsnitt 9.1.2 är strukturen med olika registerförfattningar för en myndighets olika verksamheter ingen nyhet.

Den nya dataskyddsregleringen gör det nödvändigt att dela upp regleringen av åklagarväsendets personuppgiftsbehandling på ett annat sätt än i dag. Det skulle i och för sig vara möjligt att göra alla nödvändiga ändringar i den befintliga lagen. Lösningen med två

separata regleringar blir emellertid enligt utredningens mening tydligare och lättare att tillämpa. Trots de skäl som anges i förarbetena till åklagardatalagen bör därför åklagarväsendets personuppgiftsbehandling fortsättningsvis regleras i olika registerförfattningar. Den del av personuppgiftsbehandlingen som ligger inom brottsdatalagens tillämpningsområde bör regleras i den befintliga lagen med hänsyn till att den i dag till största delen rör brottsbekämpande verksamhet. Mot den bakgrunden bör 2 kap. 5 § andra stycket åklagardatalagen, som reglerar behandling av personuppgifter utanför brottsdatalagens tillämpningsområde, upphävas.

Åklagardatalagen ges ett nytt namn

Eftersom endast den del av åklagarväsendets personuppgiftsbehandling som ligger inom brottsdatalagens tillämpningsområde ska regleras i åklagardatalagen, bör det övervägas om lagens namn bör bytas. Av de skäl som anges i avsnitt 7.1.2 finns det anledning att byta namn på registerförfattningarna inom brottsdatalagens tillämpningsområde. Namnet bör knyta an till hur brottsdatalagen benämns. Det bör vara kort och ange för vem författningen gäller och vad den handlar om. Eftersom lagen ska gälla för både Åklagarmyndigheten och Ekobrottsmyndigheten bör det av namnet framgå att lagen omfattar båda myndigheterna, som tillsammans bildar åklagarväsendet. Utredningen föreslår därför att lagen ska benämnas åklagarväsendets brottsdatalag. Åklagardataförordningen bör i konsekvens med det benämnas åklagarväsendets brottsdataförordning. Som en konsekvens av att lagens namn ändras måste alla hänvisningar till den ändras.

11.2 Tillämpningsområdet

Utredningens förslag: Lagen ska gälla utöver brottsdatalagen när myndigheterna i åklagarväsendet i egenskap av behöriga myndigheter behandlar personuppgifter i åklagarverksamhet i syfte att bekämpa eller lagföra brott eller handlägga frågor om ändring eller verkställighet av straffrättsliga påföljder eller upprätthållande av allmän ordning och säkerhet.

Skälen för utredningens förslag

Den nuvarande regleringen behöver anpassas

I avsnitt 4.4.1 tar utredningen ställning till att registerförfattningarna även i fortsättningen ska innehålla bestämmelser om tillämpningsområdet och anger övergripande vad som bör gälla för den regleringen. Vidare föreslår utredningen i avsnitt 5.2 att registerförfattningarna ska gälla utöver brottsdatalagen.

Enligt 1 kap. 2 § åklagardatalagen gäller lagen vid behandling av personuppgifter i åklagarväsendets operativa verksamhet. Tillämpningsområdet måste anpassas till brottsdatalagens, så att det dels utgår från syftet med behandlingen, dels omfattar bara den personuppgiftsbehandling som Åklagarmyndigheten och Ekobrottsmyndigheten utför inom brottsdatalagens tillämpningsområde och som inte regleras i någon annan lag. Det bör framgå att åklagarväsendets brottsdatalag endast gäller när någon av myndigheterna agerar i egenskap av behöriga myndigheter, eftersom det är en viktig avgränsning för tillämpningsområdet (se SOU 2017:29 s. 159 f.).

Närmare om tillämpningsområdet

Som framgår av avsnitt 5.4.6 anses lagföring av brott i dag ingå i begreppet brottsbekämpning, medan det i brottsdatalagen görs skillnad mellan brottsbekämpning och lagföring. För att tillämpningsområdet ska täcka det som i dag omfattas av regleringen bör det därför inkludera personuppgiftsbehandling i syfte att bekämpa eller lagföra brott.

Brottsdatalagens tillämpningsområde omfattar även personuppgiftsbehandling i syfte att verkställa straffrättsliga påföljder. Åklagare för talan om ändring av påföljd enligt bestämmelser i 27, 28 och 38 kap. brottsbalken. Åklagare prövar även vissa frågor om straffverkställighet vid beslut att utfärda en europeisk eller nordisk arresteringsorder (se 2 och 4 §§ förordningen [2003:1178] om överlämnande till Sverige enligt en europeisk arresteringsorder och 2 och 4 §§ förordningen [2012:566] om överlämnande till Sverige enligt en nordisk arresteringsorder). Åklagare ska också yttra sig i vissa frågor om rättspsykiatrisk vård med särskild utskrivningsprövning. Personuppgiftsbehandling när åklagare handlägger frågor

som rör ändring av påföljd eller frågor om straffverkställighet bör därför också omfattas av lagens tillämpningsområde.

Brottsdatalagens tillämpningsområde omfattar även personuppgiftsbehandling i syfte att upprätthålla allmän ordning och säkerhet. Enligt 6 § lagen (2005:321) om tillträdesförbud vid idrottsarrangemang prövar allmän åklagare frågor om tillträdesförbud. Som framgår av delbetänkandet är brottsdatalagen tillämplig på behandling av personuppgifter vid sådan prövning (se SOU 2017:29 s. 228 f.). Tillämpningsområdet bör därför också omfatta personuppgiftsbehandling när åklagare handlägger frågor om upprätthållande av allmän ordning och säkerhet.

Särskilt om verksamheten vid Ekobrottsmyndigheten

Ekobrottsmyndigheten är en åklagarmyndighet som ansvarar för bekämpning av ekonomisk brottslighet. Åklagarmyndigheten ansvarar för all annan åklagarverksamhet än den som ankommer på Ekobrottsmyndigheten. I avsnitt 7.2.1 redogör utredningen för Ekobrottsmyndighetens organisation och arbetsuppgifter. Som framgår där består Ekobrottsmyndighetens operativa verksamhet av underrättelseverksamhet, utrednings- och lagföringsverksamhet och brottsförebyggande verksamhet. Huvuddelen av myndighetens verksamhet är att utreda brott.

Personuppgiftsbehandlingen vid Ekobrottsmyndigheten regleras i dag i både åklagardatalagen och polisdatalagen. Polisdatalagen gäller i den polisiära verksamheten, medan åklagardatalagen gäller i den övriga operativa verksamheten. Utredningen föreslår i avsnitt 7.2.1 att uttrycket åklagarverksamhet ska användas för att avgränsa tillämpningsområdet för polisdatalagen. Skälet till det är att det är tydligare vad som ingår i åklagarverksamhet än i polisiär verksamhet. Utredningen föreslår där att polisens brottsdatalag ska gälla vid personuppgiftsbehandling i syfte att utreda brott, om det inte är fråga om åklagarverksamhet. Åklagarväsendets brottsdatalag bör med hänsyn till det gälla vid personuppgiftsbehandling som utförs i åklagarverksamhet i syfte att utreda och lagföra brott.

Behandling av personuppgifter i den underrättelseverksamhet som bedrivs vid Ekobrottsmyndigheten ska inte omfattas av åklagarväsendets brottsdatalag, eftersom den verksamheten leds, styrs

och utförs av Polismyndigheten på Ekobrottsmyndighetens uppdrag. Den utgör därmed inte någon åklagarverksamhet.

11.3 Grundläggande bestämmelser om behandling

11.3.1 Tillåtna rättsliga grunder och behandling för nya ändamål

Utredningens förslag: Personuppgifter ska få behandlas om det är nödvändigt för att utföra en arbetsuppgift i syfte att

1. förebygga eller förhindra brottslig verksamhet,
2. utreda eller lagföra brott,
3. handlägga frågor om ändring eller verkställighet av straffrättsliga påföljder,
4. handlägga frågor som rör upprätthållande av allmän ordning och säkerhet, eller
5. fullgöra förpliktelser som följer av internationella åtaganden.

Arbetsuppgiften ska framgå av en bindande unionsrättsakt eller av en lag, en förordning eller ett särskilt beslut i vilket regeringen uppdragit åt myndigheten att ansvara för en sådan uppgift.

Det ska framgå genom en hänvisning att personuppgifter som behandlas med stöd av lagen ska få behandlas för nya ändamål enligt de förutsättningar som anges i brottsdatalagen.

Skälen för utredningens förslag

En bestämmelse som ersätter brottsdatalagens bestämmelse om tillåtna rättsliga grunder för behandling

Som anges i avsnitt 6.3.1 bör registerförfattningarna innehålla bestämmelser om tillåtna rättsliga grunder för behandling av personuppgifter. Regleringen i 2 kap. 5 § första stycket åklagardatalagen bör alltså behållas, men det ska framgå att det inte är en ändamålsbestämmelse i egentlig mening. Bestämmelsen är på samma sätt

som 2 kap. 1 § brottsdatalagen en del av den rättsliga grunden och ger åklagare rättsligt stöd för att behandla personuppgifter automatiserat för att utföra sina arbetsuppgifter (se avsnitt 6.1.2).

I dag får personuppgifter behandlas i åklagarväsendets brottsbekämpande verksamhet om det behövs för att förebygga eller förhindra brottslig verksamhet, utreda eller beivra brott eller fullgöra de förpliktelser som följer av internationella åtaganden. Åklagarmyndigheten och Ekobrottsmyndigheten bör givetvis även i fortsättningen få behandla personuppgifter om det är nödvändigt för att fullgöra sådana arbetsuppgifter, men regleringen bör anpassas till brottsdatalagens terminologi.

Åklagare för talan om ändring av påföljder bl.a. med stöd av 38 kap. 2 och 2 a §§ brottsbalken. Som framgår av avsnitt 11.2 prövar åklagare numera även vissa frågor om straffverkställighet när de utfärdar en nordisk eller europeisk arresteringsorder. Eftersom det ingår i åklagares arbetsuppgifter att handlägga frågor om ändring eller verkställighet av straffrättsliga påföljder bör det också vara en tillåten rättslig grund för åklagares personuppgiftsbehandling.

Utredningen föreslår i avsnitt 11.2 att tillämpningsområdet för åklagarväsendets brottsdatalag ska omfatta personuppgiftsbehandling när åklagare handlägger frågor om upprätthållande av allmän ordning och säkerhet. Att handlägga frågor som rör upprätthållande av allmän ordning och säkerhet bör därför också vara en tillåten rättslig grund för personuppgiftsbehandlingen.

Åklagarväsendets brottsdatalag föreslås gälla utöver brottsdatalagen. För att det inte ska råda någon osäkerhet om hur bestämmelsen i 2 kap. 1 § brottsdatalagen förhåller sig till bestämmelsen om tillåtna rättsliga grunder i registerförfattningen bör den senare helt ersätta bestämmelsen i brottsdatalagen. Det bör därför, på samma sätt som i brottsdatalagen, föreskrivas att den arbetsuppgift som ska utföras ska framgå av en bindande unionsrättsakt eller en lag, en förordning eller ett särskilt beslut i vilket regeringen uppdragit åt åklagare att ansvara för en sådan uppgift. Vad det innebär utvecklas i delbetänkandet (se SOU 2017:29 s. 238 f.).

Behandling för nya ändamål

I dag regleras behandling för nya ändamål till viss del i den sekundära ändamålsbestämmelsen i 2 kap. 6 § åklagardatalagen. Utredningen anser som framgår av avsnitt 6.3.2 och 6.4.2 att de sekundära ändamålsbestämmelserna bör upphävas. Förutsättningarna för behandling för nya ändamål bör i stället regleras i brottsdatalagen. Innan personuppgifter får behandlas för nya ändamål inom brottsdatalagens tillämpningsområde ska det enligt 2 kap. 4 § brottsdatalagen säkerställas att behandlingen är nödvändig och proportionerlig för det nya ändamålet. Utredningen föreslår att samma prövning ska göras när de brottsbekämpande myndigheterna behandlar personuppgifter för nya ändamål utanför tillämpningsområdet. Det bör införas en bestämmelse i åklagarväsendets brottsdatalag som tydliggör att förutsättningarna för att behandla personuppgifter, som behandlas med stöd av den lagen, för nya ändamål regleras i brottsdatalagen.

11.3.2 Behandling av biometriska och genetiska uppgifter

Utredningens bedömning: Åklagarmyndigheten och Ekobrottsmyndigheten bör inte få behandla biometriska och genetiska uppgifter.

Skälen för utredningens bedömning: I avsnitt 7.3.2 redovisas vad som avses med biometriska och genetiska uppgifter och vilken betydelse de har vid brottsbekämpning.

Enligt 2 kap. 12 och 13 §§ brottsdatalagen utgör biometriska uppgifter som används för att identifiera en person och genetiska uppgifter känsliga personuppgifter. Sådana uppgifter får endast behandlas om det är särskilt föreskrivet och det är absolut nödvändigt för ändamålet med behandlingen.

Det är svårt att se att åklagare har något behov av att behandla biometriska och genetiska uppgifter och utredningen anser därför att det inte bör finnas någon bestämmelse som medger sådan behandling i åklagarväsendets brottsdatalag.

Det bör anmärkas att de personuppgifter som förekommer i ett utlåtande som baseras på en teknisk bearbetning av biometriska

eller genetiska uppgifter inte i sig utgör sådana uppgifter. Åklagare kommer alltså att kunna behandla personuppgifter i sådana utlåtanden i samma utsträckning som i dag.

11.3.3 Sökning på känsliga personuppgifter

Utredningens förslag: Sökförbudet i brottsdatalagen ska inte hindra att brottsrubriceringar eller uppgifter som beskriver en persons utseende används vid sökning.

Skälen för utredningens förslag

Undantag från sökförbudet i brottsdatalagen vid sökning i alla slags personuppgifter

I avsnitt 5.3.8 föreslår utredningen att förbudet i 3 kap. 4 § första stycket åklagardatalagen att använda känsliga personuppgifter som sökbegrepp ska upphävas, eftersom det finns ett generellt sökförbud i 2 kap. 14 § brottsdatalagen. Det förbudet utgår till skillnad från dagens reglering från syftet med sökningen. Om syftet inte är att få fram ett personurval grundat på känsliga personuppgifter är sökningen tillåten, även om känsliga personuppgifter används vid sökningen (se SOU 2017:29 s. 272 f.).

Eftersom sökförbudet har en ny utformning är det nödvändigt att se över bestämmelserna om sökning. Enligt 3 kap. 4 § andra stycket åklagardatalagen är det tillåtet att använda brottsrubriceringar eller uppgifter som beskriver en persons utseende som sökbegrepp vid sökning i uppgifter som har gjorts gemensamt tillgängliga. Myndigheterna har även i fortsättningen behov av att kunna använda sådana uppgifter vid sökning, även om det leder till att man får fram ett personurval grundat på känsliga personuppgifter. Det bör därför enligt utredningens mening göras undantag från brottsdatalagens sökförbud i åklagarväsendets brottsdatalag för sådana sökningar. För att möjligheterna till sökning ska vara desamma som i dag bör undantaget omfatta sökning i alla slags personuppgifter, dvs. oberoende av om uppgifterna har gjorts gemensamt tillgängliga eller inte.

Behövs det undantag vid sökning i personuppgifter som inte har gjorts gemensamt tillgängliga?

Det nuvarande förbudet i åklagardatalagen mot att använda känsliga personuppgifter som sökbegrepp gäller endast vid sökning i personuppgifter som har gjorts gemensamt tillgängliga. Det innebär att känsliga personuppgifter får användas vid sökning i uppgifter som enbart ett fåtal har tillgång till.

Utredningens utgångspunkt är att de behöriga myndigheternas möjlighet att använda känsliga personuppgifter vid sökning inte ska försämrats. Enligt utredningens mening behövs det inte något undantag vid sökning i uppgifter som inte har gjorts gemensamt tillgängliga, eftersom sammanställningar grundande på känsliga personuppgifter normalt inte görs av åklagare. Förändringen innebär därmed inte någon försämring.

Hur förhåller sig sökmöjligheterna till sekretessbestämmelsen?

I avsnitt 7.3.3 redogörs för hur den nu föreslagna bestämmelsen om undantag från sökförbudet förhåller sig till bestämmelser om sekretess. Som framgår där kommer utredningens förslag om att absolut sekretess ska gälla hos behöriga myndigheter till skydd för enskild för uppgifter i ett sådant personurval som avses i 2 kap. 14 § brottsdatalagen inte att gälla för sökning som görs med stöd av ett undantag från sökförbudet. Utlämnande av känsliga personuppgifter i en sådan sammanställning får i stället prövas mot andra bestämmelser om sekretess.

11.4 Gemensamt tillgängliga uppgifter

Utredningens förslag: Bestämmelsen som begränsar resultatet vid sökning i gemensamt tillgängliga uppgifter med hjälp av namn, personnummer, samordningsnummer eller liknande identitetsbeteckningar ska enbart gälla i automatiserade behandlingssystem.

Vid en sådan sökning ska även uppgifter få tas fram som anger att den sökta personen är anmäld för brott.

Skälen för utredningens förslag

Begränsning endast i automatiserade behandlingssystem

Eftersom sökning med hjälp av namn, personnummer och samordningsnummer är ett viktigt inslag i åklagares verksamhet och sådana identitetsbeteckningar är av stor betydelse för att säkerställa identiteten och undvika personförväxlingar, ansågs det nödvändigt att medge sådan sökning i gemensamt tillgängliga uppgifter (se prop. 2014/15:63 s. 88 f. och avsnitt 7.5.2). I 3 kap. 5 § åklagardatalagen regleras därför vilka uppgifter som får tas fram vid sökning på namn, personnummer, samordningsnummer eller andra liknande identitetsbeteckningar. I 3 kap. 6 § görs undantag från bestämmelserna i 3 kap. 5 § vid sökning i en viss handling eller i ett visst ärende. I förarbetena diskuteras ingående vilka typer av sökning som bör vara tillåtna och vilka begränsningar som bör gälla (se prop. 2014/15:63 s. 88 f.). Paragraferna är utformade efter mönster av polisdatalagen.

Av de skäl som anges i avsnitt 7.5.2 bör det tydliggöras att regleringen enbart gäller vid sökning i automatiserade behandlingssystem. Där görs också vissa uttalanden om hur regleringen bör tolkas som är giltiga även för åklagarväsendet.

Bör ytterligare uppgifter få tas fram vid sökning?

Som nyss nämnts föreskrivs det i 3 kap. 5 § åklagardatalagen vilka uppgifter som får tas fram vid sökning på namn, personnummer, samordningsnummer eller andra liknande identitetsbeteckningar i uppgifter som har gjorts gemensamt tillgängliga. Det rör sig bl.a. om uppgifter som anger att den sökta personen är eller har varit misstänkt för brott, är misstänkt för att ha utövat eller komma att utöva brottslig verksamhet eller har anmält ett brott. Motsvarande bestämmelser finns i bl.a. 3 kap. 6 § polisdatalagen, 4 kap. 5 § kustbevakningsdatalagen och 3 kap. 6 § tullbrottsdatalagen. De senare bestämmelserna skiljer sig dock från bestämmelsen i åklagardatalagen på det sättet att de även anger att uppgift om att någon är anmäld för brott får tas fram. Frågan är om det bör införas en motsvarande bestämmelse i åklagarväsendets brottsdatalag.

Utgångspunkten är att brott normalt ska anmälas till Polismyndigheten eller någon av de andra myndigheter som har till uppgift att ta upp anmälningar om brott. I vissa fall görs dock en brottsanmälan direkt till åklagare. Det gäller t.ex. anmälningar enligt 7 kap. 16 § konkurslagen (1987:672) från konkursförvaltare, men det kan även förekomma i andra fall. Det förhållandet att vissa anmälningar görs direkt till åklagare motiverar enligt utredningens mening att även sådana uppgifter bör vara sökbara.

12 Domstolsdatalagen

12.1 Behovet av ny reglering

12.1.1 Nuvarande reglering

Domstolsdatalagen gäller enligt 2 § vid behandling av personuppgifter i de allmänna domstolarnas, de allmänna förvaltningsdomstolarnas och hyres- och arrendenämndernas rättskipande och rättsvårdande verksamhet. Lagen gäller också när personuppgifter vidarebehandlas i den administrativa verksamheten för att lämnas ut efter begäran.

Lagen gäller enligt 4 § i stället för personuppgiftslagen, men vissa bestämmelser i den lagen som räknas upp i 5 § ska ändå tillämpas. Domstolsdatalagen kompletteras av domstolsdataförordningen, som framför allt innehåller mer preciserade bestämmelser om sökning och direktåtkomst.

12.1.2 Regleringen för domstolarna kräver särskilda överväganden

Domstolsdatalagen liknar i vissa avseenden övriga registerförfattningar. Den räknar upp vilka bestämmelser i personuppgiftslagen som ska tillämpas i domstolarnas verksamhet och delar upp ändamålen i primära och sekundära. Det som framför allt skiljer domstolsdatalagen från övriga registerförfattningar är att den har en annan lagteknisk struktur. Lagen är inte kapitelindeldad och större delen av regleringen finns i förordning. I de avseendena liknar den mer kriminalvårdens registerlagstiftning. Vissa bestämmelser i domstolsdatalagen avviker från motsvarande bestämmelser i övriga registerförfattningar, där det också finns bestämmelser som helt saknar motsvarighet i domstolsdatalagen. Som exempel kan nämnas

att lagen inte innehåller några bestämmelser om bevarande och gallring, utan i stället bestämmelser som begränsar möjligheterna att söka i avgjorda mål och ärenden. Lagen är inte heller tillämplig på behandling av uppgifter om juridiska personer.

Domstolsdatalagen kräver därför särskilda överväganden, vilket gör att utredningen behandlar den för sig. De överväganden som görs i kapitel 5 och 6 om övriga registerförfattningar har trots det i stor utsträckning bäring på regleringen av domstolarnas personuppgiftsbehandling inom brottsdatalagens tillämpningsområde.

I domstolsdatalagen regleras personuppgiftsbehandling inom både brottsdatalagens och dataskyddsförordningens tillämpningsområde. De delar av domstolsdatalagen och domstolsdataförordningen som ligger utanför brottsdatalagens tillämpningsområde har övervägts av en annan utredare. Förslagen redovisas i promemorian En omarbetad domstolsdatalag (Ds 2017:41).

12.1.3 En särskild registerlagstiftning inom brottsdatalagens tillämpningsområde

Utredningens förslag: En ny lag och en ny förordning, som inom brottsdatalagens tillämpningsområde ersätter domstolsdatalagen med tillhörande förordning, ska införas. De ska benämnas domstolarnas brottsdatalag och domstolarnas brottsdataförordning.

Skälen för utredningens förslag

Den nuvarande regleringen bör renodlas

Domstolsdatalagen med tillhörande förordning reglerar personuppgiftsbehandling såväl inom som utanför brottsdatalagens tillämpningsområde. Utredningen redovisar i delbetänkandet sin syn på när brottsdatalagen är tillämplig vid personuppgiftsbehandling inom domstolsväsendet (se SOU 2017:29 s. 181 f., 206 f., 225 f. och 228 f.). När brottsdatalagen och dataskyddsförordningen börjar tillämpas kommer domstolsdatalagen alltså att vara tillämplig både vid personuppgiftsbehandling inom och utanför brottsdatalagens tillämpningsområde, om ingen ändring görs. Som utredning-

en utvecklar i avsnitt 9.1.2 och 11.1.2 bör lösningen med en gemensam reglering som dels kompletterar dataskyddsförordningen, dels gäller utöver brottsdatalagen inte väljas. Utredningen har samrått med den utredare som haft i uppdrag att anpassa domstolsdatalagen till dataskyddsförordningen om att dela upp regleringen i två separata regelverk – ett som ska gälla för brottsdatalagens tillämpningsområde och ett för dataskyddsförordningens. Den utredaren föreslår i enlighet med det att domstolsdatalagen renodlas så att den enbart reglerar personuppgiftsbehandling inom dataskyddsförordningens tillämpningsområde (se Ds 2017:41 s. 55 f.).

Det bör mot den bakgrunden införas en ny lag och en ny förordning som ersätter domstolsdatalagen med tillhörande förordning inom brottsdatalagens tillämpningsområde. Lagen bör ha samma struktur som övriga registerförfattningar.

Registerförfattningens namn

Eftersom endast den del av domstolarnas personuppgiftsbehandling som ligger inom brottsdatalagens tillämpningsområde ska regleras i den nya lagen bör lagen ha ett namn som tydliggör registerförfattningens anknytning till brottsdatalagen. Namnet bör vara kort och tydligt ange för vem författningen gäller och vad den rör. Den nya lagens namn bör följa samma systematik som föreslås för registerförfattningarna i övrigt (se t.ex. avsnitt 7.1.2). Utredningen föreslår därför att lagen ska benämnas domstolarnas brottsdatalag. Den tillhörande förordningen bör i konsekvens med det benämnas domstolarnas brottsdataförordning.

12.2 Utgångspunkter för regleringen

12.2.1 Den nya lagen ska gälla utöver brottsdatalagen

Utredningens förslag: Den nya lagen ska gälla utöver brottsdatalagen.

Skälen för utredningens förslag: I avsnitt 5.2 föreslår utredningen att registerförfattningarna för övriga myndigheter i rättskedjan ska gälla utöver brottsdatalagen. Detsamma bör gälla den nya lagen för

domstolarna. Lagen bör innehålla bestämmelser som innebär preciseringar, undantag eller avvikelser från bestämmelserna i brottsdatalagen. Det medför att bestämmelserna i den nya lagen måste läsas tillsammans med regleringen i brottsdatalagen och tolkas i ljuset av den regleringen.

12.2.2 Domstolsdatalagen kan bilda mönster

Vid personuppgiftsbehandling inom brottsdatalagens tillämpningsområde kommer den lagen att fylla ungefär samma funktion som personuppgiftslagen gör i dag, eftersom den innehåller grundläggande bestämmelser om behandlingen. Det behövs emellertid också bestämmelser som tar hänsyn till domstolarnas särskilda behov av att kunna behandla personuppgifter (se SOU 2017:29 s. 140 f.).

Domstolsdatalagen har nyligen införts. Det innebär att den, som konstateras i avsnitt 4.3, i likhet med övriga registerförfattningar uppfyller kraven som ställs i dataskyddsrambeslutet. Mot bakgrund av att direktivet i stor utsträckning bygger vidare på regleringen i dataskyddsrambeslutet är domstolsdatalagen därmed till stor del redan anpassad till de krav som ställs i direktivet. Det innebär att den nya lagen kan utformas med domstolsdatalagen som mönster.

Som framgår av avsnitt 12.1.3 kommer det att finnas olika regelverk för domstolarnas personuppgiftsbehandling i den rättskipande och rättsvårdande verksamheten. Det är en fördel om regleringen i den nya lagen kan stämma överens med regleringen i domstolsdatalagen. I vissa avseenden skiljer sig dock dataskyddsdirektivets reglering från dataskyddsförordningens. Eftersom den nya lagen måste vara förenlig med direktivet är det oundvikligt att den till viss del kommer att avvika från regleringen i domstolsdatalagen.

12.2.3 Vissa bestämmelser i domstolsdatalagen behövs inte

Utredningens bedömning: Eftersom brottsdatalagen innehåller en generell reglering behövs inte vissa av de bestämmelser som i dag finns i domstolsdatalagen.

Skälen för utredningens bedömning: Den nya lagen ska som nyss nämnts gälla utöver brottsdatalagen. Eftersom brottsdatalagen innehåller en generell reglering behövs ingen motsvarighet till vissa bestämmelser som i dag finns i domstolsdatalagen. Det gäller bl.a. bestämmelserna om lagens syfte, personuppgiftsombud, behandling av känsliga personuppgifter och tillgången till personuppgifter (jfr avsnitt 5.3.3, 5.3.6, 5.3.8 och 5.3.9). Ett annat exempel är bestämmelsen om att lagen enbart gäller för automatiserad och annan strukturerad behandling (jfr avsnitt 5.3.4). Utredningen återkommer i avsnitt 12.7 till i vilken utsträckning föreskrifter om tillgång till personuppgifter bör kunna meddelas.

I 11 § första stycket domstolsdatalagen föreskrivs att den som är personuppgiftsombud ska föra en förteckning över de behandlingar som utförs. Enligt förarbetena bör domstolarna vara skyldiga att sammanställa och tillgängliggöra den information som en anmälan enligt 36 § första stycket personuppgiftslagen av automatiserad behandling skulle ha innehållit (se prop. 2014/15:148 s. 85 f.). Enligt 3 kap. 3 § brottsdataförordningen ska den personuppgiftsansvarige föra register över behandlingar. Där ska bl.a. kategorier av behandlingar av personuppgifter förtecknas och för varje kategori ska registret ange bl.a. den rättsliga grunden för behandlingen och ändamålen med behandlingen. Någon bestämmelse motsvarande 11 § domstolsdatalagen behövs därför inte i den nya lagen. Det gäller även föreskriftsrätten som är knuten till den paragrafen.

Enligt 12 § domstolsdatalagen ska den personuppgiftsansvarige till var och en som begär det lämna upplysningar om sina behandlingar av personuppgifter. Upplysningarna ska i princip omfatta samma information som ska framgå av den förteckning som personuppgiftsombudet ska föra enligt 11 §. Motsvarande bestämmelse finns i 42 § personuppgiftslagen, men av lagtekniska skäl ansåg lagstiftaren att det inte var lämpligt att hänvisa till den (se prop. 2014/15:148 s. 86). Som utredningen konstaterar i avsnitt 5.3.1 finns det ingen motsvarighet till 42 § personuppgiftslagen i direktivet. Även om det inte finns något som hindrar att en motsvarande bestämmelse tas in i den nya lagen ser utredningen inget behov av det. Regleringen i 3 kap. 3 § brottsdataförordningen fyller behovet av sådan information.

12.3 Allmänna bestämmelser

12.3.1 Tillämpningsområdet

Utredningens förslag: Lagen ska gälla utöver brottsdatalagen när allmän domstol i egenskap av behörig myndighet behandlar personuppgifter, om uppgifterna behandlas i syfte att handlägga mål eller ärenden om utredning av eller lagföring för brott, ändring eller verkställighet av straffrättsliga påföljder eller upprätthållande av allmän ordning och säkerhet.

Lagen ska också gälla när allmän förvaltningsdomstol i egenskap av behörig myndighet behandlar personuppgifter, om uppgifterna behandlas i syfte att handlägga mål om verkställighet av häktning eller straffrättsliga påföljder.

Skälen för utredningens förslag

Nya utgångspunkter för avgränsningen av tillämpningsområdet

I avsnitt 4.4.1 tar utredningen ställning till att registerförfattningarna ska innehålla bestämmelser om tillämpningsområdet. Domstolsdatalagen gäller vid personuppgiftsbehandling i domstolarnas rättskipande och rättsvårdande verksamhet och när personuppgifterna vidarebehandlas i den administrativa verksamheten för att lämnas ut efter begäran.

Brottsdatalagen gäller enligt 1 kap. 2 § för behandling av personuppgifter som utförs av behöriga myndigheter i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller verkställa straffrättsliga påföljder. Den gäller också för behandling av personuppgifter som en behörig myndighet utför i syfte att upprätthålla allmän ordning och säkerhet. Det som är avgörande för brottsdatalagens tillämpning är alltså, förutom att det ska vara en behörig myndighet som behandlar personuppgifterna, att personuppgiftsbehandlingen görs för något av dessa syften. Tillämpningsområdet för den nya lagen kan därför inte knytas till domstolarnas rättskipande och rättsvårdande verksamhet utan bör avgränsas på ett annat sätt. Tillämpningsområdet bör i stället utgå från syftet med behandlingen. Det bör också framgå att den nya lagen gäller när domstolar agerar i egenskap av behöriga myndig-

heter, eftersom det är en viktig avgränsning för tillämpningsområdet (se SOU 2017:29 s. 159 f.).

Närmare om tillämpningsområdet

Den nya lagen bör omfatta all personuppgiftsbehandling som domstolar utför inom brottsdatalagens tillämpningsområde. Domstolarnas kärnverksamhet består i att handlägga mål och ärenden (jfr 6 § domstolsdatalagen). Tillämpningsområdet för den nya lagen bör därför knytas till personuppgiftsbehandling som utförs i syfte att handlägga mål och ärenden av vissa slag.

För allmän domstol bör tillämpningsområdet framför allt omfatta brottmålsförfarandet. Tillämpningsområdet bör alltså omfatta personuppgiftsbehandling i syfte att handlägga mål och ärenden om lagföring för brott.

Allmän domstol prövar också ofta frågor om häktning och andra straffprocessuella tvångsmedel under en förundersökning. Domstolarna fattar även beslut enligt 23 kap. 19 § rättegångsbalken om komplettering av förundersökningar och kan hålla vittnesförhör och besluta i andra frågor under pågående förundersökningar. Personuppgiftsbehandling för sådana syften bör också omfattas av tillämpningsområdet. I konsekvens med hur tillämpningsområdet uttrycks för de brottsbekämpande myndigheterna bör den arbetsuppgiften anges som handläggning av mål eller ärenden om utredning av brott.

Vidare prövar allmän domstol vissa frågor om ändring av påföljd och om verkställighet av påföljd (se SOU 2017:29 s. 228 f.). Handläggning av mål och ärenden som rör ändring och verkställighet av straffrättsliga påföljder bör därmed ingå i tillämpningsområdet.

Eftersom allmän domstol även prövar frågor om tillträdesförbud vid idrottsarrangemang bör tillämpningsområdet också omfatta handläggning av mål och ärenden om upprätthållande av allmän ordning och säkerhet (se SOU 2017:29 s. 228 f.).

För allmän förvaltningsdomstol bör tillämpningsområdet endast omfatta personuppgiftsbehandling i syfte att handlägga mål om verkställighet av häktning och straffrättsliga påföljder. Det avser verkställighet av rättspsykiatrisk vård, andra vårdpåföljder och vissa frihetsberövande påföljder (se SOU 2017:29 s. 226). Även när den

gren inom de allmänna förvaltningsdomstolarna som handlägger migrationsmål, dvs. Migrationsöverdomstolen och migrationsdomstolarna, handlägger mål som rör personer som av allmän domstol utvisats på grund av brott behandlas personuppgifter i sådant syfte.

Eftersom hyres- och arrendenämnderna inte behandlar personuppgifter för något av de syften som omfattas av direktivets tillämpningsområde är det inte möjligt att reglera deras personuppgiftsbehandling i den nya lagen. Tillämpningsområdet bör därför endast omfatta allmän domstol och allmän förvaltningsdomstol.

Hela målets eller ärendets handläggning bör omfattas

När mål eller ärenden handläggs för något av de syften som anges i lagen bör hela handläggningen fram till dess att domstolen slutligt avgjort frågan omfattas av lagens tillämpningsområde. Det innebär att all personuppgiftsbehandling som utförs vid handläggningen av ett brottmål omfattas av tillämpningsområdet. Även handläggning av enskilda anspråk bör omfattas, trots att det är en civilrättslig talan, så länge de handläggs inom ramen för brottmålet. Lagen bör dock inte vara tillämplig om anspråket avskiljs för att handläggas som tvistemål. Det bör på motsvarande sätt gälla vissa andra former av särskild talan och talan om förbud som förs i brottmål (se SOU 2017:29 s. 208 f.).

Vidare bör all expediering i ett mål eller ärende som är en del av handläggningen omfattas. Det spelar alltså ingen roll om domar eller beslut expedieras till Kriminalvården för verkställighet av påföljd eller till Inspektionen för vård och omsorg för att den ska kunna ta ställning till om en läkare som dömts för brott ska få behålla sin läkarlegitimation. Även expediering för att tillgodose partsinsynen i mål eller ärenden bör omfattas. Det avgörande är att expedieringen utförs i mål eller ärenden som domstolen handlägger för något av de syften som omfattas av lagens tillämpningsområde och att expedieringen utgör en del av handläggningen. Tillämpningsområdet bör även omfatta den expediering som är direkt knuten till att avgörandet får laga kraft.

Däremot bör domstolens behandling av personuppgifter för arkivering eller för att överlämna allmänna handlingar till en arkivmyndighet inte omfattas av den nya lagens tillämpningsområde.

Som anges i delbetänkandet omfattas behandling för arkivändamål av dataskyddsförordningens tillämpningsområde, oavsett om det är den behöriga myndigheten som arkiverar personuppgifterna eller om de överlämnas till en arkivmyndighet (se SOU 2017:29 s. 287).

Om handläggning för något av de syften som anges i lagen aktualiseras på nytt, t.ex. genom en ansökan om resning i ett brottmål, är den nya lagen tillämplig på handläggningen.

Utlämnande omfattas inte av tillämpningsområdet

Domstolsdatalagen gäller inte bara i den rättskipande och rättsvårdande verksamheten utan även i den del av den administrativa verksamheten som avser att på begäran lämna ut uppgifter ur mål och ärenden till en enskild eller en myndighet (se prop. 2014/15:148 s. 27 f.). Domstolsdatalagens tillämpningsområde omfattar exempelvis utlämnande av allmänna handlingar enligt 2 kap. tryckfrihetsförordningen. Sådan vidarebehandling av personuppgifter omfattas inte av direktivets tillämpningsområde och kan därför inte heller ingå i den nya lagens tillämpningsområde. Det gäller oavsett om målet eller ärendet är under handläggning eller har avslutats.

12.3.2 Personuppgiftsansvar

Utredningens förslag: Varje domstol ska vara personuppgiftsansvarig för den behandling av personuppgifter som den utför.

Skälen för utredningens förslag: Personuppgiftsansvarig definieras i 1 kap. 6 § brottsdatalagen som den behöriga myndighet som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter. Enligt 3 kap. 1 § är den personuppgiftsansvarige ansvarig för all behandling av personuppgifter som utförs under dennes ledning eller på dennes vägnar.

Enligt 9 § domstolsdatalagen är varje domstol personuppgiftsansvarig för den behandling av personuppgifter som den utför. Att varje domstol ansvarar för den behandling som domstolen utför är med hänsyn till domstolarnas självständighet centralt. En bestäm-

melse som motsvarar 9 § domstolsdatalagen bör därför tas in i den nya lagen.

12.3.3 Ska domstolarna utse dataskyddsbud?

Utredningens bedömning: Domstolarna bör inte undantas från skyldigheten i brottsdatalagen att utse dataskyddsbud.

Skälen för utredningens bedömning: Enligt 3 kap. 13 § brottsdatalagen ska behöriga myndigheter utse dataskyddsbud (se SOU 2017:29 s. 340 f.). Domstolars och andra oberoende rättsliga myndigheters dömande verksamhet får dock enligt artikel 32 i direktivet undantas från skyldigheten att utse dataskyddsbud.

Enligt 10 § domstolsdatalagen är domstolarna i dag skyldiga att utse ett eller flera personuppgiftsbud. Personuppgiftsbud motsvarar det som i brottsdatalagen benämns dataskyddsbud. I förarbetena till domstolsdatalagen framhålls att hanteringen av personuppgifter i den rättskipande och rättsvårdande verksamheten indirekt begränsas av de processuella regelverken. I syfte att åstadkomma ett starkt integritetsskydd ansåg regeringen dock att domstolarna borde vara skyldiga att utse ett eller flera personuppgiftsbud (se prop. 2014/15:148 s. 91).

Direktivet innebär att dataskyddsbuden delvis får nya arbetsuppgifter som har karaktär av intern rådgivning. Deras uppdrag syftar tydligare till att bistå tillsynsmyndigheten. Dataskyddsbudens roll i förhållande till enskilda regleras inte i brottsdatalagen. Tanken är att de ändå ska fylla samma funktion som personuppgiftsbuden (se SOU 2017:29 s. 344 f.) Ombuden fortsätter alltså att vara av central betydelse för skyddet för personlig integritet. Det finns därför inte skäl att utnyttja möjligheten i artikel 32 i direktivet att undanta domstolarna från skyldigheten att utse dataskyddsbud i den dömande verksamheten. Den utredare som övervägt anpassningar av domstolsdatalagen till dataskyddsförordningen föreslår inte heller att motsvarande undantag i förordningen ska utnyttjas (se Ds 2017:41 s. 157 f.).

12.3.4 Uppgifter om juridiska personer

Utredningens bedömning: Lagen bör inte reglera behandling av uppgifter om juridiska personer.

Skälen för utredningens bedömning: Frågan om domstolsdatalagen skulle tillämpas på uppgifter om juridiska personer lyftes under lagstiftningsarbetet men ledde inte till något lagförslag. Som skäl för det angavs att det är tveksamt om begreppet personlig integritet har någon relevans för juridiska personer (se Ds 2013:10 s. 49 f.). Domstolsdatalagen är alltså inte tillämplig på uppgifter om juridiska personer.

I 1 kap. 6 § polisdatalagen, 1 kap. 3 § kustbevakningsdatalagen, 1 kap. 4 § åklagardatalagen, 1 kap. 4 § tullbrottsdatalagen och 1 kap. 4 § skattebrottsdatalagen föreskrivs däremot att vissa bestämmelser i respektive lag ska tillämpas på uppgifter om juridiska personer. Även om juridiska personer inte har samma behov av integritetskydd som fysiska personer har det ansetts att vissa grundläggande bestämmelser om personuppgiftsbehandling bör tillämpas även på uppgifter om juridiska personer. Dessutom kan det vara svårt att i elektronisk hantering skilja uppgifter om juridiska personer från uppgifter om fysiska personer som är ägare av eller ställföreträdare för sådana (se t.ex. prop. 2009/10:85 s. 78). Utredningen anser att bestämmelserna som skyddar uppgifter om juridiska personer bör behållas i övriga registerförfattningar (se avsnitt 5.4.1).

Frågan är om det finns skäl att införa en motsvarande reglering i den nya lagen, trots att uppgifter om juridiska personer inte har något särskilt skydd i dag. Det bör beaktas att den utredare som föreslagit anpassningar av domstolsdatalagen till dataskyddsförordningen inte föreslår att uppgifter om juridiska personer ska ha något särskilt skydd. Om den nya lagen skulle tillämpas på uppgifter om juridiska personer skulle regleringen av domstolarnas personuppgiftsbehandling bli olika utan att det krävs för att genomföra direktivet. Även om det finns fördelar med en enhetlig reglering för myndigheterna i rättskedjan bör en enhetlig reglering för domstolarna i detta fall väga tyngre. Mot den bakgrunden bör den nya lagen inte reglera behandling av uppgifter om juridiska personer.

12.4 Grundläggande bestämmelser om behandling

12.4.1 Tillåtna rättsliga grunder för behandling

Utredningens förslag: Personuppgifter ska få behandlas om det är nödvändigt och syftet är att handlägga mål eller ärenden om

1. utredning av eller lagföring för brott,
2. verkställighet av häktning eller ändring eller verkställighet av straffrättsliga påföljder, eller
3. upprätthållande av allmän ordning och säkerhet.

Arbetsuppgiften ska framgå av en bindande unionsrättsakt eller av en lag, en förordning eller ett särskilt beslut i vilket regeringen uppdragit åt domstol att ansvara för en sådan uppgift.

Skälen för utredningens förslag

En bestämmelse som ersätter brottsdatalagens bestämmelse om tillåtna rättsliga grunder för behandling

I 6 och 7 §§ domstolsdatalagen regleras för vilka ändamål domstolarna får behandla personuppgifter. Ändamålen delas liksom för de brottsbekämpande myndigheterna upp i primära och sekundära. De primära ändamålen reglerar den behandling av personuppgifter som behövs vid domstolens handläggning av mål och ärenden. De sekundära ändamålen reglerar i vilken utsträckning personuppgifter som behandlas för något av de primära ändamålen får behandlas för att tillgodose andras behov av information.

Som framgår av avsnitt 6.1.3 anser utredningen att en ändamålsbestämmelse bör ge någon ledning för prövningen av vilka personuppgifter som är adekvata och relevanta för behandlingen. Den primära ändamålsbestämmelsen i 6 § domstolsdatalagen ger enligt utredningens mening inte någon egentlig ledning för prövningen av vilka personuppgifter som får behandlas. Där anges endast att personuppgifter får behandlas om det behövs för att domstolarna ska kunna utföra sin huvudsakliga arbetsuppgift, att handlägga mål och ärenden. Syftet med bestämmelsen är att precisera när personuppgifter alls får behandlas i domstolarnas rättskipande och rättsvår-

dande verksamhet. Den utgör den yttre ramen inom vilken de särskilda, uttryckliga och berättigade ändamålen med behandlingen i enskilda fall ska bestämmas. Av samma skäl som anges beträffande de primära ändamålsbestämmelserna i de brottsbekämpande myndigheternas registerförfattningar anser utredningen därför att 6 § domstolsdatalagen inte i egentlig mening är en ändamålsbestämmelse. Den är i stället, på samma sätt som 2 kap. 1 § brottsdatalagen, en del av den rättsliga grunden och tydliggör att personuppgiftsbehandling är tillåten när arbetsuppgifterna fullgörs.

I avsnitt 6.3.1 konstaterar utredningen att de bestämmelser i de brottsbekämpande myndigheternas registerförfattningar som i dag kallas primära ändamålsbestämmelser bör behållas, men att det ska framgå att de inte är ändamålsbestämmelser i egentlig mening. I domstolarnas brottsdatalag bör det av samma skäl finnas en bestämmelse som motsvarar 6 § domstolsdatalagen. Det bör dock framgå att det inte är en ändamålsbestämmelse i egentlig mening.

Domstolarna bör givetvis få behandla personuppgifter om det är nödvändigt för att fullgöra en arbetsuppgift inom den nya lagens tillämpningsområde. För att bestämmelsen ska stämma överens med den terminologi som används i brottsdatalagen måste den utformas på annat sätt än 6 § domstolsdatalagen. Allmän domstol bör få behandla personuppgifter om det är nödvändigt för att handlägga mål och ärenden om utredning av eller lagföring för brott, ändring eller verkställighet av straffrättsliga påföljder eller upprätthållande av allmän ordning och säkerhet. Allmän förvaltningsdomstol bör få behandla personuppgifter om det är nödvändigt för att handlägga mål om verkställighet av häktning eller straffrättsliga påföljder.

Domstolarnas brottsdatalag föreslås gälla utöver brottsdatalagen. För att det inte ska råda någon osäkerhet om hur 2 kap. 1 § brottsdatalagen förhåller sig till bestämmelsen om tillåtna rättsliga grunder i registerförfattningen bör den senare helt ersätta bestämmelsen i brottsdatalagen. I domstolarnas brottsdatalag bör det därför på samma sätt som i brottsdatalagen föreskrivas att den arbetsuppgift som domstolen ska utföra ska framgå av en bindande unionsrättsakt eller en lag, en förordning eller ett särskilt beslut i vilket regeringen uppdragit åt domstol att ansvara för en sådan uppgift. Utredningen utvecklar i delbetänkandet vad det innebär (se SOU 2017:29 s. 238 f.).

12.4.2 Behandling för nya ändamål

Utredningens förslag: Det ska framgå genom en hänvisning att personuppgifter som behandlas med stöd av lagen ska få behandlas för nya ändamål inom den nya lagens tillämpningsområde enligt de förutsättningar som anges i brottsdatalagen.

Det ska framgå genom en hänvisning att förutsättningarna för att behandla personuppgifter, som behandlas med stöd av den nya lagen, för nya ändamål utanför tillämpningsområdet regleras i brottsdatalagen. Någon prövning av om behandlingen är nödvändig och proportionerlig ska inte krävas när domstolsdatalagen ska tillämpas.

Skälen för utredningens förslag

Nya ändamål inom brottsdatalagens tillämpningsområde

I 9 § första stycket d personuppgiftslagen finns en generell bestämmelse om vidarebehandling. Där regleras finalitetsprincipen, enligt vilken personuppgifter inte får behandlas för något ändamål som är oförenligt med det ändamål för vilket uppgifterna samlades in. Bestämmelsen gäller för domstolarna genom en hänvisning i 5 § första stycket 3 domstolsdatalagen. I den sekundära ändamålsbestämmelsen i 7 § domstolsdatalagen regleras även viss vidarebehandling. Personuppgifter som behandlas med stöd av den primära ändamålsbestämmelsen i 6 § får även behandlas för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning.

Innan personuppgifter behandlas för ett nytt ändamål inom brottsdatalagens tillämpningsområde ska det enligt 2 kap. 4 § den lagen säkerställas dels att det finns en tillåten rättslig grund för behandlingen, dels att behandlingen är nödvändig och proportionerlig för det nya ändamålet. För domstolarnas del kan det vara fallet t.ex. när personuppgifter i ett brottmål behövs för handläggningen av ett annat brottmål.

Enligt förarbetena tillåter 7 § domstolsdatalagen att domstolen lämnar ut personuppgifter inte bara om det finns en uttrycklig skyldighet i lag eller förordning att göra det, utan också i de fall där det kan anses påbjudet eller önskvärt att domstolen gör det (se prop. 2014/15:148 s. 41 f.). En prövning av nödvändighet och pro-

proportionalitet krävs enligt artikel 4.2 i direktivet alltid innan personuppgifter behandlas för ett nytt ändamål inom tillämpningsområdet. Som framgår i avsnitt 6.5 anser utredningen att det bara är i de fall där det finns en uttrycklig uppgiftsskyldighet som lagstiftaren kan anses ha tagit ställning till att uppgiftslämnandet är nödvändigt och proportionerligt. Det skulle därför inte vara förenligt med direktivet att ha en bestämmelse som motsvarar 7 § domstolsdatalagen i den nya lagen. Det bör i stället tas in en bestämmelse som tydliggör att förutsättningarna för att behandla personuppgifter, som redan behandlas, för nya ändamål inom lagens tillämpningsområde regleras i brottsdatalagen.

Nya ändamål utanför brottsdatalagens tillämpningsområde

I 2 kap. 21 § brottsdatalagen upplyses om att dataskyddsförordningen ska tillämpas när en behörig myndighet behandlar personuppgifter för ändamål utanför lagens tillämpningsområde. Som anges i delbetänkandet ska förordningen tillämpas redan när en behörig myndighet tillhandahåller personuppgifter till andra, om ändamålet ligger utanför brottsdatalagens tillämpningsområde (se SOU 2017:29 s. 292). Utredningen föreslår i avsnitt 6.4.3 att samma prövning av nödvändighet och proportionalitet ska göras vid behandling för nya ändamål utanför brottsdatalagens tillämpningsområde som vid behandling för nya ändamål inom tillämpningsområdet. Frågan är om den regleringen bör gälla även för domstolarna.

Regleringen av domstolarnas personuppgiftsbehandling skiljer sig i detta avseende från de brottsbekämpande myndigheternas. Domstolsdatalagen gäller i dag även när personuppgifter vidarebehandlas i den administrativa verksamheten för att tillhandahållas enskilda eller myndigheter som begär att få ta del av personuppgifter som behandlas i den rättskipande och rättsvårdande verksamheten (se prop. 2014/15:148 s. 101). Den utredare som övervägt hur domstolsdatalagen ska anpassas till dataskyddsförordningen anser att den ordningen bör bestå (se Ds 2017:41 s. 89).

När personuppgifter ska behandlas för nya ändamål och ändamålet omfattas av domstolsdatalagens tillämpningsområde, t.ex. utlämnande på begäran, skulle en möjlig lösning därför kunna vara

att föreskriva att domstolarna ska tillämpa den lagen i stället för att göra den prövning som utredningen föreslår i brottsdatalagen (se avsnitt 6.4.3). En stor del av behandlingen för nya ändamål utanför brottsdatalagens tillämpningsområde skulle med en sådan lösning följa samma regelverk som domstolarnas personuppgiftsbehandling inom dataskyddsförordningens tillämpningsområde. Det skulle naturligtvis underlätta för domstolarna om regleringen är densamma. Utredningen har samrått med den utredare som föreslår anpassningar av domstolsdatalagen till dataskyddsförordningen. Den utredaren föreslår en reglering som möjliggör det (se Ds 2017:41 s. 89 f. och 119 f.).

Förutsättningarna för att behandla personuppgifter, som behandlas med stöd av den nya lagen, för nya ändamål utanför lagens tillämpningsområde bör på samma sätt som för övriga myndigheter i rättskedjan regleras i brottsdatalagen, men lösningen bör vara annorlunda. Någon prövning av nödvändighet och proportionalitet bör inte krävas när domstolsdatalagen ska tillämpas. All behandling för nya ändamål utanför brottsdatalagens tillämpningsområde kommer dock inte att omfattas av domstolsdatalagens tillämpningsområde. Vid behandling för sådana nya ändamål som varken omfattas av brottsdatalagens eller domstolsdatalagens tillämpningsområde bör domstolarna göra samma prövning som i avsnitt 6.4.3 föreslås för de brottsbekämpande myndigheterna.

12.4.3 Särskilda upplysningar

Utredningens bedömning: Lagen bör inte innehålla något undantag från brottsdatalagens bestämmelser om särskilda upplysningar.

Skälen för utredningens bedömning: Enligt 2 kap. 3 § andra stycket brottsdatalagen ska det ändamål som personuppgifter behandlas för tydliggöras genom en särskild upplysning, om det inte framgår av sammanhanget eller på något annat sätt. I 2 kap. 9 § brottsdatalagen föreskrivs att personuppgifter som rör olika kategorier av registrerade så långt det är möjligt ska särskiljas, t.ex. personer som är misstänkta eller dömda för brott, brottsoffer eller andra som berörs av ett brott. Om det inte framgår av samman-

hanget eller på något annat sätt vilken kategori personen tillhör, ska det tydliggöras genom en särskild upplysning. Enligt 2 kap. 10 § brottsdatalagen ska personuppgifter som grundar sig på fakta så långt det är möjligt skiljas från personuppgifter som grundar sig på personliga bedömningar. Om grunden inte framgår av sammanhanget eller på något annat sätt ska den tydliggöras genom en särskild upplysning (se SOU 2017:29 s. 260 f.).

I avsnitt 5.3.10 föreslår utredningen att bestämmelser om särskilda upplysningar på samma sätt som i dag enbart ska gälla vid behandling av personuppgifter som har gjorts gemensamt tillgängliga. Domstolarna har i dag inga bestämmelser om särskilda upplysningar. Det beror på att det i domstolsdatalagen inte görs någon skillnad mellan uppgifter som har gjorts gemensamt tillgängliga och uppgifter som endast ett fåtal personer har tillgång till. I motsats till de brottsbekämpande myndigheterna behöver domstolarna därför inte något undantag från brottsdatalagens bestämmelser. Som konstateras i delbetänkandet framgår det vid handläggning i domstol oftast varför personuppgifter behandlas, vilken kategori av registrerade de gäller och om de grundar sig på fakta eller inte (se SOU 2017:29 s. 242 f. och 260 f.).

12.4.4 Behandling av personnummer

Utredningens förslag: Personnummer, samordningsnummer och liknande identitetsbeteckningar får endast behandlas när det är motiverat med hänsyn till vikten av en säker identifiering eller något annat beaktansvärt skäl.

Skälen för utredningens förslag: Enligt 22 § personuppgiftslagen får personnummer eller samordningsnummer behandlas utan samtycke bara när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl. Det innebär att den personuppgiftsansvarige ska göra en intresseavvägning mellan skälen för att behandla uppgifterna och de integritetsrisker det innebär. Domstolsdatalagen hänvisar till paragrafen i fråga för att markera vikten av den principen (se prop. 2014/15:148 s. 51).

I delbetänkandet konstaterar utredningen att det, utöver reglerna om känsliga personuppgifter, inte bör tas in några regler i brottsdatalagen om vilka personuppgifter som får behandlas (se SOU 2017:29 s. 276 f.). I avsnitt 5.3.1 gör utredningen bedömningen att det inte bör finnas någon motsvarighet till 22 § personuppgiftslagen i övriga registerförfattningar.

Frågan är om det finns skäl att göra en annan bedömning för domstolarnas del. Behovet av säker identifiering är givetvis lika stort för domstolarna som för övriga myndigheter i rättskedjan. Det som skiljer domstolarnas verksamhet från de övrigas är att verksamheten till allra största delen är offentlig. Allmänheten har därmed mycket större möjligheter att få kännedom om de personer vilkas uppgifter behandlas. Tillgången till personnummer öppnar ytterligare möjligheter att få fram uppgifter om dem. Det kan enligt utredningens mening motivera en fortsatt reglering av hur personnummer och andra liknande identitetsbeteckningar får behandlas i domstolarnas verksamhet. Dessutom föreslås en liknande reglering på dataskyddsförordningens område (se 3 kap. 13 § lagen med kompletterande bestämmelser till EU:s dataskyddsförordning). Den utredare som övervägt anpassningar av domstolsdatalagen till dataskyddsförordningen anser att den bestämmelsen bör gälla för domstolarna (se Ds 2017:47 s. 130 f.). Det bör mot den bakgrunden tas in en bestämmelse som motsvarar 22 § personuppgiftslagen i den nya lagen.

Den omständigheten att det enbart är i domstolarnas registerförfattning som möjligheterna att behandla personnummer begränsas påverkar inte övriga myndigheters möjlighet att utbyta sådana personuppgifter med domstolarna. Det strukturerade informationsflödet i RIF-samarbetet som nämns i avsnitt 5.6.2 påverkas således inte. Bestämmelsen innebär endast att domstolen måste pröva behovet av att behandla personnummer och liknande identitetsbeteckningar så att de inte behandlas i onödan.

12.4.5 Behandling av biometriska och genetiska uppgifter

<p>Utredningens bedömning: Domstolarna bör inte få behandla biometriska och genetiska uppgifter.</p>

Skälen för utredningens bedömning: Biometriska uppgifter är enligt 1 kap. 6 § brottsdatalagen personuppgifter som rör en persons fysiska, fysiologiska eller beteendemässiga kännetecken, som tagits fram genom särskild teknisk behandling och som möjliggör eller bekräftar unik identifiering av personen i fråga. Genetiska uppgifter är enligt samma paragraf personuppgifter som rör en persons nedärvda eller förvärvade genetiska kännetecken och som härrör från analys av ett spår av eller ett prov från personen i fråga. Enligt 2 kap. 13 § brottsdatalagen utgör biometriska uppgifter som används för att identifiera en person och genetiska uppgifter känsliga personuppgifter. Sådana uppgifter får enligt 2 kap. 12 § brottsdatalagen endast behandlas om det är särskilt föreskrivet och det är absolut nödvändigt för ändamålet med behandlingen.

Det är svårt att se att domstolarna har något behov av att behandla biometriska och genetiska uppgifter och utredningen anser därför att det inte bör finnas någon bestämmelse som medger sådan behandling i domstolarnas brottsdatalog.

Det bör anmärkas att de personuppgifter som förekommer i ett utlåtande som baseras på en teknisk bearbetning av biometriska eller genetiska uppgifter inte i sig utgör sådana uppgifter. Domstolarna kommer alltså att kunna behandla personuppgifter i sådana utlåtanden i samma utsträckning som i dag.

12.5 Sökning

12.5.1 Sökförbudet i brottsdatalagen ska inte gälla

Utredningens förslag: Förbudet i brottsdatalagen mot sökning i syfte att få fram ett personurval grundat på känsliga personuppgifter ska inte gälla för domstolarna.

Skälen för utredningens förslag: I 2 kap. 11–13 §§ brottsdatalagen anges vilka uppgifter som betecknas som känsliga personuppgifter. I 2 kap. 14 § förbjuds sökning i syfte att få fram ett personurval grundat på känsliga personuppgifter. Förbudet kompletteras av en bestämmelse om absolut sekretess för sammanställningar grundade på känsliga personuppgifter.

Enligt 14 § domstolsdatalagen är det förbjudet att vid sökning i personuppgifter som sökbegrepp använda bl.a. känsliga personuppgifter. Regleringen omfattar även uppgifter om nationell anknytning och brott eller misstanke om brott, eftersom sökning med användande av sådana uppgifter har ansetts innebära särskilda risker i domstolarnas verksamhet. Från sökförbudet görs sedan vissa undantag i 14 § andra stycket och 15 §. Undantagen begränsas emellertid i 3–6 §§ domstolsdataförordningen (2015:729).

Regleringen av vilken sökning som är tillåten har utformats med beaktande av dels domstolarnas behov och intresset av insyn, dels skyddet för enskildas personliga integritet. I förarbetena konstateras att det inte är motiverat att begränsa endast domstolspersonalens möjligheter till sökning, om inte allmänhetens möjligheter att med stöd av offentlighetsprincipen begära sökning begränsas på motsvarande sätt. De största integritetsriskerna ligger inte i de sökningar som domstolens personal gör utan i de möjligheter till kartläggning som sökningar på begäran av allmänheten innebär (se prop. 2014/15:148 s. 53 f.). Någon särskild sekretessbestämmelse för sådana personuppgifter som sökningar kan resultera i finns inte, eftersom principiella skäl har ansetts tala mot att ha en sådan bestämmelse. Intresset av insyn och öppenhet anses vara särskilt starkt i domstolarna och det finns ett betydande värde i att både journalister och enskilda kan begära att avgöranden söks fram efter bestämda kriterier (se prop. 2014/15:148 s. 55 f.).

Utredningen bedömer mot den bakgrunden att sökförbudet i brottsdatalagen inte bör gälla för domstolarna utan att en annan, för den verksamheten särskilt anpassad, reglering bör gälla i stället.

12.5.2 Särskilda sökföbud

Utredningens förslag: Vid sökning i personuppgifter ska det vara förbjudet att som sökbegrepp använda uppgifter som avslöjar känsliga personuppgifter eller nationell anknytning.

I allmän domstol får sökbegrepp som avslöjar brott eller misstanke om brott inte användas vid sökning i personuppgifter i mål eller ärenden som har avgjorts slutligt genom en dom eller ett beslut längre än fem år efter utgången av det kalenderår då avgörandet fick laga kraft. Sådana sökbegrepp får inte heller användas vid sökning i tvistemål.

I allmän förvaltningsdomstol får sökbegrepp som avslöjar brott eller misstanke om brott inte användas vid sökning i personuppgifter i mål som har avgjorts slutligt genom en dom eller ett beslut längre än tjugو år efter utgången av det kalenderår då avgörandet fick laga kraft. Sådana sökbegrepp får inte heller användas i mål som handläggs av Migrationsöverdomstolen eller en migrationsdomstol.

Namn, personnummer, samordningsnummer och andra direkta personuppgifter får inte användas som sökbegrepp vid sökning i personuppgifter i brottmål som har avgjorts slutligt genom en dom eller ett beslut längre än fem år efter utgången av det kalenderår då avgörandet fick laga kraft.

Skälen för utredningens förslag

Nuvarande reglering

I 14 § domstolsdatalagen förbjuds som nyss nämnts användning av sökbegrepp som avslöjar känsliga personuppgifter, uppgifter om brott eller misstanke om brott eller nationell anknytning. Förbudet omfattar dock inte användning av särskilda beteckningar för identifiering av vissa mål- eller ärendetyper. Från förbudet undantas enligt 15 § sökning i en viss handling eller i ett visst mål eller ärende. Förbudet gäller inte heller i allmän domstol eller allmän förvaltningsdomstol, såvitt gäller sökbegrepp som avslöjar brott eller misstanke om brott, eller i allmän förvaltningsdomstol såvitt gäller sökbegrepp som avslöjar hälsa.

I 3–5 §§ domstolsdataförordningen begränsas möjligheten till sökning i äldre avgjorda mål och ärenden. Vidare förbjuds användning av sökbegrepp som avslöjar brott eller misstanke om brott i allmän domstol vid sökning i tvistemål och i Migrationsöverdomstolen och migrationsdomstolarna användning av sökbegrepp som avslöjar brott eller misstanke om brott eller hälsa. Det görs också undantag från sökförbuden vid sökning i viss handling eller i visst mål eller ärende.

Utgångspunkter för regleringen i den nya lagen

Den nuvarande regleringen tillgodoser både domstolarnas berättigade behov av att kunna utföra sökning på känsliga personuppgifter och andra integritetskänsliga uppgifter och skyddet för enskildas integritet. Den är enligt utredningens mening också en rimlig avvägning mellan domstolarnas behov och allmänhetens rätt till insyn. Det innebär att regleringen i domstolsdatalagen kan bilda utgångspunkt för regleringen i den nya lagen. Det bör dock övervägas om det finns skäl att ändra utformningen av bestämmelserna om sökning även om innehållet i sak blir detsamma.

Förbud att söka på vissa typer av personuppgifter är ett viktigt inslag i skyddet för enskildas integritet. Sådana bestämmelser bör finnas i lag. Argumentet för att reglera vissa begränsningar av möjligheten till sökning i domstolarnas verksamhet i förordning i stället för i lag har enligt utredningens mening inte samma tyngd när brottsdatalagen är tillämplig (jfr prop. 2014/15:148 s. 62 f.). Utredningen anser därför att sökförbuden bör regleras i den nya lagen. Regeringen eller den myndighet som regeringen bestämmer bör på samma sätt som i dag kunna meddela föreskrifter om användningen av sökbegrepp.

Sökförbud för känsliga personuppgifter

Enligt direktivet får känsliga personuppgifter behandlas bara om det är absolut nödvändigt och det finns särskilda skyddsåtgärder. Som framgår av delbetänkandet anser utredningen att sökförbudet i 2 kap. 14 § brottsdatalagen är en sådan skyddsåtgärd som direktivet kräver (se SOU 2017:29 s. 272). Eftersom sökförbudet i brotts-

datalagen inte ska gälla för domstolarna behövs det någon annan form av skyddsåtgärd i den nya lagen. En lämplig lösning är att på samma sätt som i dag förbjuda användningen av känsliga personuppgifter som sökbegrepp och att kombinera det med undantag. Genom en hänvisning till bestämmelserna om känsliga personuppgifter i brottsdatalagen kommer alla uppgifter som benämns känsliga personuppgifter att omfattas av förbudet.

Sökförbud för andra integritetskänsliga uppgifter

Sökförbudet i domstolsdatalagen gäller inte bara för känsliga personuppgifter utan även för vissa andra uppgifter som ansetts vara särskilt integritetskänsliga, nämligen uppgifter som avslöjar nationell anknytning och brott eller misstanke om brott. I motsats till regleringen i det nu gällande dataskyddsdirektivet och dataskyddsförordningen finns det inte några särskilda restriktioner för behandling av uppgifter om lagöverträdelser i det nya dataskyddsdirektivet. Uppgifter om nationell anknytning regleras inte heller. Något sökförbud som motsvarar 14 § första stycket punkterna 7 och 8 krävs därför inte för att genomföra direktivet. De skäl som ligger bakom att sökförbudet i domstolsdatalagen även omfattar sådana uppgifter har dock enligt utredningens mening alltjämt bärkraft. Direktivet tillåter nationella regler som ger starkare integritetsskydd. Även uppgifter om brott och misstanke om brott och om nationell anknytning bör därför omfattas av sökförbudet i den nya lagen.

När det gäller användningen av uppgifter som avslöjar brott eller misstanke om brott som sökbegrepp bör dock regleringen i den nya lagen inte utgå från domstolsdatalagens systematik som bygger på förbud och generella undantag.

Förbuden mot behandling bör motsvara de begränsningar som finns i domstolsdataförordningen. Det innebär för allmän domstol att sökbegrepp som avslöjar brott eller misstanke om brott inte bör få användas vid sökning i personuppgifter i tvistemål eller efter viss tid i andra mål och ärenden som är slutligt avgjorda. För allmän förvaltningsdomstol innebär det att sökbegrepp som avslöjar brott eller misstanke om brott inte bör få användas vid sökning i personuppgifter efter viss tid. Migrationsöverdomstolen och migra-

tionsdomstolarna bör på samma sätt som i dag överhuvudtaget inte få använda sådana sökbegrepp.

Förbud mot att använda direkta personuppgifter vid sökning

I 4 § domstolsdataförordningen förbjuds användning av namn, personnummer, samordningsnummer och andra uppgifter som direkt kan hänföras till en fysisk person som är i livet som sökbegrepp vid sökning i personuppgifter i brottmål som har avgjorts slutligt fem år efter utgången av det kalenderår då avgörandet fick laga kraft. De skäl som ligger bakom detta förbud har enligt utredningens mening alltså bärkraft. Direktivet ställer inga sådana krav men tillåter nationella regler som ger starkare integritetsskydd. En bestämmelse som motsvarar 4 § domstolsdataförordningen bör därför tas in i den nya lagen.

12.5.3 Tillåtna sökningar

Utredningens förslag: Sökförbuden hindrar inte sökning i en viss handling eller i ett visst mål eller ärende, eller med användande av särskilda beteckningar för identifiering av en viss mål- eller ärendetyp.

Sökförbuden hindrar inte att allmän förvaltningsdomstol använder uppgifter som avslöjar hälsa som sökbegrepp. Sådana uppgifter får dock inte användas vid sökning i personuppgifter i mål som har avgjorts slutligt genom en dom eller ett beslut längre än tjugo år efter utgången av det kalenderår då avgörandet fick laga kraft. Undantaget från sökförbudet ska inte heller gälla vid sökning i personuppgifter i mål som handläggs av Migrationsöverdomstolen eller en migrationsdomstol.

Skälen för utredningens förslag: Det behövs på samma sätt som i dag vissa undantag från sökförbuden. Domstolarna använder i stor utsträckning särskilda beteckningar för att identifiera vissa mål- eller ärendetyper, s.k. målgrupps- och måltypskoder. Av de skäl som anförs i förarbetena till domstolsdatalagen bör sökning

med användning av sådana beteckningar undantas från sökförbuden i den nya lagen (se prop. 2014/15:148 s. 63).

Sökförbuden bör på samma sätt som i dag inte heller gälla vid sökning i en viss handling eller i ett visst mål eller ärende. Som regeringen konstaterar i förarbetena innebär sökning bland en begränsad mängd uppgifter mindre integritetsrisker än sökning i större uppgiftsmängder (se prop. 2014/15:148 s. 63 f.). Det bör således göras undantag från sökförbuden även för sådana sökningar.

De allmänna förvaltningsdomstolarna får genom undantag i 15 § domstolsdatalagen använda uppgifter om hälsa som sökbegrepp. Det får dock inte göras tjugo år efter det kalenderår då det slutliga avgörandet i målet eller ärendet fick laga kraft. Ett motsvarande undantag bör finnas i den nya lagen. Det svarar mot domstolarnas behov av att kunna söka på sådana uppgifter. På samma sätt som i dag bör det undantaget emellertid inte omfatta sökningar i mål som handläggs av Migrationsöverdomstolen eller en migrationsdomstol (jfr prop. 2014/15:148 s. 59 f.).

Regeringen eller den myndighet som regeringen bestämmer bör på samma sätt som i dag kunna meddela föreskrifter om användningen av sökbegepp.

12.6 Utlämnande av personuppgifter

12.6.1 Direktåtkomst

Utredningens förslag: Direktåtkomst ska få medges

1. en allmän domstol,
2. en allmän förvaltningsdomstol, eller
3. en part eller partens ombud, biträde eller försvarare.

Direktåtkomst enligt punkten 3 får endast avse personuppgifter i partens mål eller ärende.

Begränsning av direktåtkomst och behörighet och säkerhet vid direktåtkomst ska regleras i förordning.

Skälen för utredningens förslag: Enligt 17 § domstolsdatalagen får direktåtkomst endast medges en allmän domstol, en allmän förvaltningsdomstol, en hyres- och arrendenämnd eller en part eller partens ombud, biträde eller försvarare. I 7–13 §§ domstolsdataförordningen preciseras när direktåtkomst är tillåten till äldre avgjorda mål och ärenden, vid överklagande, till rättspraxis och i samband med beredskapsverksamhet.

Reglerna om direktåtkomst i domstolsdatalagen och domstolsdataförordningen är resultatet av en avvägning mellan domstolarnas behov och skyddet för enskildas integritet. Den bedömning som gjordes i dessa avseenden vid domstolsdatalagens tillkomst har alltså bärkraft och regleringen i den nya lagen bör därför utformas på samma sätt. Det gäller även uppdelningen av bestämmelserna mellan lag och förordning (se prop. 2014/15:148 s. 64 f.).

Hyres- och arrendenämnderna bör inte kunna medges direktåtkomst enligt lagen. De ska som framgår av avsnitt 12.3.1 inte tillämpa lagen, eftersom de inte handlägger mål eller ärenden i något av de syften som lagen omfattar. Hyres- och arrendenämnderna har inte heller av något annat skäl behov av direktåtkomst till personuppgifter som behandlas med stöd av lagen.

Regeringen eller den myndighet som regeringen bestämmer bör på samma sätt som i dag kunna meddela föreskrifter om begränsning av direktåtkomsten och om behörighet och säkerhet vid sådan åtkomst.

12.6.2 Elektroniskt utlämnande

Utredningens förslag: Personuppgifter ska få lämnas ut elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt.

Begränsning av möjligheten att lämna ut personuppgifter på sådant sätt ska regleras i förordning.

Skälen för utredningens förslag: Enligt 16 § domstolsdatalagen får personuppgifter lämnas ut på medium för automatiserad behandling om det inte är olämpligt. Regeringen eller den myndighet som regeringen bestämmer kan meddela ytterligare föreskrifter om be-

gränsning av möjligheten att lämna ut personuppgifter på det sättet (se prop. 2014/15:148 s. 73 f.).

Varken brottsdatalagen eller direktivet innehåller bestämmelser om på vilket sätt personuppgifter får lämnas ut. Det finns inget som hindrar att nationell lagstiftning innehåller sådana bestämmelser. I avsnitt 5.6.4 föreslår utredningen att uttrycket utlämnande på medium för automatiserad behandling ska ersättas med elektroniskt utlämnande på annat sätt än genom direktåtkomst. Domstolarna bör enligt utredningens mening kunna lämna ut handlingar elektroniskt i samma utsträckning som i dag. En bestämmelse som motsvarar 16 § domstolsdatalagen bör därför tas in i den nya lagen och formuleras på samma sätt som i övriga registerförfattningar. Begränsning av möjligheten att lämna ut uppgifter på sådant sätt kan regleras i förordning.

12.7 Frågor om föreskriftsrätt

Utredningens förslag: Den myndighet som regeringen bestämmer ska få meddela föreskrifter om tillgången till personuppgifter, om begränsning av möjligheten att lämna ut personuppgifter elektroniskt och frågor som hör samman med det och om möjligheterna till sökning.

Innan myndigheten utfärdar föreskrifter i frågor som berör särskilda risker för intrång i den personliga integriteten ska den samråda med Datainspektionen. Det ska regleras i förordning.

Skälen för utredningens förslag

Föreskriftsrätt för Domstolsverket

I domstolsdatalagen finns det ett flertal bestämmelser där det anges att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter i en viss fråga.

När det gäller föreskriftsrätt skiljer sig regleringen för domstolarna från vad som gäller för övriga myndigheter i rättskedjan. I dag har Domstolsverket genom bestämmelser i domstolsdataförordningen rätt att utfärda föreskrifter som rör behandling av personuppgifter. Domstolarnas nuvarande verksamhetsstöd för handlägg-

ning av mål och ärenden, Vera, utvecklas och tillhandahålls av Domstolsverket i myndighetens egenskap av tekniskt serviceorgan åt domstolarna och är gemensamt för alla domstolar. Någon motsvarighet till den rollen finns inte för de andra myndigheterna i rättskedjan.

Domstolsverket har även i fortsättningen behov av att kunna meddela föreskrifter för domstolarna för att säkerställa att personuppgiftsbehandlingen i gemensamma it-system uppfyller författningskraven på bl.a. säkerhet. Föreskriftsrätten bör avse tillgång till personuppgifter, begränsning av möjligheten att lämna ut personuppgifter elektroniskt och frågor om behörighet och säkerhet vid sådant utlämnande. Föreskriftsrätten bör också omfatta begränsning av sökning och de ytterligare föreskrifter som behövs för verkställighet av den nya lagen och förordningen. Det innebär att Domstolsverket kommer att ha samma föreskriftsrätt som i dag.

Utredningen föreslår i avsnitt 5.3.9 att det ska tas in en generell bestämmelse i brottsdataförordningen som föreskriver att den personuppgiftsansvarige vid tilldelning av behörighet, utöver behovet av uppgifterna, särskilt ska beakta utbildning och erfarenhet. Den bestämmelsen ska tillämpas av domstolarna. Den är däremot inte tillämplig på Domstolsverket, eftersom verket inte är en behörig myndighet och inte heller personuppgiftsansvarig för behandlingen. Föreskriftsrätten bör därför på samma sätt som i dag kompletteras med motsvarande reglering om vad som ska beaktas vid tilldelning av behörighet.

Samråd inför utfärdande av föreskrifter

Som framgår av avsnitt 5.7 är de brottsbekämpande myndigheterna skyldiga att samråda med eller ge Datainspektionen tillfälle att yttra sig innan föreskrifter utfärdas i frågor som berör särskilda risker för intrång i den personliga integriteten. Domstolsverket som i dag har föreskriftsrätt enligt domstolsdataförordningen har ingen sådan samrådsskyldighet.

Även om Domstolsverket inte är personuppgiftsansvarig för behandling av personuppgifter som utförs enligt brottsdatalagen eller den nya lagen har verket genom sin föreskriftsrätt en roll som motsvarar t.ex. Åklagarmyndighetens när den utfärdar föreskrifter.

Därför bör även Domstolsverket vara skyldig att samråda med Datainspektionen innan verket meddelar sådana föreskrifter.

12.8 Administrativa sanktionsavgifter

Utredningens förslag: Sanktionsavgift ska få tas ut av den personuppgiftsansvarige vid överträdelse av bestämmelser om tillåten rättslig grund för behandling och om sökbegränsningar.

Sanktionsavgiften ska bestämmas till minst 50 000 kronor och högst 20 000 000 kronor.

Skälen för utredningens förslag: I delbetänkandet konstaterar utredningen att tillsyn kommer att kunna utövas över domstolarnas personuppgiftsbehandling men att regeringsformens skydd för självständigheten i dömande verksamhet ska beaktas. Till tillsynsmyndighetens befogenheter hör enligt 5 kap. 7 § första stycket 4 brottsdatalagen att kunna besluta om sanktionsavgift enligt 6 kap. brottsdatalagen. De överträdelser som enligt brottsdatalagen kan leda till att sanktionsavgift tas ut är bl.a. bestämmelser om hur personuppgifter får behandlas (se SOU 2017:29 s. 506 f.)

Reglerna om sanktionsavgift i brottsdatalagen gäller vid överträdelse av bestämmelser i den lagen. Som framgår av avsnitt 5.4.2 anser utredningen att sanktionsavgift också bör kunna tas ut vid överträdelse av vissa bestämmelser i registerförfattningarna. Det gäller bestämmelser som ersätter, preciserar eller kompletterar bestämmelser i brottsdatalagen som kan föranleda sanktionsavgift. Överträdelse av vissa bestämmelser i den nya lagen bör av samma skäl kunna föranleda sanktionsavgift.

Det som bör kunna föranleda sanktionsavgift är överträdelse av bestämmelser om tillåtna rättsliga grunder för behandling. Enligt brottsdatalagen är det möjligt att ta ut sanktionsavgift vid överträdelse av sökförbudet avseende känsliga personuppgifter. För domstolarna kommer dock det sökförbudet inte att gälla. Utredningen föreslår i stället i avsnitt 12.5 särskilda bestämmelser om sökförbud för domstolarna som inte bara gäller känsliga personuppgifter. Överträdelse av de bestämmelserna bör kunna leda till att sanktionsavgift tas ut. Det finns dock inte skäl att föreskriva att sanktionsavgift får tas ut om någon överträder bestämmelser om tillåtna

sökningar. Det beror på att en sådan sökning automatiskt blir en överträdelse av det generella sökförbudet, vilket kan föranleda sanktionsavgift. Det bör framgå av en bestämmelse i den nya lagen i vilka fall det är möjligt att ta ut sanktionsavgift.

Som konstateras i avsnitt 5.4.2 är de överträdelser som kan föranleda sanktionsavgift enligt registerförfattningarna av den arten att det är fråga om allvarligare överträdelser. Det gäller även de överträdelser som bör kunna leda till sanktionsavgift enligt den nya lagen. Sanktionsavgift bör därför tas ut med minst 50 000 kronor och högst 20 000 000 kronor. Sanktionsavgift bör av de skäl som anges i avsnitt 5.4.2 endast kunna tas ut av den personuppgiftsansvarige.

I 6 kap. 3 § tredje stycket, 4 och 5 §§ brottsdatalagen finns det bestämmelser om hur sanktionsavgiften ska bestämmas och i 6 kap. 6 och 7 §§ om vad som gäller i fråga om beslut om sanktionsavgift. Den nya lagen föreslås gälla utöver brottsdatalagen. Det innebär enligt utredningens mening att handläggnings- och verkställighetsreglerna i brottsdatalagen gäller även i de fall där sanktionsavgiften fastställs med stöd av en bestämmelse i den nya lagen. Några bestämmelser om handläggningen behövs därför inte.

12.9 Skadestånd

Utredningens förslag: Bestämmelsen om skadestånd i brottsdatalagen ska tillämpas på motsvarande sätt vid behandling av personuppgifter i strid med den nya lagen eller föreskrifter som har meddelats i anslutning till den.

Skälen för utredningens förslag: Enligt 7 kap. 1 § brottsdatalagen ska den personuppgiftsansvarige ersätta den registrerade för den skada och kränkning av den personliga integriteten som behandling av personuppgifter i strid med brottsdatalagen, eller föreskrifter som har meddelats i anslutning till den, har orsakat (SOU 2017:29 s. 532 f.).

Rätten till skadestånd vid skada och kränkning bör gälla även när personuppgifter behandlas i strid med det nya regelverket. Det bör därför framgå att 7 kap. 1 § brottsdatalagen ska tillämpas på motsvarande sätt vid behandling av personuppgifter i strid med den

nya lagen eller föreskrifter som har meddelats i anslutning till den (jfr avsnitt 5.4.3).

12.10 Överklagande

Utredningens förslag: I lagen ska det framgå att det finns bestämmelser om överklagande i brottsdatalagen.

Sådana beslut av en hovrätt, en tingsrätt eller en förvaltningsrätt, som får överklagas enligt brottsdatalagen, överklagas till kammarrätt. Beslut av en kammarrätt överklagas till Högsta förvaltningsdomstolen. Prövningstillstånd ska inte krävas.

Beslut som Högsta domstolen eller Högsta förvaltningsdomstolen fattar i egenskap av personuppgiftsansvarig får dock inte överklagas.

Skälen för utredningens förslag

Inga bestämmelser om överklagande i den nya lagen

Brottsdatalagen innehåller generella bestämmelser om överklagande. I 7 kap. 2 § brottsdatalagen föreskrivs att beslut i fråga om rättelse eller komplettering, radering eller begränsning av behandlingen av personuppgifter, som har meddelats av en myndighet i egenskap av personuppgiftsansvarig, får överklagas till allmän förvaltningsdomstol. Detsamma gäller beslut att inte lämna information på begäran av en registrerad, att ta ut avgift för att lämna information eller att inte medge omprövning av ett automatiserat beslut. I 7 kap. 3 § finns en särskild bestämmelse om dröjsmålstalan. Även beslut med stöd av den paragrafen får överklagas. Enligt 7 kap. 4 § får tillsynsmyndighetens beslut enligt lagen eller enligt föreskrifter som har meddelats i anslutning till den överklagas till allmän förvaltningsdomstol. I 7 kap. 5 § föreskrivs att andra beslut än de nu nämnda inte får överklagas (se SOU 2017:29 s. 537 f.).

I 19–22 §§ domstolsdatalagen finns det bestämmelser om överklagande. I avsnitt 5.4.4 konstaterar utredningen att det inte längre behövs några bestämmelser om överklagande i de övriga registerförfattningarna. Det beror på att frågan om vilka beslut som har fattats av de behöriga myndigheterna i egenskap av personuppgifts-

ansvariga som får överklagas regleras uttömmande i brottsdatalagen. Den nya lagen bör av samma skäl inte reglera möjligheterna att överklaga. Av tydlighetsskäl bör det dock finnas en hänvisning till brottsdatalagens bestämmelser om överklagande.

En särskild instansordning

Enligt 7 kap. 2 § brottsdatalagen ska som nyss nämnts beslut som en myndighet fattar i egenskap av personuppgiftsansvarig överklagas till allmän förvaltningsdomstol. För att förhindra att förvaltningsdomstolarna överprövar sina egna beslut eller högre instansers beslut behövs det en särskild regel om instansordningen i den nya lagen. På samma sätt som i dag bör en förvaltningsrätts beslut överklagas till kammarrätt och en kammarrätts beslut till Högsta förvaltningsdomstolen. Beslut av en tingsrätt eller en hovrätt bör också överklagas till kammarrätt (jfr prop. 2014/15:148 s. 93 f.). Kammarrätten blir därmed första instans. Något krav på prövningstillstånd bör därför inte gälla (se prop. 2014/15:148 s. 94). Den särskilda instansordningen bör framgå av den nya lagen. Av tydlighetsskäl bör det också framgå att beslut som Högsta domstolen eller Högsta förvaltningsdomstolen har fattat i egenskap av personuppgiftsansvarig inte får överklagas.

12.11 Övergångsbestämmelser

Utredningens förslag: Begränsningar avseende sökning och direktåtkomst i fråga om slutligt avgjorda mål och ärenden behöver inte tillämpas förrän den 1 januari 2019.

Skälen för utredningens förslag: I 3–5 och 13 §§ domstolsdataförordningen begränsas möjligheten till sökning i och direktåtkomst till slutligt avgjorda mål och ärenden. Till dem finns det övergångsbestämmelser i punkten 2 som föreskriver att bestämmelserna om sökbegränsning och direktåtkomst till slutligt avgjorda mål och ärenden ska tillämpas första gången den 1 januari 2019.

Utredningen föreslår motsvarande reglering i avsnitt 12.5.2, 12.5.3 och 12.6.1. Frågan är om det bör finnas övergångsbestäm-

meler till den nya regleringen som motsvarar dem som finns i punkten 2 .

Enligt uppgift från Domstolsverket finns det fortfarande behov av övergångsbestämmelser för att verksamhetsstöden ska hinna anpassas. Det finns inget som hindrar att övergångsbestämmelser till bestämmelserna om sökning tas in i den nya lagen, eftersom direktivet inte ställer några krav på sökbegränsning. Detsamma gäller övergångsbestämmelser om direktåtkomst. Det bör därför tas in motsvarande övergångsbestämmelser i den nya regleringen.

Behovet av övergångsbestämmelser i övrigt och frågan om ikraftträdande behandlas i kapitel 18.

13 Lagen om behandling av personuppgifter inom kriminalvården

13.1 Lagen om behandling av personuppgifter inom kriminalvården behöver anpassas

13.1.1 Lagens nuvarande struktur

I kriminalvården ingår myndigheten Kriminalvården och övervakningsnämnderna. Lagen om behandling av personuppgifter inom kriminalvården gäller enligt 1 § vid behandling av personuppgifter i kriminalvårdens verksamhet i fråga om vissa personkategorier, bl.a. den som är föremål för personutredning, häktad eller dömd till fängelse, skyddstillsyn eller villkorlig dom med föreskrift om samhällstjänst. Kriminalvården får enligt 3 § behandla personuppgifter bara om det behövs för vissa särskilt angivna ändamål, däribland att fullgöra sina uppgifter i enlighet med vad som föreskrivs i lag eller förordning och att underlätta tillgången till sådana uppgifter om verkställighet av påföljd eller häktning som rättsväsendets övriga myndigheter behöver.

Lagen, som enligt 2 § gäller utöver personuppgiftslagen, innehåller även bestämmelser om personuppgiftsansvar (4 §), behandling av känsliga personuppgifter (5 §), direktåtkomst (6 §), gallring (7 §) och utlämnande av uppgifter för rättsstatistiken (9 §). I fråga om rättelse och skadestånd gäller personuppgiftslagens bestämmelser (8 §). Lagen innehåller särskilda bestämmelser om omprövning och överklagande (12–16 §§). Merparten av regleringen finns emellertid i förordningen (2001:682) om behandling av personuppgifter inom kriminalvården.

Även annan reglering av personuppgiftsbehandling är i viss utsträckning tillämplig i Kriminalvården. Det gäller bl.a. patientdatalagen (2008:355), som gäller när Kriminalvården bedriver hälso- och sjukvård.

13.1.2 En omodern lagstiftning

Kriminalvårdens lagstiftning avviker i många avseenden från den modernare lagstiftning som gäller för övriga myndigheter i rättskedjan. De andra registerförfattningarna har tillkommit under de senaste åren, medan kriminalvårdens registerlagstiftning tillkom bara några år efter personuppgiftslagen. Den har inte setts över materiellt sedan dess.

Kriminalvårdens lagstiftning har en annan lagteknisk struktur än övriga registerförfattningar. Den gäller utöver personuppgiftslagen. Lagen är inte som de andra registerförfattningarna indelad i kapitel och består endast av 16 paragrafer. Större delen av regleringen finns i stället i den till lagen hörande förordningen. Den ordningen kan ifrågasättas mot bakgrund av det utökade grundlagsskyddet i 2 kap. 6 § andra stycket regeringsformen. Grundlagsskyddet tar sikte på integritetsintrång i form av övervakning och kartläggning som görs utan samtycke. Det ligger i sakens natur att viss verksamhet på häkten och kriminalvårdsanstalter kan omfattas av grundlagsskyddet, t.ex. teknisk övervakning eller registrering av personuppgifter. Det är dock endast betydande intrång som omfattas av grundlagsskyddet (se En reformerad grundlag, prop. 2009/10:80, s. 171 f.). Vad det närmare innebär är inte helt klart. I förarbetena pekas bl.a. på att myndighetsregister med ett stort antal registrerade och särskilt känsligt innehåll normalt ska regleras i lag (se prop 2009/10:80 s. 183). Det krävs därför en närmare bedömning av i vilken utsträckning de register som Kriminalvården för i dag kan fortsätta att i sin helhet regleras i förordning. Utredningen återkommer till det i avsnitt 13.4.

Under de mer än 15 år som förflutit efter tillkomsten av kriminalvårdens registerlagstiftning har förutsättningarna för verksamheten på häkten och kriminalvårdsanstalter förändrats avsevärt. Brottsligheten har ändrat karaktär. Ändringarna i påföljdsystemet, särskilt möjligheten att avtjäna fängelsestraff med fotboja, medför

att de som verkställer fängelsestraff i anstalt i dag generellt sett avtjänar straff för tyngre kriminalitet än förr. Även demografiska faktorer påverkar hur verksamheten på häkten och i kriminalvårdsanstalter bedrivs. Kriminalvården måste t.ex. vid placering av intagna ta större hänsyn än tidigare till sådana faktorer som organiserad brottslighet och tillhörighet till olika kriminella grupperingar.

Vidare har synen på hur registerlagstiftning för myndigheterna inom rättskedjan bör utformas och vad som bör regleras i lag respektive förordning ändrats. Modernare registerlagstiftning bygger inte i samma utsträckning på en detaljerad uppräkningslista av vilka personuppgifter som får behandlas.

Mot den bakgrunden behöver kriminalvårdens registerlagstiftning enligt utredningens mening ses över och moderniseras. Det finns t.ex. fördelar om den kan ges en struktur och ett innehåll som i större utsträckning liknar övriga registerförfattningar, vilket utvecklas i avsnitt 13.4.2. Även om utredningen nu föreslår vissa förändringar som ett led i anpassningen till brottsdatalagen, krävs det en total översyn av kriminalvårdens registerlagstiftning för att kriminalvården ska kunna behandla personuppgifter på ett ändamålsenligt sätt. Utredningen föreslår därför ingen ny lag, trots att alla bestämmelser ändras och lagen får en ny utformning.

I kapitel 4 behandlas behovet av ändringar i myndigheternas registerförfattningar. Anpassningar och ändringar som är gemensamma för registerförfattningarna behandlas i kapitel 5. De ytterligare ändringar som bör göras i lagen om behandling av personuppgifter inom kriminalvården med tillhörande förordning behandlas i detta kapitel.

En annan utredare har i uppdrag att anpassa den del av kriminalvårdens registerlagstiftning som ligger utanför brottsdatalagens tillämpningsområde till dataskyddsförordningen (Ju 2016:G).

13.1.3 Två olika registerlagar för kriminalvården

Utredningens förslag: Lagen och förordningen om behandling av personuppgifter inom kriminalvården ska bara innehålla bestämmelser om personuppgiftsbehandling inom brottsdatalagens tillämpningsområde. De ska benämnas kriminalvårdens brottsdatalag respektive kriminalvårdens brottsdataförordning.

Skälen för utredningens förslag

Den nuvarande regleringen renodlas

Lagen om behandling av personuppgifter inom kriminalvården reglerar huvudsakligen personuppgiftsbehandling inom brottsdatalagens tillämpningsområde, men även till viss del inom dataskyddsförordningens. Utredningen redovisar i delbetänkandet sin syn på när brottsdatalagen är tillämplig på verksamhet inom kriminalvården (se SOU 2017:29 s. 191 f., 214 f. och 217 f.). Om man skulle behålla en samlad reglering för kriminalvårdens personuppgiftsbehandling skulle den därför till största delen gälla utöver brottsdatalagen, men skulle i övrigt komplettera dataskyddsförordningen med tillhörande lagstiftning. Ett alternativ är att dela upp regleringen i två separata regelverk – ett för brottsdatalagens tillämpningsområde och ett för dataskyddsförordningens. Som anges i avsnitt 9.1.2 är strukturen med olika registerförfattningar för en myndighets olika verksamheter ingen nyhet.

Den nya dataskyddsregleringen gör det nödvändigt att dela upp regleringen av kriminalvårdens personuppgiftsbehandling på ett annat sätt än i dag. Det skulle i och för sig vara möjligt att göra alla nödvändiga ändringar i den befintliga regleringen. Lösningen med två separata regleringar blir emellertid enligt utredningens mening tydligare och lättare att tillämpa. Den del av kriminalvårdens personuppgiftsbehandling som ligger inom brottsdatalagens tillämpningsområde bör regleras i den befintliga registerförfattningen eftersom den till största delen rör häktning och straffverkställighet. De bestämmelser i kriminalvårdens registerförfattningar som tar sikte på frågor som ligger utanför brottsdatalagens tillämpningsområde bör därför upphävas. Utredningen har samrått om den lösningen med den utredare som har i uppdrag att anpassa kriminalvårdens registerförfattningar till dataskyddsförordningen.

Registerförfattningen ges ett nytt namn

Eftersom endast den del av kriminalvårdens personuppgiftsbehandling som ligger inom brottsdatalagens tillämpningsområde ska regleras i lagen om behandling av personuppgifter inom kriminalvården, bör det övervägas om namnet på lagen ska bytas. Av de skäl

som anges i avsnitt 7.1.2 finns det anledning att byta namn på registerförfattningarna inom brottsdatalagens tillämpningsområde. Namnet bör knyta an till hur brottsdatalagen benämns. Det bör vara kort och ange för vem författningen gäller och vad den rör.

Övriga registerförfattningar föreslås få namn där ordet brottsdatalag ingår. En nackdel med det är att det då inte framgår att lagen gäller för behandling av personuppgifter vid straffverkställighet. Det är kriminalvårdens huvudsakliga arbetsuppgift, men som utredningen konstaterar i delbetänkandet består den i att verkställa påföljder för brott (se SOU 2017:29 s. 142 f.). Den tydliga kopplingen mellan straffverkställighet och brott gör att namnet brottsdatalag inte blir missvisande. Fördelen med ett namn som följer samma systematik som övriga registerförfattningar uppväger nackdelen med att namnet inte helt återspeglar lagens tillämpningsområde. Utredningen föreslår därför att lagen ska benämnas kriminalvårdens brottsdatalag. Förordningen som kompletterar lagen bör då benämnas kriminalvårdens brottsdataförordning.

Eftersom lagens och förordningens namn ändras måste alla hänvisningar till dem i andra författningar ändras.

13.2 Allmänna bestämmelser

13.2.1 Tillämpningsområdet

Utredningens förslag: Lagen ska gälla utöver brottsdatalagen när någon av myndigheterna inom kriminalvården i egenskap av behörig myndighet behandlar personuppgifter i syfte att verkställa häktning eller straffrättsliga påföljder eller biträda en annan behörig myndighet när den utför arbetsuppgifter för något av de syften som anges i brottsdatalagen.

Skälen för utredningens förslag

Den nuvarande regleringen behöver anpassas

I avsnitt 4.4.1 tar utredningen ställning till att registerförfattningarna även i fortsättningen ska innehålla bestämmelser om tillämpningsområdet och anger övergripande vad som bör gälla för den

regleringen. Vidare föreslår utredningen i avsnitt 5.2 att registerförfattningarna ska gälla utöver brottsdatalagen.

Enligt 1 § lagen om behandling av personuppgifter inom kriminalvården gäller lagen vid behandling av personuppgifter i kriminalvårdens verksamhet i fråga om personer som är föremål för personutredning, som är häktade eller som är dömda till fängelse, skyddstillsyn eller villkorlig dom med föreskrift om samhällstjänst, som är ålagda fängelse som förvandlingsstraff för böter eller vite, som på grund av utländsk dom ska verkställa nämnda påföljder i Sverige, som på annan grund är intagna i häkte eller kriminalvårdsanstalt eller som annars transporteras av kriminalvårdens transporttjänst.

Tillämpningsområdet utgår i dag alltså från att personuppgiftsbehandlingen ska avse en person i någon av de uppräknade kategorierna. Den utformningen är inte förenlig med regleringen i brottsdatalagen, eftersom det är syftet med personuppgiftsbehandlingen som är avgörande för vilket regelverk som ska tillämpas, inte om personen tillhör en viss kategori. Regleringen kan därför inte bygga enbart på en uppräkning av personkategorier. Uppräkningar av det slaget hör inte heller hemma i en modern registerförfattning. Tillämpningsområdet bör i stället utgå från syftet med personuppgiftsbehandlingen. Det bör också framgå att lagen endast gäller när myndigheterna agerar i egenskap av behöriga myndigheter, eftersom det är en viktig avgränsning för tillämpningsområdet (se SOU 2017:29 s. 159 f.).

Personuppgiftsbehandling vid verkställighet av häktning och straffrättsliga påföljder

En av Kriminalvårdens huvuduppgifter är enligt 1 § förordningen (2007:1172) med instruktion för Kriminalvården att verkställa utdömda påföljder. Det som avses är verkställighet av fängelsestraff och vissa frivårdspåföljder. Personuppgiftsbehandling för sådana syften bör därför omfattas av tillämpningsområdet

Enligt 2 § instruktionen ska Kriminalvården verka för att påföljder verkställs på ett säkert sätt och att återfall i brott förebyggs. Kriminalvården ska särskilt vidta åtgärder som syftar till att brottslighet under verkställigheten förhindras. Enligt 3 § första stycket 3 lagen om behandling av personuppgifter inom kriminalvården får

Kriminalvården behandla personuppgifter om det behövs för att upprätthålla säkerheten och förebygga brott under häktning och verkställighet av påföljder. Personuppgiftsbehandling för sådana syften bör även i fortsättningen omfattas av tillämpningsområdet.

En annan av Kriminalvårdens huvuduppgifter är enligt 1 § instruktionen att bedriva häktesverksamhet. Utredningen konstaterar i delbetänkandet att brottsdatalagen ska tillämpas vid behandling av personuppgifter avseende den som är anhållen eller häktad för brott (se SOU 2017:29 s. 191 f.). Detsamma gäller den som är häktad efter dom i avvaktan på att domen får laga kraft och vid häktning för att hindra att den dömda undandrar sig verkställighet av beslut om utvisning på grund av brott. Lagen ska också tillämpas på den som är omhändertagen efter beslut enligt 26 kap. 22 § och 28 kap. 6 b § brottsbalken och förvaras i häkte. Personuppgiftsbehandling i syfte att verkställa häktning bör därmed också omfattas av tillämpningsområdet. Verkställighet av häktning för syften som ligger utanför brottsdatalagens tillämpningsområde bör dock inte omfattas av tillämpningsområdet. All förvaring i häkte och alla transporter som Kriminalvården utför bör inte omfattas, utan enbart sådana åtgärder för ändamål inom brottsdatalagens tillämpningsområde.

Övervakningsnämnderna prövar vissa frågor om verkställighet utanför anstalt enligt fängelselagen (2010:610). Nämnderna har även uppgifter som rör verkställigheten av skyddstillsyn. När övervakningsnämnderna hanterar personuppgifter för sådana syften görs det inom ramen för straffverkställighet och bör därför omfattas av tillämpningsområdet.

Personuppgiftsbehandling vid biträde åt andra behöriga myndigheter

Kriminalvården ansvarar för att utföra personutredningar i brottmål. I lagen (1991:2041) om särskild personutredning i brottmål, m.m. föreskrivs att Kriminalvården dels ska genomföra sådan utredning om en misstänkts personliga förhållanden som krävs för att domstolen ska kunna avgöra påföljdsfrågan, dels ska avge yttranden som belyser återfallsrisken. När Kriminalvården genomför en personutredning eller avger ett yttrande görs det primärt för att det ska finnas ett tillräckligt underlag för att kunna lagföra någon för

brott. Vid personutredning kan Kriminalvården sägas biträda framför allt domstolarna vid lagföring av brott.

Enligt överenskommelse med Polismyndigheten driver Kriminalvården Polismyndighetens arrestverksamhet på vissa platser i landet. I sådan verksamhet får Kriminalvården anses biträda Polismyndigheten i dess brottsbekämpande och ordningshållande verksamhet.

Kriminalvården bedriver även transporttjänst. När t.ex. häktade transporteras till och från häkten i samband med domstolsförhandlingar biträder Kriminalvården åklagare och domstolar vid brottsbekämpning och lagföring. När personer transporteras från häkten till kriminalvårdsanstalter eller mellan kriminalvårdsanstalter görs det inom ramen för straffverkställigheten. Transporter som inte görs för lagföring eller straffverkställighet utan med stöd av t.ex. tvångsvårdslagstiftningen eller utlänningslagstiftningen, ligger däremot utanför tillämpningsområdet (se SOU 2017:29 s. 194).

Kriminalvården ansvarar vidare för den som av domstol eller övervakningsnämnd har omhändertagits med stöd av 28 kap. 11 § brottsbalken och som förvaras i häkte. Kriminalvården biträder i dessa fall andra behöriga myndigheter vid verkställighet av påföljd. Lagens tillämpningsområde bör därför även omfatta behandling av personuppgifter vid Kriminalvårdens biträde åt andra behöriga myndigheter för något syfte inom brottsdatalogens tillämpningsområde.

13.2.2 Personuppgiftsansvar

Utredningens förslag: Kriminalvården ska vara personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför.

En övervakningsnämnd ska vara personuppgiftsansvarig för den personuppgiftsbehandling som nämnden utför.

Skälen för utredningens förslag: Enligt 4 § lagen om behandling av personuppgifter inom kriminalvården är Kriminalvården personuppgiftsansvarig. Bestämmelsen fick sin nuvarande utformning i samband med att Kriminalvården blev en myndighet (se Kriminalvården – en myndighet, prop. 2004/05:176, s. 76). Det bör enligt

utredningens mening även i fortsättningen framgå av lagen att Kriminalvården är personuppgiftsansvarig för den personuppgiftsbehandling som myndigheten utför.

Övervakningsnämnderna ska som framgår av avsnitt 13.2.1 tillämpa lagen. Det finns i dag 28 övervakningsnämnder. De är fristående myndigheter och har en domstolsliknande funktion. För övervakningsnämnderna gäller förordningen (2007:1174) med instruktion för övervakningsnämnderna. I dag är det oklart vilken myndighet som är personuppgiftsansvarig för den personuppgiftsbehandling som utförs av en övervakningsnämnd. Med hänsyn till vikten av att det finns ett tydligt regelverk som anger vem som är ansvarig för personuppgiftsbehandlingen är det inte godtagbart. Det är enligt utredningens mening inte lämpligt att Kriminalvården ansvarar för den personuppgiftsbehandling som utförs av övervakningsnämnderna, eftersom de är fristående myndigheter. Det bör därför framgå av lagen att varje övervakningsnämnd är personuppgiftsansvarig för sin personuppgiftsbehandling.

Den omständigheten att övervakningsnämnderna blir personuppgiftsansvariga hindrar inte att de samarbetar med Kriminalvården, t.ex. på det sättet att Kriminalvården kan vara personuppgiftsbiträde åt nämnderna. Möjligheten att utse ett gemensamt data-skyddsombud kan också övervägas (se SOU 2017:29 s. 342 f.).

13.3 Grundläggande bestämmelser om behandling

13.3.1 Tillåtna rättsliga grunder och behandling för nya ändamål

Utredningens förslag: Personuppgifter ska få behandlas om det är nödvändigt för att utföra en arbetsuppgift i syfte att

1. verkställa häktning eller straffrättsliga påföljder,
2. förebygga, förhindra eller upptäcka brottslig verksamhet i samband med sådan verkställighet,
3. biträda andra myndigheter när de fullgör arbetsuppgifter för något av de syften som anges i brottsdatalagen, eller
4. fullgöra förpliktelser som följer av internationella åtaganden.

Arbetsuppgiften ska framgå av en bindande unionsrättsakt eller av en lag, en förordning eller ett särskilt beslut i vilket regeringen uppdragit åt kriminalvården att ansvara för en sådan uppgift.

Det ska framgå genom en hänvisning att personuppgifter som behandlas med stöd av lagen ska få behandlas för nya ändamål enligt de förutsättningar som anges i brottsdatalagen.

Skälen för utredningens förslag

Den nuvarande regleringen behöver anpassas

Enligt 2 kap. 1 § brottsdatalagen får personuppgifter behandlas om det är nödvändigt för att en behörig myndighet ska kunna utföra en arbetsuppgift i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet.

Enligt 3 § lagen om behandling av personuppgifter inom kriminalvården får kriminalvården behandla personuppgifter om det behövs för att myndigheten ska kunna fullgöra sina uppgifter i enlighet med vad som föreskrivs i lag eller förordning, underlätta tillgången till sådana uppgifter om verkställighet av påföljd eller häktning som rättsväsendets myndigheter behöver eller upprätthålla säkerheten och förebygga brott under den tid som en åtgärd enligt 1 § första stycket 2–9 pågår. Hänvisningen avser tid under vilken någon är häktad eller avtjänar ett fängelsestraff, verkställer en frivårdande påföljd i form av villkorlig dom med föreskrift om samhällstjänst eller skyddstillsyn, är ålagd fängelse som förvandlingsstraff för böter eller vite eller på grund av utländsk dom verkställer någon av nämnda påföljder i Sverige, på annan grund är intagen i häkte eller kriminalvårdsanstalt eller annars transporteras av Kriminalvårdens transporttjänst. De personuppgifter som kriminalvården får behandla får också behandlas om det behövs för tillsyn, planering, uppföljning och kvalitetssäkring av verksamheten.

Som anges i avsnitt 6.3.1 bör de brottsbekämpande myndigheternas registerförfattningar innehålla bestämmelser om tillåtna rättsliga grunder för behandling av personuppgifter. Det bör även gälla för kriminalvården.

En bestämmelse som ersätter brottsdatalagens bestämmelse om tillåtna rättsliga grunder för behandling

Kriminalvårdens brottsdatalag bör alltså innehålla en bestämmelse om tillåtna rättsliga grunder för behandling av personuppgifter som ger kriminalvården rättsligt stöd för att behandla personuppgifter automatiserat för att utföra sina arbetsuppgifter (jfr avsnitt 6.1.2).

I avsnitt 13.2.1 föreslår utredningen att tillämpningsområdet ska omfatta behandling av personuppgifter vid verkställighet av häktning eller straffrättsliga påföljder. Det bör framgå av lagen att personuppgifter får behandlas för de syftena. Det omfattar även behandling av personuppgifter som rör säkerheten vid verkställighet, exempelvis frågor om en intagen medför förhöjd risk för rymning eller fritagning och vem som besöker den häktade eller intagne.

Personuppgifter bör även få behandlas när Kriminalvården biträder andra behöriga myndigheter vid brottsbekämpning, lagföring, verkställighet av straffrättsliga påföljder eller upprätthållande av allmän ordning och säkerhet. Vad sådant biträde kan innebära redovisas i avsnitt 13.2.1. I biträdet ingår att ge rättsväsendets myndigheter information om häktesverksamheten och verkställigheten av påföljder och att tillhandahålla de personuppgifter som behövs för att andra myndigheter ska kunna fullgöra arbetsuppgifter inom brottsdatalagens tillämpningsområde. Ett exempel på det förstnämnda är information till åklagare och domstolar som rör häktade och på det sistnämnda den information som Kriminalvården ger Polismyndigheten om avslutade vårdvistelser. Kriminalvården bör därför få behandla personuppgifter om det är nödvändigt för att biträda en annan behörig myndighet för något av de syften som anges i brottsdatalagen.

Kriminalvården har vissa internationella förpliktelser, bl.a. att under vissa förutsättningar ta över verkställigheten av en utländsk frivårdspåföljd eller ett utländskt fängelsestraff och att förvara personer som är föremål för transitering genom Sverige för verkställighet av fängelsestraff i annat land. Fullgörande av internationella förpliktelser bör därför vara en tillåten rättslig grund för Kriminalvårdens personuppgiftsbehandling (jfr bl.a. 2 kap. 7 § polisdatalagen, 2 kap. 5 § skattebrottsdatalagen och 2 kap. 5 § tullbrottsdatalagen).

Kriminalvårdens brottsdatalag föreslås i avsnitt 5.2 gälla utöver brottsdatalagen. För att det inte ska råda någon osäkerhet om hur bestämmelsen i 2 kap. 1 § brottsdatalagen förhåller sig till bestämmelsen om tillåtna rättsliga grunder i registerförfattningen bör den senare helt ersätta den i brottsdatalagen. Av bestämmelsen bör det därför på samma sätt som i brottsdatalagen framgå att den arbetsuppgift som kriminalvården ska utföra ska framgå av en bindande unionsrättsakt eller en lag, en förordning eller ett särskilt beslut i vilket regeringen uppdragit åt myndigheten att ansvara för en sådan uppgift. Vad det innebär utvecklas i delbetänkandet (se SOU 2017:29 s. 238 f.).

Särskilt om Kriminalvårdens brottsförebyggande arbete

Enligt 2 § myndighetens instruktion ska Kriminalvården särskilt vidta åtgärder som syftar till att brottslighet under verkställigheten förhindras, frigivningen förbereds, narkotikamissbruket bekämpas och innehållet i verkställigheten anpassas efter varje individs behov. Arbetet med att förebygga och förhindra att brott begås av den som verkställer straff är enligt utredningens mening en viktig del i straffverkställigheten. Fokus är att förhindra både att brott planeras eller begås under verkställigheten och att de intagna återfaller i brott senare. Andra viktiga frågor är att förhindra att narkotika förekommer på häkten och i kriminalvårdsanstalter och att hindra rymning och fritagning.

Det bör emellertid framhållas att Kriminalvården varken har särskilda arbetsuppgifter eller befogenheter på området, utöver rätten att ta hand om och förstöra narkotika som påträffas på häkten och i kriminalvårdsanstalter. Det brottsförebyggande arbetet består därför i åtgärder som Kriminalvården vidtar eller beslutar om under själva verkställigheten, även om syftet är att förebygga att den häktade eller intagne begår brott efter frigivning eller avslutad straffverkställighet. Kriminalvården har således inte någon arbetsuppgift som syftar till brottsbekämpning som inte har att göra med häktesverksamheten eller verkställighet av straff.

Kriminalvården behöver kunna behandla personuppgifter för den brottsförebyggande verksamheten. Det bör därför framgå av lagen att Kriminalvården har rätt att behandla uppgifter för att

förebygga, förhindra eller upptäcka brottslig verksamhet i samband med verkställighet av häktning eller straffrättsliga påföljder.

Kriminalvårdens forsknings- och statistikverksamhet

Kriminalvården ansvarar i dag för underlaget till en stor del av den samlade rättsstatistiken. Myndigheten har även för sin egen verksamhet behov av omfattande statistik. Dessutom bedriver Kriminalvården sedan länge viss forskning som rör framför allt verkställighet av straffrättsliga påföljder. Enligt 2 kap. 5 § brottsdatalagen får en behörig myndighet behandla personuppgifter för vetenskapliga, statistiska eller historiska ändamål inom lagens tillämpningsområde (se SOU 2017:29 s. 253 f.). Kriminalvårdens statistik- och forskningsverksamhet är ett led i arbetsuppgifter som ligger inom brottsdatalagens tillämpningsområde. Den rättsliga grunden i kriminalvårdens brottsdatalag täcker därmed även behandling av personuppgifter för sådana syften.

Behandling för nya ändamål

Kriminalvårdens registerförfattning reglerar inte när personuppgifter får behandlas för nya ändamål. Det styrs i stället av finalitetsprincipen i personuppgiftslagen.

I brottsdatalagen regleras förutsättningarna för att personuppgifter ska få behandlas för nya ändamål. Enligt 2 kap. 4 § brottsdatalagen ska den som överväger att behandla personuppgifter för ett nytt ändamål göra en prövning av om behandlingen är nödvändig och proportionerlig innan uppgifterna får behandlas för nya ändamål inom lagens tillämpningsområde. Utredningen föreslår att samma prövning ska göras när de brottsbekämpande myndigheterna behandlar personuppgifter för nya ändamål utanför tillämpningsområdet (se avsnitt 6.4.3). En sådan prövning utgör enligt utredningens mening en lämplig avvägning mellan mottagarens behov av personuppgifterna och skyddet för enskildas personliga integritet även i kriminalvården. Samma prövning bör göras av kriminalvården innan personuppgifter behandlas för ett nytt ändamål utanför brottsdatalagens tillämpningsområde. Det bör införas en bestämmelse i kriminalvårdens brottsdatalag som tydliggör att förut-

sättningarna för att behandla personuppgifter, som behandlas med stöd av den lagen, för nya ändamål regleras i brottsdatalagen.

13.3.2 Behandling av biometriska och genetiska uppgifter

Utredningens förslag: Kriminalvården ska få behandla biometriska uppgifter enligt de förutsättningar som anges i brottsdatalagen.

Utredningens bedömning: Kriminalvården bör inte få behandla genetiska uppgifter.

Skälen för utredningens förslag och bedömning: I avsnitt 7.3.2 redovisas vad som avses med biometriska och genetiska uppgifter. Enligt 2 kap. 12 § brottsdatalagen får sådana uppgifter behandlas endast om det är särskilt föreskrivet och det är absolut nödvändigt för ändamålet med behandlingen.

I dag behandlar Kriminalvården varken biometriska eller genetiska uppgifter. Det pågår emellertid utveckling av teknik för att med hjälp av biometri möjliggöra säkrare identifiering vid exempelvis transporter inom en kriminalvårdsanstalt. På samma sätt som för polisen och Tullverket är det viktigt för Kriminalvården att den rättsliga regleringen inte hämmar eller hindrar utvecklingen och användningen av ny teknik (jfr avsnitt 7.3.2). Även om Kriminalvården i dagsläget inte använder biometri anser utredningen att myndigheten bör ges rättslig möjlighet att behandla biometriska uppgifter, eftersom det inom en snar framtid kommer att finnas behov av det. Utredningen bedömer att det för närvarande inte finns skäl att begränsa möjligheten att behandla biometriska uppgifter utöver vad som föreskrivs i brottsdatalagen. Det bör därför införas en bestämmelse i kriminalvårdens brottsdatalag som medger behandling av biometriska uppgifter enligt de förutsättningar som anges i brottsdatalagen.

Det har inte framkommit att Kriminalvården har behov av att behandla genetiska uppgifter och utredningen anser därför att myndigheten inte bör få behandla sådana uppgifter. Någon bestämmelse som medger sådan behandling bör därför inte finnas i kriminalvårdens brottsdatalag.

13.3.3 Utlämnande av personuppgifter

Utredningens förslag: Kriminalvården ska till en utländsk myndighet få lämna ut de personuppgifter som behövs för

1. prövning och genomförande av överflyttning av straffverkställighet,
2. transitering och förvaring av en person som är frihetsberövad för brottsbekämpning, lagföring eller verkställighet av straff, eller
3. tillfällig överflyttning av en frihetsberövad person för brottsbekämpning, lagföring eller straffverkställighet.

Skälen för utredningens förslag: I 48 § förordningen om behandling av personuppgifter inom kriminalvården regleras förutsättningarna för att lämna ut personuppgifter till en annan stat när verkställighet av påföljd ska överflyttas dit. Enligt paragrafen får uppgifter lämnas ut om bl.a. namn, personnummer eller andra identifikationsbeteckningar, genomförd personutredning och andra liknande utredningar, domstols dom och avräkningsunderlag, liksom uppgifter i journal för häktad, fängelsedömd, skyddstillsynsdömd eller den som är dömd till villkorlig dom med föreskrift om samhällstjänst. Sådana personuppgifter får lämnas ut till den myndighet i den andra staten som är ansvarig för verkställigheten.

Utredningen anser att bestämmelsen om att personuppgifter får lämnas ut till annan stat om det behövs för att den staten ska kunna överta straffverkställigheten av en påföljd är av sådant slag att den bör ha lagform (jfr avsnitt 13.1.2). Den bör därför tas in i kriminalvårdens brottsdatalog. Bestämmelsen bör dock göras mer generell. Det kan förutses att det internationella samarbetet kommer att öka, särskilt inom EU. Den nya bestämmelsen bör därför utformas så att den täcker de områden där det kan förutses behov av att kunna behandla och överlämna personuppgifter till en annan stats myndigheter. Den bör vara sekretessbrytande. Det är framför allt för tre typer av ärenden som det finns behov av att kunna lämna information.

En av dessa är överflyttning av straffverkställighet. Den ökade rörligheten över gränserna har medfört att frågor om överflyttning

av verkställighet till en annan stat är betydligt vanligare i dag än tidigare. I de fallen behövs ofta ingående information om den dömda, både för att pröva frågan om överflyttning och för den framtida verkställigheten om överflyttning kommer till stånd. Den reglering som i dag finns i 48 § förordningen om behandling av personuppgifter inom kriminalvården ger ledning för vilka typer av personuppgifter som kan behöva överföras. Regleringen behöver dock enligt utredningens mening inte vara så detaljerad.

En annan situation där Kriminalvården behöver kunna överföra personuppgifter är vid transitering av frihetsberövade. Vid transitering ska den frihetsberövade tas om hand tillfälligt i transiteringsstaten. Kriminalvården måste då kunna lämna nödvändig information till en annan stats myndigheter om personen som ska transiteras och i samband med det tillfälligt förvaras i den andra staten.

Den tredje situationen som den nya bestämmelsen bör täcka är tillfällig överflyttning till en annan stat. Om exempelvis en person som avtjänar ett längre fängelsestraff i Sverige behöver överföras tillfälligt till en annan stat för att lagföras eller medverka i en brottsutredning där behöver personuppgifter överföras för att den andra staten ska kunna förvara den dömda på ett säkert sätt till dess att han eller hon återförs till Sverige för att återuppta straffverkställigheten.

Förslaget tar sikte på Kriminalvårdens behov av att kunna överföra personuppgifter till en annan stat. Att Kriminalvården i motsvarande fall får behandla personuppgifter som myndigheten får från en annan stat följer av rätten att behandla personuppgifter för att fullgöra förpliktelser som följer av internationella åtaganden.

13.4 Kriminalvårdens register

13.4.1 Nuvarande reglering

I förordningen om behandling av personuppgifter inom kriminalvården regleras två register, det centrala kriminalvårdsregistret och säkerhetsregistret. Det centrala kriminalvårdsregistret innehåller uppgifter om i princip alla som verkställer en påföljd som Kriminalvården ansvarar för. Säkerhetsregistret innehåller något förenklat uppgifter om personer som verkställer häktning eller påföljd och

som kan utgöra en säkerhetsrisk i något avseende. Det finns också ett flertal bestämmelser i förordningen om journalföring.

I 34 § förordningen om behandling av personuppgifter inom kriminalvården regleras det centrala kriminalvårdsregistret, som förs av Kriminalvården. Registret innehåller uppgifter om personer som har dömts till fängelse, skyddstillsyn eller villkorlig dom med föreskrift om samhällstjänst, har ålagts förvandlingsstraff för böter eller vite eller som på grund av en utländsk brottmålsdom verkställer en sådan påföljd i Sverige. I 35 § anges genom hänvisningar till andra bestämmelser i förordningen vilka uppgifter registret får innehålla. Andra myndigheters skyldighet att lämna uppgifter som ska registreras i centrala kriminalvårdsregistret regleras i 36 §. Kriminalvårdens skyldighet att lämna uppgifter till andra myndigheter regleras i 37 §. Där anges också vilka myndigheter som får medges direktåtkomst till registret.

Enligt 39 § för Kriminalvården också säkerhetsregistret. Registret innehåller uppgifter om häktade eller intagna som är dömda till fängelse eller på grund av utländsk dom verkställer fängelsestraff och som på något av de i paragrafen uppräknade sätten utgör en säkerhetsrisk. Det är fråga om personer som är eller tidigare har varit placerade på säkerhetsavdelning, under tid i häkte eller under verkställighet av ett fängelsestraff har gjort sig skyldiga till allvarligt hot eller våld mot personal eller andra intagna, under sådan tid har befattat sig med narkotika som inte varit avsedd för eget bruk eller som rymt eller fritagits från häkte eller kriminalvårdsanstalt eller förberett eller gjort försök till rymning eller fritagning. Dessutom omfattar regleringen personer som misstänks för att under tid i häkte eller under verkställighet av ett fängelsestraff ha deltagit i nätverk som bidrar till allvarliga ordningsstörningar eller brottslig verksamhet.

Utöver de personkategorier som nämnts får säkerhetsregistret enligt 40 § innehålla uppgifter om häktade eller intagna, om det finns särskild anledning att anta att de under häktning eller verkställighet av fängelsestraff kan komma att utöva allvarlig brottslig verksamhet tillsammans med andra, göra sig skyldiga till hets mot folkgrupp eller vissa andra brott mot allmän verksamhet, allvarligt störa ordningen inom häktet eller anstalten, delta i nätverk som bidrar till allvarliga ordningsstörningar eller brottslig verksamhet eller förbereda rymning eller fritagning.

Säkerhetsregistret får enligt 41 § första stycket föras för att samlas, bearbeta och analysera information som ger underlag för åtgärder för att upprätthålla säkerheten eller förebygga brott. Registret får innehålla de uppgifter som behövs för det. Enligt andra stycket ska säkerhetsregistret innehålla skälen för registrering, med särskilt angivande av de omständigheter som ger anledning till ett sådant antagande som avses i 40 §, och upplysning om varifrån uppgifterna kommer och, om det inte är obehövt, en bedömning av uppgiftslämnarens trovärdighet. I 43 och 44 §§ finns det bestämmelser om direktåtkomst till uppgifter i och utlämnande av uppgifter ur säkerhetsregistret. I 45 § regleras gallring av uppgifter i registret.

13.4.2 Hur bör den framtida regleringen se ut?

Både det centrala kriminalvårdsregistret och säkerhetsregistret innehåller uppgifter om ett stort antal registrerade. Enligt 2 kap. 6 § andra stycket regeringsformen är enskilda gentemot det allmänna skyddade mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av personliga förhållanden. Det skydd som bestämmelsen ger får endast begränsas genom lag och under vissa förutsättningar. I förarbetena pekas bl.a. på att myndighetsregister med ett stort antal registrerade och särskilt känsligt innehåll normalt ska regleras i lag (se prop. 2009/10:80 s. 183). Det kan enligt utredningens mening ifrågasättas om inte de två större register som Kriminalvården för bör regleras i lag, både med hänsyn till antalet registrerade och karaktären av de uppgifter som registreras (jfr *Behandling av personuppgifter inom kriminalvården*, prop. 2000/01:126, s. 21).

Vid en allmän översyn av hur kriminalvårdens personuppgiftsbehandling bör regleras i framtiden bör enligt utredningens mening en reglering som ligger mera i linje med vad som gäller för övriga myndigheter i rättskedjan övervägas. Det skulle t.ex. kunna övervägas om registren bör regleras på samma sätt som i dag eller om det skulle vara möjligt att skapa en mer generell reglering som utgår från vilka uppgifter som behöver göras gemensamt tillgängliga för verksamhetens behov.

Det ingår inte i utredningens uppdrag att göra en materiell översyn av de författningar som berörs av brottsdatalagen utan enbart att anpassa dem till den lagen. Det står emellertid utredningen fritt att ta upp och lämna förslag i närliggande frågor som aktualiseras under utredningsarbetet (dir. 2016:21 s. 14). Med hänsyn till det har utredningen valt att ändå se över regleringen av säkerhetsregistret, som bl.a. innehåller uppgifter från Kriminalvårdens under rättelseverksamhet. Behandling av personuppgifter av det slaget regleras sedan länge i lag när det gäller andra myndigheter. Förslagen utgår från hur registret är reglerat i dag, eftersom det finns skäl som talar för att registret även i framtiden kan behöva särregleras. Det är emellertid en fråga för en materiell översyn av kriminalvårdens registerlagstiftning.

Att utredningen endast tar upp frågor som rör säkerhetsregistret innebär inte att det är mindre angeläget med en översyn av behandlingen av personuppgifter i det centrala kriminalvårdsregistret. Överväganden beträffande det registret kräver dock enligt utredningens bedömning betydligt mer arbete, bl.a. på grund av att regleringen av vilka uppgifter som får föras i registret är svåröverskådlig och att behovet av registrering och informationsutbyte behöver analyseras närmare.

13.5 Säkerhetsregistret

13.5.1 Reglering i lag

Utredningens förslag: Det ska i lagen föreskrivas att Kriminalvården får föra ett säkerhetsregister. I säkerhetsregistret ska personuppgifter få behandlas i syfte att

1. förebygga, förhindra eller upptäcka brott eller brottslig verksamhet på häkten och i kriminalvårdsanstalter eller i samband med annan straffverkställighet, och
2. säkerställa ordning och säkerhet på häkten och i kriminalvårdsanstalter och annan verksamhet som Kriminalvården bedriver.

Skälen för utredningens förslag: Behandling av personuppgifter i register med många registrerade eller känsligt innehåll regleras inom brottsdatalagens tillämpningsområde huvudsakligen i lag. Frågan om säkerhetsregistret borde lagregleras aktualiserades redan före grundlagsändringen (se Antagande av rambeslut om skydd för personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete, Ds 2008:30, s. 147, jfr också prop. 2000/01:126, s. 21). Säkerhetsregistret innehåller personuppgifter av sådant slag att åtminstone huvuddragen enligt utredningens mening bör regleras i lag.

Det bör således av lagen framgå att Kriminalvården får föra ett säkerhetsregister. Syftet med registret bör vara att Kriminalvården ska kunna förebygga, förhindra eller upptäcka brott eller brottslig verksamhet på häkten och i kriminalvårdsanstalter eller i samband med annan straffverkställighet som Kriminalvården ansvarar för. Uppgifterna i registret bör också kunna användas i syfte att säkerställa ordning och säkerhet på häkten och i kriminalvårdsanstalter och annan verksamhet som Kriminalvården bedriver. Att även annan verksamhet omfattas är viktigt med tanke på kriminalvårdens frivårdsverksamhet och att fängelsestraff till stor del kan verkställas utanför anstalt.

När rätten att föra säkerhetsregistret lagregleras bör också de bestämmelser om registret som i motsvarande fall brukar finnas i lag tas in i kriminalvårdens brottsdatalag. Det gäller bestämmelser om innehållet i registret, sökning på känsliga personuppgifter, vilka som får medges direktåtkomst och hur länge personuppgifterna får behandlas. Vissa detaljer beträffande säkerhetsregistret bör dock alltjämt regleras i förordning.

13.5.2 Registrering av häktade och intagna

Utredningens förslag: I säkerhetsregistret ska uppgifter få behandlas om en person som är häktad eller verkställer fängelsestraff och som är eller har varit placerad på säkerhetsavdelning. I registret ska även uppgifter få behandlas om en person som är häktad eller verkställer fängelsestraff, om det finns risk för att han eller hon

1. under häktning eller verkställighet av fängelsestraff begår brott som inte är ringa eller deltar i brottslig verksamhet som är allvarlig,
2. förbereder rymning eller försöker rymma,
3. blir föremål för fritagning,
4. medverkar i eller på annat sätt bidrar till att allvarligt störa ordningen eller säkerheten på ett häkte eller i en kriminalvårdsanstalt, eller
5. utsätts för våld eller hot under verkställigheten.

Skälen för utredningens förslag

En riskbedömning blir avgörande

Säkerhetsregistret bör i allt väsentligt omfatta uppgifter om samma kategorier av häktade och intagna som i dag. Det ska således inte omfatta uppgifter om alla häktade eller intagna utan enbart de som är häktade eller intagna för de syften som anges i brottsdatalagen och som bedöms medföra särskilda säkerhetsrisker. De personkategorier som i dag anges i 39 § förordningen om behandling av personuppgifter inom kriminalvården kan enligt utredningens mening medföra sådana särskilda risker vid verkställigheten eller för häktesverksamheten att behandling av personuppgifter i säkerhetsregistret är motiverad. Regleringen bör dock moderniseras och göras generell. Eftersom den nuvarande regleringen är svårtolkad och saknar förarbeten finns det risk att den tolkas på ett sätt som inte har varit avsett. Den svarar inte heller mot dagens behov.

Regleringen bör enligt utredningens mening utgå från vilka personer som kan medföra säkerhetsrisk under verkställigheten och en bedömning av den risken. Rekviritet risk förekommer i olika typer av lagstiftning. Det används t.ex. i 4 § lagen (2006:45) om omvandling av fängelse på livstid. Det är också ett centralt rekvirit i 24 kap. 1 § och 25 kap. 1 § rättegångsbalken för när vissa straffprocessuella tvångsmedel får användas. Enligt 23 och 24 a §§ polislagen ska likaså en bedömning av risken för att något inträffar göras. Ett annat exempel är bestämmelsen i 4 kap. 12 § andra stycket utsokningsbalken. Inom Kriminalvården är man van vid att göra olika former av riskbedömningar, se t.ex. 2 kap. 4 §, 10 kap. 1 och 2 §§ och 11 kap. 1–5 §§ fängelselagen (2010:610). Utredningen anser därför att förutsättningen för att registrera någon i säkerhetsregistret som huvudregel ska utgå från en riskbedömning.

Bara vissa häktade och intagna får registreras

En viktig utgångspunkt för behandling av personuppgifter i säkerhetsregistret bör vara om någon som är häktad eller intagen är eller har varit placerad på säkerhetsavdelning. I dag är placering på säkerhetsavdelning enligt 39 § 1 förordningen om behandling av personuppgifter inom kriminalvården en grund för registrering i säkerhetsregistret. Förutsättningarna för placering på säkerhetsavdelning anges i 2 kap. 4 § fängelselagen. Sådan placering förutsätter antingen varaktig risk för rymning eller fritagning och att det kan antas att den intagne är särskilt benägen att fortsätta brottslig verksamhet eller att det finns särskild anledning att anta att placeringen behövs för att hindra den intagne från allvarlig brottslig verksamhet under anstaltsvistelsen. Om omständigheterna är sådana att det finns grund för placering på säkerhetsavdelning bör också förutsättningarna för behandling av personuppgifter i säkerhetsregistret vara uppfyllda.

Risk för brott eller att brottslig verksamhet utövas

Enligt 39 § 2 förordningen om behandling av personuppgifter inom kriminalvården får personuppgifter behandlas i säkerhetsregistret bl.a. om någon under tid i häkte eller under verkställighet gjort sig

skyldig till allvarligt hot eller våld mot personal eller andra intagna. Enligt 39 § 3 får vidare uppgifter behandlas om någon befattat sig med narkotika som inte varit avsedd för eget bruk. Enligt utredningens mening bör dessa bestämmelser vara utgångspunkten för i vilka andra fall personer får registreras i säkerhetsregistret. Regleringen bör dock göras mer generell.

Om det finns risk för att personer kan begå brott på häkte eller under verkställighet av fängelsestraff, bör uppgifter om dem få behandlas i säkerhetsregistret om det är fråga om brott som kan antas påverka vistelsen på häktet eller i anstalten eller annars påverka Kriminalvårdens verksamhet. Det finns andra typer av brott än de som i dag räknas upp i förordningen som kan skapa säkerhetsrisker. Som exempel kan nämnas att brott som rör dopningsmedel kan innebära en minst lika stor risk för säkerheten och ordningen under verkställigheten som brott som rör narkotika. En mer generell reglering ger Kriminalvården bättre förutsättningar att reagera bl.a. mot pågående brott eller brottslig verksamhet.

Enligt utredningens mening kan i princip alla typer av brott som en häktad eller intagen begår på ett häkte eller under verkställighet i anstalt eller motsvarande, innebära risk för att han eller hon begår nya brott i den miljön. Det skulle emellertid kunna leda till att betydligt fler än i dag skulle kunna bli föremål för registrering i säkerhetsregistret om alla brott fick läggas till grund för registrering. Det ter sig inte rimligt att ringa brott, t.ex. snatteri eller andra brott som har ett lågt straffvärde, skulle få sådana konsekvenser. Därför bör endast brott som inte är ringa kunna läggas till grund för registrering i säkerhetsregistret.

Av samma skäl bör endast risk för brottslig verksamhet av allvarligare slag kunna föranleda registrering. Med det avser utredningen sådan brottslig verksamhet som innefattar brott där två års fängelse eller mer ingår i straffskalan. Det motsvarar det krav för registrering i säkerhetsregistret som gäller i dag (se 2 § förordningen om behandling av personuppgifter inom kriminalvården).

Det nuvarande kravet att någon ska ha gjort sig skyldig till våld eller hot kan uppfattas som att det krävs en straffrättslig prövning för att personuppgifter ska få behandlas, vilket knappast kan ha varit avsikten. Det bör enligt utredningens mening vara tillräckligt att det finns risk för att en häktad eller intagen begår brott, t.ex. utsätter personal eller andra intagna för hot eller våld.

Risk för rymning eller fritagning

Enligt 39 § 4 förordningen får personuppgifter behandlas i säkerhetsregistret om den som har rymt eller fritagits från häkte eller kriminalvårdsanstalt eller har förberett eller gjort försök till rymning eller fritagning. Dessa kategorier bör liksom i dag kunna registreras, men regleringen bör i stället utgå från risken för att personen rymmer eller blir föremål för fritagning. Har en rymning eller fritagning inträffat får det anses föreligga risk för framtida rymning eller fritagning, om inte omständigheterna talar emot det.

Risk för allvarliga ordningsstörningar

Enligt 39 § 5 förordningen får personuppgifter registreras om en häktad eller intagen som under tid i häkte eller under verkställighet av ett fängelsestraff misstänks för att ha deltagit i nätverk som bidrar till allvarliga ordningsstörningar eller brottslig verksamhet. Utredningen anser att formuleringen att någon misstänks för att ha deltagit i ett nätverk är för otydlig och svårtillämpad. Användningen av uttrycket misstänks ger också intryck av att deltagande i nätverk är kriminaliserat, vilket inte är fallet. Grunden för registrering bör därför uttryckas annorlunda. Regleringen bör utgå från behovet av att förebygga allvarliga ordningsstörningar och annat som kan äventyra säkerheten på häkten och i kriminalvårdsanstalter. Om det finns risk för att en person medverkar i eller på annat sätt bidrar till att allvarligt störa ordningen eller säkerheten på ett häkte eller i en kriminalvårdsanstalt under verkställigheten bör det kunna vara grund för behandling av personuppgifter i säkerhetsregistret.

Risk för våld eller hot mot häktade eller intagna

I dag har Kriminalvården inte rätt att behandla uppgifter i säkerhetsregistret om häktade eller intagna som inte själva utgör säkerhetsrisker men som riskerar att utsättas för våld eller hot av andra häktade eller intagna. Oftast kan ett hot härledas till andra häktade eller intagna och därmed utgöra en grund för att behandla personuppgifter om dem. Det kan emellertid ibland finnas en allvarlig hotbild mot en häktad eller intagen, samtidigt som det saknas kun-

skap om vem eller vilka som ligger bakom hotet. Det är då viktigt att Kriminalvården kan ta hänsyn till hotbilden vid placering och transporter, för att undvika att den häktade eller intagne utsätts för brott under verkställigheten. Det kan också ha betydelse för vilka säkerhetsåtgärder och andra åtgärder som krävs för att möta hotet och hur personalen bör dimensioneras vid ett visst tillfälle. Att det finns risk för att en häktad eller intagen utsätts för våld eller hot bör således enligt utredningens mening också kunna utgöra grund för behandling av personuppgifter i säkerhetsregistret. Det följer av 2 kap. 9 § brottsdatalagen att det ska framgå att personen i fråga inte själv utgör en säkerhetsrisk.

13.5.3 Registrering av den som utövar våld eller hot

Utredningens förslag: I säkerhetsregistret ska uppgifter få behandlas om en person som verkställer en påföljd inom kriminalvården, om det finns risk för att han eller hon utövar våld eller hot mot eller otillbörlig påverkan på personal eller andra personer som uppehåller sig i kriminalvårdens lokaler.

Skälen för utredningens förslag: I dag har Kriminalvården ingen rätt att registrera uppgifter i säkerhetsregistret om andra än häktade och intagna, trots att det kan finnas personer som utgör säkerhetsrisker i Kriminalvårdens övriga verksamhet. Det finns enligt utredningens mening behov av att i vissa fall kunna registrera uppgifter om personer oavsett vilken påföljd de avtjänar dels för att de ska kunna bemötas på rätt sätt, dels för att trygga personalens och andra klienters säkerhet. Förutsättningarna för att få behandla uppgifter i säkerhetsregistret på denna grund bör dock vara betydligt snävare. Det bör krävas att det finns risk för att klienten riktar hot mot eller utövar våld mot eller otillbörlig påverkan på personal, klienter eller andra personer som uppehåller sig i kriminalvårdens lokaler. Regleringen bör täcka angrepp mot både kriminalvårdens personal och andra som befinner sig i kriminalvårdens lokaler.

13.5.4 Registrering avseende andra

Utredningens förslag: Om det är absolut nödvändigt för ändamålet med behandlingen ska uppgifter få behandlas i säkerhetsregistret om en person som har personlig anknytning till eller annan nära förbindelse med en registrerad. Om den förstnämnde inte är häktad eller verkställer fängelsestraff ska det framgå genom en särskild upplysning.

Skälen för utredningens förslag: Även den häktades eller intagnes kontakter med omvärlden kan vara förknippade med säkerhetsrisker, t.ex. besök och annan kommunikation. Kriminalvården bör därför även få behandla uppgifter om vissa andra personer i säkerhetsregistret. Registrering av andra personer än häktade och intagna bör bl.a. kunna avse personer som den registrerade får besök av eller på annat sätt håller kontakt med. Behovet av registrering rör i första hand anhöriga eller andra som har en personlig anknytning till den registrerade. Det är störst risk att intagna försöker påverka närstående att t.ex. medföra otillåtna föremål till häkten eller kriminalvårdsanstalter. Även andra personer som på något sätt har en nära förbindelse med den registrerade kan på motsvarande sätt leda till säkerhetsrisker. Det kan t.ex. vara fråga om personer som har begått brott tillsammans. Det kan även röra sig om personer som tillhör samma kriminella nätverk eller våldsbejakande extremistiska rörelse. Regleringen bör inte omfatta personer som har professionella kontakter med registrerade, exempelvis advokater.

Ett grundläggande krav för registrering bör vara att personuppgiftsbehandlingen är absolut nödvändig för ändamålet med att uppgifter om den häktade eller intagne behandlas i säkerhetsregistret. Det innebär att bestämmelsen ska tillämpas restriktivt. Det kan exempelvis vara absolut nödvändigt att behandla personuppgifter om någon som försökt arrangera fritagning eller försökt föra in eller har fört in otillåtna föremål på ett häkte eller i en kriminalvårdsanstalt.

Det är viktigt att den som tar del av uppgifter i säkerhetsregistret får vetskap om det är den registrerade som utgör säkerhetsrisken eller om registreringen gjorts av något annat skäl. Enligt 2 kap. 9 § brottsdatalagen ska olika personkategorier kunna särskiljas. Det kravet gäller även för dem som registreras i säkerhetsregistret. Den

regleringen täcker t.ex. den situationen att en intagen utgör ett hot mot en annan intagen (se avsnitt 13.5.2). Den täcker emellertid inte behovet av att kunna skilja ut personer som registreras på grund av deras anknytning till någon som förekommer i säkerhetsregistret. För att det tydligt ska framgå om personerna inte själva är häktade eller verkställer fängelsestraff bör registreringen förses med en särskild upplysning om det.

13.5.5 Sökning på känsliga personuppgifter

Utredningens förslag: Sökförbudet i brottsdatalagen hindrar inte sökning i personuppgifter i säkerhetsregistret i syfte att få fram ett personurval grundat på etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller uppgifter som rör hälsa, sexualliv eller sexuell läggning.

Skälen för utredningens förslag: Sökförbudet i 2 kap. 14 § brottsdatalagen utgår till skillnad från dagens reglering från syftet med sökningen. Om syftet inte är att få fram ett personurval grundat på känsliga personuppgifter är sökningen tillåten, även om känsliga personuppgifter används vid sökningen (se SOU 2017:29 s 272 f.).

Enligt 41 § tredje stycket andra meningen förordningen om behandling av personuppgifter inom kriminalvården får känsliga personuppgifter användas som sökbegrepp för sökning i säkerhetsregistret. Kriminalvården har även i fortsättningen behov av att kunna använda känsliga personuppgifter vid sökning i personuppgifter i säkerhetsregistret. Det bör därför göras undantag i kriminalvårdens brottsdatalag från det generella sökförbudet i brottsdatalagen. För att kunna placera intagna och av hänsyn till de intagnas och personalens säkerhet har Kriminalvården behov av att kunna göra sökning i syfte att få fram personurval grundade på de flesta kategorier av känsliga personuppgifter. Det kan aldrig finnas behov av att söka på ras, eftersom det inte finns någon vetenskaplig grund för att dela in människor i skilda raser (se SOU 2017:29 s. 267). Kriminalvården har inte heller behov av att kunna göra sökning i syfte att få fram ett personurval grundat på medlemskap i fackförening eller biometriska eller genetiska uppgifter. Sådana sökningar bör därför inte vara tillåtna. Det innebär att möjlighe-

terna att använda känsliga personuppgifter vid sökning i säkerhetsregistret begränsas i förhållande till vad som gäller i dag. Eftersom Kriminalvården inte har behov av ett generellt undantag bedömer utredningen att undantaget inte innebär någon försämring.

13.5.6 Direktåtkomst och annat utlämnande

Utredningens förslag: Polismyndigheten, Säkerhetspolisen, Ekobrottsmyndigheten och Åklagarmyndigheten ska få medges direktåtkomst till personuppgifter i säkerhetsregistret.

I förordning ska föreskrivas att åtkomsten ska begränsas till uppgift om huruvida någon förekommer i registret.

Skälen för utredningens förslag

Direktåtkomst till uppgifter i säkerhetsregistret

Enligt 44 § förordningen om behandling av personuppgifter inom kriminalvården får rikspolischefen, säkerhetspolischefen och de personer som respektive chef utser ha direktåtkomst till uppgifter om huruvida en person är registrerad i säkerhetsregistret. Polismyndigheten och Säkerhetspolisen får i sin tur lämna ut en sådan uppgift till Åklagarmyndigheten och Ekobrottsmyndigheten, om uppgiften kan antas ha särskild betydelse för en pågående undersökning i myndighetens brottsutredande verksamhet eller för andra brottsbekämpande åtgärder. Bestämmelsen om direktåtkomst till personuppgifter i säkerhetsregistret är omodern, bl.a. av det skälet att den detaljreglerar tillgången till uppgifterna och att den även reglerar mottagarens användning.

Direktåtkomst bör enligt utredningens mening medges myndigheter i stället för enskilda befattningshavare. Det bör därför föreskrivas att Polismyndigheten och Säkerhetspolisen får medges direktåtkomst. Även Ekobrottsmyndigheten och Åklagarmyndigheten bör kunna medges direktåtkomst, om samma krets som i dag ska kunna få tillgång till uppgifter i registret. Direktåtkomsten bör på samma sätt som i dag begränsas till enbart uppgift om huruvida någon förekommer i registret. Uppgift om att någon har registrerats på grund av risk för att utsättas för hot eller våld eller på grund

av personlig anknytning till eller annan nära förbindelse med en registrerad bör dock inte kunna lämnas ut. Detaljerna kan regleras i förordning.

Skälet till att vissa befattningshavare pekas ut i 44 § får antas vara att endast en mycket begränsad krets ska ges tillgång till uppgifter i registret. I 3 kap 6 § brottsdatalagen föreskrivs att den personuppgiftsansvarige ska se till att tillgången till personuppgifter begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter. Det gäller även uppgifter som en myndighet får tillgång till genom direktåtkomst (se SOU 2017:29 s. 312). Som framgår av avsnitt 5.3.9 behövs därför inte längre bestämmelser som begränsar tillgången till uppgifter.

Tillgången till personuppgifter i registret för Kriminalvårdens personal bör inte längre regleras genom en bestämmelse om direktåtkomst. Regleringen i 3 kap. 6 § brottsdatalagen är tillräcklig. Kriminalvården kan, förutom att begränsa behörigheten tekniskt, utfärda interna föreskrifter om tillgången om det anses nödvändigt. Någon ytterligare reglering av tillgången till personuppgifter i registret behövs därför inte.

Det bör inte heller regleras hur mottagaren får behandla sådana personuppgifter. Det styrs av brottsdatalagen och den mottagande myndighetens registerförfattning.

Behovet av en sekretessbrytande bestämmelse

Direktåtkomsten till uppgifter i säkerhetsregistret är som framgått författningsreglerad i dag. Frågan om det behövs sekretessbrytande bestämmelser för att kunna medge direktåtkomst övervägs normalt innan det införs möjlighet till direktåtkomst (se avsnitt 14.12.2). Den frågan berördes emellertid inte i förarbetena till kriminalvårdens registerlagstiftning och förefaller hittills inte ha utgjort något problem. Att vissa bestämmelser om registret nu föreslås flyttas till lag gör dock att frågan om det krävs sekretessbrytande bestämmelser aktualiseras. Utredningen har inte haft utrymme att behandla den frågan.

13.5.7 Längsta tid som personuppgifter får behandlas

Utredningens förslag: Personuppgifter i säkerhetsregistret ska inte få behandlas längre än fem år efter det att den registrerade blivit villkorligt frigiven från fängelsestraff eller annars helt har verkställt straffet eller, utan att ha dömts till sådant straff, har frigetts från häkte.

Skälen för utredningens förslag: Enligt 45 § förordningen om behandling av personuppgifter inom kriminalvården ska uppgifter i säkerhetsregistret gallras senast fem år efter det att den registrerade har frigetts från häkte eller blivit frigiven. Om villkorlig frigivning inte har ägt rum ska uppgifterna gallras senast fem år efter att den registrerade helt verkställt fängelsestraffet. En bestämmelse med motsvarande innehåll bör tas in i lagen.

Bestämmelsen syftar till att skydda enskildas integritet och är därför inte en gallringsbestämmelse i arkivrättslig mening. Den bör av de skäl som anges i avsnitt 5.5.2 i stället ange hur länge personuppgifter i registret får behandlas.

13.5.8 Föreskrifter

Utredningens förslag: Regeringen eller den myndighet som regeringen bestämmer ska kunna meddela föreskrifter om innehållet i säkerhetsregistret och utlämnande av personuppgifter ur registret.

Skälen för utredningens förslag: I 40 § förordningen om behandling av personuppgifter inom kriminalvården anges vissa kategorier av personer utöver dem som anges i 39 § som får registreras i säkerhetsregistret. Enligt 41 § ska bl.a. skälen för registrering och ytterligare upplysningar om omständigheterna kring registreringen framgå. I 43 och 44 §§ finns bestämmelser om utlämnande av personuppgifter ur registret.

Även fortsättningsvis bör enligt utredningens mening vissa bestämmelser om innehållet i säkerhetsregistret och utlämnande av uppgifter ur registret finnas i förordning. Det bör därför framgå av

lagen att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter i sådana frågor.

13.6 Bestämmelser som inte längre behövs

13.6.1 Sökning på känsliga personuppgifter

Utredningens förslag: Bestämmelsen om att känsliga personuppgifter inte får användas som sökbegrepp om inte regeringen har föreskrivit det ska upphävas.

Skälen för utredningens förslag: I 2 kap. 14 § brottsdatalagen finns ett generellt förbud mot att utföra sökningar i syfte att få fram ett personurval grundat på känsliga personuppgifter. Enligt 5 § tredje stycket lagen om behandling av personuppgifter inom kriminalvården får känsliga personuppgifter inte användas som sökbegrepp om inte regeringen har föreskrivit det. I paragrafen anges de närmare förutsättningarna för att få meddela sådana föreskrifter. Mot bakgrund av att brottsdatalagen innehåller ett generellt sökförbud bör bestämmelsen i 5 § om förbud mot att använda känsliga personuppgifter som sökbegrepp upphävas. I avsnitt 13.5.5 föreslås en särskild regel om sökningar i säkerhetsregistret.

13.6.2 Tillgången till personuppgifter

Utredningens förslag: Bestämmelsen om tillgång till personuppgifter vid direktåtkomst ska upphävas.

Skälen för utredningens förslag: Enligt 3 kap. 6 § brottsdatalagen ska den personuppgiftsansvarige se till att tillgången till personuppgifter begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter. Eftersom det finns en bestämmelse i brottsdatalagen som begränsar tillgången till personuppgifter föreslår utredningen i avsnitt 5.3.9 att sådana bestämmelser i registerförfattningarna ska upphävas.

Enligt 6 § första stycket lagen om behandling av personuppgifter inom kriminalvården ska direktåtkomst till de personuppgifter

som behandlas enligt lagen vara förbehållen de personer som på grund av sina arbetsuppgifter inom kriminalvården behöver tillgång till uppgifterna. Syftet med bestämmelsen är att internt begränsa tillgången till de personuppgifter som behandlas. Endast de personer som på grund av sina arbetsuppgifter behöver ha tillgång till personuppgifterna ska ha åtkomst till dem (se prop. 2000/01:126 s. 34 f.). Bestämmelsen fyller samma funktion som 3 kap. 6 § brottsdatalagen. Den bör därför upphävas.

I 6 § andra stycket föreskrivs att 10 § gäller i fråga om direktåtkomst till uppgifter som får lämnas ut till en annan myndighet. Där föreskrivs att direktåtkomst till personuppgifter ska förbehållas de personer som på grund av sina arbetsuppgifter behöver tillgång till dem. Med hänsyn till regleringen i 3 kap. 6 § brottsdatalagen finns det inte behov av en bestämmelse om tillgången till personuppgifter hos andra behöriga myndigheter. Bestämmelsen bör därför upphävas.

13.6.3 Omprövning

Utredningens förslag: Bestämmelserna om omprövning av beslut ska upphävas.

Skälen för utredningens förslag: Enligt 13 § lagen om behandling av personuppgifter inom kriminalvården får Kriminalvårdens beslut om rättelse och om information enligt 26 § personuppgiftslagen inte överklagas innan beslutet har omprövats av Kriminalvården. Omprövning får begäras av den som beslutet angår om det har gått honom eller henne emot. Överklagande av ett beslut som inte har omprövats ska enligt 13 § ses som en begäran om omprövning. Vid omprövningen får beslutet inte ändras till den enskildes nackdel. I 14 och 15 §§ anges formkraven för begäran om omprövning och rättidsprövning. Omprövningsförfarandet tillkom i samband med att Kriminalvården blev en myndighet. Syftet var bl.a. att begränsa antalet överklaganden och undvika att måltillströmningen till de allmänna förvaltningsdomstolarna ökade (se prop. 2004/05:176 s. 61 f.).

Varken direktivet eller brottsdatalagen ställer krav på att ett beslut ska omprövas innan det får överklagas. I övriga registerför-

fattningar föreskrivs inte heller något omprövningsförfarande. Det är svårt att se att den särreglering som finns för Kriminalvården är ändamålsenlig, särskilt som antalet överklaganden uppges vara få. Det saknas därför enligt utredningens mening anledning att fördröja överklagandena genom krav på omprövning. Omprövningsförfarandet bör därför tas bort och samtliga bestämmelser som rör det upphävas.

13.6.4 Överklagande

Utredningens förslag: De särskilda bestämmelserna om överklagande ska upphävas.

Skälen för utredningens förslag

Överklagandebestämmelsen upphävs

I 7 kap. 2 § brottsdatalagen föreskrivs att beslut i fråga om rättelse eller komplettering enligt 4 kap. 9 § första stycket, radering enligt 4 kap. 10 § första stycket eller begränsning av behandlingen enligt 4 kap. 9 § andra stycket eller 10 § andra stycket, som har meddelats av en myndighet i egenskap av personuppgiftsansvarig, får överklagas till allmän förvaltningsdomstol. Detsamma gäller beslut att inte lämna information enligt 4 kap. 3 eller 4 §, att ta ut avgift enligt 4 kap. 12 § andra stycket eller att inte medge omprövning av ett automatiserat beslut enligt 2 kap. 19 § första stycket. Av överklagandebestämmelsen framgår även att det krävs prövningstillstånd vid överklagande till kammarrätten och att beslut av regeringen, Högsta domstolen, Högsta förvaltningsdomstolen och riksdagens ombudsmän inte får överklagas.

Enligt 12 § lagen om behandling av personuppgifter inom kriminalvården får beslut om rättelse och om information enligt 26 § personuppgiftslagen överklagas hos allmän förvaltningsdomstol. Prövningstillstånd krävs vid överklagande till kammarrätten.

Eftersom det finns generella bestämmelser om överklagande i brottsdatalagen finns det inte anledning att behålla den särskilda regleringen. Av de skäl som anges i avsnitt 5.4.4 bör det i stället

införas en bestämmelse som upplyser om att bestämmelser om överklagande finns i brottsdatalagen.

Den särskilda forumbestämmelsen upphävs

Enligt 14 § lagen (1971:289) om allmänna förvaltningsdomstolar ska beslut överklagas till en förvaltningsrätt, om det i lag eller annan författning föreskrivs att talan ska väckas vid eller beslut överklagas till allmän förvaltningsdomstol. Som huvudregel ska ett beslut överklagas till den förvaltningsrätt inom vars domkrets ärendet först prövats.

I 16 § lagen om behandling av personuppgifter inom kriminalvården finns en särskild forumbestämmelse. Kriminalvårdens beslut om rättelse och om information enligt 26 § personuppgiftslagen ska överklagas till den förvaltningsrätt inom vars domkrets den kriminalvårdsanstalt, det häkte eller det frivårdskontor är beläget där den enskilde var inskriven när det första beslutet i ärendet fattades. Beslut som gäller en person som inte är inskriven vid en kriminalvårdsanstalt, ett häkte eller ett frivårdskontor i landet ska överklagas till den förvaltningsrätt som regeringen bestämmer. Enligt 7 d § 2 förordningen (1977:937) om allmänna förvaltningsdomstolars behörighet m.m. ska beslut av Kriminalvården som överklagas till en förvaltningsrätt tas upp av Förvaltningsrätten i Linköping om beslutet gäller en person som inte är inskriven vid en kriminalvårdsanstalt, ett häkte eller ett frivårdskontor i landet och beslutet avser bl.a. ärenden enligt lagen om behandling av personuppgifter inom kriminalvården.

Den särskilda forumbestämmelsen tillkom i samband med att Kriminalvården blev en myndighet. Syftet var att så långt möjligt sprida målen över landets samtliga förvaltningsdomstolar (se prop. 2004/05:176 s. 67).

Utredningen bedömer att det i dag inte finns något behov av en särskild forumbestämmelse för överklagande av beslut som rör personuppgiftsbehandling. Någon motsvarande bestämmelse finns varken i brottsdatalagen eller i övriga registerförfattningar. Den särskilda forumbestämmelsen bör därför upphävas. Det innebär att de allmänna bestämmelserna om forum ska tillämpas vid överklagande av beslut som meddelas inom kriminalvården.

13.7 Anpassningar av förordningen om behandling av personuppgifter inom kriminalvården

13.7.1 Behovet av översyn

I utredningens uppdrag ingår också att anpassa den förordning som kompletterar lagen om behandling av personuppgifter inom kriminalvården till brottsdatalagen. Utredningen anser att det finns ett stort behov av en total översyn av förordningen. Den detaljerade regleringen svarar inte mot dagens krav på registerförfattningar. Utredningen lämnar därför i huvudsak bara förslag till de ändringar som är nödvändiga för att anpassa förordningen till regleringen i brottsdatalagen och de övriga förslag som lämnas beträffande kriminalvårdens registerlag. Vissa redaktionella ändringar görs också, t.ex. sammanslagningar och omflyttningar av paragrafer och viss modernisering av språk och terminologi. Sådana ändringar kommenteras inte vidare här. Kriminalvården har under utredningsarbetet påtalat några problem med den nuvarande regleringen som utredningen ser som angeläget att genomföra, trots att det inte ingår i uppdraget.

13.7.2 Anpassningar till brottsdatalagen och kriminalvårdens brottsdatalag

Utredningens förslag: Bestämmelser om behandling av känsliga personuppgifter ska upphävas. I övrigt ska bestämmelserna anpassas till kriminalvårdens brottsdatalag och bestämmelser som inte längre behövs upphävas.

Skälen för utredningens förslag

Bestämmelser om behandling av känsliga personuppgifter upphävs

Enligt 2 kap. 11 § brottsdatalagen får personuppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening eller som rör hälsa, sexualliv eller sexuell läggning inte behandlas. Om uppgifter om en person redan behandlas, är det dock tillåtet att komplettera dem med

sådana personuppgifter när det är absolut nödvändigt för ändamålet med behandlingen.

I 4, 7, 12, 18, 23, 27 och 32 §§ förordningen om behandling av personuppgifter inom kriminalvården föreskrivs att känsliga personuppgifter får behandlas om det är oundgängligen nödvändigt. Enligt 41 § tredje stycket får säkerhetsregistret innehålla känsliga personuppgifter om det är oundgängligen nödvändigt. I 48 § andra stycket föreskrivs att vid överflyttning av verkställighet av påföljd till annan stat får känsliga personuppgifter lämnas ut endast om det kan anses oundgängligen nödvändigt.

Eftersom det i brottsdatalagen finns generella bestämmelser om behandling av känsliga personuppgifter finns det inte skäl att behålla särskilda regler om det i förordningen. Bestämmelserna om behandling av känsliga personuppgifter bör därför upphävas.

Anpassningar till kriminalvårdens brottsdatalag

I flera paragrafer i förordningen finns det hänvisningar till lagen om behandling av personuppgifter inom kriminalvården där det med utgångspunkt i personkategorier anges vilka personuppgifter som får behandlas och för vilka ändamål. Sådana hänvisningar bör ändras till att i stället gälla i förhållande till kriminalvårdens brottsdatalag och tillåtna rättsliga grunder för personuppgiftsbehandling. Eftersom regleringen i lagen inte längre bygger på en uppräknning av personkategorier bör det, om det behövs, i förordningen uttryckligen anges vilka personer som avses, t.ex. personer dömda till fängelse. I vissa fall är det dock lämpligare att hänvisa till för vilket syfte personuppgifter får behandlas.

Behandling av uppgifter om sådana personer som i dag anges i 1 § första stycket 8 och 9 lagen om behandling av personuppgifter inom kriminalvården, dvs. personer som är intagna i häkte eller kriminalvårdsanstalt eller transporteras av Kriminalvårdens transporttjänst, görs för andra syften än de som anges i brottsdatalagen. Behandling av sådana personuppgifter ligger utanför tillämpningsområdet för kriminalvårdens brottsdatalag och bestämmelser som rör personkategorierna i fråga bör därför tas bort.

Gallringsbestämmelserna i förordningen bör av de skäl som anges i avsnitt 5.5.2 formuleras om så att de i stället utgår från hur länge personuppgifter får behandlas.

I 50 § förordningen finns bestämmelser om gallring när en överrätt i vissa fall ändrar en underrätts dom eller beslut. Eftersom det i 2 kap. 17 § första stycket brottsdatalagen föreskrivs att personuppgifter inte får behandlas under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen fyller bestämmelsen inte någon funktion. Är det inte relevant att behandla en personuppgift, vilket t.ex. kan bero på att personen har beviljats resning och därefter frikänts, får uppgiften inte längre behandlas. Paragrafen bör därför upphävas.

I 2 § förordningen om behandling av personuppgifter inom kriminalvården definieras uttrycken känsliga personuppgifter, personutredning och allvarlig brottslighet. Eftersom det inte kommer att finnas kvar några bestämmelser om känsliga personuppgifter i förordningen finns det inte något behov av en sådan definition. Uttrycket allvarlig brottslighet kommer enligt utredningens förslag inte heller att användas i förordningen. När det gäller ordet personutredning råder det enligt utredningens mening ingen tvekan om vad som avses. Kriminalvården anser att det inte finns behov av definitionen i fråga. Bestämmelsen om definitioner bör därför upphävas.

13.7.3 Andra ändringar i förordningen

Utredningens förslag: Uppgifter om häktade ska få föras in i centrala kriminalvårdsregistret.

Om en häktad har frigetts från häkte och sedan döms till fängelse, skyddstillsyn eller villkorlig dom med föreskrift om samhällstjänst, ska personuppgifter inte få behandlas längre än tio år efter det att påföljden helt har verkställts.

Bestämmelser om Kriminalvårdens underrättelseskyldighet ska brytas ut och regleras i en särskild förordning.

Skälen för utredningens förslag

Uppgifter om häktade får föras in i centrala kriminalvårdsregistret

Kriminalvården för centrala kriminalvårdsregistret bl.a. för att underlätta tillgången till sådana uppgifter om verkställighet av påföljd eller häktning som rättsväsendets myndigheter behöver. Enligt 34 § förordningen om behandling av personuppgifter inom kriminalvården ska registret innehålla uppgifter om personer som har dömts till fängelse, skyddstillsyn eller villkorlig dom med föreskrift om samhällstjänst eller har ålagts förvandlingsstraff för böter eller vite eller på grund av en utländsk brottmålsdom ska verkställa någon sådan påföljd i Sverige.

I dag saknas det uttryckligt stöd för att registrera uppgifter om häktade i centrala kriminalvårdsregistret. Både Kriminalvården och övriga myndigheter i rättskedjan har stort behov av sådana uppgifter. Eftersom registerlagstiftningen är omodern är det oklart i vilken utsträckning uppgifter om häktade får behandlas i centrala kriminalvårdsregistret, trots att häktade enligt 1 § lagen om behandling av personuppgifter inom kriminalvården är en kategori vars personuppgifter får behandlas. Det bör genom en ändring i förordningen tydliggöras att sådan registrering är tillåten.

Längsta tid för behandling av personuppgifter om häktade

Enligt 13 § förordningen om behandling av personuppgifter inom kriminalvården ska uppgifter om en häktad person gallras senast två år efter det att den häktade har frigetts från häktet.

Den nuvarande formuleringen av bestämmelsen vållar enligt uppgift problem genom att tidsfristen löper från det att den häktade har frigetts från häktet. Ett exempel är att en person har varit häktad men frigetts i avvaktan på dom och senare döms till ett fängelsestraff eller en frivårdspåföljd som han eller hon börjar verkställa. Det är då inte rimligt att den längsta tid som personuppgifterna får behandlas räknas från när personen frigavs från häktet, eftersom det kan leda till att behandlingen av personuppgifterna måste upphöra trots att straffet inte är helt verkställt. Om en person döms till fängelse, skyddstillsyn eller villkorlig dom med föreskrift om samhällstjänst bör samma regler gälla för hur länge per-

sonuppgifterna får behandlas, oavsett om personen har varit häktad och frigetts eller inte. Personuppgifterna bör således inte få behandlas längre än tio år efter det att påföljden helt har verkställts. Längsta tid för behandling av personuppgifter rörande den som varit häktad men inte dömts till en påföljd som verkställs inom Kriminalvården bör inte ändras. Hur bestämmelsen bör formuleras behandlas i avsnitt 5.5.2.

Det kan anmärkas att 8 § förordningen, som rör uppgifter om personer som är föremål för personutredning, är utformad på det sätt som nu föreslås. Det kan därför antas att det inte har varit lagstiftarens avsikt att gallringsregeln beträffande häktade skulle ha någon annan innebörd.

Bestämmelser om underrättelseskyldighet

Förordningen om behandling av personuppgifter inom kriminalvården innehåller bestämmelser om dels andra myndigheters underrättelseskyldighet gentemot Kriminalvården för att myndigheten ska kunna föra det centrala kriminalvårdsregistret, dels Kriminalvårdens underrättelseskyldighet till vissa myndigheter om verkställigheten av straffrättsliga påföljder.

Att en registerförfattning innehåller bestämmelser om skyldighet att lämna uppgifter som ska utgöra underlag för ett visst register som regleras i författningen är inte ovanligt. Däremot regleras andra underrättelseskyldigheter ofta på annat sätt än i registerförfattningar. Eftersom förordningen om behandling av personuppgifter inom kriminalvården är detaljbetonad och i många avseenden skiljer sig från andra motsvarande författningar, skulle det enligt utredningens mening bidra till att renodla förordningen om Kriminalvårdens underrättelseskyldighet bryts ut och placeras i en ny förordning. I den bör det även regleras att Kriminalvården ska vara skyldig att ge Tullverket besked om var en häktad eller intagen vistas (se avsnitt 8.3.3).

14 Säkerhetspolisens behandling av personuppgifter

14.1 Bakgrund

14.1.1 Säkerhetspolisens uppdrag och verksamhet

Enligt 1 § andra stycket polislagen bedrivs polisverksamhet av Polismyndigheten och Säkerhetspolisen. Säkerhetspolisens huvudsakliga uppgifter och ansvar framgår av 3 §. Säkerhetspolisen ska förebygga, förhindra och upptäcka brottslig verksamhet som innefattar brott mot rikets säkerhet eller terrorbrott och utreda och beivra sådana brott, fullgöra uppgifter i samband med personskydd av den centrala statsledningen och andra som regeringen eller Säkerhetspolisen bestämmer, fullgöra uppgifter enligt säkerhetskyddslagen (1996:627), leda annan polisverksamhet om regeringen föreskriver det och i övrigt bedriva sådan verksamhet som framgår av lag eller förordning eller som regeringen uppdragit åt Säkerhetspolisen att i särskilda hänseenden ansvara för. I förordningen med instruktion för Säkerhetspolisen preciseras myndighetens uppdrag. Enligt 1 § ska Säkerhetspolisen, i egenskap av säkerhetstjänst, bedriva underrättelse- och säkerhetsarbete. I 3 § anges vilka typer av brott som Säkerhetspolisen ansvarar för och i 4 § utvecklas vad som avses med personskydd för den centrala statsledningen.

Säkerhetspolisens verksamhet är indelad i fem huvudområden. Kontraspionageverksamheten ska förebygga och avslöja spioneri och annan olovlig underrättelseverksamhet som kan rikta sig mot Sverige och svenska intressen utomlands, mot utländska intressen i Sverige och mot flyktingar. Kontraterrorismverksamheten syftar till att förebygga och avslöja bl.a. terrorism som riktas mot Sverige, svenska intressen utomlands och utländska intressen i Sverige, internationella terroristnätverks förgreningar i Sverige och stöd och

finansiering av terroristverksamhet. Den författningsskyddande verksamheten har till uppgift att motverka verksamhet som genom trakasserier, hot, våld, tvång eller korrupcion syftar till att påverka det demokratiska statsskickets funktioner. Säkerhetspolisen ansvarar även för personskyddet av den centrala statsledningen och främmande statsbeskickningsmedlemmar och vid statsbesök och liknande händelser. Säkerhetspolisen bedriver också säkerhetskyddsverksamhet, som syftar till att höja säkerhetsnivån i samhället genom analyser, registerkontroller, tillsyn och rekommendationer till myndigheter vilkas verksamhet har betydelse för rikets säkerhet.

Säkerhetspolisen har också vissa uppgifter enligt utlännings- och medborgarskapslagstiftningen. Enligt 1 kap. 7 § utlänningslagen är säkerhetsärenden ärenden där Säkerhetspolisen av skäl som rör rikets säkerhet eller som annars har betydelse för allmän säkerhet förordar att vissa beslut ska meddelas, exempelvis att en utlänning ska avvisas eller utvisas eller att en utlännings ansökan om uppehållstillstånd ska avslås. Säkerhetspolisen har rätt att överklaga Migrationsverkets beslut i sådana ärenden. Säkerhetspolisen är också verkställande myndighet i säkerhetsärenden, vilket ger myndigheten rätt att fatta beslut i frågor om förvar och uppsikt. Säkerhetspolisen utför även uppgifter enligt lagen (1991:572) om särskild utlänningskontroll. Med stöd av den lagen kan myndigheten ansöka om att en utlänning ska utvisas ur landet. Säkerhetspolisen ansvarar för att beslut om utvisning enligt lagen verkställs. Enligt lagen (2001:82) om svenskt medborgarskap kan Säkerhetspolisen förorda att en ansökan om svenskt medborgarskap ska avslås av skäl som rör rikets säkerhet eller allmän säkerhet. Myndigheten har även rätt att överklaga sådana beslut.

Säkerhetspolisen arbetar även med frågor som rör ickespridning. Den verksamheten syftar till att förhindra spridning och anskaffning av produkter som kan användas för att producera massförstörelsevapen. Arbetet går främst ut på att förhindra att kunskaper, produkter, ämnen eller mikroorganismer förs från eller via Sverige till aktörer som har ambitioner att anskaffa eller vidareutveckla massförstörelsevapen.

Säkerhetspolisen samverkar också med Polismyndigheten inom vissa områden, exempelvis verkställighet av hemlig rumsavlyssning och hemliga tvångsmedel på teleområdet.

14.1.2 Säkerhetspolisens organisation

Säkerhetspolisen blev den 1 januari 2015 en självständig myndighet. Myndigheten leds av en säkerhetspolischef, som är generaldirektör, och en biträdande säkerhetspolischef. De biträds av generaldirektörens stab.

Sedan den 1 oktober 2016 är Säkerhetspolisens kärnverksamhet uppdelad i två avdelningar; säkerhetsunderrättelseavdelningen och säkerhetsavdelningen. Den förstnämnda ansvarar för myndighetens säkerhetsunderrättelseverksamhet, dvs. arbetet med att bedöma och reducera hotaktörers avsikt och förmåga att bedriva säkerhetshotande verksamhet. Avdelningen ansvarar även för brottsutredningar och ärenden enligt utlännings- och medborgarskapslagstiftningen. Där bedrivs också underrättelsearbete med främsta syfte att förse myndigheten med beslutsunderlag för säkerhetsåtgärder. Säkerhetsavdelningen ansvarar för verksamhet inom områdena säkerhetsskydd och personskydd och för det interna säkerhetsarbetet och den interna riskhanteringen.

Det finns också en inhämtningsavdelning, en informations- och utvecklingsavdelning och en avdelning för verksamhetsstöd. Inhämtningsavdelningen utför på uppdrag av säkerhets- eller säkerhetsunderrättelseavdelningen inhämtnings- eller åtgärdsuppdrag. Avdelningen ansvarar för operativ stödverksamhet avseende bl.a. hemliga tvångsmedel. Vid avdelningen finns också myndighetens funktion för finansiella underrättelser och Säkerhetspolisens kommunikationscentral. Informations- och utvecklingsavdelningen ansvarar för myndighetens samlade informationsförsörjning genom att registrera och grundbearbeta den information som kommer in till myndigheten och göra den tillgänglig för övriga delar av myndigheten. Avdelningen samordnar utvecklingsarbetet avseende bl.a. systemförvaltning. Avdelningen för verksamhetsstöd ansvarar för Säkerhetspolisens administrativa verksamhet som rör bl.a. personal och ekonomi.

14.1.3 Regleringen av personuppgiftsbehandlingen

Polisdatalagen

Allmänt

I 6 kap. polisdatalagen regleras behandling av personuppgifter i Säkerhetspolisens brottsbekämpande verksamhet. Där anges ändamålen för Säkerhetspolisens personuppgiftsbehandling, som delvis avviker från Polismyndighetens. Det finns även särskilda bestämmelser om behandling av känsliga personuppgifter och om bevarande och gallring. I 6 kap. 4 § polisdatalagen hänvisas till ett flertal bestämmelser i 2 kap. i lagen som ska tillämpas även av Säkerhetspolisen. Polisdatalagen gäller enligt 2 kap. 1 § i stället för personuppgiftslagen, men i 2 kap. 2 § hänvisas till ett antal bestämmelser i personuppgiftslagen som gäller vid behandling av personuppgifter enligt polisdatalagen. Många bestämmelser som gäller för Polismyndigheten gäller således även för Säkerhetspolisen.

Polisdataförordningen gäller också i tillämpliga delar för Säkerhetspolisen. Där finns ytterligare bestämmelser om bl.a. behörighetstilldelning, ändamål, elektroniskt utlämnande och bevarande och gallring.

Ändamål för behandling

I 6 kap. 1–3 §§ polisdatalagen anges för vilka ändamål Säkerhetspolisen får behandla personuppgifter. Ändamålen delas in i primära och sekundära. De primära ändamålen, som avser behandling av personuppgifter för behoven i Säkerhetspolisens brottsbekämpande verksamhet, anges uttömmande i 6 kap. 1 § polisdatalagen. Personuppgifter får behandlas om det behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott mot rikets säkerhet, terrorbrott eller tryck- eller yttrandefrihetsbrott med rasistiska eller främlingsfientliga motiv. Personuppgifter får även behandlas för att utreda eller beivra sådana brott eller, efter särskilt beslut, annat brott. Säkerhetspolisen får också behandla personuppgifter om det behövs för att fullgöra uppgifter i samband med personskydd av den centrala statsledningen och andra som regeringen eller Säkerhetspolisen bestämmer, fullgöra uppgifter enligt säkerhetsskyddslagen, fullgöra förpliktelser som följer av inter-

nationella åtaganden, lämna tekniskt biträde till Polismyndigheten, Ekobrottsmyndigheten, Åklagarmyndigheten eller Tullverket eller fullgöra annan verksamhet som anges i lag eller förordning eller särskilt beslut av regeringen.

De sekundära ändamålen aktualiseras när personuppgifter som redan behandlas i Säkerhetspolisens brottsbekämpande verksamhet lämnas ut till andra myndigheter eller organisationer för deras behov. Enligt de sekundära ändamålen, som anges i 6 kap. 2 § polisdatalagen, får personuppgifter behandlas när det är nödvändigt för att tillhandahålla information som behövs i brottsbekämpande verksamhet hos Polismyndigheten, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket eller hos en utländsk myndighet eller mellanfolklig organisation. Utlämnande är vidare tillåtet om behandlingen är nödvändig för att tillhandahålla information som behövs i en myndighets verksamhet, om informationen tillhandahålls inom ramen för myndighetsöverskridande samverkan mot brott eller i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst om det finns särskilda skäl att tillhandahålla informationen. Detsamma gäller om Säkerhetspolisen enligt lag eller förordning ska bistå en myndighet med viss uppgift. Säkerhetspolisen får även behandla personuppgifter om det är nödvändigt för att tillhandahålla information till bl.a. riksdagen och regeringen. Personuppgifter får dessutom behandlas för att tillhandahålla information för något annat ändamål, under förutsättning att ändamålet inte är oförenligt med det ändamål för vilket uppgifterna samlades in (finalitetsprincipen). I 12 § polisdataförordningen finns ytterligare bestämmelser om ändamål för utlämnande av personuppgifter.

Personuppgifter får enligt 6 kap. 3 § polisdatalagen också behandlas om det är nödvändigt för diarieföring eller om uppgifterna har lämnats till Säkerhetspolisen i en anmälan eller liknande och behandlingen är nödvändig för handläggningen.

Utlämnande av personuppgifter

När det gäller utlämnande av personuppgifter och uppgiftsskyldighet gäller i huvudsak samma bestämmelser för Säkerhetspolisen som för Polismyndigheten. Bestämmelserna i 2 kap. 14 och 15 §§

polisdatalagen gäller även för Säkerhetspolisen. I 14 § föreskrivs att personuppgifter får lämnas ut för att framställa rättsstatistik. I 15 § finns sekretessbrytande bestämmelser som anger i vilken utsträckning personuppgifter får lämnas ut till bl.a. Interpol, Europol, utländsk underrättelse- eller säkerhetstjänst och annan utländsk myndighet eller mellanfolklig organisation.

Även bestämmelserna om elektroniskt utlämnande i 2 kap. 20 och 21 §§ polisdatalagen gäller för Säkerhetspolisen. Där föreskrivs att enstaka personuppgifter får lämnas ut på medium för automatiserad behandling och att utlämnande genom direktåtkomst är tillåtet bara i den utsträckning som följer av lagen. Säkerhetspolisen har inte getts någon möjlighet att lämna ut personuppgifter genom direktåtkomst. I polisdataförordningen finns kompletterande bestämmelser om elektroniskt utlämnande. Där föreskrivs bl.a. att fler än enstaka personuppgifter under vissa förutsättningar får lämnas ut på medium för automatiserad behandling till ett antal angivna myndigheter.

Behandling av känsliga personuppgifter

Bestämmelserna om behandling av känsliga personuppgifter i 2 kap. 10 § polisdatalagen gäller för Säkerhetspolisen. Uppgifter om en person får inte behandlas enbart på grund av vad som är känt om personens ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexualliv. Om uppgifter om en person behandlas på annan grund får de kompletteras med sådana uppgifter om det är absolut nödvändigt för syftet med behandlingen.

Behandling av gemensamt tillgängliga uppgifter

På samma sätt som för Polismyndigheten regleras Säkerhetspolisens behandling av gemensamt tillgängliga uppgifter särskilt. I 6 kap. 8 § polisdatalagen föreskrivs att personuppgifter får göras gemensamt tillgängliga i Säkerhetspolisens verksamhet om det behövs för de ändamål för vilka Säkerhetspolisen får behandla personuppgifter.

När personuppgifter görs gemensamt tillgängliga ska det, enligt 6 kap. 9 §, genom en särskild upplysning eller på något annat sätt framgå för vilket närmare ändamål personuppgifterna behandlas. Om uppgifterna direkt kan hänföras till en person som inte är misstänkt för brott eller för att ha utövat eller komma att utöva brottslig verksamhet ska det enligt 6 kap. 10 § framgå att personen inte är misstänkt. Uppgifter om en person som kan antas ha samband med misstänkt brottslig verksamhet ska försees med upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak. Sådana upplysningar behöver dock inte lämnas om det på grund av särskilda omständigheter är onödigt eller om uppgifterna ingår i en uppgiftssamling som har skapats för att bearbeta och analysera information och bearbetningen och analysen befinner sig i ett inledande skede.

Vid sökning i gemensamt tillgängliga uppgifter får Säkerhetspolisen enligt 6 kap. 11 § polisdatalagen använda känsliga personuppgifter som sökbegrepp endast om det är absolut nödvändigt.

Bevarande och gallring

I 6 kap. 6 § polisdatalagen föreskrivs att Säkerhetspolisen inte får bevara personuppgifter under längre tid än vad som behövs för något eller några av de ändamål som anges i lagen. I 6 kap. 7 och 12–14 §§ regleras hur länge uppgifter länge får bevaras.

Personuppgifter som inte har gjorts gemensamt tillgängliga ska, om de behandlas i ett ärende, gallras senast ett år efter att ärendet avslutats. Om uppgifterna inte kan hänföras till ett ärende ska de gallras senast ett år efter att de behandlades automatiserat första gången.

Personuppgifter som har gjorts gemensamt tillgängliga ska gallras senast tio år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes. Särskilda regler gäller för personuppgifter som behandlas i en uppgiftssamling som har skapats för att bearbeta och analysera information och som enbart särskilt angivna tjänstemän har tillgång till. Sådana personuppgifter ska gallras senast tre år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes. Om det finns särskilda skäl får Säkerhetspolisen besluta att personuppgifter får

bevaras längre tid om uppgifterna fortfarande behövs för det ändamål för vilket de behandlas.

Annan tillämplig lagstiftning

Säkerhetspolisens tillämpar också lagen om internationellt polisiärt samarbete och föreskrifter som har meddelats i anslutning till den lagen. Lagen tillämpas på polisiärt samarbete mellan Sverige och andra stater i den utsträckning som Sverige i en internationell överenskommelse har gjort sådana åtaganden som avses i lagen. Enligt 6 kap. 1 § lagen om internationellt polisiärt samarbete gäller polisdatalagen för polisens behandling av personuppgifter vid internationellt polisiärt samarbete, om inte annat följer av lagen om internationellt polisiärt samarbete eller föreskrifter som regeringen har meddelat i anslutning till den lagen.

I 7–9 kap. lagen om internationellt polisiärt samarbete regleras informationsutbyte enligt vissa EU-rättsakter; Prüm-rådsbeslutet, CBE-direktivet och VIS-rådsbeslutet.

Säkerhetspolisens kan även tillämpa 2013 års lag, men i delbetänkandet föreslår utredningen att den lagen ska upphävas (se SOU 2017:29 s. 145 f.).

14.2 En ny lag för Säkerhetspolisens personuppgiftsbehandling

14.2.1 Allmänna utgångspunkter

En fristående myndighet

Vid polisdatalagens tillkomst var Säkerhetspolisens en avdelning vid Rikspolisstyrelsen. Den tidigare gällande polisdatalagen (1998:622) gällde vid behandling av personuppgifter i polisens brottsbekämpande verksamhet vid Rikspolisstyrelsen, polismyndigheterna och Ekobrottsmyndigheten. Vid den nuvarande polisdatalagens tillkomst ansåg regeringen att detsamma borde gälla för den lagen (se prop. 2009/10:85 s. 71). Regeringen framhöll att Säkerhetspolisens verksamhet i stor utsträckning bedrivs på liknande sätt som annan polisverksamhet och att den reglering som föreslogs för polisen i

övrigt därför i många avseenden borde tillämpas även av Säkerhetspolisen. I förarbetena konstaterades dock att särdragen i Säkerhetspolisens verksamhet motiverade att vissa bestämmelser utformades på ett sätt som var mer anpassat till den verksamheten (se prop. 2009/10:85 s. 250 f.). Säkerhetspolisens behandling av personuppgifter i den brottsbekämpande verksamheten regleras därför i dag i ett särskilt kapitel i polisdatalagen.

När Säkerhetspolisen blev en fristående myndighet gjordes det vissa ändringar i polisdatalagen (se Den nya polisorganisationen – några frågor om personuppgiftsbehandling m.m., prop. 2014/15:94, s. 82 f.). Eftersom Säkerhetspolisens personuppgiftsbehandling var föremål för grundlig översyn när polisdatalagen infördes ansåg regeringen emellertid att det inte fanns något behov av att se över den materiella regleringen (se prop. 2013/14:110 s. 480 f.). Säkerhetspolisens personuppgiftsbehandling i den brottsbekämpande verksamheten regleras därför även efter omorganisationen i polisdatalagen.

Säkerhetspolisens verksamhet skiljer sig från Polismyndighetens

Även om Säkerhetspolisens och Polismyndighetens verksamhet i stor utsträckning bedrivs på liknande sätt, skiljer sig Säkerhetspolisens uppdrag från Polismyndighetens. Säkerhetspolisen har en betydligt mer begränsad verksamhet, inriktad på några få områden. Tyngdpunkten ligger på att förebygga och förhindra brott. Säkerhetspolisen har i uppdrag att skydda Sveriges demokratiska system, medborgarnas fri- och rättigheter och den nationella säkerheten. Säkerhetspolisens verksamhet rör därmed i princip uteslutande nationell säkerhet.

Säkerhetspolisens uppdrag är att förebygga, förhindra och upptäcka brottslig verksamhet som innefattar brott mot rikets säkerhet och terrorbrott och att utreda och beivra sådana brott och vissa andra brott. Arbetet förutsätter att myndigheten har förmåga att identifiera och kartlägga sådan brottslig verksamhet. Säkerhetspolisen behöver kunna behandla personuppgifter på ett tidigt stadium, innan en person eller en gruppering har konkreta brottsplaner eller har vidtagit åtgärder för att begå brott. Säkerhetspolisens arbete är alltså främst inriktat mot att identifiera planer på och förstadiet av

brottslig verksamhet. När Säkerhetspolisen identifierar brottslig verksamhet i ett så tidigt skede kan brottsligheten normalt förhindras. Då kan konkreta brottsliga gärningar vara svåra att urskilja. Säkerhetspolisens polisiära verksamhet fokuserar alltså på att förebygga och förhindra brott. Det innebär att det finns avgörande skillnader i Säkerhetspolisens verksamhet och arbetsmetoder jämfört med Polismyndighetens.

I motsats till vad som gäller för Polismyndigheten är Säkerhetspolisens brottsutredande verksamhet mycket liten och initieras endast undantagsvis genom anmälningar om brott. Vid misstanke om brott inleds förundersökning, som bedrivs enligt samma regler som gäller för Polismyndigheten. Vid misstanke om vissa brott ska utredningen alltid skötas av Säkerhetspolisen. Det gäller bl.a. spioneri, grovt spioneri, obehörig befattning med hemlig uppgift, grov obehörig befattning med hemlig uppgift, olovlig underrättelseverksamhet och vissa tryckfrihets- och yttrandefrihetsbrott. Förundersökningen leds alltid av åklagare. Säkerhetspolisen får även utreda vissa andra brott men kan avstå från det och överlämna frågan till Polismyndigheten. Under en förundersökning har Säkerhetspolisen samma befogenheter som Polismyndigheten och genomför exempelvis husrannsakan och förhör i syfte att få fram ett tillräckligt beslutsunderlag för åklagaren.

Säkerhetspolisen är också säkerhetstjänst

Säkerhetspolisen är, förutom polisiär myndighet, också nationell säkerhetstjänst. En säkerhetstjänst arbetar för att höja säkerhetsnivån i den egna staten. Det görs dels genom att avslöja och reducera säkerhetshot som riktas mot staten, dels genom att reducera sårbarheter. Säkerhetspolisen bedriver i egenskap av säkerhetstjänst underrättelse- och säkerhetsarbete. Myndigheten bedriver omfattande säkerhetsunderrättelseverksamhet för att ta fram hot- och sårbarhetsbedömningar. Verksamheten är inriktad på att avslöja om viss brottslighet kan komma att begås. Bedömningarna tjänar som underlag för beslut om vilka åtgärder Säkerhetspolisen ska vidta i sitt förebyggande arbete. De ligger också till grund för beslut om t.ex. personskydd eller andra säkerhetsskyddsåtgärder. Ett övergripande mål med säkerhetsunderrättelseverksamheten är att hämta in

kunskap som kan omsättas i operativ verksamhet (se En tydligare organisation för Säkerhetspolisen, SOU 2012:77, s. 56 f.).

Den brottslighet som Säkerhetspolisen ska förebygga har ofta koppling till andra stater. Det gäller inte minst bekämpning av terrorbrott. Säkerhetsunderrättelseverksamheten förutsätter därför ett väl fungerande informationsutbyte med utländska underrättelse- och säkerhetstjänster.

Brottsdatalagen gäller inte i Säkerhetspolisens verksamhet

Brottsdatalagen ska enligt 1 kap. 2 § gälla för behandling av personuppgifter som utförs i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet. Enligt 1 kap. 4 § gäller lagen dock inte vid Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet eller om Polismyndigheten har övertagit en arbetsuppgift som rör nationell säkerhet från Säkerhetspolisen.

Till Säkerhetspolisens huvuduppgifter hör som nyss nämnts att förebygga, förhindra och upptäcka brottslig verksamhet som innefattar brott mot rikets säkerhet och terrorbrott och att utreda och beivra sådana brott. Säkerhetspolisen ansvarar vidare för personskyddet av den centrala statsledningen. De uppgifterna avser nationell säkerhet. Säkerhetspolisen har även andra uppgifter som avser nationell säkerhet eller som har mycket nära samband med sådan verksamhet. Merparten av Säkerhetspolisens behandling av personuppgifter ligger härigenom utanför brottsdatalagens tillämpningsområde (se SOU 2017:29 s. 174 f.).

Dataskyddsförordningens tillämpning utvidgas

Nationell säkerhet har undantagits även från dataskyddsförordningens tillämpningsområde. Dataskyddsutredningen föreslår dock att dataskyddsförordningens tillämpningsområde ska utsträckas och gälla generellt, även vid sådan behandling av personuppgifter som inte omfattas av EU-rätten (se SOU 2017:39 s. 89 f.). Genom den regleringen säkerställs det enligt Dataskyddsutredningen att det finns ett fullgott skydd för behandlingen av personuppgifter

inom varje verksamhet. Genom förslaget kommer Säkerhetspolisens personuppgiftsbehandling att regleras av dataskyddsförordningen med kompletterande lagstiftning, om det inte finns avvikande bestämmelser.

14.2.2 En särskild lag för Säkerhetspolisens personuppgiftsbehandling

Utredningens förslag: Det ska införas en ny lag om Säkerhetspolisens behandling av personuppgifter och 6 kap. polisdatalagen ska upphävas. Den nya lagen ska benämnas Säkerhetspolisens datalag. När personuppgifter behandlas enligt den nya lagen ska lagen med kompletterande bestämmelser till EU:s dataskyddsförordning inte gälla.

Skälen för utredningens förslag

Förutsättningarna har förändrats

Säkerhetspolisen har lika stort behov av särregler för sin personuppgiftsbehandling när brottsdatalagen träder i kraft som myndigheten har i dag. Frågan är då om behovet av särreglering även fortsättningsvis bör tillgodoses genom särskilda regler i polisdatalagen eller om personuppgiftsbehandlingen bör regleras i en särskild lag.

Brottsdatalagen förutsätter att myndigheternas registerförfattningar ses över och anpassas till den nya regleringen. I avsnitt 5.2 föreslår utredningen att polisdatalagen ska gälla utöver brottsdatalagen. Många frågor som i dag regleras i polisdatalagen kommer då i stället att regleras i brottsdatalagen. Det medför att ett stort antal bestämmelser i polisdatalagen upphävs. Eftersom brottsdatalagen inte kommer att vara tillämplig i större delen av Säkerhetspolisens verksamhet och polisdatalagen kommer att anpassas till brottsdatalagen blir det komplicerat att reglera Säkerhetspolisens personuppgiftsbehandling i polisdatalagen. Det finns därför starka lagtekniska skäl som talar för att Säkerhetspolisens behandling av personuppgifter bör regleras i en särskild lag.

Dataskyddsförordningen görs generellt tillämplig

Enligt 1 kap. 4 § brottsdatalagen omfattas Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet inte av lagens tillämpningsområde. Samtidigt föreslår Dataskyddsutredningen att dataskyddsförordningen ska vara generellt tillämplig och omfatta även personuppgiftsbehandling som utförs i verksamhet som rör nationell säkerhet.

Eftersom dataskyddsförordningen varken är tillämplig på personuppgiftsbehandling som rör nationell säkerhet eller som utförs i brottsbekämpande syfte har bestämmelserna i förordningen inte skapats med beaktande av den typen av verksamhet. Merparten av bestämmelserna i förordningen är därmed inte anpassade till Säkerhetspolisens verksamhet och kan inte heller tillämpas direkt där. Att dataskyddsförordningen föreslås bli generellt tillämplig innebär inte att behovet av särregler för Säkerhetspolisens verksamhet har förändrats.

Dataskyddsutredningen föreslår att det på områden som inte regleras av EU-rätten ska vara möjligt att genom sektorsspecifik lagstiftning göra undantag från dataskyddsförordningens bestämmelser (se SOU 2017:39 s. 91 f.). Säkerhetspolisens verksamhet är av sådan karaktär att det med hänsyn både till effektivitets- och integritetsskäl krävs en reglering som avviker från dataskyddsförordningen. Eftersom verksamhet som rör nationell säkerhet ligger utanför förordningens tillämpningsområde behöver förordningens bestämmelser inte beaktas vid införandet av särregler.

En ny lag bör införas

Mot bakgrund av att det nationella regelverket för personuppgiftsbehandling kommer att förändras, att Säkerhetspolisens verksamhet förutsätter en delvis annan reglering och att Säkerhetspolisen numera är en självständig myndighet framstår det som lämpligast att bryta ut regleringen av Säkerhetspolisens personuppgiftsbehandling ur polisdatalagen och ta in den i en särskild lag.

Utredningen gör i delbetänkandet bedömningen att Säkerhetspolisen bör kunna tillämpa vissa bestämmelser i brottsdatalagen även i verksamhet som rör nationell säkerhet (se SOU 2017:29 s. 176). Eftersom Säkerhetspolisens personuppgiftsbehandling som

rör nationell säkerhet uttryckligen undantas från brottsdatalagens tillämpningsområde ter det sig dock mindre lämpligt att föreskriva att Säkerhetspolisen trots det ska tillämpa den lagen i vissa delar. Den nya lagen bör därför inte hänvisa till bestämmelser i brottsdatalagen. Den bör säkerställa att Säkerhetspolisen kan fortsätta att behandla personuppgifter på i huvudsak samma sätt som i dag och innehålla alla de bestämmelser som behövs för det.

Med hänsyn till att en ny lag föreslås bör bestämmelserna om Säkerhetspolisens personuppgiftsbehandling i 6 kap. polisdatalagen upphävas.

Lagens benämning

Flertalet registerförfattningar inom brottsdatalagens tillämpningsområde har ordet datalag i namnet, t.ex. polisdatalagen, åklagardatalagen och domstolsdatalagen. Även Tullverkets och Skatteverkets nya registerförfattningar innehåller ordet datalag. Utredningen har bl.a. av den anledningen valt att benämna den lag som genomför direktivet brottsdatalagen (se SOU 2017:29 s. 142 f.).

När det gäller övriga registerförfattningar föreslår utredningen som huvudregel att myndighetsnamnet tillsammans med ordet brottsdatalag ska bilda författningens namn, t.ex. Tullverkets brottsdatalag och Kustbevakningens brottsdatalag (se avsnitt 8.1.2 och 9.1.2). Eftersom Säkerhetspolisens personuppgiftsbehandling som rör nationell säkerhet undantas från brottsdatalagens tillämpningsområde kan den nya lagen inte gälla utöver brottsdatalagen på det sätt som föreslås för övriga myndigheter i rättskedjan (se avsnitt 5.2). Mot den bakgrunden är det inte lämpligt att kalla den nya lagen Säkerhetspolisens brottsdatalag. Det namnet skulle ge ett felaktigt intryck av att lagen har samma kopplingar till brottsdatalagen som övriga registerförfattningar.

Den nya lagen för Säkerhetspolisens personuppgiftsbehandling bör ha ett så enkelt och tydligt namn som möjligt. Samtidigt bör namnet återspegla lagens innehåll. Att knyta lagens namn till tillämpningsområdet skulle resultera i ett för långt namn. Ett namn med den utformningen kritiserades dessutom av Lagrådet när polisdatalagen granskades (se prop. 2009/10:85 s. 66 och 519). Enligt utredningens mening är de författningarnas namn som innehåller

ordet datalag tydliga och ändamålsenliga. Lagen bör därför benämnas Säkerhetspolisens datalag.

Förhållandet till lagen med kompletterande bestämmelser till EU:s dataskyddsförordning

Som nyss nämnts föreslår Dataskyddsutredningen att dataskyddsförordningens tillämpningsområde ska utsträckas till att omfatta även personuppgiftsbehandling som utförs i verksamhet som rör nationell säkerhet. Lagen (2018:000) med kompletterande bestämmelser till EU:s dataskyddsförordning föreslås vara subsidiär till avvikande bestämmelser i annan lag eller i förordning. Det bör tydliggöras i den nya lagen att dataskyddsförordningen och lagen med kompletterande bestämmelser till den inte i någon del ska tillämpas när Säkerhetspolisen behandlar personuppgifter enligt den nya lagen (jfr 1 kap. 1 § andra stycket lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet).

14.2.3 Lagens syfte

Utredningens förslag: Syftet med lagen ska vara att skydda fysiska personers grundläggande fri- och rättigheter i samband med behandling av personuppgifter och att säkerställa att Säkerhetspolisen kan behandla och utbyta personuppgifter på ett ändamålsenligt sätt.

Skälen för utredningens förslag: Enligt 1 kap. 1 § polisdatalagen är syftet med lagen att ge polisen möjlighet att behandla personuppgifter på ett ändamålsenligt sätt i sin brottsbekämpande verksamhet och att skydda människor mot att deras personliga integritet kränks vid sådan behandling. Enligt 1 kap. 1 § brottsdatalagen är syftet med lagen att skydda fysiska personers grundläggande fri- och rättigheter i samband med behandling av personuppgifter och att säkerställa att behöriga myndigheter kan behandla och utbyta personuppgifter med varandra på ett ändamålsenligt sätt.

Det har inte enbart en symbolisk eller informativ betydelse att uttryckligen slå fast lagens syfte. Att en lags syfte uttryckligen anges kan få relevans i rättstillämpningen genom att det ger vägledning för tolkningen av de materiella bestämmelserna i lagen (se SOU 2017:29 s. 144 f.). En bestämmelse som anger lagens syfte bör därför finnas i den nya lagen. Bestämmelsen bör formuleras som motsvarande bestämmelse i brottsdatalagen.

14.3 Lagens tillämpningsområde

14.3.1 Avgränsningen av tillämpningsområdet

Utredningens förslag: Lagen ska gälla vid behandling av personuppgifter som rör nationell säkerhet i Säkerhetspolisens brottsbekämpande och lagförande verksamhet.

Lagen ska gälla för sådan behandling av personuppgifter som är helt eller delvis automatiserad och för annan behandling av personuppgifter som ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

Skälen för utredningens förslag

Lagen ska gälla för behandling av personuppgifter som rör nationell säkerhet

I 1 kap. 4 § brottsdatalagen undantas Säkerhetspolisens personuppgiftsbehandling som rör nationell säkerhet från tillämpningsområdet. Den begränsade del av Säkerhetspolisens personuppgiftsbehandling som ligger inom brottsdatalagens tillämpningsområde ska därför inte omfattas av den nya lagen. Den får därmed ett något snävare tillämpningsområde än den nuvarande regleringen. Förändringen av tillämpningsområdet är dock marginell.

I 19 kap. brottsbalken används numera uttrycket Sveriges säkerhet i stället för det äldre rikets säkerhet. När uttrycket byttes ut konstaterade regeringen att innebörden av rikets säkerhet hade förändrats och blivit vidare. Regeringen konstaterade emellertid att rikets säkerhet har en tillräckligt klar och tydlig innebörd och att

uttrycket är väl etablerat i praxis. Regeringen ansåg därför att uttrycket även i framtiden borde tjäna som utgångspunkt för straffbestämmelserna i 19 kap. brottsbalken, men att det, på grund av att det var ålderdomligt, borde ändras till Sveriges eller landets säkerhet (se Förstärkt skydd mot främmande makts underrättelseverksamhet, prop. 2013/14:51, s. 20 och 36).

I betänkandet En ny säkerhetsskyddslag används också uttrycket Sveriges säkerhet. Utredningen om säkerhetsskyddslagen påtalar emellertid att det, mot bakgrund av att uttrycket är centralt i annan lagstiftning där orsaken till skyddsbehoven kan sägas vara snävare, finns viss risk för att tillämpningsområdet tolkas för snävt. Den utredningen diskuterar några andra uttryck, men stannar ändå för att använda Sveriges säkerhet i beskrivningen av det område som ska skyddas (se SOU 2015:25 s. 267 f.).

Undantagen från tillämpningsområdet utgår både i direktivet och dataskyddsförordningen från uttrycket nationell säkerhet. I delbetänkandet har utredningen bl.a. av det skälet valt att använda uttrycket nationell säkerhet för att avgränsa det som undantas från brottsdatalagens tillämpningsområde (se SOU 2017:29 s. 174 f.). Det uttrycket kan ges en något vidare innebörd än uttrycket Sveriges säkerhet. En fråga som rör nationell säkerhet i något av våra grannländer kan t.ex. vara av den karaktären att den även indirekt kan komma att påverka Sveriges nationella säkerhet. När det gäller gränsöverskridande terrorism är det av stor betydelse att Säkerhetspolisen både kan ta emot och lämna information som kan bidra till att förhindra terrorbrott, oavsett vilken stats nationella säkerhet som hotas. Uttrycket Sveriges säkerhet kan därför bli för snävt. Av det skälet och då det är viktigt att inget faller utanför brottsdatalagens och den nya lagens tillämpningsområde bör samma uttryck användas för att avgränsa tillämpningsområdet i båda lagarna.

Lagen ska gälla vid behandling av personuppgifter i brottsbekämpande och lagförande verksamhet

Brottsdatalagens tillämpningsområde avgränsas framför allt genom syftet med behandlingen. Det beror på att direktivets tillämpningsområde är avgränsat på det sättet (se SOU 2017:29 s. 159 f.). I direktivet och dataskyddsförordningen anges att de inte ska tilläm-

pas på behandling som utgör ett led i en verksamhet som inte omfattas av unionsrätten. Säkerhetspolisens verksamhet ligger därmed som nyss nämnts till allra största delen utanför både direktivets och förordningens tillämpningsområde. Syftet med behandlingen behöver därför inte användas för att avgränsa tillämpningsområdet för den nya lagen. Tillämpningsområdet bör i stället, på samma sätt som i dag, kopplas till Säkerhetspolisens verksamhet.

Frågan är om tillämpningsområdet i den nya lagen bör avgränsas på samma sätt som i polisdatalagen, dvs. genom en hänvisning till brottsbekämpande verksamhet, eller genom någon annan formulering, t.ex. operativ verksamhet (jfr 1 kap. 2 § åklagardatalagen).

I förarbetena till polisdatalagen konstaterar regeringen att arbetet inom Säkerhetspolisens olika verksamhetsområden är förebyggande och ytterst syftar till att förhindra att brott begås och att det därför får anses utgöra en del av Säkerhetspolisens brottsbekämpande verksamhet (se prop. 2009/10:85 s. 255 f.). Därför räknas samtliga områden där myndigheten bedriver verksamhet upp i 6 kap. 1 § polisdatalagen som reglerar för vilka ändamål personuppgifter får behandlas. Även i senare förarbeten har det uttalats att all verksamhet vid Säkerhetspolisen i någon mån är brottsbekämpande (se prop. 2013/14:110 s. 480 f.). Det talar för att uttrycket brottsbekämpande verksamhet bör användas även i den nya lagen.

Även om all Säkerhetspolisens verksamhet har ansetts vara i någon mån brottsbekämpande finns det delar av verksamheten som inte har ett lika tydligt brottsbekämpande syfte som övrig verksamhet. Det beror på att Säkerhetspolisen också är en säkerhetstjänst. I den rollen arbetar Säkerhetspolisen för att höja nivån på säkerheten i Sverige. Verksamheten är främst inriktad på att bedöma om viss säkerhetshotande brottslighet kan antas komma att begås. Bedömningarna tjänar som underlag för beslut om vilka åtgärder Säkerhetspolisen vidtar i sitt förebyggande arbete. De ligger också till grund för beslut om t.ex. personskydd för den centrala statsledningen eller andra säkerhetsskyddsåtgärder. Eftersom verksamheten och åtgärderna är inriktade på att förebygga att säkerhetshot skapas och kan förverkligas kan de indirekt sägas ha brottsbekämpande syfte.

Det kan diskuteras om Säkerhetspolisens roll som säkerhetstjänst gör det lämpligare att använda ett annat uttryck än brottsbekämpning. Uttrycket operativ verksamhet skulle kunna användas

för att avgränsa lagens tillämpningsområde. Ett alternativ skulle kunna vara att låta lagen omfatta brottsbekämpande och annan operativ verksamhet. Det har inte framkommit några problem med att använda uttrycket brottsbekämpande verksamhet för att avgränsa tillämpningsområdet. Inarbetade begrepp bör inte ändras om inte starka skäl talar för det. Även om det skulle finnas fördelar med ett annat uttryck talar enligt utredningens mening övervägande skäl för att behålla samma avgränsning som i dag.

Med brottsbekämpning avses i dag både arbetsuppgifterna att förebygga, förhindra och upptäcka brottslig verksamhet och att utreda och beivra brott. I brottsdatalagen görs det emellertid skillnad mellan brottsbekämpning och lagföring. Det beror på att direktivet är utformat på det sättet. Uppgiften att beivra brott hänförs till lagföring. Brottsbekämpning har därmed i brottsdatalagen fått en snävare innebörd än i dag (se avsnitt 5.4.6). Brottsbekämpning bör ha samma innebörd i den nya lagen. Säkerhetspolisen har enligt sin instruktion i uppgift att utreda och beivra, dvs. lagföra, vissa typer av brott. Den nuvarande regleringen omfattar således även lagföring. Den nya lagen bör därför gälla personuppgiftsbehandling som rör nationell säkerhet i Säkerhetspolisens brottsbekämpande och lagförande verksamhet.

Intern och administrativ verksamhet bör inte omfattas

För Säkerhetspolisens behandling av personuppgifter i intern och administrativ verksamhet gäller i dag personuppgiftslagen. Som exempel på administrativ verksamhet kan nämnas personalfrågor och ekonomihantering. Exempel på interna åtgärder är framtagande av interna föreskrifter, handböcker och policydokument.

Viss behandling av personuppgifter som utförs i Säkerhetspolisens interna eller administrativa verksamhet kan vara av sådan karaktär att den gäller nationell säkerhet, t.ex. vissa personaladministrativa ärenden. När det gäller vissa kategorier av anställda vid Säkerhetspolisen anses i princip alla uppgifter om den anställde och hans eller hennes anställning röra nationell säkerhet, t.ex. tidsrapportering, ledighetsansökningar och tjänsteresor. Sekretess gäller därför i större utsträckning än normalt för uppgifter som rör Säkerhetspolisens personal (se t.ex. 15 kap. 2 § och 18 kap. 2 och

5 §§ offentlighets- och sekretesslagen). Det ska inte vara möjligt för en annan stat att med hjälp av offentliga uppgifter kunna kartlägga hela Säkerhetspolisens organisation, även om öppenheten är mycket större i Sverige än i många andra stater.

I den mån personuppgifter behandlas i intern och administrativ verksamhet görs det för andra syften än brottsbekämpning. Behandlingen bygger dessutom som regel på samtycke från den enskilde. Det har därför inte ansetts nödvändigt att specialreglera behandlingen av personuppgifter i sådan verksamhet (se t.ex. prop. 2014/15:63 s. 45). Enligt utredningens mening finns det inte anledning att göra någon annan bedömning när det gäller Säkerhetspolisens personuppgiftsbehandling i sådan verksamhet. Mot den bakgrunden anser utredningen att det inte finns skäl att låta den nya lagen omfatta personuppgiftsbehandling i intern och administrativ verksamhet ens om behandlingen rör nationell säkerhet.

Helt eller delvis automatiserad behandling

Den nya lagen bör på samma sätt som i dag gälla för behandling av personuppgifter som är helt eller delvis automatiserad och för annan behandling av personuppgifter som ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

14.3.2 Ska andra myndigheter tillämpa lagen?

Utredningens förslag: Polismyndigheten ska tillämpa den nya lagen när myndigheten har övertagit en arbetsuppgift som rör nationell säkerhet från Säkerhetspolisen.

Skälen för utredningens förslag

Polismyndigheten

Enligt 28 § förordningen med instruktion för Polismyndigheten ska myndigheten bistå vid polisverksamhet som leds av Säkerhetspolisen om Säkerhetspolisen i ett enskilt fall begär det och det inte

finns särskilda skäl mot det. Polismyndigheten ska vidare, i den utsträckning som myndigheterna kommer överens om, lämna tekniskt biträde och annan hjälp till Säkerhetspolisen. Enligt 15 § instruktionen för Säkerhetspolisen får biträdande säkerhetspolischefen i samråd med chefen för Nationella operativa avdelningen, trots den ansvarsfördelning som annars gäller mellan myndigheterna, i ett enskilt fall bestämma att en förundersökning eller annan uppgift i den brottsbekämpande verksamheten ska lämnas över till Polismyndigheten för fortsatt handläggning.

Eftersom det när Säkerhetspolisen begär biträde av Polismyndigheten eller överlämnar en arbetsuppgift till myndigheten med stöd av 15 § instruktionen för Säkerhetspolisen i de flesta fall är fråga om en arbetsuppgift som rör nationell säkerhet, föreslår utredningen i delbetänkandet att Polismyndigheten inte ska tillämpa brottsdatalagen i vidare mån än vad Säkerhetspolisen skulle ha gjort om uppgiften legat kvar där (se SOU 2017:29 s. 178). I dessa fall bör Polismyndigheten i stället tillämpa den särreglering som gäller för Säkerhetspolisen. Det bör därför framgå av den nya lagen att den gäller för Polismyndigheten i vissa situationer. Skulle det vara fråga om en arbetsuppgift i brottsbekämpningen som inte rör nationell säkerhet skulle Säkerhetspolisen tillämpa brottsdatalagen om uppgiften legat kvar där och då bör även Polismyndigheten tillämpa den regleringen om den biträder eller övertar arbetsuppgiften från Säkerhetspolisen.

Försvarsmakten

Säkerhetspolisen får enligt 1 § andra stycket lagen (2006:343) om Försvarsmaktens stöd till polisen vid terrorismbekämpning begära visst stöd från Försvarsmakten. Som framgår av delbetänkandet bör Försvarsmakten i sådana situationer inte tillämpa brottsdatalagen i vidare mån än vad Säkerhetspolisen skulle ha gjort i samma situation (se SOU 2017:29 s. 178). Enligt utredningens mening är det inte heller lämpligt att Försvarsmakten tillämpar Säkerhetspolisens nya lag i sådana situationer. Den reglering som gäller för Försvarsmaktens verksamhet bör i stället tillämpas.

14.3.3 Säkerhetspolisen ska även tillämpa brottsdatalagen

Utredningens förslag: Det ska framgå genom en hänvisning att Säkerhetspolisen ska tillämpa brottsdatalagen och polisens brottsdatalag vid behandling av personuppgifter i frågor som inte rör nationell säkerhet.

Skälen för utredningens förslag: Även om merparten av Säkerhetspolisens personuppgiftsbehandling rör nationell säkerhet och därför undantas från brottsdatalagens tillämpningsområde, omfattas viss behandling i myndighetens brottsbekämpande verksamhet av brottsdatalagen och polisens brottsdatalag (se avsnitt 7.2.1). Den nya lagen bör innehålla en bestämmelse som upplyser om att de lagarna i vissa fall är tillämpliga.

14.4 Regleringen ska utgå från regleringen i polisdatalagen

Anledningen till att utredningen föreslår att Säkerhetspolisens personuppgiftsbehandling ska regleras i en särskild lag är främst att EU:s dataskyddsreform medför andra krav än i dag på regelverket för nationell personuppgiftsbehandling. Regleringen i polisdatalagen av Säkerhetspolisens personuppgiftsbehandling är relativt ny och den har i allt väsentligt fungerat som avsett. Enligt utredningens direktiv ska en utgångspunkt vara att regleringen av Säkerhetspolisens personuppgiftsbehandling nyligen har moderniserats och bedömts vara ändamålsenlig (dir. 2016:21 s. 13). Bestämmelserna i polisdatalagen bör därför till stor del kunna bilda mönster för bestämmelserna i den nya lagen.

Då den nya lagen ska vara heltäckande kommer den dock att bli betydligt mer omfattande än den nuvarande regleringen för Säkerhetspolisen. Den bör därför indelas i kapitel. Det kan också finnas skäl att överväga om några av de nya bestämmelser som föreslås i polisens brottsdatalag även bör tas in i den nya regleringen för Säkerhetspolisen.

Eftersom varken direktivet eller dataskyddsförordningen omfattar behandling av personuppgifter som utförs i verksamhet som rör nationell säkerhet finns det ur EU-rättslig synvinkel inte något

som hindrar att den nya lagen utformas på annat sätt än brottsdatalagen. Den EU-rättsliga regleringen bygger emellertid på och vidareutvecklar dataskyddskonventionen. Konventionen gäller även i verksamhet som rör nationell säkerhet och Sverige är folkrättsligt bundet av konventionen med dess tilläggsprotokoll. En särreglering av Säkerhetspolisens personuppgiftsbehandling får således inte strida mot bestämmelserna i dataskyddskonventionen.

Även om det EU-rättsliga regelverket inte är tillämpligt på behandling av personuppgifter i verksamhet som rör nationell säkerhet bör särregleringen för Säkerhetspolisen enligt utredningens mening ändå till största delen följa brottsdatalagens systematik och innehåll. Det är en fördel eftersom myndigheten kommer att tillämpa båda regelverken i sin verksamhet.

14.5 Allmänna bestämmelser

14.5.1 Förhållandet till annan lagstiftning

Utredningens förslag: Avvikande bestämmelser om behandling av personuppgifter i lagen om internationellt polisiärt samarbete eller i föreskrifter som meddelats i anslutning till den lagen ska tillämpas i stället för bestämmelserna i den nya lagen.

Bestämmelserna i den nya lagen ska inte tillämpas i den utsträckning det skulle inskränka skyldigheten enligt 2 kap. tryckfrihetsförordningen att lämna ut personuppgifter.

Skälen för utredningens förslag: Av 1 kap. 4 § polisdatalagen framgår att om det i lagen om internationellt polisiärt samarbete finns avvikande bestämmelser om behandling av personuppgifter, ska de bestämmelserna tillämpas i stället för polisdatalagen. I övrigt tillämpas de generella bestämmelserna i polisdatalagen, inklusive vissa bestämmelser i personuppgiftslagen, vid behandling av personuppgifter enligt lagen och förordningen om internationellt polisiärt samarbete.

Säkerhetspolisen tillämpar bestämmelserna i lagen om internationellt polisiärt samarbete vid samarbete med andra stater. Den ordningen bör gälla även i fortsättningen. Det bör därför i den nya lagen finnas en bestämmelse som tydliggör förhållandet till lagen

och förordningen om internationellt polisiärt samarbete. Det kräver en följdändring i uppräkningslagen i 6 kap. 1 § lagen om internationellt polisiärt samarbete.

Av 8 § första stycket personuppgiftslagen framgår att personuppgiftslagen inte ska tillämpas i den utsträckning det skulle inskränka en myndighets skyldighet att lämna ut personuppgifter enligt 2 kap tryckfrihetsförordningen. I 2 kap. 2 § första stycket 2 polisdatalagen hänvisas till 8 § i personuppgiftslagen, vilket innebär att den bestämmelsen gäller för personuppgiftsbehandling hos Säkerhetspolisen. En bestämmelse som motsvarar 8 § första stycket personuppgiftslagen bör tas in i den nya lagen.

14.5.2 Personuppgiftsansvar

Utredningens förslag: Säkerhetspolisen ska vara personuppgiftsansvarig för den personuppgiftsbehandling som myndigheten utför. Polismyndigheten ska vara personuppgiftsansvarig för den behandling som myndigheten utför. Personuppgiftsansvaret ska omfatta all behandling av personuppgifter som utförs under respektive myndighets ledning eller på dess vägnar.

Säkerhetspolisen ska få vara gemensamt personuppgiftsansvarig med annan endast i den utsträckning det följer av lag eller förordning eller om regeringen i ett enskilt fall beslutar om det.

Skälen för utredningens förslag

Det ska framgå vem som är personuppgiftsansvarig

Enligt 6 kap. 5 § första stycket polisdatalagen är Säkerhetspolisen personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför. Det bör även gälla enligt den nya lagen. Eftersom Polismyndigheten i vissa fall ska tillämpa lagen bör myndigheten vara personuppgiftsansvarig för den behandlingen.

I 3 kap. 1 § brottsdatalagen föreskrivs att den personuppgiftsansvarige är ansvarig för all behandling av personuppgifter som utförs under dennes ledning eller på dennes vägnar. Det bör gälla även enligt den nya lagen. På så sätt tydliggörs att personuppgiftsansvaret omfattar dels den personuppgiftsbehandling som förekommer

vid respektive myndighet, dels den personuppgiftsbehandling som ett personuppgiftsbiträde utför på någon av myndigheternas vägnar. Det är myndigheten som är personuppgiftsansvarig, inte chefen eller någon anställd. Ytterst är det dock respektive myndighets chef som bär ansvaret för hur personuppgifter behandlas.

Gemensamt personuppgiftsansvar bara om statsmakterna medger det

Utredningen redogör i delbetänkandet för sin syn på gemensamt personuppgiftsansvar inom brottsdatalogens tillämpningsområde. Där framgår att sådant ansvar endast bör övervägas i speciella situationer där samarbetet mellan behöriga myndigheter är utformat så att ansvarsfördelningen inte kan utläsas på annat sätt. Bedömningen av när gemensamt personuppgiftsansvar är sakligt motiverat bör enligt förslaget inte lämnas till de behöriga myndigheterna själva utan göras av riksdagen eller regeringen (se SOU 2017:29 s. 362 f.). I 3 kap. 21 § brottsdatalogen föreskrivs därför att två eller flera behöriga myndigheter får vara gemensamt personuppgiftsansvariga endast i den utsträckning det följer av lag eller förordning eller om regeringen i ett enskilt fall beslutar om det. I delbetänkandet diskuterar utredningen ingående skillnaden mellan delat ansvar och gemensamt ansvar (se SOU 2017:29 s. 360 f.).

Det som sägs om gemensamt personuppgiftsansvar i delbetänkandet gör sig gällande även för Säkerhetspolisen. Det bör därför i den nya lagen tas in en bestämmelse som föreskriver att gemensamt personuppgiftsansvar endast får förekomma i den utsträckning det följer av lag eller förordning eller om regeringen i ett enskilt fall beslutar om det.

14.5.3 Definitioner

Utredningens förslag: Vissa uttryck som används i den nya lagen ska definieras. Definitionerna ska i allt väsentligt stämma överens med dem som används i brottsdatalogen.

Skälen för utredningens förslag: I 3 § personuppgiftslagen definieras vissa uttryck som är centrala vid behandling av personuppgifter. Den bestämmelsen gäller för Säkerhetspolisen, vilket framgår genom hänvisningar i 2 kap. 2 § och 6 kap. 4 § polisdatalagen.

I 1 kap. 6 § brottsdatalagen definieras vissa uttryck som används i den lagen. Motsvarande reglering bör finnas i den nya lagen. Definitionerna bör så långt möjligt stämma överens med dem som används i brottsdatalagen.

Uttrycken behandling av personuppgifter, biometriska uppgifter, dataskyddsombud, genetiska uppgifter, internationell organisation, mottagare, personuppgift, personuppgiftsansvarig, personuppgiftsbiträde, registrerad, tredje man och uppgift som rör hälsa bör definieras i den nya lagen och ha samma innebörd som i brottsdatalagen (se SOU 2017:29 s. 148 f.).

Utredningen återkommer till definitionen av tillsynsmyndighet i avsnitt 15.3 och till definitionen av tredjeland i avsnitt 14.17.1.

I polisdatalagen definieras även uttrycken dna-analys, dna-profil och fingeravtryck. De används inte i den nya lagen och det finns därför inte något behov av att definiera dem.

14.5.4 Uppgifter om juridiska personer

Utredningens förslag: Lagen ska i viss utsträckning tillämpas vid behandling av uppgifter om juridiska personer.

Skälen för utredningens förslag: I 1 kap. 6 § polisdatalagen föreskrivs att vissa bestämmelser i lagen även ska tillämpas på uppgifter om juridiska personer. För Säkerhetspolisen gäller det bestämmelserna om ändamålen med behandlingen, tillgången till personuppgifter, bevarande och gallring och gemensamt tillgängliga uppgifter. Utredningen föreslår i avsnitt 5.4.1 att bestämmelser om skydd för uppgifter om juridiska personer i övriga registerförfattningar ska behållas. Eftersom det bör gälla även för Säkerhetspolisen bör den nya lagen ha en motsvarande reglering.

14.6 Ändamål och rättsliga grunder för behandlingen

14.6.1 Ändamål för behandling av personuppgifter

Utredningens förslag: Säkerhetspolisen ska få behandla personuppgifter bara för särskilda, uttryckligt angivna och berättigade ändamål. Personuppgifter ska inte få behandlas för något ändamål som är oförenligt med det ändamål för vilket personuppgifterna ursprungligen behandlades.

Säkerhetspolisen ska få behandla personuppgifter för vetenskapliga, statistiska eller historiska ändamål inom den nya lagens tillämpningsområde.

Skälen för utredningens förslag

Behandling för särskilda, uttryckligt angivna och berättigade ändamål.

Det grundläggande kravet på att personuppgifter får samlas in bara för särskilda, uttryckligt angivna och berättigade ändamål finns i 9 § första stycket c personuppgiftslagen. Kravet gäller för Säkerhetspolisens personuppgiftsbehandling genom hänvisningar i 2 kap. 2 § och 6 kap. 4 § polisdatalagen. En liknande bestämmelse bör tas in i den nya lagen.

I delbetänkandet redovisar utredningen vad som avses med särskilda, uttryckligt angivna och berättigade ändamål (se SOU 2017:29 s. 243 f.). En mycket stor del av den information som Säkerhetspolisen behandlar är underrättelseinformation. I underrättelseverksamhet, där personuppgifter behandlas på ett tidigt stadium i processen, är det långtifrån alltid möjligt att ange ändamålen för behandlingen lika tydligt och detaljerat som i annan brottsbekämpande verksamhet. I Säkerhetspolisens verksamhet går det exempelvis inte att urskilja lika tydliga kopplingar till konkreta brott eller till brottslig verksamhet som i annan brottsbekämpande verksamhet. Å andra sidan är Säkerhetspolisens verksamhet inriktad mot ett fåtal väl avgränsade företeelser som är av särskilt samhällsfarlig karaktär (se prop. 2009/10:85 s. 256). Det får därför accepteras att beskrivningen av ändamålen inte alltid kan ha samma precision som i annan brottsbekämpande verksamhet. Utredningen

återkommer till frågan om att ändamålen i vissa fall ska framgå genom en särskild upplysning (se avsnitt 14.9.2).

Behandling för nya ändamål

Av 9 § första stycket d personuppgiftslagen följer att personuppgifter inte får behandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in. Bestämmelsen ger uttryck för den s.k. finalitetsprincipen som gäller för Säkerhetspolisen genom hänvisningar i 2 kap. 2 § och 6 kap. 4 § polisdatalagen.

I 2 kap. 4 § brottsdatalagen föreskrivs att det, innan personuppgifter får behandlas för ett nytt ändamål inom lagens tillämpningsområde, ska säkerställas att det finns en tillåten rättslig grund för den nya behandlingen och att behandlingen är nödvändig och proportionerlig för det nya ändamålet. Att en sådan bedömning ska göras vid behandling för nya ändamål inom brottsdatalagens tillämpningsområde framgår av artikel 4.2 i direktivet. Finalitetsprincipen regleras emellertid också i direktivet. I artikel 4.1 b anges att personuppgifter inte får behandlas på ett sätt som står i strid med de ändamål som uppgifterna samlades in för. Som framgår av delbetänkandet gör utredningen bedömningen att all behandling för ändamål inom direktivets tillämpningsområde ska anses vara förenlig med insamlingsändamålen, under förutsättning att behandlingen är nödvändig och står i proportion till det nya ändamålet. Någon prövning mot det ursprungliga ändamålet behöver således inte göras vid behandling för nya ändamål inom brottsdatalagens tillämpningsområde (se SOU 2017:29 s. 247 f.). Eftersom bestämmelserna i dataskyddsförordningen ska tillämpas vid behandling för ändamål utanför brottsdatalagens tillämpningsområde ska någon prövning mot det ursprungliga ändamålet inte göras då heller. Det beror på att den behandlingen blir ursprungsbehandling enligt förordningen och att det därför inte är fråga om någon vidarebehandling där finalitetsprincipen ska tillämpas (se SOU 2017:29 s. 292 f.). Finalitetsprincipen regleras därför inte i brottsdatalagen.

Säkerhetspolisen behöver i likhet med andra brottsbekämpande myndigheter kunna behandla personuppgifter för nya ändamål, t.ex. använda information från en förundersökning för att förebygga nya brott. Frågan är om prövningen enligt finalitetsprincipen

bör ersättas av samma prövning av nödvändighet och proportionalitet som för övriga brottsbekämpande myndigheter.

Kraven på nödvändighet och proportionalitet i brottsdatalagen har sin grund i direktivet. Säkerhetspolisens är inte bunden av de kraven, eftersom behandling av personuppgifter som rör nationell säkerhet undantas från direktivets tillämpningsområde. Det finns därför inget som hindrar att en reglering som bygger på finalitetsprincipen väljs för Säkerhetspolisens. Utredningen anser att det med tanke på Säkerhetspolisens uppdrag finns fördelar med att behålla den inarbetade ordningen. Finalitetsprincipen bör därför fortsätta att gälla för Säkerhetspolisens behandling av personuppgifter för nya ändamål.

När Säkerhetspolisens ska behandla personuppgifter för nya ändamål bör myndigheten alltid pröva om det nya ändamålet är förenligt med det ändamål som personuppgifterna samlades in för. Eftersom verksamheten är inriktad på att bekämpa brott som är systemhotande kan Säkerhetspolisens behandling av personuppgifter för nya ändamål för den egna verksamheten i de allra flesta fall anses förenlig med ursprungsåndamålet. Vad som bör gälla när myndigheten behandlar personuppgifter för att tillhandahålla information som behövs i annan verksamhet tas upp i avsnitt 14.6.5.

Behandling för vetenskapliga, statistiska och historiska ändamål

Enligt 9 § andra stycket personuppgiftslagen ska behandling av personuppgifter för historiska, statistiska eller vetenskapliga ändamål inte anses oförenlig med de ändamål för vilka personuppgifterna samlades in. Bestämmelsen gäller genom hänvisningar i 2 kap. 2 § och 6 kap. 4 § polisdatalagen för Säkerhetspolisens och innebär att personuppgifter som regel får behandlas för sådana ändamål.

I 2 kap. 5 § brottsdatalagen föreskrivs att en behörig myndighet får behandla personuppgifter för vetenskapliga, statistiska eller historiska ändamål inom lagens tillämpningsområde. Genom att det lyfts fram att behandling av personuppgifter kan inbegripa vetenskaplig, statistisk eller historisk användning blir det tydligt att lagens övriga bestämmelser ska tillämpas även vid behandling för sådana ändamål (se SOU 2017:29 s. 253 f.). Behandling för vetenskapliga, statistiska och historiska ändamål bör vara tillåten enligt

den nya lagen. Bestämmelsen bör formuleras på samma sätt som motsvarande bestämmelse i brottsdatalagen.

14.6.2 Primära och sekundära ändamålsbestämmelser är bestämmelser om rättslig grund

Utredningens bedömning: Det som i dag kallas primära och sekundära ändamålsbestämmelser är en del av den rättsliga grunden för behandling av personuppgifter. Regleringen bör ha i huvudsak samma innehåll som i dag.

Det bör på samma sätt som i dag göras skillnad mellan Säkerhetspolisens behandling av personuppgifter för den egna verksamhetens behov och behandling för att tillhandahålla information för andras behov.

Skälen för utredningens bedömning

De primära ändamålsbestämmelserna

I 6 kap. 1 och 2 §§ polisdatalagen anges för vilka ändamål Säkerhetspolisen får behandla personuppgifter i sin brottsbekämpande verksamhet. Ändamålen delas upp i primära och sekundära på samma sätt som i 2 kap. 7 och 8 §§ polisdatalagen.

I avsnitt 6.1.3 konstaterar utredningen att vad som i dataskyddsrättslig mening är tillåtna rättsliga grunder för behandling och vad som är renodlade ändamålsbestämmelser ibland har blandats samman. En ändamålsbestämmelse bör enligt utredningens mening ge ledning för prövningen av vilka personuppgifter som är adekvata och relevanta för behandlingen. Utredningen anser att 2 kap. 7 § polisdatalagen inte är en ändamålsbestämmelse i egentlig mening utan att den är en del av den rättsliga grunden och anger ramen för när personuppgifter får behandlas.

Regleringen i 6 kap. 1 § polisdatalagen är delvis annorlunda utformad än de primära ändamålsbestämmelserna i övriga registerförfattningar. Paragrafen är mer detaljerad. Trots det ger den enligt utredningens mening inte någon egentlig ledning för prövningen av vilka personuppgifter som får behandlas. Det anges endast att

Säkerhetspolisen får behandla personuppgifter för att utföra vissa av sina arbetsuppgifter. Syftet är att precisera när personuppgifter alls får behandlas i Säkerhetspolisens brottsbekämpande verksamhet. Paragrafen utgör den yttre ram inom vilken de särskilda, uttryckligt angivna och berättigade ändamålen med behandlingen i enskilda fall ska bestämmas. Den är därför av samma skäl som de primära ändamålsbestämmelserna i övriga registerförfattningar inte en ändamålsbestämmelse i egentlig mening, utan en del av den rättsliga grunden. Regleringen bör som utredningen utvecklar i avsnitt 14.6.3 i huvudsak ha samma innehåll som i dag.

De sekundära ändamålsbestämmelserna

De sekundära ändamålsbestämmelserna i 6 kap. 2 § polisdatalagen reglerar i vilken utsträckning personuppgifter som behandlas för något primärt ändamål även får behandlas för att tillhandahållas andra för att tillgodose deras behov. De reglerar alltså behandling för nya ändamål.

Paragrafen motsvarar till stor del Polismyndighetens sekundära ändamålsbestämmelser i 2 kap. 8 § polisdatalagen. I avsnitt 6.1.3 konstaterar utredningen att i princip alla punkter i den paragrafen är så allmänt hållna att de inte ger någon egentlig ledning för prövningen av vilka personuppgifter som får behandlas. De är därför inte att anse som ändamålsbestämmelser i egentlig mening utan som bestämmelser om rättslig grund. Säkerhetspolisens sekundära ändamålsbestämmelser har utformats på samma sätt som Polismyndighetens och utredningen gör därför samma bedömning beträffande innehållet i 6 kap. 2 §. Regleringen bör som utvecklas i avsnitt 14.6.5 i huvudsak ha samma innehåll som i dag.

Skillnaden mellan behandling för egna behov och andras behov behålls

Regleringen av Säkerhetspolisens personuppgiftsbehandling skiljer i dag mellan behandling för den egna brottsbekämpande verksamhetens behov och behandling för att tillhandahålla information för andras behov. När personuppgifter lämnas ut som ett led i myndig-

hetens egen brottsbekämpande verksamhet, inte i syfte att tillgodose någon annans behov, omfattas det av de primära ändamålen.

Som utredningen konstaterar i avsnitt 6.3.2 och 6.4.2 är det varken möjligt eller lämpligt att behålla den nuvarande utformningen av de sekundära ändamålsbestämmelserna för övriga brottsbekämpande myndigheter. Det beror på att direktivet ställer nya krav på att en prövning alltid ska föregå varje behandling för nya ändamål, vilket innebär att finalitetsprincipen inte ska tillämpas. Som framgår av avsnitt 14.6.1 är Säkerhetspolisen inte bunden av kravet på sådan prövning, eftersom behandling av personuppgifter som rör nationell säkerhet undantas från direktivets tillämpningsområde. Det finns inte heller något annat hinder mot att tillämpa finalitetsprincipen vid Säkerhetspolisens personuppgiftsbehandling. Utredningen anser därför att den nuvarande regleringen som bygger på en uppräkningslista av olika situationer där utlämnande kan komma i fråga och som kompletteras med en möjlighet att tillämpa finalitetsprincipen i enskilda fall bör behållas (se avsnitt 14.6.5).

En konsekvens av att regleringen i huvudsak kommer att se ut som i dag är att skillnaden mellan behandling för egna behov och för andras behov består. Säkerhetspolisens reglering kommer däri-genom att skilja sig från övriga brottsbekämpande myndigheters.

14.6.3 Rättslig grund för behandling – huvudregeln

Utredningens förslag: Säkerhetspolisen ska få behandla personuppgifter om det är nödvändigt för att utföra en arbetsuppgift i syfte att

1. förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar
 - a) brott mot rikets säkerhet,
 - b) terrorbrott, eller
 - c) tryckfrihetsbrott eller yttrandefrihetsbrott med rasistiska eller främlingsfientliga motiv,
2. utreda eller lagföra sådana brott som avses i 1, eller, efter särskilt beslut, annat brott,
3. fullgöra uppgifter
 - a) i samband med personskydd av den centrala statsledningen och andra som regeringen eller Säkerhetspolisen bestämmer,
 - b) enligt säkerhetsskyddslagen (1996:627), eller
 - c) enligt utlännings- och medborgarskapslagstiftningen,
4. fullgöra annan arbetsuppgift som rör nationell säkerhet och som anges i lag eller förordning eller särskilt beslut av regeringen, eller
5. fullgöra förpliktelser som följer av internationella åtaganden.

Arbetsuppgiften ska framgå av en lag, en förordning eller ett särskilt beslut i vilket regeringen uppdragit åt myndigheten att ansvara för en sådan uppgift.

Skälen för utredningens förslag

En bestämmelse om tillåtna rättsliga grunder behövs

Som konstateras i avsnitt 6.1.2 krävs det både en rättslig grund i form av en reglerad arbetsuppgift och bestämmelser om att personuppgifter får behandlas för att utföra arbetsuppgiften för att personuppgiftsbehandling ska vara tillåten. Detsamma bör gälla för Säkerhetspolisen. Det bör därför finnas en bestämmelse i den nya

lagen som anger de tillåtna rättsliga grunderna för personuppgiftsbehandlingen.

Regleringen i 6 kap. 1 § polisdatalagen korresponderar i princip med 3 § polislagen som anger Säkerhetspolisens huvudsakliga arbetsuppgifter. Bestämmelsen har endast förändrats marginellt sedan polisdatalagens tillkomst. Den bedömning av Säkerhetspolisens behov av att behandla personuppgifter som gjordes då gör sig fortfarande gällande (se prop. 2009/10:85 s. 255 f.). Enligt utredningens mening bör den nya lagen i huvudsak innehålla samma reglering. Terminologin bör anpassas så att den stämmer överens med terminologin i brottsdatalagen och de övriga registerförfattningarna. Det bör dessutom anges att arbetsuppgifterna ska framgå av en lag, en förordning, eller ett särskilt beslut i vilket regeringen uppdragit åt myndigheten att ansvara för en viss arbetsuppgift.

Enligt 6 kap. 1 § 5 polisdatalagen får Säkerhetspolisen behandla personuppgifter om det behövs för att lämna tekniskt biträde till vissa andra brottsbekämpande myndigheter. Den arbetsuppgiften kommer att omfattas av brottsdatalagens tillämpningsområde (se avsnitt 7.2.1). Personuppgiftsbehandling för sådant biträde bör därför inte regleras i den nya lagen.

Uppgifter enligt utlännings- och medborgarskapslagstiftningen

Som redovisas i avsnitt 14.1.1 har Säkerhetspolisen vissa uppgifter enligt utlännings- och medborgarskapslagstiftningen. Det framgår inte av förarbetena till polisdatalagen hur lagstiftaren ser på personuppgiftsbehandling för sådana ändamål.

I förarbetena till utlänningsdatalagen (2016:27) konstaterar regeringen att all verksamhet hos Säkerhetspolisen i någon mening är brottsbekämpande. Mot den bakgrunden och då Säkerhetspolisens uppgifter på utlännings- och medborgarskapsområdet är förhållandevis begränsade ansågs det inte vara ändamålsenligt att låta Säkerhetspolisen omfattas av utlänningsdatalagens reglering. Konsekvensen blev att Säkerhetspolisen i stället antingen ska tillämpa de särskilda regler om personuppgiftsbehandling som gäller för myndigheten enligt polisdatalagen eller personuppgiftslagen (se Utlänningsdatalag, prop. 2015/16:65, s. 40). Mot bakgrund av förarbetsuttalandena och att personuppgiftslagen ska upphävas är det

nödvändigt att reglera myndighetens personuppgiftsbehandling på området.

Säkerhetspolisens arbetsuppgifter enligt utlännings- och medborgarskapslagstiftningen syftar till att förhindra att individer som är eller kan bli ett säkerhetshot mot Sverige etablerar sig i landet. Utifrån vad som är känt om personens bakgrund, kontakter eller egna aktiviteter gör Säkerhetspolisen en bedömning av om han eller hon kan komma att ägna sig åt säkerhetshotande verksamhet. Säkerhetsskäl kan exempelvis bestå av kopplingar till personer som antas syssla med olovlig underrättelseverksamhet eller terrorism. Mot den bakgrunden anser utredningen att Säkerhetspolisens uppgifter enligt utlännings- och medborgarskapslagstiftningen är ett led i uppgifterna som rör nationell säkerhet och bör anges som en tillåten rättslig grund för behandling av personuppgifter.

14.6.4 Rättslig grund i undantagsfall för diarieföring och handläggning

Utredningens förslag: Personuppgifter ska få behandlas om det är nödvändigt för diarieföring eller om uppgifterna har lämnats till Säkerhetspolisen i en anmälan, ansökan eller liknande och behandlingen är nödvändig för myndighetens handläggning.

Skälen för utredningens förslag: Säkerhetspolisen tar dagligen emot stora mängder information, ofta i elektronisk form. De inkommande uppgifterna kan vara en del av en allmän handling i tryckfrihetsförordningens mening. Enligt 5 kap. 1 § offentlighets- och sekretesslagen ska som huvudregel allmänna handlingar som kommit in till en myndighet registreras, dvs. diarieföras, så snart som möjligt. En myndighet måste därför alltid ha möjlighet att behandla personuppgifter för att diarieföra och handlägga inkommande handlingar. Det gäller även i de fall där myndigheten inte behöver behandla personuppgifterna för att utföra sina arbetsuppgifter (se prop. 2009/10:85 s. 112 f.) I 6 kap. 3 § polisdatalagen föreskrivs att Säkerhetspolisen får behandla personuppgifter om det är nödvändigt för diarieföring eller om uppgifterna har lämnats i en anmälan eller liknande och behandlingen är nödvändig för handlägg-

ningen. Det bör tas in en motsvarande bestämmelse i den nya lagen som tydliggör att det är en tillåten rättslig grund för behandling.

14.6.5 Rättslig grund för behandling genom utlämnande

Utredningens förslag: Personuppgifter som Säkerhetspolisen behandlar ska även få behandlas om det är nödvändigt för att tillhandahålla information som behövs

1. för brottsbekämpning, lagföring, straffverkställighet eller upprätthållande av allmän ordning och säkerhet hos Polismyndigheten, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket,
2. i en myndighets verksamhet, om informationen tillhandahålls inom ramen för myndighetsöverskridande samverkan mot brott,
3. i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst och i Försvarets radioanstalts försvarsunderrättelseverksamhet, om det finns särskilda skäl att tillhandahålla informationen,
4. i en myndighets verksamhet om Säkerhetspolisen enligt lag eller förordning ska bistå myndigheten med viss uppgift,
5. i brottsbekämpande verksamhet hos en utländsk myndighet eller mellanfolklig organisation, eller
6. i verksamhet hos en utländsk underrättelse- eller säkerhetstjänst.

Personuppgifter ska även få behandlas om det är nödvändigt för att tillhandahålla information till riksdagen och regeringen och till andra, om skyldighet att lämna uppgifter följer av lag eller förordning.

I ett enskilt fall ska personuppgifter få behandlas för att tillhandahålla information för något annat ändamål än de ovan uppräknade, om det nya ändamålet inte är oförenligt med det ändamål som uppgifterna samlades in för.

Skälen för utredningens förslag: Som framgår av avsnitt 14.6.2 anser utredningen att den nuvarande regleringen som bygger på en uppräkningslista av olika situationer där information behöver tillhandahållas och som kompletteras med möjligheten att tillämpa finalitetsprincipen i enskilda fall bör behållas. Utredningen anser att regleringen i 6 kap. 2 § polisdatalagen återspeglar Säkerhetspolisens behov av att behandla personuppgifter för att tillgodose andras informationsbehov. De skäl som anfördes när regleringen infördes gör sig fortfarande gällande (se prop. 2009/10:85 s. 260 f. och prop. 2014/15:94 s. 83 f.). Den nya lagen bör därför i huvudsak ha samma innehåll.

Som framgår av avsnitt 14.11.3 behöver Säkerhetspolisen i vissa fall även lämna ut uppgifter till Försvarets radioanstalt. Säkerhetspolisen och försvarsunderrättelsemyndigheterna har angränsande uppdrag som förutsätter nära samarbete och kontinuerligt informationsutbyte. Även om Säkerhetspolisen i de flesta fall lämnar information till Försvarets radioanstalt för den egna verksamhetens behov, kan det inte uteslutas att Försvarets radioanstalt kan behöva sådan information för sin egen verksamhet. Det bör därför enligt utredningens mening finnas rättsligt stöd även för sådant utlämnande. Av samma anledning som när det gäller information till Försvarsmakten bör det krävas särskilda skäl för att Säkerhetspolisen ska få lämna ut uppgifterna (se prop. 2009/10:85 s. 262). Försvarets radioanstalt bör därför läggas till i bestämmelsen som reglerar utlämnande till Försvarsmakten.

Enligt 16 § instruktionen för Säkerhetspolisen ska myndigheten samarbeta med utländska myndigheter och organ i den utsträckning som behövs för myndighetens verksamhet och som regeringen närmare bestämmer. Säkerhetspolisen har flera utländska samarbetspartner och utbyter kontinuerligt information med dem. I avsnitt 14.11.4 föreslås att Säkerhetspolisen ska kunna medge underrättelse- och säkerhetstjänster i EU och EES direktåtkomst till vissa uppgifter. Även om Säkerhetspolisen i de flesta fall lämnar informationen till dem för den egna verksamhetens behov, kan det inte uteslutas att Säkerhetspolisen även kan behöva lämna information för att tillgodose de utländska tjänsternas behov. Det kan t.ex. gälla misstanke om ett förestående attentat som uteslutande berör en annan stat. I 6 kap. 2 § polisdatalagen anges endast brottsbekämpande verksamhet hos utländsk myndighet eller mellanfolklig

organisation som mottagare. Utländska underrättelse- och säkerhetstjänster har inte alltid den arbetsuppgiften. För att det ska vara tydligt att Säkerhetspolisen får lämna information om det behövs för sådana tjänsters behov bör det införas rättsligt stöd för det.

14.7 Grundläggande krav på behandlingen

14.7.1 Författningensenlig och korrekt behandling

Utredningens förslag: Personuppgifter ska behandlas författningensenligt och på ett korrekt sätt.

Skälen för utredningens förslag: Enligt 9 § första stycket a och b personuppgiftslagen får personuppgifter behandlas bara om det är lagligt. Personuppgifterna ska vidare behandlas på ett korrekt sätt och i enlighet med god sed. Bestämmelserna gäller genom hänvisningar i 2 kap. 2 § och 6 kap. 4 § polisdatalagen för Säkerhetspolisen. I 2 kap. 6 § brottsdatalagen föreskrivs att personuppgifter ska behandlas författningensenligt och på ett korrekt sätt. Skälen bakom bestämmelsen och vad den innebär framgår av delbetänkandet (se SOU 2017:29 s. 256 f.). En motsvarande bestämmelse bör tas in i den nya lagen.

14.7.2 Personuppgifter ska vara korrekta, adekvata och relevanta

Utredningens förslag: De personuppgifter som behandlas ska vara korrekta och, om det är nödvändigt, uppdaterade.

Uppgifter som beskriver en persons utseende ska utformas på ett objektivt sätt med respekt för människovärdet.

De personuppgifter som behandlas ska vara adekvata och relevanta i förhållande till ändamålen med behandlingen. Fler personuppgifter än vad som är nödvändigt med hänsyn till ändamålen med behandlingen ska inte få behandlas.

Skälen för utredningens förslag

Personuppgifter ska vara korrekta och uppdaterade

Enligt 9 § första stycket g personuppgiftslagen ska personuppgifter som behandlas vara riktiga och, om nödvändigt, aktuella. Bestämmelsen gäller för Säkerhetspolisen genom hänvisningar i 2 kap. 2 § och 6 kap. 4 § polisdatalagen. I 2 kap. 7 § första stycket brottsdatalagen föreskrivs att personuppgifter ska vara korrekta och, om det är nödvändigt, uppdaterade. En motsvarande bestämmelse bör tas in i den nya lagen. Vad som avses med korrekta och uppdaterade framgår av delbetänkandet (se SOU 2017:29 s. 258 f.).

I 2 kap. 10 § tredje stycket polisdatalagen, som gäller för Säkerhetspolisen, föreskrivs att uppgifter som beskriver en persons utseende ska utformas på ett objektivt sätt och med respekt för människovärdet. Samma reglering finns i 2 kap. 7 § andra stycket brottsdatalagen. En motsvarande bestämmelse bör finnas i den nya lagen. Som utredningen konstaterar i delbetänkandet bör den placeras tillsammans med bestämmelserna om personuppgifternas kvalitet (se SOU 2017:29 s. 259).

Personuppgifter ska vara adekvata och relevanta

Enligt 9 § första stycket e och f personuppgiftslagen ska de personuppgifter som behandlas vara adekvata och relevanta i förhållande till ändamålen med behandlingen. Fler personuppgifter får inte behandlas än vad som är nödvändigt med hänsyn till ändamålen. Bestämmelsen gäller för Säkerhetspolisen genom hänvisningar i 2 kap. 2 § och 6 kap. 4 § polisdatalagen. Motsvarande reglering finns i 2 kap. 8 § brottsdatalagen. En likadan bestämmelse bör tas in i den nya lagen.

Vilka uppgifter som är adekvata och relevanta ska bedömas i förhållande till ändamålen med behandlingen. Detsamma gäller hur många personuppgifter det finns behov av att behandla. Det kan emellertid vara svårare att bedöma att uppgifterna är adekvata och relevanta i Säkerhetspolisens verksamhet än i annan polisverksamhet, eftersom det som regel inte är lika tydligt vari den brottsliga verksamheten eller säkerhetsshotet består.

Att det krävs att uppgifterna ska vara adekvata och relevanta får betydelse för hur s.k. överskottsinformation ska hanteras, dvs. uppgifter som samlas in och som visar sig inte vara adekvata eller relevanta för det bestämda ändamålet. Om uppgifterna inte behövs för något annat tillåtet ändamål får de inte lagras för framtida behov. Det finns särskilda regler om i vilken utsträckning överskottsinformation överhuvudtaget får behandlas i vissa sammanhang (se t.ex. 27 kap. 23 a § rättegångsbalken).

Med hänsyn till Säkerhetspolisens känsliga verksamhet kan det, bl.a. vid bedömningen av hur många personuppgifter som behöver behandlas i förhållande till ändamålet, vara nödvändigt att utöver behoven i det konkreta ärendet ta hänsyn till andra aspekter, framför allt kravet på informationssäkerhet. Säkerhetspolisen kan t.ex. i vissa situationer behöva begära uppgifter om fler personer än den som är misstänkt, för att inte avslöja vem eller vilka personer som myndigheten intresserar sig för i underrättelsearbetet eller en brottsutredning. Kravet på att uppgifterna ska vara adekvata och relevanta och inte för många i förhållande till ändamålet med behandlingen bör då ändå anses vara uppfyllt. Behandlingen av uppgifter om de personer som myndigheten inte har något intresse av annat än för att avleda uppmärksamheten ska givetvis upphöra så snart det syftet är uppnått. Behovet av att behandla sådana uppgifter är alltså kortvarigt.

Särskilt om material från användning av hemliga tvångsmedel

Säkerhetspolisen behandlar i stor utsträckning material från hemliga tvångsmedel. Det beror dels på att Säkerhetspolisen biträder andra brottsbekämpande myndigheter med tekniska åtgärder, dels på att sådana tvångsmedel förekommer i Säkerhetspolisens egen verksamhet. För behandling av uppgifter som inhämtas genom hemliga tvångsmedel gäller dels reglerna i rättegångsbalken eller motsvarande lagstiftning, dels myndighetens registerlagstiftning (se prop. 2009/10:85 s. 78). Material av nu aktuellt slag kan både behöva bearbetas tekniskt eller på annat sätt, och i vissa fall även tolkas eller översättas, innan det kan granskas på det sätt som förutsätts i rättegångsbalken och annan motsvarande lagstiftning. Det ligger i sakens natur att kravet på granskning av det materiella inne-

hållet inte kan uppfyllas innan det har gjorts tillgängligt på sådant sätt att en åklagare eller den utredningspersonal som biträder honom eller henne kan ta del av det. Det innebär att personuppgifter måste kunna behandlas för att den granskningen ska kunna komma till stånd. Kravet på att sådant material som härrör från hemliga tvångsmedel och som är ovidkommande ska tas bort så snabbt som möjligt måste därför ses i ljuset av möjligheterna att på ett tidigt stadium kunna bedöma värdet av informationen.

14.7.3 Känsliga personuppgifter

Utredningens förslag: Säkerhetspolisen ska inte få behandla personuppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening eller som rör hälsa, sexualliv eller sexuell läggning. Om uppgifter om en person behandlas ska de dock få kompletteras med sådana uppgifter när det är absolut nödvändigt för ändamålet med behandlingen.

Säkerhetspolisen ska få behandla biometriska uppgifter endast om det är absolut nödvändigt för ändamålet med behandlingen men ska inte få behandla genetiska uppgifter.

Känsliga personuppgifter ska också få behandlas om det är nödvändigt för diarieföring eller om uppgifterna har lämnats till Säkerhetspolisen i en anmälan, ansökan eller liknande och behandlingen är nödvändig för myndighetens handläggning.

Det ska vara förbjudet att utföra sökningar i syfte att få fram ett personurval grundat på känsliga personuppgifter. Sökförbudet ska inte hindra att brottsrubriceringar, uppgifter om tillvägagångssätt vid brott eller uppgifter som beskriver en persons utseende används vid sökning. Det ska inte heller hindra sökning i syfte att få fram ett personurval grundat på etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller uppgifter som rör hälsa, sexualliv eller sexuell läggning, om sökningen är absolut nödvändig för något av de syften som Säkerhetspolisen får behandla personuppgifter för.

Skälen för utredningens förslag

Säkerhetspolisen ska få behandla känsliga personuppgifter i samma utsträckning som i dag

Enligt 2 kap. 10 § polisdatalagen, som genom en hänvisning i 6 kap. 4 § gäller för Säkerhetspolisen, får uppgifter om en person inte behandlas enbart på grund av vad som är känt om personens ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexualliv. Om uppgifter om en person redan behandlas på någon annan grund, får de dock kompletteras med känsliga personuppgifter, om det är absolut nödvändigt för syftet med behandlingen. Innebörden är att det t.ex. inte är tillåtet att föra särskilda register över personer baserat på deras politiska åsikter. Om uppgifter om en person redan behandlas får dock uppgifter om politiska åsikter behandlas, om det bedöms vara absolut nödvändigt för ändamålet med behandlingen. Det kan t.ex. vara fallet om motivet för ett brott är politiskt.

I brottsdatalagen utökas uppräkningslistan av vad som betecknas som känsliga personuppgifter. Dit hör enligt 2 kap. 11 § även uppgifter som rör sexuell läggning och enligt 2 kap. 12 § biometriska uppgifter som används för att identifiera en person och genetiska uppgifter.

För att den nya regleringen så långt möjligt ska stämma överens med övriga registerförfattningar bör uppräkningslistan av känsliga personuppgifter i den nya lagen omfatta både uppgifter som rör sexualliv och sexuell läggning. Även biometriska och genetiska uppgifter bör i den nya lagen betecknas som känsliga personuppgifter. Vad som avses med genetiska och biometriska uppgifter redovisas i delbetänkandet (se SOU 2017:29 s. 265 f.).

På samma sätt som i dag bör Säkerhetspolisen bara få behandla känsliga personuppgifter om uppgifter om personen redan behandlas på någon annan grund och behandlingen av känsliga personuppgifter är absolut nödvändig för ändamålet med behandlingen. Bestämmelserna i den nya lagen om känsliga personuppgifter bör formuleras på samma sätt som i brottsdatalagen. Det blir då tydligare vilka uppgifter som utgör känsliga personuppgifter och när de får behandlas. Någon förändring av synen på vad som är absolut nödvändigt vid behandling av känsliga personuppgifter är inte avsedd. Sådana uppgifter ska alltså användas restriktivt och behovet

av att komplettera med sådana uppgifter ska prövas noga i det enskilda ärendet (se prop. 2009/10:85 s. 325).

Behandling av biometriska och genetiska uppgifter

I avsnitt 7.3.2 redogör utredningen för vad som avses med biometriska och genetiska uppgifter. Säkerhetspolisen har som framgår där behov av att kunna behandla biometriska uppgifter. Det gäller även när behandlingen rör nationell säkerhet. En motsvarande bestämelse bör därför tas in i den nya lagen.

Att behandling av genetiska uppgifter regleras i brottsdatalagen beror på att det är nödvändigt för att genomföra direktivet. Utredningen föreslår i avsnitt 7.8.4 att sådana uppgifter enbart ska få behandlas i Polismyndighetens forensiska verksamhet. Säkerhetspolisen behandlar inte genetiska uppgifter i dag och det kan inte heller förutses något framtida behov av det. Det bör framgå av den nya lagen att Säkerhetspolisen inte får behandla sådana uppgifter.

Behandling för diarieföring eller liknande

Enligt 2 kap. 10 § andra stycket polisdatalagen får Säkerhetspolisen behandla känsliga personuppgifter om det är nödvändigt för diarieföring eller om uppgifterna har lämnats till myndigheten i en anmälan eller liknande och behandlingen är nödvändig för handläggningen. Som framgår av avsnitt 14.6.4 måste Säkerhetspolisen alltid ha möjlighet att behandla personuppgifter för att diarieföra och handlägga inkommande anmälningar, ansökningar och andra liknande handlingar. Det bör gälla även i de fall där sådana handlingar innehåller känsliga personuppgifter, eftersom det ligger utanför Säkerhetspolisens kontroll om sådana uppgifter finns i handlingarna. Det bör därför framgå att sådan behandling är tillåten.

Ett sökförbud med undantag

Enligt 6 kap. 11 § polisdatalagen får Säkerhetspolisen använda känsliga personuppgifter som sökbegrepp vid sökning i personuppgifter som har gjorts gemensamt tillgängliga endast om det är absolut

nödvändigt för de ändamål som myndigheten får behandla personuppgifter för. Brottsrubriceringar och uppgifter som beskriver en persons utseende får dock användas som sökbegrepp utan några begränsningar. Några begränsningar gäller inte heller vid sökning i personuppgifter som endast ett fåtal har tillgång till.

I 2 kap. 14 § brottsdatalagen finns ett generellt sökförbud som förbjuder sökningar i syfte att få fram ett personurval grundat på känsliga personuppgifter. Utredningen redogör för innebörden av förbudet i delbetänkandet (se SOU 2017:29 s. 272 f.). Utredningen föreslår att det i övriga registerförfattningar ska föreskrivas undantag från sökförbudet som är anpassade till de behov som respektive myndighet har (se avsnitt 7.3.3, 8.3.3, 9.3.3, 10.3.3, 11.3.3 och 13.5.5). Frågan är om samma systematik bör väljas även för Säkerhetspolisen.

Vid polisdatalagens tillkomst ansåg regeringen att verksamhets-skal talade för att Säkerhetspolisen inte borde förbjudas att använda känsliga personuppgifter som sökbegrepp, eftersom uppgifter av det slaget kan ha stor betydelse i myndighetens verksamhet. Regeringen framhöll samtidigt att verksamhetsintresset måste vägas mot intresset av att skydda de personer, vilkas uppgifter behandlas, mot intrång i den personliga integriteten. Vidare framhölls att utformningen av bestämmelsen om sökning gör att känsliga personuppgifter inte rutinmässigt kan användas som sökbegrepp utan först sedan det vid en prövning av behovet i det enskilda fallet konstaterats att det finns ett påtagligt behov (se prop. 2009/10:85 s. 266).

Säkerhetspolisen har alltjämt behov av att kunna använda känsliga personuppgifter vid sökning. I arbetet med att förebygga och upptäcka terroristbrott kan t.ex. uppgifter om en persons politiska åsikt eller religiösa övertygelse vara viktiga. Vid brott mot rikets säkerhet kan uppgifter av det slaget bidra till att fastställa motivet för gärningen. Säkerhetspolisen bör därför ges i huvudsak samma möjligheter som i dag att använda känsliga personuppgifter vid sökning.

Eftersom Säkerhetspolisens reglering i större utsträckning än övriga registerförfattningar tillåter sökning skulle det kunna hävdas att ett generellt sökförbud skulle bli innehållslöst då det skulle behöva förses med så många undantag. Utredningen anser dock att en reglering som bygger på ett generellt förbud med undantag som är anpassade för verksamheten ger en tydligare signal om att känsliga

personuppgifter ska användas restriktivt. Det finns också fördelar med att regleringen för alla brottsbekämpande myndigheter överensstämmer i den delen. Regleringen i den nya lagen bör därför bygga på ett generellt förbud som utgår från syftet med sökningen. Förbudet bör på samma sätt som för övriga brottsbekämpande myndigheter gälla vid sökning i alla slags uppgifter, dvs. även i uppgifter som bara behandlas av ett fåtal. Från förbudet bör det göras undantag som tillgodoser Säkerhetspolisens behov av att kunna använda känsliga personuppgifter.

Genom att sökförbudet utgår från syftet med sökningen är sökning som inte görs i syfte att få fram ett personurval grundat på känsliga personuppgifter tillåten, även om känsliga personuppgifter används vid sökningen (jfr SOU 2017:29 s. 272 f.). Även tillåtna sökningar kan således resultera i ett personurval grundat på känsliga personuppgifter. I vilken utsträckning det är tillåtet att behandla personuppgifterna i en sådan sammanställning får prövas mot huvudregeln om behandling av känsliga personuppgifter.

Som anges i delbetänkandet kan det ifrågasättas om utformningen av sökförbudet i brottsdatalagen uppfyller kraven för att omfattas av begränsningsregeln i tryckfrihetsförordningen. För att allmänheten inte med stöd av offentlighetsprincipen ska kunna få del av sammanställningar grundade på känsliga personuppgifter föreslår utredningen en bestämmelse om absolut sekretess för dem (se SOU 2017:29 s. 274 f. och 643 f.). Samma sekretess bör gälla hos Säkerhetspolisen. Ett tillägg bör därför göras i sekretessbestämmelsen.

Vilka undantag bör göras från sökförbudet?

Enligt 6 kap. 11 § andra stycket polisdatalagen är det tillåtet att använda brottsrubriceringar och uppgifter som beskriver en persons utseende som sökbegrepp. Säkerhetspolisen har också i fortsättningen behov av att kunna använda sådana uppgifter vid sökning, även om det leder till att man får fram ett personurval grundat på känsliga personuppgifter. I likhet med Polismyndigheten behöver Säkerhetspolisen också kunna söka på tillvägagångssätt vid brott, även om det skulle avslöja känsliga personuppgifter som t.ex.

politiska åsikter (se avsnitt 7.3.3). Det bör därför göras undantag från sökförbudet för sådana sökningar.

Utredningen föreslår att övriga brottsbekämpande myndigheter tillåts göra sökningar i syfte att få fram personurval grundade på vissa känsliga personuppgifter, under förutsättning att sökningen görs i personuppgifter som inte har gjorts gemensamt tillgängliga. För att Säkerhetspolisens sökmöjligheter ska vara desamma som i dag bör myndigheten tillåtas att göra sökningar i syfte att få fram personurval grundade på i princip alla typer av känsliga personuppgifter. Även om det i dag inte finns någon begränsning när det gäller vilka uppgifter som får användas som sökbegrepp bör det emellertid av de skäl som anges i avsnitt 7.3.3 inte vara tillåtet att ta fram personurval grundat på uppgifter som kan avslöja ras. Säkerhetspolisen har enligt uppgift inte heller något behov av att göra sökningar på medlemskap i fackförening eller på genetiska uppgifter. Det bör därför inte vara tillåtet att ta fram personurval grundade på sådana uppgifter.

Teknik för ansiktsgenkänning används i dag bl.a. för att underlätta identifiering när endast en del av ett ansikte är synligt på en bild eller en film eller om bildkvaliteten är dålig. Behandlingen i ett ansiktsgenkänningsprogram kan i sådana fall resultera i en träfflista med flera möjliga kandidater. Det skulle kunna hävdas att resultatet blir ett personurval grundat på biometriska uppgifter. Det är dock i dessa fall inte fråga om sökning i syfte att få fram ett visst personurval, utan om normal behandling av biometriska uppgifter. Sådan behandling föreslås vara tillåten om den är absolut nödvändig för ändamålet med behandlingen. Det finns därför enligt utredningens mening inte något behov av att göra undantag från sökförbudet för att sådan behandling ska vara tillåten.

Säkerhetspolisen får i dag använda känsliga personuppgifter som sökbegrepp vid sökning i alla slags uppgifter, dvs. oavsett om de har gjorts gemensamt tillgängliga eller inte. Eftersom Säkerhetspolisen även i fortsättningen bör tillåtas att göra sökningar i alla slags personuppgifter, går det inte att utforma undantaget på samma sätt som i övriga registerförfattningar. För att sökmöjligheterna inte ska bli alltför vida bör det på samma sätt som i dag krävas att det är absolut nödvändigt att göra sökningen.

Även om regleringen utformas på ett delvis annorlunda sätt och det inte längre blir möjligt att söka på ras och medlemskap i fack-

förening bedömer utredningen att Säkerhetspolisens möjligheter att använda känsliga personuppgifter vid sökning inte försämrats jämfört med i dag.

14.7.4 Åtgärder för att säkerställa personuppgifternas kvalitet

Utredningens förslag: Säkerhetspolisen ska vidta alla rimliga åtgärder för att personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålet med behandlingen rättas utan onödigt dröjsmål. Detsamma gäller för att förhindra att sådana uppgifter lämnas ut eller görs tillgängliga. Personuppgifter som är inaktuella ska uppdateras om det är nödvändigt.

Alla rimliga åtgärder ska vidtas för att personuppgifter som behandlas på otillåtet sätt utan onödigt dröjsmål raderas och för att förhindra att sådana uppgifter lämnas ut eller görs tillgängliga. Detsamma ska gälla om radering krävs för att utföra en rättslig förpliktelse.

I stället för att radera personuppgifterna ska Säkerhetspolisen utan onödigt dröjsmål begränsa behandlingen av dem, om de behöver finnas kvar som bevisning.

Skyldigheten att underrätta mottagare av personuppgifterna om att de är felaktiga eller behandlas på otillåtet sätt ska regleras i förordning.

Skälen för utredningens förslag

Nuvarande reglering och bestämmelserna i brottsdatalagen

Enligt 9 § första stycket i personuppgiftslagen ska alla rimliga åtgärder vidtas för att rätta, blockera eller utplåna sådana personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålen med behandlingen. Det gäller för Säkerhetspolisen genom hänvisningar i 2 kap. 2 § och 6 kap. 4 § i brottsdatalagen.

Bestämmelserna i brottsdatalagen, som reglerar den personuppgiftsansvariges skyldighet att på eget initiativ rätta, radera eller begränsa behandlingen av personuppgifter, är mer detaljerade och anger på ett tydligare sätt vilken åtgärd som ska vidtas. Enligt 2 kap. 15 § första stycket i brottsdatalagen ska alla rimliga åtgärder

vidtas för att personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålet med behandlingen utan onödigt dröjsmål rättas och för att förhindra att sådana uppgifter lämnas ut eller görs tillgängliga. Personuppgifter som är inaktuella ska uppdateras om det är nödvändigt. När personuppgifter lämnas ut till en behörig myndighet, ska mottagaren så långt det är möjligt ges information som gör det möjligt att bedöma i vilken utsträckning uppgifterna är korrekta, fullständiga, uppdaterade och tillförlitliga. Enligt 2 kap. 16 § ska alla rimliga åtgärder vidtas för att personuppgifter som behandlas på ett otillåtet sätt utan onödigt dröjsmål raderas och för att förhindra att sådana uppgifter lämnas ut eller görs tillgängliga. Detsamma gäller om radering krävs för att utföra en rättslig förpliktelse. I stället för att radera personuppgifterna ska den personuppgiftsansvarige utan onödigt dröjsmål begränsa behandlingen av dem, om de behöver finnas kvar som bevisning. Regleringen i brottsdatalagen utgår alltså från att felaktiga personuppgifter ska rättas och att personuppgifter som behandlas på otillåtet sätt ska raderas.

Regleringen ska i huvudsak motsvara regleringen i brottsdatalagen

När det gäller skyldigheten att på eget initiativ rätta, radera eller begränsa behandlingen av felaktiga eller ofullständiga personuppgifter eller personuppgifter som behandlats på otillåtet sätt, anser utredningen att i princip samma krav bör ställas på Säkerhetspolisen som på övriga brottsbekämpande myndigheter. Det gäller även ansvaret att se till att felaktiga eller ofullständiga uppgifter inte lämnas ut eller görs tillgängliga. Det bör därför i den nya lagen tas in bestämmelser med samma innebörd som 2 kap. 15 och 16 §§ brottsdatalagen.

Kravet på information i samband med utlämnande eller tillgängliggörande av personuppgifter som regleras i 2 kap. 15 § andra stycket brottsdatalagen har sin grund i direktivet. Något sådant krav ställs inte på Säkerhetspolisen i dag. Det ligger i sakens natur att Säkerhetspolisen inte i samma utsträckning som andra brottsbekämpande myndigheter kan avslöja vilken information som ligger till grund för t.ex. en misstanke om någons delaktighet i brotts-

lig verksamhet. Någon motsvarande bestämmelse bör därför inte tas in i den nya lagen.

Som utredningen konstaterar i delbetänkandet är det naturligt att, om det upptäcks att felaktiga personuppgifter eller personuppgifter som behandlas på otillåtet sätt har lämnats ut, den som har fått uppgifterna underrättas så att uppgifterna kan rättas eller raderas eller behandlingen av dem begränsas (se SOU 2017:29 s. 281). Underrättelseskyldigheten kan regleras i förordning.

14.8 Uppgifter från transportföretag

Utredningens förslag: I den nya lagen ska det regleras hur Säkerhetspolisen får behandla personuppgifter som transportföretag på begäran tillhandahåller myndigheten enligt polislagen. Sådana personuppgifter ska endast i enskilda fall få behandlas för nya ändamål.

Skälen för utredningens förslag: I avsnitt 7.4.1 redovisas bestämmelserna i polislagen om transportföretags skyldighet att på begäran lämna vissa personuppgifter till polisen. Utredningen föreslår där att bestämmelserna om personuppgiftsbehandling ska föras över till polisens brottsdatalog. Det skäl som anges där för att personuppgiftsbehandlingen bör regleras i myndighetens registerförfattning har giltighet även för Säkerhetspolisen. Regleringen av hur sådana personuppgifter får behandlas bör därför tas in i den nya lagen och utformas i huvudsak på samma sätt som i polisens brottsdatalog. Det innebär att samma begränsningar bör gälla vid terminalåtkomst. Vidare bör sådana personuppgifter endast i enskilda fall få behandlas för nya ändamål.

I avsnitt 7.4.2 föreslås att samma sökbegränsningar som gäller för Tullverket i dag ska gälla vid behandling enligt polisens brottsdatalog av personuppgifter som tillhandahålls av transportföretag. I förarbetena till polisdatalogen konstaterar regeringen att det varken är möjligt eller lämpligt att ha samma sökbegränsningar för Säkerhetspolisen som för Polismyndigheten (se prop. 2009/10:85 s. 267). Mot den bakgrunden anser utredningen att Säkerhetspolisens användning av direkta personuppgifter vid sökning i uppgifter från transportföretag inte bör begränsas i större utsträckning än

i dag. Regeringen bör dock ha möjlighet att meddela föreskrifter om begränsning av möjligheterna att göra sökning.

14.9 Gemensamt tillgängliga uppgifter

14.9.1 Allmänt om regleringen

Utredningens förslag: Särskilda bestämmelser ska gälla för behandling av personuppgifter som görs eller har gjorts gemensamt tillgängliga.

Personuppgifter ska få göras gemensamt tillgängliga om det behövs för något av de syften för vilka Säkerhetspolisens får behandla personuppgifter.

Bestämmelserna om gemensamt tillgängliga uppgifter ska inte gälla när personuppgifter behandlas med stöd av bestämmelsen om behandling av personuppgifter för diarieföring eller för att utföra andra nödvändiga handläggningsuppgifter.

Skälen för utredningens förslag: I 6 kap. polisdatalagen finns särskilda bestämmelser som gäller vid behandling av personuppgifter som görs eller har gjorts gemensamt tillgängliga. Med gemensamt tillgängliga uppgifter avses uppgifter som inte enbart ett fåtal har tillgång till. För behandling av sådana uppgifter ställs det t.ex. krav på särskilda upplysningar och vidare begränsas möjligheten till sökning. Sådana bestämmelser bör finnas även i den nya lagen. För att få en enhetlig systematik bör regleringen om gemensamt tillgängliga uppgifter finnas i ett särskilt kapitel.

Av 6 kap. 8 § polisdatalagen framgår att personuppgifter får göras gemensamt tillgängliga i Säkerhetspolisens verksamhet om det behövs för något av de ändamål för vilka personuppgifter får behandlas. Bestämmelsen är inte lika preciserad och begränsande som motsvarande bestämmelse för Polismyndigheten. I förarbetena till polisdatalagen konstaterar regeringen att de intressen som Säkerhetspolisens har till uppgift att skydda motiverar att myndigheten ges större handlingsfrihet i fråga om vilka uppgifter som får göras gemensamt tillgängliga. Skälet till det är bl.a. att Säkerhetspolisens verksamhet är inriktad mot brottslighet som till sin natur är svår att upptäcka och att tyngdpunkten i dess brottsbekämpande

arbete ligger på underrättelsearbete och renodlat förebyggande arbete. Det konstateras vidare att det är svårt att förutse och i lag uttrycka de olika kategorier av personuppgifter som bör få göras gemensamt tillgängliga hos Säkerhetspolisen och att myndighetens verksamhet till sin natur är sådan att informationen sprids i mindre utsträckning än inom polisen i övrigt (se prop. 2009/10:85 s. 264).

Enligt utredningens mening är de skäl som anges i förarbetena fortfarande aktuella. Regleringen av när personuppgifter får göras gemensamt tillgängliga bör därför i princip tas in oförändrad i den nya lagen. Den bör dock knytas till de syften för vilka Säkerhetspolisen får behandla personuppgifter, i stället för till ändamålen med behandlingen.

I 6 kap. 8 § andra stycket polisdatalagen föreskrivs att bestämmelserna om gemensamt tillgängliga uppgifter inte gäller när personuppgifter behandlas med stöd av den särskilda bestämmelsen om behandling av personuppgifter för diarieföring eller för att utföra andra nödvändiga handläggningsuppgifter. En motsvarande bestämmelse bör tas in i den nya lagen.

14.9.2 Särskilda upplysningar

Utredningens förslag: Om det ändamål som gemensamt tillgängliga personuppgifter behandlas för inte framgår av sammanhanget eller på något annat sätt, ska det tydliggöras genom en särskild upplysning.

Om uppgifter som är gemensamt tillgängliga direkt kan hänföras till en person som inte är misstänkt för brott eller för att ha utövat eller komma att utöva brottslig verksamhet, ska det framgå genom en särskild upplysning eller på något annat sätt att personen inte är misstänkt för brott eller brottslig verksamhet som omfattas av lagens tillämpningsområde.

Uppgifter om en person som kan antas ha direkt samband med misstänkt brottslig verksamhet ska som regel föras med en upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak. Någon sådan upplysning behöver dock inte lämnas om det på grund av omständigheterna är onödigt.

Skälen för utredningens förslag

Särskild upplysning om ändamålet med behandlingen

Enligt 6 kap. 9 § polisdatalagen ska det genom en särskild upplysning eller på något annat sätt framgå för vilket närmare ändamål personuppgifter som har gjorts gemensamt tillgängliga behandlas. Både av hänsyn till verksamheten och till den personliga integriteten är det viktigt att det framgår för vilket ändamål en personuppgift behandlas. Från integritetssynpunkt har det betydelse bl.a. för möjligheterna att genom tekniska förfaranden eller administrativa bestämmelser kunna styra åtkomsten till vissa uppgifter. Att ändamålet med behandlingen framgår kan vara en förutsättning för att en tillsynsmyndighet ska kunna kontrollera om viss behandling är berättigad och utförs i enlighet med lagens bestämmelser. Information om ändamålet med behandlingen behövs för att de tjänstemän som får tillgång till personuppgifter ska kunna värdera uppgifterna korrekt och använda sig av dem på ett effektivt och lagenligt sätt. Informationen behövs bl.a. för att kunna ta ställning till om uppgiften får och bör behandlas för ett nytt ändamål. En bestämmelse som föreskriver att det ska framgå för vilket ändamål personuppgifter behandlas bör därför tas in i den nya lagen. På samma sätt som i dag bör dock särskilda upplysningar krävas endast om ändamålet inte framgår av sammanhanget eller på något annat sätt. Bestämmelsen bör formuleras på samma sätt som 2 kap. 3 § andra stycket brottsdatalagen.

Kravet på att ändamålet med behandlingen ska framgå omfattar i dag bara uppgifter som har gjorts gemensamt tillgängliga. Om uppgifter behandlas av en liten, klart avgränsad grupp vet de inblandade personerna som regel varifrån uppgifterna kommer och varför de behandlas. I de fallen framgår det normalt av sammanhanget för vilket ändamål personuppgifter behandlas. Som utredningen konstaterar i delbetänkandet vore det orimligt att kräva att uppgifterna då ska förse med en särskild upplysning (se SOU 2017:29 s. 245). Kravet på att ändamålet med behandlingen ska framgå bör därför även i den nya lagen gälla endast för uppgifter som har gjorts gemensamt tillgängliga (jfr avsnitt 5.3.10).

Upplysning om att den registrerade inte är misstänkt

Om uppgifter direkt kan hänföras till en person som inte är misstänkt för brott eller för att ha utövat eller komma att utöva brottslig verksamhet, ska det enligt 6 kap. 10 § första stycket polisdatalagen genom en särskild upplysning eller på något annat sätt framgå att personen inte är misstänkt. En liknande bestämmelse finns i 2 kap. 9 § brottsdatalagen. Där föreskrivs att så långt det är möjligt ska personuppgifter som rör olika kategorier av registrerade, som personer som är misstänkta eller dömda för brott, brottsoffer eller andra som berörs av ett brott, särskiljas. Om det inte framgår av sammanhanget eller på något annat sätt vilken kategori personen tillhör, ska det tydliggöras genom en särskild upplysning. I avsnitt 5.3.10 föreslår utredningen att bestämmelserna om särskilda upplysningar ska finnas kvar i övriga registerförfattningar vid personuppgiftsbehandling i underrättelseverksamhet.

Det är av stor betydelse för skyddet av den personliga integriteten vid brottsbekämpning att personuppgifter behandlas på ett sådant sätt att det framgår om personen är misstänkt eller inte. En bestämmelse motsvarande den som finns i polisdatalagen bör därför tas in i den nya lagen. Det bör tydliggöras att upplysningen ska avse om personen i fråga är misstänkt för sådant brott eller sådan brottslig verksamhet som Säkerhetspolisen har till uppgift att bekämpa. Ofta framgår det av omständigheterna eller sammanhanget i vilket personuppgifterna behandlas att en uppgift avser en person som inte är misstänkt. Som utredningen konstaterar i delbetänkandet är det främst i det inledande skedet av en förundersökning och i underrättelseverksamhet som det kan vara tydligt vilken roll en person har och det är framför allt när uppgifter behandlas utanför sitt ursprungliga sammanhang som särskilda upplysningar kan behövas (se SOU 2017:29 s. 261 f.).

På samma sätt som när det gäller upplysning om ändamålet bör upplysning om att en registrerad inte är misstänkt endast krävas för uppgifter som har gjorts gemensamt tillgängliga. Om uppgifterna bara är tillgängliga för ett fåtal framgår det normalt av sammanhanget till vilken kategori personen hör och det vore då orimligt att ställa upp ett krav på särskild upplysning (se SOU 2017:29 s. 262).

Upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak

I 6 kap. 10 § andra stycket polisdatalagen ställs det krav på att uppgifter om en person som kan antas ha samband med misstänkt brottslig verksamhet ska förses med en upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak. Någon upplysning krävs dock inte om det på grund av särskilda omständigheter är onödigt eller om uppgifterna ingår i en uppgiftssamling som har skapats för att bearbeta och analysera information och bearbetningen och analysen befinner sig i ett inledande skede.

På samma sätt som det är viktigt att det framgår om en uppgift rör en icke misstänkt person, är det viktigt att det framgår hur tillförlitlig en underrättelseuppgift bedöms vara. Syftet med en sådan bestämmelse är dels att stärka skyddet för den enskildes integritet, dels att förhindra att uppgifter, vilkas tillförlitlighet och trovärdighet är begränsad, läggs till grund för bedömningar och åtgärder som inte är sakligt motiverade (se prop. 2009/10:85 s. 265). En motsvarande bestämmelse bör därför tas in i den nya lagen. Av de skäl som anges i avsnitt 5.3.10 bör bestämmelsen dock formuleras något annorlunda än i dag. Kravet på särskild upplysning bör på samma sätt som i dag endast gälla för uppgifter som har gjorts gemensamt tillgängliga. Utredningen återkommer till undantaget för ostrukturerad underrättelseinformation.

14.10 Behandling av personuppgifter i ostrukturerad information

14.10.1 Behovet av reglering

Informationsmängden ökar ständigt

Säkerhetspolisen tar varje dag emot stora mängder information i olika former och från olika källor. Informationsflödet påverkas av vad som händer i omvärlden och är av naturliga skäl som mest intensivt i samband med särskilda händelser. Som exempel kan nämnas när Säkerhetspolisen valde att lämna information till media om en person som vistades i Sverige och som man befarade inom kort skulle utföra ett terroristattentat. Det resulterade i en oerhört stor

mängd tips från allmänheten. Samtidigt var informationsutbytet intensivt både nationellt och internationellt. Motsvarande kraftiga informationsflöde uppkom vid terroristattentatet på Drottninggatan i Stockholm i april 2017. Även händelser utomlands kan periodvis generera stora mängder information. Säkerhetspolisen kan också förväntas få ta emot allt större informationsmängder generellt.

Bearbetning och analys av underrättelseinformation

Alla handlingar som kommer in till eller upprättas vid Säkerhetspolisen diarieförs i myndighetens dokument- och ärendehanteringssystem. Den första bedömningen av uppgifterna görs så snart som möjligt av ansvarig handläggare i det systemet. Om uppgifterna behöver behandlas i Säkerhetspolisens underrättelseverksamhet förs de därefter som regel över till it-systemet för bearbetning och analys. Det systemet innehåller två delar. Den ena delen är en uppgiftssamling med uppgifter för bearbetning och analys och den andra en uppgiftssamling med bedömd information.

När en handling har tillförts uppgiftssamlingen för bearbetning och analys bedöms den även av en särskild granskningsfunktion. Granskningen syftar bl.a. till att säkerställa att Säkerhetspolisen överhuvudtaget får behandla uppgifterna. Behovet av att behandla känsliga personuppgifter prövas särskilt. Känsliga personuppgifter som inte får behandlas tas bort genom maskning. Därefter bearbetas informationen genom att uppgifterna bryts ut och kopplas samman med annan information, tematiseras och tillförs särskilda upplysningar om det krävs.

När bearbetningen är klar kan uppgifterna föras över till uppgiftssamlingen med bedömd information eller tas bort. Det förekommer dock att uppgifterna ligger kvar i uppgiftssamlingen med uppgifter under bearbetning och analys även en tid efter det att bearbetningen är färdig.

14.10.2 Undantag från kravet på särskilda upplysningar

Utredningens förslag: Gemensamt tillgängliga personuppgifter behöver inte förses med en upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak om

1. uppgifterna ingår i en uppgiftssamling som har skapats för att bearbeta och analysera information och som enbart särskilt angivna tjänstemän har åtkomst till och
2. bearbetningen av uppgifterna inte har genomförts.

Skälen för utredningens förslag

Särskilda bestämmelser för gemensamt tillgängliga uppgifter

I 6 kap. polisdatalagen finns det särskilda bestämmelser om gemensamt tillgängliga uppgifter, bl.a. att de vid behov ska förses med särskilda upplysningar. I avsnitt 14.9.1 föreslår utredningen att sådana bestämmelser ska finnas även i den nya lagen.

När det gäller ostrukturerad information kan det vara svårt för Säkerhetspolisen att uppfylla vissa av de krav som ställs på gemensamt tillgängliga uppgifter. Svårigheten gäller främst kravet i 6 kap. 10 § andra stycket polisdatalagen på upplysningar om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak (se avsnitt 14.9.2). Uppgifterna kan normalt inte förses med sådana upplysningar förrän de har bearbetats. Därför görs det i 6 kap. 10 § andra stycket undantag från kravet på sådan upplysning, om personuppgifterna ingår i en uppgiftssamling som har skapats för att bearbeta och analysera information och bearbetningen och analysen befinner sig i ett inledande skede. Enligt förarbetena ska det vara fråga om en kortare period (se prop. 2009/10:85 s. 370 f.).

Bör undantaget justeras?

Som framgår av förarbetena till polisdatalagen är det inte meningen att ostrukturerad underrättelseinformation ska behandlas i en uppgiftssamling för bearbetning och analys någon längre tid utan att den bearbetas. Utgångspunkten är att Säkerhetspolisen ska genom-

föra analysen av den ostrukturerade informationen så snabbt som möjligt. På grund av den omfattande mängd information som periodvis kan komma in till Säkerhetspolisen har myndigheten dock inte alltid möjlighet att strukturera de uppgifter som förs in i uppgiftssamlingen för bearbetning och analys så snabbt som förutsätts i 6 kap. 10 § andra stycket polisdatalagen. Konsekvensen blir att uppgifterna inte kan göras gemensamt tillgängliga, eftersom de inte helt uppfyller de krav som ställs på sådana uppgifter.

Säkerhetspolisen behöver emellertid kunna tillgängliggöra sådan ostrukturerad information till fler än ett fåtal tjänstemän som arbetar med bearbetning och analys och i vissa fall under längre tid än under ett inledande skede. Det finns risk för att relevant information inte kommer den operativa verksamheten till del om den inte kan göras gemensamt tillgänglig. En konsekvens kan bli att viktig information om t.ex. nära förestående attentat inte upptäcks i tid. Om sådan information inte tillgängliggörs förrän den är färdigbearbetad kan det också leda till att Säkerhetspolisens förmåga att identifiera, bedöma och reducera hot och sårbarheter minskar. Tillgång till ostrukturerad information är enligt uppgift särskilt viktig för att kunna identifiera aktörer som agerar ensamma.

Säkerhetspolisen har till uppgift att skydda grundläggande samhällsfunktioner och att bekämpa terrorism. Vid en intresseavvägning mellan verksamhetens behov och enskildas integritet väger därför verksamhetsintresset tyngre än annars. Att tillåta att information tillgängliggörs i något större utsträckning än i dag trots att den inte hunnit struktureras och, där det krävs, förses med särskilda upplysningar får enligt utredningens mening mot den bakgrunden accepteras.

Det befintliga undantaget från kravet på upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak behöver därför enligt utredningens mening justeras.

Utformningen av undantaget

I Säkerhetspolisens underrättelsearbete är utgångspunkten att uppgifter som inte har bedömts och tillförts en upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak varken kan läggas till grund för beslut, bedömningar eller åtgärder. Per-

sonalen är således van vid att hantera svårbedömd information och det finns, enligt myndigheten, tydliga rutiner för hur ostrukturerad information ska behandlas. Risken för att sådan information leder till felbedömningar och åtgärder som inte är sakligt motiverade anses mot den bakgrunden vara liten.

De skäl som Säkerhetspolisen har fört fram för att undantaget bör tillåta att ostrukturerad information får tillgängliggöras i större utsträckning än i dag gör att undantaget bör omformuleras. Det är först när bearbetningen är genomförd som det är möjligt att påföra de särskilda upplysningar om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak som krävs i vissa fall. Undantaget bör därför gälla fram till dess att bearbetningen av uppgifterna är genomförd. En sådan lösning tillgodoser Säkerhetspolisens behov på ett bättre sätt. Genom den formuleringen blir det också tydligare hur länge undantaget gäller. Viktig underrättelseinformation kan då vid behov göras gemensamt tillgänglig på ett sätt som bättre svarar mot Säkerhetspolisens behov. Utgångspunkten är dock fortfarande att Säkerhetspolisen ska genomföra bearbetningen och analysen av den ostrukturerade informationen så snart som möjligt.

Det är viktigt att understryka att hela uppgiftssamlingen för bearbetning och analys inte undantas från kravet på särskilda upplysningar. Undantaget omfattar endast sådana uppgifter i uppgiftssamlingen som inte har hunnit bearbetas. Så snart bearbetningen är genomförd och informationen strukturerad är undantaget inte längre tillämpligt. Personuppgifterna ska då förses med särskilda upplysningar om det behövs.

När ska behandlingen senast upphöra?

Enligt 6 kap. 12 § andra stycket polisdatalagen ska personuppgifter i en uppgiftssamling för bearbetning och analys gallras senast tre år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes. Enligt huvudregeln i 6 kap. 6 § första stycket polisdatalagen får uppgifter dock inte bevaras under längre tid än som behövs för något eller några av de ändamål för vilka Säkerhetspolisen får behandla personuppgifter. Utredningen föreslår i avsnitt 14.13.2 och 14.13.4 att motsvarande reglering ska finnas i den nya lagen.

Den generella bestämmelsen om längsta tid för behandling innebär att behandlingen ska upphöra så fort Säkerhetspolisen bedömer att det inte längre finns behov av att behandla uppgifterna för något eller några av de syften för vilka myndigheten får behandla personuppgifter. Behandlingen ska således upphöra även om tidsfristen om tre år inte har löpt ut. Det förutsätter dock att det går att bedöma om personuppgifterna behövs för något av dessa syften. Bestämmelsen ger stöd för fortsatt behandling så länge uppgifterna behövs för något eller några av de syften som anges i lagen (se avsnitt 14.13.2). Det finns således stöd för fortsatt behandling om Säkerhetspolisen t.ex. bedömer att uppgifterna allmänt är värdefulla för att förebygga, förhindra och upptäcka brottslig verksamhet (se prop. 2009/10:85 s. 327 och 367 f.).

När det gäller ostrukturerad underrättelseinformation ligger det i sakens natur att det är svårt att bedöma det fortsatta behovet av behandling. Bedömningen måste innan bearbetningen och analysen är klar göras på ett mer övergripande plan och i större utsträckning utgå från sannolikheten att uppgifterna kan komma att behövas i verksamheten än en reell bedömning av den enskilda uppgiften. Enligt utredningens mening kan det vid en sådan övergripande bedömning ofta finnas behov av fortsatt behandling av den ostrukturerade informationen för något av de syften som anges i lagen.

14.11 Elektroniskt utlämnande

14.11.1 Elektroniskt utlämnande på annat sätt än genom direktåtkomst

Utredningens förslag: Säkerhetspolisen ska få lämna ut personuppgifter elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt.

Regeringen ska genom föreskrifter kunna begränsa möjligheten att lämna ut personuppgifter på det sättet.

Skälen för utredningens förslag: Enligt 2 kap. 20 § polisdatalagen får enstaka personuppgifter lämnas ut på medium för automatiserad behandling. Regleringen i 2 kap. 20 § polisdatalagen gäller genom en hänvisning i 6 kap. 4 § för Säkerhetspolisen. Regeringen

kan meddela föreskrifter om att uppgifter får lämnas ut på sådant medium även i andra fall. Sådana föreskrifter finns i bl.a. 18 § polisdataförordningen. I avsnitt 5.6.4 föreslår utredningen att möjligheten att lämna ut personuppgifter i annan elektronisk form än genom direktåtkomst ska utvidgas i de brottsbekämpande myndigheternas registerförfattningar. De skäl som anges där för en utvidgning är giltiga även för Säkerhetspolisen. I den nya lagen bör det därför tas in en bestämmelse som ger Säkerhetspolisen möjlighet att lämna ut uppgifter elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt. Regeringen bör kunna meddela föreskrifter om begränsning av möjligheten att lämna ut personuppgifter på det sättet.

14.11.2 Behovet av direktåtkomst

Utredningens förslag: Elektroniskt utlämnande genom direktåtkomst ska vara tillåtet enbart i den utsträckning som anges i den nya lagen.

Skälen för utredningens förslag

Nuvarande reglering

I avsnitt 5.6.1 och 5.6.2 redogör utredningen för vad som är direktåtkomst och vilka risker det anses medföra. I förarbetena till polisdatalagen konstaterar regeringen att en ordning som innebär informationsutbyte enbart genom manuell behandling skapar praktiska problem, eftersom brottsbekämpningen bedrivs dygnet runt. Uppgifter som en tjänsteman behöver omedelbart för att kunna utföra en tjänsteåtgärd måste vara lätt tillgängliga även utanför vanlig kontorstid. Därför infördes regler om direktåtkomst i polisdatalagen. Regeringen ansåg dock att det inte borde vara möjligt att medge direktåtkomst till personuppgifter som behandlas av Säkerhetspolisen, eftersom myndigheten behandlar särskilt känsliga uppgifter. Några skäl för att ge möjlighet till direktåtkomst till sådana personuppgifter framkom varken under det utredningsarbete som låg till grund för lagstiftningen eller under remissbehandlingen (se prop.

2009/10:85 s. 178 f.). Säkerhetspolisen har därför i dag inte någon möjlighet att tillhandahålla personuppgifter genom direktåtkomst.

Ett effektivare informationsutbyte är nödvändigt

Säkerhetspolisen utbyter i dag information med andra myndigheter manuellt. Begränsningarna när det gäller elektroniskt utlämnande av personuppgifter medför att myndigheten måste delge operativ information antingen i pappersform eller elektroniskt i enskilda handlingar. Det gäller både i förhållande till svenska och utländska myndigheter. Eftersom Säkerhetspolisen dagligen utbyter mellan 50 och 100 meddelanden med andra staters underrättelse- och säkerhetstjänster innebär det en avsevärd begränsning. Information som andra myndigheter har behov av kommer enligt Säkerhetspolisen inte myndigheterna till del i den utsträckning som är önskvärd på grund av att sätten för utlämnande är ineffektiva och resurskrävande. Det finns därför risk att viktig och brådskande information inte når fram i tid.

Säkerhetspolisens behov av effektivare informationsutbyte har ökat markant under de senaste åren. Det politiska läget i Sverige och i omvärlden, med bl.a. omfattande flyktingströmmar och ett ständigt terrorhot, ställer nya krav på samarbete och effektivt informationsutbyte med både svenska och utländska myndigheter. Säkerhetspolisen har under utredningsarbetet understrukt behovet av att kunna dela viss information med andra myndigheter genom direktåtkomst.

Ökade möjligheter till elektroniskt utlämnande räcker inte

Lagstiftaren såg vid polisdatalagens tillkomst inte något behov av att reglera direktåtkomst till personuppgifter som Säkerhetspolisen behandlar. Någon egentlig analys av det lämpliga i att tillåta direktåtkomst gjordes inte (se prop. 2009/10:85 s. 178 f.). Saken har nu kommit i ett annat ljus i och med att Säkerhetspolisen har påtalat behovet av att kunna dela information på ett helt annat sätt än tidigare, bl.a. i det europeiska samarbetet mot terrorism. Regeringens uttalanden i förarbetena hindrar inte att en annan bedömning görs nu, särskilt mot bakgrund av att regeringen nyligen föreslagit viss

direktåtkomst till Säkerhetspolisens information (se lagrådsremissen den 7 september 2017, Ett mer effektivt informationsutbyte vid Nationellt centrum för terrorhotbedömning, s. 19 f.).

Eftersom brottsbekämpning bedrivs dygnet runt är en ordning med i huvudsak manuellt utlämnande begränsande. Uppgifter som en tjänsteman behöver omedelbart för att kunna genomföra en tjänsteåtgärd måste vara tillgängliga även utanför kontorstid. Elektroniskt utlämnande på annat sätt än genom direktåtkomst förutsätter att det finns personal på plats och att de har utrymme att bedöma om informationen kan lämnas ut. Om så inte är fallet fördröjs informationsöverföringen, vilket kan få allvarliga konsekvenser för brottsbekämpningen. I förarbetena till polisdatalagen konstaterar regeringen också att direktåtkomst inte bara är ett enkelt och arbetsbesparande sätt att lämna ut information utan ibland det enda i praktiken möjliga sättet att göra uppgifterna tillgängliga när de behövs (se prop. 2009/10:85 s. 168).

I jämförelse med annat elektroniskt utlämnande innebär direktåtkomst effektivitetsvinster. Den myndighet som vill ha information behöver inte begära att få uppgifterna, utan kan söka i den information som har gjorts tillgänglig. Den myndighet som medgett direktåtkomst behöver inte avsätta resurser för att hantera förfrågningar från den andra myndigheten. Utlämnande genom direktåtkomst kan även innebära fördelar ur informationssäkerhetssynpunkt, eftersom överföring av information vid direktåtkomst kan göras på säkrare sätt än genom t.ex. e-post (se nyss nämnda lagrådsremiss s. 21). Uppgifter som lämnas ut elektroniskt på annat sätt än genom direktåtkomst, t.ex. via e-post, riskerar att snabbt bli inaktuella, eftersom de inte uppdateras automatiskt. Inaktuella uppgifter kan ibland vara mer skadliga än ingen information alls.

Det kan ofta vara bråttom att hantera den information som kommer in till Säkerhetspolisen. Det kan t.ex. röra sig om information om ett planerat attentat mot mål i Sverige eller mot svenska intressen. Det är då viktigt att Säkerhetspolisen kan dela med sig av informationen till andra berörda myndigheter så fort som möjligt. Om det kan göras genom direktåtkomst sparas tid och resurser samtidigt som berörda mottagare kan ta del av informationen när det passar dem. Information som inte behöver förmedlas muntligt eller genom att särskilda dokument framställs utan i stället kan delas i sitt ursprungliga skick ökar kvaliteten i informationsutbytet.

Den utökade möjlighet att lämna ut personuppgifter elektroniskt som föreslås i avsnitt 14.11.1 räcker därför enligt utredningens mening inte för att effektivisera Säkerhetspolisens informationsutbyte. Myndigheten har behov av att kunna lämna ut vissa uppgifter genom direktåtkomst.

Den nya lagen bör medge direktåtkomst

Direktåtkomst medför att uppgifter blir tillgängliga för fler personer och att den utlämnande myndighetens möjligheter att kontrollera användningen av uppgifterna minskar. En möjlighet till direktåtkomst anses därför generellt sett medföra ökad risk för intrång i den personliga integriteten. Säkerhetspolisen behandlar stora mängder personuppgifter i sina uppgiftssamlingar och många av dem är av känslig karaktär. Ju fler personer som har tillgång till sådana uppgiftssamlingar desto mer påtaglig är risken för intrång. Även om det är möjligt att genom särskilda åtgärder motverka eventuella risker är det viktigt att mottagarnas behov av direktåtkomst övervägs noga och att behoven vägs mot integritetsriskerna. Verksamhetsbehoven måste därför vägas mot hänsynen till den enskildes integritet.

Enligt 2 kap. 21 § första stycket polisdatalagen är utlämnande genom direktåtkomst tillåtet bara i den utsträckning som följer av lagen. I förarbetena till polisdatalagen framhålls att det från integritetssynpunkt finns fördelar med en lösning där det i lagen framgår i vilken utsträckning direktåtkomst får medges. Det underlättar för tillämparen om det anges i vilken utsträckning direktåtkomst kan förekomma (se prop. 2009/10:85 s. 172). En motsvarande bestämmelse bör därför införas i den nya lagen. Genom det säkerställs att riksdagen beslutar om i vilken utsträckning det är tillåtet att medge direktåtkomst.

Säkerhetspolisen utbyter redan en stor mängd information med både nationella och utländska myndigheter. Möjligheten att medge direktåtkomst innebär inte att Säkerhetspolisen får behandla eller lämna ut fler eller andra personuppgifter än i dag. Utlämnande genom direktåtkomst är endast ett mer effektivt sätt att tillhandahålla den information som ändå får lämnas ut. Det ligger också i sakens natur att Säkerhetspolisen lägger särskild vikt vid att pröva

om information ska delas med andra. Myndigheten har starkt intresse av att se till att inte fler uppgifter än nödvändigt tillgängliggörs för andra. Möjligheten att medge direktåtkomst förändrar ingenting i det avseendet.

14.11.3 Direktåtkomst för vissa svenska myndigheter

Utredningens förslag: Polismyndigheten ska för att kunna förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott få medges direktåtkomst till personuppgifter som Säkerhetspolisen behandlar för vissa syften.

Försvarets radioanstalt och Försvarmakten ska i sin försvarsunderrättelseverksamhet och militära säkerhetstjänst få medges direktåtkomst till personuppgifter som Säkerhetspolisen behandlar för vissa syften.

Direktåtkomsten ska endast få avse personuppgifter som har gjorts gemensamt tillgängliga.

Vad som ska gälla angående omfattningen av direktåtkomsten och behörighet och säkerhet vid sådan åtkomst ska regleras i förordning.

Skälen för utredningens förslag

Direktåtkomst bara för några få myndigheter

De brottsbekämpande myndigheterna behöver samarbeta för att bekämpa brottslighet. Av samma skäl som det är viktigt att man inom Säkerhetspolisen på ett effektivt sätt kan tillgodogöra sig den information som samlats inom myndigheten är det viktigt att nyttiggöra informationen i samarbetet med andra brottsbekämpande myndigheter (jfr prop. 2009/10:85 s. 166 f.). Bland de brottsbekämpande myndigheterna är det dock enligt utredningens mening bara Polismyndigheten som har sådana arbetsuppgifter att det bör övervägas om Säkerhetspolisen ska kunna tillhandahålla information genom direktåtkomst.

Säkerhetspolisen samarbetar också nära med försvarsunderrättelsemyndigheterna. Samarbetet är av stor betydelse för att Säkerhetspolisen ska kunna fullgöra sina uppgifter som säkerhetstjänst.

Även i förhållande till dessa myndigheter bör det därför övervägas om Säkerhetspolisen ska kunna tillhandahålla information genom direktåtkomst.

För att Säkerhetspolisen på ett effektivt sätt ska kunna förebygga, förhindra och upptäcka brottslig verksamhet och utreda och lagföra brott krävs det ett utvecklat samarbete även med andra myndigheter. Säkerhetspolisen är initiativtagare och sammankallande i Samverkansrådet mot terrorism där 13 andra myndigheter ingår. Samarbetet syftar till att stärka Sveriges förmåga att motverka och hantera terrorism. Ett annat exempel är Säkerhetspolisens samarbete med Migrationsverket i syfte att identifiera säkerhetshot i migrationsströmmarna till Sverige. Utredningen anser att det i dag inte finns något behov av att kunna medge någon av dessa myndigheter direktåtkomst.

Direktåtkomst för Polismyndigheten

Säkerhetspolisen och Polismyndigheten har ett väl utvecklat samarbete. Säkerhetspolisen ska enligt 11 § instruktionen samarbeta med Polismyndigheten i den utsträckning som behövs för att polisverksamheten ska kunna bedrivas effektivt. Ett effektivt polisiärt samarbete kräver ett omfattande utbyte av information. Informationsutbytet kan vara helt avgörande för att kunna bedöma och reducera hot. I operativa ärenden är behovet av information dessutom tidskritiskt. Som exempel kan nämnas attentatet på Drottninggatan i Stockholm i april 2017 och mordet på statsminister Olof Palme. Det går i sådana situationer inte att förlita sig enbart på manuell hantering. Det talar för att Säkerhetspolisen bör ges möjlighet att medge Polismyndigheten direktåtkomst till personuppgifter som behandlas hos myndigheten.

Personuppgifter som Säkerhetspolisen typiskt sett bör kunna delge Polismyndigheten behandlas med stöd av flertalet av de tillåtna rättsliga grunderna som gäller för Säkerhetspolisen. Ett stort antal av de personer som Säkerhetspolisen har ögonen på är samtidigt föremål för underrättelseverksamhet eller brottsutredning hos Polismyndigheten, på grund av att de misstänks för annan brottslighet. I Säkerhetspolisens brottsbekämpning kan inte sällan andra brott avslöjas. Information som rör allvarliga brott som har begåtts

eller planeras bör naturligtvis kunna delas. Ett effektivt informationsutbyte mellan Säkerhetspolisen och Polismyndigheten är därför en förutsättning för att kunna förebygga och förhindra såväl terrorism som organiserad brottslighet. Myndigheterna kan vidare ha ett ömsesidigt intresse av att känna till om den andra myndigheten vill ha hjälp med iakttagelser rörande vissa personer. Likaså finns det ibland intresse av att se till att den andra myndigheten inte ingriper mot en viss person om ett obetydligt brott skulle begås, eftersom det skulle kunna skada pågående brottspaning eller brottsutredning som rör allvarligare brott.

Säkerhetspolisen har intresse av att sprida information om personer som skulle kunna utgöra säkerhetshot och om företeelser som Polismyndigheten bör vara vaksam på. Sådana uppgifter kan behöva spridas exempelvis för att underlätta personskyddsarbetet eller skapa bättre förutsättningar för samarbete om hotnivån förändras. Även Säkerhetspolisens arbetsuppgifter inom författningsskyddet och på utlännings- och medborgarskapsområdet kan generera behov av informationsutbyte.

Polismyndigheten har inte behov av att ta del av information från Säkerhetspolisen genom direktåtkomst i alla sina verksamhetsgrenar. Behovet gör sig främst gällande när Polismyndigheten utför en arbetsuppgift i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet eller att utreda eller lagföra brott. Myndigheten har således inget behov av direktåtkomst till uppgifter hos Säkerhetspolisen för att fullgöra förpliktelser som följer av internationella åtaganden eller för att utföra en arbetsuppgift i syfte att upprätthålla allmän ordning och säkerhet. Direktåtkomst bör därför inte få medges för sådana syften.

Direktåtkomst för Försvarets radioanstalt och Försvarsmakten

Säkerhetspolisen, Försvarsmakten och Försvarets radioanstalt har uppdrag som till viss del tangerar eller överlappar varandra och därmed förutsätter ett nära samarbete och kontinuerligt informationsutbyte. Försvarsmakten och Försvarets radioanstalt har möjlighet att medge Säkerhetspolisen direktåtkomst till vissa uppgiftssamlingar hos respektive myndighet. Vidare är Säkerhetspolisen en av de myndigheter som enligt 4 § lagen (2008:717) om signalspaning i

försvarsunderrättelseverksamhet får ange inriktning för Försvarets radioanstalts signalspaning.

Ett exempel på ett mer formaliserat samarbete mellan myndigheterna är samarbetet inom ramen för Nationellt centrum för terrorhotbedömning. Där arbetar myndigheterna tillsammans i gemensamma lokaler och tar gemensamt fram rapporter om terrorhotet mot Sverige och svenska intressen. Syftet är att stärka den samlade förmågan hos Säkerhetspolisen, Försvarmakten och Försvarets radioanstalt och att ta tillvara myndigheternas samlade kompetens. Samarbetet kräver ett omfattande informationsutbyte (se *Behandling av personuppgifter inom Nationellt centrum för terrorhotbedömning*, Ds 2016:31, s. 170 f.). Regeringen har som nyss nämnts beslutat en lagrådsremiss med förslag om att Säkerhetspolisen ska få medge dessa myndigheter direktåtkomst till vissa uppgifter inom ramen för det samarbetet.

Myndigheternas behov av att utbyta information är emellertid inte begränsat till arbetet vid Nationellt centrum för terrorhotbedömning. Uppgifter som behandlas av en av myndigheterna kan tillsammans med uppgifter som behandlas av en annan ge en helhetsbild som inte framträder om bara den ena delen analyseras. Ett effektivt informationsutbyte kan alltså vara en förutsättning för att myndigheterna ska kunna fullgöra sina respektive uppdrag.

Mot den bakgrunden anser utredningen att övervägande skäl talar för att Säkerhetspolisen bör ges möjlighet att medge Försvarets radioanstalt och Försvarmakten direktåtkomst till personuppgifter som behandlas hos Säkerhetspolisen.

Försvarets radioanstalt har enligt utredningens mening behov av att ta del av information från Säkerhetspolisen genom direktåtkomst enbart i sin försvarsunderrättelseverksamhet. Försvarmakten har behov av att ta del av information genom direktåtkomst i både försvarsunderrättelseverksamheten och den militära säkerhetstjänsten.

Risken för integritetsintrång ska minimeras

Direktåtkomst innebär som nyss nämnts inte att fler eller andra personuppgifter får behandlas eller tillhandahållas. För att det ska vara acceptabelt att tillåta direktåtkomst måste det emellertid

säkerställas att det finns ett tillfredsställande skydd för den personliga integriteten.

En första viktig aspekt är vilket sekretesskydd personuppgifterna har hos den mottagande myndigheten. Sekretessregleringen ger i princip samma skydd för uppgifter i den brottsbekämpande verksamheten och i försvarsunderrättelseverksamheten. Uppgifter hos Säkerhetspolisen omfattas som regel av sekretess enligt 15 kap. 1 och 2 §§ och 18 kap. 1 och 2 §§ offentlighets- och sekretesslagen, dvs. utrikessekretess, försvarssekretess och sekretess till skydd för brottsbekämpning. Dessa sekretessbestämmelser gäller även hos Polismyndigheten, Försvarsmakten och Försvarets radioanstalt. Skyddet för enskildas personliga och ekonomiska förhållanden regleras i olika kapitel i offentlighets- och sekretesslagen för myndigheterna i fråga. För Säkerhetspolisen och Polismyndigheten finns reglerna i 35 kap. och 37 kap. offentlighets- och sekretesslagen, medan de för försvarsunderrättelsemyndigheterna finns i 38 kap. Regleringen ger dock i princip samma skydd.

En annan viktig fråga är hur uppgifterna kommer att användas hos den mottagande myndigheten. Om kretsen av personer som får tillgång till uppgifterna kan begränsas är risken för integritetsintrång generellt sett mindre. Av respektive myndighets registerförfattning framgår att tillgången till personuppgifter ska begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter. Det är således endast de tjänstemän som har behov av uppgifterna som får ges tillgång till dem.

Informationssäkerheten hos den mottagande myndigheten är också en viktig fråga. Är den säkerheten hög, så att det kan garanteras att informationen endast når dem som har rätt till den, inger möjlighet till direktåtkomst mindre betänkligheter från integritetsynpunkt än vad som annars hade varit fallet (jfr prop. 2009/10:85 s. 176). Polismyndigheten, Försvarets radioanstalt och Försvarsmakten har generellt en mycket hög säkerhet när det gäller hantering av information.

I förarbetena till polisdatalagen framhålls att det i fråga om direktåtkomst bör vara den myndighet som ansvarar för datasystemen som avgör i vilken utsträckning en annan myndighet kan anses tillgodose kraven på tillräcklig säkerhet. Den som medger direktåtkomst ska kunna ha kontroll över att det egna datasystemet alltså har tillräcklig säkerhet även efter det att andra myndigheter

fått tillgång till det (se prop. 2009/10:85 s. 178). Den närmare bedömningen av tekniska och andra förutsättningar för direktåtkomst bör därför göras av Säkerhetspolisens. Innan Säkerhetspolisens medger direktåtkomst bör myndigheten således försäkra sig om att den mottagande myndigheten har en acceptabel säkerhetsnivå. Det kan exempelvis vara fråga om system för utlämnande av behörighet, loggning av transaktioner och annan intern kontroll. Säkerhetspolisens bör kunna ställa upp villkor som rör sådana frågor. Det kan regleras i förordning.

De ökade integritetsrisker som möjlighet till direktåtkomst skulle kunna medföra kan alltså motverkas genom reglering av annat slag, som bestämmelser om sekretess, tillgång till uppgifter, informationssäkerhet och en effektiv tillsyn. Mot den bakgrunden anser utredningen att Säkerhetspolisens bör få möjlighet att medge vissa myndigheter direktåtkomst.

I avsnitt 14.12.2 och 14.12.3 behandlas frågan om hur sekretessregleringen förhåller sig till de föreslagna bestämmelserna om direktåtkomst.

Hur bör direktåtkomsten avgränsas?

Det föreslagna informationsutbytet innebär att uppgifter som behandlas av Säkerhetspolisens blir tillgängliga utanför det sammanhang där de ursprungligen behandlades. Det är då ur ett integritetsperspektiv rimligt att de särskilda, mer begränsande, reglerna om gemensamt tillgängliga uppgifter alltid tillämpas. Direktåtkomst bör därför endast kunna medges till uppgifter som är gemensamt tillgängliga i Säkerhetspolisens verksamhet.

Från ett integritetsperspektiv är det en fördel om det tydligt framgår av författningstexten vilka uppgifter som får lämnas ut genom direktåtkomst. Några begränsningar av det slaget har emellertid inte ansetts möjliga att utforma inom annan brottsbekämpande verksamhet. De enda undantagen är direktåtkomsten till dna-register och fingeravtrycksregister, där de myndigheter som har direktåtkomst endast får veta om en person förekommer i registren. Det är enligt utredningens mening varken möjligt eller lämpligt att i den nya lagen begränsa vilken typ av uppgifter som

direktåtkomsten får avse. Åtkomsten bör i stället begränsas till personuppgifter som Säkerhetspolisen behandlar för vissa syften.

När det gäller Polismyndigheten har Säkerhetspolisen främst behov av att dela information som behandlas inom områdena kontraterrorism, kontrapionage, författningsskydd och personskydd. Sådana uppgifter kan ha betydelse för Polismyndighetens brottsbekämpande verksamhet, särskilt när det gäller underrättelseverksamheten och det brottsförebyggande arbetet, men även för brottsutredningar i enskilda fall. För försvarsunderrättelsemyndigheterna är det främst uppgifter som rör kontraterrorism, kontrapionage och författningsskydd som kan behöva delas. Direktåtkomsten bör därför begränsas till sådana uppgifter.

Som tidigare konstaterats behöver de mottagande myndigheterna bara ta del av uppgifter från Säkerhetspolisen inom vissa delar av sin verksamhet. Det bör framgå av bestämmelserna om direktåtkomst att den endast får medges för vissa syften eller viss verksamhet. På så sätt kan åtkomsten begränsas. Finns det behov av att begränsa omfattningen av direktåtkomsten ytterligare bör det göras i förordning eller i myndighetsinterna regler.

En annan fråga är hur direktåtkomsten bör avgränsas tekniskt. Ett alternativ är att direktåtkomst endast ges till en avskild uppgiftssamling som upprättats i syfte att dela information. I avsnitt 14.11.4 föreslår utredningen en sådan lösning när det gäller direktåtkomst för utländska underrättelse- och säkerhetstjänster. Nackdelen med den lösningen är att den inte är teknikneutral. Dessutom finns det risk att de uppgifter som Säkerhetspolisen överför till uppgiftssamlingen inte uppdateras när uppgifterna uppdateras i verksamheten. Det kan därför vara lämpligare att medge direktåtkomst till viss information i Säkerhetspolisens it-system och i stället begränsa tillgången till informationen genom tilldelning av behörighet eller på annat sätt. Möjligheten att begränsa tillgången är i stort sett densamma oavsett vilken teknisk lösning som väljs. Bestämmelserna om direktåtkomst i den nya lagen bör mot den bakgrunden utformas teknikneutralt och inte begränsas till en uppgiftssamling eller någon liknande teknisk lösning.

Det bör framgå av lagen att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter om omfattningen av direktåtkomsten och om behörighet och säkerhet vid sådan åtkomst.

14.11.4 Direktåtkomst för underrättelse- och säkerhetstjänster inom EU och EES

Utredningens förslag: Om det behövs för samarbetet mot terrorism ska Säkerhetspolisen få medge en underrättelse- eller säkerhetstjänst i en medlemsstat i Europeiska unionen eller Europeiska ekonomiska samarbetsområdet direktåtkomst till personuppgifter i en avskild uppgiftssamling som upprättats i syfte att dela information med sådana mottagare. Uppgiftssamlingen ska endast få innehålla personuppgifter som har gjorts gemensamt tillgängliga och som behandlas i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar terrorbrott.

Innan direktåtkomst medges en utländsk underrättelse- eller säkerhetstjänst ska Säkerhetspolisen underrätta regeringen.

Skälen för utredningens förslag

Säkerhetsläget har förändrats

Antalet terroristattentat i Europa har ökat efter att den s.k. islamska staten i september 2014 uppmanade sina sympatisörer att agera mot västvärlden. Under de senaste åren har antalet attentat och attentatshot med koppling till Sverige ökat. Sverige har också i större utsträckning kommit att omnämnas som ett legitimt attentatsmål (se 2016 års redogörelse för tillämpningen av lagen om särskild utlänningskontroll, skr. 2016/17:72, s. 7). Från den 2 mars 2016 bedöms hotnivån avseende terrorism ligga på nivå tre (förhöjt hot). Det innebär att Säkerhetspolisen bedömer att terrorattentat kan drabba Sverige.

Det största terrorhotet mot Sverige kommer enligt Säkerhetspolisen från våldsbejakande islamistiska grupper. Flera hundra personer har rest från Sverige till konfliktområden för att ansluta sig till al-Qaidainspirerade grupper eller till islamiska staten. Motsvarande situation råder i andra europeiska länder. Bara av dem som rest till konflikten i Syrien och Irak har ett hundratal återvänt till Sverige (se skr. 2016/17:72 s. 5 f.). De som rest till ett konfliktområde utomlands och tränat eller stridit för våldsfrämjande grupper har förvärvat förmågor och skapat kontakter med individer som

kan hjälpa dem att begå terroristattentat eller radikaliseras eller rekrytera andra efter hemkomsten. De som rest till konfliktområden för att strida återvänder inte nödvändigtvis till det land de reste ifrån. Attentaten i Bryssel i mars 2016, där två personer med kopplingar till Sverige deltog, visar att hotaktörer ibland planerar dåden i ett land och utför dem i ett annat (se Säkerhetspolisens årsbok 2016 s. 40 f.). Återvändare utgör enligt Säkerhetspolisen ett potentiellt hot mot Sverige och Europa, oavsett deras vistelseort, ursprungsland och nationalitet.

Behovet av att kunna medge direktåtkomst

Enligt 16 § instruktionen för Säkerhetspolisen ska myndigheten samarbeta med utländska myndigheter och organ i den utsträckning som behövs för Säkerhetspolisens verksamhet och som regeringen närmare bestämmer. Enligt Säkerhetspolisen är det i kontraterrorverksamheten som behovet av gränsöverskridande samarbete är störst.

Den internationella utvecklingen på terrorområdet, den våldsbejakande islamismens alltmer globala karaktär och ambitioner och utvecklingen i Sverige har enligt Säkerhetspolisen sammantaget ökat behovet av nära samverkan med säkerhets- och underrättelse-tjänster i andra stater på både strategisk, taktisk och operativ nivå (se Ds 2016:31 s. 158). De våldsbejakande islamistiska grupperna är internationella organisationer med följare i hela världen. Hotet från sådana grupper är därför ett för många stater gemensamt problem. Att Säkerhetspolisen, utöver att motverka terrorism i Sverige, även ska bidra till att förhindra terrorism utomlands ligger inte bara i svenskt intresse utan följer också av internationella åtaganden. Ett väl fungerande samarbete med andra underrättelse- och säkerhetstjänster är därför en förutsättning för att Säkerhetspolisen ska kunna fullgöra sina arbetsuppgifter.

Underrättelse- och säkerhetstjänster i de nordiska länderna och inom EU är särskilt viktiga samarbetsparter. Utöver de bilaterala kontakterna deltar Säkerhetspolisen i flera arbetsgrupper inom ramen för EU-samarbetet, i arbetet vid Europol och i det europeiska forumet Counter-terrorism Group (CTG).

Utvecklingen av det internationella samarbetet mot terrorism går mot ett allt snabbare och mer omfattande elektroniskt utbyte av information. Mot bakgrund av den nuvarande hotbilden är det viktigt att Säkerhetspolisen kan bidra aktivt till samarbetet inom CTG. För att Säkerhetspolisen ska kunna dela information om hot, händelser och personer när det behövs för att motverka terrorism behöver myndigheten enligt utredningens mening rättsliga förutsättningar för att kunna utbyta information effektivare än i dag.

Direktåtkomst för utländska myndigheter

Polisdatalagen ger i dag inte någon av de myndigheter som tillämpar lagen möjlighet att medge en utländsk myndighet direktåtkomst till personuppgifter. Det innebär emellertid inte att det saknas sådant informationsutbyte. Inom ramen för EU-samarbetet har olika lösningar skapats som ger större möjligheter att överföra personuppgifter elektroniskt än vad polisdatalagen ger intryck av. Ett exempel är Schengen Information System (SIS), som regleras i lagen om Schengens informationssystem. Varje stat ansvarar för sin del av systemet och registrerar uppgifter som genom EU:s försorg är åtkomliga genom direktåtkomst i varje stat som är medlem i Schengensamarbetet. Inom ramen för samarbetet enligt Prümrådsbeslutet får medlemsstaterna medge varandra direktåtkomst till uppgifter i dna- och fingeravtrycksregister. Ett annat exempel är samarbetet med Europol. Europol ansvarar för olika databaser och uppgiftssamlingar och ger myndigheter i medlemsstaterna tillgång till vissa uppgiftssamlingar genom direktåtkomst. Införlivandet av CBE-direktivet ger brottsbekämpande myndigheter direktåtkomst till uppgifter i andra staters fordonsregister. Även brottsbekämpande myndigheters tillgång till uppgifter i EU:s viseringsdatabas (VIS) är exempel på direktåtkomst över gränserna.

Eftersom nationell säkerhet ligger utanför EU-samarbetet kan det inte förväntas att liknande lösningar kommer att finnas inom Säkerhetspolisens verksamhetsområde. För att möjliggöra direktåtkomst krävs därför en annan reglering. I avsnitt 14.11.2 konstaterar utredningen att den utökade möjligheten att lämna ut uppgifter elektroniskt som föreslås i avsnitt 14.11.1 inte är tillräcklig för att

tillgodose Säkerhetspolisens nuvarande behov. Det gäller även utlämnande till utländska underrättelse- och säkerhetstjänster.

Bör direktåtkomst kunna medges?

Vid risk för terroristattentat är snabbhet i informationsutbytet av avgörande betydelse för att undvika skador. På samma sätt som när det gäller informationsutbytet med svenska myndigheter finns det därför behov av att kunna dela viss information genom direktåtkomst med utländska myndigheter. Det gäller framför allt andra staters underrättelse- och säkerhetstjänster.

Det ligger närmast till hands att tillåta informationsutbyte av nu aktuellt slag med de andra nordiska länderna. Det nära samarbete som förekommer inom EU när det gäller bekämpning av terrorism och de kopplingar till Sverige som man har kunnat konstatera vid några av terroristattentaten i Europa under senare år gör emellertid enligt utredningens mening att en begränsning till enbart de nordiska länderna blir för snäv. Mot den bakgrunden bör möjligheten till direktåtkomst omfatta medlemsstater i EU och EES.

När personuppgifter lämnas ut till utländska myndigheter för behandling där kan det inte sällan vara svårt att avgöra vilket skydd uppgifterna får. Det gäller emellertid inte om utlämnandet begränsas till underrättelse- och säkerhetstjänster inom EU och EES. Där är regleringen av personuppgiftsbehandling och skyddet för personuppgifter till stor del desamma, eftersom alla stater är bundna av dataskyddskonventionen. För EU:s medlemsstater gäller även andra rättsakter som skapar en enhetlig reglering. Det rör sig vidare om utlämnande till myndigheter som generellt sett har mycket hög säkerhet när det gäller hantering av information.

Utredningen anser alltså att det i den nya lagen bör tas in en bestämmelse som möjliggör utlämnande genom direktåtkomst till underrättelse- och säkerhetstjänster inom EU och EES.

Hur bör direktåtkomsten avgränsas?

Förutom att endast underrättelse- och säkerhetstjänster i stater som är medlemmar i EU eller EES bör få medges direktåtkomst bör uppgiftslämnandet begränsas till personuppgifter som Säker-

hetspolisen behandlar i syfte att förebygga, förhindra eller upptäcka terrorbrott eller utreda sådana brott och som behövs för samarbetet mot terrorism. Möjligheten till direktåtkomst kommer inte att innebära att Säkerhetspolisen får tillhandahålla andra uppgifter än i dag. Ett effektivare uppgiftsutbyte och formen för utlämnandet kan ändå leda till att något fler uppgifter tillhandahålls.

För att ytterligare begränsa åtkomsten till uppgifterna och förhindra att utländska myndigheter får del av fler uppgifter än vad de behöver bör direktåtkomst endast få ges till en avskild uppgiftssamling som Säkerhetspolisen har upprättat i direkt syfte att dela information med sina utländska motsvarigheter. Med den lösningen säkerställs att Säkerhetspolisen på förhand dels avgör om det finns sakliga skäl att låta en utländsk underrättelse- eller säkerhetstjänst få del av personuppgiften, dels bedömer de rättsliga förutsättningarna att lämna ut den. Det görs då innan personuppgiften tillförs uppgiftssamlingen. Det minimerar risken för att fler uppgifter än nödvändigt tillgängliggörs. På samma sätt som när det gäller direktåtkomst för Polismyndigheten och försvarsunderrättelsemyndigheterna bör direktåtkomst bara kunna ges till uppgifter som har gjorts gemensamt tillgängliga. Innan Säkerhetspolisen tillhandahåller uppgifter till utländska myndigheter ska en sekretessprövning givetvis göras (se avsnitt 14.12.3). Uppgiftslämnandet ska också vara förenligt med bestämmelserna i övrigt i den nya lagen.

Underrättelseskyldighet till regeringen

Det är enligt utredningens mening särskilt viktigt att ett beslut att medge en utländsk myndighet direktåtkomst föregås av noggranna överväganden, även om det bara är fråga om tillgång till vissa uppgiftssamlingar som Säkerhetspolisen upprättar i syfte att kunna dela med sig av information. För att säkerställa att sådana överväganden görs och att det lämpliga i att en annan stats myndighet bereds möjlighet att genom direktåtkomst få del av sådana uppgiftssamlingar noga övervägs, bör det i den nya lagen tas in en bestämmelse som föreskriver att Säkerhetspolisen, innan direktåtkomst medges första gången, ska underrätta regeringen. En sådan underrättelse ger regeringen möjlighet att, om det skulle visa sig vara nödvändigt, kunna utfärda närmare föreskrifter om direktåtkomsten.

14.12 Sekretessbrytande bestämmelser

14.12.1 Uppgiftsskyldighet gällande rättsstatistik

Utredningens förslag: Personuppgifter som är nödvändiga för att framställa rättsstatistik ska lämnas till den myndighet som ansvarar för att framställa sådan statistik.

Skälen för utredningens förslag: Enligt 2 kap. 14 § polisdatalagen ska personuppgifter som är nödvändiga för att framställa rättsstatistik lämnas till den myndighet som ansvarar för att framställa sådan statistik. Bestämmelsen gäller för Säkerhetspolisen. Enligt 2 § förordningen (2016:1201) med instruktion för Brottsförebyggande rådet är rådet statistikansvarig myndighet. Enligt 24 kap. 8 § första stycket offentlighets- och sekretesslagen gäller absolut sekretess för uppgifter om en enskilds personliga och ekonomiska förhållanden i sådan särskild verksamhet hos en myndighet som avser framställning av statistik. I avsnitt 5.4.5 föreslås att skyldigheten att lämna uppgifter till rättsstatistiken ska regleras i brottsdatalagen. En motsvarande bestämmelse bör finnas i den nya lagen.

14.12.2 Sekretessgenombrott gentemot svenska myndigheter

Utredningens förslag: Polismyndigheten ska, trots sekretess enligt 21 kap. 3 § första stycket, 35 kap. 1 § och 37 kap. 1 § offentlighets- och sekretesslagen, ha rätt att ta del av personuppgifter som har gjorts gemensamt tillgängliga och som Säkerhetspolisen behandlar för vissa syften, om Polismyndigheten behöver uppgifterna för brottsbekämpning eller lagföring.

Försvarets radioanstalt och Försvarsmakten ska, trots sekretess enligt 21 kap. 3 § första stycket, 35 kap. 1 § och 37 kap. 1 § offentlighets- och sekretesslagen, ha rätt att ta del av personuppgifter som har gjorts gemensamt tillgängliga och som Säkerhetspolisen behandlar för vissa syften, om den mottagande myndigheten behöver uppgifterna i sin försvarsunderrättelseverksamhet eller militära säkerhetstjänst.

Skälen för utredningens förslag

Sekretess hos Säkerhetspolisen

De personuppgifter som Säkerhetspolisen behandlar omfattas som regel av sekretess enligt 15 kap. 1 och 2 §§ och 18 kap. 1 och 2 §§ offentlighets- och sekretesslagen. Där regleras utrikes- och försvarssekretessen och sekretessen till skydd för brottsbekämpningen. Bestämmelserna är tillämpliga på uppgifter som hänför sig till eller rör viss verksamhet. Det innebär att de gäller i all verksamhet där sådana uppgifter förekommer.

Uppgifter om enskilda i Säkerhetspolisens verksamhet omfattas som regel av sekretess enligt 35 kap. 1 § offentlighets- och sekretesslagen. Enligt paragrafen gäller sekretess för uppgifter som rör enskildas personliga och ekonomiska förhållanden och som förekommer i verksamhet för att bl.a. förebygga brott. Uppgifter om enskilda kan även omfattas av sekretess enligt 37 kap. 1 § och 21 kap. 3 och 5 §§. Enligt 37 kap. 1 § gäller sekretess i verksamhet för kontroll över utläningar och i ärenden om svenskt medborgarskap. Enligt 21 kap. 3 § gäller sekretess för enskildas kontaktuppgifter i vissa situationer och enligt 5 § gäller sekretess till skydd för utlännings säkerhet i vissa fall.

Sekretessen måste brytas

I avsnitt 14.11.3 föreslår utredningen att Säkerhetspolisen ska ges möjlighet att lämna ut personuppgifter till Polismyndigheten, Försvarets radioanstalt och Försvarsmakten genom direktåtkomst. Eftersom de uppgifter som Säkerhetspolisen behandlar i sin brottsbekämpande verksamhet som regel omfattas av sekretess behövs det bestämmelser som bryter sekretessen för att sådant utlämnande ska vara möjligt. Några sådana bestämmelser finns inte i dag.

Offentlighets- och sekretesslagen innehåller flera sekretessbrytande bestämmelser. Exempelvis hindrar sekretess inte att uppgifter lämnas till en annan myndighet om uppgiftsskyldighet följer av lag eller förordning, vilket framgår av 10 kap. 28 §. En bestämmelse om direktåtkomst reglerar endast själva formen för utlämnandet, dvs. på vilket sätt uppgifterna får lämnas ut, och är inte en sådan uppgiftsskyldighet som har sekretessbrytande verkan. Bestämmelser

om direktåtkomst brukar därför ofta kompletteras med sekretessbrytande bestämmelser som är utformade som uppgiftsskyldigheter på det sätt som avses i 10 kap. 28 §. Sådana bestämmelser bör enligt utredningen införas i den nya lagen för att möjliggöra utlämnande genom direktåtkomst.

Bestämmelser om uppgiftsskyldighet

Det ligger i sakens natur att sekretessbrytande bestämmelser som ska möjliggöra direktåtkomst mellan myndigheter måste vara generellt utformade, eftersom det vid direktåtkomst saknas möjlighet att göra en sekretessprövning i varje enskilt fall. Prövningen måste i stället göras i förväg (se prop. 2009/10:85 s. 192).

Sekretessbrytande bestämmelser i form av uppgiftsskyldighet brukar formuleras som en rätt för mottagaren att ta del av vissa uppgifter. Så har bestämmelserna om uppgiftsskyldighet formulerats i övriga registerförfattningar. Den formuleringen bör därför användas i den nya lagen.

Uppgiftsskyldigheten bör endast omfatta sådana uppgifter som de mottagande myndigheterna får ta del av genom direktåtkomst. De mottagande myndigheterna bör dessutom bara få tillgång till de aktuella uppgifterna när de behöver det för att kunna utföra vissa av sina arbetsuppgifter. Det bör framgå av bestämmelserna.

Vilka sekretessbestämmelser ska den nya regleringen avse?

Frågan är vilken slags sekretess som behöver brytas för att Säkerhetspolisen ska kunna lämna ut uppgifter genom direktåtkomst. Bestämmelserna i 15 kap. 1 och 2 §§ och 18 kap. 1 och 2 §§ offentlighets- och sekretesslagen avser att skydda nationens intressen och den verksamhet som Säkerhetspolisen bedriver. Enligt utredningens mening bör det inte medföra någon fara för rikets säkerhet eller innebära någon skada för Säkerhetspolisens verksamhet eller för nationen att sådana uppgifter som Säkerhetspolisen anser bör göras tillgängliga för Polismyndigheten och försvarsunderrättelsemyndigheterna lämnas ut till dessa myndigheter. Skaderekvisitet är då inte uppfyllt och något generellt behov av att bryta sekretessen enligt dessa bestämmelser kan inte anses föreligga. I de fall där ut-

lämnandet av en uppgift till någon av de aktuella myndigheterna skulle innebära att Säkerhetspolisens egen verksamhet riskerar att skadas, bör direktåtkomst givetvis inte komma ifråga.

Utredningen gör samma bedömning i fråga om uppgifter som omfattas av sekretess enligt 21 kap. 5 § offentlighets- och sekretesslagen. Den sekretessen gäller till skydd för utlännings säkerhet i vissa fall. Sekretess gäller om det kan antas att röjande av uppgiften skulle medföra fara för att någon utsätts för övergrepp eller lider annat allvarligt men som föranleds av förhållandet mellan utlänningen och en utländsk stat eller myndighet eller organisation av utläningar. Uppgiftslämnande till de angivna myndigheterna bör inte medföra någon sådan fara för enskilda. Bestämmelsen är dessutom tillämplig hos de mottagande myndigheterna. Det finns därför inget behov av att bryta sekretessen enligt den paragrafen.

Uppgifter om enskildas personliga och ekonomiska förhållanden omfattas hos Säkerhetspolisen av sekretess enligt 21 kap. 3 §, 35 kap. 1 § och 37 kap. 1 § offentlighets- och sekretesslagen. Utlämnande av sådana uppgifter torde nästan alltid anses vara till skada eller men för den enskilde. När sådana uppgifter ska lämnas ut måste dessutom en sekretessprövning göras i varje enskilt fall. Det är inte möjligt att på förhand göra en generell intresseavvägning beträffande sådana uppgifter. För att Säkerhetspolisen ska kunna lämna ut den typen av uppgifter till Polismyndigheten och försvarsunderrättelsemyndigheterna genom direktåtkomst krävs det därför att sekretessen bryts.

Bestämmelserna om sekretess till skydd för enskilda i 35 kap. 1 § och 37 kap. 1 § offentlighets- och sekretesslagen gäller även i Polismyndighetens verksamhet. För försvarsunderrättelsemyndigheterna finns en motsvarande bestämmelse om sekretess till skydd för enskilda i 38 kap. 4 §. Samtliga nu angivna bestämmelser gäller för uppgift om en enskilds personliga och ekonomiska förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till honom eller henne lider skada eller men. Sekretesskyddet för uppgifter om enskilda ser således i princip likadant ut för de aktuella myndigheterna. Bestämmelsen i 21 kap. 3 § är tillämplig i hela den statliga förvaltningen och gäller således hos alla myndigheter.

Bestämmelserna om uppgiftsskyldighet gentemot Polismyndigheten, Försvarets radioanstalt och Försvarsmakten bör således

bryta den sekretess som gäller enligt 21 kap. 3 § första stycket, 35 kap. 1 § och 37 kap. 1 § offentlighets- och sekretesslagen. I den mån andra sekretessbestämmelser är tillämpliga får det, på samma sätt som nu, göras en bedömning i det enskilda fallet av om sekretessen hindrar att uppgifterna lämnas ut.

14.12.3 Sekretessgenombrott i övrigt

Utredningens förslag: Om det är förenligt med svenska intressen, ska personuppgifter få lämnas ut till Interpol eller Europol, eller till en polismyndighet eller åklagarmyndighet i en stat som är ansluten till Interpol, om det behövs för att myndigheten eller organisationen ska kunna förebygga, förhindra, upptäcka, utreda eller lagföra brott. Om det är förenligt med svenska intressen ska personuppgifter också få lämnas ut till en utländsk underrättelse- eller säkerhetstjänst.

Personuppgifter ska vidare få lämnas ut till en utländsk myndighet eller mellanfolklig organisation, om utlämnandet följer av en internationell överenskommelse som Sverige har tillträtt efter riksdagens godkännande.

Skälen för utredningens förslag: Uppgifter som omfattas av sekretess får inte röjas för en utländsk myndighet. Lagstiftaren har dock föreskrivit undantag från denna huvudregel bl.a. om utlämnandet görs i enlighet med särskild föreskrift i lag eller förordning. Det framgår av 8 kap. 3 § 1 offentlighets- och sekretesslagen. En sådan föreskrift finns i 2 kap. 15 § polisdatalagen. Där regleras utlämnande av personuppgifter till utländska myndigheter och organ. Bestämmelsen gäller genom hänvisningen i 6 kap. 4 § i Säkerhetspolisens verksamhet. Om det är förenligt med svenska intressen får personuppgifter lämnas ut till Interpol eller Europol, eller till en polismyndighet eller åklagarmyndighet i en stat som är ansluten till Interpol, om det behövs för att myndigheten eller organisationen ska kunna förebygga, förhindra, upptäcka, utreda eller lagföra brott. Om det är förenligt med svenska intressen får personuppgifter också lämnas ut till utländsk underrättelse- eller säkerhetstjänst. Personuppgifter får dessutom lämnas ut till en utländsk myndighet eller mellanfolklig organisation, om utlämnandet följer

av en internationell överenskommelse som Sverige har tillträtt efter riksdagens godkännande.

Säkerhets- och integritetsskyddsnämnden har vid en granskning uttalat sig om den bedömning som ska göras vid utlämnande med stöd av 2 kap. 15 § polisdatalagen. Nämnden hänvisar till förarbetena till den tidigare gällande sekretesslagen (1980:100), där det anges att det intresse som sekretessen ska skydda ska tas med i bedömningen av om ett utlämnande kan anses förenligt med svenska intressen. Nämnden konstaterar att Säkerhetspolisens behov av att lämna uppgifter alltid måste vägas mot sekretessintresset, t.ex. det integritetsintrång och de konsekvenser som det kan innebära för den enskilde, vid bedömningen av om känslig underrättelseinformation kan lämnas till utlandet (se uttalande den 22 maj 2013, dnr 205-2012 s. 3).

Säkerhetspolisen bör kunna lämna ut uppgifter till en utländsk myndighet eller mellanfolklig organisation i samma utsträckning som i dag. En bestämmelse om det bör därför tas in i den nya lagen.

Det bör påpekas att när Säkerhetspolisen lämnar personuppgifter till mottagare i tredjeland eller till internationella organisationer måste myndigheten se till att utlämnandet är förenligt med bestämmelserna om överföring till sådana mottagare (se avsnitt 14.17).

14.13 Längsta tid som personuppgifter får behandlas

14.13.1 Innebörden av nuvarande reglering

Utredningens bedömning: Bestämmelserna om gallring och bevarande i polisdatalagen syftar till att skydda den personliga integriteten och reglerar inte gallring eller bevarande i arkivlagens mening. Motsvarande bestämmelser bör tas in i den nya lagen men formuleras så att det framgår att det är fråga om data-skyddsbestämmelser.

Skälen för utredningens bedömning

Olika typer av bestämmelser

Enligt huvudregeln i 6 kap. 6 § första stycket polisdatalagen får personuppgifter som Säkerhetspolisen behandlar inte bevaras under längre tid än vad som behövs för något eller några av de ändamål som anges i kapitlet. I 6 kap. polisdatalagen finns det ytterligare två typer av bestämmelser om bevarande och gallring av personuppgifter. De gäller enbart personuppgifter som behandlas automatiserat.

Den ena typen är bestämmelser om gallring och finns i 6 kap. 7 och 12 §§. De gäller för personuppgifter som inte förekommer i ärenden om utredning av eller lagföring för brott. Regleringen innebär att personuppgifterna inte får behandlas automatiserat efter vissa i lagen angivna tidsfrister. De får alltså inte heller arkiveras digitalt. Det följer av att det i 2 kap. 2 § andra stycket polisdatalagen, som gäller även för Säkerhetspolisen, görs undantag från 8 § andra stycket personuppgiftslagen, som föreskriver att arkivlagstiftningen har företräde framför personuppgiftslagstiftningen. Behandling för arkivändamål är dock tillåten om det med stöd av 6 kap. 7 § tredje stycket eller 6 kap. 14 § har meddelats föreskrifter om att personuppgifterna får bevaras för historiska, statistiska eller vetenskapliga ändamål.

Den andra typen av bestämmelser finns i 6 kap. 13 § polisdatalagen, som hänvisar till 3 kap. 9–13 §§ samma lag. De begränsar möjligheten att behandla personuppgifter i myndighetens brottsbekämpande verksamhet. Bestämmelserna gäller för personuppgifter som har gjorts gemensamt tillgängliga i ärenden om utredning av eller lagföring för brott. De föreskriver hur länge personuppgifterna får behandlas i den brottsbekämpande verksamheten, men det hindrar inte att uppgifterna behandlas bl.a. för arkivändamål. Regeringen kan enligt 6 kap. 6 § tredje stycket meddela föreskrifter om digital arkivering.

Bestämmelserna är inte arkivrättsliga regler

Bestämmelser som reglerar hur länge personuppgifter får behandlas är viktiga för att skydda den personliga integriteten. Det bör därför tas in bestämmelser i den nya lagen som motsvarar regleringen i

polisdatalagen om hur länge olika typer av personuppgifter får behandlas. I avsnitt 5.5.1 redovisar utredningen sin syn på dagens regler om gallring och bevarande. Det som sägs där har giltighet även för Säkerhetspolisens regelverk. När syftet med bestämmelserna är att skydda den personliga integriteten bör regleringen därför ange den yttersta gränsen för hur länge personuppgifterna får behandlas (se SOU 2017:29 s. 282 f.). Det gäller både gallringsbestämmelserna och bestämmelserna som begränsar möjligheten att behandla personuppgifter i den brottsbekämpande verksamheten. Bestämmelserna i den nya lagen bör formuleras så att det framgår att de är dataskyddsregler. De kan lämpligen samlas i ett särskilt kapitel som i övriga registerförfattningar.

14.13.2 Hur länge får personuppgifter behandlas?

Utredningens förslag: Personuppgifter ska inte få behandlas under längre tid än vad som behövs för något eller några av de syften för vilka Säkerhetspolisen får behandla personuppgifter. Det hindrar inte att Säkerhetspolisen arkiverar och bevarar allmänna handlingar eller att arkivmaterial lämnas till en arkivmyndighet.

Skälen för utredningens förslag

En generell bestämmelse om hur länge personuppgifter får behandlas

Enligt huvudregeln i 6 kap. 6 § första stycket polisdatalagen får personuppgifter inte bevaras under längre tid än vad som behövs för något eller några av de ändamål som anges i kapitlet. Bestämmelsen kompletteras av mer precisa bestämmelser om bevarande och gallring av vissa kategorier av personuppgifter.

En generell bestämmelse som anger hur länge personuppgifter får behandlas bör tas in i den nya lagen. Den bör utformas med 6 kap. 6 § första stycket polisdatalagen som mönster. För att tydliggöra att det inte är fråga om bevarande i arkivlagens mening bör ordet behandlas användas i stället för bevaras. Säkerhetspolisen bör alltså inte få behandla personuppgifter under längre tid än vad som behövs för något eller några av de syften för vilka myndigheten får

behandla personuppgifter enligt lagen. Liksom i polisdatalagen bör bestämmelsen kompletteras med mer detaljerade bestämmelser om hur länge vissa kategorier av personuppgifter får behandlas. Utredningen återkommer till det.

Behandling för arkivändamål

Enligt 8 § andra stycket personuppgiftslagen hindrar bestämmelserna i lagen inte att en myndighet arkiverar och bevarar allmänna handlingar eller att arkivmaterial tas om hand av en arkivmyndighet. Arkivlagstiftningen har alltså i fråga om allmänna handlingar företräde framför personuppgiftslagens bestämmelser om längsta bevarandetid. För Säkerhetspolisens del görs i polisdatalagen undantag från 8 § andra stycket personuppgiftslagen när det gäller personuppgifter som ska gallras enligt polisdatalagen.

Undantaget i polisdatalagen gäller bara när bestämmelser om gallring är tillämpliga. I övriga delar av Säkerhetspolisens verksamhet gäller 8 § andra stycket personuppgiftslagen, vilket innebär att arkivlagstiftningen har företräde. En bestämmelse med motsvarande innehåll bör tas in i den nya lagen.

Det bör anmärkas att behandling för arkivändamål omfattas av dataskyddsförordningens tillämpningsområde, oavsett om det är Säkerhetspolisen som arkiverar personuppgifterna eller om de överlämnas till en arkivmyndighet (jfr SOU 2017:29 s. 287).

14.13.3 Personuppgifter som inte har gjorts gemensamt tillgängliga

Utredningens förslag: Personuppgifter som inte har gjorts gemensamt tillgängliga ska inte få behandlas längre än ett år efter det att ärendet avslutades, om de behandlas i ett ärende, och inte längre än ett år efter det att de behandlades automatiserat första gången, om de inte kan hänföras till ett ärende.

Skälen för utredningens förslag: I 6 kap 7 § första stycket polisdatalagen föreskrivs att personuppgifter som behandlas automatiserat av Säkerhetspolisen och som inte har gjorts gemensamt till-

gängliga ska gallras senast ett år efter det att ärendet avslutades, om de behandlas i ett ärende. Om de inte kan hänföras till ett ärende ska uppgifterna gallras senast ett år efter det att de behandlades automatiserat första gången. Enligt utredningens mening finns det inte skäl att ändra på hur länge sådana uppgifter får behandlas. En motsvarande bestämmelse bör därför tas in i den nya lagen men den bör reglera hur länge personuppgifterna får behandlas.

Av 2 kap. 2 § andra stycket polisdatalagen följer att arkivlagstiftningen inte ska ha företräde om 6 kap. 7 § är tillämplig. Syftet med regleringen är att förtydliga att personuppgifter i dessa fall inte får behandlas automatiserat för arkivändamål. Det bör gälla även enligt den nya lagen. Det bör således göras undantag från bestämmelsen om att arkivlagstiftningen ska ha företräde (se avsnitt 14.13.2).

Den nu föreslagna regleringen bör inte gälla personuppgifter i ärenden om utredning av eller lagföring för brott. Den frågan behandlas i avsnitt 14.13.6.

14.13.4 Personuppgifter som har gjorts gemensamt tillgängliga

Utredningens förslag: Personuppgifter som har gjorts gemensamt tillgängliga ska inte få behandlas längre än tio år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes. Uppgifter om en person som vid tiden för registreringen inte fyllt 18 år ska dock inte få behandlas längre än fem år efter utgången av det kalenderår då den senaste registreringen gjordes avseende den unge. Det förutsätter att någon ny registrering inte har gjorts efter det att han eller hon fyllt 18 år.

Personuppgifter som behandlas i en uppgiftssamling som har skapats för att bearbeta och analysera information ska inte få behandlas längre än tre år efter utgången av det kalenderår då den senaste registreringen gjordes avseende personen.

När personuppgifter behandlas i underrättelseverksamhet ska endast registrering som avser personens anknytning till brottslig verksamhet påverka längsta tid för behandling.

Skälen för utredningens förslag

Gemensamt tillgängliga personuppgifter ska som huvudregel få behandlas lika länge som i dag

Enligt 6 kap. 12 § polisdatalagen ska gemensamt tillgängliga personuppgifter gallras senast tio år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes. Personuppgifter som behandlas i en uppgiftssamling som har skapats för att bearbeta och analysera information ska dock gallras senast tre år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes.

I förarbetena till polisdatalagen görs bedömningen att en allmän gallringsfrist om tio år utgjorde en lämplig avvägning mellan Säkerhetspolisens behov och den enskildes krav på att uppgifter inte bevaras alltför lång tid. I fråga om personuppgifter som förekommer i en uppgiftssamling som skapats för att bearbeta och analysera information gjordes dock bedömningen att en kortare gallringsfrist borde gälla (se prop. 2009/10:85 s. 269). Den bedömning som gjordes då av hur länge personuppgifter bör få behandlas har enligt utredningens mening fortfarande fog för sig. Bestämmelserna bör av de skäl som anges i avsnitt 14.13.1 formuleras så att de anger hur länge uppgifterna får behandlas. Utredningen återkommer till behovet av att beträffande några kategorier av personuppgifter ha en mer differentierad reglering.

Av 2 kap. 2 § andra stycket polisdatalagen följer att arkivlagstiftningen inte ska ha företräde om 6 kap. 12 § är tillämplig. Det samma bör gälla enligt den nya lagen. Det bör därför göras undantag från den föreslagna regeln om att arkivlagstiftningen ska ha företräde för nu aktuella personuppgifter.

En särskild bestämmelse för personuppgifter som rör barn

Polisdatalagen innehåller inte några särskilda bestämmelser om behandling av personuppgifter som avser barn. Samma bestämmelser gäller således vid personuppgiftsbehandlingen oavsett den registrerades ålder. Säkerhetspolisen har i sina interna styrdokument reglerat gallringsfristen i myndighetens centralregister för personer som vid tiden för registreringen inte fyllt 18 år. Sådana uppgifter gallras

senast fem år efter det att en uppgift om personen senast infördes. Säkerhets- och integritetsskyddsnämnden har särskilt granskat hur brottsbekämpande myndigheter behandlar personuppgifter om barn. Nämnden har uttalat att integritetsskyddande regler i polisdatalagen gör sig gällande i särskilt hög grad vid behandling av uppgifter om barn. Nämnden är också positiv till Säkerhetspolisens interna bestämmelser om kortare gallringsfrist för sådana uppgifter (se uttalande den 17 februari 2016, dnr 50-2015 s. 5 och 8). Mot den bakgrunden anser utredningen att det i den nya lagen bör föreskrivas kortare tid för behandling av uppgifter om personer som vid registreringen inte hade fyllt 18 år. Sådana uppgifter bör inte få behandlas längre än fem år efter utgången av det kalenderår då den senaste registreringen avseende den unge gjordes.

Omständigheter som kan påverka längsta tid för behandling

I avsnitt 5.5.4 föreslås att endast sådana omständigheter som har betydelse för personens anknytning till brottslig verksamhet bör kunna påverka att personuppgifter får fortsätta att behandlas i underrättelseverksamhet på grund av att det har tillkommit en ny registrering. Av de skäl som anges där bör regleringen i den nya lagen utformas på motsvarande sätt när det gäller personuppgifter i Säkerhetspolisens underrättelseverksamhet. När det gäller personuppgifter som behandlas för bl.a. personskydd, säkerhetsskydd eller ärenden enligt utlännings- och medborgarskapslagstiftningen bör regleringen på samma sätt som i dag utgå från när den senaste registreringen avseende personen gjordes.

14.13.5 Personuppgifter som rör viss säkerhetshotande verksamhet

Utredningens förslag: Personuppgifter som hänför sig till sådan säkerhetshotande verksamhet som avses i 18 och 19 kap. brottsbalken som utövas av främmande makt ska inte få behandlas längre än 40 år efter utgången av det kalenderår då den senaste registreringen gjordes avseende personens anknytning till brott eller brottslig verksamhet.

Skälen för utredningens förslag

Vad är kontraspionage?

Säkerhetspolisens kontraspionageverksamhet har till uppgift att förebygga, förhindra och upptäcka spioneri, olaglig underrättelseverksamhet och andra brott mot rikets säkerhet. Kontraspionage omfattar inhämtning av underrättelser om och bedömning av andra staters spionage mot Sverige. Sådant underrättelsearbete skapar underlag för olika typer av åtgärder mot andra staters säkerhets-hotande underrättelseverksamhet och är en del av Sveriges försvar.

Spioneribrott utövas ofta av två aktörer i förening. Den ena är en underrättelseofficer som tillhör en utländsk underrättelsetjänst. Den andra är spionen som t.ex. kan ha tillgång till information och miljöer där information kan inhämtas på uppdrag av underrättelseofficeren. Underrättelseofficerare arbetar långsiktigt med att leta efter lämpliga mål, att närma sig och odla kontakter med personer som har information om målet, för att i senare skeden eventuellt kunna rekrytera dem som spioner och handleda dem. Andra stater söker alltså fortlöpande efter lämpliga personer att rekrytera. Själva processen fram till värvningstillfället kan ta några år och i vissa fall ännu längre tid. I den efterföljande handledningsfasen kan den värvade personen handledas så länge han eller hon har tillgång eller kan få tillgång till den information som den andra statens underrättelsetjänst är intresserad av. Det kan pågå i flera decennier. En underrättelseofficer är däremot som regel bara stationerad i Sverige några år och förflyttas sedan till ett annat land. Eftersom stationeringstiden är begränsad måste värvning och handledning av spioner lämnas över mellan underrättelseofficerare.

Säkerhetspolisen arbetar med två olika metoder för att identifiera spioner. En metod är att leta direkt efter dem. En annan är att kartlägga och följa utländska underrättelseofficerares aktiviteter för att kunna identifiera misstänkta spioner. Genom att underrättelseofficerare lämnar handledningen vidare till sina efterträdare innebär byte av underrättelseofficerare en möjlighet för Säkerhetspolisen att kunna identifiera misstänkta spioner. Det är emellertid svårt, eftersom underrättelseofficerare är tränade i att undvika värdlandets säkerhetstjänst. Det innebär att iakttagelser som görs bekräftande en underrättelseofficer kanske inte byggs på med nya

iakttagelser förrän efter flera byten på posten. Under tiden behöver informationen från kartläggningen behållas.

Andra staters underrättelseverksamhet i Sverige bygger således på långsiktigt arbete. En anledning till det är att det är relativt svårt att värva spioner. Alla stater strävar därför efter att använda dem så länge som möjligt. Spioneri är oftast en livslång sysselsättning. Det finns också exempel både i Sverige och utomlands på att spioner rekryterar sina barn som spioner. Säkerhetspolisens kontrapionageverksamhet måste därför anpassas till det långsiktiga tidsperspektivet.

Oavsett vilken metod Säkerhetspolisen använder kräver kontrapionage lagring av information i flera decennier. Exempelvis använder Säkerhetspolisen i dag regelmässigt uppgifter som inhämtades på 1980- och 90-talen. Erfarenheter från både Sverige och andra länder visar att det ofta tar mycket lång tid innan en spion avslöjas. Spionerna Stig Wennerström och Arne Treholt kan nämnas som exempel på det.

Nuvarande bestämmelser är inte ändamålsenliga

Säkerhetspolisen har i dag möjlighet att behandla personuppgifter i sin brottsbekämpande verksamhet under relativt lång tid. Enligt 6 kap. 12 § första stycket polisdatalagen ska personuppgifter som gjorts gemensamt tillgängliga gallras senast tio år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes. Om det finns särskilda skäl får Säkerhetspolisen dock besluta att personuppgifter får bevaras längre, om uppgifterna fortfarande behövs för det ändamål för vilket de behandlas. Säkerhetspolisen kan således under vissa förutsättningar besluta att förlänga gallringsfristen för personuppgifter inom kontrapionaget med ytterligare tio år.

Säkerhetspolisen förlänger regelmässigt gallringsfristen för personuppgifter i kontrapionaget. Från den 1 januari 2017 till den 23 mars 2017 fattades enligt Säkerhetspolisen drygt 400 enskilda beslut om att förlänga gallringsfristen för personuppgifter som behandlas inom kontrapionaget. Det rör sig således om fler än tusen enskilda förlängningsbeslut per år. Hanteringen medför omfattande administrativt arbete för personal med särskild sakkunskap

på området, eftersom lagstiftningen kräver att det fattas beslut om bevarande i varje enskilt fall.

Det finns risk för att personuppgifter, som borde bevaras, tas bort på grund av att Säkerhetspolisen i vissa fall måste prioritera operativa insatser före förlängningsbeslut. Inom kontraspionaget är det dessutom ofta svårt att vid tidpunkten för beslut om förlängning veta exakt vilka uppgifter som kommer att behövas i framtiden. Förlängning av fristen kan inte beslutas retroaktivt. Säkerhetspolisen har uppgett att myndigheten i ett flertal fall har gallrat personuppgifter där det i efterhand har visat sig att informationen varit relevant och därför borde ha behandlats längre.

Uppgifter inom kontraspionaget ska få behandlas längre

Enligt utredningens mening finns det på grund av kontraspionagets särdrag behov av att behandla personuppgifter hänförliga till sådan verksamhet under betydligt längre tid än huvudregeln i polisdatalagen medger. Säkerhetspolisen har visserligen möjlighet att genom särskilda beslut förlänga tiden för behandling. Det är emellertid inte rimligt att lägga betydande resurser på att regelbundet fatta beslut om sådan förlängning när det ofta på förhand kan förutses att förlängning av fristen är nödvändig. Risken att uppgifter gallras på grund av tidsbrist eller felaktiga beslut bör också vägas in.

Mot den bakgrunden anser utredningen att Säkerhetspolisen bör få behandla personuppgifter hänförliga till området kontraspionage under längre tid än vad som är tillåtet i dag. Det gäller framför allt uppgifter där grunden för registreringen är att personen är en misstänkt utländsk underrättelseofficer och hans eller hennes närmaste anhöriga. Det gäller också uppgifter om misstänkta spioner och deras närmaste anhöriga och händelser kopplade till dessa personer. Om sådana personuppgifter får behandlas under längre tid skulle det ge Säkerhetspolisen större möjligheter att inte bara identifiera misstänkta spioner och underrättelseofficerare, utan också att avföra eventuella felaktiga misstankar. På så sätt kan en förlängd tidsfrist i det här fallet också till viss del stärka integritetsskyddet.

Frågan är hur tidsfristen för behandling av aktuella uppgifter bör bestämmas. Från integritetssynpunkt är det viktigt att personuppgifter inte behandlas för länge. Samtidigt måste tidsfristen be-

stämmas på ett sätt som är ändamålsenligt och tillgodoser de behov som finns.

Försvarssekretessen, som regleras i 15 kap. 2 § offentlighets- och sekretesslagen, gäller enligt 4 § offentlighets- och sekretessförordningen (2009:641) i 95 år om uppgifterna rör underrättelseverksamheten inom underrättelse- och säkerhetstjänsten. Den svenska militära underrättelsetjänstens arbete och källor skyddas således under lång tid och man skulle kunna argumentera för att Säkerhetspolisens uppgifter som rör kontraspionage borde kunna behandlas lika länge. En annan möjlighet är att utgå från hur länge sekretess gäller för uppgifter i brottsbekämpande verksamhet, vilket är 70 år. En så lång tidsfrist som någon av de nu nämnda skulle dock innebära betydligt större integritetsintrång än i dag, eftersom det inte är sannolikt att Säkerhetspolisen fattar förlängningsbeslut för hela den tiden. Enligt utredningens mening kan verksamhetsbehoven tillgodoses med en kortare tidsfrist.

Erfarenheterna har visat att spioneri under 30–40 år inte är ovanligt. Med beaktande av det anser utredningen att fristen för hur länge personuppgifter i kontraspionageverksamheten ska få behandlas inte bör vara kortare än 40 år. Behandlingen av personuppgifterna kan då fortgå under en tid som motsvarar en spions yrkesverksamma liv. Med hänsyn till att det är fråga om mycket allvarliga brott anser utredningen att den föreslagna tidsfristen är en rimlig avvägning mellan samhällsintressena och enskildas integritet. I avsnitt 14.13.7 föreslår utredningen att Säkerhetspolisen även fortsättningsvis ska kunna fatta beslut om att i enskilda fall förlänga fristen för behandling av uppgifter.

Det bör alltså i den nya lagen tas in en bestämmelse som föreskriver att personuppgifter som hänför sig till sådan säkerhetshotande verksamhet som avses i 18 och 19 kap. brottsbalken som utövas av främmande makt inte får behandlas längre än 40 år efter utgången av det kalenderår då den senaste registreringen gjordes avseende personens anknytning till brott eller brottslig verksamhet. Utredningen återkommer till det i avsnitt 14.3.7. Undantag bör göras för uppgifter som behandlas i en uppgiftssamling för bearbetning och analys. För sådana uppgifter bör tidsfristen om tre år gälla (se avsnitt 14.13.4).

14.13.6 Ärenden om utredning av eller lagföring för brott

Utredningens förslag: Bestämmelser om begränsningar i möjligheten att behandla gemensamt tillgängliga uppgifter i brottsanmälningar, avslutade förundersökningar och andra liknande utredningar ska tas in i den nya lagen. Det ska framgå av bestämmelserna att de endast begränsar behandling för ändamål inom lagens tillämpningsområde.

Skälen för utredningens förslag

Nuvarande reglering

I 3 kap. 10–12 §§ polisdatalagen regleras hur länge personuppgifter som har gjorts gemensamt tillgängliga i ärenden om utredning av eller lagföring för brott längst får behandlas automatiserat i den brottsbekämpande verksamheten. Där föreskrivs bl.a. att om en brottsanmälan avskrivs på grund av att den påstådda gärningen inte utgör brott, får personuppgifterna i anmälan inte längre behandlas i den brottsbekämpande verksamheten. När det gäller förundersökningar och andra liknande utredningar föreskrivs att personuppgifter inte får behandlas i den brottsbekämpande verksamheten när det har förflutit fem år efter utgången av det kalenderår då en dom, eller ett beslut med anledning av domstolsprövning, vunnit laga kraft eller sedan fem år förflutit från utgången av det kalenderår då förundersökningen lades ned eller avslutades på annat sätt. I 3 kap. 13 § föreskrivs att om en förundersökning har lagts ned, om åtal har lagts ned eller om frikännande dom som har vunnit laga kraft har meddelats, får personen inte vara sökbar som misstänkt. Att bestämmelserna gäller i Säkerhetspolisens verksamhet framgår genom en hänvisning i 6 kap. 13 § polisdatalagen.

Samma reglering som i dag

Bestämmelserna om längsta tid för behandling av personuppgifter i ärenden om utredning av och lagföring för brott är utförligt motiverade i förarbetena (se prop. 2009/10:85 s. 223 f.). Skälen bakom den nuvarande ordningen gör sig fortfarande gällande. Det har inte

heller framkommit skäl att ändra regelverket. Därför bör bestämmelser med motsvarande innehåll tas in i den nya lagen.

Bestämmelserna i 3 kap. 10 och 11 §§ polisdatalagen hindrar inte att personuppgifter som behandlas automatiserat i den brottsbekämpande verksamheten fortsätter att behandlas automatiserat för ändamål utanför lagens tillämpningsområde under längre tid än vad som anges i bestämmelserna. De inskränker alltså enbart behandling i den brottsbekämpande verksamheten, vilket innebär att personuppgifterna t.ex. får behandlas automatiserat för arkivändamål. För att tydliggöra det bör det framgå av bestämmelserna i den nya lagen att de enbart reglerar hur länge personuppgifter får behandlas för ändamål inom lagens tillämpningsområde.

14.13.7 Möjlighet att förlänga tiden för behandling

Utredningens förslag: Om det finns särskilda skäl ska Säkerhetspolisen få besluta att personuppgifter får behandlas under längre tid än vad som anges för en viss kategori av uppgifter, om de fortfarande behövs för det ändamål för vilket de behandlas. Om personuppgifter behandlas med stöd av ett sådant beslut ska frågan om fortsatt behandling prövas på nytt senast vid utgången av det tionde kalenderåret efter beslutet eller, om det är fråga om uppgifter i en uppgiftssamling som har skapats för att bearbeta och analysera information, senast vid utgången av det tredje kalenderåret efter beslutet. Tiden för behandling får vid varje tillfälle förlängas med längst samma tid som den ursprungliga eller, om uppgifterna rör säkerhetshotande verksamhet eller avser någon som är under 18 år, längst tio år.

Skälen för utredningens förslag: Säkerhetspolisen har enligt 6 kap. 12 § tredje stycket polisdatalagen möjlighet att besluta att personuppgifter får bevaras längre än vad som anges i paragrafen, om det finns särskilda skäl och uppgifterna fortfarande behövs för det ändamål för vilket de behandlas. För uppgifter som får bevaras längst tio år får tiden förlängas med tio år och för uppgifter som får bevaras längst tre år får tiden förlängas med tre år.

Säkerhetspolisen bör även fortsättningsvis ha möjlighet att i vissa fall besluta om förlängd tid för behandling. En motsvarande

bestämmelse bör därför tas in i den nya lagen, men den bör formuleras så att den anger hur länge uppgifterna får behandlas.

Det bör enligt utredningens mening inte införas någon särskild frist för uppgifter om personer som vid tiden för registreringen inte har fyllt 18 år. Om Säkerhetspolisen gör bedömningen att det i ett enskilt fall finns särskilda skäl att förlänga fristen för behandling av sådana personuppgifter bör de kunna behandlas som längst ytterligare tio år.

Enligt utredningens mening bör Säkerhetspolisen ges möjlighet att förlänga tidsfristen även för behandling av personuppgifter som enligt den särskilda bestämmelsen om personuppgifter som rör viss säkerhetshotande verksamhet får behandlas längst 40 år. En förlängning motsvarande den tid som personuppgifterna ursprungligen får behandlas skulle dock i dessa fall leda till att uppgifterna får behandlas alltför länge. I likhet med vad som gäller för gemensamt tillgängliga uppgifter i övrigt bör uppgifterna få behandlas som längst tio år efter beslutet, om inte ett nytt beslut om förlängning fattas inom den fristen.

14.13.8 Föreskrifter

Utredningens förslag: Regeringen ska kunna meddela föreskrifter om att vissa kategorier av personuppgifter får behandlas för ändamål inom den nya lagens tillämpningsområde under längre tid än vad som anges i lagen.

Regeringen eller den myndighet som regeringen bestämmer ska kunna meddela föreskrifter om att personuppgifter får behandlas under längre tid än vad som anges i den nya lagen för arkivändamål av allmänt intresse och vetenskapliga, statistiska eller historiska ändamål och om begränsning av behandlingen av personuppgifter för ändamål inom den nya lagens tillämpningsområde vid digital arkivering.

Skälen för utredningens förslag

Föreskrifter om fortsatt behandling av vissa kategorier av personuppgifter

Enligt 3 kap. 12 § polisdatalagen har regeringen möjlighet att meddela föreskrifter om att vissa kategorier av personuppgifter i en brottsanmälan, förundersökning eller annan utredning som handläggs enligt bestämmelserna i 23 kap. rättegångsbalken får behandlas i den brottsbekämpande verksamheten under längre tid än vad som anges i 3 kap. 10 och 11 §§. Skälen för regleringen är utförligt redovisade i förarbetena till polisdatalagen (se prop. 2009/10:85 s. 226 f.). De gör sig alltjämt gällande och en motsvarande föreskriftsrätt bör därför tas in i den nya lagen.

Föreskrifter om fortsatt behandling för arkivändamål

Regeringen eller den myndighet som regeringen bestämmer har enligt 6 kap. 7 § tredje stycket och 14 § polisdatalagen möjlighet att meddela föreskrifter om att personuppgifter får bevaras för historiska, statistiska eller vetenskapliga ändamål. Motsvarande föreskriftsrätt bör finnas i den nya lagen. För att terminologin ska stämma överens med dataskyddsförordningen och övriga registerförfattningar inom brottsdatalagens tillämpningsområde bör det göras ett tillägg som innebär att föreskriftsrätten även omfattar behandling för arkivändamål av allmänt intresse (jfr avsnitt 5.5.2).

Föreskrifter om digital arkivering

Regeringen eller den myndighet som regeringen bestämmer har enligt 6 kap. 6 § tredje stycket polisdatalagen möjlighet att meddela föreskrifter om digital arkivering. Brottsanmälningar, förundersökningar och andra brottsutredningar bör få behandlas för arkivändamål med stöd av arkivlagen trots att de inte längre får behandlas i den brottsbekämpande verksamheten. Mot bakgrund av att arkivlagen inte hindrar eller ställer upp några begränsningar för fortsatt behandling av digitalt arkiverade uppgifter i den brottsbekämpande verksamheten, behövs det föreskrifter som anger ramen för fortsatt behandling inom lagens tillämpningsområde för att skapa nödvän-

digt integritetsskydd (jfr avsnitt 5.5.3). Sådana föreskrifter kan tas in i förordning. Det bör därför finnas en bestämmelse om föreskrifträtt som motsvarar 6 kap. 6 § tredje stycket polisdatalagen i den nya lagen.

14.14 Skyldigheter som personuppgiftsansvarig

Utredningens förslag: Det ska i den nya lagen tas in bestämmelser motsvarande dem i brottsdatalagen om den personuppgiftsansvariges skyldigheter i fråga om

- tekniska och organisatoriska åtgärder,
- tillgången till personuppgifter,
- konsekvensbedömning och förhandssamråd,
- skyddsåtgärder,
- samarbete med tillsynsmyndigheten,
- dataskyddsombud, och
- personuppgiftsbiträden.

Skyldigheten att föra register över kategorier av behandling av personuppgifter och att införa interna rutiner för anmälan av överträdelser ska regleras i förordning. Föreskrifter som fyller ut och preciserar bestämmelserna om Säkerhetspolisens skyldigheter som personuppgiftsansvarig ska också tas in i förordning.

Skälen för utredningens förslag

Nuvarande reglering

Som personuppgiftsansvarig är Säkerhetspolisen skyldig att vidta en mängd åtgärder, bl.a. för att säkerställa att personuppgiftsbehandlingen utförs författningsenligt och att skydda personuppgifterna. Skyldigheterna regleras dels i personuppgiftslagen, dels i polisdatalagen.

I 30 och 31 §§ personuppgiftslagen finns det bestämmelser om säkerhetsåtgärder och krav vid anlitande av personuppgiftsbiträden och i 38–40 §§ regleras personuppgiftsombudens uppgifter. I 2 kap. 11 § polisdatalagen föreskrivs att tillgången till personuppgifter ska begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter och i 6 kap. 5 § andra stycket föreskrivs att Säkerhetspolisen ska utse ett eller flera personuppgiftsombud. Vidare ska Säkerhetspolisen enligt 2 § polisdataförordningen i vissa situationer samråda med Datainspektionen och Säkerhets- och integritetsskyddsnämnden.

Regleringen i brottsdatalagen

I 3 kap. brottsdatalagen regleras de personuppgiftsansvarigas skyldigheter. Där ställs krav på olika åtgärder för att säkerställa författningens personuppgiftsbehandling och lämplig säkerhetsnivå. Det föreskrivs också att ett eller flera dataskyddsombud ska utses och det regleras utförligt vilka arbetsuppgifter ombuden ska ha. Det finns också bestämmelser om vad som gäller vid anlitande av personuppgiftsbiträden och vilka skyldigheter sådana biträden har. Vidare ställs det krav på samarbete med tillsynsmyndigheten. Regeringen kan meddela föreskrifter om skyldigheten att föra register över behandlingar och skyldigheten att införa interna rutiner för anmälan av överträdelser.

Regleringen bör vara densamma som i brottsdatalagen

Flertalet av de skyldigheter som behöriga myndigheter har enligt brottsdatalagen i egenskap av personuppgiftsansvariga gäller redan för Säkerhetspolisen. Vissa bestämmelser har motsvarigheter i Säkerhetspolisens nuvarande reglering, men är mer detaljerade eller har en något annorlunda utformning i brottsdatalagen. En del bestämmelser har emellertid ingen motsvarighet i dagens reglering och innebär således nya skyldigheter.

Enligt utredningens mening är huvuddelen av bestämmelserna om personuppgiftsansvarigas skyldigheter i brottsdatalagen av sådan karaktär att de bör tillämpas av Säkerhetspolisen. Ett flertal av skyldigheterna gäller redan i dag. Mot bakgrund av det anser utred-

ningen att merparten av bestämmelserna i 3 kap. brottsdatalagen bör ha sin motsvarighet i den nya lagen.

Vilka bestämmelser bör gälla för Säkerhetspolisen?

Bestämmelserna i 3 kap. 2–5 §§ brottsdatalagen som reglerar kraven på tekniska och organisatoriska åtgärder, t.ex. inbyggt dataskydd, dataskydd som standard och loggning, har ingen direkt motsvarighet i dag (se SOU 2017:29 s. 300 f.). Det bör dock i detta avseende ställas samma krav på Säkerhetspolisen som på övriga brottsbekämpande myndigheter. Det bör därför tas in bestämmelser med samma innehåll i den nya lagen.

Eftersom Säkerhetspolisen enligt polisdatalagen är skyldig att se till att tillgången till personuppgifter begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter bör en bestämmelse som motsvarar 3 kap. 6 § brottsdatalagen tas in i den nya lagen.

Säkerhetspolisen är i dag skyldig att i vissa situationer samråda med Datainspektionen och Säkerhets- och integritetsskyddsmyndigheten. Polismyndigheten har motsvarande samrådsskyldighet och Kustbevakningen ska i liknande situationer samråda med Datainspektionen. För Polismyndigheten och Kustbevakningen kommer samrådsskyldigheten att ersättas av regleringen i 3 kap. 7 § brottsdatalagen. För att uppnå enhetlighet för tillsynsmyndigheten bör enligt utredningens mening samrådsskyldigheten för Säkerhetspolisen formuleras på samma sätt som i brottsdatalagen. Eftersom samrådsskyldigheten i brottsdatalagen är knuten till skyldigheten att göra konsekvensbedömningar bör även en bestämmelse som föreskriver sådan skyldighet tas in i den nya lagen. Säkerhetspolisens skyldighet att samråda med tillsynsmyndigheten kommer härigenom att förändras något, men utredningen anser att kravet på konsekvensbedömning fyller en viktig funktion ur ett integritetsperspektiv. Utredningen återkommer till frågan om vilken tillsynsmyndighet som Säkerhetspolisen ska samråda med i avsnitt 15.4.2.

I 3 kap. 8 § brottsdatalagen regleras vilka skyddsåtgärder den personuppgiftsansvarige ska vidta. Regleringen motsvarar 31 § personuppgiftslagen och gäller således för Säkerhetspolisen i dag. I brottsdatalagen har skyldigheten dock preciserats genom att det

anges vad personuppgifterna särskilt ska skyddas mot. En bestämmelse med motsvarande innehåll bör tas in i den nya lagen.

Det är enligt utredningens mening rimligt att kräva att Säkerhetspolisen i samma utsträckning som andra brottsbekämpande myndigheter ska samarbeta med den myndighet som utövar tillsyn över myndighetens personuppgiftsbehandling. En bestämmelse motsvarande 3 kap. 12 § brottsdatalagen om skyldigheten att samarbeta med tillsynsmyndigheten bör därför tas in i den nya lagen.

Liksom i dag bör Säkerhetspolisen också vara skyldig att utse ett eller flera dataskyddsombud och anmäla det till tillsynsmyndigheten. Dataskyddsombud bör vara anställda vid myndigheten. En bestämmelse om skyldigheten att utse dataskyddsombud bör tas in i den nya lagen. Eftersom dataskyddsombudens arbetsuppgifter bör vara enhetliga bör också bestämmelser motsvarande 3 kap. 14 och 15 §§ brottsdatalagen tas in i den nya lagen. Säkerhetspolisens dataskyddsombud kommer därmed att få en något förändrad roll och några fler arbetsuppgifter (se SOU 2017:29 s. 344 f.)

Bestämmelserna om personuppgiftsbiträden och sådana biträdens skyldigheter i 3 kap. 17–20 §§ brottsdatalagen bör för Säkerhetspolisens del utformas på samma sätt. De motsvarar i allt väsentligt vad som redan gäller enligt personuppgiftslagen.

Skyldigheten att föra register över kategorier av behandlingar och skyldigheten att införa interna rutiner för anmälan av överträdelser bör enligt utredningens mening gälla även för Säkerhetspolisen. Det kan regleras i förordning (jfr SOU 2017:29 s. 319 f. och 323 f.). En förteckning över de behandlingar som utförs av myndigheten förs i dag av personuppgiftsombudet. Den nya ordningen innebär att skyldigheten i stället läggs på myndigheten i egenskap av personuppgiftsansvarig. Skyldigheten att införa interna rutiner för anmälan av överträdelser har ingen motsvarighet i dag.

Det kan finnas behov av att precisera och fylla ut de bestämmelser som reglerar Säkerhetspolisens skyldigheter som personuppgiftsansvarig (jfr SOU 2017:29 s. 364 f.). Det kan t.ex. röra sig om dokumentations- eller underrättelseskyldigheter eller bestämmelser som reglerar ett visst förfarande. För att undvika en alltför detaljerad lagreglering bör sådana bestämmelser tas in i förordning.

Ingen skyldighet att anmäla personuppgiftsincidenter

I 3 kap. 9–11 §§ brottsdatalagen regleras den personuppgiftsansvariges skyldigheter vid en personuppgiftsincident. Där föreskrivs bl.a. att sådana incidenter ska anmälas till tillsynsmyndigheten inom viss tid och att den registrerade i vissa fall ska underrättas om incidenten. Enligt 3 kap. 9 § första stycket gäller anmälningsskyldigheten inte om personuppgiftsincidenten rör nationell säkerhet.

It-incidenter ska som huvudregel anmälas till Myndigheten för samhällsskydd och beredskap. Det framgår av 20 § första stycket förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap. Det gäller dock inte sådana it-incidenter som enligt 10 a § säkerhetsskyddsförordningen (1996:633) ska rapporteras till Säkerhetspolisen eller Försvarsmakten. Exempel på sådana incidenter är incidenter i informationssystem där hemliga uppgifter som gäller Sveriges säkerhet behandlas eller i informationssystem som särskilt behöver skyddas mot terrorism. Behovet av att skydda sådan information anses vara så viktigt att endast den myndighet som utövar tillsyn över säkerhetsskyddet ska få ta del av den. Mot bakgrund av det, och då nationell säkerhet ligger utanför direktivets tillämpningsområde, har personuppgiftsincidenter som rör nationell säkerhet undantagits från anmälningsskyldigheten i brottsdatalagen (se SOU 2017:29 s. 331 f.).

Den nya lagen ska tillämpas vid behandling av personuppgifter som rör nationell säkerhet i Säkerhetspolisens brottsbekämpande och lagförande verksamhet. Personuppgiftsincidenter som inträffar i myndighetens informationssystem och som drabbar personuppgifter som behandlas med stöd av den nya lagen kommer alltid att röra nationell säkerhet och därmed, enligt brottsdatalagens reglering, vara undantagna från anmälningsskyldighet. Det finns därför inte skäl att i den nya lagen ta in bestämmelser som reglerar anmälan av personuppgiftsincidenter till tillsynsmyndigheten.

14.15 Enskildas rättigheter

Utredningens förslag: Det ska i den nya lagen tas in bestämmelser om Säkerhetspolisens skyldighet att

- lämna allmän information till registrerade,
- på begäran lämna besked om personuppgiftsbehandling, och
- på begäran rätta, radera eller begränsa behandlingen av personuppgifter.

Det ska också tas in bestämmelser som reglerar möjligheten att begränsa rätten till information och som anger när avgift får tas ut för informationen.

Föreskrifter som fyller ut och preciserar bestämmelserna om enskildas rättigheter ska tas in i förordning.

Skälen för utredningens förslag

Nuvarande reglering

I 23 och 25–27 §§ personuppgiftslagen, som genom hänvisningar i 2 kap. 2 § och 6 kap. 4 § polisdatalagen ska tillämpas av Säkerhetspolisen, regleras vilken information som ska lämnas till den registrerade och när informationsskyldigheten inte gäller. I 23 och 25 §§ regleras vad som gäller om uppgifterna har lämnats av den registrerade själv och vilken information som den personuppgiftsansvarige då ska lämna. För Säkerhetspolisen görs enligt 2 kap. 2 § tredje stycket polisdatalagen undantag från informationsskyldigheten i 23 § dels vid insamling av personuppgifter genom bilder eller ljud, dels om uppgifterna samlas in i samband med larm och det med hänsyn till omständigheterna inte finns tid att lämna informationen. I 26 § personuppgiftslagen föreskrivs att den personuppgiftsansvarige är skyldig att till var och en som ansöker om det en gång per kalenderår gratis lämna besked om personuppgifter som rör den sökande behandlas eller inte. Det anges också vilken information som i sådana fall ska lämnas. Av 27 § framgår att undantag från informationsskyldigheten gäller vid sekretess och tystnadsplikt.

I 28 § personuppgiftslagen regleras den personuppgiftsansvariges skyldighet att på begäran av den registrerade rätta, blockera eller utplåna sådana personuppgifter som inte har behandlats på det sätt som föreskrivs i lagen eller föreskrifter som har utfärdats med stöd av den. Bestämmelsen gäller genom nyss nämnda hänvisningar för Säkerhetspolisen.

Regleringen i brottsdatalagen

I 4 kap. 1–3 §§ brottsdatalagen regleras dels vilken allmän information som ska göras tillgänglig för registrerade, dels vilken personrelaterad information som ska lämnas till den registrerade om det behövs i specifika fall eller om den enskilde begär det.

I 4 kap. 5–7 §§ regleras begränsning av rätten till personrelaterad information. Informationen får bara begränsas för vissa i lagen angivna syften. Liksom i personuppgiftslagen föreskrivs att informationsskyldigheten inte omfattar personuppgifter i löpande text som inte fått sin slutliga utformning när begäran gjordes eller som utgör minnesanteckningar eller liknande. Om en begäran om information är orimlig eller uppenbart ogrundad får den personuppgiftsansvarige avslå den.

Rätten till rättelse, radering och begränsning av behandling regleras i 4 kap. 9 och 10 §§. Bestämmelserna motsvarar i princip 28 § personuppgiftslagen men är mer detaljerade och anger tydligare när rättelse, radering respektive begränsning ska vidtas.

I 4 kap. 12 § regleras förutsättningarna för att ta ut avgift för personrelaterad information.

Merparten av bestämmelserna bör tillämpas av Säkerhetspolisen

Bestämmelser som reglerar enskildas rättigheter fyller en mycket viktig funktion i dataskyddslagstiftningen. Enligt utredningens mening bör i princip samma krav ställas på Säkerhetspolisen som på andra myndigheter när det gäller enskildas rättigheter. På så sätt blir det lättare för den enskilde att ta tillvara sina rättigheter. Regleringen i brottsdatalagen skiljer sig inte i någon större utsträckning från vad som gäller enligt personuppgiftslagen. Enligt utredningens bedömning kan merparten av bestämmelserna i 4 kap. brottsdata-

gen utan problem tillämpas av Säkerhetspolisen. Mot den bakgrunden bör huvuddelen av bestämmelserna i brottsdatalagen som reglerar enskildas rättigheter ha sin motsvarighet i den nya lagen.

Vilka bestämmelser bör gälla för Säkerhetspolisen?

Det bör finnas en bestämmelse som reglerar Säkerhetspolisens skyldighet att självant göra allmän information om myndighetens personuppgiftsbehandling tillgänglig. Det bör också finnas en bestämmelse som föreskriver att Säkerhetspolisen ska lämna skriftligt besked till den som begär det om personuppgifter som rör honom eller henne behandlas, s.k. registerutdrag. Bestämmelserna bör formuleras på samma sätt som motsvarande bestämmelser i brottsdatalagen. En närmare genomgång av vilken information det är fråga om finns i delbetänkandet (se SOU 2017:29 s. 377 f. och 381 f.). Brottsdatalagen föreskriver att behöriga myndigheter ska informera om möjligheten att lämna in klagomål till tillsynsmyndigheten och kontaktuppgifter till den, eftersom direktivet kräver det och har en särskild reglering för handläggningen av klagomål. Utredningen föreslår ingen motsvarighet till den regleringen i den nya lagen. Säkerhetspolisens informationsskyldighet bör därför inte omfatta sådana uppgifter.

Sådan allmän information som ska göras tillgänglig får enligt brottsdatalagen inte begränsas med hänsyn till sekretess utan ska alltid finnas tillgänglig för de registrerade. Det rör sig om så allmän information att det enligt utredningens mening inte bör utgöra något problem för Säkerhetspolisen att leva upp till kraven. Regleringen i den nya lagen bör mot den bakgrunden utformas på samma sätt som i brottsdatalagen.

Eftersom hantering av frågor som rör nationell säkerhet är av mycket känslig natur bör det inte ställas krav på att Säkerhetspolisen självant ska lämna ut information i andra situationer än de tidigare nämnda. Någon bestämmelse motsvarande 4 kap. 2 § brottsdatalagen bör därför inte tas in i den nya lagen. Eftersom det inte förekommer automatiserade beslut i Säkerhetspolisens verksamhet behöver inte heller information om sådana beslut regleras.

Säkerhetspolisens möjlighet att begränsa rätten till information bör också regleras i den nya lagen. Till skillnad från vad som gäller

enligt brottsdatalagen bör sådan begränsning dock inte enbart få göras med hänsyn till vissa angivna intressen. Det kravet ställs upp i direktivet men bör inte gälla för Säkerhetspolisen. Regleringen bör i stället utformas med 27 § personuppgiftslagen som mönster. Bestämmelserna om begränsning av rätten till information bör i övrigt formuleras på samma sätt som i 4 kap. brottsdatalagen.

Bestämmelser som reglerar den enskildes rätt till rättelse, radering och begränsning av behandling bör också finnas i den nya lagen. De bör formuleras på samma sätt som 4 kap. 9–11 §§ brottsdatalagen. Regleringen kommer således, liksom för övriga brottsbekämpande myndigheter, att bli mer preciserad än i dag. Innebörden är dock i stort sett densamma. Säkerhetspolisen bör också få avgöra vilken åtgärd som ska vidtas med anledning av en begäran om rättelse, radering eller begränsning av behandlingen.

På samma sätt som för övriga myndigheter bör den information som Säkerhetspolisen lämnar som huvudregel vara kostnadsfri. En bestämmelse som anger det bör tas in i den nya lagen. Den bör formuleras på samma sätt som 4 kap. 12 § brottsdatalagen. Säkerhetspolisen ges då möjlighet att ta ut avgift för personrelaterad information om sådan begärs oftare än en gång per år.

Det kan finnas behov av att på olika sätt kunna precisera och fylla ut bestämmelserna om enskildas rättigheter. Sådana bestämmelser bör tas in i förordning.

14.16 Sanktioner, skadestånd och rättsmedel

14.16.1 Ingen straffbestämmelse i den nya lagen

Utredningens bedömning: Överträdelse av bestämmelserna om personuppgiftsbehandling bör inte vara straffsanktionerade, utöver vad som gäller enligt brottsbalken.

Skälen för utredningens bedömning: Bestämmelsen om straffansvar i 49 § personuppgiftslagen gäller inte för Säkerhetspolisen. Skälet till det är enligt förarbetena att det i brottsbalken föreskrivs straffrättsligt ansvar för otillåten hantering av personuppgifter, t.ex. tjänstefel enligt 20 kap. 1 § brottsbalken och dataintrång enligt 4 kap. 9 c § brottsbalken. Därför ansågs det inte vara aktuellt att

tillämpa straffbestämmelsen i personuppgiftslagen mot någon anställd inom polisen (se prop. 2009/10:85 s. 91).

Någon straffbestämmelse föreslås inte heller i brottsdatalagen. Som framgår av delbetänkandet anser utredningen att en kriminalisering motsvarande 49 § personuppgiftslagen inte skulle vara en tillräckligt effektiv sanktion, eftersom den i huvudsak skulle träffa andra än personuppgiftsansvariga och personuppgiftsbiträden (se SOU 2017:29 s. 495 f.).

De skäl mot en straffbestämmelse som framförs i förarbetena till polisdatalagen och i delbetänkandet gör sig gällande även för Säkerhetspolisens behandling av personuppgifter enligt polisdatalagen inte är straffsanktionerad och någon straffbestämmelse inte heller föreslås i brottsdatalagen bör någon sådan bestämmelse inte tas in i den nya lagen.

14.16.2 Sanktionsavgift bör inte få tas ut

Utredningens bedömning: Det bör inte tas in bestämmelser om sanktionsavgift i den nya lagen.

Skälen för utredningens bedömning

Dagens sanktionssystem

Vid sidan om reglerna om straffansvar i 49 § personuppgiftslagen finns det i 44 och 45 §§ bestämmelser som ger tillsynsmyndigheten rätt att vid vite förbjuda behandling på annat sätt än genom lagring. Vidare får tillsynsmyndigheten enligt 47 § hos domstol ansöka om att personuppgifter som behandlats på olagligt sätt ska utplånas. Regleringen i 44, 45 och 47 §§ gäller för Säkerhetspolisens behandling genom hänvisning i 2 kap. 2 § och 6 kap. 4 § polisdatalagen. Av 2 kap. 2 § fjärde stycket polisdatalagen framgår emellertid att förbud enligt 44 eller 45 § personuppgiftslagen inte får förenas med vite. I förarbetena motiveras undantaget med att vite inte bör användas mellan statliga myndigheter (se prop. 2009/10:85 s. 90).

Ett nytt sanktionssystem i brottsdatalagen

Enligt dataskyddsdirektivet ska medlemsstaterna föreskriva sanktioner för överträdelse av de bestämmelser som genomför direktivet. Sanktionerna ska vara effektiva, proportionerliga och avskräckande. Utredningen föreslår att det i brottsdatalagen införs en ny administrativ sanktion – sanktionsavgift. Som framgår av delbetänkandet ska sanktionsavgift kunna tas ut av personuppgiftsansvariga och personuppgiftsbiträden vid överträdelse av vissa bestämmelser i brottsdatalagen (se SOU 2017:29 s. 496 f.). Enligt 6 kap. 6 § brottsdatalagen ska tillsynsmyndigheten fatta beslut om sanktionsavgift (se SOU 2017:29 s. 520 f.). I avsnitt 5.4.2 föreslår utredningen att sanktionsavgift ska kunna tas ut av den personuppgiftsansvarige även vid överträdelse av vissa bestämmelser i registerförfattningarna.

Sanktionsavgift bör inte kunna tas ut av Säkerhetspolisen

Frågan är om det bör införas ett sanktionssystem som motsvarar det i brottsdatalagen för Säkerhetspolisen. Säkerhetspolisen ska tillämpa brottsdatalagen och polisens brottsdatalag i vissa fall (se avsnitt 7.2.1. Myndigheten kommer då att omfattas av sanktionssystemet i de lagarna. Även dataskyddsförordningen föreskriver att administrativa sanktionsavgifter ska kunna tas ut vid överträdelse av bestämmelser om personuppgiftsbehandling. Det bör därför övervägas om sanktionsavgift bör kunna tas ut vid överträdelse av bestämmelser i den nya lagen.

Huvudskälet till att utredningen föreslår att sanktionsavgift ska kunna tas ut av behöriga myndigheter är att motsvarande sanktionssystem gäller enligt dataskyddsförordningen. Eftersom de behöriga myndigheterna kommer att tillämpa båda regelverken finns det fördelar med en enhetlig reglering. För flera av myndigheterna kommer sannolikt en större del av personuppgiftsbehandlingen att regleras av dataskyddsförordningen. Det gäller Skatteverket, Tullverket och domstolarna. Även Polismyndigheten kommer i betydande utsträckning att tillämpa dataskyddsförordningen. Det är då svårt att motivera att helt olika sanktionssystem ska gälla beroende på om brottsdatalagen eller förordningen är tillämplig vid överträ-

delsor som är likartade och som därför kan antas motivera samma sanktion (se SOU 2017:29 s. 492).

Säkerhetspolisen kommer att tillämpa dataskyddsförordningen i en begränsad del av verksamheten som är av intern och administrativ karaktär. Det är också bara i speciella fall som myndigheten kommer att tillämpa brottsdatalagen och polisens brottsdatalag. Skälen för ett enhetligt sanktionssystem gör sig därför inte gällande på samma sätt i Säkerhetspolisens verksamhet. Eftersom Säkerhetspolisens verksamhet som rör nationell säkerhet inte omfattas av vare sig dataskyddsdirektivets eller dataskyddsförordningens tillämpningsområde är lagstiftaren inte heller bunden av de krav på sanktioner som ställs i dessa rättsakter.

Dataskyddskonventionen, som även omfattar personuppgiftsbehandling som rör nationell säkerhet, ställer krav på att det ska finnas lämpliga sanktioner för överträdelser av bestämmelser om dataskydd. I konventionen anges dock inte vilka krav som ställs på sådana sanktioner. Konventionens krav på sanktioner är därmed enligt utredningens bedömning inte lika långtgående som dataskyddsdirektivets och dataskyddsförordningens krav. Den nuvarande regleringen ger möjlighet till ersättning genom skadestånd. Vidare kan straffrättsligt ansvar utkrävas enligt brottsbalken. Det har ansetts att rätten till skadestånd tillsammans med tillsynsmyndighetens befogenheter uppfyller kraven i konventionen på lämpliga sanktioner. Utredningen har ingen annan uppfattning.

I avsnitt 14.16.3 föreslår utredningen att Säkerhetspolisen ska kunna åläggas skadestånd vid felaktig personuppgiftsbehandling. I kapitel 15 diskuterar utredningen hur tillsynen över Säkerhetspolisens personuppgiftsbehandling bör utövas och vilka befogenheter tillsynsmyndigheten bör ha. Sanktionssystemet i den nya lagen kommer att motsvara det som gäller i dag.

Enligt utredningens mening är de sanktionsmöjligheter som finns i dag tillräckliga. Med beaktande av det, och då skälen för ett enhetligt sanktionssystem inte har samma styrka när det gäller behandling av personuppgifter som rör nationell säkerhet, anser utredningen att det inte bör införas någon möjlighet att ta ut sanktionsavgift vid överträdelse av bestämmelser i den nya lagen.

14.16.3 Skadestånd

Utredningens förslag: Säkerhetspolisen ska ersätta den registrerade för den skada och kränkning av den personliga integriteten som behandling av personuppgifter i strid med den nya lagen, eller föreskrifter som har meddelats i anslutning till den, har orsakat.

Skälen för utredningens förslag: Enligt 48 § personuppgiftslagen ska den personuppgiftsansvarige ersätta den registrerade för skada och kränkning av den personliga integriteten som behandling av personuppgifter i strid med lagen har orsakat. Ersättningsskyldigheten kan jämkas om den personuppgiftsansvarige visar att felet inte berodde på honom eller henne. I polisdatalagen hänvisas till 48 § personuppgiftslagen. Säkerhetspolisens skadeståndsansvar omfattar därmed överträdelser av de bestämmelser i polisdatalagen och personuppgiftslagen som gäller för myndigheten.

I 7 kap. 1 § brottsdatalagen finns en bestämmelse som motsvarar 48 § första stycket personuppgiftslagen. Eftersom det inte finns någon exculperingsbestämmelse i direktivet har utredningen dock inte ansett det möjligt att öppna möjlighet till jämkning i brottsdatalagen (se SOU 2017:29 s. 535 f.).

Det bör i den nya lagen finnas en bestämmelse som reglerar Säkerhetspolisens skadeståndsansvar. Den bör formuleras på samma sätt som i brottsdatalagen. Bestämmelsen skulle kunna föreskriva att skadeståndsersättning får jämkas, eftersom regleringen inte behöver följa direktivets bestämmelser. Det underlättar emellertid både för tillämparen och för den enskilde om regleringen i den delen stämmer överens med övriga registerförfattningar på området. Intresset av en enhetlig personuppgiftsreglering väger enligt utredningen tyngre än Säkerhetspolisens behov av att kunna få jämkning av eventuella skadeståndsanspråk. Den nya lagen bör därför inte innehålla någon jämkningsbestämmelse.

Av de skäl som anges i avsnitt 5.4.3 bör Justitiekanslern pröva frågor om skadeståndsskyldighet för staten för felaktig personuppgiftsbehandling vid tillämpning av den nya lagen. Ett tillägg som klargör det bör göras i 3 § förordningen om handläggning av skadeståndsanspråk mot staten.

14.16.4 Överklagande

Utredningens förslag: Beslut i fråga om rättelse, komplettering, radering eller begränsning av behandlingen som har meddelats på begäran av den registrerade, ska kunna överklagas till allmän förvaltningsdomstol. Detsamma gäller beslut att inte lämna information på begäran av en registrerad eller att ta ut avgift för att lämna sådan information. Vid överklagande till kammarrätten ska det krävas prövningstillstånd.

Några andra beslut än de som uttryckligen anges i lagen ska inte få överklagas.

Skälen för utredningens förslag: I 52 § första stycket personuppgiftslagen, som polisdatalagen hänvisar till, anges att vissa beslut som fattas av den personuppgiftsansvarige får överklagas till allmän förvaltningsdomstol. Det gäller beslut om information enligt 26 §, om rättelse och underrättelse till tredje man enligt 28 §, om information enligt 29 § andra stycket och om upplysningar enligt 42 §. Av 53 § framgår att andra beslut som en personuppgiftsansvarig myndighet fattat enligt lagen inte får överklagas och att prövningstillstånd krävs vid överklagande till kammarrätten.

I 7 kap. 2 § brottsdatalagen föreskrivs att beslut som har meddelats på begäran av den registrerade i fråga om rättelse, komplettering, radering eller begränsning av behandlingen får överklagas till allmän förvaltningsdomstol. Detsamma gäller beslut att inte lämna information på begäran av en registrerad, att ta ut avgift för att lämna sådan information eller att inte medge omprövning av ett automatiserat beslut. Vid överklagande till kammarrätten krävs det prövningstillstånd. Av 7 kap. 5 § framgår att andra beslut inte får överklagas. Bestämmelserna i brottsdatalagen om överklagande av en personuppgiftsansvarig myndighets beslut har således i princip samma innehåll som överklagandebestämmelserna i personuppgiftslagen.

Bestämmelser om överklagande som motsvarar dem i brottsdatalagen bör tas in i den nya lagen. Eftersom det inte förekommer några automatiserade beslut i Säkerhetspolisens verksamhet behövs dock inte någon bestämmelse om överklagande av sådana beslut. På samma sätt som i brottsdatalagen bör det i lagen anges att några andra beslut än de som räknas upp inte ska få överklagas.

Överklagande av tillsynsmyndighetens beslut behandlas i avsnitt 15.6.2.

14.17 Överföring av personuppgifter till tredjeland och internationella organisationer

14.17.1 Utgångspunkter

Utredningens bedömning: Överföring av personuppgifter till tredjeland och internationella organisationer bör regleras i den nya lagen. Regleringen bör i huvudsak motsvara den som finns i brottsdatalagen.

Utredningens förslag: Tredjeland ska definieras som en stat som inte är medlem i Europeiska unionen eller Europeiska ekonomiska samarbetsområdet och som inte heller på grund av avtal med Europeiska unionen har en motsvarande ställning.

Skälen för utredningens bedömning och förslag

Nuvarande reglering

I 33–35 §§ personuppgiftslagen finns det bestämmelser om överföring av personuppgifter till tredjeland. De gäller genom hänvisningar i 2 kap. 2 § och 6 kap. 4 § polisdatalagen för Säkerhetspolisen. Enligt 33 § personuppgiftslagen är det förbjudet att till tredjeland föra över personuppgifter som är under behandling, om landet inte har en adekvat skyddsnivå för personuppgifter. Förbudet gäller även överföring av personuppgifter för behandling där. Trots avsaknad av adekvat skyddsnivå är, enligt 34 § personuppgiftslagen, överföring av personuppgifter till tredjeland tillåten om den enskilde har lämnat sitt samtycke till överföringen eller om överföringen är nödvändig i vissa särskilt uppräknade fall. Paragrafen reglerar således vissa undantag från överföringsförbudet i 33 §. Ett viktigt undantag är att personuppgifter får överföras för användning enbart i en stat som har anslutit sig till dataskyddskonventionen. Enligt 35 § personuppgiftslagen kan regeringen föreskriva ytterligare undantag från förbudet, bl.a. om det behövs med

hänsyn till ett viktigt allmänt intresse. Sådana föreskrifter finns i 12–14 §§ personuppgiftsförordningen (1998:1191).

Regleringen i brottsdatalagen

Överföring av personuppgifter till tredjeland och internationella organisationer regleras i 8 kap. brottsdatalagen. Av 8 kap. 1 § framgår att personuppgifter får överföras till ett tredjeland eller en internationell organisation om överföringen är nödvändig för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet. Överföringen ska riktas till en behörig myndighet i ett tredjeland eller till en internationell organisation som är en behörig myndighet. Personuppgifter får dessutom överföras endast om Europeiska kommissionen (i fortsättningen kommissionen) har antagit beslut om adekvat skyddsnivå, om personuppgifterna omfattas av tillräckliga skyddsåtgärder hos adressaten eller om ett undantag för särskilda situationer är tillämpligt. I 8 kap. 2 § föreskrivs att personuppgifter som en svensk myndighet har fått från en annan medlemsstat får överföras till ett tredjeland eller en internationell organisation endast om den medlemsstat som lämnat uppgifterna till en svensk myndighet har medgett att de överförs.

I 8 kap. 3–5 §§ brottsdatalagen regleras de tillåtna grunderna för överföring närmare. Det finns också bestämmelser om vidareöverföring (6 och 7 §§), om överföring till andra än behöriga myndigheter (8 §) och om användningsbegränsningar (9 och 10 §§).

Överföring av personuppgifter till tredjeland och internationella organisationer ska regleras

Informationsutbyte är en central del av Säkerhetspolisens samarbete med andra stater. Samarbetet berör stater både inom och utanför EU. På samma sätt som på många andra områden är samarbetet med övriga nordiska länder särskilt nära. Eftersom Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet inte omfattas av EU-rätten, behöver regleringen om överföring av personuppgifter till andra länder inte göra skillnad mellan överföring

till medlemsstater i EU och tredjeland. I förarbetena till polisdatalagen ansågs emellertid att bestämmelserna om överföring av personuppgifter till tredjeland borde gälla även för Säkerhetspolisen (se prop. 2009/10:85 s. 88 och 252 f.). Den nuvarande regleringen, som är väl inarbetad, är därmed uppbyggd på det sättet.

En reglering som innebär högre krav för överföringar till stater som inte är medlemmar i EU eller anslutna till EES-samarbetet är viktig ur integritetssynpunkt, eftersom det inte kan garanteras samma skydd för personuppgifterna i sådana stater. I 8 kap. brottsdatalagen ställs det högre krav när personuppgifter ska överföras till tredjeland och internationella organisationer. Enligt utredningens mening bör i huvudsak samma krav gälla för Säkerhetspolisen. Det finns därför inte skäl att nu välja en annan lösning beträffande överföring av personuppgifter till tredjeland och internationella organisationer. Villkoren för sådana överföringar bör således regleras i den nya lagen.

Utgångspunkten bör vara att Säkerhetspolisen ska kunna överföra personuppgifter till tredjeland och internationella organisationer i samma utsträckning som i dag. Bestämmelserna i brottsdatalagen bör tas som utgångspunkt. Regleringen av överföringar till tredjeland och internationella organisationer kommer därmed att bli betydligt utförligare men ger samtidigt större möjligheter att överföra personuppgifter till sådana mottagare än i dag.

Regleringen för Säkerhetspolisen bör dock anpassas till att det internationella samarbetet mellan underrättelse- och säkerhetstjänster har en annan prägel än det allt närmare samarbetet mellan brottsbekämpande myndigheter inom EU. Mot den bakgrunden bör lagtexten inte byggas med utgångspunkt i uttrycket medlemsstat utan stat.

Definitionen av vad som är tredjeland bör i sak vara densamma som i brottsdatalagen men formuleras annorlunda. Med tredjeland bör avses en stat som inte är medlem i EU eller EES eller som på grund av avtal har motsvarande ställning. Definitionen innebär att EU:s medlemsstater, Island, Norge, Liechtenstein och Schweiz inte är tredjeland i lagens mening.

14.17.2 Grundläggande förutsättningar för överföring

Utredningens förslag: Säkerhetspolisen ska få överföra personuppgifter som behandlas till ett tredjeland eller en internationell organisation om överföringen riktas till en brottsbekämpande myndighet, en underrättelse- eller säkerhetstjänst eller en internationell organisation med brottsbekämpande uppdrag. Personuppgifterna ska dock endast få överföras om kommissionen har antagit ett beslut om adekvat skyddsnivå, om personuppgifterna annars omfattas av tillräckliga skyddsåtgärder eller om ett undantag för särskilda situationer är tillämpligt.

Regleringen ska gälla även vid överföring av personuppgifter för behandling i ett tredjeland eller av en internationell organisation.

Personuppgifter som Säkerhetspolisen har fått från en annan stat ska få överföras till ett tredjeland eller en internationell organisation endast om den stat som lämnat uppgifterna till Säkerhetspolisen har medgett att de överförs.

Skälen för utredningens förslag

De grundläggande förutsättningarna för överföring ska anges

Utgångspunkten i den nya lagen bör, liksom i brottsdatalagen, vara att Säkerhetspolisen ska få överföra personuppgifter till ett tredjeland eller en internationell organisation om vissa villkor är uppfyllda. En bestämmelse som anger de grundläggande förutsättningarna för överföring bör tas in i den nya lagen.

Enligt direktivet får personuppgifter överföras endast om det är nödvändigt för vissa angivna ändamål och överföringen görs till någon som är behörig myndighet. Bestämmelsen i brottsdatalagen har utformats med det som utgångspunkt. I personuppgiftslagen ställs inte några sådana krav. Det går inte heller att knyta Säkerhetspolisens reglering till behöriga myndigheter, eftersom nationell säkerhet undantagits från direktivets tillämpningsområde. Regleringen i den nya lagen bör utformas med brottsdatalagen som mönster, men vissa frågor kräver en annan lösning.

Säkerhetspolisen har i motsats till andra brottsbekämpande myndigheter inte några internationella åtaganden som tvingar myn-

digheten att lämna viss information. Säkerhetspolisen råder därmed i större utsträckning över vilken information som lämnas, på vilket sätt det görs och vilka villkor som ställs för den andra statens användning av informationen. Uppgiftsutbyte sker huvudsakligen inom ramen för överenskommelser och bygger på ömsesidigt förtroende. Mot den bakgrunden bör någon motsvarighet till kravet i brottsdatalagen på att överföringen ska vara nödvändig för vissa angivna ändamål inte finnas.

Frågan är om regleringen, på samma sätt som i brottsdatalagen, bör ta sikte på överföring till vissa mottagare. En sådan reglering ger större förutsebarhet och bättre integritetsskydd och bör därför väljas framför en mer generell reglering. I den grundläggande bestämmelsen bör det därför anges att överföringen ska riktas till en brottsbekämpande myndighet eller en underrättelse- eller säkerhetstjänst i tredjeland eller till en internationell organisation med brottsbekämpande uppdrag. Det tillgodoser enligt utredningens mening Säkerhetspolisens behov av att kunna överföra personuppgifter i syfte att bistå myndigheter i andra stater. Säkerhetspolisens möjlighet att i vissa fall överföra personuppgifter till andra aktörer behandlas i avsnitt 14.17.4.

Liksom i brottsdatalagen bör det ställas krav på att viss skyddsnivå ska vara säkerställd. Personuppgifterna bör endast få överföras om det finns beslut om adekvat skyddsnivå, om personuppgifterna omfattas av tillräckliga skyddsåtgärder hos adressaten eller om ett undantag för särskilda situationer är tillämpligt. Syftet med regleringen är att den skyddsnivå som säkerställs genom dataskyddsdirektivet och som gäller inom EU som utgångspunkt ska gälla även när personuppgifter överförs till ett tredjeland eller en internationell organisation (se SOU 2017:29 s. 585 f.). Enligt utredningens mening är det rimligt att samma krav ställs på Säkerhetspolisen även om myndighetens verksamhet inte omfattas av direktivets tillämpningsområde. Liknande krav på skydd ställs i dag i personuppgiftslagen och personuppgiftsförordningen.

Överföring av uppgifter från andra stater ska vara medgiven

I 8 kap. 2 § brottsdatalagen föreskrivs att en överföring av personuppgifter som härrör från en annan medlemsstat ska vara medgiven. Något sådant krav gäller inte för Säkerhetspolisen i dag.

För att skydda underrättelseinformation tillämpar Säkerhetspolisen en s.k. tredjepartsregel i det internationella samarbetet med utländska underrättelse- och säkerhetstjänster. Den innebär att uppgifter som myndigheten har fått från en utländsk samarbetspartner inte får föras vidare utan uttryckligt samtycke. Regeln är central i Säkerhetspolisens verksamhet och utgör grunden för ett effektivt underrättelseutbyte. Den har tillkommit i syfte att skapa förtroende mellan underrättelse- och säkerhetstjänsterna, eftersom det finns ett stort behov av att skydda uppgifter om bl.a. källor och arbetsmetoder. Principen att uppgifter som kommer från en annan stat inte får föras vidare till ett tredjeland eller en internationell organisation utan medgivande tillämpas således redan i dag. Eftersom det i brottsdatalagen ställs krav på medgivande vid överföring till tredjeland och internationella organisationer bör det enligt utredningens mening införas en sådan bestämmelse i den nya lagen. Den bör återspegla den tredjepartsregel som redan tillämpas och omfatta information från alla stater och oberoende vilken myndighet som lämnat informationen. Den bör således ha ett vidare tillämpningsområde än motsvarande bestämmelse i brottsdatalagen.

Eftersom Säkerhetspolisen aldrig lämnar ut uppgifter som myndigheten fått från en annan medlemsstat utan medgivande från den staten bör något undantag från kravet på medgivande av det slag som finns i 8 kap. 2 § andra stycket brottsdatalagen inte tas in i den nya lagen.

14.17.3 Tillåtna grunder för överföring

Utredningens förslag: Det ska finnas bestämmelser om tillåtna grunder för överföring i den nya lagen. I första hand ska det krävas beslut om adekvat skyddsnivå och i andra hand tillräckliga skyddsåtgärder. Först i tredje hand ska personuppgifter få överföras i särskilda situationer.

Skälen för utredningens förslag

Viss skyddsnivå ska vara säkerställd

Som framgår av avsnitt 14.17.2 bör personuppgifter få överföras till tredjeland och internationella organisationer endast om en viss nivå på skyddet för personuppgifter kan säkerställas. Det innebär att överföringen bör omfattas av i första hand ett beslut om adekvat skyddsnivå, i andra hand tillräckliga skyddsåtgärder och i tredje hand ett undantag för särskilda situationer. Bestämmelser om dessa villkor bör tas in i den nya lagen och utformas på i huvudsak samma sätt som i brottsdatalagen.

Det kan anmärkas att Säkerhetspolisen naturligtvis aldrig är skyldig att överföra personuppgifter till ett tredjeland eller en internationell organisation.

Beslut om adekvat skyddsnivå

Personuppgifter bör som huvudregel få överföras om det tredjelandet eller den internationella organisationen omfattas av beslut från kommissionen om att landet eller organisationen har adekvat skyddsnivå (se SOU 2017:29 s. 589 f.). Det motsvarar vad som gäller i dag enligt 13 § första stycket 1 personuppgiftsförordningen. Även om Säkerhetspolisens verksamhet som rör nationell säkerhet inte omfattas av unionsrätten bör kommissionens beslut om adekvat skyddsnivå vara vägledande för myndigheten. Finns det inget beslut om adekvat skyddsnivå får Säkerhetspolisen i stället pröva om det finns tillräckliga skyddsåtgärder eller om det är fråga om en sådan undantagssituation som anges i lagen.

Tillräckliga skyddsåtgärder

Om det inte finns ett beslut om adekvat skyddsnivå, bör personuppgifter ändå få överföras till ett tredjeland eller en internationell organisation om skyddsåtgärder för personuppgifter har fastställts i ett avtal som ger tillräckliga garantier till skydd för registrerades rättigheter, eller om den myndighet eller organisation som uppgifterna ska överföras till på annat sätt garanterar tillräckligt skydd för dem (jfr SOU 2017:29 s. 591 f.).

Tillräckliga skyddsåtgärder fastställs främst genom att den mottagande myndigheten eller organisationen garanterar tillräckligt skydd för uppgifterna. Informationsutbyte mellan underrättelse- och säkerhetstjänster bygger i stor utsträckning på förtroende. Om en underrättelse- eller säkerhetstjänst missbrukar förtroendet blir konsekvensen att den inte längre kommer att få del av relevant information i samma utsträckning som andra. Det har en självreglerande effekt genom att den mottagande underrättelse- och säkerhetstjänsten måste garantera tillräckligt skydd för uppgifterna för att kunna få del av dem.

Överföring i särskilda situationer

I enskilda fall kan det, trots bristen på skydd för personuppgifter, vara angeläget att kunna föra över vissa personuppgifter till ett tredjeland eller en internationell organisation. Så kan t.ex. vara fallet om Säkerhetspolisen har information om att en misstänkt terrorist befinner sig här i landet men personen identifieras först när han eller hon har rest till ett tredjeland och kan antas komma att begå allvarliga brott där. Säkerhetspolisen har även i vissa fall behov av att kunna utbyta information med underrättelse- och säkerhetstjänster i tredjeländer som har svårt att garantera tillräckligt skydd för personuppgifterna. Det kan gälla vissa särskilda ärenden, situationer eller tidsperioder.

Om det varken finns beslut om adekvat skyddsnivå eller tillräckliga skyddsåtgärder garanteras bör personuppgifter få överföras till ett tredjeland eller en internationell organisation endast om överföringen är nödvändig i vissa särskilda undantagssituationer. Samma undantagssituationer som i brottsdatalagen bör gälla för Säkerhetspolisen. Utredningen redogör närmare för undantagssituationerna i delbetänkandet (se SOU 2017:29 s. 595 f.). När det gäller undantag för myndigheters intresse i enskilda fall bör bestämmelsen anpassas till Säkerhetspolisens verksamhet. Överföringen bör vara nödvändig för att i ett enskilt fall kunna förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott.

Det bör, på samma sätt som i brottsdatalagen, ställas krav på en intresseavvägning. Personuppgifter bör inte få överföras till ett

tredjeland eller en internationell organisation om den registrerades intresse av skydd mot kränkning av grundläggande fri- och rättigheter väger tyngre än det allmännas intresse av att överföringen görs i det enskilda fallet för ett myndighetsintresse eller för att kunna fastslå, göra gällande eller försvara ett rättsligt anspråk.

14.17.4 Överföring till andra mottagare

Utredningens förslag: Säkerhetspolisen ska i ett enskilt fall få överföra personuppgifter till andra mottagare i ett tredjeland än brottsbekämpande myndigheter och underrättelse- och säkerhetstjänster. En sådan överföring ska få göras endast om det är absolut nödvändigt för att Säkerhetspolisen ska kunna utföra vissa arbetsuppgifter och det skulle vara ineffektivt eller olämpligt att överföra personuppgifterna till en brottsbekämpande myndighet eller en underrättelse- eller säkerhetstjänst i det tredjelandet.

Sådana överföringar ska inte få göras om den registrerades intresse av skydd mot kränkning av grundläggande fri- och rättigheter väger tyngre än det allmännas intresse av att överföringen görs.

Skälen för utredningens förslag: Regleringen i personuppgiftslagen gör ingen skillnad mellan myndigheter och andra mottagare när det gäller överföringar till tredjeland. Säkerhetspolisen kan således enligt den nuvarande regleringen överföra personuppgifter både till myndigheter, andra aktörer och enskilda i tredjeländer om villkoren i övrigt är uppfyllda.

I delbetänkandet redogör utredningen för övriga myndigheters behov av att kunna överföra personuppgifter till andra än behöriga myndigheter i tredjeland (se SOU 2017:29 s. 613 f.). I 8 kap. 8 § brottsdatalagen regleras överföringar till andra än behöriga myndigheter i tredjeland. Sådana överföringar får göras om vissa villkor är uppfyllda. Säkerhetspolisen har samma behov som övriga brottsbekämpande myndigheter att i vissa fall kunna överföra personuppgifter till andra mottagare än brottsbekämpande myndigheter eller underrättelse- eller säkerhetstjänster i ett tredjeland. En liknande bestämmelse bör därför tas in i den nya lagen.

Enligt 8 kap. 8 § brottsdatalagen ska den svenska myndigheten informera den som tar emot personuppgifter om de specifika ändamål för vilka uppgifterna får behandlas. Ytterligare informations-skyldighet föreskrivs i 7 kap. 2 § brottsdataförordningen. Skyldigheterna har sin grund i direktivet och har ingen motsvarighet i dag. Frågan är om de bör gälla för Säkerhetspolisen.

Det finns situationer där det inte är lämpligt att Säkerhetspolisen avslöjar att det är myndigheten som överför viss information. Så kan exempelvis vara fallet när Säkerhetspolisen gör sökningar i vissa utländska databaser som innehåller uppgifter om t.ex. fastigheter eller bolag eller använder liknande tjänster. Sådana sökningar innebär en överföring av personuppgifter till den aktör som ansvarar för databasen eller tjänsten. Säkerhetspolisen kan då i vissa fall behöva dölja att det är myndigheten som gör sökningen. Syftet med informationsskyldigheten är att kunna begränsa den fortsatta användningen av personuppgifterna. Det kan emellertid göras på andra sätt, som inte riskerar att äventyra verksamheten. Något krav på att Säkerhetspolisen alltid ska informera den som tar emot uppgifterna om för vilka ändamål uppgifterna får behandlas eller informera behörig myndighet på det sätt som anges i 7 kap. 2 § brottsdataförordningen bör därför inte införas.

Säkerhetspolisen bör alltså i ett enskilt fall få överföra personuppgifter till en mottagare som inte är en brottsbekämpande myndighet eller en underrättelse- eller säkerhetstjänst i ett tredjeland om överföringen är absolut nödvändig för att Säkerhetspolisen ska kunna utföra vissa arbetsuppgifter inom lagens tillämpningsområde och det skulle vara ineffektivt eller olämpligt att överföra personuppgifterna till en brottsbekämpande myndighet eller en underrättelse- eller säkerhetstjänst i det tredjelandet. Utredningen redogör närmare för innebörden av dessa villkor i delbetänkandet (se SOU 2017:29 s. 611 f.).

På samma sätt som i brottsdatalagen bör det föreskrivas att en intresseavvägning ska göras vid överföringar av detta slag.

14.17.5 Villkor för användningen av personuppgifter

Utredningens förslag: Säkerhetspolisen ska kunna ställa villkor för användningen av personuppgifter.

Skälen för utredningens förslag

Villkor som ställs upp av utländska myndigheter eller organ

I 8 kap. 9 § brottsdatalagen föreskrivs att en svensk behörig myndighet som har fått personuppgifter från en annan stat ska följa de villkor för användningen av personuppgifterna som ställs upp i en överenskommelse som har träffats med den som har lämnat uppgifterna (se SOU 2017:29 s. 618 f.). Som tidigare nämnts är sådana villkor viktiga i Säkerhetspolisens internationella samarbete. En motsvarande bestämmelse bör därför tas in i den nya lagen. Villkor av det slaget ska följas oavsett vad som annars gäller.

Villkor när Säkerhetspolisen överför personuppgifter

Som utredningen konstaterar i delbetänkandet finns det, när en svensk myndighet överför personuppgifter till ett tredjeland eller en internationell organisation, ibland skäl att ställa villkor som begränsar användningen av uppgifterna, t.ex. för vilket ändamål och hur länge de får behandlas. Att personuppgifterna förses med villkor för användningen kan vara en förutsättning för att det ska anses vara lämpligt att överföra dem (se SOU 2017:29 s. 619).

I flera lagar på det brottsbekämpande området finns det bestämmelser om att svenska myndigheter under vissa förutsättningar får ställa upp villkor som begränsar möjligheten att använda uppgifter som lämnas till en annan stat (se SOU 2017:29 s. 620). Även i brottsdatalagen finns det en sådan bestämmelse. En bestämmelse som reglerar Säkerhetspolisens möjlighet att ställa upp villkor för användningen bör med hänsyn till vikten av att myndigheten kan begränsa användningen av känslig information tas in i den nya lagen. Den bör utformas efter mönster av bestämmelsen i brottsdatalagen.

14.17.6 Dokumentationskrav

Utredningens förslag: Skyldigheten att i vissa fall dokumentera överföringar som görs till tredjeland och internationella organisationer ska regleras i förordning.

Skälen för utredningens förslag: Utredningen föreslår i delbetänkandet att de behöriga myndigheterna i vissa fall ska vara skyldiga att dokumentera överföringar som görs till tredjeland och internationella organisationer, men att det ska regleras i förordning. Detsamma gäller skyldigheten att informera tillsynsmyndigheten om vissa sådana överföringar (se SOU 2017:29 s. 621 f.). Kraven på dokumentation och information har sin grund i direktivet och gäller inte i dag.

Enligt utredningens mening är det lämpligt att Säkerhetspolisen dokumenterar överföringar som gjorts till tredjeland eller internationella organisationer i samma utsträckning som övriga brottsbekämpande myndigheter. Skyldigheten kan regleras i förordning.

Skyldigheten att självmant informera tillsynsmyndigheten om de överföringar som görs till tredjeland och internationella organisationer riskerar att medföra resurskrävande administrativt arbete för både Säkerhetspolisen och tillsynsmyndigheten. Något sådant krav bör därför inte ställas. I avsnitt 15.5.1 föreslås att Säkerhetspolisen ska ge tillsynsmyndigheten tillgång till dokumentation av behandlingen om den begär det. Det är enligt utredningens mening tillräckligt att dokumentationen görs tillgänglig för tillsynsmyndigheten inom ramen för den skyldigheten.

15 Tillsyn över Säkerhetspolisen

15.1 Det behövs en särskild reglering

Utredningens bedömning: Tillsynen över Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet bör regleras i Säkerhetspolisens datalag.

Skälen för utredningens bedömning

Tillsynen enligt dagens reglering

I dag utövas tillsynen över Säkerhetspolisens behandling av personuppgifter i den brottsbekämpande verksamheten både av Datainspektionen och Säkerhets- och integritetsskyddsmyndigheten (i fortsättningen nämnden). I delbetänkandet redovisa vilken tillsyn som i dag utövas över personuppgiftsbehandling inom brottsdatalogens tillämpningsområde (se SOU 2017:29 s. 425 f.).

Datainspektionen är enligt 2 § personuppgiftsförordningen tillsynsmyndighet enligt personuppgiftslagen. Datainspektionen har därmed det generella ansvaret för tillsyn över behandling av personuppgifter. Tillsynen avser personuppgiftsbehandling enligt både personuppgiftslagen och myndigheters registerförfattningar, t.ex. polisdatalagen. Av hänvisningarna i 2 kap. 2 § första stycket 11 och 13 och 6 kap. 4 § 1 polisdatalagen följer att personuppgiftslagens bestämmelser om tillsyn är tillämpliga i Säkerhetspolisens brottsbekämpande verksamhet.

Enligt 1 § andra stycket lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet utövar nämnden tillsyn över den behandling av personuppgifter enligt polisdatalagen som utförs av Polismyndigheten, Säkerhetspolisen och Ekobrottsmyndigheten.

Tillsynen ska särskilt avse behandling av känsliga personuppgifter. Tillsynen över Säkerhetspolisen omfattar även behandling enligt den tidigare gällande polisdatalagen (1998:622). Nämnden utövar också tillsyn över de brottsbekämpande myndigheternas användning av hemliga tvångsmedel och kvalificerade skyddsidentiteter och därmed sammanhängande verksamhet.

Om en annan myndighet har behörighet att utöva tillsyn avstår Datainspektionen normalt från att utöva tillsyn på det området (se Ett samlat ansvar för tillsyn över den personliga integriteten, SOU 2016:65, s. 79).

Förslag från Utredningen om tillsynen över den personliga integriteten

Utredningen om tillsynen över den personliga integriteten föreslår att Datainspektionen ska utses till tillsynsmyndighet enligt både dataskyddsdirektivet och dataskyddsförordningen och representera Sverige i den styrelse som inrättas genom dataskyddsförordningen (se SOU 2016:65 s. 142). Som representant för Sverige i styrelsen kommer Datainspektionen att delta i arbetet med att utfärda riktlinjer, rekommendationer och bästa praxis i frågor som rör personuppgiftsbehandling inom både direktivets och förordningens tillämpningsområden.

Utredningen föreslår också att nämnden inte längre ska utöva någon tillsyn över Polismyndighetens personuppgiftsbehandling. Däremot föreslås tillsynen över Säkerhetspolisens personuppgiftsbehandling i den brottsbekämpande verksamheten även fortsättningsvis utövas av både Datainspektionen och nämnden. Nämndens tillsyn över brottsbekämpande myndigheters användning av hemliga tvångsmedel och användning av kvalificerade skyddsidentiteter och därmed sammanhängande verksamhet ska enligt förslaget inte ändras. Nämnden ska liksom i dag på begäran av enskild kontrollera om han eller hon i strid med lag eller annan författning har utsatts för ett hemligt tvångsmedel eller varit föremål för Säkerhetspolisens personuppgiftsbehandling (se SOU 2016:65 s. 175 f. och 189).

Tillsyn enligt brottsdatalagen

I delbetänkandet redogör utredningen för vilka uppgifter och befogenheter tillsynsmyndigheten bör ha enligt brottsdatalagen och föreslår hur tillsynen ska bedrivas (se SOU 2017:29 s. 445 f.).

I tillsynsmyndighetens uppgifter ingår enligt 5 kap. 2 och 4 §§ brottsdatalagen att utöva allmän tillsyn över personuppgiftsbehandling, handlägga klagomål från registrerade, på begäran av fysiska personer kontrollera om deras personuppgifter behandlas författningsenligt, på begäran bistå utländska tillsynsmyndigheter med tillsynsåtgärder och lämna råd och stöd till personuppgiftsansvariga och personuppgiftsbiträden. Tillsynsmyndigheten förutsätts följa den tekniska utvecklingen och är inom ramen för ett formaliserat förhandssamråd i vissa fall skyldig att lämna råd om sådana nya typer av behandling eller förändringar av pågående behandling som antas medföra särskilda integritetsrisker (5 kap. 4 § brottsdataförordningen).

Tillsynsmyndigheten har rätt att få tillgång till de personuppgifter som behandlas, upplysningar och dokumentation om behandlingen och om säkerhets- och skyddsåtgärder. Myndigheten har också rätt till tillträde till lokaler där personuppgifter behandlas och till det biträde och den information som den behöver för sin tillsyn (5 kap. 5 § brottsdatalagen).

Till tillsynsmyndighetens förebyggande befogenheter, som inte är bindande, hör råd, rekommendationer och påpekanden. Tillsynsmyndigheten har också möjlighet att utfärda skriftlig varning om att det finns risk för att viss behandling kan komma att stå i strid med regelverket. Till de korrigerande befogenheterna, som är bindande, hör förelägganden om rättelse, radering och begränsning av behandlingen, beslut om förbud mot fortsatt behandling och beslut om sanktionsavgift (5 kap. 6 och 7 §§ brottsdatalagen).

Tillsynen över Säkerhetspolisen bör särregleras

På samma sätt som i dag bör naturligtvis personuppgiftsbehandling som rör nationell säkerhet stå under tillsyn och en utgångspunkt bör vara att tillsynen inte ska försämrats.

Enligt 1 kap. 4 § brottsdatalagen gäller lagen inte vid Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet.

Den gäller inte heller för Polismyndigheten när den övertagit en arbetsuppgift från Säkerhetspolisen som rör nationell säkerhet. Dataskyddsutredningen föreslår som framgår av avsnitt 14.2.1 att dataskyddsförordningen ska vara tillämplig även på verksamheter som inte regleras i EU-rätten. Eftersom verksamhet som rör nationell säkerhet inte omfattas av förordningens tillämpningsområde är förordningens bestämmelser om tillsyn inte anpassade till sådan verksamhet. Det är därför nödvändigt att särreglera tillsynen över Säkerhetspolisens personuppgiftsbehandling som rör nationell säkerhet.

I avsnitt 14.2.2 föreslår utredningen en särskild lag – Säkerhetspolisens datalag – som ska gälla vid Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet i syfte att bekämpa och lagföra brott. Även Polismyndigheten föreslås i begränsad utsträckning tillämpa lagen (se avsnitt 14.3.2). I den nya lagen bör det regleras vilken tillsyn över personuppgiftsbehandling enligt den nya lagen som ska förekomma.

Utgångspunkter för regleringen

Eftersom behandling av personuppgifter som rör nationell säkerhet har undantagits från både direktivets och förordningens tillämpningsområde styr bestämmelserna om tillsyn i rättsakterna inte hur den svenska lagstiftningen bör utformas. Som framgår av avsnitt 14.3.1 anses all Säkerhetspolisens operativa verksamhet vara i någon mening brottsbekämpande. Det talar för att regleringen bör efterlikna brottsdatalagens bestämmelser om tillsyn.

Säkerhetspolisens brottsbekämpande verksamhet syftar till att på ett tidigt stadium förebygga och förhindra brott som utgör ett samhällshot eller hotar grundläggande demokratiska funktioner. Säkerhetspolisen har för att kunna utföra sitt uppdrag behov av omfattande informationshantering och att kunna utbyta information med andra myndigheter. Brott som rör nationell säkerhet har ofta sin grund i ideologiska uppfattningar, bl.a. religiös övertygelse eller politiska åsikter. Säkerhetspolisen har därmed särskilt stort behov av att behandla känsliga personuppgifter.

För verksamheten vid Säkerhetspolisen gäller i stor utsträckning sekretess och allmänheten och enskilda har begränsad insyn i den.

Det innebär bl.a. att enskilda inte på samma sätt som i annan verksamhet kan reagera över felaktigheter eller komma med allmänna klagomål över hur verksamheten bedrivs. Den kontroll som allmänhetens tillgång till allmänna handlingar normalt innebär för offentlig verksamhet ger, på grund av den omfattande sekretessen, därmed inte samma effekt som i annan verksamhet.

I delbetänkandet diskuteras utredningen ingående vilka utgångspunkter som är viktiga vid överväganden om tillsyn över personuppgiftsbehandling inom brottsdatalogens tillämpningsområde. Åtskilligt av det som sägs där är relevant även för tillsynen över Säkerhetspolisens personuppgiftsbehandling. Här bör nämnas att en fri och oberoende tillsyn måste värnas, vilket bl.a. bör komma till uttryck på det sättet att tillsynen inte detaljregleras. Det är även viktigt med tydliga regler för verksamheten så att både tillsynsmyndigheten, tillsynsobjekten och enskilda vet vilka rättigheter och skyldigheter som gäller och kan förhålla sig till det. Utredningen konstaterar att en effektiv tillsyn bäst gagnas av att den som utövar tillsynen får så stor frihet som möjligt att välja arbetsformer, utan att det görs avkall på rättssäkerheten (se SOU 2017:29 s. 431).

15.2 Vem ska utöva tillsyn över Säkerhetspolisen?

15.2.1 För- och nackdelar med parallell tillsyn

Det finns skäl att överväga tillsynen över Säkerhetspolisen på nytt

Dataskyddsutredningens förslag att dataskyddsförordningen ska vara generellt tillämplig och vårt förslag att Säkerhetspolisens personuppgiftsbehandling ska regleras i en ny lag innebär att förutsättningarna för tillsynen över Säkerhetspolisens personuppgiftsbehandling har förändrats sedan Utredningen om tillsynen över den personliga integriteten lämnade sitt betänkande. Det finns därför anledning att på nytt överväga hur tillsynen över Säkerhetspolisens behandling av personuppgifter bör utövas.

För- och nackdelar med parallell tillsyn

Den första frågan är om tillsynen bör utövas av en eller två myndigheter. En fördel med parallell tillsyn är att myndigheterna kan inrikta sin granskning på olika områden, vilket kan bidra till en mer omfattande och allsidig tillsyn. Två tillsynsmyndigheter med olika uppdrag och fokus kan på så sätt komplettera varandra. En sådan förstärkt tillsyn har ansetts vara särskilt värdefull i verksamhet som omfattas av stark sekretess och där allmänheten och enskilda har begränsad insyn (se Ytterligare rättssäkerhetsgarantier vid användandet av hemliga tvångsmedel, m.m., prop. 2006/07:133, s. 30 f., prop. 2009/10:85 s. 273 f. och SOU 2016:65 s. 175 f.).

Nackdelarna med parallell tillsyn är att det kan leda till oklar ansvarsfördelning mellan tillsynsmyndigheterna. Det finns då risk för att vissa frågor aldrig blir föremål för tillsyn eller att samma fråga granskas gång på gång. Även om myndigheterna har olika fokus och inriktning på sin tillsyn kan parallell tillsyn vidare leda till motstridig praxis. Ett överlappande ansvar riskerar också att medföra dubbelarbete och skapa samordningsbehov och därmed inte vara resurseffektivt (se Riksrevisionens rapport om Säkerhets- och integritetsskyddsmyndighetens tillsyn över brottsbekämpande myndigheter, skr. 2015/16:188, s. 31 f.).

En särskild nackdel med parallell tillsyn är att den kan leda till att fler personer får insyn i speciellt känslig verksamhet där hemliga uppgifter hanteras i stor omfattning.

Den parallella tillsynen över Polismyndighetens personuppgiftsbehandling har enligt Utredningen om tillsynen över den personliga integriteten visat sig medföra gränsdragningsproblem och otydlighet om vem som ska utföra tillsynen, vad tillsynen ska avse och resultaten av den. Den utredningen ser inte några fördelar med dagens parallella tillsyn över Polismyndigheten (se SOU 2016:65 s. 185 f.). Det kan enligt den utredningen dock förekomma att någon annan myndighet har begränsade tillsynsuppgifter inom vissa särskilda områden och att den ordningen inte bör eller kan ersättas med en ordning där all tillsyn utövas av en myndighet. I fråga om tillsyn över Säkerhetspolisen föreslår den utredningen därför att dagens parallella tillsyn behålls. De särskilda omständigheter som motiverar att det bedrivs parallell tillsyn över Säkerhetspolisen gör sig dock enligt den utredningens mening inte gällande med

samma styrka vid tillsyn över Polismyndigheten. Beträffande den tillsynen talar enligt den utredningen övervägande skäl för att bara en myndighet bör utöva tillsyn (se SOU 2016:65 s. 143 f., 175 f. och 185 f.).

15.2.2 Bör den parallella tillsynen bestå?

Utredningens bedömning: Tillsynen över Säkerhetspolisens behandling av personuppgifter bör utövas av både Datainspektionen och Säkerhets- och integritetsskyddsnämnden. Deras tillsyn bör i huvudsak vara densamma som i dag.

Skälen för utredningens bedömning

En lösning med en tillsynsmyndighet vore bäst

Enligt utredningens mening var lagstiftarens intentioner goda när parallell tillsyn över Säkerhetspolisens personuppgiftsbehandling infördes. Parallell tillsyn ger dock fördelar endast om fler än en tillsynsmyndighet faktiskt utför tillsynen och myndigheterna samarbetar för att reducera de negativa effekter som parallell tillsyn kan medföra. Datainspektionen har inte förrän nyligen utövat någon egentlig tillsyn över Säkerhetspolisen, som därmed i praktiken inte har varit föremål för parallell tillsyn.

De skäl som har lyfts fram för att bara en myndighet ska utöva tillsyn över Polismyndighetens personuppgiftsbehandling talar enligt utredningens mening lika starkt för att endast en myndighet bör utöva tillsyn över Säkerhetspolisens personuppgiftsbehandling. Frågan är då vilken myndighet som skulle vara bäst lämpad att göra det, om endast en myndighet ska göra det. Valet står mellan Datainspektionen och nämnden.

För- och nackdelar med nämnden som tillsynsmyndighet

Nämnden inrättades bl.a. för att förstärka tillsynen över Säkerhetspolisen. Nämndens särskilda beslutsform, med parlamentarisk förankring, har ansetts utgöra dess styrka och vara särskilt viktig för

att tillgodose allmänhetens insyn i verksamhet som omfattas av stark sekretess (se prop. 2006/07:133 s. 65 och prop. 2009/10:85 s. 272 f.). Bestämmelserna i 42 kap. offentlighets- och sekretesslagen om sekretess hos nämnden har också anpassats till behovet av att kunna hantera hemliga uppgifter i tillsynen. Regeringen har framhållit att nämnden har särskild insikt i och erfarenhet av sådan verksamhet som nu är ifråga. Det ökar enligt förarbetena till polisdatalagen förutsättningarna för att tillsynen inriktas på de områden där det finns särskilda risker för intrång i enskildas integritet (se prop. 2009/10:85 s. 273 f.).

Det som särskilt talar för att välja nämnden som tillsynsmyndighet är därför dess särskilda kompetens, erfarenhet och vana att utöva tillsyn över personuppgiftsbehandling i känslig verksamhet där sekretessen är mycket omfattande. Förutom att ha god kännedom om den verksamhet som tillsynen avser är nämnden också väl förtrogen med den personuppgiftsbehandling som utförs och vilka personuppgiftssamlingar som förs av Säkerhetspolisen. En annan fördel är att nämnden har ett begränsat tillsynsuppdrag, vilket ger den goda förutsättningar att säkerställa att tillsyn över Säkerhetspolisen bedrivs på ett aktivt och kontinuerligt sätt. Nämnden har hittills i praktiken ensam utövat tillsynen över Säkerhetspolisen. Riksrevisionen har nyligen granskat verksamheten och funnit att nämnden utför sina uppgifter på ett ändamålsenligt sätt (se skr. 2015/16:188 s. 3). Sekretessregleringen är också särskilt anpassad för tillsynen över Säkerhetspolisen.

Det som kan tala mot att nämnden ensam utses till tillsynsmyndighet är att den är liten och därmed sårbar för personalförändringar vilket kan leda till att värdefull erfarenhet går förlorad. Ur ett säkerhetsperspektiv kan det samtidigt vara en fördel att nämnden är liten, eftersom det innebär att färre personer blir involverade i tillsynen.

Det som framför allt talar mot att välja nämnden är att den i dag inte har de befogenheter som krävs för att utöva tillsynen på egen hand, vilket är nödvändigt för att Sverige ska leva upp till kraven på ett effektivt rättsmedel enligt artikel 13 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen). Det är också tveksamt om det är lämpligt att ge nämnden sådana befogenheter med hänsyn till hur nämnden är organiserad. Vidare får nämndens avgöranden inte

överklagas. Samtidigt talar starka skäl för att det bör finnas möjlighet att klaga på vissa av tillsynsmyndighetens beslut, eftersom de kan få långtgående konsekvenser för tillsynsobjektet.

För- och nackdelar med Datainspektionen som tillsynsmyndighet

Det som särskilt talar för att välja Datainspektionen som tillsynsmyndighet är att den har bred kompetens och lång erfarenhet av tillsyn över hur personuppgifts- och integritetsskyddslagstiftning tillämpas. Inspektionen har därför goda förutsättningar att utöva tillsyn över tillämpningen av allmänna principer för behandling av personuppgifter. Eftersom inspektionen utövar tillsyn över övriga brottsbekämpande myndigheter får den också en allmän överblick som nämnden saknar.

Datainspektionen kommer att ha ett generellt uppdrag att följa den tekniska utvecklingen på personuppgiftsområdet. Inspektionen kommer också att genomföra förhandssamråd med de flesta myndigheter och andra personuppgiftsansvariga. Genom samarbetet inom EU kommer inspektionen att få en överblick över den tekniska utvecklingen även i andra stater. Det skapar goda förutsättningar för rådgivning i frågor som gäller uppbyggnad av it-system.

Datainspektionen utövar i dag tillsyn över Försvarmakten enligt lagen (2007:258) om behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst och över Försvarets radioanstalt enligt lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet. Inspektionen har därmed erfarenhet av att utöva tillsyn över känslig verksamhet med omfattande sekretess som liknar Säkerhetspolisens.

Det som främst talar mot att välja Datainspektionen är att inspektionen har ett mycket omfattande tillsynsuppdrag och att tillsynen över en viss myndighet därför av naturliga skäl bara kan ägnas begränsade resurser. Inspektionen har i praktiken inte heller förrän nyligen utövat någon tillsyn över Säkerhetspolisen och har därför inte samma kunskap som nämnden om Säkerhetspolisens verksamhet och personuppgiftsbehandling. Genom EU:s dataskyddsreform får inspektionen dessutom ett utökat uppdrag som

kan medföra att utrymmet att bedriva tillsyn över enskilda myndigheter i praktiken begränsas ytterligare.

Myndigheternas tillsyn ska i huvudsak vara oförändrad

Enligt utredningens mening finns det alltså både för- och nackdelar om någon av de två myndigheterna skulle väljas som ensam tillsynsmyndighet. Även om det ideala vore att ta bort den parallella tillsynen över Säkerhetspolisen, på samma sätt som Utredningen om tillsynen över den personliga integriteten föreslår beträffande tillsynen över Polismyndigheten, går det inte att välja bara en av myndigheterna eftersom deras styrkor kompletterar varandra. Den utredningen lyfter fram det som argument för att nämnden, vid sidan av Datainspektionen, ska fortsätta att ha tillsyn över Säkerhetspolisens personuppgiftsbehandling (se SOU 2016:65 s. 179).

En annan viktig faktor att ta hänsyn till är att tillsynen över Säkerhetspolisens personuppgiftsbehandling skulle minska betydligt i omfattning om den parallella tillsynen skulle upphöra, eftersom det inte är realistiskt att förvänta sig att Datainspektionens tillsyn skulle kunna ersätta den omfattande tillsyn som i dag utövas av nämnden. Även utredningen om tillsynen över den personliga integriteten påpekar att fortsatt parallell tillsyn torde innebära att de huvudsakliga tillsynsinsatserna på samma sätt som i dag kommer utföras av nämnden (se SOU 2016:65 s. 183). Tillsynen över Säkerhetspolisens personuppgiftsbehandling bör mot den bakgrunden i huvudsak vara densamma som i dag.

Utredningen om tillsynen över den personliga integriteten hade som en av sina huvuduppgifter att analysera och bedöma vilken myndighet som bör utöva tillsyn över personuppgiftsbehandling enligt både dataskyddsförordningen och direktivet. Det kommer sannolikt inte att finnas något ställningstagande i den frågan när vi ska redovisa vårt uppdrag. Vi utgår därför, på samma sätt som i delbetänkandet, från det förslag som Utredningen om tillsynen över den personliga integriteten presenterat om vem som bör utöva tillsyn över personuppgiftsbehandlingen på direktivets område. Det innebär att vi inte tar ställning till om nämnden bör utöva tillsyn över Polismyndighetens personuppgiftsbehandling.

15.3 Tillsynsområdet

Utredningens förslag: Tillsynsmyndighet ska definieras som den myndighet som regeringen utser att enligt Säkerhetspolisens datalag utöva tillsyn över behandlingen av personuppgifter.

Skälen för utredningens förslag: På samma sätt som brottsdatalagen bör Säkerhetspolisens datalag innehålla bestämmelser om tillsynen. Det bör då också tas in en definition av uttrycket tillsynsmyndighet som preciserar vad tillsynen ska omfatta.

Eftersom Säkerhetspolisens datalag ska tillämpas av både Säkerhetspolisen och Polismyndigheten och sistnämnda myndighet endast i mycket begränsad omfattning kommer att tillämpa lagen är det inte möjligt att knyta tillsynsområdet till viss verksamhet. Tillsynsområdet bör i stället knytas till behandling av personuppgifter enligt lagen.

En särskild fråga är om tillsynen bör omfatta både de myndigheter som tillämpar lagen och eventuella personuppgiftsbiträden som de anlitar. När det gäller Säkerhetspolisens verksamhet är de faktiska möjligheterna att låta personuppgiftsbiträden hantera personuppgifter i den operativa verksamheten betydligt mer begränsade än i annan brottsbekämpande verksamhet på grund av sekretessen. Behovet av att låta tillsynen omfatta personuppgiftsbiträden är därmed begränsat. Det finns emellertid inte skäl att ha en annan lösning för tillsynen enligt Säkerhetspolisens datalag än den som gäller för andra brottsbekämpande myndigheter. Tillsynen bör således även omfatta personuppgiftsbehandling som personuppgiftsbiträden utför enligt lagen.

Av lagen bör det även framgå att det finns ytterligare bestämmelser om tillsyn i lagen om tillsyn över viss brottsbekämpande verksamhet.

Som framgår av avsnitt 14.3.3 ska Säkerhetspolisen tillämpa brottsdatalagen och polisens brottsdatalag med tillhörande förordningar vid behandling av personuppgifter som avser brottsbekämpning eller lagföring och som inte rör nationell säkerhet. Då gäller i stället bestämmelserna om tillsyn i brottsdatalagen.

15.4 Tillsynen enligt Säkerhetspolisens datalag

15.4.1 Allmän tillsyn

Utredningens förslag: Tillsynsmyndigheten ska utöva allmän tillsyn över Säkerhetspolisens personuppgiftsbehandling.

Skälen för utredningens förslag

Allmän tillsyn har stor betydelse

Det bör av lagen framgå att tillsynsmyndigheten ska utöva allmän tillsyn. Det som avses är rättslig tillsyn över hur Säkerhetspolisen tillämpar den nya lagen om personuppgiftsbehandling. Sådan tillsyn har av naturliga skäl främst ett tillbakablickande perspektiv. Den inriktas i första hand på att kontrollera om behandlingen av personuppgifter är författningenenlig. Sådan tillsyn utförs normalt genom granskning av dokumentation och inspektioner på plats. Vad det innebär att utöva allmän tillsyn över personuppgiftsbehandling vid brottsbekämpning och lagföring utvecklas i delbetänkandet (se SOU 2017:29 s. 460).

Som utredningen påpekar i avsnitt 15.1 saknas det en viktig faktor för tillsynen över Säkerhetspolisens personuppgiftsbehandling, nämligen de impulser som klagomål från enskilda kan ge. Enskilda har visserligen samma rätt att framföra klagomål mot Säkerhetspolisens personuppgiftsbehandling till myndigheten eller till någon tillsynsmyndighet som mot annan offentlig verksamhet. De praktiska förutsättningarna för sådana klagomål är emellertid annorlunda när det gäller Säkerhetspolisens verksamhet, eftersom de registrerade sällan känner till att deras personuppgifter behandlas. Tillsynen kan därför inte i samma utsträckning som annars bygga på klagomål från allmänheten och mediegranskning. Den allmänna tillsynen måste i stället bygga på att de som utövar tillsyn har goda kunskaper om både verksamheten och de risker för den personliga integriteten som personuppgiftsbehandlingen i den kan föra med sig. Det sagda innebär att uppgiften att bedriva allmän tillsyn är viktigare än annars och delvis kräver andra överväganden.

Klagomålshanteringen bör inte regleras

Som nyss nämnts har enskilda samma rätt att framföra klagomål mot Säkerhetspolisens personuppgiftsbehandling som mot andra brottsbekämpande myndigheters. I delbetänkandet redovisar utredningen vad som allmänt gäller i fråga om hantering av klagomål (se SOU 2017:29 s. 449 och 541 f.). Den formella regleringen i brottsdatalagen av hur klagomål bör hanteras har sin grund i direktivet. Någon motsvarande reglering krävs därför inte när det gäller Säkerhetspolisen. De allmänna principerna för tillsyn och reglerna i förvaltningslagen (1986:223) är enligt utredningens mening tillräckliga för att tillsynsmyndigheten ska kunna handlägga eventuella klagomål mot Säkerhetspolisens personuppgiftsbehandling. Klagomålshanteringen bör således inte regleras.

Inga ytterligare tillsynsuppgifter

I dag ingår det inte i Datainspektionens tillsynsuppgifter att på begäran av enskild kontrollera om personuppgiftsbehandlingen är författningsenlig. Däremot utförs sådan kontroll över Säkerhetspolisens personuppgiftsbehandling av nämnden. Även om Datainspektionen i brottsdatalagen ges motsvarande uppgift finns det inte anledning att nu införa parallell tillsyn när det gäller kontroll på begäran av enskild. Sådan kontroll är resurskrävande och till det kommer att parallell tillsyn skulle kräva samordning mellan tillsynsmyndigheterna på ett helt annat sätt än i dag, eftersom den enskilde har rätt att kräva att kontrollen utförs. Utredningen anser därför att det inte bör införas bestämmelser om kontroll på begäran av enskild i Säkerhetspolisens datalag.

Det finns i dag inga internationella åtaganden om samarbete mellan tillsynsmyndigheter när det gäller tillsyn över personuppgiftsbehandling som rör nationell säkerhet. Någon motsvarighet till regleringen i 5 kap. 2 § 4 brottsdatalagen om bistånd till utländska tillsynsmyndigheter behövs därför inte i Säkerhetspolisens datalag.

15.4.2 Förhandssamråd och annat råd och stöd

Utredningens förslag: Tillsynsmyndigheten ska ge råd och stöd till Säkerhetspolisen och personuppgiftsbiträden om deras skyldigheter enligt lag eller annan författning vid förhandssamråd och när det i övrigt är påkallat. Tillsynsmyndighetens närmare skyldigheter ska regleras i förordning.

Tillsynsmyndigheten ska om det är lämpligt låta nämnden yttra sig inom ramen för förhandssamråd.

Skälen för utredningens förslag

Dagens samrådsskyldighet

Enligt 2 § polisdataförordningen ska Polismyndigheten och Säkerhetspolisen samråda med Datainspektionen i god tid innan beslut fattas om nya it-system av större omfattning eller betydande förändringar genomförs i befintliga it-system om de kan innebära särskilda risker för intrång i den personliga integriteten. Om det krävs ska Säkerhetspolisen även samråda med nämnden.

Säkerhetspolisen samråder normalt med båda myndigheterna. Deras rådgivning skiljer sig åt på så sätt att Datainspektionen lämnar mer omfattande och generella synpunkter, medan nämndens uttalanden oftast är kortare och riktar in sig mer på konkreta frågor om personuppgiftsbehandlingen. Säkerhetspolisen anser att det är värdefullt med båda myndigheternas råd.

Polismyndigheten har kritiserat den dubbla samrådsskyldigheten enligt 2 § polisdataförordningen och framhållit att den får negativa konsekvenser. Det krävs ofta tolkning av hur myndigheternas samrådssynpunkter förhåller sig till varandra (se skr. 2015/16:188 s. 31 f.). Även Säkerhetspolisen har påtalat risken att tillsynsmyndigheterna lämnar motstridiga råd.

Tillsynsmyndighetens skyldigheter vid förhandssamråd

I avsnitt 14.14 föreslås att Säkerhetspolisen ska samråda med tillsynsmyndigheten om en konsekvensbedömning visar särskild risk för intrång i registrerades personliga integritet eller om typen av

behandling innebär särskild risk för intrång. Förhandssamrådet motsvarar i stort det samråd som regleras i 2 § polisdataförordningen.

Tillsynsmyndighetens skyldigheter vid samråd är i dag inte närmare reglerade. Som framgår av avsnitt 14.14 bör Säkerhetspolisens skyldigheter vid förhandssamråd regleras på samma sätt som i brottsdatalagen. Tillsynsmyndigheten bör då också ha i huvudsak motsvarande skyldigheter. Det innebär att tillsynsmyndigheten bör vara skyldig att lämna skriftliga råd i vissa fall. Detaljfrågorna kan regleras i förordning.

Nämndens roll vid förhandssamråd

Frågan är om Säkerhetspolisen även i fortsättningen bör ha samma skyldighet att samråda med nämnden som den har i dag.

Nämndens tillsynsuppdrag avser rättslig granskning i efterhand och uttalanden om behov av förändringar i verksamheten eller i lagstiftningen. I förarbetena framhålls att planerade åtgärder inte kan bli föremål för granskning och att nämndens verksamhet således inte kan uppfattas som ett godkännande av framtida åtgärder (se prop. 2006/07:133 s. 63). Även om tyngdpunkten i nämndens tillsyn alltså kommer att vara tillsyn i efterhand, bör nämnden inte stängas ute vid överväganden som kan komma att påverka den framtida personuppgiftsbehandlingen. Eftersom Datainspektionens och nämndens kompetens och erfarenheter kompletterar varandra anser utredningen att nämnden även i fortsättningen bör ha en roll vid förhandssamråd.

Det är dock inte lämpligt att behålla den dubbla samrådsskyldigheten som den är utformad i dag. I stället bör tillsynsmyndigheten, om det är lämpligt, ge nämnden tillfälle att yttra sig inom ramen för förhandssamrådet. Nämnden bör då också ha rätt att ta del av underlaget för förhandssamrådet. Nämnden får på det sättet möjlighet att lämna synpunkter utan att det uppfattas som ett godkännande av viss behandling på förhand. Den lösningen innebär att risken för att Säkerhetspolisen får motstridiga råd kan undvikas. Skulle Säkerhetspolisen föreslå att Datainspektionen låter nämnden yttra sig bör inspektionen givetvis beakta det. Samrådsskyldigheten kan regleras i förordning.

Annat råd och stöd

En viktig uppgift vid tillsyn är att även i andra fall lämna råd och stöd till personuppgiftsansvariga och personuppgiftsbiträden om deras skyldigheter enligt lagstiftningen. Den skyldigheten bör återspeglas i lagen.

I avsnitt 14.14 föreslås bestämmelser om Säkerhetspolisens skyldigheter i egenskap av personuppgiftsansvarig som i huvudsak motsvarar regleringen i brottsdatalagen. Säkerhetspolisen kan därför ha samma behov som andra brottsbekämpande myndigheter av att rådgöra med tillsynsmyndigheten på eget initiativ. Tillsynsmyndigheten bör mot den bakgrunden ha rådgivande uppgifter som motsvarar dem som anges i 5 kap. 4 § brottsdatalagen.

15.5 Befogenheter vid tillsynen enligt den nya lagen

15.5.1 Undersökningsbefogenheter

Utredningens förslag: Tillsynsmyndigheten ska ha rätt att av Säkerhetspolisen eller ett personuppgiftsbiträde på begäran få

1. tillgång till alla personuppgifter som behandlas,
2. upplysningar om och dokumentation av behandlingen av personuppgifter och säkerhets- och skyddsåtgärder,
3. tillträde till lokaler som Säkerhetspolisen eller ett personuppgiftsbiträde disponerar och tillgång till utrustning och andra medel för behandling av personuppgifter, och
4. det biträde och annan information som behövs för tillsynen.

Skälen för utredningens förslag: Som utredningen utvecklar i delbetänkandet består rättslig tillsyn till stor del av granskning av dokumentation, men den kan även kräva besök på plats hos den personuppgiftsansvarige för att ta del av personuppgifterna. Förutom tillgång till de personuppgifter som behandlas behöver tillsynsmyndigheten även upplysningar om och dokumentation av pågående behandlingar. Tillsynsmyndigheten kan även behöva annan information som inte är direkt kopplad till den behandling som ska granskas och besöka lokaler där personuppgiftsbehandling

pågår för att bl.a. inspektera säkerhetsåtgärder. Myndigheten kan även behöva praktiskt biträde vid sin tillsyn (se SOU 2017:29 s. 464 f.). Tillsynsmyndighetens undersökande befogenheter bör enligt utredningens mening vara desamma vid tillsyn över Säkerhetspolisens personuppgiftsbehandling som vid tillsyn över andra brottsbekämpande myndigheter. Regleringen i Säkerhetspolisens datalag kan därför utformas på samma sätt som i 5 kap. 5 § brottsdatalagen.

15.5.2 Både förebyggande och korrigerande befogenheter behövs

Utredningens bedömning: Tillsynsmyndigheten bör ha både förebyggande och korrigerande befogenheter.

Skälen för utredningens bedömning: I direktivet och dataskyddsförordningen görs tydlig skillnad mellan förebyggande och korrigerande befogenheter, vilket återspeglas i regleringen i brottsdatalagen (se SOU 2017:29 s. 467 f.). De befogenheter som föreslås för tillsynsmyndigheten i brottsdatalagen har sin grund i regleringen i direktivet och de krav som ställs där. Som tidigare nämnts finns det inga motsvarande krav när det gäller tillsyn över personuppgiftsbehandling som rör nationell säkerhet.

Enligt utredningens mening är det lämpligt att tillsynsmyndigheten får befogenheter som ger möjlighet att successivt använda kraftfullare medel och därigenom stegra påtryckningarna om Säkerhetspolisen inte självmant rättar sig efter myndighetens anvisningar (jfr SOU 2017:29 s. 468). Det innebär att tillsynsmyndigheten bör ha både förebyggande och korrigerande befogenheter. Det bör vidare göras tydlig skillnad mellan de förebyggande och de korrigerande befogenheterna på samma sätt som i brottsdatalagen. Mot bakgrund av Säkerhetspolisens speciella verksamhet är det dock inte självklart att tillsynsmyndigheten bör ha alla de befogenheter som regleras i brottsdatalagen.

15.5.3 Förebyggande befogenheter

Utredningens förslag: Om tillsynsmyndigheten bedömer att det finns risk för att personuppgifter kan komma att behandlas i strid med lag eller annan författning, ska den genom råd, rekommendationer eller påpekanden försöka förmå den personuppgiftsansvarige att vidta åtgärder för att minska den risken.

Tillsynsmyndigheten ska få utfärda en skriftlig varning för att planerad behandling av personuppgifter riskerar att stå i strid med lag eller annan författning. Detsamma ska gälla om pågående behandling riskerar att stå i strid med lag eller annan författning.

Skälen för utredningens förslag

Råd, rekommendationer eller påpekanden

Om tillsynsmyndigheten bedömer att det finns risk för att personuppgifter kan komma att behandlas i strid med lag eller annan författning ska den enligt 5 kap. 6 § första stycket brottsdatalagen genom råd, rekommendationer eller påpekanden försöka förmå den personuppgiftsansvarige eller personuppgiftsbiträdet att vidta åtgärder för att minska den risken.

Som nyss nämnts bör tillsynsmyndigheten ha förebyggande befogenheter. En bestämmelse som motsvarar 5 kap. 6 § första stycket brottsdatalagen bör därför tas in i Säkerhetspolisens datalag. På vilket sätt råd, rekommendationer eller påpekanden ska lämnas bör inte författningsregleras. Som framgår av avsnitt 15.4.2 är dock tillsynsmyndigheten skyldig att lämna skriftliga råd vid förhandssamråd.

Varning bör kunna utfärdas

Enligt 5 kap. 6 § andra stycket brottsdatalagen får tillsynsmyndigheten utfärda varning i vissa fall. En varning är inte bindande utan är tänkt att kunna användas som ett påtryckningsmedel innan bindande föreläggande att vidta viss åtgärd utfärdas, för att i ett enskilt fall markera allvaret. Varning får även användas om en pågående

behandling riskerar att strida mot lag eller annan författning (se SOU 2017:29 s. 469). De skäl som anförs i delbetänkandet för att tillsynsmyndigheten ska kunna utfärda varning har giltighet även vid tillsyn över Säkerhetspolisen. Mot den bakgrunden bör även en bestämmelse som motsvarar 5 kap. 6 § andra stycket brottsdatalagen tas in i Säkerhetspolisens datalag.

15.5.4 Korrigerande befogenheter

Utredningens förslag: Om tillsynsmyndigheten konstaterar att personuppgifter behandlas i strid med lag eller annan författning, eller att Säkerhetspolisen eller ett personuppgiftsbiträde annars inte fullgör sina skyldigheter, får tillsynsmyndigheten

1. genom råd, rekommendationer eller påpekanden försöka förmå Säkerhetspolisen eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningssenlig eller att uppfylla andra skyldigheter,
2. förelägga Säkerhetspolisen eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningssenlig eller att fullgöra andra skyldigheter, eller
3. förbjuda fortsatt behandling om bristen är allvarlig.

Om tillsynsmyndigheten utfärdar ett föreläggande ska det av föreläggandet framgå när åtgärderna senast ska vara genomförda och, om det är lämpligt, vilka åtgärder som ska vidtas.

Skälen för utredningens förslag: För att tillsynen ska bli effektiv måste tillsynsmyndigheten kunna utfärda bindande förelägganden om att en viss åtgärd ska vidtas av den personuppgiftsansvarige (se En tydlig, rättssäker och effektiv tillsyn, skr. 2009/10:79, s. 42).

De korrigerande befogenheterna i 5 kap. 7 § brottsdatalagen är av fyra slag. Tillsynsmyndigheten får för det första använda sig av råd, rekommendationer eller påpekanden för att försöka förmå den personuppgiftsansvarige eller personuppgiftsbiträdet att vidta åtgärder för att personuppgiftsbehandlingen ska vara författningssenlig eller att fullgöra andra skyldigheter. För det andra får myndig-

heten förelägga den personuppgiftsansvarige eller personuppgiftsbiträdet att vidta sådana åtgärder. Tillsynsmyndigheten får vidare förbjuda fortsatt behandling och besluta om sanktionsavgift.

Som framgår av avsnitt 14.16.2 bör sanktionsavgift inte kunna tas ut av Säkerhetspolisen. Utredningen anser att tillsynsmyndigheten i övrigt bör ha samma korrigerande befogenheter som enligt brottsdatalagen. Vad de korrigerande åtgärderna innebär utvecklas i delbetänkandet (se SOU 2017:29 s. 470 f.).

Regleringen bör byggas upp på samma sätt som i brottsdatalagen, vilket innebär att åtgärderna i princip ska prövas i den ordning de anges i bestämmelsen. Det bör dock inte krävas att alla lindrigare åtgärder har prövats. Om omständigheterna är sådana att det redan från början står klart att fortsatt behandling bör förbjudas, bör tillsynsmyndigheten kunna besluta om det utan att ha prövat någon annan åtgärd först.

Förelägganden kan avse korrigeringsåtgärder men även andra åtgärder som den personuppgiftsansvarige eller personuppgiftsbiträdet ska vidta. När det gäller korrigeringsåtgärder kan det vara lämpligt att ange vilken åtgärd som ska vidtas, exempelvis rättelse. När det behövs andra åtgärder, t.ex. tekniska åtgärder, kan tillsynsobjektet vara bättre lämpad att avgöra vad som bör göras för att behandlingen ska bli författningsenlig. Tillsynsmyndigheten bör därför endast när de finner det lämpligt ange vilken åtgärd som ska vidtas. Däremot bör det alltid framgå av förelägandet när åtgärden senast ska vara genomförd.

15.6 Handläggningen av tillsynsfrågor

15.6.1 Kommunikationsskyldighet

Utredningens förslag: Innan tillsynsmyndigheten fattar ett bindande beslut, ska den som beslutet gäller ges tillfälle att inom en bestämd tid yttra sig över allt material av betydelse för beslutet, om det inte är uppenbart obehövligt.

Skälen för utredningens förslag: Eftersom det inte anses finnas några parter i ett tillsynsärende är förvaltningslagens regler om kommunikation inte tillämpliga (se SOU 2017:29 s. 448 och 474).

Det föreskrivs därför i 5 kap. 8 § brottsdatalagen att tillsynsmyndigheten ska ge tillsynsobjektet tillfälle att yttra sig innan beslut meddelas. Det behövs en motsvarande bestämmelse om kommunikationsskyldighet i den nya lagen. Skyldigheten bör omfatta allt material som tillförts ärendet, både inkomna handlingar från andra än tillsynsobjektet och handlingar som har upprättats av tillsynsmyndigheten. Vad skyldigheten innebär utvecklas i delbetänkandet (se SOU 2017:29 s. 474 f.).

15.6.2 Överklagande

Utredningens förslag: Tillsynsmyndighetens beslut enligt lagen eller föreskrifter meddelade i anslutning till den ska få överklagas till allmän förvaltningsdomstol.

Vid överklagande till kammarrätten ska det krävas prövningstillstånd.

Skälen för utredningens förslag: Enligt 22 § förvaltningslagen får ett beslut överklagas av den som beslutet angår, om det har gått honom eller henne emot och är överklagbart. Enligt 51 § första stycket personuppgiftslagen får Datainspektionens beslut, med undantag av beslut om föreskrifter, överklagas till allmän förvaltningsdomstol. Det innebär att exempelvis beslut om förbud mot fortsatt behandling kan överklagas. I praxis har även vissa förelägganden som inspektionen utfärdat bedömts vara överklagbara (se SOU 2015:39 s. 622 f.). Enligt 7 kap. 4 § brottsdatalagen får tillsynsmyndighetens beslut enligt lagen eller föreskrifter som meddelats i anslutning till den överklagas. I delbetänkandet redovisar utredningen vad som gäller för myndigheters rätt att överklaga (se SOU 2017:29 s. 561 f.).

Av de skäl som anges i delbetänkandet bör tillsynsmyndighetens beslut få överklagas (se SOU 2017:29 s. 562 f.). Regleringen av överklagande bör vara densamma i Säkerhetspolisens datalag som i brottsdatalagen. Det innebär att besluten bör överklagas till allmän förvaltningsdomstol och att prövningstillstånd bör krävas för att frågan ska prövas av kammarrätt.

15.6.3 Anmälningsskyldighet

Utredningens förslag: Om tillsynsmyndigheten uppmärksammar förhållanden som kan utgöra brott ska den anmäla det till Åklagarmyndigheten. Det ska regleras i förordning.

Skälen för utredningens förslag: Enligt 5 kap. 3 § brottsdataförordningen är tillsynsmyndigheten skyldig att anmäla vissa förhållanden som det ankommer på andra myndigheter att ingripa mot. Det bör gälla även vid tillsyn över personuppgiftsbehandling enligt Säkerhetspolisens datalag. Anmälningsskyldigheten bör regleras i förordning.

15.7 Säkerhets- och integritetsskyddsnämndens tillsyn

15.7.1 Nämndens allmänna tillsyn

Utredningens förslag: Nämnden ska utöva tillsyn över personuppgiftsbehandling som rör nationell säkerhet i Säkerhetspolisens brottsbekämpande och lagförande verksamhet. Det ska tydliggöras att nämnden har rätt att få tillgång till all information och alla upplysningar som den behöver för sin tillsyn.

Skälen för utredningens förslag

Tillsynsområdet

I 1 § andra stycket lagen om tillsyn över viss brottsbekämpande verksamhet föreskrivs att nämnden ska utöva tillsyn över den behandling av personuppgifter enligt polisdatalagen och lagen om polisens allmänna spaningsregister som utförs av Polismyndigheten, Säkerhetspolisen och Ekobrottsmyndigheten. När det gäller Säkerhetspolisen ska tillsynen även avse behandling enligt den tidigare gällande polisdatalagen (1998:622). Tillsynen ska särskilt avse behandlingen av känsliga personuppgifter. Av 1 § tredje stycket framgår att tillsynen ska syfta till att säkerställa att den verksamhet

som tillsynen omfattar bedrivs i enlighet med lag eller annan författning.

Utredningen om tillsynen över den personliga integriteten föreslår att paragrafen ändras på det sättet att tillsynsområdet knyts till Säkerhetspolisens brottsbekämpande verksamhet i stället för till en uppräknings av vissa författningar. Den utredningen föreslår vidare att nämndens tillsyn över Polismyndighetens personuppgiftsbehandling ska upphöra (se SOU 2016:65 s. 23).

Utredningen delar den uppfattning som framförs av Utredningen om tillsynen över den personliga integriteten om att tillsynsområdet inte bör knytas till en uppräknings av författningar. Säkerhetspolisens personuppgiftsbehandling kommer till allra största delen att regleras i Säkerhetspolisens datalag. Tillämpningsområdet för den lagen utgår från personsuppgiftsbehandling som rör nationell säkerhet. Tillsynsområdet bör anpassas till det. Nämnden bör således utöva tillsyn över Säkerhetspolisens personuppgiftsbehandling som rör nationell säkerhet i brottsbekämpande och lagförande verksamhet.

Undersökningsbefogenheter

Enligt 4 § lagen om tillsyn över viss brottsbekämpande verksamhet har nämnden rätt att av de myndigheter som omfattas av tillsynen få de uppgifter och det biträde som den begär. Regleringen omfattar alla uppgifter och handlingar som nämnden bedömer behövs för tillsynen. Biträde kan bestå i att tillsynsobjekten gör lokaler, arkiv och personuppgiftssamlingar tillgängliga för nämnden (se prop. 2006/07:133 s. 68 f. och s. 82).

Lagstiftarens intentioner verkar ha varit att nämnden ska ha rätt till alla de handlingar och uppgifter som kan behövas för att klarlägga de förhållanden som nämnden har tillsyn över. Av ordalydelsen i 4 § framgår det emellertid inte tydligt att bestämmelsen även ger rätt till information som inte har direkt anknytning till personuppgiftsbehandlingen men som behövs för tillsynen. Som framgår av delbetänkandet är det viktigt (se SOU 2017:29 s. 464). Enligt utredningens mening bör det därför förtydligas att nämnden även har rätt till sådan information och andra relevanta upplysningar. Regleringen bör därför ändras så att det framgår att nämnden har

rätt till de uppgifter, upplysningar och information som den behöver för sin tillsyn.

15.7.2 Kontroll på begäran av enskild

Utredningens förslag: Säkerhets- och integritetsskyddsnamnden ska kunna vägra att utföra kontroll på begäran av enskild om begäran är orimlig eller uppenbart ogrundad.

Skälen för utredningens förslag

En begäran om kontroll bör kunna vägras

Enligt 3 § lagen om tillsyn över viss brottsbekämpande verksamhet är nämnden skyldig att på begäran av en enskild kontrollera om han eller hon har utsatts för hemliga tvångsmedel eller viss behandling av personuppgifter och om detta har skett i enlighet med lag eller annan författning. Enskild ska enligt förarbetena tolkas så att kontroll kan begäras av antingen en fysisk eller en juridisk person (se prop. 2006/07:133 s. 81). Den enskilde ska underrättas om att kontrollen har utförts. Som framgår av avsnitt 15.2.2 och 15.4.1 bör tillsynen i huvudsak vara densamma som i dag, vilket innebär att nämnden ensam ska göra sådana kontroller.

Kontroller på begäran av enskilda fyller en viktig funktion. De kan dock vara mycket resurskrävande för nämnden. Mot den bakgrunden utformades motsvarande bestämmelse i brottsdatalagen på ett annat sätt (se SOU 2017:29 s. 452). Enligt 5 kap. 3 § brottsdatalagen ska en enskild som begär kontroll visa att han eller hon först har begärt information av den personuppgiftsansvarige för att kontrollen ska utföras. Tillsynsmyndigheten får vidare vägra att utföra kontroll om begäran är orimlig eller uppenbart ogrundad.

Frågan är om det är möjligt att begränsa nämndens skyldighet att utföra kontroll på motsvarande sätt. Eftersom en enskild i princip aldrig kan få information om huruvida uppgifter om honom eller henne behandlas genom att vända sig till Säkerhetspolisen kan det inte göras till en förutsättning för kontroll. En enskild kan inte heller känna till vilka behandlingar som utförs av myndigheten. Att ställa upp krav på att en begäran preciseras eller avgränsas på lik-

nande sätt som i brottsdatalagen är därför inte möjligt. Det är då inte heller möjligt att begränsa nämndens skyldighet att utföra kontroll på begäran av enskild på det sätt som görs i brottsdatalagen (jfr SOU 2017:29 s. 452 f.).

I dag har nämnden ingen möjlighet att vägra att utföra kontroll ens om begäran om kontroll är orimlig eller uppenbart ogrundad. Det skulle enligt utredningens mening innebära en viss lättnad om nämnden åtminstone får uttryckligt stöd för att inte utföra någon kontroll i sådana fall. Som nyss nämnts kan en vägran dock inte grundas på att den enskilde inte har gjort tillräckligt för att själv klarlägga om hans eller hennes personuppgifter behandlas eller om han eller hon varit föremål för hemliga tvångsmedel.

Vid tillsyn över Säkerhetspolisen bör det t.ex. kunna ses som orimligt att kontrollera förhållanden som ligger långt tillbaka i tiden. Finns det inte längre någon möjlighet att begära skadestånd för kränkande personuppgiftsbehandling, saknas det som regel anledning att utföra kontroll. Likaså bör det kunna anses orimligt att utföra upprepade kontroller med korta tidsintervall eller beträffande frågor som redan har kontrollerats. Utredningen föreslår därför att nämnden bör ges möjlighet att vägra att utföra kontroll om begäran är orimlig eller uppenbart ogrundad. Enligt utredningens mening bör enskildas möjlighet att begära kontroll inte begränsas utöver det, mot bakgrund av rätten till ett effektivt rättsmedel enligt Europakonventionen (jfr prop. 2006/07:133 s. 64 f. och SOU 2016:65 s. 177 f.).

Nämndens avgöranden bör inte kunna överklagas

Enligt 6 § lagen om tillsyn över viss brottsbekämpande verksamhet får nämndens avgöranden inte överklagas, vilket hör samman med att dess uttalanden inte är bindande. Det får till följd att den enskilde fritt kan återkomma med begäran om ny kontroll (se prop. 2006/07:133 s. 71). En konsekvens av att införa en ordning där nämnden kan vägra att utföra kontroll är att sådana beslut inte heller kommer att kunna överklagas. Även om nämnden måste fatta beslut om att vägra utföra kontroll bedömer utredningen att den ordningen är mindre resurskrävande för nämnden än att genomföra orimliga eller uppenbart ogrundade kontroller.

15.7.3 Anmälningsskyldighet

Utredningens förslag: Nämndens skyldighet att anmäla omständigheter som bör komma till tillsynsmyndighetens kännedom ska förtydligas.

Nämndens anmälningsskyldighet till Justitiekanslern ska begränsas till frågor som nämnden uppmärksammar vid kontroll på begäran av enskild.

Skälen för utredningens förslag: Nämnden är enligt 20 § förordningen (2007:1141) med instruktion för Säkerhets- och integritetsskyddsnämnden skyldig att anmäla vissa förhållanden som det ankommer på andra myndigheter att ingripa mot.

Om nämnden finner omständigheter som Datainspektionen bör uppmärksammas på, ska nämnden anmäla det till inspektionen. Ordalydelsen ger inte något klart besked om vad skyldigheten omfattar. Utredningen om tillsynen över den personliga integriteten påtalar att Datainspektionen och nämnden tolkar skyldigheten på olika sätt men anser inte att det krävs någon ändring av bestämmelsen (se SOU 2016:65 s. 184).

Mot bakgrund av att regleringen av tillsyn i brottsdatalagen bygger på en delvis annan syn än i dag, där framför allt skillnaden mellan förebyggande och korrigerande befogenheter betonas, anser utredningen att nämndens anmälningsskyldighet bör förtydligas. Enligt utredningens mening bör nämndens skyldighet att påtala frågor som bör komma till tillsynsmyndighetens kännedom begränsas till brister som är av så allvarlig karaktär att det kan finnas skäl för tillsynsmyndigheten att överväga om någon korrigerande befogenhet behöver användas. Anmälningsskyldigheten bör alltså inte omfatta mindre allvarliga brister, men det finns naturligtvis inget som hindrar att nämnden ändå uppmärksammar tillsynsmyndigheten på sådana brister. Skyldigheten kan lämpligen utformas på det sättet att om nämnden bedömer att Säkerhetspolisen brister i sina skyldigheter vid behandling av personuppgifter på sådant sätt att korrigerande befogenheter kan behöva användas, ska nämnden anmäla det till tillsynsmyndigheten.

Om nämnden i sin verksamhet uppmärksammar förhållanden som kan medföra skadeståndsskyldighet för staten, ska nämnden enligt 20 § anmäla det till Justitiekanslern. Anmälningsskyldigheten

omfattar alla felaktigheter som nämnden upptäcker i sin tillsynsverksamhet. När en sådan anmälan görs leder det till att integritetskänsliga uppgifter om en person kan komma att spridas utan hans eller hennes vetskap eller vilja. Om nämnden t.ex. upptäcker att känsliga personuppgifter har behandlats felaktigt är det inte självklart att den berörde vill att någon utomstående ska få kännedom om det, vilket kan bli följden av en anmälan till Justitiekanslern. Det bör inte krävas att nämnden alltid tar kontakt med den berörde för att höra om han eller hon är intresserad av eventuell möjlighet att kräva staten på skadeståndsansättning. Mot den bakgrunden anser utredningen att bestämmelsen om nämndens anmälningskyldighet till Justitiekanslern bör begränsas till de situationer där den enskilde själv har vänt sig till nämnden med begäran om kontroll enligt 3 § lagen om tillsyn över viss brottsbekämpande verksamhet. Han eller hon får då anses ha gett uttryck för att eventuella felaktigheter ska föranleda någon form av reaktion.

16 Register över tillträdesförbud vid idrottsarrangemang

16.1 Nuvarande reglering

16.1.1 Tillträdesförbudsregistret

Förutsättningarna för beslut om tillträdesförbud

Enligt 1 § lagen (2005:321) om tillträdesförbud vid idrottsarrangemang får en person förbjudas att få tillträde till och vistas på en inhägnad plats som huvudsakligen är avsedd för idrottsutövning när idrottsarrangemang anordnas på platsen av en idrottsorganisation, s.k. tillträdesförbud. Det gäller även om allmänheten har tillträde till platsen.

För att en person ska kunna meddelas tillträdesförbud ska det på grund av särskilda omständigheter finnas risk att han eller hon kommer att begå brott under idrottsarrangemang som anordnas av en idrottsorganisation på en inhägnad plats huvudsakligen avsedd för idrottsutövning och att brottet är ägnat att störa ordningen eller säkerheten där.

Frågor om tillträdesförbud prövas av åklagare, som kan utfärda tillträdesförbud för viss tid, högst tre år med möjlighet till förlängning. Åklagarens beslut kan prövas av allmän domstol. Den som bryter mot ett tillträdesförbud döms för överträdelse av tillträdesförbud till böter eller fängelse i högst sex månader.

Tillträdesförbudsregistrets syfte och innehåll

I samband med att reglerna om tillträdesförbud skärptes år 2015 infördes särskilda regler om registrering av sådana förbud. Lagen (2015:51) om register över tillträdesförbud vid idrottsarrangemang

syftar enligt 1 § till att ge dels Polismyndigheten, dels idrottsorganisationer möjlighet att behandla personuppgifter för att på ett ändamålsenligt sätt kunna upprätthålla gällande beslut om tillträdesförbud vid idrottsarrangemang. Lagen gäller enligt 4 § utöver personuppgiftslagen. Det innebär att om det inte finns avvikande bestämmelser i lagen eller föreskrifter som har meddelats med stöd av den ska personuppgiftslagen tillämpas.

Polismyndigheten för enligt 2 § ett särskilt register, tillträdesförbudsregistret. Det får enligt 8 § endast innehålla de uppgifter om en person som har meddelats tillträdesförbud

1. som behövs för de ändamål för vilka Polismyndigheten får föra registret och
2. som avser
 - a) namn,
 - b) personnummer eller samordningsnummer,
 - c) folkbokföringsadress och annan stadigvarande adress,
 - d) alias,
 - e) fotografi,
 - f) anknytning till idrott och idrottsorganisation,
 - g) omfattningen och giltighetstiden av beslut om tillträdesförbud, och
 - h) överträdelse av gällande tillträdesförbud.

En uppgift i tillträdesförbudsregistret ska enligt 12 § gallras om uppgiften inte längre behövs för något av de ändamål för vilka Polismyndigheten får behandla personuppgifter enligt lagen. Uppgifterna ska dock gallras senast när tillträdesförbudets giltighetstid löper ut eller om tillträdesförbudet dessförinnan upphävs.

16.1.2 Polismyndighetens roll

Enligt 3 § gäller lagen vid Polismyndighetens behandling av personuppgifter i tillträdesförbudsregistret. Lagen gäller vid behandling som är helt eller delvis automatiserad eller om personuppgifterna

ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier. Polismyndigheten är enligt 5 § personuppgiftsansvarig för den personuppgiftsbehandling som myndigheten utför enligt lagen.

Polisdatalagen är tillämplig på behandling av personuppgifter som rör tillträdesförbud och som inte utförs i tillträdesförbudsregistret. Polisdatalagen tillämpas således dels i sådana utredningar som ska föregå beslut om tillträdesförbud, dels vid utredning av överträdelser av tillträdesförbud.

Polismyndigheten får enligt 6 § behandla personuppgifter i tillträdesförbudsregistret om det behövs för att förebygga, förhindra eller upptäcka överträdelser av tillträdesförbud. Personuppgifter som behandlas enligt 6 § får också behandlas av Polismyndigheten för att dels tillhandahålla idrottsorganisationer den information som behövs för att de ska kunna upprätthålla gällande tillträdesförbud, dels fullgöra myndighetens uppgiftslämnande enligt lag eller förordning. I övrigt gäller 9 § första stycket d och andra stycket personuppgiftslagen.

Personuppgifter får enligt 10 § lagen om register över tillträdesförbud vid idrottsarrangemang lämnas ut på medium för automatiserad behandling.

Enligt 11 § ska tillgången till personuppgifter begränsas till vad den som arbetar vid Polismyndigheten behöver för att kunna fullgöra sina arbetsuppgifter.

I förarbetena framhålls att Polismyndighetens behandling av personuppgifter enligt lagen åtminstone delvis är brottsbekämpande (se Register över tillträdesförbud vid idrottsarrangemang, prop. 2013/14:254, s. 43).

16.1.3 Idrottsorganisationernas roll

En idrottsorganisation får enligt 7 § lagen om register över tillträdesförbud vid idrottsarrangemang behandla personuppgifter från tillträdesförbudsregistret om det behövs för att förebygga, förhindra eller upptäcka överträdelser av tillträdesförbud vid ett idrottsarrangemang som organisationen anordnar. En sådan organisation har också enligt 9 § rätt att ta del av uppgifter i tillträdesförbuds-

registret trots att det enligt 35 kap. 4 a § offentlighets- och sekretesslagen gäller sekretess för uppgifterna.

Tillgången till personuppgifter ska enligt 11 § begränsas till vad den som arbetar eller utför uppdrag åt en idrottsorganisation behöver för att kunna fullgöra arbetsuppgifterna eller uppdraget.

En uppgift som en idrottsorganisation har fått tillgång till från tillträdesförbudsregistret ska enligt 13 § tas bort om uppgiften inte längre behövs för de ändamål för vilka idrottsorganisationen får behandla uppgifter. Uppgifterna ska dock tas bort senast när tillträdesförbudets giltighetstid löper ut eller om tillträdesförbudet dessförinnan upphävs.

Den som arbetar eller utför uppdrag åt en idrottsorganisation och som tar befattning med en uppgift som har inhämtats med stöd av lagen får enligt 14 § inte obehörigen röja vad han eller hon fått veta om någon enskilds personliga förhållanden. Tystnadsplikten har ett vidare tillämpningsområde och träffar inte bara den som behandlar personuppgifter (se prop. 2013/14:254 s. 25).

16.2 Två olika regleringar

Utredningens förslag: Polismyndighetens behandling av personuppgifter i tillträdesförbudsregistret ska regleras i polisens brottsdatalag, medan lagen om register över tillträdesförbud vid idrottsarrangemang i fortsättningen bara ska reglera idrottsorganisationernas behandling av personuppgifter. Lagen ska benämnas lagen om idrottsorganisationers behandling av uppgifter om tillträdesförbud. Bestämmelserna i lagen som rör Polismyndighetens personuppgiftsbehandling ska upphävas.

Skälen för utredningens förslag

Ändrade förutsättningar

EU:s dataskyddsreform medför skillnader mellan behandling av personuppgifter som regleras i brottsdatalagen och dataskyddsförordningen. Som framgår av bl.a. avsnitt 9.1.2 får det framför allt betydelse för anpassningen av sådana författningar som reglerar personuppgiftsbehandling både inom och utanför brottsdatalagens

tillämpningsområde. Hit hör lagen om register över tillträdesförbud vid idrottsarrangemang, eftersom den både reglerar Polismyndighetens och idrottsorganisationernas behandling av personuppgifter. I delbetänkandet konstaterar utredningen att idrottsorganisationernas behandling av personuppgifter enligt lagen ligger utanför brottsdatalagens tillämpningsområde, eftersom någon myndighetsutövning inte har överlåtits till dem (se SOU 2017:29 s. 229).

Det sagda innebär att idrottsorganisationer som utgångspunkt ska tillämpa dataskyddsförordningen med kompletterande lagstiftning vid behandling av personuppgifter som härrör från tillträdesförbudsregistret. Som framgår av Dataskyddsutredningens betänkande finns det inget som hindrar att Sverige i viss utsträckning behåller särreglering även inom dataskyddsförordningens tillämpningsområde (se SOU 2017:39 s. 78 f.).

Det finns enligt utredningens mening starka skäl för att behålla den särskilda regleringen av hur idrottsorganisationer får behandla personuppgifter som härrör från tillträdesförbudsregistret. Det är uppgifter som kan vara integritetskänsliga. Är det fråga om uppgifter om överträdelse av tillträdesförbud avser uppgifterna lagöverträdelser. För att idrottsorganisationerna ska kunna behandla uppgifter om lagöverträdelser i samma utsträckning som i dag krävs det särreglering.

I delbetänkandet konstaterar utredningen att behöriga myndigheters behandling av personuppgifter som rör tillträdesförbud ligger inom brottsdatalagens tillämpningsområde, eftersom den inte bara omfattar brottsbekämpning utan även upprätthållande av allmän ordning och säkerhet (se SOU 2017:29 s. 228 f.). Bestämmelserna om Polismyndighetens personuppgiftsbehandling i tillträdesförbudsregistret behöver därmed anpassas till brottsdatalagen.

Bör dagens reglering behållas?

I förarbetena till lagen om register över tillträdesförbud vid idrottsarrangemang redovisas inte skälen för att lagstiftaren valde att reglera både Polismyndighetens och idrottsorganisationernas behandling av personuppgifter i samma författning. Det mesta talar dock för att det ansågs vara en praktisk lösning.

Om samma lagtekniska lösning skulle gälla även fortsättningsvis måste Polismyndighetens personuppgiftsbehandling regleras så att bestämmelserna gäller utöver brottsdatalagen, medan idrottsorganisationernas personuppgiftsbehandling ska förhålla sig till data-skyddsförordningen och den svenska lagstiftning som kompletterar den. Det skulle i och för sig vara möjligt att skapa en sådan reglering, t.ex. genom att dela in lagen i kapitel och låta dem förhålla sig till respektive lagstiftning. Det är emellertid enligt utredningens mening svårt att finna några övertygande skäl för att behålla en gemensam reglering. Varken handläggningsskäl eller effektivitetsskäl talar för det. Lagtekniska skäl talar också mot det, om det går att finna en annan rimlig lösning.

För idrottsorganisationerna regleras framför allt hur uppgifter som härrör från tillträdesförbudsregistret får behandlas. Motsvarande regelverk finns normalt inte i de författningar som reglerar myndighetsregister. Även det talar mot att behålla den nuvarande författningsstrukturen.

Utredningens slutsats är att den nuvarande regleringen bör delas upp på två olika regelverk – ett för Polismyndighetens personuppgiftsbehandling och ett för idrottsorganisationernas personuppgiftsbehandling.

Polismyndighetens personuppgiftsbehandling regleras i polisens brottsdatalag

Utgångspunkten för lagstiftaren var enligt förarbetena till polisdatalagen att bestämmelserna om Polismyndighetens behandling av personuppgifter så långt möjligt ska vara samlade i den lagen. Det ansågs enligt förarbetena inte lämpligt att föra in regleringen av vissa register i polisdatalagen (se prop. 2009/10:85 s. 76 f.). I dag undantas i 1 kap. 3 § polisdatalagen behandling av personuppgifter i bl.a. tillträdesförbudsregistret från lagens tillämpningsområde. Skälen för det är framför allt att lagen om register över tillträdesförbud vid idrottsarrangemang bara till viss del ansågs kunna hänföras till brottsbekämpning. För att inte fler än en författning skulle vara tillämplig på samma behandling av personuppgifter undantogs behandlingen i registret från polisdatalagens tillämpningsområde (se prop. 2013/14:254 s. 43).

Även om lagstiftningen om tillträdesförbudsregistret är relativt ny, anser utredningen att det finns skäl att på nytt överväga frågan om bestämmelserna om Polismyndighetens behandling av personuppgifter i tillträdesförbudsregistret kan föras in i polisens brottsdatalag. Det är möjligt att arbeta in bestämmelserna i den lagen när den genom dataskyddsreformen får ett bredare tillämpningsområde och även omfattar upprätthållande av allmän ordning och säkerhet (se avsnitt 7.1.2). Det tidigare hindret mot att reglera all Polismyndighetens personuppgiftsbehandling i samma författning har därmed undanröjts. En förutsättning för att föra över regleringen till polisens brottsdatalag bör dock vara att tillträdesförbudsregistret alltjämt regleras som ett särskilt register.

Om bestämmelserna om Polismyndighetens behandling av personuppgifter i tillträdesförbudsregistret upphävs och motsvarande bestämmelser införs i polisens brottsdatalag kan lagen om register över tillträdesförbud vid idrottsarrangemang renodlas till att enbart omfatta idrottsorganisationernas personuppgiftsbehandling. Utredningen anser att det är den bästa lösningen.

Idrottsorganisationernas personuppgiftsbehandling

Den som anordnar en offentlig tillställning, exempelvis sporttävlingar, ansvarar enligt 2 kap. 16 § ordningslagen (1993:1617) för att det gäller god ordning vid tillställningen. Polismyndigheten får meddela de villkor som behövs för att upprätthålla ordning och säkerhet vid tillställningen. Ansvaret för att idrottsarrangemang kan anordnas på ett tryggt sätt med hög säkerhet för såväl aktiva som publik vilar alltså i första hand på de arrangerande idrottsorganisationerna (se prop. 2013/14:254 s. 19). Det är också de som ska se till att gällande tillträdesförbud respekteras. Det är av det skälet som idrottsorganisationerna ges tillgång till uppgifter om tillträdesförbud. Att arrangörerna har kännedom om vilka personer som har tillträdesförbud och kan identifiera dem vid inpasseringskontrollen ger möjlighet att hindra att personer med tillträdesförbud släpps in när ett idrottsarrangemang äger rum.

I avsnitt 6.4.1 redovisar utredningen vilka rättsliga grunder som är tillåtna enligt dataskyddsförordningen. Enligt artikel 6.1 e är det bl.a. om behandlingen är nödvändig för att utföra en uppgift av

allmänt intresse och enligt artikel 6.1 c om behandlingen är nödvändig för att fullgöra en rättslig förpliktelse. Enligt artikel 6.3 ska den rättsliga grunden för sådan behandling fastställas i enlighet med unionsrätten eller nationell rätt.

Idrottsorganisationernas uppgift att förebygga och förhindra ordningsstörningar vid idrottsarrangemang genom att se till att utfärdade tillträdesförbud får effekt innebär enligt utredningens mening att idrottsorganisationerna utför en uppgift av allmänt intresse. Som redovisas närmare i förarbetena till lagen om register över tillträdesförbud vid idrottsarrangemang är det då nödvändigt att de kan behandla vissa personuppgifter rörande dem som har meddelats tillträdesförbud. Utredningen anser därför att reglerna om idrottsorganisationernas rätt att behandla vissa personuppgifter i lagen kan behållas. Viss anpassning av bestämmelserna kan dock krävas. Utredningen återkommer till det i avsnitt 16.4.

Idrottsorganisationernas personuppgiftsbehandling bör enligt utredningens mening även fortsättningsvis regleras i lagen om register över tillträdesförbud vid idrottsarrangemang. Om lagen renodlas på det sättet att bestämmelserna om Polismyndighetens behandling av personuppgifter om tillträdesförbud i sin helhet regleras i polisens brottsdatalag bör dock namnet på lagen ändras. Den bör benämnas lagen om idrottsorganisationers behandling av uppgifter om tillträdesförbud.

16.3 Regleringen för Polismyndigheten

Utredningens förslag: De nuvarande bestämmelserna om rätten att föra tillträdesförbudsregistret, för vilka ändamål personuppgifter får behandlas i registret, dess innehåll, hur länge uppgifterna får behandlas, under vilka förutsättningar de får lämnas ut och den sekretessbrytande bestämmelsen ska flyttas till polisens brottsdatalag.

Skälen för utredningens förslag

Bestämmelser flyttas till polisens brottsdatalog

Som framgår av avsnitt 16.2 är syftet med Polismyndighetens behandling av personuppgifter i tillträdesförbudsregistret sådant att det ligger inom brottsdatalogens tillämpningsområde. De nuvarande bestämmelserna om Polismyndighetens behandling av personuppgifter i tillträdesförbudsregistret bör oförändrade i sak föras över till polisens brottsdatalog. De bör placeras i det kapitel där vissa andra register som myndigheten för särregleras. Härigenom kommer fortsättningsvis all behandling av personuppgifter som Polismyndigheten utför när det gäller tillträdesförbud att regleras i den lagen.

Många bestämmelser som i dag reglerar Polismyndighetens behandling av personuppgifter i tillträdesförbudsregistret blir emellertid överflödiga om regleringen flyttas till polisens brottsdatalog, eftersom motsvarande bestämmelser redan finns antingen i den lagen eller brottsdatalogen. Det gäller bl.a. bestämmelserna om att behandlingen enligt huvudregeln ska vara automatiserad, om personuppgiftsansvar och om tillgången till personuppgifter. De kan därför upphävas utan att ersättas. Det behövs inte heller någon särskild bestämmelse om rättelse eller skadestånd.

De bestämmelser som bör flyttas till polisens brottsdatalog, och i förekommande fall anpassas, är bestämmelserna om rätten att föra tillträdesförbudsregistret (2 §), för vilka ändamål personuppgifter får behandlas i registret (6 §), dess innehåll (8 §) och hur länge uppgifterna får behandlas (12 §). Någon förändring i sak bör inte göras, men bestämmelserna behöver anpassas till polisens brottsdatalog. Det innebär bl.a. att gallringsbestämmelsen, av de skäl som anges i avsnitt 5.5.2, bör göras om till en bestämmelse om längsta tid för behandling.

Även den sekretessbrytande bestämmelsen, som ger idrottsorganisationer rätt att ta del av uppgifter ur registret trots den sekretess som gäller för sådana uppgifter (9 §), bör flyttas till polisens brottsdatalog. Bestämmelsen, som bör placeras i 2 kap. tillsammans med övriga sekretessbrytande regler, bör inte ändras i sak.

Förslagen kräver vissa följdändringar i förordningen (2015:54) om register över tillträdesförbud vid idrottsarrangemang.

16.4 Regleringen för idrottsorganisationerna

Utredningens förslag: En bestämmelse som anger hur lagen om idrottsorganisationers behandling av uppgifter om tillträdesförbud förhåller sig till dataskyddsförordningen och kompletterande nationell lagstiftning ska införas.

Skälen för utredningens förslag: Lagen om register över tillträdesförbud vid idrottsarrangemang gäller i dag utöver personuppgiftslagen. Den hänvisningen bör av de skäl som anges i avsnitt 5.3.1 upphävas, eftersom personuppgiftslagen upphör att gälla när dataskyddsförordningen ska börja tillämpas. Det bör i stället införas en bestämmelse som upplyser om att dataskyddsförordningen gäller och att, om det inte finns särregler i lagen, den kompletterande lagstiftningen ska tillämpas vid idrottsorganisationers behandling av uppgifter som rör tillträdesförbud. Vidare bör gallringsbestämmelsen, av de skäl som anges i avsnitt 5.5.2, göras om till en bestämmelse om längsta tid för behandling. I övrigt kan bestämmelserna om idrottsorganisationers behandling av personuppgifter enligt utredningens mening behållas oförändrade. På grund av att bestämmelserna om Polismyndighetens behandling av personuppgifter bryts ut krävs det omfattande redaktionella ändringar i lagen.

16.5 Följdändringar

Utredningens förslag: Hänvisningar till lagen om register över tillträdesförbud vid idrottsarrangemang ska ändras till hänvisningar till polisens brottsdatalog.

Skälen för utredningens förslag

Sekretessen för uppgifter i tillträdesförbudsregistret

Sekretessen för uppgifter i tillträdesförbudsregistret regleras i 35 kap. 4 a § offentlighets- och sekretesslagen. Den gäller i verksamhet som avser förande av register enligt lagen om register över

tillträdesförbud vid idrottsarrangemang för uppgift om enskildas personliga förhållanden, om det inte står klart att uppgiften kan röjas utan men för den enskilde eller någon närstående. För uppgift i en allmän handling gäller sekretessen i högst sjuttio år.

Om bestämmelserna om tillträdesförbudsregistret flyttas till polisens brottsdatalog, och regleras i 5 kap. (nuvarande 4 kap.) tillsammans med vissa andra register, kan det diskuteras om den särskilda sekretessbestämmelsen behövs. Enligt 35 kap. 1 § offentlighets- och sekretesslagen gäller sekretess för bl.a. uppgift om enskilds personliga eller ekonomiska förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till honom eller henne lider skada eller men och uppgiften förekommer i register som Polismyndigheten för enligt 4 kap. polisdatalagen. För uppgift i en allmän handling gäller sekretessen i högst sjuttio år.

Den särskilda sekretessbestämmelsen för tillträdesförbudsregistret är dock inte identisk med den som gäller för övriga register som nu regleras i 4 kap. polisdatalagen. Skaderekvisitet i 35 kap. 1 § är vidare och omfattar både skada och men. Föremålet för sekretessen skiljer sig också på det sättet att sekretessen i 35 kap. 4 a § enbart skyddar enskilds personliga förhållanden, medan sekretessen i 35 kap. 1 § skyddar enskilds personliga och ekonomiska förhållanden. Utredningen anser därför att den särskilda sekretessbestämmelsen för tillträdesförbudsregistret bör behållas men en hänvisning behöver ändras när regleringen flyttas.

Lagen och förordningen om tillträdesförbud vid idrottsarrangemang

I 8 a § lagen om tillträdesförbud vid idrottsarrangemang föreskrivs att en polisman eller annan anställd vid Polismyndigheten får fotografera en person som har eller skäligen kan antas få tillträdesförbud enligt lagen, för att fotografiet ska kunna tillföras tillträdesförbudsregistret. Eftersom regleringen av tillträdesförbudsregistret flyttas bör hänvisningen till lagen om register över tillträdesförbud vid idrottsarrangemang ändras. Det krävs även ändringar i förordningen (2005:323) om tillträdesförbud vid idrottsarrangemang.

17 Övriga författningsändringar

17.1 Tystnadsplikt för dataskyddsbud

Utredningens förslag: Den som fullgör uppgift som dataskyddsbud ska inte obehörigen få röja eller utnyttja det som han eller hon har fått veta om enskilds personliga eller ekonomiska förhållanden.

I det allmännas verksamhet ska offentlighets- och sekretesslagen tillämpas.

Skälen för utredningens förslag

Behovet av en bestämmelse om tystnadsplikt

Det är inte bara myndigheterna i rättskedjan som ska tillämpa brottsdatalagen utan även andra myndigheter. I vissa fall ska även andra aktörer tillämpa lagen. I delbetänkandet föreslår utredningen att alla som tillämpar brottsdatalagen ska utse dataskyddsbud och anmäla till tillsynsmyndigheten när dataskyddsbud utses och entledigas (se SOU 2017:29 s. 340 f.). Det gäller således även andra aktörer än myndigheter.

Utredningen konstaterar i delbetänkandet att det kommer att krävas en regel om tystnadsplikt för dataskyddsbud som inte ska tillämpa offentlighets- och sekretesslagen. Eftersom det är önskvärt att en sådan regel utformas på samma sätt för både dataskyddsförordningens och brottsdatalagens tillämpningsområden valde utredningen att avvakta Dataskyddsutredningens förslag (se SOU 2017:29 s. 631 f.).

Dataskyddsutredningens förslag

Dataskyddsutredningen gör följande bedömning när det gäller dataskyddsbud som inte är offentliganställda (se SOU 2017:39 s. 263).

Dataskyddsbudets ställning kan i vissa avseenden likställas med revisorns eller skyddsbudets, och tystnadsplikten för dataskyddsbud bör därför utformas på ett liknande sätt. Tystnadsplikten ska således avgränsas med ett obehörighetsrekvisit vilket bland annat innebär att uppgifter kan lämnas ut med samtycke, till tillsynsmyndighet eller annars som en följd av en skyldighet i lag eller författning.

Bestämmelsen om tystnadsplikt för dataskyddsbud bör enligt Dataskyddsutredningen utformas på följande sätt (se SOU 2017:39 s. 40).

Den som utsetts till dataskyddsbud enligt artikel 37 i dataskyddsförordningen får inte obehörigen röja det som han eller hon vid fullgörandet av sin uppgift har fått veta om enskilds personliga och ekonomiska förhållanden.

I det allmännas verksamhet tillämpas offentlighets- och sekretesslagen.

En bestämmelse om tystnadsplikt införs i brottsdatalagen

Dataskyddsbud som utses av myndigheter ska tillämpa bestämmelserna i offentlighets- och sekretesslagen. Det behövs enligt utredningens mening inte någon ytterligare reglering av deras tystnadsplikt. Dataskyddsutredningen gör samma bedömning när det gäller dataskyddsförordningens tillämpningsområde.

De dataskyddsbud som kommer att vara verksamma inom brottsdatalagens tillämpningsområde och som inte träffas av regleringen i offentlighets- och sekretesslagen kommer sannolikt att ha uppgifter enligt både den lagen och dataskyddsförordningen. Det är då lämpligt att reglerna om tystnadsplikt är utformade på samma sätt. Bestämmelsen om tystnadsplikt för dataskyddsbud bör därför utformas efter mönster av den bestämmelse som Dataskyddsutredningen föreslår. Det innebär att regleringen bör utgå från ett obehörighetsrekvisit och föreskriva att den som fullgör uppgift som dataskyddsbud inte obehörigen får röja eller utnyttja det som han eller hon har fått veta om enskilds personliga

och ekonomiska förhållanden. Bestämmelsen bör placeras i 3 kap. brottsdatalagen.

17.2 Sekretessfrågor

17.2.1 Följändringar i offentlighets- och sekretesslagen

Utredningens förslag: Hänvisningar i offentlighets- och sekretesslagen till de registerförfattningar vilkas namn byts ut ska ändras. Andra hänvisningar ska också ändras.

Skälen för utredningens förslag: Ett flertal paragrafer i offentlighets- och sekretesslagen innehåller hänvisningar till en eller flera av de registerförfattningar som utredningen föreslår ska anpassas till brottsdatalagen. Det gäller 18 kap. 2 och 18 §§, 35 kap. 1 och 10 §§ och 37 kap. 7 §. I 35 kap. 1 och 10 §§ offentlighets- och sekretesslagen nämns polisens, Skatteverkets, Tullverkets, Kustbevakningens och åklagarväsendets registerförfattningar vid namn. Vissa av dem nämns på motsvarande sätt i 18 kap. 2 §. Eftersom utredningen föreslår att registerförfattningarna ska få nya namn behöver hänvisningarna i dessa paragrafer ändras. Det gäller även hänvisningar till kapitel och paragrafer i vissa av lagarna. Ändringarna i polisdatalagen innebär vidare att kapitelnumreringen ändras. Hänvisningen i 35 kap. 1 § till 4 kap. polisdatalagen behöver därmed ändras. Som framgår av avsnitt 16.5 behöver även hänvisningarna i 35 kap. 4 a § och 10 b § ändras med anledning av de ändringar som föreslås beträffande regleringen av tillträdesförbudsregistret.

På motsvarande sätt behöver hänvisningarna till den reglering som gäller för Säkerhetspolisen ändras i 18 kap. 2 § och 35 kap. 1 § offentlighets- och sekretesslagen. Ett tillägg bör också göras i 35 kap. 10 §, eftersom Säkerhetspolisens personuppgiftsbehandling föreslås regleras i en särskild lag.

17.2.2 Sekretess för uppgifter i verksamhet för teknisk bearbetning och lagring

Utredningens bedömning: Bestämmelsen om sekretess i verksamhet för enbart teknisk bearbetning eller teknisk lagring för någon annans räkning behöver inte ändras.

Skälen för utredningens bedömning: Enligt 40 kap. 5 § offentlighets- och sekretesslagen gäller sekretess i verksamhet som består av enbart teknisk bearbetning eller teknisk lagring för någon annans räkning av sådana personuppgifter som avses i personuppgiftslagen. Sekretessen gäller oavsett om det är fråga om bearbetning eller lagring för en annan myndighets räkning eller för enskildas räkning. Med teknisk bearbetning avses t.ex. att text på papper scannas in för att lagras elektroniskt. Teknisk lagring avser alla former av lagring som kräver särskilda tekniska anordningar, t.ex. lagring av information på hårddisk eller i molntjänster. Sekretessbestämmelsen hänvisar i fråga om personuppgifter till personuppgiftslagen. Sekretessen, som är absolut, skyddar uppgifter om enskildas personliga och ekonomiska förhållanden.

Dataskyddsutredningen föreslår att hänvisningen till personuppgiftslagen i 40 kap. 5 § offentlighets- och sekretesslagen ska ersättas med en dynamisk hänvisning till artikel 4.1 i dataskyddsförordningen (se SOU 2017:39 s. 52 och 270 f.). Som framgår av delbetänkandet är det inte ovanligt att myndigheter agerar personuppgiftsbiträden åt varandra eller på annat sätt biträder med teknisk bearbetning eller annan behandling av personuppgifter inom brottsdatalagens tillämpningsområde (se SOU 2017:29 s. 351). Dataskyddsutredningens förslag innebär att sekretessen i 40 kap. 5 § inte längre skulle omfatta teknisk bearbetning eller teknisk lagring inom brottsdatalagens tillämpningsområde. Om det förslaget skulle genomföras skulle det därför behövas en hänvisning även till brottsdatalagen i paragrafen.

I propositionen Utökad sekretesskydd i verksamhet för teknisk bearbetning och lagring föreslår regeringen emellertid att kopplingen till personuppgiftsbehandling ska upphöra och att sekretessen ska gälla generellt för alla uppgifter om enskilds personliga eller ekonomiska förhållanden i sådan verksamhet (se prop. 2016/17:198 s. 15 f.). Där föreslås också en ny bestämmelse om överföring av

sekretess. Om en myndighet, i verksamhet för enbart teknisk bearbetning eller teknisk lagring, för en annan myndighets räkning får en uppgift som hos sistnämnda myndighet är sekretessbelagd av hänsyn till ett allmänt intresse, ska sekretessbestämmelsen även tillämpas hos den mottagande myndigheten. Lagändringarna föreslås träda i kraft den 1 januari 2018.

Under förutsättning att förslaget till ändring av 40 kap. 5 § offentlighets- och sekretesslagen antas av riksdagen knyts sekretessen inte längre till behandling av personuppgifter. Det finns då inget behov av att ändra bestämmelsen på det sätt som utredningen i delbetänkandet förutsåg kunde bli nödvändigt.

17.2.3 Sekretess för uppgifter som behandlas i strid med personuppgiftsregleringen

Utredningens bedömning: Sekretessen för personuppgifter som behandlas i strid med personuppgiftsregleringen behöver inte ändras.

Skälen för utredningens bedömning: Enligt 21 kap. 7 § offentlighets- och sekretesslagen gäller sekretess för personuppgift om det kan antas att utlämnande skulle medföra att uppgifter behandlas i strid med personuppgiftslagen. Dataskyddsutredningen föreslår att bestämmelsen ändras. Förslaget innebär för det första att det tydliggörs att det som sekretessen syftar till att skydda är att personuppgiften behandlas i strid med personuppgiftsregleringen efter det att den har lämnats ut. Vidare föreslås att hänvisningen till personuppgiftslagen byts ut mot dels en statisk hänvisning till dataskyddsförordningen, dels en hänvisning till lagen (2018:000) med kompletterande bestämmelser till EU:s dataskyddsförordning (se SOU 2017:39 s. 265 f.).

Den fråga som väcks är om det förhållandet att det när personuppgiftslagen upphör att gälla kommer att finnas två olika regelverk för personuppgiftsbehandling (dels dataskyddsförordningen med kompletterande nationell lagstiftning, dels brottsdatalagen) bör föranleda någon ändring i 21 kap. 7 § offentlighets- och sekretesslagen.

Syftet med sekretessbestämmelsen är att skydda mot att personuppgifter som lämnas ut kommer att behandlas i strid med personuppgiftsregleringen. Förslaget till ändring av paragrafen innebär att det tydliggörs att den tar sikte på den personuppgiftsbehandling som utförs efter utlämnandet. Man kan enligt utredningens mening utgå från att de som kan antas komma att behandla personuppgifter i strid med regelverket om de får tillgång till personuppgifter som har behandlats med stöd av brottsdatalagen eller någon av registerförfattningarna ska tillämpa dataskyddsförordningen. Det är därför tillräckligt att det i sekretessbestämmelsen hänvisas till det regelverket. Någon ändring i paragrafen, utöver det som Data- skyddsutredningen föreslår, behövs därför inte.

17.2.4 Sekretess för personuppgiftsincidenter

Utredningens bedömning: Det finns inte skäl att ändra sekretessregleringen för personuppgiftsincidenter.

Skälen för utredningens bedömning: I delbetänkandet konstaterar utredningen att det i dag gäller viss sekretess för rapporter om it-incidenter enligt 18 kap. offentlighets- och sekretesslagen. Sekretessen i 18 kap. 1 och 2 §§ skyddar uppgifter i brottsanmälningar. Sekretessen i 18 kap. 3 § kompletterar den sekretessen och skyddar det underlag för en brottsanmälan som tas fram av en myndighet som avser att göra en sådan anmälan. Det sekretesskyddet gäller hos alla myndigheter, oberoende av deras arbetsuppgifter. Enligt utredningens mening är den nuvarande sekretessen tillräcklig för att skydda uppgifter om sådana personuppgiftsincidenter som kan utgöra brott (se SOU 2017:29 s. 645 f.).

Utredningen redogör också för sekretessen enligt 18 kap. 8 § 3 offentlighets- och sekretesslagen som gäller för uppgift som lämnar eller kan bidra till upplysning om säkerhets- eller bevakningsåtgärd, om det kan antas att syftet med åtgärden motverkas om uppgiften röjs och åtgärden avser telekommunikation eller system för automatiserad behandling av information. Eftersom Utredningen om genomförande av NIS-direktivet hade i uppdrag att överväga om sekretesskyddet för rapportering av it-incidenter i 18 kap. 8 § 3 är tillräckligt ansåg vi att det inte fanns skäl att behandla frågan i del-

betänkandet men att det, beroende på vad Utredningen om genomförande av NIS-direktivet kom fram till, kunde finnas anledning att återkomma till den.

Utredningen om genomförande av NIS-direktivet anser att det nuvarande sekretessskyddet är tillräckligt och föreslår därför ingen ändring i sekretessregleringen (se SOU 2017:36 s. 253 f.). Den utredningen anser att allt tyder på att sekretessbestämmelsen också har tillämpats som det har varit avsett.

Utredningen om genomförande av NIS-direktivet hänvisar i sitt betänkande bl.a. till att Kammarrätten i Göteborg i flera avgöranden under senare år har kommit fram till att incidentrapporter omfattas av sekretess. Kammarrätten i Stockholm har däremot nyligen – utan att argumentera för varför skaderekvisitet inte var uppfyllt i det enskilda fallet – intagit ståndpunkten att uppgift om att en incidentrapport har lämnats inte skyddas av sekretess (dom den 20 april 2017 i mål 835-17). Datainspektionen har därefter i en skrivelse till Justitiedepartementet väckt frågan om skyndsamt utredning av sekretessen hos myndigheten för anmälningar om personuppgiftsincidenter (se inspektionens skrivelse den 7 juli 2017, dnr 1704-2017).

Det finns anledning att noga följa utvecklingen på området, men utredningen delar Utredningens om genomförande av NIS-direktivet uppfattning att det inte nu finns skäl att ändra regleringen avseende sekretess för personuppgiftsincidenter.

17.3 Lagen om internationellt polisiärt samarbete

Utredningens förslag: Lagen om internationellt polisiärt samarbete ska gälla utöver brottsdatalagen. Förhållandet mellan personuppgiftsregleringen i lagen och annan personuppgiftslagstiftning inom brottsdatalagens tillämpningsområde ska tydliggöras genom en bestämmelse i förstnämnda lag, där också vissa bestämmelser ska anpassas till brottsdatalagens reglering.

Bestämmelser i lagen om internationellt polisiärt samarbete som hänvisar till personuppgiftslagen i fråga om skadestånd ska i stället hänvisa till brottsdatalagen.

Skälen för utredningens förslag

Anpassningar till brottsdatalagen och registerförfattningarna

I lagen om internationellt polisiärt samarbete finns det bestämmelser om informationsutbyte i 6–10 kap. Regleringen behöver anpassas till den nya personuppgiftsregleringen i flera olika avseenden.

Av 6 kap. 1 § framgår att lagen gäller utöver polisdatalagen, kustbevakningsdatalagen och tullbrottsdatalagen. Det innebär att även de generella bestämmelserna i personuppgiftslagen som registerförfattningarna hänvisar till ska tillämpas vid behandling av personuppgifter vid internationellt polisiärt samarbete (se prop. 2010/11:129 s. 47 f). För att samma reglering som i dag ska gälla bör det föreskrivas att lagen om internationellt polisiärt samarbete ska gälla utöver brottsdatalagen. Lagen bör tillämpas i den utsträckning den innehåller bestämmelser om personuppgiftsbehandling som avviker från bestämmelserna i brottsdatalagen och de särskilt uppräknade registerförfattningarna. Där bör även Säkerhetspolisens datalag nämnas, eftersom myndighetens personuppgiftsbehandling föreslås regleras i en särskild lag (se avsnitt 14.2.2).

Hänvisningar till personuppgiftslagen

I 7 kap. 7 §, 8 kap. 3 §, 9 kap. 5 § och 10 kap. 3 § lagen om internationellt polisiärt samarbete finns det bestämmelser som hänvisar till personuppgiftslagens bestämmelser om rättelse och skadestånd. De bestämmelserna bör ersättas med hänvisningar till brottsdatalagen. När det gäller rättelse behövs inte någon hänvisning, eftersom lagen om internationellt polisiärt samarbete föreslås gälla utöver brottsdatalagen och den innehåller generella bestämmelser om rättelse. På samma sätt som i registerförfattningarna bör hänvisningarna till personuppgiftslagens bestämmelse om skadestånd ändras till hänvisningar till bestämmelsen om skadestånd i 7 kap. 1 § brottsdatalagen. Av de skäl som anges i avsnitt 5.4.3 bör Justitiekanslern handlägga sådana skadeståndsanspråk.

I 9 kap. 4 § och 10 kap. 1 § lagen om internationellt polisiärt samarbete finns det hänvisningar till reglerna i 33 och 34 §§ personuppgiftslagen om överföring av personuppgifter till tredjeland. De hänvisningarna bör upphävas. Hänvisningen i 9 kap. 4 § bör

ersättas med en hänvisning till motsvarande bestämmelser i brottsdatalagen. Frågan är hur hänvisningen bör utformas, eftersom reglerna i personuppgiftslagen utgår från ett förbud mot överföring, medan brottsdatalagen reglerar när överföring är tillåten. Utredningen anser att den lämpligaste lösningen är att i 9 kap. 4 § hänvisa till bestämmelsen om grundläggande förutsättningar för överföring av personuppgifter i 8 kap. 1 § brottsdatalagen. Då ger regleringen i princip samma skydd som i dag. När det gäller hänvisningen i 10 kap. 1 § är den av en annan karaktär. Den hör samman med att 33 § personuppgiftslagen förbjuder överföring till tredjeland. Eftersom brottsdatalagen har en annan lagteknisk utformning behövs inte någon motsvarande bestämmelse. Den bör därför inte ersättas.

Viss anpassning bör också göras i förordningen (2017:504) om internationellt polisiärt samarbete.

17.4 Lagen om Polismyndighetens elimineringsdatabas

Utredningens förslag: Lagen om Polismyndighetens elimineringsdatabas ska gälla utöver brottsdatalagen. Bestämmelser som blir överflödiga till följd av det ska upphävas.

Bestämmelserna om gallring ska ändras till bestämmelser om längsta tid som personuppgifter får behandlas. Hänvisningen till personuppgiftslagens bestämmelse om skadestånd ska ändras till en hänvisning till brottsdatalagen.

Skälen för utredningens förslag

Lagen ska gälla utöver brottsdatalagen

Enligt 2 § lagen (2014:400) om Polismyndighetens elimineringsdatabas gäller lagen utöver personuppgiftslagen. Av de skäl som anges i avsnitt 5.2 bör lagen om Polismyndighetens elimineringsdatabas gälla utöver brottsdatalagen. Den paragraf som anger lagens förhållande till personuppgiftslagen bör därför ändras.

Förslaget att lagen om Polismyndighetens elimineringsdatabas ska gälla utöver brottsdatalagen innebär att 6 § om skyldighet att

utse personuppgiftsombud och 7 § om tillgången till personuppgifter inte längre behövs, eftersom det finns en generell reglering om det i brottsdatalagen. De paragraferna bör därför upphävas.

Bestämmelserna om gallring och skadestånd

I avsnitt 5.5.1 konstaterar utredningen att vissa bestämmelser om gallring inte är gallringsbestämmelser i arkivrättslig mening utan dataskyddsregler. Utredningen föreslår i avsnitt 5.5.2 att sådana bestämmelser i myndigheternas registerförfattningar ska formuleras om så att de i stället reglerar hur länge personuppgifter får behandlas. Gallringsbestämmelserna i 11 § lagen om Polismyndighetens elimineringsdatabas är enligt utredningens mening dataskyddsbestämmelser. De bör därför ändras så att de i stället anger hur länge uppgifterna i registret får behandlas.

I 12 § föreskrivs att personuppgiftslagens bestämmelser om rättelse och skadestånd ska tillämpas på motsvarande sätt vid personuppgiftsbehandling enligt lagen om Polismyndighetens elimineringsdatabas eller enligt föreskrifter som har meddelats i anslutning till den. Eftersom lagen föreslås gälla utöver brottsdatalagen behövs det ingen särskild bestämmelse om rättelse. Paragrafen bör däremot ändras på det sättet att den hänvisar till brottsdatalagens bestämmelse om skadestånd. Av de skäl som anges i avsnitt 5.4.3 bör Justitiekanslern handlägga sådana skadeståndsanspråk.

Viss anpassning bör också göras i förordningen (2014:405) om Polismyndighetens elimineringsdatabas.

17.5 Hänvisningar till 2013 års lag ska upphävas

Utredningens förslag: Kvarvarande hänvisningar till 2013 års lag ska upphävas.

Skälen för utredningens förslag: I delbetänkandet föreslår utredningen att 2013 års lag ska upphävas (se SOU 2017:29 s. 145 f.). I ett flertal lagar föreskrivs det att bestämmelserna i 2013 års lag har företräde. I delbetänkandet föreslår utredningen att hänvisningarna till 2013 års lag i lagen (2000:562) om internationell rättslig hjälp i

brottmål, lagen (2000:1219) om internationellt tullsamarbete, lagen (2003:1174) om vissa former av internationellt samarbete i brottsutredningar och lagen om internationellt polisiärt samarbete ska upphävas. Även hänvisningar i andra lagar och förordningar bör upphävas. Det som nu är aktuellt är upphävande av bestämmelser i lagen om belastningsregister, lagen om misstankeregister och lagen (2001:184) om behandling av personuppgifter i Kronofogdemyndighetens verksamhet. Den uppdrag som haft i uppdrag att anpassa domstolsdatalagen till dataskyddsförordningen föreslår att motsvarande bestämmelse i domstolsdatalagen ska upphävas, varför utredningen inte lägger fram något sådant förslag (se Ds 2017:41 s. 127).

18 Ikraftträdande och övergångsbestämmelser

18.1 Ikraftträdande

Utredningens förslag: De nya författningarna, ändringarna i de befintliga registerförfattningarna och övriga författningsförslag ska träda i kraft den 1 maj 2018.

Skälen för utredningens förslag: Brottsdatalagen föreslås träda i kraft den 1 maj 2018 (se SOU 2017:29 s. 655). Registerförfattningarna föreslås gälla utöver brottsdatalagen. De nya författningarna, ändringarna i de befintliga registerförfattningarna och övriga författningsförslag som behandlas i detta betänkande bör därför träda i kraft samma dag.

18.2 Samma övergångsbestämmelser för flertalet författningar

18.2.1 Behovet av övergångsbestämmelser

I delbetänkandet föreslår utredningen övergångsbestämmelser till brottsdatalagen (se SOU 2017:29 s. 655 f.). Viss reglering kommer i fortsättningen enbart att finnas i brottsdatalagen, medan andra bestämmelser kompletteras eller preciseras i registerförfattningarna (se avsnitt 5.2). Det kan då krävas motsvarande övergångsbestämmelser till registerförfattningarna som till brottsdatalagen. Det är framför allt bestämmelserna om skadestånd och sanktionsavgift som gör att det krävs samma typ av övergångsbestämmelser till registerförfattningarna. I kapitlen som behandlar registerförfattningarna tar utredningen enbart upp frågan om befintliga över-

gångsbestämmelser kan behållas eller måste ändras (se avsnitt 8.7 och 10.5) och om det finns behov av nya specifika övergångsbestämmelser till en viss registerförfattning (se avsnitt 12.11). Det generella behovet av övergångsbestämmelser behandlas alltså i detta avsnitt.

18.2.2 Skadestånd

Utredningens förslag: Äldre bestämmelser ska fortsätta att gälla för frågor om skadestånd för skada vid personuppgiftsbehandling enligt registerförfattningarna, om skadan har orsakats före ikraftträdandet.

Skälen för utredningens förslag: Enligt punkten 8 i övergångsbestämmelserna till brottsdatalagen ska bestämmelserna om skadestånd i 48 § personuppgiftslagen fortsätta att gälla för skada som har orsakats före ikraftträdandet av brottsdatalagen vid behandling av personuppgifter som rör brottsbekämpning, lagföring, straffverkställighet och upprätthållande av allmän ordning och säkerhet (se SOU 2017:29 s. 658 f.).

Motsvarande övergångsbestämmelser behövs i registerförfattningarna, eftersom övergångsbestämmelsen till brottsdatalagen inte täcker personuppgiftsbehandling i strid med registerförfattningarna. Sådana övergångsbestämmelser behövs även i andra författningar som gäller utöver brottsdatalagen och som hänvisar till brottsdatalagens reglering i fråga om skadestånd.

18.2.3 Sanktioner

Utredningens förslag: Sanktionsavgift ska inte få tas ut för överträdelse av bestämmelser om personuppgiftsbehandling i registerförfattningarna, om överträdelsen har begåtts före ikraftträdandet.

Äldre bestämmelser ska fortsätta att gälla för sådana överträdelser som i dag kan föranleda straffansvar enligt personuppgiftslagen och som ligger före ikraftträdandet.

Skälen för utredningens förslag: Enligt punkten 4 i övergångsbestämmelserna till brottsdatalogen får sanktionsavgift inte tas ut för överträdelse av bestämmelser om personuppgiftsbehandling som har begåtts före ikraftträdandet. Om överträdelsen var straffbelagd enligt 49 § personuppgiftslagen ska enligt punkten 5 äldre föreskrifter fortsätta att gälla (se SOU 2017:29 s. 659 f.).

Utredningen föreslår att vissa överträdelse av bestämmelser i registerförfattningarna ska kunna leda till att sanktionsavgift tas ut (se avsnitt 5.4.2 och 12.8). Av samma skäl som det behövs övergångsbestämmelser till bestämmelsen om sanktionsavgift i brottsdatalogen behövs sådana till registerförfattningarna.

Straffbestämmelsen i 49 § personuppgiftslagen gäller endast för kriminalvårdens personuppgiftsbehandling. Det är således endast till kriminalvårdens brottsdatalog som det behövs en särskild övergångsbestämmelse som anger att straffbestämmelsen ska fortsätta att tillämpas på överträdelse som begåtts före ikraftträdandet.

18.3 Övergångsbestämmelser till Säkerhetspolisens datalag och domstolarnas brottsdatalog

18.3.1 Ärendehandläggning m.m.

Utredningens bedömning: Det behövs inga övergångsbestämmelser för Säkerhetspolisens och domstolarnas behandling av personuppgifter.

Utredningens förslag: För ärenden om tillsyn över personuppgiftsbehandling som omfattas av de nya lagarnas tillämpningsområde och som inte har avgjorts när de träder i kraft ska äldre bestämmelser om handläggningen fortsätta att gälla.

Äldre bestämmelser ska också fortsätta att gälla för överklaganden och frågor om skadestånd för skada vid personuppgiftsbehandling som orsakats före ikraftträdandet.

Skälen för utredningens bedömning och förslag: Utredningen föreslår att det införs nya lagar för Säkerhetspolisens personuppgiftsbehandling som rör nationell säkerhet i myndighetens brottsbekämpande och lagförande verksamhet och för domstolarnas be-

handling av personuppgifter inom brottsdatalagens tillämpningsområde. Det som behöver regleras i övergångsbestämmelser till de nya lagarna är framför allt hur pågående ärenden hos dessa myndigheter och hos tillsynsmyndigheterna bör hanteras.

I frågor som rör behandling av personuppgifter bör den nya lagstiftningen tillämpas från det att den träder i kraft. Det innebär exempelvis att framställningar om att få del av information, ärenden om rättelse och andra oavslutade ärenden ska hanteras enligt de nya lagarna. Några övergångsbestämmelser för handläggningen av frågor som rör personuppgiftsbehandlingen behövs därmed inte.

Beträffande tillsynsåtgärder följer det av allmänna principer att förelägganden och förbud som har meddelats med stöd av personuppgiftslagen och som rör den nya lagens tillämpningsområde fortsätter att gälla trots att personuppgiftslagen upphävts (se SOU 2017:29 s. 658). Det behövs därför inte några särskilda övergångsbestämmelser för det.

När det gäller andra frågor om tillsyn över behandling av personuppgifter föreslår utredningen i delbetänkandet att äldre bestämmelser ska fortsätta att gälla för ärenden som har påbörjats före ikraftträdandet men inte hunnit avgöras när brottsdatalagen träder i kraft (se SOU 2017:29 s. 658 f.). Motsvarande övergångsbestämmelser bör tas in i de nya lagarna.

Av de skäl som anges i delbetänkandet bör äldre bestämmelser fortsätta att gälla vid skada som har orsakats vid personuppgiftsbehandling enligt nuvarande reglering. Detsamma bör gälla för överklaganden i ännu inte avslutade ärenden som rör behandlingen av personuppgifter, om det överklagade beslutet har meddelats före ikraftträdandet (se SOU 2017:29 s. 658 f.). Övergångsbestämmelser med den innebörden bör därför tas in i de nya lagarna.

18.3.2 Övergångsbestämmelser i övrigt

Utredningens förslag: Bestämmelserna om loggning behöver inte tillämpas förrän den 1 maj 2023 i automatiserade behandlingssystem som Säkerhetspolisen har inrättat före den nya lagens ikraftträdande.

Skälen för utredningens förslag

Särskilda övergångsbestämmelser för existerande behandlingssystem

Utredningen föreslår en övergångsbestämmelse till brottsdatalagen som föreskriver att bestämmelserna om loggning inte behöver tillämpas förrän den 1 maj 2023 i automatiserade behandlingssystem som har inrättats före den 6 maj 2018, vilket är det datum då de författningar som genomför direktivet senast ska vara i kraft. Skälet till det är att det skulle kräva oproportionerliga ansträngningar för myndigheterna att redan när brottsdatalagen träder ikraft anpassa sina system till de nya loggningskraven och att direktivet medger anstånd med anpassningen (se SOU 2017:29 s. 663).

Säkerhetspolisen använder automatiserade behandlingssystem som har inrättats före den 1 maj 2018, vilket är det datum då den nya lagen föreslås träda i kraft. Det som har framförts angående övriga myndigheters behov av extra tid för anpassning av systemen är relevant även för Säkerhetspolisen. Det finns därmed behov av en övergångsbestämmelse som reglerar kraven på loggning i den nya lagen med tillhörande förordning. Den bör föreskriva att de nya reglerna om loggning inte behöver tillämpas förrän vid en senare tidpunkt om det är fråga om automatiserade behandlingssystem som har inrättats före den nya lagens ikraftträdande. Enligt utredningens mening bör Säkerhetspolisen få samma tid för anpassning av it-systemen som övriga brottsbekämpande myndigheter. Övergångsbestämmelsen bör således föreskriva att bestämmelserna om loggning inte behöver tillämpas förrän den 1 maj 2023. Någon motsvarande övergångsbestämmelse behövs inte för domstolarna, eftersom de omfattas av övergångsbestämmelsen till brottsdatalagen.

Som utredningen påpekar i delbetänkandet påverkar den nu aktuella övergångsbestämmelsen inte de generella krav på loggning som redan gäller (se SOU 2017:29 s. 663).

18.4 Särskilda övergångsproblem

18.4.1 Den nya dataskyddsregleringen medför särskilda övergångsproblem

Direktivet ska vara genomfört den 6 maj 2018. Utredningen föreslår därför att brottsdatalagen och övriga författningsförslag ska träda i kraft den 1 maj 2018. Dataskyddsförordningen ska däremot börja tillämpas först den 25 maj 2018. Den nationella lagstiftningen som kompletterar den föreslås träda i kraft samma dag, då personuppgiftslagen ska upphöra att gälla. Den omständigheten att tidpunkterna för när direktivet ska vara genomfört och när förordningen ska börja tillämpas är olika kan leda till övergångsproblem när det gäller de registerförfattningar som i dag innehåller bestämmelser inom både brottsdatalagens och dataskyddsförordningens tillämpningsområde. Det gäller kriminalvårdens, Kustbevakningens och åklagarväsendets registerförfattningar.

För Säkerhetspolisen är eventuella övergångsproblem i stället kopplade till om polisdatalagen ändras innan det finns ny lagstiftning för Säkerhetspolisens personuppgiftsbehandling. För domstolarna är det den omständigheten att arbetet med att genomföra direktivet kan dra ut på tiden som kan medföra problem.

Några motsvarande problem finns inte för övriga registerförfattningar.

18.4.2 Problemen med olika ikraftträdandetidpunkter

Utredningens bedömning: Om ändringarna i lagen om behandling av personuppgifter inom kriminalvården, kustbevakningsdatalagen och åklagardatalagen träder i kraft innan det finns nya författningar som reglerar personuppgiftsbehandlingen utanför brottsdatalagens tillämpningsområde, bör de nuvarande bestämmelserna i registerförfattningarna i fråga och i personuppgiftslagen fortsätta att gälla tills vidare.

Om ändringarna i polisdatalagen träder i kraft innan det finns ny lagstiftning för Säkerhetspolisen, bör bestämmelserna i polisdatalagen och personuppgiftslagen fortsätta att gälla tills vidare.

Utredningens förslag: Vissa bestämmelser som reglerar idrottsorganisationernas behandling av uppgifter om tillträdesförbud ska börja tillämpas senare än ändringarna som reglerar Polismyndighetens personuppgiftsbehandling i tillträdesförbudsregistret.

Skälen för utredningens bedömning och förslag

Kustbevakningens, åklagarväsendets och kriminalvårdens registerförfattningar

Utredningen föreslår att endast de delar av Kustbevakningens, åklagarväsendets och kriminalvårdens personuppgiftsbehandling som ligger inom brottsdatalagens tillämpningsområde ska regleras i de befintliga registerförfattningarna. Det innebär att den 1 maj 2018, då lagstiftningen som genomför direktivet föreslås träda i kraft, kommer de bestämmelser i myndigheternas registerförfattningar som reglerar frågor utanför brottsdatalagens tillämpningsområde att upphävas.

Som tidigare nämnts utreds de delar av lagen om behandling av personuppgifter inom kriminalvården och kustbevakningsdatalagen som ligger utanför brottsdatalagens tillämpningsområde av andra utredare, medan motsvarande fråga beträffande åklagardatalagen hanteras i Regeringskansliet (se avsnitt 9.1.1, 11.1.1 och 13.1.2). De andra utredarna har föreslagit eller förväntas föreslå att personuppgiftsregleringen utanför brottsdatalagens tillämpningsområde ska träda i kraft den 25 maj 2018 när dataskyddsförordningen ska börja tillämpas. Om den lagstiftning som genomför direktivet träder i kraft den 1 maj 2018 kommer det under mellantiden inte att finnas någon reglering för den personuppgiftsbehandling som ligger utanför brottsdatalagens tillämpningsområde. Därför behövs det övergångsbestämmelser så att de bestämmelser i kriminalvårdens, Kustbevakningens och åklagarväsendets nuvarande registerförfattningar som reglerar frågor utanför brottsdatalagens tillämpningsområde fortsätter att gälla fram till dess att de nya lagarna träder i kraft. Eftersom registerförfattningarna hänvisar till bestämmelser i personuppgiftslagen måste även förhållandet till den lagen regleras. En sådan reglering skulle kunna utformas på följande sätt.

Lagen om behandling av personuppgifter inom kriminalvården i dess lydelse före den 1 maj 2018 och personuppgiftslagen (1998:204) gäller fortfarande för sådan behandling av personuppgifter som inte utförs i syfte att verkställa häktning eller straffrättsliga påföljder eller biträda en annan behörig myndighet när den utför arbetsuppgifter för något av de syften som anges i 1 kap. 2 § brottsdatalagen (2018:000).

Kustbevakningsdatalagen i dess lydelse före den 1 maj 2018 och personuppgiftslagen (1998:204) gäller fortfarande för sådan behandling av personuppgifter som inte utförs i syfte att bekämpa eller lagföra brott eller upprätthålla allmän ordning och säkerhet.

Åklagardatalagen i dess lydelse före den 1 maj 2018 och personuppgiftslagen (1998:204) gäller fortfarande för sådan behandling av personuppgifter som inte utförs i syfte att bekämpa eller lagföra brott eller handlägga frågor om ändring eller verkställighet av straffrättsliga påföljder eller upprätthållande av allmän ordning och säkerhet.

Övergångsbestämmelserna kan upphävas när de nya lagarna träder i kraft.

Säkerhetspolisens registerförfattning

Utredningen föreslår i avsnitt 14.2.2 att Säkerhetspolisens personuppgiftsbehandling inte längre ska regleras i polisdatalagen utan i en ny lag. De bestämmelser som rör Säkerhetspolisens personuppgiftsbehandling i polisdatalagen ska därför enligt förslaget upphävas. Om ändringarna i polisdatalagen träder i kraft innan den nya lagen träder i kraft, kommer Säkerhetspolisens personuppgiftsbehandling att vara oreglerad under viss tid. Det behövs därför en övergångsbestämmelse som föreskriver att bestämmelserna i polisdatalagen ska fortsätta att gälla fram till dess att den nya lagen träder i kraft. Dessutom måste det säkerställas att de hänvisningar till personuppgiftslagen som görs i polisdatalagen också fortsätter att gälla. En sådan reglering skulle kunna utformas på följande sätt.

Polisdatalagen i dess lydelse före den 1 maj 2018 och personuppgiftslagen (1998:204) gäller fortfarande för Säkerhetspolisens behandling av personuppgifter.

Övergångsbestämmelsen kan upphävas när den nya lagen träder i kraft.

Lagen om register över tillträdesförbud vid idrottsarrangemang

När det gäller ändringarna i lagen om register över tillträdesförbud vid idrottsarrangemang bör ändringarna träda i kraft den 1 maj 2018, eftersom bestämmelserna om Polismyndighetens personuppgiftsbehandling bör börja tillämpas samtidigt som övriga anpassningar av myndighetens registerlagstiftning. Även de ändringar som föreslås för idrottsorganisationernas personuppgiftsbehandling kan till största delen börja tillämpas då. Däremot är det inte möjligt att låta de bestämmelser som i dag är knutna till personuppgiftslagen upphöra förrän dataskyddsförordningen börjar tillämpas den 25 maj 2018. De paragrafer som hänvisar till bestämmelser i personuppgiftslagen (4 och 15 §§) bör därför fortsätta att gälla fram till dess. Den bestämmelse som tydliggör att dataskyddsförordningen med kompletterande lagstiftning ska tillämpas vid idrottsorganisationernas personuppgiftsbehandling kan inte börja tillämpas förrän den 25 maj 2018, vilket bör framgå genom en övergångsbestämmelse.

18.4.3 Problem om genomförandet av direktivet fördröjs

Utredningens bedömning: Om ändringarna i domstolsdatalagen träder i kraft före domstolarnas brottsdatalag, bör domstolsdatalagen i dess lydelse före den 25 maj 2018 och personuppgiftslagen fortsätta att gälla tills vidare för sådan behandling av personuppgifter som undantas från dataskyddsförordningens tillämpningsområde.

Skälen för utredningens bedömning: För domstolarna kan övergångsproblem uppstå om ändringarna i domstolsdatalagen träder i kraft före domstolarnas brottsdatalag. Det skulle kunna inträffa om arbetet med att genomföra direktivet drar ut på tiden. Som framgår av delbetänkandet bedömer utredningen att det finns viss risk för det och att det därför kan komma att krävas en övergångsreglering (se SOU 2017:29 s. 655 f.).

Domstolsdatalagen föreslås endast innehålla bestämmelser om domstolarnas personuppgiftsbehandling inom dataskyddsförordningens tillämpningsområde (se Ds 2017:41 s. 55). Det innebär att

om ändringarna i domstolsdatalagen träder i kraft innan domstolarnas brottsdatalag gör det, kommer det under mellantiden inte att finnas någon registerförfattning för domstolarnas personuppgiftsbehandling inom brottsdatalagens tillämpningsområde. Då behövs det en övergångsbestämmelse som reglerar vad som ska gälla fram till dess att domstolarnas brottsdatalag träder i kraft. En sådan reglering bör tas in i domstolsdatalagen. Regleringen bör av de skäl som anges i delbetänkandet varken utgå från direktivet eller brottsdatalagen (se SOU 2017:29 s. 657). Den lagstiftning som genomför direktivet och som mejslar ut dess tillämpningsområde kommer nämligen inte att gälla vid den tidpunkten. Eftersom direktivets tillämpningsområde utgör en spegling av det undantag som görs i artikel 2.2 i dataskyddsförordningen bör regleringen i stället utgå från hur tillämpningsområdet formuleras i den artikeln.

Övergångsregleringen bör innebära att domstolsdatalagen i dess lydelse före den 25 maj 2018 ska fortsätta att gälla tills vidare för den del av domstolarnas personuppgiftsbehandling som ligger inom brottsdatalagens tillämpningsområde fram till dess att domstolarnas brottsdatalag träder i kraft. Dessutom måste det säkerställas att de hänvisningar till personuppgiftslagen som görs i domstolsdatalagen också fortsätter att gälla. Bestämmelsen bör kunna utformas på följande sätt.

Domstolsdatalagen i dess lydelse före den 25 maj 2018 och personuppgiftslagen (1998:204) gäller fortfarande för sådan behandling av personuppgifter som avses i artikel 2.2 d i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), i den ursprungliga lydelsen.

Övergångsbestämmelsen kan upphävas när domstolarnas brottsdatalag träder i kraft.

19 Konsekvenser

19.1 Allmänt om konsekvenserna

19.1.1 Anpassningar av registerförfattningarna

Utredningens bedömning: Anpassningarna av registerförfattningarna medför inga andra konsekvenser än dem som följer av att brottsdatalagen införs och att författningarna därmed får ett delvis annat tillämpningsområde än tidigare.

Skälen för utredningens bedömning: Samtliga registerförfattningar för myndigheterna i rättskedjan ändras i större eller mindre utsträckning till följd av att de föreslås gälla utöver brottsdatalagen. Det innebär framför allt att registerförfattningarna får nya tillämpningsområden, som är anpassade till brottsdatalagens. I fortsättningen är det syftet med behandlingen, inte den verksamhet som uppgifterna behandlas i, som är avgörande för om en registerförfattning är tillämplig.

De registerförfattningar som i dag reglerar personuppgiftsbehandling både inom och utanför brottsdatalagens tillämpningsområde renodlas så att de bara reglerar personuppgiftsbehandling inom tillämpningsområdet. Kriminalvårdens, Kustbevakningens och åklagarväsendets lagstiftning ändras på det sättet. För domstolarna införs en ny lag (se avsnitt 19.1.2).

För övriga myndigheter ändras också tillämpningsområdet för registerförfattningarna. För polisens del flyttas den reglering som gäller för Säkerhetspolisen till en särskild lag. Att tillämpningsområdet för brottsdatalagen omfattar upprätthållande av allmän ordning och säkerhet påverkar tillämpningsområdena för Polismyndigheten, Kustbevakningen, åklagarväsendet och domstolarna. För Ekobrottsmyndigheten förtydligas det när myndigheten ska till-

lämpa polisens respektive åklagarväsendets brottsdatalog. Även tillämpningsområdena för Tullverkets och Skatteverkets registerförfattningar påverkas, men det beror på att tillämpningsområdena inte längre knyts till viss verksamhet utan till vilket syfte personuppgifterna behandlas för.

Förslagen till anpassningar innebär att den generella regleringen i brottsdatalogen till stor del ersätter bestämmelser i registerförfattningarna, som inte blir lika omfattande som tidigare. De kompletteras med bestämmelser om sanktionsavgift för överträdelse av bestämmelserna i dem. Terminologin ändras också och görs mer enhetlig. Ett annat led i att göra registerförfattningarna mer enhetliga är att samla vissa bestämmelser, antingen i ett visst kapitel eller inom kapitlen. Bestämmelserna om föreskrifter anpassas också till den nya regleringen.

Anpassningarna medför inga andra konsekvenser än dem som följer av att brottsdatalogen införs. Konsekvenserna av det redovisar utredningen i delbetänkandet (se SOU 2017:29 s. 647 f.)

19.1.2 Två nya lagar men inga nya arbetsuppgifter

Utredningens bedömning: Den nya lagen för domstolarnas personuppgiftsbehandling innebär inga nya arbetsuppgifter och ansluter nära till den reglering som finns i dag.

Den nya lagen för Säkerhetspolisens behandling av personuppgifter innebär inte heller några nya arbetsuppgifter. Säkerhetspolisens skyldigheter i egenskap av personuppgiftsansvarig motsvarar till stor del vad som gäller i dag. Vissa av förslagen kommer att innebära förenklingar och förbättringar för Säkerhetspolisen, bl.a. ökade möjligheter till elektroniskt informationsutbyte.

Skälen för utredningens bedömning: I kapitel 12 föreslår utredningen att det ska införas en ny lag för domstolarnas personuppgiftsbehandling inom brottsdatalogens tillämpningsområde, domstolarnas brottsdatalog. Utredningen föreslår i kapitel 14 att det ska införas en ny lag för Säkerhetspolisens personuppgiftsbehandling vid brottsbekämpning och lagföring som rör nationell säkerhet, Säkerhetspolisens datalog. Lagarna ersätter till stor del tidigare lag-

stiftning. Utredningen gör samma bedömning när det gäller konsekvenserna av de nya lagarna som beträffande brottsdatalagen, nämligen att de visserligen innebär förändringar men inte kräver att det inrättas några nya it-system eller leder till några nya arbetsuppgifter.

För domstolarna har utredningen strävat efter lösningar som ligger nära den reglering som kan förväntas gälla för domstolarna när de ska tillämpa dataskyddsförordningens regelverk. Utredningen bedömer därför att den nya lagstiftningen inte får några särskilda konsekvenser, utöver dem som hör samman med att man i framtiden måste tillämpa olika regelverk beroende på för vilket syfte personuppgifterna behandlas.

När det gäller Säkerhetspolisen anpassas lagen till myndighetens verksamhet, vilket innebär att myndigheten får en modern och skräddarsydd lagstiftning. Regleringen förefaller bli betydligt mer omfattande än i dag, med det beror på att den ska vara heltäckande och inte hänvisa till annan generell reglering. Vissa av förslagen, framför allt möjligheten att i ökad utsträckning tillhandahålla personuppgifter elektroniskt både genom direktåtkomst och på annat sätt, innebär att Säkerhetspolisens verksamhet kan effektiviseras och lättare möta de ökade kraven på informationsutbyte bl.a. för att bekämpa terrorism. En annan effektivisering är att vissa personuppgifter får behandlas under längre tid än i dag, eftersom myndigheten inte i samma utsträckning behöver avsätta resurser för att fatta beslut om förlängning av den tid under vilka uppgifterna får behandlas.

Utredningen föreslår att tillsynen över Säkerhetspolisens personuppgiftsbehandling i huvudsak ska bedrivas på samma sätt som i dag, men tillsynsmyndigheterna får tydligare befogenheter. Som utredningen påpekar i delbetänkandet ligger frågan om ekonomiska konsekvenser av förslagen när det gäller tillsynsverksamheten utanför utredningens uppdrag (se SOU 2017:29 s. 648).

19.1.3 Modernisering av vissa författningar

<p>Utredningens bedömning: Förslagen till moderniseringar och förtydliganden bör leda till förenklingar för myndigheterna.</p>

Skälen för utredningens bedömning: Utöver nödvändiga anpassningar till det nya dataskyddsregelverket föreslår utredningen som nyss nämnts att registerförfattningarna i större utsträckning görs enhetliga. Om regleringen överensstämmer underlättar det informationsutbytet mellan myndigheterna, vilket är ett av syftena med dataskyddsdirektivet.

När det gäller polisdatalagen flyttas dels bestämmelserna om tillträdesförbudsregistret, dels de bestämmelser om personuppgiftsbehandling som i dag finns i polislagen till polisens brottsdatalag. Registerförfattningen blir därmed mer heltäckande och regleringen mer enhetlig.

Vissa bestämmelser om personuppgiftsbehandling i tullagen och lagen om Sveriges gräns mot ett annat land inom Europeiska unionen flyttas på motsvarande sätt till Tullverkets brottsdatalag.

För de brottsbekämpande myndigheterna ändras vissa bestämmelser om hur gemensamt tillgängliga uppgifter får behandlas så att de blir mer funktionella. I andra bestämmelser förtydligas vilka krav som ställs på behandlingen, vilket gör lagstiftningen mer transparent och lättillämpad. Dessutom moderniseras bestämmelserna om utlämnande på medium för automatiserad behandling i de brottsbekämpande myndigheternas registerförfattningar. Personuppgifter ska få tillhandahållas på det sättet om det inte är olämpligt, vilket underlättar elektronisk kommunikation.

Kriminalvårdens registerlag får en betydligt modernare utformning. Regleringen görs mer generell och lättillämpad. Bestämmelserna om säkerhetsregistret lyfts av integritetsskäl upp i lag. Detaljregler rensas bort ur både lagen och förordningen. Utredningen bedömer att förslagen skapar en tydligare och mer transparent lagstiftning, men behovet av en genomgripande materiell översyn av regleringen kvarstår.

I kriminalvårdens registerförfattning finns det i dag särskilda bestämmelser om överklagande och om omprövning. Utredningen föreslår i avsnitt 13.6.3 och 13.6.4 att de ska upphävas, liksom även den särskilda forumregel som finns. Ändringarna kan komma att påverka Förvaltningsrätten i Linköping marginellt, eftersom det inte kan uteslutas att de leder till att domstolen får något fler mål. Utredningen bedömer dock att förändringen inte kommer att öka belastningen på domstolen annat än mycket obetydligt, mot bak-

grund av att överklagandena under de senaste åren varit så få att det inte gått att få fram några statistiska uppgifter om dem.

19.2 Ekonomiska konsekvenser

19.2.1 Konsekvenser för staten

Utredningens bedömning: Anpassningarna av registerförfattningarna medför inga extra kostnader för berörda myndigheter. Eventuella merkostnader är inte större än att de ryms inom befintliga ekonomiska ramar.

Eftersom tillsynen över Säkerhetspolisens personuppgiftsbehandling ska bedrivas på i huvudsak samma sätt som i dag leder förslagen i den delen inte till några merkostnader.

Förslagen till moderniseringar ger utrymme för viss effektivisering.

Skälen för utredningens bedömning: Förslagen i detta betänkande innebär inga skyldigheter för myndigheterna att inrätta nya it-system. Några kostnader för det bör således inte beräknas med anledning av förslagen. Förslagen medför, av de skäl som anges i delbetänkandet, inte heller några ökade kostnader i övrigt för behöriga myndigheter utöver vad som kan krävas för utbildning av personalen angående den nya lagstiftningen. I delbetänkandet gör utredningen bedömningen att kostnaderna för utbildning ryms inom befintliga ekonomiska ramar (se SOU 2017:29 s. 649 f.). Utredningen gör samma bedömning beträffande de förslag som läggs fram nu.

När det gäller tillsynen över Säkerhetspolisen konstaterar utredningen att den i huvudsak bör bedrivas på samma sätt som i dag. Förslagen bör därmed inte leda till några merkostnader.

Förändringen beträffande överklagande av Kriminalvårdens beslut ger så marginella effekter att de ryms inom befintliga ekonomiska ramar.

Förslagen till moderniseringar ger utrymme för viss effektivisering. Det gäller särskilt utökade möjligheter att kommunicera elektroniskt. Det är dock svårt att bedöma effekterna av förslagen i dessa delar.

19.2.2 Konsekvenser för kommuner, landsting och enskilda

Utredningens bedömning: Förslagen medför inga ökade kostnader för kommuner och landsting eller för enskilda.

Skälen för utredningens bedömning: I detta betänkande behandlas inga frågor som direkt berör kommuner och landsting, utöver den prövning som utredningen föreslår i avsnitt 6.4. Den innebär att innan en personuppgift behandlas för ett nytt ändamål ska en prövning göras av om behandlingen för det nya ändamålet är nödvändig och proportionerlig. Den prövningen ska göras av alla som ska tillämpa brottsdatalagen, vilket innebär att den även ska göras av aktörer som verkställer exempelvis vårdpåföljder. Förslaget i den delen kan dock inte antas påverka dem ekonomiskt, eftersom prövningen ersätter den finalitetsprövning som ska göras enligt personuppgiftslagen.

Förslagen syftar, i likhet med förslagen i delbetänkandet, till att stärka integritetsskyddet för enskilda och att ge dem bättre möjligheter att kunna kontrollera hur deras personuppgifter behandlas. Förslagen förväntas inte leda till några kostnadsökningar för enskilda. Visserligen föreslår utredningen i de nya lagarna att de personuppgiftsansvariga i vissa fall ska kunna ta ut avgift för information som begärs, men det är i situationer där den enskilde alltför ofta återkommer med begäran om information. Den personuppgiftsansvarige kan då ge den enskilde informationen mot avgift i stället för att avslå begäran.

19.3 Konsekvenser för det brottsförebyggande arbetet

Utredningens bedömning: Förbättrat dataskydd och moderna författningar ger möjlighet till ökat informationsutbyte mellan brottsbekämpande myndigheter, vilket är positivt för det brottsförebyggande arbetet. Förslagen förväntas inte få några direkta effekter på brottsligheten.

Skälen för utredningens bedömning: Förslagen kan inte förväntas få några direkta effekter på brottsligheten, eftersom det handlar om en administrativ reform. Som utredningen framhåller i delbetänkandet kan däremot ett ökat informationsutbyte inom Sverige och mellan medlemsstaterna få positiv effekt på det brottsförebyggande arbetet.

19.4 Konsekvenser i övrigt

Utredningens bedömning: Förslagen förväntas inte få några andra konsekvenser.

Skälen för utredningens bedömning: Förslagen får inte några samhällsekonomiska konsekvenser eller några konsekvenser för den kommunala självstyrelsen. Förslagen får inte heller några konsekvenser för jämställdheten eller andra sådana konsekvenser som avses i 14 § kommittéförordningen (1998:1474) eller 7 § förordningen (2007:1244) om konsekvensutredning vid regelgivning.

20 Författningskommentar

20.1 Förslaget till Säkerhetspolisens datalag (2018:000)

1 kap. Allmänna bestämmelser

Syftet med lagen

1 §

I paragrafen, som behandlas i avsnitt 14.2.3, anges syftet med lagen. Syftet är att skydda fysiska personers grundläggande fri- och rättigheter i samband med behandling av personuppgifter och att säkerställa att Säkerhetspolisen kan behandla och utbyta personuppgifter på ett ändamålsenligt sätt. Paragrafen motsvarar 1 kap. 1 § brottsdatalagen (2018:000).

Lagens tillämpningsområde

2 §

Paragrafen reglerar, tillsammans med 3 §, lagens tillämpningsområde. Den behandlas i avsnitt 14.2.2, 14.3.1 och 14.3.2.

I *första stycket* anges att lagen gäller vid behandling av personuppgifter som rör nationell säkerhet i Säkerhetspolisens brottsbekämpande och lagförande verksamhet. Vad som är en personuppgift och behandling av personuppgifter definieras i 9 §.

I Säkerhetspolisens brottsbekämpande verksamhet ingår att förebygga, förhindra och upptäcka brottslig verksamhet och att utreda brott. Den lagförande verksamheten syftar till att ställa personer till ansvar för brott. All verksamhet vid Säkerhetspolisen anses i någon mån vara brottsbekämpande (se prop. 2013/14:110

s. 480 f.). I avsnitt 14.3.1 utvecklas vad som avses med uttrycken brottsbekämpande och lagförande verksamhet.

Lagen gäller endast vid behandling av personuppgifter som rör nationell säkerhet. Nationell säkerhet behöver inte alltid avse enbart Sveriges säkerhet. En fråga som rör nationell säkerhet i något av våra grannländer kan t.ex. vara av den karaktären att den även indirekt berör Sveriges nationella säkerhet, exempelvis vid gränsöverskridande terrorism.

I 6 § upplyses om att Säkerhetspolisen i vissa fall ska tillämpa brottsdatalagen och polisens brottsdatalag i stället för denna lag. Behandling av personuppgifter i intern och administrativ verksamhet ligger utanför lagens tillämpningsområde.

Av *andra stycket* framgår att lagen i tillämpliga delar gäller vid Polismyndighetens behandling av personuppgifter när myndigheten har övertagit en arbetsuppgift som rör nationell säkerhet från Säkerhetspolisen. Det innebär att det som sägs i lagen om Säkerhetspolisen då i stället gäller Polismyndigheten. Enligt 15 § förordningen (2014:1103) med instruktion för Säkerhetspolisen får biträdande säkerhetspolischefen i samråd med chefen för Nationella operativa avdelningen, trots den ansvarsfördelning som annars gäller mellan myndigheterna, bestämma att en förundersökning eller annan uppgift i den brottsbekämpande verksamheten ska lämnas över till Polismyndigheten för fortsatt handläggning. Enligt 28 § förordningen (2014:1102) med instruktion för Polismyndigheten ska myndigheten också bistå vid polisverksamhet som leds av Säkerhetspolisen, om Säkerhetspolisen i ett enskilt fall begär det och det inte finns särskilda skäl mot det. Polismyndigheten ska vidare, i den utsträckning som myndigheterna kommer överens om, lämna tekniskt biträde och annan hjälp till Säkerhetspolisen. Det får avgöras i det enskilda fallet om biståndet eller biträdet är av den arten att lagen ska tillämpas.

Enligt *tredje stycket* gäller inte lagen (2018:000) med kompletterande bestämmelser till EU:s dataskyddsförordning när personuppgifter behandlas enligt denna lag.

3 §

Paragrafen, som motsvarar 1 kap. 3 § brottsdatalogen (2018:000), begränsar lagens tillämpningsområde huvudsakligen till helt eller delvis automatiserad behandling av personuppgifter, men även viss manuell behandling omfattas. Vad bestämmelsen innebär utvecklas i SOU 2017:29 s. 671.

Förhållandet till annan reglering

4 §

Paragrafen anger hur regleringen i lagen förhåller sig till lagen (2017:496) om internationellt polisiärt samarbete med tillhörande förordning. Paragrafen, som motsvarar nuvarande 1 kap. 4 § polis-datalogen (2010:361), behandlas i avsnitt 14.5.1.

Av paragrafen framgår att det i de nämnda författningarna finns särbestämmelser om behandling av personuppgifter som följer av internationella överenskommelser. Exempel på en sådan överenskommelse är Prömrådsbeslutet. Om det i de nämnda författningarna finns bestämmelser som avviker från förevarande lag, ska de tillämpas i stället.

5 §

Paragrafen, som behandlas i avsnitt 14.5.1, klargör att bestämmelserna i lagen inte ska tillämpas om det skulle inskränka Säkerhetspolisens skyldighet enligt 2 kap. tryckfrihetsförordningen att lämna ut personuppgifter. Paragrafen har utformats efter mönster av 8 § första stycket personuppgiftslagen (1998:204). Den innebär t.ex. att Säkerhetspolisen inte kan vägra att ta fram och lämna ut uppgifter i enlighet med tryckfrihetsförordningens bestämmelser med hänvisning till att personuppgifterna inte får behandlas enligt 2 kap. 1 §. Offentlighetsprincipen innebär dock inte någon skyldighet att lämna ut uppgifter elektroniskt. Enligt 2 kap. 19 § får personuppgifter bara lämnas ut elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt. Vidare måste det prövas om sekretess hindrar utlämnande.

6 §

I paragrafen, som behandlas i avsnitt 7.2.1 och 14.3.3, upplyses om att Säkerhetspolisen ska tillämpa brottsdatalagen och polisens brottsdatalag med tillhörande förordningar vid behandling av personuppgifter i frågor som inte rör nationell säkerhet. Det framgår av 1 kap. 1 § första stycket 3 polisens brottsdatalag (2010:361).

Personuppgiftsansvar

7 §

I paragrafen, som behandlas i avsnitt 14.5.2, regleras personuppgiftsansvaret. Personuppgiftsansvarig definieras i 1 kap. 9 §. Skyldigheterna som personuppgiftsansvarig regleras i 5 kap.

I *första stycket*, som motsvarar nuvarande 6 kap. 5 § första stycket polisdatalagen (2010:361), föreskrivs att Säkerhetspolisen är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför. Det gäller även den personuppgiftsbehandling som utförs av personuppgiftsbiträden som myndigheten anlitar.

Eftersom Polismyndigheten i vissa fall ska tillämpa lagen föreskrivs det i *andra stycket* att myndigheten är personuppgiftsansvarig för den behandling som myndigheten utför när den tillämpar lagen.

I *tredje stycket* regleras personuppgiftsansvarets omfattning. Bestämmelsen motsvarar 3 kap. 1 § brottsdatalagen (2018:000). Vad personuppgiftsansvaret innebär utvecklas i SOU 2017:29 s. 698 f.

8 §

Paragrafen, som behandlas i avsnitt 14.5.2, reglerar gemensamt personuppgiftsansvar. Paragrafen motsvarar 3 kap. 21 § brottsdatalagen (2018:000). Vad bestämmelsen innebär utvecklas i SOU 2017:29 s. 715.

Uttryck i lagen

9 §

I paragrafen, som behandlas i avsnitt 14.5.3, definieras olika uttryck som används i lagen. Definitionerna stämmer, med undantag för definitionerna av tillsynsmyndighet och tredjeland, överens med dem som finns i 1 kap. 6 § brottsdatalagen (2018:000). Uttrycken förklaras i SOU 2017:29 s. 672 f.

Tillsynsmyndighet

Med tillsynsmyndighet avses den myndighet som regeringen utser att enligt lagen utöva tillsyn över personuppgiftsbehandling. Definitionen behandlas i avsnitt 15.3.

Tredjeland

Tredjeland definieras som en stat som inte är medlem i Europeiska unionen eller Europeiska ekonomiska samarbetsområdet och som inte heller på grund av avtal med Europeiska unionen har en motsvarande ställning. Förutom medlemsstaterna i EU är det Island, Liechtenstein, Norge och Schweiz som inte är tredjeland i lagens mening. Definitionen behandlas i avsnitt 14.17.1.

Lagens tillämpning på uppgifter om juridiska personer

10 §

I paragrafen anges vilka bestämmelser i lagen som gäller för behandling av uppgifter om juridiska personer. Paragrafen behandlas i avsnitt 14.5.4. Uppräkningen i paragrafen av bestämmelser som ska gälla vid behandling av uppgifter om juridiska personer motsvarar nuvarande 1 kap. 6 § polisdatalagen (2010:361).

2 kap. Behandling av personuppgifter

Tillåtna rättsliga grunder för behandling av personuppgifter

1 §

Paragrafen reglerar tillsammans med 2 och 3 §§ de tillåtna rättsliga grunderna för behandling av personuppgifter. Den behandlas i avsnitt 14.6.3. Paragrafen motsvarar nuvarande 6 kap. 1 § polisdata-lagen (2010:361).

Personuppgifter får enligt *första stycket* behandlas om det är nödvändigt för att utföra en arbetsuppgift i vissa särskilt angivna syften. Bestämmelsen bildar den yttre ramen för när behandling av personuppgifter är tillåten. Att ordet nödvändigt används i stället för behövs innebär ingen ändring i sak.

Enligt *punkten 1 a–c* får personuppgifter behandlas i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott mot rikets säkerhet, terrorbrott eller tryckfrihetsbrott eller yttrandefrihetsbrott med rasistiska eller främlingsfientliga motiv. Brott mot rikets säkerhet brukar anses innefatta bl.a. sådana brott som avses i 18 och 19 kap. brottsbalken. Med terrorbrott avses brott mot lagen (2003:148) om straff för terroristbrott, lagen (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall och lagen (2010:299) om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet.

Med uttrycket förebygga, förhindra eller upptäcka brottslig verksamhet avses framför allt Säkerhetspolisens underrättelseverksamhet. I sådan verksamhet samlas information in, analyseras och bearbetas i syfte att förhindra eller upptäcka brottslig verksamhet när det ännu inte finns misstankar om att något konkret brott har begåtts (se prop. 2009/10:85 s. 318). Om det finns misstankar om ett konkret brott kan personuppgifter behandlas för att utreda brottet enligt punkten 2.

I punkten 1 ingår bl.a. myndighetens kartläggning och kontroll av personer, företeelser och annat som kan belysa riskerna för brott av nu aktuellt slag. Insamling av uppgifter om verksamheter, sammanslutningar och annat som kan utvecklas till konkreta hot mot det svenska samhället eller mot enskilda personer i statsledningen är ett annat exempel. Även spaning i syfte att uppvisa sådan

brottslig verksamhet som Säkerhetspolisen bekämpar hör hit (se prop. 2009/10:85 s. 362 f.).

Under den punkten ryms också handläggningen av tvångsmedelsfrågor enligt lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott och lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet. Även behandling av överskottsinformation med stöd av 27 kap. 23 a § rättegångsbalken omfattas, om syftet är att förhindra brott. Personuppgiftsbehandling vid annan brottsförebyggande verksamhet omfattas också.

Enligt *punkten 2* får personuppgifter behandlas i syfte att utreda eller lagföra sådana brott som avses i punkten 1. Vidare omfattas utredning och lagföring av brott i de fall där Säkerhetspolisen har hand om eller är delaktig i en brottsutredning efter särskilt beslut.

Att utreda brott innebär framför allt att genomföra förundersökning enligt 23 kap. rättegångsbalken. Med brott avses konkreta brott, men det kan vara fråga om såväl brott som bevisligen har begåtts som brott som det enbart finns misstankar om. Misstankarna behöver inte vara riktade mot någon bestämd person. Även personuppgiftsbehandling vid åtgärder som vidtas med stöd av 23 kap. 3 och 8 §§ rättegångsbalken omfattas. Under denna punkt ligger också det biträde som Säkerhetspolisen ger åklagare i förundersökningar, vilket även inkluderar hanteringen av hemliga tvångsmedel. Även spaning under förundersökning hör hit, liksom användning av överskottsinformation för att utreda brott (se prop. 2009/10:85 s. 363).

Enligt *punkten 3 a* får Säkerhetspolisen behandla personuppgifter för att fullgöra uppgifter i samband med personskydd av den centrala statsledningen och andra som regeringen eller Säkerhetspolisen bestämmer. Det innefattar exempelvis behandling av uppgifter rörande den skyddade personen själv, personer i hans eller hennes närmaste krets och andra personer som han eller hon kommer i kontakt med och uppgifter om personer som kan utgöra hot mot den skyddade personen. Det är dock bara uppgifter som behövs för att skyddsuppgiften ska kunna fullgöras som får behandlas med stöd av den här punkten. Den omfattar även behandlingen av personuppgifter för själva bevaknings- och säkerhetsarbetet, exem-

pelvis uppgifter om vem som fullgör bevakningsuppgiften vid ett visst tillfälle (se prop. 2009/10:85 s. 363).

Punkten 3 b ger Säkerhetspolisen möjlighet att behandla personuppgifter för att fullgöra uppgifter som anges i säkerhetsskyddslagen (1996:627). I uppgifterna ingår bl.a. registerkontroll och utlämnande av uppgifter med anledning av sådan kontroll.

I *punkten 3 c* regleras Säkerhetspolisens personuppgiftsbehandling för att fullgöra uppgifter enligt utlännings- och medborgarskapslagstiftningen. Det som avses är framför allt Säkerhetspolisens personuppgiftsbehandling i s.k. säkerhetsärenden enligt utlänningslagen (2005:716), men även i verkställighetsärenden enligt den lagen. Säkerhetspolisen har också uppgifter enligt lagen (1991:572) om särskild utlänningskontroll och lagen (2001:82) om svenskt medborgarskap. Personuppgiftsbehandling i sådana ärenden omfattas också.

I *punkten 4* föreskrivs att Säkerhetspolisen får behandla personuppgifter om det är nödvändigt för att utföra en annan arbetsuppgift som rör nationell säkerhet, om arbetsuppgiften anges i lag eller förordning eller särskilt beslut av regeringen.

I *punkten 5* regleras den personuppgiftsbehandling som krävs för att Säkerhetspolisen ska kunna fullgöra förpliktelser som följer av internationella åtaganden. Till dem hör bl.a. att skydda vissa företrädare för utländska stater som besöker Sverige, främst statsöverhuvuden och regeringsföreträdare. I den mån personuppgiftsbehandling vid skyddet av dem inte regleras i punkten 3 a, t.ex. därför att skyddet i huvudsak fullgörs av utländsk säkerhetspersonal, regleras det i denna punkt.

Säkerhetspolisen lämnar, i likhet med Polismyndigheten, i viss utsträckning andra länder rättslig hjälp i brottsutredningar. Punkten omfattar den behandling av personuppgifter som behövs för det. Den täcker också Säkerhetspolisens informations- och erfarenhetsutbyte med motsvarande myndigheter i andra stater, i den mån utbytet grundar sig på ett internationellt åtagande. Om informationsutbytet äger rum enbart i svenskt intresse hör det normalt hemma under någon av de andra punkterna. Däremot hör sådant informationsutbyte som enbart gagnar den utländska myndigheten, t.ex. uppgifter om brott i en annan stat, hemma under denna punkt (se prop. 2009/10:85 s. 363 f.).

Enligt *andra stycket* ska det vara fråga om en arbetsuppgift som framgår av en lag, en förordning eller ett särskilt beslut i vilket regeringen uppdragit åt myndigheten att ansvara för en sådan uppgift. Personuppgiftsbehandlingen måste således alltid ha stöd i Säkerhetspolisens arbetsuppgifter så som de kommer till uttryck i svensk lagstiftning och andra för verksamheten bindande beslut om arbetsuppgifter som regeringen meddelat.

2 §

Paragrafen reglerar tillsammans med 1 och 3 §§ de tillåtna rättsliga grunderna för Säkerhetspolisens behandling av personuppgifter. Den behandlas i avsnitt 14.6.5. Bestämmelsen motsvarar nuvarande 6 kap. 2 § polisdatalagen (2010:361). Behandling enligt denna paragraf förutsätter att uppgifterna redan är föremål för behandling med stöd av 1 §.

Första stycket ger Säkerhetspolisen stöd för att behandla personuppgifter för att kunna lämna ut dem till bl.a. andra brottsbekämpande myndigheter. Enligt *punkten 1* får Säkerhetspolisen, vars brottsbekämpning rör ett relativt begränsat område, utföra den behandling som krävs för att till rätt myndighet vidarebefordra bl.a. uppgifter om brott eller brottslig verksamhet som Säkerhetspolisen upptäcker men själv saknar behörighet att handlägga (se prop. 2009/10:85 s. 365).

Punkten 2 ger Säkerhetspolisen stöd för att behandla uppgifter för att lämna ut dem till en annan myndighet inom ramen för myndighetsöverskridande samverkan mot brott. I första hand tillgodoser punkten behovet av informationsutbyte med andra myndigheter än brottsbekämpande, eftersom punkten 1 i huvudsak täcker det behovet.

Enligt *punkten 3* får Säkerhetspolisen behandla personuppgifter för att kunna lämna ut dem till Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst eller till Försvarets radioanstalts försvarsunderrättelseverksamhet. Punkten medger att Säkerhetspolisen behandlar personuppgifter som den anser kan vara värdefulla för någon av dessa myndigheter och vill vidarebefordra dit. Möjligheterna till sådan behandling begränsas genom

kravet på att det ska finnas särskilda skäl att tillhandahålla informationen (se prop. 2009/10:85 s. 365 f.).

I *punkten 4* ges Säkerhetspolisen rättsligt stöd för att behandla personuppgifter om myndigheten enligt lag eller förordning har till uppgift att bistå en annan myndighet med viss uppgift. Punkten omfattar bl.a. den behandling som kan krävas för att Säkerhetspolisen ska kunna bistå Riksdagens ombudsmän eller Justitiekanslern med uppgifter när de uppträder som förundersökningsledare och åklagare (se prop. 2014/15:94 s. 137).

Enligt *punkten 5* får information som behandlas med stöd av 1 § också behandlas för att tillhandahålla information som är nödvändig för den brottsbekämpande verksamheten vid en utländsk myndighet eller en mellanfolklig organisation (se prop. 2009/10:85 s. 366). I 16 § finns en sekretessbrytande bestämmelse som möjliggör sådant utlämnande.

Punkten 6 ger Säkerhetspolisen möjlighet att behandla personuppgifter för att lämna ut dem till en utländsk underrättelse- eller säkerhetstjänst om det inte täcks av någon av de övriga punkterna i paragrafen.

Av *andra stycket* framgår att personuppgifter får behandlas om det är nödvändigt för att tillhandahålla information till riksdagen eller regeringen och, i den utsträckning skyldighet att lämna uppgifter följer av lag eller förordning, till andra. Vad bestämmelsen innebär utvecklas i prop. 2009/10:85 s. 323 och 366.

I *tredje stycket* tydliggörs att de i paragrafen angivna rättsliga grunderna för att lämna ut personuppgifter som redan behandlas inte är uttömmande. Bestämmelsen ger Säkerhetspolisen stöd för att i ett enskilt fall behandla personuppgifter, som behandlas med stöd av 1 §, för något annat syfte än de som anges första och andra styckena. För att sådan behandling ska vara tillåten krävs det dock att ändamålet med behandlingen inte är oförenligt med det ändamål för vilket personuppgifterna samlades in (finalitetsprincipen).

3 §

Paragrafen reglerar, tillsammans med 1 och 2 §§, de tillåtna rättsliga grunderna för behandling av personuppgifter. Den motsvarar nuvarande 6 kap. 3 § polisdatalagen (2010:361).

I paragrafen, som behandlas i avsnitt 14.6.4, regleras två särskilt angivna fall där det är tillåtet att behandla personuppgifter, trots att förutsättningarna för behandling enligt 1 eller 2 § inte är uppfyllda. Tillämpningsområdet för paragrafen är begränsat, eftersom det enbart är personuppgifter som inkommit till Säkerhetspolisen som får behandlas. Vad regleringen innebär utvecklas i SOU 2017:29 s. 682 f.

Ändamål för behandling av personuppgifter

4 §

I paragrafen regleras kravet på ändamål för behandling av personuppgifter. Den behandlas i avsnitt 14.6.1.

I *första stycket* föreskrivs att personuppgifter får behandlas bara för särskilda, uttryckligt angivna och berättigade ändamål. En motsvarande bestämmelse finns i 2 kap. 3 § brottsdatalagen (2018:000). Vad bestämmelsen innebär utvecklas i SOU 2017:29 s. 683 f.

Eftersom Säkerhetspolisens personuppgiftsbehandling till övervägande del utförs i myndighetens underrättelseverksamhet är det inte alltid möjligt att ange ändamålen för behandlingen lika preciserat som i annan brottsbekämpande verksamhet. Verksamhetens natur innebär att ändamålen ofta får anges mer övergripande. Kravet på särskilda ändamål måste ses i ljuset av detta.

I *andra stycket* föreskrivs att personuppgifter inte får behandlas för något ändamål som är oförenligt med det ändamål för vilket personuppgifterna ursprungligen behandlades (finalitetsprincipen). När Säkerhetspolisen ska behandla personuppgifter för nya ändamål måste myndigheten alltid pröva om det nya ändamålet är förenligt med det ändamål som personuppgifterna samlades in för. Eftersom Säkerhetspolisens verksamhet är inriktad på att bekämpa brott som till sin natur är systemhotande kan behandling av personuppgifter för nya ändamål inom den egna organisationen i de allra flesta fall anses förenlig med ursprungsändamålet. I de fall som anges i 2 § får behandlingen som regel också anses förenlig med de ändamål för vilka personuppgifterna ursprungligen behandlades.

5 §

I paragrafen slås fast att Säkerhetspolisen får behandla personuppgifter för vetenskapliga, statistiska eller historiska ändamål inom lagens tillämpningsområde. Paragrafen behandlas i avsnitt 14.6.1. En motsvarande bestämmelse finns i 2 kap. 5 § brottsdatalagen (2018:000). Vad bestämmelsen innebär utvecklas i SOU 2017:29 s. 685.

Grundläggande krav på behandling av personuppgifter

Laglig och korrekt behandling

6 §

I paragrafen, som motsvarar 2 kap. 6 § brottsdatalagen (2018:000), föreskrivs att personuppgifter ska behandlas författningsenligt och på ett korrekt sätt. Den behandlas i avsnitt 14.7.1. Vad regleringen innebär utvecklas i SOU 2017:29 s. 686.

Personuppgifternas kvalitet

7 §

Paragrafen, som motsvarar 2 kap. 7 § brottsdatalagen (2018:000), reglerar hur de personuppgifter som behandlas ska vara beskaffade. Den behandlas i avsnitt 14.7.2.

I *första stycket* föreskrivs att de personuppgifter som behandlas ska vara korrekta och, om nödvändigt, uppdaterade. Vad det innebär utvecklas i SOU 2017:29 s. 687.

Av *andra stycket* framgår att uppgifter som beskriver en persons utseende ska utformas på ett objektivt sätt och med respekt för människovärdet. Vad det innebär utvecklas i SOU 2017:29 s. 687 f.

8 §

Paragrafen, som motsvarar 2 kap. 8 § brottsdatalagen (2018:000), reglerar omfattningen av behandlingen av personuppgifter. Vad bestämmelsen innebär utvecklas i SOU 2017:29 s. 688 f.

Det kan vara svårare att bedöma om uppgifterna är adekvata och relevanta i Säkerhetspolisens verksamhet än i annan polisverksamhet, eftersom det som regel inte är lika tydligt vari den brottsliga verksamheten eller säkerhetshotet består. Vid bedömningen av mängden personuppgifter som behöver behandlas i förhållande till ändamålet kan hänsyn också behöva tas till andra aspekter än enbart behoven i det enskilda fallet. För att pågående underrättelse- eller utredningsverksamhet inte ska avslöjas kan Säkerhetspolisen ibland behöva behandla fler uppgifter än vad som krävs i ett visst ärende, för att inte avslöja vem eller vilka som myndigheten intresserar sig för. Kravet på att uppgifterna ska vara adekvata och relevanta och inte för många i förhållande till ändamålet med behandlingen får i dessa fall ändå anses vara uppfyllt.

Paragrafen behandlas i avsnitt 14.7.2.

Känsliga personuppgifter

9 §

Paragrafen, som motsvarar 2 kap. 11 § brottsdatalagen (2018:000), reglerar tillsammans med 10–12 §§ i vilken utsträckning känsliga personuppgifter får behandlas. Att uppgifterna betecknas som känsliga framgår av 11 §. Paragrafen behandlas i avsnitt 14.7.3.

I *första stycket* föreskrivs förbud mot att behandla personuppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening eller som rör hälsa, sexualliv eller sexuell läggning. Om andra uppgifter om en person behandlas får de dock, enligt *andra stycket*, kompletteras med sådana uppgifter när det är absolut nödvändigt för ändamålet med behandlingen. Vad regleringen innebär utvecklas i SOU 2017:29 s. 690 f.

10 §

I paragrafen, som tillsammans med 9, 11 och 12 §§ reglerar i vilken utsträckning känsliga personuppgifter får behandlas, föreskrivs att Säkerhetspolisen får behandla biometriska uppgifter endast om det

är absolut nödvändigt för ändamålet med behandlingen. Biometriska uppgifter definieras i 1 kap. 9 §.

Bestämmelsen möjliggör användning av särskild teknisk behandling för att bekräfta unik identifiering av en person. Det innebär att t.ex. fingeravtryck, ansiktsgeometri, röstigenkänning eller rörelsemönster kan användas för att identifiera en person. Behovet av att behandla biometriska uppgifter måste prövas noga i ett enskilt ärende. Paragrafen behandlas i avsnitt 14.7.3.

Säkerhetspolisen får däremot inte behandla genetiska uppgifter. Uttrycket definieras i 1 kap. 9 §.

11 §

Paragrafen reglerar tillsammans med 9, 10 och 12 §§ i vilken utsträckning känsliga personuppgifter får behandlas. Paragrafen behandlas i avsnitt 14.7.3.

I paragrafen klargörs att sådana personuppgifter som avses i 9 och 10 §§ betecknas som känsliga personuppgifter i lagen. Vidare slås fast att sådana uppgifter alltid får behandlas i de fall som avses i 3 §, dvs. om det är nödvändigt för diarieföring eller, i fråga om uppgifter i en anmälan, ansökan eller liknande, om det är nödvändigt för myndighetens handläggning. Vad regleringen innebär utvecklas i SOU 2017:29 s. 692 f.

12 §

Paragrafen, som behandlas i avsnitt 14.7.3, reglerar användningen av känsliga personuppgifter vid sökning. I 9 och 10 §§ anges vilka personuppgifter som är känsliga personuppgifter.

Paragrafen gäller vid sökning i alla slags personuppgifter, dvs. såväl personuppgifter som har gjorts gemensamt tillgängliga som personuppgifter som inte har det.

Enligt *första stycket* är det förbjudet att utföra sökning i syfte att få fram ett personurval grundat på känsliga personuppgifter. Därmed förbjuds sökning i syfte att att få fram ett urval av personer som t.ex. har viss politisk åskådning eller religiös övertygelse.

I *andra stycket* klargörs att brottsrubriceringar, uppgifter om tillvägagångssätt vid brott och uppgifter som beskriver en persons

utseende får användas vid sökning, även om det skulle leda till ett personurval grundat på känsliga personuppgifter.

Enligt *tredje stycket* hindrar sökförbudet inte sökning i syfte att få fram ett personurval grundat på etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller uppgifter som rör hälsa, sexualliv eller sexuell läggning, om sökningen är absolut nödvändig för de syften som anges i 1 §. Säkerhetspolisen kan behöva söka på uppgifter som rör politiska åsikter, religiös övertygelse eller etniskt ursprung, eftersom det ingår i Säkerhetspolisens uppdrag att kartlägga sådan verksamhet som kan komma att hota vitala samhällsfunktioner och att skydda statsledningen. Sådan sökning kan även behöva göras t.ex. för att förebygga och förhindra tryck- eller yttrandefrihetsbrott med rasistiska eller främlingsfientliga motiv.

Kravet på att det ska vara absolut nödvändigt att göra sökningen gör att utrymmet för sådana sökningar är begränsat och att rutinmässiga sökningar på känsliga uppgifter inte är tillåtna.

I vilken utsträckning det är tillåtet att behandla någon eller några av personuppgifterna i en sammanställning av sådana uppgifter som sökningen resulterat i får prövas mot huvudregeln om behandling av känsliga personuppgifter i 9 §. Rätten att göra sökning medför således inte en generell rätt att fortsätta att behandla uppgifterna.

Åtgärder för att säkerställa personuppgifternas kvalitet

13 §

I paragrafen föreskrivs vad Säkerhetspolisen ska göra för att förhindra att felaktiga eller ofullständiga personuppgifter behandlas, lämnas ut eller görs tillgängliga och hur inaktuella uppgifter ska hanteras. Paragrafen behandlas i avsnitt 14.7.4 och motsvarar 2 kap. 15 § första stycket brottsdatalagen (2018:000). I 6 kap. 6 § regleras vad som gäller när den registrerade begär att personuppgifter ska rättas eller kompletteras.

Vad regleringen innebär utvecklas i SOU 2017:29 s. 693 f.

14 §

I paragrafen, som motsvarar 2 kap. 16 § brottsdatalogen (2018:000), föreskrivs vilka åtgärder som ska vidtas om personuppgifter behandlas på otillåtet sätt. Den behandlas i avsnitt 14.7.4. I 6 kap. 7 § regleras vad som gäller när den registrerade begär att motsvarande åtgärder ska vidtas.

I *första stycket* föreskrivs att alla rimliga åtgärder ska vidtas för att personuppgifter som behandlas i strid med 1–6, 8–10 eller 12 § eller 4 kap. 1 § första stycket, 2–4 eller 7–11 § utan onödigt dröjsmål ska raderas. Säkerhetspolisen ska också se till att sådana uppgifter inte lämnas ut eller görs tillgängliga. Det gäller också när radering krävs för att utföra en rättslig förpliktelse. När radering kan komma i fråga, förutsättningarna för det och vad som kan vara en rättslig förpliktelse utvecklas i SOU 2017:29 s. 726 f.

I stället för att radera personuppgifter som behandlas på otillåtet sätt ska Säkerhetspolisen enligt *andra stycket* utan onödigt dröjsmål begränsa behandlingen av uppgifterna om de behöver sparas som bevisning. Vad det innebär utvecklas i SOU 2017:29 s. 727 f.

Uppgiftsskyldighet och utlämnande av personuppgifter

15 §

Paragrafen, som behandlas i avsnitt 14.12.1, reglerar utlämnande för att framställa rättsstatistik. Den motsvarar nuvarande 2 kap. 14 § polisdatalogen (2010:361).

Bestämmelsen bryter den sekretess som kan gälla för personuppgifterna. Av 2 § förordningen (2016:1201) med instruktion för Brottsförebyggande rådet framgår att myndigheten ansvarar för kriminalstatistiken.

16 §

Paragrafen, som behandlas i avsnitt 14.12.3, innehåller sekretessbrytande bestämmelser om utlämnande till utländska myndigheter och mellanfolkliga organisationer. Den motsvarar nuvarande 2 kap. 15 § polisdatalogen (2010:361). I fråga om innebörden av bestämmelsen hänvisas till prop. 2009/10:85 s. 329 f.

17 §

Paragrafen innehåller en bestämmelse som bryter viss sekretess som annars skulle ha gällt gentemot Polismyndigheten. Den behandlas i avsnitt 14.12.2.

I paragrafen regleras Polismyndighetens rätt att, trots viss i paragrafen angiven sekretess till skydd för enskild, för vissa syften få del av personuppgifter som har gjorts gemensamt tillgängliga och som Säkerhetspolisen behandlar i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller fullgöra uppgifter i samband med personskydd. Paragrafen har utformats som en uppgiftsskyldighet. En förutsättning för att uppgifter ska lämnas ut är att Polismyndigheten behöver uppgifterna för att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott. Det är Säkerhetspolisen som avgör om Polismyndigheten behöver uppgifterna.

18 §

Paragrafen innehåller en bestämmelse som bryter viss sekretess som annars skulle ha gällt gentemot Försvarets radioanstalt och Försvarsmakten. Den behandlas i avsnitt 14.12.2.

I paragrafen regleras rätten för Försvarets radioanstalt och Försvarsmakten att, trots viss i paragrafen angiven sekretess till skydd för enskild, i försvarsunderrättelseverksamheten och den militära säkerhetstjänsten få del av personuppgifter som har gjorts gemensamt tillgängliga och som Säkerhetspolisen behandlar i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott. Paragrafen har utformats som en uppgiftsskyldighet. En förutsättning för att uppgifter ska lämnas ut är att uppgifterna behövs i försvarsunderrättelseverksamheten eller den militära säkerhetstjänsten. Det är Säkerhetspolisen som avgör om Försvarets radioanstalt och Försvarsmakten behöver uppgifterna.

19 §

Paragrafen reglerar elektroniskt utlämnande.

I *första stycket* föreskrivs att personuppgifter får lämnas ut elektroniskt på annat sätt än genom direktåtkomsten om det inte är olämpligt. En motsvarande bestämmelse finns i 2 kap. 16 § polisens brottsdatalog (2010:361). I fråga om innebörden av bestämmelsen hänvisas till kommentaren till den paragrafen. Frågan behandlas i avsnitt 14.11.1.

I *andra stycket* klargörs att elektroniskt utlämnande genom direktåtkomst bara får förekomma i den utsträckning som anges i 3 kap. 5–7 §§. Frågan behandlas i avsnitt 14.11.2. Vad direktåtkomst innebär utvecklas i avsnitt 5.6.1.

Personuppgifter från transportföretag

20 §

Paragrafen reglerar, tillsammans med 21 §, hur personuppgifter som ett transportföretag enligt 25 § polislagen (1984:387) tillhandahåller Säkerhetspolisen får behandlas. Regleringen avser uppgifter om ankommande eller avgående transporter av passagerare och fordon som företagen befordrar till och från Sverige. Det rör sig alltså om bokningsuppgifter i flyg- och färjetrafik. Paragrafen behandlas i avsnitt 14.8. Transportföretagens skyldighet att tillhandahålla uppgifter regleras alltså i polislagen.

I *första stycket* tydliggörs att personuppgifter från transportföretag endast får behandlas i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller för personskydd.

Av *andra stycket* framgår att personuppgifter får behandlas för ett nytt ändamål endast i ett enskilt fall. Ett typiskt exempel är att uppgifterna behövs i ett visst underrättelseärende. Att sådana uppgifter får göras gemensamt tillgängliga framgår av 3 kap. 2 §.

21 §

I paragrafen anges hur bokningsuppgifter som Säkerhetspolisen får del av genom terminalåtkomst får användas. Paragrafen, som motsvarar nuvarande 26 § andra stycket polislagen (1984:387), behandlas i avsnitt 14.8.

Paragrafen reglerar enbart behandling vid terminalåtkomst till personuppgifter hos transportföretag, medan 20 § anger vad som gäller i fråga om personuppgifter som förs över till myndighetens it-system eller behandlas strukturerat på annat sätt.

Genom terminalåtkomsten till företagens it-system får Säkerhetspolisen tillgång till omfattande överskottsinformation om resande. Myndigheten får inte ändra eller på annat sätt bearbeta uppgifter i sådana system. Syftet med regleringen är att myndigheten inte ska kunna föra över en hel sådan uppgiftssamling till sina egna it-system för att bearbeta, ändra och lagra personuppgifterna där. Som framgår av 20 § andra stycket får däremot uppgifter föras över i enskilda fall om förutsättningarna för det är uppfyllda.

Föreskrifter

22 §

I paragrafen upplyses om att regeringen kan meddela föreskrifter om att personuppgifter får lämnas ut även i andra fall än som anges i 15–18 §§ (vilket motsvarar nuvarande 2 kap. 19 § första stycket polisdatalagen), om begränsning av möjligheten att lämna ut personuppgifter elektroniskt på annat sätt än genom direktåtkomst och om underrättelseskyldighet och sökning i personuppgifter.

3 kap. Gemensamt tillgängliga uppgifter

Allmän bestämmelse

1 §

Av paragrafen, som behandlas i avsnitt 14.9.1, framgår att kapitlet innehåller bestämmelser om behandling av personuppgifter som görs eller har gjorts gemensamt tillgängliga. Vad som avses med

gemensamt tillgängliga uppgifter utvecklas i prop. 2009/10:85 s. 334 f.

Av *andra stycket* framgår att bestämmelserna i kapitlet inte gäller för behandling av personuppgifter med stöd av den särskilda bestämmelsen om behandling för diarieföring och nödvändiga handläggningsåtgärder i 2 kap. 3 §.

Personuppgifter som får göras gemensamt tillgängliga

2 §

Paragrafen reglerar vilka personuppgifter som får göras gemensamt tillgängliga. Frågan behandlas i avsnitt 14.9.1. Av paragrafen framgår att personuppgifter får göras gemensamt tillgängliga om det behövs för något av de syften som anges 2 kap. 1 §.

Särskilda upplysningar

3 §

Enligt paragrafen ska det framgå för vilket ändamål gemensamt tillgängliga uppgifter behandlas om det inte framgår av sammanhanget eller på något annat sätt. Paragrafen behandlas i avsnitt 14.9.2 och motsvarar nuvarande 6 kap. 9 § polisdatalagen (2010:361). I fråga om innebörden hänvisas till prop. 2009/10:85 s. 369 f.

4 §

Enligt paragrafen, som behandlas i avsnitt 14.9.2 och 14.10.2, ska uppgifter som är gemensamt tillgängliga förses med särskilda upplysningar i vissa fall. Den motsvarar nuvarande 6 kap. 10 § polisdatalagen (2010:361).

Enligt *första stycket* ska gemensamt tillgängliga uppgifter som direkt kan hänföras till en person som inte är misstänkt för brott eller för att ha utövat eller komma att utöva brottslig verksamhet förses med en särskild upplysning om det, om det inte på annat sätt framgår att personen inte är misstänkt. Det kan t.ex. framgå att personen är uppgiftslämnare. Genom hänvisningen till 2 kap. 1 §

första stycket 1 eller 2 klagörs att upplysningen ska avse om personen i fråga är misstänkt för brott eller brottslig verksamhet som Säkerhetspolisen har till uppgift att bekämpa.

Enligt *andra stycket* ska uppgifter om personer som kan antas ha direkt samband med sådan brottslig verksamhet som avses i 2 kap. 1 § första stycket 1 fördes med upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak. Kravet på samband är lågt ställt. Så snart det finns något som stöder ett antagande om att en person har direkt samband med sådan brottslig verksamhet och det är fråga om uppgifter som görs gemensamt tillgängliga ska uppgifterna om personen fördes med en särskild upplysning. Sambandet kan t.ex. bestå i att en person ofta träffar eller har annan kontakt med någon annan som är misstänkt för att utöva brottslig verksamhet eller rör sig i en miljö där brottslighet förekommer, utan att ha naturliga skäl att befinna sig där. Personuppgifter om den som är anhörig till en person som kan antas ha samband med misstänkt brottslig verksamhet faller alltså utanför, utom i de fall där båda kan antas ha samband med brottslig verksamhet.

Det är bara uppgifter som rör en person som behöver fördes med upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak. Det är, förutom uppgifter om på vilket sätt personen är knuten till den brottsliga verksamheten, framför allt fråga om uppgifter som belyser brottslighetens art och omfattning. Uppgifterna kan då behöva fördes med särskilda upplysningar för att personens anknytning till brottsligheten ska kunna bedömas.

Det krävs inte någon upplysning om det på grund av omständigheterna är onödigt. Det kan vara fallet om uppgiftslämnaren är en polisman eller någon annan vars trovärdighet är väl känd. Även i sådana fall kan det behövas en särskild upplysning om uppgifternas riktighet i sak, om inte källan framgår på annat sätt.

Av *tredje stycket* framgår att uppgifter som ingår i en uppgiftssamling som har skapats för att bearbeta och analysera information och som enbart särskilt angivna tjänstemän har tillgång till, inte behöver fördes med någon upplysning enligt *andra stycket* om bearbetningen inte har genomförts. Undantaget innebär att personuppgifter i en sådan uppgiftssamling får göras gemensamt tillgängliga trots att de inte har hunnit fördes med upplysningar om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak. Så snart bearbetningen är genomförd och uppgifterna kopplats till

annan information måste personuppgifterna kompletteras med sådana upplysningar om det behövs.

Undantaget är kopplat till om bearbetningen av uppgifterna är genomförd. Hur lång tid det kan ta kan variera beroende på bl.a. mängden information och uppgifternas karaktär. Utgångspunkten är att bearbetningen ska genomföras så snart som möjligt.

I 4 kap. 9 § anges hur länge uppgifter i en sådan uppgiftssamling får behandlas.

Direktåtkomst

5 §

I paragrafen föreskrivs att Polismyndigheten under vissa förutsättningar får medges direktåtkomst till personuppgifter som Säkerhetspolisen behandlar. Paragrafen behandlas i avsnitt 14.11.2 och 14.11.3.

Direktåtkomsten får bara avse personuppgifter som har gjorts gemensamt tillgängliga och som Säkerhetspolisen behandlar i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller fullgöra uppgifter i samband med personskydd.

Möjligheten att ge Polismyndigheten direktåtkomst begränsas till personuppgifter som behövs för något av de syften som anges i 2 kap. 1 § första stycket 1 och 2 polisens brottsdatalog (2010:361). Det innebär att Polismyndigheten bara får ta del av uppgifter genom direktåtkomst för att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott. Om Polismyndigheten behöver få tillgång till personuppgifter för att utföra andra arbetsuppgifter ska uppgifterna lämnas på något annat sätt.

Paragrafen innebär inte att Polismyndigheten har rätt till direktåtkomst. En bestämmelse om direktåtkomst anger endast i vilken form personuppgifter får tillhandahållas. Det är Säkerhetspolisen som avgör om personuppgifterna kan lämnas på det sättet. Möjligheten att tillhandahålla vissa personuppgifter genom direktåtkomst kan också begränsas av att uppgifterna är skyddade av sekretess. I 2 kap. 17 § finns en sekretessbrytande bestämmelse. Direktåtkomsten kan begränsas till t.ex. en viss typ av uppgifter, enskilda upp-

giftssamlingar eller ärenden eller till uppgifter om vissa företeelser som har anknytning till en viss person eller händelse.

6 §

I paragrafen anges att Försvarets radioanstalt och Försvarsmakten under vissa förutsättningar får medges direktåtkomst till personuppgifter som behandlas av Säkerhetspolisen. Frågan behandlas i avsnitt 14.11.3.

Försvarsunderrättelsemyndigheterna får endast medges direktåtkomst inom ramen för försvarsunderrättelseverksamheten och den militära säkerhetstjänsten. Direktåtkomsten får bara avse personuppgifter som har gjorts gemensamt tillgängliga och som Säkerhetspolisen behandlar i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott.

Paragrafen innebär inte att de mottagande myndigheterna har rätt till direktåtkomst. En bestämmelse om direktåtkomst anger endast i vilken form personuppgifter får lämnas ut. Möjligheten att lämna ut vissa personuppgifter genom direktåtkomst kan vara begränsad genom att uppgifterna är skyddade av sekretess. Det finns en sekretessbrytande bestämmelse i 2 kap. 18 §.

Säkerhetspolisen avgör om den kan medge försvarsunderrättelsemyndigheterna direktåtkomst och i vilken omfattning. Direktåtkomsten kan begränsas t.ex. till en viss typ av uppgifter eller på annat lämpligt sätt.

7 §

I paragrafen regleras Säkerhetspolisens möjlighet att medge underrättelse- och säkerhetstjänster inom EU och EES direktåtkomst till vissa personuppgifter. Paragrafen behandlas i avsnitt 14.11.4.

I *första stycket* anges förutsättningarna för att direktåtkomst ska kunna medges. Möjligheten att dela information genom direktåtkomst begränsas till underrättelse- och säkerhetstjänster i medlemsstater inom EU och EES. Underrättelse- och säkerhetstjänsterna får endast medges direktåtkomst om det behövs för samarbetet mot terrorism. Direktåtkomsten får endast avse personuppgifter som Säkerhetspolisen behandlar i syfte att förebygga, förhindra

eller upptäcka brottslig verksamhet som innefattar terrorbrott. Det kan även vara fråga om uppgifter som har kommit fram vid utredning av eller lagföring för terrorbrott och som Säkerhetspolisen fortsätter att behandla med stöd av 2 kap. 1 § första stycket 1 b.

Direktåtkomst får endast medges till en avskild uppgiftssamling som Säkerhetspolisen upprättat i syfte att dela sådan information som rör arbete mot terrorism med de aktuella mottagarna. Personuppgifter som Säkerhetspolisen avser att dela med utländska underrättelse- eller säkerhetstjänster måste således först föras över till en särskild uppgiftssamling.

Innan personuppgifter tillförs en sådan uppgiftssamling måste Säkerhetspolisen avgöra om det finns sakliga skäl att låta utländska underrättelse- och säkerhetstjänster få del av uppgifterna, dvs. om det finns behov av att lämna ut uppgifterna för att främja bekämpningen av terrorism. Innan uppgifterna förs över ska Säkerhetspolisen bedöma om det finns rättsliga förutsättningar att lämna ut uppgifterna till utländska mottagare, bl.a. om sekretess hindrar det.

Av *andra stycket* framgår att Säkerhetspolisen ska underrätta regeringen innan direktåtkomst medges en utländsk underrättelse- eller säkerhetstjänst enligt paragrafen. Underrättelseskyldigheten omfattar enbart det förhållandet att Säkerhetspolisen avser att dela information genom direktåtkomst, inte innehållet i informationen.

Föreskrifter

8 §

I paragrafen upplyses om att regeringen kan meddela föreskrifter om underrättelseskyldighet vid direktåtkomst. Det är underrättelseskyldigheten i 7 § andra stycket som avses.

9 §

I paragrafen upplyses om att regeringen, eller den myndighet som regeringen bestämmer, kan meddela föreskrifter om bl.a. omfattningen av direktåtkomsten och om behörighet och säkerhet när personuppgifter lämnas ut på det sättet.

4 kap. Längsta tid som personuppgifter får behandlas

Allmän bestämmelse

1 §

Paragrafen, som behandlas i avsnitt 14.13.2, innehåller en generell bestämmelse om hur länge Säkerhetspolisen får behandla personuppgifter.

I *första stycket* föreskrivs att personuppgifter inte får behandlas under längre tid än vad som behövs för något eller några av de syften som anges i 2 kap. 1–3 §§. Bestämmelsen motsvarar nuvarande 6 kap. 6 § första stycket polisdatalagen (2010:361). Regleringen gäller vid all behandling av personuppgifter som omfattas av lagens tillämpningsområde, dvs. såväl automatiserad behandling som annan behandling av personuppgifter som ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier (se 1 kap. 3 §).

Personuppgifter behandlas ibland för flera olika syften samtidigt. Att det inte längre finns behov av att behandla personuppgiften för ett visst syfte medför inte att behandlingen av den måste upphöra för alla andra syften samtidigt. Å andra sidan innebär det förhållandet att personuppgiften fortfarande behövs för ett visst syfte inte att den får fortsätta att behandlas för alla syften lika länge.

Bestämmelsen ger exempelvis stöd för fortsatt behandling av personuppgifter i ett avslutat ärende om uppgifterna bedöms ha ett allmänt värde för Säkerhetspolisens verksamhet att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott. En grundläggande förutsättning för fortsatt behandling är att Säkerhetspolisen bedömer att uppgifterna behöver finnas tillgängliga ytterligare en viss tid för brottsbekämpning eller lagföring eller något annat av de ändamål för vilka Säkerhetspolisen får behandla personuppgifter.

Behandlingen av personuppgifterna ska upphöra så snart det står klart att de inte längre behövs för något av de syften som anges i lagen. När det gäller ostrukturerad underrättelseinformation kan det vara särskilt svårt att bedöma det fortsatta behovet av behandling. Bedömningen måste innan bearbetningen är genomförd göras

på ett mer övergripande plan och i större utsträckning utgå från sannolikheten av att personuppgifterna kan komma att behövas i verksamheten än en reell bedömning av den enskilda uppgiften.

Av *andra stycket* framgår att bestämmelsen om längsta tid för behandling inte hindrar att Säkerhetspolisen arkiverar och bevarar allmänna handlingar eller att arkivmaterial lämnas till en arkivmyndighet. Bestämmelsen tydliggör att arkivlagstiftningen i fråga om allmänna handlingar har företräde framför lagens bestämmelser om längsta tid för behandling.

I *tredje stycket* föreskrivs att övriga bestämmelser i kapitlet, som anger hur länge en viss typ av personuppgifter får behandlas inom den ram som sätts av huvudregeln i första stycket, endast gäller vid automatiserad behandling. Det innebär att de paragraferna inte gäller för annan strukturerad behandling som omfattas av lagens tillämpningsområde.

Oavsett vilken bedömning som görs av nyttan med behandlingen av en viss personuppgift får den inte behandlas längre än vad som anges i respektive paragraf. Om det redan vid en tidigare tidpunkt står klart att uppgifterna saknar betydelse för det syfte för vilket de behandlas, ska behandlingen upphöra då.

Personuppgifter som inte har gjorts gemensamt tillgängliga

2 §

I paragrafen, som motsvarar nuvarande 6 kap. 7 § polisdatalagen (2010:361), anges hur länge personuppgifter som inte har gjorts gemensamt tillgängliga får behandlas. Paragrafen behandlas i avsnitt 14.13.3.

Enligt *första stycket* får personuppgifter som behandlas i ett ärende inte behandlas längre än ett år efter det att ärendet avslutades, medan uppgifter som inte hör till något ärende inte får behandlas längre än ett år efter det att de behandlades automatiserat första gången. Vad som avses med ett ärende i denna paragraf utvecklas i prop. 2009/10:85 s. 328.

Det klargörs att uppgifterna, trots det som sägs 1 § andra stycket om att arkivlagstiftningen har företräde, inte får arkiveras digitalt. Utgångspunkten är alltså att all automatiserad behandling av personuppgifterna ska upphöra när den tid som anges i para-

grafen har löpt ut, vilket innebär att de ska tas bort. Endast om det har meddelats uttryckliga föreskrifter som innebär att uppgifterna i fråga får behandlas för arkivändamål av allmänt intresse eller för vetenskapliga, statistiska eller historiska ändamål får de behandlas automatiserat längre än vad som anges i denna paragraf (jfr 13 §).

Enligt *andra stycket* gäller paragrafen inte personuppgifter i ärenden om utredning av eller lagföring för brott.

Gemensamt tillgängliga uppgifter i ärenden om utredning av eller lagföring för brott

3 §

I paragrafen, som motsvarar nuvarande 3 kap. 10 § polisdatalagen (2010:361), anges hur länge personuppgifter i en anmälan om brott får behandlas. Paragrafen behandlas i avsnitt 14.13.6. I fråga om innebörden av regleringen hänvisas till prop. 2009/10:85 s. 347.

Enligt paragrafen inskränks enbart behandlingen av personuppgifter för de ändamål som regleras i lagen, vilket innebär att uppgifterna får fortsätta att behandlas automatiserat för t.ex. arkivändamål efter de tidpunkter som anges i paragrafen.

4 §

Paragrafen, som motsvarar nuvarande 3 kap. 11 § polisdatalagen (2010:361), reglerar hur länge personuppgifter i förundersökningar och andra utredningar som handläggs enligt bestämmelserna i 23 kap. rättegångsbalken får behandlas. Paragrafen behandlas i avsnitt 14.13.6. I fråga om innebörden av bestämmelsen hänvisas till prop. 2009/10:85 s. 347 f. Enligt paragrafen inskränks enbart behandlingen av personuppgifter för de ändamål som regleras i lagen. Det innebär att uppgifterna får fortsätta att behandlas automatiserat för t.ex. arkivändamål efter de tidpunkter som anges.

I *första stycket* anges hur länge personuppgifter i mål och ärenden som varit föremål för domstolsprövning får behandlas. I *andra stycket* regleras hur länge personuppgifter i nedlagda förundersökningar får behandlas. Av *tredje stycket* framgår att regleringen i

paragrafen även ska tillämpas på andra utredningar som handläggs enligt bestämmelser i 23 kap. rättegångsbalken.

5 §

Paragrafen, som behandlas i avsnitt 14.13.6 och motsvarar nuvarande 3 kap. 13 § polisdatalagen (2010:361), reglerar vad som gäller i fråga om personuppgifter som rör någon som har varit misstänkt i en förundersökning som har lagts ner eller där åtal har lagts ner eller frikännande dom har meddelats och fått laga kraft. En sådan person får då inte längre vara sökbar som misstänkt. I fråga om innebörden av regleringen hänvisas till prop. 2009/10:85 s. 348 f.

Övriga gemensamt tillgängliga uppgifter

6 §

I paragrafen anges att det i de följande paragraferna regleras hur vissa typer av gemensamt tillgängliga personuppgifter som inte förekommer i ärenden om utredning av eller lagföring för brott som längst får behandlas. Det klargörs att uppgifterna, trots det som sägs i 1 § andra stycket om att arkivlagstiftningen har företräde, inte får arkiveras digitalt. Utgångspunkten är alltså att all automatiserad behandling av personuppgifterna ska upphöra när den tid som anges i 7–11 §§ har löpt ut, vilket innebär att uppgifterna ska tas bort. Endast om det har meddelats uttryckliga föreskrifter som innebär att uppgifterna i fråga får behandlas för arkivändamål av allmänt intresse eller för vetenskapliga, statistiska eller historiska ändamål får de behandlas automatiserat längre än vad som anges i de följande paragraferna (jfr 13 §).

7 §

Paragrafen, som motsvarar nuvarande 6 kap. 12 § första stycket polisdatalagen (2010:361), reglerar hur länge personuppgifter som avses i 2 kap. 1 § första stycket 1, och som har gjorts gemensamt tillgängliga, får behandlas. Paragrafen behandlas i avsnitt 14.13.4.

Huvudregeln i *första stycket* innebär att personuppgifter som har gjorts gemensamt tillgängliga inte får behandlas längre än tio år efter utgången av det kalenderår då den senaste registreringen gjordes avseende personens anknytning till brottslig verksamhet. Registrering av t.ex. ändrade bostadsförhållanden eller något annat som inte har betydelse för anknytningen till den brottsliga verksamheten påverkar alltså inte hur länge uppgifterna får behandlas. Det saknar också betydelse om uppgifterna har samband med den först aktuella brottsliga verksamheten eller registreras av något annat skäl (jfr prop. 2009/10:85 s. 372).

Uppgifter om en person som vid tiden för registreringen inte fyllt 18 år får dock enligt *andra stycket* inte behandlas längre än fem år efter utgången av det kalenderår då den senaste registreringen gjordes avseende den unges anknytning till brottslig verksamhet. Femårsfristen gäller bara registreringar som har gjorts innan den unge fyllt 18 år. Om nya uppgifter om honom eller henne registreras därefter, förlängs tidsfristen för alla uppgifter enligt huvudregeln i första stycket.

8 §

Paragrafen reglerar hur länge personuppgifter som avses i 2 kap. 1 § första stycket 3–5, och som har gjorts gemensamt tillgängliga, får behandlas. Paragrafen behandlas i avsnitt 14.13.4.

Huvudregeln i *första stycket* innebär att sådana personuppgifter som har gjorts gemensamt tillgängliga och som behandlas för bl.a. personskydd, säkerhetsskydd och för handägning av frågor enligt utlännings- eller medborgarskapslagstiftningen inte får behandlas längre än tio år efter utgången av det kalenderår då den senaste registreringen beträffande personen gjordes.

Om uppgiften rör en person under 18 år är tiden som framgår av *andra stycket* längst fem år, om inte en ny registrering beträffande den unge har gjorts innan han eller hon har fyllt 18 år. Om nya uppgifter om honom eller henne registreras senare och de är av den arten att de påverkar hur länge personuppgifterna får behandlas, förlängs tidsfristen för alla uppgifter enligt huvudregeln i första stycket.

9 §

Paragrafen, som motsvarar nuvarande 6 kap. 12 § andra stycket polisdatalagen (2010:361), reglerar hur länge uppgifter i sådana särskilda uppgiftssamlingar som avses i 3 kap. 4 § tredje stycket får behandlas. Paragrafen behandlas i avsnitt 14.13.4.

I *punkten 1* föreskrivs att uppgifter i uppgiftssamlingar som behandlas i underrättelseverksamhet får behandlas längst tre år efter utgången av det kalenderår då den senaste registreringen gjordes avseende personens anknytning till brottslig verksamhet. Enligt *punkten 2* får uppgifter som Säkerhetspolisen behandlar för andra syften i en sådan uppgiftssamling inte behandlas längre än tre år efter utgången av det kalenderår då den senaste registreringen gjordes avseende personen.

Om nya uppgifter om personen samlas in förlängs alltså tidsfristen, under förutsättning att uppgifterna är av den arten att de påverkar hur länge personuppgifterna får behandlas. Vad det innebär utvecklas i kommentaren till 7 §.

10 §

Paragrafen anger hur länge personuppgifter som hänför sig till sådan säkerhetshotande verksamhet som avses i 18 och 19 kap. brottsbalken och som utövas av främmande makt får behandlas. Frågan behandlas i avsnitt 14.13.5.

Sådana personuppgifter som anges i paragrafen får behandlas längst 40 år efter utgången av det kalenderår då den senaste registreringen gjordes avseende personens anknytning till brott eller brottslig verksamhet. Den tidsfristen gäller dock inte personuppgifter som behandlas i sådana särskilda uppgiftssamlingar som avses i 3 kap. 4 § tredje stycket. För sådana personuppgifter gäller 9 § även om uppgifterna hänför sig till sådan säkerhetshotande verksamhet som avses i 18 och 19 kap. brottsbalken.

Uppgifter som hänför sig till sådan säkerhetshotande verksamhet kan t.ex. vara uppgifter där grunden för registreringen är att personen antas vara utländsk underrättelseofficer och hans eller hennes anhöriga. Det kan också vara uppgifter om personer som misstänks för spioneri eller andra brott enligt 18 och 19 kap. brottsbalken som främmande makt står bakom och om personer

med anknytning till dem. Registreringen kan även avse händelser kopplade till dessa personer.

11 §

I paragrafen, som motsvarar nuvarande 6 kap. 12 § tredje stycket polisdatalagen (2010:361), ges Säkerhetspolisen möjlighet att, om det finns särskilda skäl, genom ett beslut i det enskilda fallet förlänga tidsfristen för behandlingen av vissa personuppgifter. Paragrafen behandlas i avsnitt 14.13.7. Vad regleringen innebär utvecklas i prop. 2009/10:85 s. 372.

Tidsfristerna om tio respektive tre år motsvarar den nuvarande regleringen. Samma tid gäller även om personuppgifterna rör någon som inte har fyllt 18 år. Den gäller också för sådana personuppgifter som anges i 10 §.

Föreskrifter

12 §

I paragrafen, som motsvarar nuvarande 3 kap. 12 § polisdatalagen (2010:361) och behandlas i avsnitt 14.13.8, upplyses om att regeringen kan meddela föreskrifter om att vissa kategorier av personuppgifter i en brottsanmälan, förundersökning eller annan utredning om brott får fortsätta att behandlas för ändamål inom lagens tillämpningsområde under längre tid än vad som anges i respektive paragraf i kapitlet.

13 §

I paragrafen, som behandlas i avsnitt 14.13.8, upplyses om att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter dels om avvikelse från bestämmelserna i 2 § första stycket och 7–11 §§ att personuppgifter får behandlas under längre tid för arkivändamål av allmänt intresse och vetenskapliga, statistiska eller historiska ändamål (vilket motsvarar nuvarande 6 kap. 7 § tredje stycket och 6 kap. 14 § polisdatalagen [2010:361]), dels om begränsning av behandlingen av personuppgifter för ända-

mål inom lagens tillämpningsområde vid digital arkivering (vilket motsvarar nuvarande 6 kap. 6 § tredje stycket polisdatalagen).

5 kap. Skyldigheter som personuppgiftsansvarig

Åtgärder för att säkerställa författningenlig behandling

Tekniska och organisatoriska åtgärder

1 §

Paragrafen reglerar, tillsammans med 2–4 §§, de krav som ställs på Säkerhetspolisen i fråga om tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen av personuppgifter är författningenlig och att registrerades rättigheter skyddas. Tekniska och organisatoriska åtgärder för att skydda personuppgifterna regleras i 7 §.

Paragrafen, som behandlas i avsnitt 14.14, motsvarar 3 kap. 2 § brottsdatalagen (2018:000). Vad regleringen innebär utvecklas i SOU 2017:29 s. 699 f.

I 16 § upplyses om att det kan finnas föreskrifter på lägre nivå om sådana åtgärder som avses i paragrafen.

2 §

Paragrafen, som behandlas i avsnitt 14.14, reglerar skyldigheten att beakta principen om inbyggt dataskydd vid behandling av personuppgifter. Paragrafen kan ses som en precisering av den övergripande skyldigheten i 1 § och är också tätt förknippad med regleringen i 3 och 7 §§.

Paragrafen motsvarar 3 kap. 3 § brottsdatalagen (2018:000). Vad bestämmelsen innebär utvecklas i SOU 2017:29 s. 700 f.

I 16 § upplyses om att det kan finnas föreskrifter på lägre nivå om sådana åtgärder som avses i paragrafen.

3 §

Paragrafen, som behandlas i avsnitt 14.14, föreskriver att Säkerhetspolisen är skyldig att i automatiserade behandlingssystem införa dataskydd som standard. Paragrafen kan i likhet med 2 § ses som en precisering av den övergripande skyldigheten i 1 §.

Paragrafen motsvarar 3 kap. 4 § brottsdatalagen (2018:000). Vad bestämmelsen innebär utvecklas i SOU 2017:29 s. 701 f.

I 16 § upplyses om att det kan finnas föreskrifter på lägre nivå om sådana åtgärder som avses i paragrafen.

4 §

Paragrafen, som behandlas i avsnitt 14.14, reglerar Säkerhetspolisens skyldighet att säkerställa att det i automatiserade behandlingssystem förs loggar över vissa typer av behandlingar.

Paragrafen motsvarar 3 kap. 5 § brottsdatalagen (2018:000). Vad bestämmelsen innebär utvecklas i SOU 2017:29 s. 702 f. Paragrafen gäller enligt 15 § även för personuppgiftsbiträden som Säkerhetspolisen anlitar.

I 16 § upplyses om att det kan finnas föreskrifter på lägre nivå om sådana åtgärder som avses i paragrafen.

Tillgången till personuppgifter

5 §

Paragrafen, som behandlas i avsnitt 14.14, reglerar den interna tillgången till personuppgifter för dem som arbetar vid Säkerhetspolisen.

Paragrafen motsvarar 3 kap. 6 § brottsdatalagen (2018:000). Vad bestämmelsen innebär utvecklas i SOU 2017:29 s. 703 f. Paragrafen gäller enligt 15 § även för personuppgiftsbiträden som Säkerhetspolisen anlitar.

I 16 § upplyses om att det kan finnas föreskrifter på lägre nivå om sådana åtgärder som avses i paragrafen.

Konsekvensbedömning och förhandssamråd

6 §

Paragrafen, som behandlas i avsnitt 14.14, slår fast Säkerhetspolisens skyldighet att inför vissa behandlingar göra en konsekvensbedömning och samråda med tillsynsmyndigheten. Paragrafen motsvarar 3 kap. 7 § brottsdatalagen (2018:000).

Av *första stycket* framgår att en konsekvensbedömning ska göras om det kan antas att en viss typ av ny behandling kommer att medföra särskild risk för intrång i registrerades personliga integritet. Detsamma gäller vid betydande förändringar av redan pågående behandling som kan antas medföra sådan risk. Vad regleringen innebär utvecklas i SOU 2017:29 s. 704.

Andra stycket reglerar s.k. förhandssamråd. När en konsekvensbedömning pekar på att det finns särskild risk för intrång i registrerades personliga integritet eller när typen av behandling innebär särskild risk för intrång, ska Säkerhetspolisen samråda med tillsynsmyndigheten. Vad det innebär utvecklas i SOU 2017:29 s. 704. Tillsynsmyndighetens roll vid förhandssamråd regleras i 7 kap. 1 § 2.

I 16 § upplyses om att det kan finnas föreskrifter på lägre nivå om sådana åtgärder som avses i paragrafen.

Säkerheten för personuppgifter

7 §

I paragrafen, som behandlas i avsnitt 14.14, regleras Säkerhetspolisens skyldighet att genom lämpliga tekniska och organisatoriska åtgärder skydda de personuppgifter som behandlas.

Paragrafen motsvarar 3 kap. 8 § brottsdatalagen (2018:000). Vad bestämmelsen innebär utvecklas i SOU 2017:29 s. 705 f. Paragrafen gäller enligt 15 § även för personuppgiftsbiträden som Säkerhetspolisen anlitar.

I 16 § upplyses om att det kan finnas föreskrifter på lägre nivå om sådana åtgärder som avses i paragrafen.

Samarbete med tillsynsmyndigheten

8 §

I paragrafen, som behandlas i avsnitt 14.14, regleras Säkerhetspolisens skyldighet att samarbeta med tillsynsmyndigheten. Paragrafen motsvarar 3 kap. 12 § brottsdatalagen (2018:000). Skyldigheten omfattar enbart samarbete med den myndighet som enligt lagen har utsetts till tillsynsmyndighet. I 7 kap. 3 § finns ytterligare bestämmelser om skyldighet att bistå tillsynsmyndigheten.

Paragrafen gäller enligt 15 § även för personuppgiftsbiträden som Säkerhetspolisen anlitar.

Dataskyddsombud

9 §

Paragrafen, som behandlas i avsnitt 14.14, reglerar Säkerhetspolisens skyldighet att utse dataskyddsombud. Dataskyddsombud definieras i 1 kap. 9 §. Paragrafen motsvarar 3 kap. 13 § brottsdatalagen (2018:000).

I paragrafen föreskrivs att ett eller flera dataskyddsombud ska utses. Dataskyddsombudet ska vara anställd hos myndigheten. Säkerhetspolisen ska anmäla till tillsynsmyndigheten när dataskyddsombud utses och entledigas.

10 §

I paragrafen, som behandlas i avsnitt 14.14, anges vilka uppgifter dataskyddsombud ska utföra. Paragrafen motsvarar 3 kap. 14 § brottsdatalagen (2018:000). Vad bestämmelsen innebär både i fråga om interna uppgifter, samarbete med tillsynsmyndigheten och kontakter med enskilda utvecklas i SOU 2017:29 s. 710 f.

11 §

Paragrafen, som behandlas i avsnitt 14.14, reglerar dataskyddsbudens skyldighet att anmäla brister till tillsynsmyndigheten. Paragrafen motsvarar 3 kap. 15 § brottsdatalagen (2018:000). Vad bestämmelsen innebär utvecklas i SOU 2017:29 s. 712.

Personuppgiftsbiträden

12 §

Av paragrafen framgår att personuppgiftsbiträden får anlitas om det är lämpligt och vad Säkerhetspolisen måste göra innan ett personuppgiftsbiträde anlitas. Personuppgiftsbiträde definieras i 1 kap. 9 §. Paragrafen, som behandlas i avsnitt 14.14, motsvarar 3 kap. 17 § brottsdatalagen (2018:000). Vad bestämmelsen innebär utvecklas i SOU 2017:29 s. 712 f.

13 §

Paragrafen reglerar förhållandet mellan Säkerhetspolisen och personuppgiftsbiträden. Den behandlas i avsnitt 14.14 och motsvarar 3 kap. 18 § brottsdatalagen (2018:000).

I *första stycket* regleras kravet på att det ska finnas ett skriftligt avtal eller en annan skriftlig överenskommelse med personuppgiftsbiträden. I *andra stycket* föreskrivs att personuppgiftsbiträdet inte får anlita underbiträden utan skriftligt tillstånd från Säkerhetspolisen. Vad regleringen innebär utvecklas i SOU 2017:29 s. 713.

I 16 § upplyses om att det kan finnas föreskrifter på lägre nivå om innehållet i sådana avtal och överenskommelser som avses i första stycket.

14 §

Paragrafen, som behandlas i avsnitt 14.14, reglerar vad som gäller vid behandling av personuppgifter hos ett personuppgiftsbiträde. Paragrafen motsvarar 3 kap. 19 § brottsdatalagen (2018:000).

I *första stycket* slås fast att personuppgiftsbiträdet och de som arbetar under bitrådets ledning bara får behandla personuppgifter i enlighet med instruktioner från Säkerhetspolisen.

Av *andra stycket* framgår att ett personuppgiftsbiträde som i strid med Säkerhetspolisens instruktioner fastställer ändamålen med och medlen för behandlingen anses vara personuppgiftsansvarig för den behandlingen.

Vad regleringen innebär utvecklas i SOU 2017:29 s. 714.

15 §

I paragrafen föreskrivs vilka skyldigheter som gäller för personuppgiftsbiträden. Paragrafen, som behandlas i avsnitt 14.14, motsvarar 3 kap. 20 § brottsdatalogen (2018:000).

Hänvisningen till 4 och 5 §§ innebär att de personuppgiftsbiträden som Säkerhetspolisens anlitar är skyldiga att dels säkerställa att loggar förs i automatiserade behandlingssystem, dels se till att anställda bara ges tillgång till de personuppgifter som krävs för att fullgöra arbetsuppgifterna. Innebörden av bestämmelserna framgår av SOU 2017:29 s. 702 f.

Skyldigheten enligt 7 § att vidta lämpliga skyddsåtgärder gäller även för personuppgiftsbiträden. Innebörden av skyldigheten utvecklas i SOU 2017:29 s. 705 f.

Personuppgiftsbiträden är också, genom hänvisningen till 8 §, skyldiga att i samma utsträckning som Säkerhetspolisen samarbeta med tillsynsmyndigheten. Innebörden av skyldigheten framgår av kommentaren till den paragrafen. Vad skyldigheten därutöver kan innebära utvecklas i SOU 2017:29 s. 714 f.

Att personuppgiftsbiträden åläggs vissa skyldigheter frántar inte Säkerhetspolisen dess ansvar. Säkerhetspolisen är, som framgår av kommentaren till 1 kap. 7 §, ansvarig för den behandling av personuppgifter som personuppgiftsbiträdet utför på myndighetens vägnar. Den omständigheten att personuppgiftsbiträden ges en direkt skyldighet att vidta vissa åtgärder innebär dock att tillsynsmyndigheten vid brister kan vidta åtgärder mot både personuppgiftsbiträdet och Säkerhetspolisen.

Föreskrifter

16 §

I paragrafen, som behandlas i avsnitt 14.14, upplyses om att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter om sådana åtgärder som avses i 1–4, 6 och 7 §§, om tillgången till personuppgifter, om skyldigheten att föra register över kategorier av behandlingar av personuppgifter, om skyldigheten att införa rutiner för anmälan av överträdelser och om innehållet i sådana avtal och överenskommelser som avses i 13 §.

6 kap. Enskildas rättigheter

Rätten till information

Allmän information

1 §

I paragrafen, som behandlas i avsnitt 14.15, anges vilken allmän information som Säkerhetspolisen på eget initiativ ska göra tillgänglig för registrerade. Informationen, som riktar sig till allmänheten eller en obestämd, större krets av registrerade, kan göras tillgänglig t.ex. på myndighetens webbplats. Paragrafen motsvarar 4 kap. 1 § brottsdatalagen (2018:000).

Enligt *punkten 1* ska myndighetens identitet och kontaktuppgifter göras tillgängliga. Med det avses uppgifter om myndighetens namn, post- och besöksadress, telefonnummer och e-postadress.

Säkerhetspolisen är enligt 5 kap. 9 § skyldig att utse dataskyddsombud. Enligt *punkten 2* ska dataskyddsombudets kontaktuppgifter anges. Det behöver inte vara en kontaktuppgift direkt till dataskyddsombudet, t.ex. hans eller hennes e-postadress, utan det är tillräckligt att ombudet går att nå med hjälp av uppgifterna.

I *punkten 3* föreskrivs att ändamålen med behandlingen ska framgå. Det är inte ändamålen med behandlingen av personuppgifter i enskilda fall som avses utan för vilka typer av ändamål som myndigheten behandlar personuppgifter. Det kan vara förundersökning, underrättelsearbete och åtgärder inom ett särskilt verksamhetsområde, t.ex. kontraterrorism, eller åtgärder som vidtas

inom ramen för säkerhetsskyddsarbetet, exempelvis säkerhetsprovning och registerkontroll.

I *punkterna 4 och 5* föreskrivs att Säkerhetspolisen ska upplysa om de rättigheter som enskilda har enligt 2, 6 och 7 §§. Det gäller rätten för registrerade att få information om behandlingen av personuppgifter och att få del av dem och rätten att begära rättelse, komplettering, radering eller begränsning av behandlingen.

I 10 § upplyses om att det kan finnas föreskrifter på lägre nivå om sådan information som regleras i denna paragraf.

Personrelaterad information

2 §

I paragrafen regleras enskildas rätt att få besked om huruvida deras personuppgifter behandlas, att få del av sådana uppgifter och att få viss information om behandlingen av dem. Paragrafen behandlas i avsnitt 14.15 och motsvarar 4 kap. 3 § brottsdatalogen (2018:000).

I *första stycket* anges vilken information sökanden kan få del av. I *andra stycket* undantas sådana personuppgifter som sökanden har tagit del av från skyldigheten att lämna ut uppgifterna. Sökanden ska dock informeras om att personuppgifterna i fråga behandlas. Vad regleringen innebär utvecklas i SOU 2017:29 s. 719 f.

I 9 § föreskrivs att informationen ska lämnas till den registrerade avgiftsfritt en gång per år och att utlämnande därutöver kan avgiftsbeläggas. Om en begäran om information är orimlig eller uppenbart ogrundad får den avslås enligt 5 § första stycket. Beslut att vägra att lämna information får enligt 8 kap. 2 § överklagas.

I 10 § upplyses om att det kan finnas föreskrifter på lägre nivå om sådan information som regleras i denna paragraf och om kraven på en begäran om information.

Begränsning av rätten till information

3 §

I paragrafen, som behandlas i avsnitt 14.15, görs undantag från Säkerhetspolisens informationsskyldighet. Paragrafen är delvis utformad efter mönster av 27 § personuppgiftslagen (1998:204).

Enligt *första stycket* gäller Säkerhetspolisens skyldighet att tillhandahålla personrelaterad information enligt 2 § inte i den utsträckning det är särskilt föreskrivet i lag eller annan författning eller annars framgår av beslut som har meddelats med stöd av författning att uppgifterna inte får lämnas ut. Det är främst sekretess och tystnadsplikt enligt offentlighets- och sekretesslagen som avses. Även andra bestämmelser om tystnadsplikt och bestämmelser som begränsar möjligheten att använda uppgifter som en svensk myndighet har fått från en myndighet i en annan stat kan begränsa informationsskyldigheten. Regleringen innebär att Säkerhetspolisen får begränsa eller utelämna informationen. Undantaget från informationsskyldigheten gäller även vid beslut som har meddelats med stöd av författning, t.ex. beslut om förbehåll enligt 10 kap. 4 eller 4 a § offentlighets- och sekretesslagen (2009:400).

Säkerhetspolisen är enligt *andra stycket* inte heller skyldig att lämna ut skälen för beslut enligt första stycket och beslut i fråga om rättelse, radering eller begränsning av behandlingen om motiveringen skulle riskera att skada något av de intressen som sekretessen eller tystnadsplikten avser att skydda.

4 §

I paragrafen föreskrivs i *första stycket* undantag från informationskyldigheten i 2 § för personuppgifter i viss typ av text. Undantaget gäller dock enligt *andra stycket* inte i vissa fall. Paragrafen, som behandlas i avsnitt 14.15, motsvarar 4 kap. 6 § brottsdatalagen (2018:000). Vad regleringen innebär utvecklas i SOU 2017:29 s. 723 f.

5 §

I paragrafen föreskrivs att information enligt 2 § inte behöver lämnas om begäran är orimlig eller uppenbart ogrundad. Paragrafen, som behandlas i avsnitt 14.15, motsvarar 4 kap. 7 § brottsdatalagen (2018:000).

Enligt *första stycket* får Säkerhetspolisen avslå en begäran om information om behandlingen av personuppgifter och att få del av

uppgifterna om begäran är orimlig eller uppenbart oggrundad. Vad regleringen innebär utvecklas i SOU 2017:29 s. 724 f.

I *andra stycket* upplyses det om att myndigheten med stöd av 9 § andra stycket i vissa fall får ta ut avgift i stället för att avslå begäran.

Rätten till rättelse, radering och begränsning av behandlingen

6 §

Paragrafen reglerar enskildas rätt att begära rättelse eller komplettering av felaktiga eller ofullständiga personuppgifter. Paragrafen, som behandlas i avsnitt 14.15, motsvarar 4 kap. 9 § brottsdatalagen (2018:000). I 2 kap. 13 § regleras Säkerhetspolisens skyldighet att på eget initiativ rätta felaktiga eller ofullständiga personuppgifter och uppdatera inaktuella personuppgifter.

I *första stycket* regleras registrerades rätt att begära rättelse eller komplettering. Om Säkerhetspolisen inte kan fastställa att personuppgifterna är korrekta, ska myndigheten enligt *andra stycket* i stället begränsa behandlingen av dem. Vad regleringen innebär utvecklas i SOU 2017:29 s. 687 och 725 f.

Beslut i fråga om rättelse eller komplettering av personuppgifter eller begränsning av behandlingen får enligt 8 kap. 2 § överklagas.

I 10 § upplyses om att det kan finnas föreskrifter på lägre nivå om kraven på en begäran om korrigeringsåtgärd.

7 §

Paragrafen reglerar enskildas rätt att vid otillåten behandling av personuppgifter begära radering eller, om personuppgifterna behöver finnas kvar som bevisning, begränsning av behandlingen. Paragrafen behandlas i avsnitt 14.15 och motsvarar 4 kap. 10 § brottsdatalagen (2018:000). I 2 kap. 14 § regleras Säkerhetspolisens skyldighet att på eget initiativ radera eller begränsa behandlingen av personuppgifter som behandlas på otillåtet sätt.

Enligt *första stycket* ska Säkerhetspolisen på begäran av den registrerade radera personuppgifter som rör honom eller henne om uppgifterna behandlas i strid med 2 kap. 1–6, 8–10 eller 12 § eller 4 kap. 1 § första stycket, 2–4 eller 7–11 § eller om det krävs för att

myndigheten ska utföra en rättslig förpliktelse. Vårdnadshavare och andra ställföreträdare kan begära radering för en registrerad som inte har rätt att själv göra det. Vad regleringen innebär utvecklas i SOU 2017:29 s. 726 f.

Om förutsättningarna för att radera personuppgifterna är uppfyllda, men uppgifterna behöver finnas kvar som bevisning, ska Säkerhetspolisen enligt *andra stycket* på begäran av den registrerade i stället begränsa behandlingen av uppgifterna. Vad det innebär utvecklas i SOU 2017:29 s. 727 f.

Beslut i fråga om radering av personuppgifter och begränsning av behandlingen får enligt 8 kap. 2 § överklagas.

I 10 § upplyses om att det kan finnas föreskrifter på lägre nivå om kraven på en begäran om radering eller begränsning av behandlingen.

8 §

Enligt paragrafen, som behandlas i avsnitt 14.15 och motsvarar 4 kap. 11 § brottsdatalagen (2018:000), avgör Säkerhetspolisen vilken åtgärd som ska vidtas med anledning av en begäran om rättelse, radering eller begränsning av behandlingen. Vad bestämmelsen innebär utvecklas i SOU 2017:29 s. 728.

Avgiftsfri information

9 §

Paragrafen, som motsvarar 4 kap. 12 § brottsdatalagen (2018:000), föreskriver att information som huvudregel ska vara avgiftsfri. Den behandlas i avsnitt 14.15.

I *första stycket* slås fast att den information som Säkerhetspolisen på eget initiativ ska göra tillgänglig ska vara avgiftsfri, medan den information om behandlingen av den registrerades personuppgifter som lämnas på hans eller hennes begäran ska vara utan avgift en gång per år.

Om någon begär att få information om behandlingen av personuppgifter och att få del av dem oftare än en gång per år får Säkerhetspolisen enligt *andra stycket* ta ut en rimlig avgift för det. Ett

sådant beslut får enligt 8 kap. 2 § överklagas. Säkerhetspolisen får, i stället för att ta ut avgift, avslå begäran, vilket regleras i 5 § första stycket. Vad bestämmelsen innebär utvecklas i SOU 2017:29 s. 729.

I 10 § upplyses om att det kan finnas föreskrifter på lägre nivå om avgift för information.

Föreskrifter

10 §

I paragrafen upplyses om att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter om allmän och personrelaterad information, om kraven på begäran om information och begäran om rättelse-, raderings- eller begränsningsåtgärder och om avgift för informationen.

7 kap. Tillsyn

Tillsyn över personuppgiftsbehandlingen

1 §

I paragrafen, som behandlas i avsnitt 15.4.1 och 15.4.2, anges vilka tillsynsuppgifter som tillsynsmyndigheten har.

I *punkten 1* föreskrivs att tillsynsmyndigheten ska utöva allmän tillsyn över behandlingen av personuppgifter. Vad tillsynen innebär utvecklas i SOU 2017:29 s. 460 f. och 730 f. Tillsynsmyndigheten avgör om och i vilken utsträckning tillsyn ska utövas och hur tillsynen ska genomföras.

I *punkten 2* regleras tillsynsmyndighetens rådgivande uppgifter. De omfattar både allmän rådgivning till personuppgiftsansvariga och personuppgiftsbiträden och rådgivning vid förhandssamråd enligt 5 kap. 6 §. Vad uppgifterna innebär utvecklas i SOU 2017:29 s. 732 f.

2 §

Paragrafen upplyser om den tillsyn som Säkerhets- och integritetsskyddsnämnden utövar över Säkerhetspolisens personuppgiftsbehandling enligt lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet. Den behandlas i avsnitt 15.1 och 15.7.

Befogenheter

Undersökningsbefogenheter

3 §

I paragrafen, som behandlas i avsnitt 15.5.1, regleras tillsynsmyndighetens undersökningsbefogenheter.

Undersökningsbefogenheterna omfattar bl.a. rätt att få tillgång till de personuppgifter som behandlas och till dokumentation, lokaler och utrustning. Tillsynsmyndigheten ska också ha rätt till det biträde som behövs för tillsynen.

Paragrafen motsvarar 5 kap. 5 § brottsdatalogen (2018:000). Vad den innebär utvecklas i SOU 2017:29 s. 733.

Förebyggande befogenheter

4 §

Paragrafen, som behandlas i avsnitt 15.5.3, reglerar tillsynsmyndighetens befogenheter i det förebyggande arbetet. De åtgärder som regleras i paragrafen är inte av tvingande karaktär. De syftar till att förebygga att framtida behandling av personuppgifter kommer att stå i strid med regelverket.

I *första stycket* regleras vad tillsynsmyndigheten kan göra om den bedömer att det finns risk för att personuppgifter kan komma att behandlas i strid med lag eller annan författning. Det kan gälla såväl planerad som pågående behandling. Tillsynsmyndigheten ska i första hand försöka förmå Säkerhetspolisen eller personuppgiftsbiträdet att minska den risken genom råd, rekommendationer eller påpekanden. Bestämmelsen motsvarar 5 kap. 6 § första stycket

brottsdatalagen (2018:000). Vad den innebär utvecklas i SOU 2017:29 s. 734 f.

I *andra stycket* regleras tillsynsmyndighetens möjlighet att utfärda en skriftlig varning för att planerad eller pågående behandling av personuppgifter riskerar att stå i strid med lag eller annan författning. Bestämmelsen motsvarar 5 kap. 6 § andra stycket brottsdatalagen. Vad den innebär utvecklas i SOU 2017:29 s. 735.

Korrigerande befogenheter

5 §

I paragrafen, som behandlas i avsnitt 15.5.4, regleras tillsynsmyndighetens korrigerande befogenheter. De är avsedda att användas om tillsynsmyndigheten har konstaterat att personuppgifter behandlas i strid med lag eller annan författning.

Enligt *första stycket punkten 1* får tillsynsmyndigheten även när den har konstaterat att behandlingen inte är författningssenlig använda icke bindande påtryckningsmedel i form av råd, rekommendationer eller påpekanden för att försöka förmå Säkerhetspolisen eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningssenlig eller för att uppfylla andra skyldigheter.

Enligt *punkten 2* får tillsynsmyndigheten förelägga Säkerhetspolisen eller personuppgiftsbiträdet att vidta en viss åtgärd eller uppfylla någon annan skyldighet. Sådana förelägganden är bindande för mottagaren. Tillsynsmyndigheten kan t.ex. förelägga Säkerhetspolisen att ändra viss personuppgiftsbehandling eller att uppfylla krav på loggning eller dokumentationsskyldighet.

Punkten 3 ger tillsynsmyndigheten möjlighet att förbjuda att viss behandling fortsätter. Ett sådant beslut är också bindande för mottagaren. Förbud får dock bara meddelas om bristen är allvarlig och förutsätter att tillsynsmyndigheten bedömer att det inte finns något annat sätt att komma till rätta med bristen.

I *andra stycket* föreskrivs att det av ett föreläggande ska framgå när åtgärderna senast ska ha vidtagits. Om det är lämpligt ska det också anges vilka åtgärder som ska vidtas. Ett exempel kan vara att en viss personuppgift ska korrigeras eller tas bort.

Paragrafen motsvarar 5 kap. 7 § punkterna 1–3 brottsdatalagen (2018:000). I SOU 2017:29 s. 735 f. utvecklas innebörden av befogenheterna.

Kommunikation

6 §

Paragrafen reglerar tillsynsmyndighetens kommunikationsskyldighet. Den behandlas i avsnitt 15.6.1.

Paragrafen motsvarar 5 kap. 8 § brottsdatalagen. Vad skyldigheten innebär utvecklas i SOU 2017:29 s 738.

8 kap. Skadestånd och rättsmedel

Skadestånd

1 §

I paragrafen, som motsvarar 7 kap. 1 § brottsdatalagen (2018:000), regleras den registrerades rätt till skadestånd för den skada och kränkning som behandling av personuppgifter i strid med regelverket har orsakat. Paragrafen behandlas i avsnitt 14.16.3.

Rätt till skadestånd kan uppkomma på grund av behandling i strid med bestämmelser i lagen eller i föreskrifter som meddelats i anslutning till den. Säkerhetspolisen eller ett personuppgiftsbiträde som är personuppgiftsansvarig enligt 5 kap. 14 § andra stycket kan åläggas skadestånd. Vad regleringen innebär utvecklas i SOU 2017:29 s. 749 f.

Överklagande

Överklagande av Säkerhetspolisens beslut

2 §

I paragrafen, som motsvarar 7 kap. 2 § brottsdatalagen (2018:000), anges vilka av Säkerhetspolisens beslut som får överklagas. Paragrafen behandlas i avsnitt 14.16.4.

Vilka typer av beslut som får överklagas räknas upp i *första stycket*. Uppräkningen är uttömmande. Att andra beslut än de som anges i paragrafen inte får överklagas framgår av 4 §.

Beslut i fråga om rättelse, komplettering eller radering av personuppgifter eller begränsning av behandlingen av personuppgifter får överklagas om den registrerade har begärt åtgärden och beslutet har gått honom eller henne emot. Rätten att överklaga kan gälla även i de fall där myndigheten har vidtagit en annan åtgärd än den som den registrerade begärt. Beslut som innebär att Säkerhetspolisen, helt eller delvis, inte har tillmötesgått en begäran om personrelaterad information får också överklagas. Detsamma gäller beslut att ta ut avgift för sådan information.

Besluten överklagas till allmän förvaltningsdomstol. Vilken förvaltningsdomstol som är behörig framgår av 14 § lagen (1971:289) om allmänna förvaltningsdomstolar. För att kammarrätten ska ta upp ett beslut till prövning krävs det enligt *andra stycket* prövnings-tillstånd.

Överklagande av tillsynsmyndighetens beslut

3 §

I paragrafen, som behandlas i avsnitt 15.6.2, regleras överklagande av tillsynsmyndighetens beslut.

I *första stycket* föreskrivs att tillsynsmyndighetens beslut enligt lagen får överklagas till allmän förvaltningsdomstol. Det är fråga om beslut enligt 7 kap. 5 §, exempelvis beslut om rättelse eller radering. Även beslut som tillsynsmyndigheten meddelat med stöd av föreskrifter som meddelats i anslutning till lagen kan överklagas.

För att kammarrätten ska ta upp ett beslut till prövning krävs det enligt *andra stycket* prövningstillstånd.

Beslut som inte får överklagas

4 §

Enligt paragrafen, som behandlas i avsnitt 14.16.4, får inga andra beslut än de som räknas upp i 2 och 3 §§ överklagas. Uppräkningen är uttömmande. Någon rätt att med stöd av förvaltningslagen över-

klaga andra beslut som har fattats med stöd av lagen finns alltså inte. Det gäller både beslut av Säkerhetspolisen, tillsynsmyndigheten och personuppgiftsbiträden.

9 kap. Överföring av personuppgifter till tredjeland och internationella organisationer

Grundläggande förutsättningar för överföring

1 §

I paragrafen anges de grundläggande förutsättningarna för att få överföra personuppgifter till ett tredjeland eller en internationell organisation. Paragrafen har utformats efter mönster av 8 kap. 1 § brottsdatalagen (2018:000). Den behandlas i avsnitt 14.17.2.

Enligt *första stycket* får personuppgifter som behandlas i Sverige överföras till ett tredjeland eller en internationell organisation. Det gäller också om personuppgifterna överförs till ett tredjeland eller en internationell organisation för att behandlas där. Tredjeland och internationell organisation definieras i 1 kap. 9 §.

Överföring är en form av personuppgiftsbehandling. Behandling av personuppgifter definieras i 1 kap. 9 §. För att personuppgifter ska få överföras till ett tredjeland eller en internationell organisation måste de grundläggande förutsättningarna för att behandla personuppgifter alltid vara uppfyllda. Vad som avses med överföring och vilka överföringar som omfattas av regleringen utvecklas i SOU 2017:29 s. 754 f.

Överföring till ett tredjeland eller en internationell organisation får endast göras om de i punkten 1 angivna villkoren och något av alternativen i punkten 2 samtidigt är uppfyllda.

Punkten 1 anger till vilka utländska mottagare personuppgifter får överföras. Personuppgifter får som huvudregel bara överföras till en brottsbekämpande myndighet eller en underrättelse- eller säkerhetstjänst i ett tredjeland eller till en internationell organisation med brottsbekämpande uppdrag. Möjligheten att i vissa fall överföra personuppgifter till andra regleras i 6 §.

Kravet på att överföringen ska göras till en brottsbekämpande myndighet innebär att den myndighet eller organisation som ska ta emot personuppgifterna ska ha som arbetsuppgift att förebygga,

förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott. När det gäller internationella organisationer är det framför allt Interpol som är av intresse. Även vissa utredningsorgan under FN torde kunna ha brottsbekämpande uppdrag, liksom internationella tribunaler.

I *punkten 2* ställs det krav på att viss skydds nivå ska vara säkerställd för att personuppgifter ska få överföras till ett tredjeland eller till en internationell organisation. Kraven motsvarar de som ställs i 8 kap. 1 § första stycket 3 brottsdatalagen (2018:000). Vad kraven innebär utvecklas i SOU 2017:29 s. 757.

2 §

Paragrafen, som behandlas i avsnitt 14.17.2, anger förutsättningarna för att få överföra personuppgifter som Säkerhetspolisen har fått från en annan stat till ett tredjeland eller till en internationell organisation. Paragrafen motsvarar 8 kap. 2 § första stycket brottsdatalagen (2018:000).

Enligt paragrafen krävs det medgivande från den stat som Säkerhetspolisen har fått personuppgifterna från för att uppgifterna ska få överföras till ett tredjeland eller till en internationell organisation. Sådant medgivande krävs oavsett från vilken stat som uppgifterna kommer och ska alltid finnas innan överföringen får göras.

Tillåtna grunder för överföring

Beslut om adekvat skydds nivå

3 §

Paragrafen, som motsvarar 8 kap. 3 § brottsdatalagen (2018:000), innehåller den första tillåtna grunden för att överföra personuppgifter till ett tredjeland eller till en internationell organisation. Det är först om förutsättningarna i denna paragraf inte är uppfyllda som alternativet att överföra personuppgifter med stöd av reglerna om tillräckliga skyddsåtgärder i 4 § eller särskilda situationer i 5 § ska prövas. Paragrafen behandlas i avsnitt 14.17.3.

Säkerhetspolisen får alltid överföra personuppgifter till ett tredjeland eller en internationell organisation som enligt ett beslut

av Europeiska kommissionen har en adekvat skyddsnivå för personuppgifter. Eftersom Säkerhetspolisens verksamhet som rör nationell säkerhet inte omfattas av unionsrätten är kommissionens beslut inte formellt bindande för myndigheten, men paragrafen ger Säkerhetspolisen samma möjlighet som andra brottsbekämpande myndigheter att överföra personuppgifter till ett tredjeland eller en internationell organisation om det finns ett sådant beslut. Om kommissionen har meddelat ett sådant beslut för ett territorium eller en sektor i ett tredjeland får personuppgifter överföras dit. Avgränsningen avgörs av innehållet i kommissionens beslut.

De grundläggande förutsättningarna för överföring av personuppgifter till ett tredjeland eller en internationell organisation i 1 § ska alltid vara uppfyllda för att personuppgifter ska få överföras med stöd av ett beslut om adekvat skyddsnivå. Är det fråga om personuppgifter som Säkerhetspolisen har fått från en annan stat ska även kravet i 2 § vara uppfyllt.

Om kommissionen beslutar att ett tredjeland, eller en del av det, eller en internationell organisation inte längre säkerställer en adekvat skyddsnivå får personuppgifter inte överföras dit med stöd av paragrafen. Det hindrar inte att personuppgifter överförs till det tredjelandet eller den internationella organisationen om någon av de andra tillåtna grunderna för överföring är tillämplig.

Tillräckliga skyddsåtgärder

4 §

I paragrafen behandlas den andra tillåtna grunden för överföring av personuppgifter till ett tredjeland eller en internationell organisation. Paragrafen motsvarar 8 kap. 4 § brottsdatalagen (2018:000) och behandlas i avsnitt 14.17.3.

Om det inte finns ett beslut om adekvat skyddsnivå enligt 3 § får Säkerhetspolisen ändå överföra personuppgifter till ett tredjeland, eller till en internationell organisation, om det garanteras tillräckliga skyddsåtgärder för uppgifterna. De grundläggande förutsättningarna i 1 och 2 §§ ska dock alltid vara uppfyllda.

Enligt *punkten 1* kan tillräckliga skyddsåtgärder finnas om sådana har fastställts i ett avtal som ger tillräckliga garantier till skydd för registrerades rättigheter. Personuppgifter kan normalt överfö-

ras till länder som är anslutna till dataskyddskonventionen eller om det annars finns avtal om internationellt samarbete som innehåller dataskyddsregler som är tillämpliga på överföringen. Det kan t.ex. vara fråga om bilaterala avtal som Sverige ingått med ett tredjeland och som sörjer för att kravet på dataskydd uppfylls och att registrerades rättigheter respekteras.

Enligt *punkten 2* får personuppgifter också överföras om den myndighet eller organisation som uppgifterna ska överföras till garanterar tillräckligt skydd för dem på annat sätt än genom avtal. Säkerhetspolisen ska bedöma alla omständigheter kring överföringen och komma till slutsatsen att skyddsåtgärderna är tillräckliga för att överföringen ska vara tillåten. Exempel på sådant som kan vägas in vid bedömningen av om tillräckligt skydd garanteras är bl.a. åtaganden att inte sprida personuppgifterna vidare eller att inte använda personuppgifterna efter viss tidpunkt.

Överföring i särskilda situationer

5 §

Paragrafen reglerar möjligheten att överföra personuppgifter till ett tredjeland eller till en internationell organisation när det varken finns beslut om adekvat skyddsnivå eller tillräckliga skyddsåtgärder kan garanteras för uppgifterna. Kravet är att det då ska vara fråga om en särskild situation som motiverar överföringen. Paragrafen, som behandlas i avsnitt 14.17.3, motsvarar 8 kap. 5 § brottsdatalagen (2018:000).

Överföringen ska enligt *första stycket* vara nödvändig i någon av de särskilda situationer som räknas upp i punkterna 1–4. Punkterna är alternativa. Oavsett vilken situation som är för handen ska de grundläggande förutsättningarna för överföring till tredjeland och internationella organisationer i 1 och 2 §§ alltid vara uppfyllda.

I *punkten 1* regleras två situationer som kan göra överföringen nödvändig. Det är dels för att skydda vitala intressen för den registrerade eller en annan fysisk person, dels för att skydda andra berättigade intressen för den registrerade. Vad det innebär utvecklas i SOU 2017:29 s. 761 f.

Punkten 2 tillgodoser behovet av att i ett enskilt fall kunna överföra personuppgifter till ett tredjeland eller en internationell

organisation som inte uppfyller kraven på adekvat skyddsnivå eller garanterar tillräckligt skydd för personuppgifterna. Överföringen ska vara nödvändig för något av de ändamål som omfattas av lagens tillämpningsområde. Som exempel på när personuppgifter kan behöva överföras i ett enskilt fall för ett sådant syfte kan nämnas bevisupptagning vid utländsk domstol, kvarstad på och beslag av egendom som finns i ett tredjeland och husrannsakan i en bostad eller lokal som är belägen där. En annan situation kan vara att Säkerhetspolisen har information om att en misstänkt terrorist befinner sig i landet men personen identifieras först när han eller hon har rest till ett tredjeland och kan antas komma att begå brott där. Överföringen kan även avse information som rör personskydd.

Åtgärden behöver inte vara nödvändig för att tillgodose Säkerhetspolisens behov och intressen. Det kan finnas förutsättningar för att tillämpa punkten om ett tredjeland behöver få tillgång till svenska personuppgifter, t.ex. uppgift om att en viss person är dömd för ett visst brott. Personuppgifter kan överföras både på begäran och på Säkerhetspolisens eget initiativ.

Punkten 3 innebär att personuppgifter kan överföras till ett tredjeland eller en internationell organisation om överföringen är nödvändig i ett enskilt fall för att kunna fastställa, göra gällande eller försvara ett rättsligt anspråk. Det rättsliga anspråket ska vara hänförligt till ett ändamål som omfattas av lagens tillämpningsområde. Exempel på sådana rättsliga anspråk är bl.a. skadestånd i anledning av brott.

Enligt *punkten 4* får en överföring också göras till ett tredjeland eller en internationell organisation om det behövs för att avvärja en omedelbar och allvarlig fara för allmän säkerhet. Vad som avses med sådan fara och vad regleringen i övrigt innebär utvecklas i SOU 2017:29 s. 763.

Enligt *andra stycket* ska en intresseavvägning göras när personuppgifter ska överföras enligt punkten 2 eller 3. Vad regleringen innebär utvecklas i SOU 2017:29 s. 763.

Överföring till andra mottagare

6 §

Paragrafen, som behandlas i avsnitt 14.17.4, reglerar undantag från kravet i 1 § första stycket 1 att överföring av personuppgifter till tredjeland ska göras till brottsbekämpande myndigheter, internationella organisationer med brottsbekämpande uppdrag eller underrättelse- och säkerhetstjänster. Om förutsättningarna i paragrafen är uppfyllda får personuppgifter överföras även till andra än sådana myndigheter. Det kan t.ex. vara till företag och privatpersoner i ett tredjeland. Det kan också vara fråga om överföring till andra kategorier av myndigheter än de som anges i 1 § första stycket, t.ex. en specialmyndighet som hanterar frågor om finansiering av terrorism. Överföring till andra mottagare får dock göras endast om samtliga i första stycket angivna förutsättningar är uppfyllda. Paragrafen har utformats efter mönster av 8 kap. 8 § brottsdatalagen (2018:000).

Enligt *punkten 1* ska överföringen vara absolut nödvändig för att Säkerhetspolisen ska kunna utföra en sådan arbetsuppgift som anges i 2 kap. 1 eller 2 §. Kravet på absolut nödvändighet innebär att överföringen inte kan underlåtas. Ett exempel kan vara att Säkerhetspolisen i sin underrättelseverksamhet behöver kontakta ett privat företag i ett tredjeland för att få fram information som behövs omedelbart i den brottsbekämpande verksamheten.

Enligt *punkten 2* krävs det också att Säkerhetspolisen bedömer att det skulle vara ineffektivt eller på något annat sätt olämpligt att i stället överföra personuppgifterna till en brottsbekämpande myndighet eller en underrättelse- eller säkerhetstjänst i det tredjelandet. Det kan vara något i tidigare kontakter med myndigheten i det landet eller andra indikationer som ger anledning att tro att syftet med överföringen kan komma att förfelas eller att det på något annat sätt skulle vara olämpligt att överföra personuppgifterna via en sådan myndighet.

Ett exempel är överföringar till olika internetoperatörer i syfte att t.ex. identifiera och kartlägga misstänkta terrorister och andra personer som kan utgöra säkerhetshot. Det skulle vara ineffektivt om varje sådan överföring skulle behöva göras genom en myndighet i mottagarlandet med hänsyn både till mängden förfrågningar och till den brådska som ofta råder. Ett annat exempel är information som lämnas till en bank för att förhindra att banken utnyttjas

för brottsliga penningöverföringar, t.ex. finansiering av terrorism. I sådana fall kan kontakt behöva tas omedelbart.

Enligt *andra stycket* ska det göras en intresseavvägning mellan den registrerades intresse av skydd mot kränkning av grundläggande fri- och rättigheter och det allmännas intresse av att en överföring kommer till stånd. Intresseavvägningen motsvarar den som enligt 5 § *andra stycket* ska göras när personuppgifter ska överföras i vissa särskilda situationer. Vad regleringen innebär utvecklas i SOU 2017:29 s. 768.

Villkor om användningsbegränsning

7 §

I paragrafen, som behandlas i avsnitt 14.17.5, anges vad som gäller om Säkerhetspolisen har fått personuppgifter från ett tredjeland eller en internationell organisation och överföringen försetts med villkor för användningen av uppgifterna. Paragrafen motsvarar 8 kap. 9 § brottsdatalagen (2018:000). Vad regleringen innebär utvecklas i SOU 2017:29 s. 768.

8 §

Enligt paragrafen får Säkerhetspolisen, när den överför personuppgifter till ett tredjeland eller en internationell organisation ställa upp villkor som begränsar det tredjelandets eller den internationella organisationens rätt att använda uppgifterna. Paragrafen behandlas i avsnitt 14.17.5.

Säkerhetspolisen har normalt anledning att ställa upp villkor som begränsar användningen av personuppgifter för att skydda sin egen verksamhet och de källor som myndigheten använder sig av. Villkor kan också behövas för att skydda andra allmänna intressen. Villkoren kan t.ex. gälla för vilka ändamål personuppgifterna får behandlas och hur länge behandlingen får pågå. Det finns oftast också skäl att ställa upp villkor som begränsar möjligheten att lämna personuppgifterna vidare.

I vissa fall kan Säkerhetspolisen även behöva ställa upp villkor av hänsyn till enskild. Det kan t.ex. vara fallet om uppgifter från

användning av hemliga tvångsmedel lämnas ut till en annan stat. Då kan det vara lämpligt att ställa upp villkor om att uppgifterna ska förstöras efter viss tid.

Liknande bestämmelser finns i 8 kap. 10 § brottsdatalagen (2018:000), 5 kap. 2 § lagen (2000:562) om internationell rättslig hjälp i brottmål och 6 kap. 4 § lagen (2017:496) om internationellt polisiärt samarbete.

Föreskrifter

9 §

I paragrafen upplyses om att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter om dokumentation av överföringar till tredjeland och internationella organisationer. Frågan behandlas i avsnitt 14.17.6.

Övergångsbestämmelser

Ikraftträdande- och övergångsbestämmelserna tas upp i avsnitt 18.1 och 18.3.

Punkten 1 föreskriver när lagen ska träda i kraft.

I *punkten 2* föreskrivs att bestämmelsen om loggning i 5 kap. 4 § inte behöver tillämpas på automatiserade behandlingssystem som har inrättats före lagens ikraftträdande förrän den 1 maj 2023.

Punkten 3 föreskriver att ärenden om tillsyn över Säkerhetspolisens behandling av personuppgifter i verksamhet inom lagens tillämpningsområde som har inletts hos Datainspektionen eller Säkerhets- och integritetsskyddsnämnden före ikraftträdandet men ännu inte har avgjorts när lagen träder i kraft ska handläggas enligt äldre föreskrifter.

Enligt *punkten 4* ska äldre föreskrifter också gälla för överklagande av sådana beslut om behandling av personuppgifter som rör behandling av personuppgifter som rör nationell säkerhet i verksamhet inom lagens tillämpningsområde och som har meddelats före ikraftträdandet. Med äldre föreskrifter avses här personuppgiftslagen och personuppgiftsförordningen. Punkten tar emellertid sikte inte bara på själva överklagandet utan också på vilket regel-

verk som ska tillämpas när överklagandet prövas. Äldre föreskrifter i polisdatalagen (2010:361) och föreskrifter som har meddelats i anslutning till den ska då tillämpas.

Punkten 5 innebär att bestämmelserna om skadestånd i 48 § personuppgiftslagen (1998:204) fortfarande ska gälla för skada som har orsakats före ikraftträdandet vid behandling av personuppgifter i strid med regelverket.

20.2 Förslaget till domstolarnas brottsdatalag (2018:000)

1 kap. Allmänna bestämmelser

Lagens tillämpningsområde

1 §

I paragrafen, som behandlas i avsnitt 12.3.1, anges lagens tillämpningsområde.

Lagen gäller utöver brottsdatalagen för de allmänna domstolarna och de allmänna förvaltningsdomstolarna när de i egenskap av behöriga myndigheter enligt brottsdatalagen behandlar personuppgifter för vissa syften. Behörig myndighet, personuppgift och behandling av personuppgifter definieras i 1 kap. 6 § brottsdatalagen (2018:000).

Att lagen gäller utöver brottsdatalagen innebär bl.a. att lagen enligt 1 kap. 3 § brottsdatalagen bara gäller för sådan behandling av personuppgifter som är helt eller delvis automatiserad och för annan behandling av personuppgifter som ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

I brottsdatalagen finns alla de grundläggande bestämmelserna om hur personuppgifter får behandlas. Den nu aktuella lagen innehåller bestämmelser som innebär preciseringar, undantag eller avvikelser från bestämmelser i brottsdatalagen. Det innebär att bestämmelserna i lagen ska läsas tillsammans med regleringen i brottsdatalagen och tolkas i ljuset av den regleringen.

Enligt *punkten 1* får en allmän domstol behandla personuppgifter i syfte att handlägga mål och ärenden om utredning av eller

lagföring för brott, ändring eller verkställighet av straffrättsliga påföljder eller upprätthållande av allmän ordning och säkerhet. Vad det innebär utvecklas i kommentaren till 2 kap. 1 §.

Enligt *punkten* 2 får allmän förvaltningsdomstol behandla personuppgifter enligt lagen i syfte att handlägga mål och ärenden om verkställighet av häktning eller straffrättsliga påföljder. Vad det innebär utvecklas i kommentaren till 2 kap. 1 §.

Lagen är tillämplig under hela handläggningen av ett sådant mål eller ärende som anges i paragrafen. Om t.ex. ett enskilt anspråk handläggs tillsammans med ett brottmål är lagen tillämplig även på den personuppgiftsbehandling som krävs för handläggningen av anspråket. Detsamma gäller vissa andra former av särskild talan och talan om förbud som förs i brottmål (se SOU 2017:29 s. 208 f.). Om ett enskilt anspråk avskiljs för att handläggas i den ordning som gäller för tvistemål är lagen inte längre tillämplig.

Personuppgiftsansvar

2 §

I paragrafen, som motsvarar 9 § domstolsdatalagen (2015:728), anges vem som är personuppgiftsansvarig. Paragrafen behandlas i avsnitt 12.3.2. Domstolarnas personuppgiftsansvar innebär att en domstol är personuppgiftsansvarig för all den behandling av personuppgifter som utförs vid domstolen eller under dess ledning. Personuppgiftsansvarigas skyldigheter regleras i 3 kap. brottsdatalagen (2018:000).

2 kap. Grundläggande bestämmelser om behandling

Tillåtna rättsliga grunder för behandling av personuppgifter

1 §

Paragrafen reglerar de tillåtna rättsliga grunderna för behandling av personuppgifter. Den behandlas i avsnitt 12.4.1.

Paragrafen, som är anpassad till hur de rättsliga grunderna för behandling av personuppgifter anges i 2 kap. 1 § brottsdatalagen (2018:000), ersätter den bestämmelsen. Regleringen i 2 kap. 2 §

brottsdatalagen ger domstolarna rättsligt stöd för att behandla personuppgifter för diarieföring och nödvändig handläggning, trots brist på stöd i denna paragraf.

Personuppgifter får enligt *första stycket* behandlas om det är nödvändigt och syftet är att handlägga mål och ärenden inom lagens tillämpningsområde. Bestämmelsen bildar den yttre ramen för när behandling av personuppgifter är tillåten. Behandlas personuppgifter för något annat syfte gäller inte lagen. Eftersom lagen tillämpas både av allmän domstol och allmän förvaltningsdomstol och dessa handlägger olika typer av mål och ärenden inom lagens tillämpningsområde, måste paragrafen läsas tillsammans med regleringen i 1 kap. 1 § för att avgöra vilka punkter som är relevanta.

För allmän domstol gäller lagen vid all handläggning i brottmål. Även behandling vid expediering inom ramen för målet eller ärendets handläggning omfattas, t.ex. underrättelser till andra myndigheter om påföljden som dömts ut eller om den dömda tillhör en viss yrkeskategori där domstolen är skyldig att underrätta ett tillsynsorgan om domen. Även expediering för att tillgodose partsynen omfattas.

Lagen ska tillämpas vid handläggning av mål eller ärenden om utredning av eller lagföring för brott, verkställighet av häktning eller ändring eller verkställighet av straffrättsliga påföljder eller upprätthållande av allmän ordning och säkerhet. Den gäller även vid handläggning av mål och ärenden om resning eller användning av något annat extraordinärt rättsmedel om det ursprungliga målet eller ärendet ligger inom lagens tillämpningsområde. Möjligheten att ta fram ett arkiverat mål eller ärende regleras däremot inte i lagen.

Typiska frågor som hänför sig till *punkten 1* och som rör utredning av brott är när en domstol prövar häktningsfrågor eller ger tillstånd till eller prövar andra frågor om användning av straffprocessuella tvångsmedel under en förundersökning. Under punkten hör också en domstols beslut om vittnesförhör under förundersökningen eller förordnande av sakkunnig enligt 23 kap. 13 § respektive 14 § rättegångsbalken och prövning av frågor som rör komplettering av förundersökning eller insyn i förundersökning eller 23 kap. 19 § rättegångsbalken. Den omfattar även handläggning av ärenden där frågor som anges i lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott prövas.

Till lagföring hör prövning av ansvarstalan och annan talan som förs i ett brottmål, t.ex. talan om enskilt anspråk, näringsförbud eller skattetillägg. Även frågor om resning eller andra extraordinära rättsmedel hör hit.

Punkten 2 innebär att en domstol får behandla personuppgifter om syftet är att handlägga mål eller ärenden om verkställighet av häktning eller ändring eller verkställighet av straffrättsliga påföljder. Allmän domstol prövar frågor om ändring av påföljd bl.a. enligt 28 kap. 8 § brottsbalken (undanröjande av skyddstillsyn) och 38 kap. 2 och 2 a §§ brottsbalken (omprövning av påföljden på grund av ändrade förutsättningar). Allmän domstol prövar också enligt 15–19 §§ bötesverkställighetslagen (1979:189) om böter ska omvandlas till fängelse.

Allmän förvaltningsdomstol prövar vissa beslut av Kriminalvården enligt bl.a. 14 kap. fängelselagen (2010:610) och 7 kap. häkteslagen (2010:611). Allmän förvaltningsdomstol prövar också frågor om rättspsykiatrisk vård och vissa beslut av övervakningsnämnd. Även beslut enligt lagen (1998:603) om verkställighet av sluten ungdomsvård prövas av allmän förvaltningsdomstol. Migrationsöverdomstolen och migrationsdomstolar prövar vissa frågor som rör utvisning på grund av brott. En närmare redogörelse för vilka frågor som kan vara aktuella finns i SOU 2017:29 s. 181 f., 207 f. och 225 f.

Åklagares beslut enligt lagen (2005:321) om tillträdesförbud vid idrottsarrangemang kan prövas av allmän domstol. Handläggning av sådana frågor omfattas av *punkten 3*, upprätthållande av allmän ordning och säkerhet. Prövning av frågor som regleras i ordningslagen (1993:1617) ligger däremot utanför tillämpningsområdet (se SOU 2017:29 s. 228).

Behandling av personuppgifter vid utlämnande enligt tryckfrihetsförordningen eller som ett led i serviceskyldigheten till andra myndigheter ligger också utanför tillämpningsområdet. Enligt 2 § andra stycket tillämpas domstolsdatalagen (2015:728) i dessa fall. Behandling av personuppgifter för arkivändamål omfattas inte av lagens tillämpningsområde.

Enligt *andra stycket* ska det vara fråga om en arbetsuppgift som framgår av en bindande unionsrättsakt eller av en lag, en förordning eller ett särskilt beslut i vilket regeringen uppdragit åt domstol att

ansvara för uppgiften. Motsvarande bestämmelse finns i 2 kap. 1 § brottsdatalagen. Vad den innebär utvecklas i SOU 2017:29 s. 238 f.

2 §

Paragrafen, som behandlas i avsnitt 12.4.2, anger vad som gäller när fråga uppkommer om att behandla personuppgifter, som behandlas med stöd av 1 §, för nya ändamål.

I *första stycket* upplyses om att förutsättningarna för att behandla personuppgifter för nya ändamål inom lagens tillämpningsområde regleras i 2 kap. 4 § brottsdatalagen (2018:000). Innan personuppgifter får behandlas för ett nytt ändamål krävs en prövning enligt den paragrafen. Vad prövningen innebär utvecklas i SOU 2017:29 s. 249 f.

Enligt *andra stycket* regleras förutsättningarna för behandling för nya ändamål som inte omfattas av lagens tillämpningsområde i 2 kap. 22 § brottsdatalagen. Innan personuppgifter får behandlas för ett nytt ändamål utanför lagens tillämpningsområde krävs en prövning enligt den paragrafen. Vad prövningen innebär utvecklas i avsnitt 6.4.3. Om det nya ändamålet omfattas av domstolsdatalagens (2015:728) tillämpningsområde ska emellertid den lagen tillämpas och någon prövning enligt 2 kap. 22 § andra stycket brottsdatalagen krävs då inte.

Behandling av personnummer

3 §

Paragrafen, som behandlas i avsnitt 12.4.4, reglerar användningen av personnummer, samordningsnummer och liknande identitetsbeteckningar.

Enligt *första stycket* får sådana identitetsbeteckningar behandlas endast när det är motiverat med hänsyn till vikten av en säker identifiering eller något annat beaktansvärt skäl. Den har utformats efter mönster av 22 § personuppgiftslagen (1998:204).

Personnummer måste kunna behandlas av domstolarna i många situationer. De behöver bl.a. kunna ta emot, lagra, vidarebefordra och på andra sätt behandla stämningsansökningar och andra inlagor

i mål och ärenden som omfattas av lagens tillämpningsområde. Handlingar av det slaget innehåller ofta personnummer, samordningsnummer och andra liknande identitetsbeteckningar. Det gäller även sådana handlingar som sänds in elektroniskt. Domstolarna behöver också i stor utsträckning använda identitetsbeteckningar i sitt verksamhetsstöd, i domar och beslut och vid expedieringen av dem. Paragrafen hindrar således inte att andra myndigheter lämnar uppgifter om personnummer och andra identitetsbeteckningar till domstolarna och att domstolarna lagrar eller vidarebefordrar dem eller behandlar dem på annat sätt. Behovet av att behandla sådana uppgifter kan dock förändras över tid. En parts personnummer kan t.ex. behöva behandlas i ett skede av handläggningen av ett mål eller ärende men inte i ett annat. Ett exempel kan vara att målsägandens personnummer behövs för att identifiera honom eller henne, för att säkerställa att rätt person kallas till rättegången för att höras. Personnumret behöver däremot inte anges i domen om målsäganden inte för talan.

Behandlingen av personnummer och andra identitetsbeteckningar får aldrig bli slentrianbetonad. Paragrafen ska i likhet med 22 § personuppgiftslagen förhindra omotiverad behandling av personnummer och andra liknande identitetsbeteckningar (se prop. 2014/15:148 s. 51).

I *andra stycket* upplyses om att det i 8 § finns bestämmelser om i vilken utsträckning sådana identitetsbeteckningar som anges i paragrafen får användas vid sökning.

Sökning

Undantag från brottsdatalagens sökförbud

4 §

Paragrafen, som behandlas i avsnitt 12.5.1, innebär att det generella sökförbudet i 2 kap. 14 § brottsdatalagen (2018:000) inte gäller för domstolarna vid personuppgiftsbehandling enligt lagen. För dem gäller i stället de särskilda bestämmelserna om sökning i 5–10 §§ och föreskrifter som har meddelats i anslutning till lagen.

Känsliga personuppgifter och nationell anknytning

5 §

Paragrafen, som behandlas i avsnitt 12.5.2, förbjuder att uppgifter som avslöjar sådana uppgifter som anges i 2 kap. 11 och 12 §§ brottsdatalagen (2018:000), dvs. känsliga personuppgifter, används som sökbegrepp vid sökning i personuppgifter. Med känsliga personuppgifter avses uppgifter om ras, etniskt ursprung, politisk åsikt, religiös eller filosofisk övertygelse, medlemskap i fackförening eller uppgifter som kan avslöja hälsa, sexualliv eller sexuell läggning. Även biometriska och genetiska uppgifter betecknas som känsliga personuppgifter. Biometriska och genetiska uppgifter som rör hälsa definieras i 1 kap. 6 § brottsdatalagen.

Vidare är det förbjudet för en domstol att använda uppgifter som avslöjar nationell anknytning som sökbegrepp. Med uppgifter som avslöjar nationell anknytning avses bl.a. uppgifter om medborgarskap, födelseort eller utlandsfödda föräldrar. Varje form av nationell anknytning omfattas dock inte av bestämmelsen utan det krävs att uppgifterna visar på en anknytning till ett visst land som inte är alltför svag. En uppgift om att en person besökt ett land eller känner någon i landet är inte uppgifter som omfattas av sökförbudet. Normalt anses uppgifter om språkkunskaper eller om behov av tolk inte som uppgifter om nationell anknytning (se prop. 2014:15/148 s. 112).

Brott eller misstanke om brott

6 §

I paragrafen, som behandlas i avsnitt 12.5.2, regleras möjligheterna för allmän domstol att använda sökbegrepp som avslöjar brott eller misstanke om brott vid sökning i personuppgifter. Vad som gäller för användning av sådana sökbegrepp i allmän förvaltningsdomstol regleras i 7 §.

Lagen innehåller inte något generellt förbud mot användning av sökbegrepp som avslöjar brott eller misstanke om brott, exempelvis brottsrubriceringar (se prop. 2014/15:148 s. 113). Utgångspunkten är alltså att det är tillåtet att använda sökbegrepp som

avslöjar brott eller misstanke om brott. I paragrafen anges två olika situationer i vilka det inte är tillåtet att använda sådana sökbegrepp.

Enligt *punkten 1* får sökbegrepp som avslöjar brott eller misstanke om brott inte användas vid sökning i slutligt avgjorda mål eller ärenden längre än fem år efter utgången av det kalenderår då avgörandet fick laga kraft.

I *punkten 2* får sökbegrepp som avslöjar brott eller misstanke om brott inte användas i tvistemål. Sådana mål handläggs visserligen inte i något av de syften som omfattas av lagen, men bestämmelsen klargör att det inte heller är tillåtet att använda sökbegrepp som avslöjar brott eller misstanke om brott vid sökningar i sådana mål i syfte att samla in information för att användas i t.ex. ett brottmål.

7 §

I paragrafen, som behandlas i avsnitt 12.5.2, regleras möjligheterna för allmän förvaltningsdomstol att använda sökbegrepp som avslöjar brott eller misstanke om brott. Vad som gäller för användning av sådana sökbegrepp i allmän domstol regleras i 6 §.

Enligt *punkten 1* får sökbegrepp som avslöjar brott eller misstanke om brott inte användas vid sökning i personuppgifter i slutligt avgjorda mål längre än tjugo år efter utgången av det kalenderår då avgörandet fick laga kraft. Sådana sökbegrepp får enligt *punkten 2* inte heller användas av Migrationsöverdomstolen och migrationsdomstolarna.

Direkta personuppgifter

8 §

I paragrafen, som behandlas i avsnitt 12.5.2, regleras hur länge direkta personuppgifter får användas som sökbegrepp vid sökning i personuppgifter i brottmål som har avgjorts slutligt.

Enligt paragrafen får personnamn, personnummer, samordningsnummer och andra uppgifter som direkt kan hänföras till en fysisk person som är i livet inte användas som sökbegrepp i brottmål som har avgjorts slutligt längre än fem år efter utgången av det

kalenderår då avgörandet fick laga kraft. Eftersom regleringen avser sökning i brottmål innebär det att paragrafen bara är tillämplig i allmän domstol.

Tillåtna sökningar

9 §

I paragrafen, som behandlas i avsnitt 12.5.3, regleras generella undantag från sökförbuden i 5–8 §§. Paragrafen är tillämplig i både i allmän domstol och allmän förvaltningsdomstol.

Enligt *punkten 1* gäller sökförbuden inte vid sökning i en viss handling eller i ett visst mål eller ärende.

I *punkten 2* klargörs att användning av särskilda beteckningar för identifiering av en viss mål- eller ärendetyp inte omfattas av förbuden. Bestämmelsen tar sikte på s.k. målgrupps- och måltypskoder. Sökning med hjälp av sådana är alltså tillåten.

10 §

I paragrafen, som behandlas i avsnitt 12.5.3, föreskrivs att allmän förvaltningsdomstol får använda uppgifter som avslöjar hälsa som sökbegrepp. Det får dock enligt *punkten 1* inte göras vid sökning i personuppgifter i slutligt avgjorda mål längre än tjugo år efter utgången av det kalenderår då avgörandet fick laga kraft. Av *punkten 2* framgår dock att Migrationsöverdomstolen eller en migrationsdomstol aldrig får använda uppgifter som avslöjar hälsa som sökbegrepp.

Utlämnande av personuppgifter

11 §

I paragrafen, som behandlas i avsnitt 12.6.2, föreskrivs att personuppgifter får lämnas ut elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt. Elektroniskt utlämnade genom direktåtkomst är tillåtet bara i den utsträckning som anges i 12 § och i föreskrifter som har meddelats i anslutning till lagen. Bestäm-

melsen motsvarar 16 § domstolsdatalagen (2015:728), men terminologin ändras. Hur bestämmelsen ska tillämpas utvecklas i prop. 2014/15:148 s. 113 f.

12 §

Paragrafen, som behandlas i avsnitt 12.6.1, reglerar direktåtkomst. Den motsvarar 17 § domstolsdatalagen (2015:728). Hur den ska tillämpas utvecklas i prop. 2014/15:148 s. 114 f.

I *första stycket* ange vilka domstolar och andra som får medges direktåtkomst.

I *andra stycket* begränsas direktåtkomsten för andra än domstolar. Ytterligare begränsning av möjligheten att medge direktåtkomst regleras i förordning.

Föreskrifter

13 §

I paragrafen upplyses om att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter om ytterligare begränsning av möjligheten att använda de sökbegrepp som anges i 6, 7 och 10 §§ (vilket motsvarar nuvarande 15 § tredje stycket domstolsdatalagen [2015:728]), om direktåtkomst och behörighet och säkerhet vid sådan åtkomst (vilket motsvarar nuvarande 17 § tredje stycket domstolsdatalagen), om begränsning av möjligheterna att lämna ut personuppgifter elektroniskt på annat sätt än genom direktåtkomst (vilket motsvarar nuvarande 16 § andra stycket domstolsdatalagen) och om behandling av personuppgifter i slutligt avgjorda mål och ärenden (vilket motsvarar nuvarande 18 § domstolsdatalagen).

3 kap. Administrativa sanktionsavgifter och rättsmedel

Administrativa sanktionsavgifter

1 §

Paragrafen reglerar vid vilka överträdelser sanktionsavgift får tas ut. Frågan behandlas i avsnitt 12.8.

I *första stycket* anges vid vilka överträdelser sanktionsavgift får tas ut av den personuppgiftsansvarige. Tillsynsmyndigheten avgör i det enskilda fallet om det är påkallat att ta ut sanktionsavgift, vilket framgår av formuleringen att avgift får tas ut. Uppräkningen av vilka överträdelser som kan föranleda sanktionsavgift är uttömmande. Sanktionsavgift kan tas ut för överträdelse av bestämmelserna om tillåtna rättsliga grunder och bestämmelser om sökning. Brottsdatalagens förfaranderegler när det gäller sanktionsavgift tillämpas även vid överträdelser enligt denna lag. I brottsdatalagen och tillhörande förordning finns också bestämmelser om handläggningen av frågor om sanktionsavgift.

I *andra stycket* anges storleken på de sanktionsavgifter som kan komma i fråga. De överträdelser som enligt lagen kan föranleda sanktionsavgift är alla av allvarligt slag. Lägsta sanktionsavgift är därför 50 000 kronor.

Skadestånd

2 §

I paragrafen regleras den registrerades rätt till skadestånd för behandling av personuppgifter i strid med regelverket. Paragrafen behandlas i avsnitt 12.9.

Paragrafen hänvisar till 7 kap. 1 § brottsdatalagen (2018:000), som ska tillämpas på motsvarande sätt när det har förekommit felaktig behandling av personuppgifter enligt förevarande lag eller föreskrifter som har meddelats i anslutning till den. Det innebär att den personuppgiftsansvarige ska ersätta den registrerade för den skada och kränkning av den personliga integriteten som behandlingen av personuppgifter har orsakat. Med skada avses personskada, sakskada eller ren förmögenhetsskada. Med kränkning avses ideell skada som består i att den enskildes integritet kränkts genom

behandlingen. Någon möjlighet till jämkning av skadeståndet finns inte.

Överklagande

3 §

I paragrafen upplyses om att det finns bestämmelser om överklagande och om vilka beslut som får överklagas i 7 kap. brottsdatalagen (2018:000). Paragrafen behandlas i avsnitt 12.10.

4 §

Paragrafen, som har utformats efter mönster av 20 § domstolsdatalagen (2015:728), behandlas i avsnitt 12.10.

I *första stycket* föreskrivs en annan instansordning än den som gäller enligt 7 kap. 2 § brottsdatalagen (2018:000) vid överklagande av beslut som en domstol har fattat i egenskap av personuppgiftsansvarig.

Av *andra stycket* framgår att det inte finns någon möjlighet att överklaga beslut som har fattats av de högsta domstolarna.

I *tredje stycket* föreskrivs att kravet på prövningstillstånd i 7 kap. 2 § andra stycket brottsdatalagen inte gäller vid överklagande, vilket hör samman med den särskilda instansordningen.

Övergångsbestämmelser

Ikraftträdande- och övergångsbestämmelserna behandlas i avsnitt 12.11, 18.1, 18.2 och 18.3.1.

Punkten 1 föreskriver när lagen ska träda i kraft.

Enligt *punkten 2* behöver bestämmelserna i 2 kap. 6 § 1, 7 § 1, 8 § och 10 § 1 om begränsning av sökning i slutligt avgjorda mål och ärenden inte tillämpas förrän den 1 januari 2019.

Punkten 3 föreskriver att ärenden om tillsyn över behandling av personuppgifter, som rör behandling av personuppgifter vid handläggningen av sådana mål och ärenden som anges i 2 kap. 1 § första stycket, som har inletts hos Datainspektionen före ikraftträdandet

men ännu inte har avgjorts när lagen träder i kraft ska handläggas enligt äldre föreskrifter.

Enligt *punkten 4* ska äldre föreskrifter också gälla för överklagande av sådana beslut om behandling av personuppgifter som rör behandling av personuppgifter vid handläggningen av sådana mål och ärenden som anges i 2 kap. 1 § första stycket som har meddelats före ikraftträdandet. Med äldre föreskrifter avses här personuppgiftslagen och personuppgiftsförordningen. Punkten tar inte bara sikte på själva överklagandet utan också på vilket regelverk som ska tillämpas när överklagandet prövas. Äldre föreskrifter ska tillämpas även i det fallet.

Sanktionsavgift får enligt *punkten 5* beslutas endast för överträdelser som har begåtts efter ikraftträdandet.

Punkten 6 innebär att bestämmelsen om skadestånd i 48 § personuppgiftslagen fortfarande ska gälla för skada som har orsakats före ikraftträdandet vid behandling av personuppgifter i sådana mål och ärenden som avses i 2 kap. 1 §.

20.3 Förslaget till lag om ändring i rättegångsbalken

28 kap.

12 a §

Paragrafen reglerar kroppsbesiktning i form av salivprov som tas på den som är skäligen misstänkt. Ändringen, som behandlas i avsnitt 7.1.2, består i en ändrad hänvisning till en lag som byter namn och redaktionella ändringar.

12 b §

Paragrafen reglerar kroppsbesiktning i form av salivprov som tas på annan än den som är skäligen misstänkt.

I *första stycket* görs endast en redaktionell ändring.

I *andra stycket* ändras en hänvisning till en lag som byter namn, vilket behandlas i avsnitt 7.1.2. Vidare görs redaktionella ändringar.

Tredje stycket är oförändrat.

20.4 Förslaget till lag om ändring i polislagen (1984:387)

26 §

I paragrafen regleras på vilket sätt Polismyndigheten och Säkerhetspolisen får ta del av uppgifter som med stöd av 25 § tillhandahålls av transportföretag. Ändringen behandlas i avsnitt 7.4.1.

Första stycket är oförändrat.

I *andra stycket* regleras numera endast i vilken omfattning Polismyndigheten och Säkerhetspolisen får ta del av uppgifter genom terminalåtkomst. Myndigheternas behandling av sådana personuppgifter regleras i polisens brottsdatalag (2010:361) och Säkerhetspolisens datalag (2018:000).

20.5 Förslaget till lag om ändring i säkerhetsskyddslagen (1996:627)

3 §

I paragrafen anges vad som avses med registerkontroll. I paragrafen ändras hänvisningen till en lag som byter namn, vilket behandlas i avsnitt 7.1.2. Hänvisningen till lagen (2010:362) om polisens allmänna spaningsregister tas bort, eftersom den lagen har upphört att gälla.

20.6 Förslaget till lag om ändring i lagen (1996:701) om Tullverkets befogenheter vid Sveriges gräns mot ett annat land inom Europeiska unionen

16 §

I paragrafen, som behandlas i avsnitt 8.4.2, regleras på vilket sätt Tullverket får ta del av uppgifter som lämnas av transportföretag med stöd av 15 §.

Första stycket är oförändrat.

I *andra stycket* regleras numera endast i vilken omfattning Tullverket får ta del av uppgifter genom terminalåtkomst. Myndighe-

tens behandling av sådana personuppgifter regleras i Tullverkets brottsdatalag (2017:447).

20.7 Förslaget till lag om ändring i lagen (2000:344) om Schengens informationssystem

5 §

I paragrafen anges övergripande vad registret får innehålla och vem som får behandla personuppgifter i registret.

Första stycket är oförändrat.

I *andra stycket* ersätts hänvisningen till personuppgiftslagen (1998:204) med en hänvisning till brottsdatalagen (2018:000). Hänvisningen till en lag som byter namn ändras också, vilket behandlas i avsnitt 7.1.2.

20.8 Förslaget till lag om ändring i lagen (2001:185) om behandling av uppgifter i Tullverkets verksamhet

1 kap.

1 §

Paragrafen anger tillämpningsområdet för lagen.

Första och andra styckena är oförändrade.

I *tredje stycket* tas en hänvisning bort, eftersom det i fortsättningen får avgöras utifrån syftet med behandlingen vilken reglering som är tillämplig när personuppgifter behandlas i Tullverkets brottsbekämpande verksamhet. Om syftet är att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott tillämpas brottsdatalagen (2018:000) och Tullverkets brottsdatalag (2017:447), medan dataskyddsförordningen med kompletterande lagstiftning är tillämplig om syftet ligger utanför dessa lagars tillämpningsområden.

4 §

I paragrafen anges i vilken utsträckning personuppgifter som behandlas med stöd av lagen får behandlas för att tillhandahållas till annan verksamhet inom Tullverket.

Första stycket är oförändrat.

I *andra stycket* ändras hänvisningen till en lag som byter namn, vilket behandlas i avsnitt 8.1.2.

20.9 Förslaget till lag om ändring i lagen (2001:617) om behandling av personuppgifter inom kriminalvården

Lagen renodlas så att den bara omfattar behandling av personuppgifter inom brottsdatalagens tillämpningsområde.

Lagen anpassas också till brottsdatalagen (2018:000), vilket leder till en kraftig omarbetning av den. Flertalet paragrafer upphävs eller ändras. Samtidigt upphävs vissa särbestämmelser som inte längre fyller någon praktisk funktion. De grundläggande bestämmelserna om säkerhetsregistret, som hittills har reglerats i förordning, tas in i lagen. Lagen delas in i kapitel på samma sätt som övriga registerförfattningar. Som en anpassning till brottsdatalagen tillkommer ett kapitel om administrativa sanktionsavgifter och rättsmedel.

De generella ändringarna i lagen behandlas i kapitel 4 och 5 och övriga ändringar i kapitel 13.

Lagen får också ett nytt namn, kriminalvårdens brottsdatalag.

1 kap. Allmänna bestämmelser

Lagens tillämpningsområde

1 §

Paragrafen anger lagens tillämpningsområde. Den behandlas i avsnitt 13.2.1.

Lagen gäller för behandling av personuppgifter när en myndighet inom kriminalvården i egenskap av behörig myndighet enligt brottsdatalagen behandlar personuppgifter för vissa syften. I krimi-

nalvården ingår dels myndigheten Kriminalvården, dels övervakningsnämnderna. Behörig myndighet, personuppgift och behandling av personuppgifter definieras i 1 kap. 6 § brottsdatalagen (2018:000).

Att lagen gäller utöver brottsdatalagen innebär bl.a. att lagen enligt 1 kap. 3 § brottsdatalagen bara gäller för sådan behandling av personuppgifter som är helt eller delvis automatiserad och för annan behandling av personuppgifter som ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

I brottsdatalagen finns alla de grundläggande bestämmelserna om hur personuppgifter får behandlas. Den nu aktuella lagen innehåller bestämmelser som innebär preciseringar, undantag eller avvikelser från bestämmelser i brottsdatalagen. Det innebär att bestämmelserna i lagen ska läsas tillsammans med regleringen i brottsdatalagen och tolkas i ljuset av den regleringen.

Tillämpningsområdet omfattar huvudsakligen verkställighet av häktning och straffrättsliga påföljder. Av häktesverksamheten omfattas endast sådan häktning som ligger inom brottsdatalagens tillämpningsområde. Det innebär att verkställighet av häktning enligt konkurslagen inte omfattas och inte heller förvaring i häkte för andra ändamål än brottsutredning, lagföring och verkställighet av straffrättsliga påföljder. Att annan häktesverksamhet ligger utanför tillämpningsområdet beror på att Kriminalvården då inte agerar som behörig myndighet enligt brottsdatalagen.

I straffverkställighet ingår verkställighet av fängelsestraff och av vissa frivårdspåföljder som Kriminalvården har ansvaret för. I verkställigheten ingår också att förhindra eller förebygga brott under häktning och verkställighet av påföljder, att förebygga återfall i brott och att upprätthålla säkerheten på häkten och i kriminalvårdsanstalter. När övervakningsnämnderna behandlar personuppgifter görs det också inom ramen för straffverkställighet. Straffverkställighet omfattar även utländska domar, om verkställigheten har övertagits från den andra staten.

Lagen gäller för sådan personuppgiftsbehandling som utförs inom kriminalvården i syfte att biträda andra behöriga myndigheter när de bekämpar eller lagför brott, verkställer straffrättsliga påföljder eller upprätthåller allmän ordning och säkerhet. Vad det innebär utvecklas i avsnitt 13.2.1 och i kommentaren till 2 kap. 1 §.

Personuppgiftsansvar

2 §

I paragrafen, som behandlas i avsnitt 13.2.2, anges vilken myndighet som är personuppgiftsansvarig. Personuppgiftsansvarig definieras i 1 kap. 6 § brottsdatalagen (2018:000). Personuppgiftsansvarigas skyldigheter regleras i 3 kap. brottsdatalagen.

I *första stycket* anges att Kriminalvården är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför. Bestämmelsen motsvarar i den delen nuvarande 4 §.

Enligt *andra stycket* är en övervakningsnämnd personuppgiftsansvarig för den behandling av personuppgifter som nämnden utför. Övervakningsnämnderna är självständiga myndigheter och ansvarar alltså för sin egen personuppgiftsbehandling. Det hindrar inte att nämnderna kan samarbeta och t.ex. utse ett gemensamt dataskyddsbud.

2 kap. Grundläggande bestämmelser om behandling

Tillåtna rättsliga grunder för behandling av personuppgifter

1 §

Paragrafen reglerar de tillåtna rättsliga grunderna för behandling av personuppgifter. Den behandlas i avsnitt 13.3.1.

Paragrafen, som är anpassad till hur de rättsliga grunderna för behandling av personuppgifter anges i 2 kap. 1 § brottsdatalagen (2018:000), ersätter den bestämmelsen. Regleringen i 2 kap. 2 § brottsdatalagen ger rättsligt stöd för att behandla personuppgifter enbart för diarieföring och nödvändig handläggning, trots brist på rättsligt stöd i denna paragraf.

Kriminalvården får enligt *första stycket* behandla personuppgifter om det är nödvändigt för att utföra en arbetsuppgift i vissa särskilt angivna syften. Bestämmelsen bildar den yttre ramen för när behandling av personuppgifter är tillåten.

Enligt *punkten 1* får kriminalvården behandla personuppgifter för att kunna verkställa häktning eller straffrättsliga påföljder. De påföljder som är aktuella är fängelsestraff, skyddstillsyn och villkorlig dom med föreskrift om samhällstjänst. Med fängelsestraff

avses här även sådant fängelsestraff som utgör förvandlingsstraff för böter eller vite. Regleringen omfattar även motsvarande straffrättsliga påföljder som utdömts i en annan stat om påföljden ska verkställas i Sverige. Verkställigheten av häktning omfattar som framgår av kommentaren till 1 kap. 1 § endast sådan häktning som ligger inom brottsdatalagens tillämpningsområde.

Kriminalvården får enligt *punkten 2* behandla personuppgifter i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet i samband med verkställighet. Med verkställighet avses här både verkställighet av häktning och verkställighet av straffrättsliga påföljder. När myndigheten behandlar personuppgifter i sådana syften, t.ex. för att undvika att placera intagna som tillhör rivaliserade gäng tillsammans eller förhindra att narkotika tas in på ett häkte eller i en kriminalvårdsanstalt, utgör det alltså en tillåten behandling. För att regleringen inte ska tolkas för snävt används här uttrycket i samband med verkställighet. Det kan t.ex. vara osäkert om ett visst handlande som har betydelse ur säkerhetssynpunkt ligger före, under eller efter verkställigheten.

Enligt *punkten 3* får Kriminalvården behandla personuppgifter vid biträde åt andra behöriga myndigheter när de bekämpar eller lagför brott, verkställer straffrättsliga påföljder eller upprätthåller allmän ordning och säkerhet. I det ingår bl.a. Kriminalvårdens personutredningar i brottmål och transporter av häktade under brottsutredningar eller till och från domstolsförhandlingar i brottmål. Vidare omfattas det biträde som består i att Kriminalvården på vissa orter hanterar Polismyndighetens arrestverksamhet. Även biträde åt övervakningsnämnder eller domstolar bl.a. vid omhändertagande enligt 28 kap. 11 § brottsbalken omfattas.

Kriminalvården får enligt *punkten 4* hantera personuppgifter om det är nödvändigt för att myndigheten ska kunna utföra en arbetsuppgift som följer av en internationell förpliktelse. Sådana internationella förpliktelser kan bestå i exempelvis att ta över straffverkställighet från en annan stat eller att tillfälligt förvara personer som transporteras genom Sverige för straffverkställighet i ett annat land. Det kan också vara fråga om att hantera någon som har frihetsberövats med stöd av en arresteringsorder.

I *andra stycket* anges att det ska vara fråga om en arbetsuppgift som framgår av en bindande unionsrättsakt eller av en lag, en förordning eller ett särskilt beslut i vilket regeringen uppdragit åt den

behöriga myndigheten att ansvara för en sådan uppgift. Motsvarande bestämmelse finns i 2 kap. 1 § brottsdatalagen. Vad den innebär utvecklas i SOU 2017:29 s. 238 f.

2 §

I paragrafen, som behandlas i avsnitt 13.3.1, upplyses om att förutsättningarna för att personuppgifter ska få behandlas för nya ändamål regleras i 2 kap. 4 och 22 §§ brottsdatalagen (2018:000). Innan personuppgifter får behandlas för ett nytt ändamål inom eller utanför brottsdatalagens tillämpningsområde krävs en prövning enligt någon av paragraferna.

Känsliga personuppgifter

3 §

I paragrafen, som behandlas i avsnitt 13.3.2, regleras när Kriminalvården får behandla biometriska uppgifter. Biometriska uppgifter definieras i 1 kap. 6 § brottsdatalagen (2018:000).

Paragrafen möjliggör användning av särskild teknisk behandling för att bekräfta unik identifiering av en person. Det innebär att t.ex. fingeravtryck, ansiktsgeometri, röstigenkänning eller rörelsemönster får användas för att identifiera en person.

Biometriska uppgifter får behandlas av Kriminalvården enligt de förutsättningar som anges i 2 kap. 12 § brottsdatalagen. Behandlingen av de biometriska uppgifterna ska vara absolut nödvändig för ändamålet med behandlingen. Det innebär att behovet av att behandla sådana uppgifter måste prövas noga.

Utlämnande av personuppgifter

4 §

I paragrafen, som behandlas i avsnitt 13.3.3, anges när personuppgifter får lämnas ut i samband med framför allt straffverkställighet. Bestämmelserna är sekretessbrytande. När personuppgifter över-

förs till tredjeland ska även bestämmelserna i 8 kap. brottsdatalagen (2018:000) beaktas.

Punkten 1 gäller vid överflyttning av straffverkställighet till en annan stat. En liknande bestämmelse finns i nuvarande 48 § förordningen (2001:682) om behandling av personuppgifter inom kriminalvården. En förutsättning är att informationen lämnas till en myndighet i den andra staten som har till uppdrag att pröva om straffverkställigheten ska överflyttas eller att genomföra överflyttningen av verkställigheten till den andra staten. De personuppgifter som det kan vara fråga om rör bl.a. påföljden och den dömdes anknytning till den andra staten. Om verkställighet pågår i Sverige är uppgifter om verkställigheten av stor betydelse.

Punkten 2 avser den situationen att Kriminalvården behöver lämna information till en annan stats myndigheter om en person som är frihetsberövad och ska transiteras genom den andra staten. Personuppgifter som kan behöva överföras kan t.ex., utöver direkta personuppgifter, röra säkerhetsfrågor eller frågor som rör den enskildes behov av specialkost eller medicinering.

Enligt *punkten 3* får personuppgifter lämnas ut till en annan stats myndigheter om det behövs t.ex. för att en person som avtjänar fängelsestraff i Sverige tillfälligt ska kunna överföras till den andra staten för att där vittna i en brottmålsrättegång eller lagföras för brott begångna i den staten. De personuppgifter som det kan röra sig om är av samma slag som anges i punkten 2.

Längsta tid som personuppgifter får behandlas

5 §

Paragrafen anger den längsta tid under vilken uppgifter om en person får behandlas automatiserat. Frågan behandlas i avsnitt 5.5.2.

Bestämmelsen i *första stycket*, som motsvarar nuvarande 7 §, anger hur länge personuppgifter får behandlas för något av de syften som anges i 2 kap. 1 §. Det klargörs att uppgifterna, trots det som sägs i 2 kap. 17 § andra stycket brottsdatalagen (2018:000) om att arkivlagstiftningen har företräde, inte får arkiveras digitalt. Utgångspunkten är alltså att all automatiserad behandling av personuppgifterna ska upphöra när den tid som anges i paragrafen har löpt ut, vilket innebär att de ska tas bort. Endast om det har meddelats

uttryckliga föreskrifter som innebär att uppgifterna i fråga får behandlas för arkivändamål av allmänt intresse eller för vetenskapliga, statistiska eller historiska ändamål får de behandlas automatiserat längre än vad som anges i denna paragraf (jfr 6 §).

I *andra stycket* upplyses om att det i 3 kap. 7 § finns bestämmelser om längsta tid för behandling av personuppgifter i säkerhetsregistret.

Föreskrifter

6 §

I paragrafen upplyses om att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter om vilka personuppgifter som får behandlas, utlämnande av personuppgifter i andra fall än som anges i lagen, frågor som rör direktåtkomst till personuppgifter och längsta tid som personuppgifter får behandlas.

Regeringen eller den myndighet som regeringen bestämmer kan även meddela föreskrifter om att personuppgifter får behandlas under längre tid än vad som följer av 5 § för arkivändamål av allmänt intresse och för vetenskapliga, statistiska eller historiska ändamål (vilket motsvarar nuvarande 7 § andra stycket).

3 kap. Säkerhetsregistret

Rätten att föra register

1 §

I paragrafen regleras rätten att föra det s.k. säkerhetsregistret. Paragrafen behandlas i avsnitt 13.5.1. Bestämmelser om säkerhetsregistret finns i nuvarande 39–41 och 43–45 §§ förordningen (2001:682) om behandling av personuppgifter inom kriminalvården.

I säkerhetsregistret får personuppgifter behandlas för två syften. Enligt *punkten 1* får personuppgifter behandlas i syfte att förebygga, förhindra eller upptäcka brott eller brottslig verksamhet på häkten och i kriminalvårdsanstalter eller i samband med annan straffverkställighet. Personuppgifter får enligt *punkten 2* behandlas för att säkerställa ordning och säkerhet på häkten och i kriminal-

vårdsanstalter och annan verksamhet som Kriminalvården bedriver. Till det sistnämnda hör bl.a. halvvägshus och utslussningsenheter som Kriminalvården driver.

Innehåll

2 §

Paragrafen reglerar, tillsammans med 3 och 4 §§, vilka personkategorier som får registreras i säkerhetsregistret. I denna paragraf anges huvudregeln för behandling av personuppgifter i registret. Den behandlas i avsnitt 13.5.2.

Utgångspunkten för att det ska få finnas uppgifter om en person i registret är att han eller hon bedöms utgöra en säkerhetsrisk. Endast uppgifter om personer som är häktade eller verkställer ett fängelsestraff och som på någon av de särskilt uppräknade grunderna bedöms medföra en säkerhetsrisk för häktesverksamheten eller vid straffverkställigheten får behandlas i registret enligt denna paragraf. Regleringen träffar bara dem som är häktade eller intagna i kriminalvårdsanstalt för sådana syften som omfattas av brottsdatalogens tillämpningsområde. Därför får t.ex. personuppgifter om den som är häktad enligt konkurslagen eller som förvaras i häkte med stöd av utlänningslagstiftningen inte behandlas i registret. Grunderna för registrering motsvarar i allt väsentligt regleringen i nuvarande 39 § förordningen (2001:682) om behandling av personuppgifter inom kriminalvården men är mer generella.

Av *första stycket* framgår att uppgifter om personer som är eller har varit placerade på säkerhetsavdelning får behandlas i registret. Vad som krävs för placering på säkerhetsavdelning framgår av 2 kap. 4 § fängelselagen (2010:610).

Registret får enligt *andra stycket* innehålla uppgifter om en intagen eller häktad, om det finns risk för att han eller hon under häkteningen eller verkställigheten av straffet begår brott eller deltar i viss brottslig verksamhet eller på annat sätt äventyrar ordning och säkerhet på ett häkte eller i en kriminalvårdsanstalt. Registreringen bygger således på en riskbedömning.

Enligt *punkten 1* får personuppgifter behandlas i registret om det finns risk att en häktad eller intagen begår brott som inte är ringa. Om ett brott är ringa eller inte får bedömas med utgångs-

punkt i omständigheterna i det enskilda fallet och brottets straffskala. Redan misstanke om brott kan läggas till grund för registrering, eftersom det är fråga om en riskbedömning. För registrering krävs det således inte att det är straffrättsligt prövat att personen har begått brott. Den som under verkställighet av ett fängelsestraff gör sig skyldig till t.ex. våld eller hot mot en annan intagen eller deltar i narkotikahandel på en anstalt lagförs långtifrån alltid.

Vidare får personuppgifter behandlas om det finns risk att den häktade eller intagne deltar i brottslig verksamhet som innefattar brott för vilket det är föreskrivet fängelse i två år eller däröver. Det är straffskalan för brottet som är avgörande för om uppgifterna får registreras. Regleringen innebär att brott som har ett maximistraff om två års fängelse eller mer omfattas. Genom formuleringen omfattas även livstidsstraff.

Det är endast brott eller brottslig verksamhet i häkte eller under verkställighet av fängelsestraff som får beaktas.

Punkten 2 innebär att personuppgifter får behandlas beträffande en häktad eller intagen, om det finns risk att han eller hon förbereder rymning eller försöker rymma. Enligt *punkten 3* får uppgifter registreras om en häktad eller intagen om det finns risk att han eller hon blir föremål för fritagning. Tidigare försök till rymning eller fritagning tyder på att det finns en sådan risk, om inte omständigheterna talar emot det.

Enligt *punkten 4* får uppgifter om en häktad eller intagen behandlas om det finns risk att han eller hon medverkar i eller på annat sätt bidrar till att allvarligt störa ordningen eller säkerheten på häkte eller i kriminalvårdsanstalt. Det behöver inte vara fråga om ett straffbart handlande. Kravet på att ordningsstörningen ska vara allvarlig innebär att inte alla störningar får beaktas.

Punkten 5 innebär att uppgifter om en person som riskerar att utsättas för våld eller hot under verkställigheten också får registreras i säkerhetsregistret. Det kan behövas för att förhindra att en intagen placeras tillsammans med personer som kan utgöra ett hot mot honom eller henne under verkställigheten. Det ska framgå av registret att personen i fråga inte själv utgör en säkerhetsrisk.

3 §

Paragrafen reglerar tillsammans med 2 och 4 §§ vilka personkategorier som registreras i säkerhetsregistret. Den behandlas i avsnitt 13.5.3.

Gruppen av personer som får registreras med stöd av denna paragraf är bredare än i 2 §. Paragrafen kan tillämpas på alla som verkställer en påföljd inom kriminalvården. Förutom fängelsestraff är det fråga om frivårdspåföljder som kriminalvården ansvarar för. Förutsättningen för att personuppgifter ska få behandlas är att det finns risk att personen utövar våld eller hot mot eller otillbörlig påverkan på personal inom kriminalvården eller andra personer som uppehåller sig i kriminalvårdens lokaler. Otillbörlig påverkan kan i vissa fall innefatta ett straffbart handlande, t.ex. utpressning, men även andra former av påverkan kan utgöra grund för registrering, t.ex. förtäckta hot. Den som t.ex. genom brev eller telefonsamtal hotar kriminalvårdens personal omfattas av regleringen, eftersom det inte krävs att hotet uttalas i kriminalvårdens lokaler. Regleringen träffar också den som i kriminalvårdens lokaler t.ex. utövar våld mot andra klienter eller personer som tillfälligt befinner sig i lokalerna.

4 §

Paragrafen, som behandlas i avsnitt 13.5.4, reglerar möjligheten att i säkerhetsregistret behandla uppgifter om personer som inte är intagna i häkte eller verkställer påföljd.

Enligt paragrafen får Kriminalvården i säkerhetsregistret även behandla uppgifter om personer som har personlig anknytning till eller annan nära förbindelse med någon som är registrerad med stöd av 2 §. Det krävs dock att registreringen är absolut nödvändig för ändamålet med behandlingen. Det ställs således väsentligt högre krav för registrering med stöd av nu aktuell paragraf.

Med personlig anknytning avses t.ex. anhöriga eller andra närstående till en registrerad. En person som har nära förbindelse med den som är registrerad enligt 2 § kan exempelvis vara en tidigare medbrottsling. Däremot omfattas inte kontakter med professionella aktörer, t.ex. försvarare, kontaktpersoner och tolkar. Uppgifter om sådana personer får alltså inte registreras.

Uppgifter om personer som registreras med stöd av paragrafen och som inte själva är häktade eller intagna ska alltid förses med en särskild upplysning om det. Genom sådana upplysningar kan man skilja anknytningspersoner från sådana personer som utgör en säkerhetsrisk.

Sökning

5 §

Paragrafen, som behandlas i avsnitt 13.5.5, reglerar Kriminalvårdens möjlighet att använda känsliga personuppgifter vid sökning i personuppgifter i säkerhetsregistret. Paragrafen motsvarar nuvarande 41 § andra stycket förordningen (2001:682) om behandling av personuppgifter inom kriminalvården.

I paragrafen görs undantag från det generella sökförbudet i 2 kap. 14 § brottsdatalagen (2018:000). Enligt paragrafen är det tillåtet att utföra sökningar i syfte att få fram ett personurval grundat på vissa känsliga personuppgifter. Därmed tillåts sökningar som görs för att få fram ett urval av personer som t.ex. har visst etniskt ursprung eller viss religiös åskådning. Sökningar av det slaget kan behövas för placering av intagna eller för att de ska ges möjlighet att utöva sin religion. Sökningar på känsliga personuppgifter kan också vara nödvändiga för att den häktade eller intagne ska få nödvändig läkarvård, medicinering eller specialkost.

Rätten att söka på känsliga personuppgifter gäller dock inte sökning på ras eller medlemskap i fackförening eller sökning i genetiska eller biometriska uppgifter. Sökning som syftar till att få fram ett personurval grundat på sådana uppgifter är alltså inte tillåten.

I vilken utsträckning det är tillåtet att behandla någon eller några av personuppgifterna i en sammanställning av sådana uppgifter som sökningen resulterat i får prövas mot huvudregeln om behandling av känsliga personuppgifter i 2 kap. 11 § brottsdatalagen. Rätten att göra sökningar enligt denna paragraf medför således inte en generell rätt att fortsätta att behandla uppgifterna.

Direktåtkomst

6 §

I paragrafen, som behandlas i avsnitt 13.5.6, regleras möjligheten att medge direktåtkomst till säkerhetsregistret. Den motsvarar nuvarande 44 § första stycket förordningen (2001:682) om behandling av personuppgifter inom kriminalvården.

De myndigheter som räknas upp i paragrafen är Polismyndigheten, Säkerhetspolisen, Ekobrottsmyndigheten och Åklagarmyndigheten. Direktåtkomst får endast medges för något av de syften som anges i 1 kap. 2 § brottsdatalagen (2018:000). Vilka personuppgifter som får göras tillgängliga genom direktåtkomst regleras i förordning.

Längsta tid som personuppgifter får behandlas

7 §

Paragrafen, som behandlas i avsnitt 13.5.7 och motsvarar nuvarande 45 § förordningen (2001:682) om behandling av personuppgifter inom kriminalvården, anger den längsta tid som personuppgifter i säkerhetsregistret får behandlas. Det klargörs att uppgifterna, trots det som sägs i 2 kap. 17 § andra stycket brottsdatalagen (2018:000) om att arkivlagstiftningen har företräde, inte får arkiveras digitalt. Utgångspunkten är alltså att all automatiserad behandling av personuppgifterna ska upphöra när den tid som anges i paragrafen har löpt ut, vilket innebär att de ska tas bort. Endast om det har meddelats uttryckliga föreskrifter som innebär att uppgifterna i fråga får behandlas för arkivändamål av allmänt intresse eller för vetenskapliga, statistiska eller historiska ändamål får de behandlas automatiserat längre än vad som anges i denna paragraf (jfr 2 kap. 6 §).

Föreskrifter

8 §

I paragrafen, som behandlas i avsnitt 13.5.8, upplyses om att regeringen, eller den myndighet som regeringen bestämmer, kan meddela föreskrifter om innehållet i säkerhetsregistret och om utlämnande av personuppgifter ur registret.

4 kap. Administrativa sanktionsavgifter och rättsmedel

Administrativa sanktionsavgifter

1 §

Paragrafen, som är ny, reglerar vid vilka överträdelser sanktionsavgift får tas ut. Frågan behandlas i avsnitt 5.4.2.

I *första stycket* anges vid vilka överträdelser sanktionsavgift får tas ut av den personuppgiftsansvarige. Tillsynsmyndigheten avgör i det enskilda fallet om det är påkallat att ta ut sanktionsavgift, vilket framgår av formuleringen att avgift får tas ut. Uppräknningen av vilka överträdelser som kan föranleda sanktionsavgift är uttömmande. Sanktionsavgift kan tas ut för överträdelse av bestämmelserna om tillåtna rättsliga grunder, särskilda upplysningar och längsta tid som personuppgifter får behandlas. Brottsdatalagens förfaranderegler när det gäller sanktionsavgifter tillämpas även vid överträdelser enligt denna lag. I brottsdatalagen och tillhörande förordning finns också bestämmelser om handläggningen av frågor om sanktionsavgift.

Enligt *andra stycket* får sanktionsavgift även tas ut vid överträdelse av föreskrifter som har meddelats i anslutning till lagen och som rör särskild upplysning eller längsta tid som personuppgifter får behandlas.

I *tredje stycket* anges storleken på de sanktionsavgifter som kan komma i fråga. De överträdelser som enligt lagen kan föranleda sanktionsavgift är alla av allvarligt slag. Lägsta sanktionsavgift är därför 50 000 kronor.

Skadestånd

2 §

I paragrafen, som motsvarar nuvarande 8 §, regleras den registrerades rätt till skadestånd för behandling av personuppgifter i strid med regelverket. Frågan behandlas i avsnitt 5.4.3.

Paragrafen hänvisar till 7 kap. 1 § brottsdatalagen (2018:000), som ska tillämpas på motsvarande sätt vid behandling av personuppgifter enligt förevarande lag eller föreskrifter som har meddelats i anslutning till den. Det innebär att den personuppgiftsansvarige ska ersätta den registrerade för den skada och kränkning av den personliga integriteten som behandling av personuppgifter i strid med lagen, eller föreskrifter som har meddelats i anslutning till den, har orsakat. Med skada avses personskada, sakskada eller ren förmögenhetsskada. Med kränkning avses ideell skada som består i att den enskildes integritet kränkts genom behandlingen. Någon möjlighet till jämkning av skadeståndet finns inte.

Överklagande

3 §

I paragrafen, som behandlas i avsnitt 5.4.4, upplyses om att det i 7 kap. brottsdatalagen (2018:000) finns bestämmelser om överklagande och om vilka beslut som får överklagas.

Övergångsbestämmelser

Ikraftträdande- och övergångsbestämmelserna tas upp i avsnitt 18.1 och 18.2.

Punkten 1 föreskriver när lagen ska träda i kraft.

Sanktionsavgift får enligt *punkten 2* beslutas endast för överträdelser som har begåtts efter ikraftträdandet. Bestämmelsen tydliggör att sanktionsavgift inte får beslutas för en överträdelse som har begåtts före ikraftträdandet, även om sanktionsavgift skulle betraktas som en mildare åtgärd än ett straff.

Enligt *punkten 3* ska äldre bestämmelser fortsätta att gälla för överträdelser av bestämmelser om personuppgiftsbehandling som

begåtts före ikraftträdandet. Den gäller endast för sådana överträdelser som varit straffbara enligt 49 § personuppgiftslagen. Vid bedömningen av om det varit fråga om en överträdelse ska de krav som gällde för personuppgiftsbehandling vid tidpunkten för överträdelsen tillämpas.

I *punkten 4* föreskrivs att äldre föreskrifter också ska gälla för överklagande av beslut om behandling av personuppgifter i sådana syften som anges i 1 kap. 1 § som har meddelats före ikraftträdandet. Punkten tar inte bara sikte på själva överklagandet utan också på vilket regelverk som ska tillämpas när överklagandet prövas. Äldre föreskrifter ska tillämpas även i det fallet.

Punkten 5 innebär att bestämmelsen om skadestånd i 48 § personuppgiftslagen fortfarande ska gälla för skada som har orsakats före ikraftträdandet vid behandling av personuppgifter enligt lagen eller föreskrifter som har meddelats i anslutning till den.

20.10 Förslaget till lag om ändring i lagen (2005:321) om tillträdesförbud vid idrottsarrangemang

8 a §

Paragrafen reglerar rätten att fotografera den som har eller skäligen kan antas få tillträdesförbud. I paragrafen, som behandlas i avsnitt 16.5, ändras en hänvisning till en lag som byter namn.

20.11 Förslaget till lag om ändring i lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet

1 §

I paragrafen anges vad Säkerhets- och integritetsskyddsmyndigheten utövar tillsyn över. Paragrafen, som behandlas i avsnitt 15.7.1, utgår från det förslag som Utredningen om tillsynen över den personliga integriteten har lagt fram (se SOU 2016:65).

Första stycket är oförändrat.

I *andra stycket* tydliggörs vad tillsynen över Säkerhetspolisens personuppgiftsbehandling omfattar. Stycket knyter an till hur till-

lämpningsområdet för Säkerhetspolisens datalag (2018:000) är utformat. Tillsynen ska särskilt avse behandling av känsliga personuppgifter.

Det *tredje stycket* finns i paragrafens nuvarande lydelse men förefaller av misstag ha fallit bort i tidigare författningsförslag. Det är oförändrat.

3 §

Paragrafen reglerar Säkerhets- och integritetsskyddsnämndens skyldighet att på begäran av enskild kontrollera om han eller hon har varit föremål för personuppgiftsbehandling eller användning av hemliga tvångsmedel och om handläggningen har varit författningssenslig.

Ändringarna i *första stycket* är enbart redaktionella.

Det *andra stycket* motsvarar sista meningen i paragrafens nuvarande lydelse.

I *tredje stycket*, som är nytt och behandlas i avsnitt 15.7.2, föreskrivs att nämnden får vägra att utföra kontroll om begäran är orimlig eller uppenbart ogrundad. Syftet med bestämmelsen är att skapa utrymme för nämnden att underlåta att utföra kontroll i vissa fall. En begäran om kontroll kan vara orimlig om den upprepas med alltför täta intervall. Det är inte heller alltid rimligt att nämnden ska behöva kontrollera personuppgiftsbehandling som ligger långt tillbaka i tiden. Finns det inte längre möjlighet att begära skadestånd för kränkande personuppgiftsbehandling saknas det som regel anledning att utföra kontroll. Någon bestämd gräns för hur gamla förhållanden som bör kontrolleras anges dock inte.

4 §

I paragrafen slås fast att nämnden har rätt att få de uppgifter och det biträde för sin tillsyn som den begär. Paragrafen behandlas i avsnitt 15.7.1.

I paragrafen tydliggörs genom ett tillägg att nämnden har rätt att få tillgång till all den information och de upplysningar som den anser sig behöva för sin tillsyn. När det gäller tillsyn över personuppgiftsbehandling innebär det exempelvis att nämnden har samma

undersökningsbefogenheter som den myndighet som är tillsynsmyndighet enligt Säkerhetspolisens datalag. Det innebär en rätt att inte bara få tillgång till de personuppgifter som behandlas och dokumentation som rör den behandlingen utan också tillgång till dokumentation som rör it-system, information om säkerhetsåtgärder och liknande.

20.12 Förslaget till lag om ändring i offentlighets- och sekretesslagen (2009:400)

18 kap.

2 §

Paragrafen reglerar sekretess till skydd för underrättelseverksamhet. I *första stycket* ändras hänvisningarna till Polismyndighetens och Säkerhetspolisens reglering av personuppgiftsbehandling. I *andra stycket* ändras hänvisningar till lagar som byter namn, vilket behandlas i avsnitt 17.2.1. *Tredje och fjärde styckena* är oförändrade.

18 §

I paragrafen, som innehåller en sekretessbrytande bestämmelse, ändras en hänvisning till en lag som byter namn, vilket behandlas i avsnitt 17.2.1.

35 kap.

1 §

Paragrafen reglerar sekretess för enskilda personliga och ekonomiska förhållanden i viss brottsbekämpande verksamhet.

I *första stycket* ändras hänvisningarna till lagar som byter namn, vilket behandlas i avsnitt 17.2.1. Vidare läggs Säkerhetspolisens datalag (2018:000) till. Hänvisningen till lagen (2010:362) om polisens allmänna spaningsregister tas bort, eftersom den lagen upphört att gälla.

Andra–fjärde styckena är oförändrade.

4 a §

Paragrafen reglerar sekretessen för tillträdesförbudsregistret.

I *första stycket* ändras hänvisningen till lagen (2015:51) om register över tillträdesförbud vid idrottsarrangemang till en hänvisning till polisdatalagen (2010:361), där registret numera regleras. Ändringen behandlas i avsnitt 16.5. *Andra stycket* är oförändrat.

4 b §

Paragrafen reglerar sekretessen för uppgifter i sammanställningar av känsliga personuppgifter.

I *första stycket* läggs personurval enligt 2 kap. 12 § Säkerhetspolisens datalag (2018:000) till så att även sådana personurval omfattas av sekretessen. Frågan behandlas i avsnitt 14.7.3.

Andra stycket är oförändrat.

10 §

Paragrafen innehåller hänvisningar till sekretessbrytande bestämmelser i ett antal andra lagar. Hänvisningar till lagar som byter namn ändras, vilket behandlas i avsnitt 17.2.1. Säkerhetspolisens datalag (2018:000) läggs till i uppräknningen i *punkten* 4. Vidare görs redaktionella ändringar.

10 b §

Paragrafen, som behandlas i avsnitt 16.5, innehåller en sekretessbrytande bestämmelse. Hänvisningen till lagen (2015:51) om register över tillträdesförbud vid idrottsarrangemang ändras till en hänvisning till polisens brottsdatalag (2010:361), där registret numera regleras.

37 kap.

7 §

I paragrafen, som innehåller en sekretessbrytande bestämmelse, ändras en hänvisning till en lag som byter namn. Frågan behandlas i avsnitt 17.2.1.

20.13 Förslaget till lag om ändring i polisdatalagen (2010:361)

Lagen anpassas till bestämmelserna i brottsdatalagen, vilket leder till en kraftig omarbetning av den. Fyra kapitel upphävs och fem nya införs. Även i de övriga kapitlen upphävs vissa paragrafer, samtidigt som nya paragrafer tillkommer. Bestämmelserna om föreskrifter, som i dag är utspridda, samlas i slutet av varje kapitel. Dessa förändringar föranleder omnumreringar av vissa paragrafer.

Vidare flyttas bestämmelserna om behandling av personuppgifter som transportföretag tillhandahåller enligt bestämmelser i polislagen och bestämmelserna i tillträdesförbudsregistret till den nu aktuella lagen.

Flertalet bestämmelser om längsta tid för behandling av personuppgifter samlas i ett särskilt kapitel. Det gäller dock inte de bestämmelser om längsta tid för behandling som är knutna till särskilda register. De regleras alltjämt i samma kapitel som registret i fråga.

Som en anpassning till brottsdatalagen tillkommer ett nytt kapitel om administrativa sanktionsavgifter och rättsmedel.

Bestämmelserna om Säkerhetspolisens behandling av personuppgifter upphävs, eftersom den fortsättningsvis regleras i en särskild lag, Säkerhetspolisens datalag (2018:000).

De generella ändringarna i lagen behandlas i kapitel 4, 5 och 6 och övriga ändringar i kapitel 7.

Lagen får också ett nytt namn, polisens brottsdatalag.

1 kap. Allmänna bestämmelser

Lagens tillämpningsområde

1 §

I paragrafen, som behandlas i avsnitt 7.2.1, anges lagens tillämpningsområde.

Av *första stycket* framgår att lagen gäller utöver brottsdatalagen för Polismyndigheten, Ekobrottsmyndigheten och Säkerhetspolisen när någon av dem i egenskap av behörig myndighet enligt den lagen behandlar personuppgifter för vissa syften. Behörig myndighet, personuppgift och behandling av personuppgifter definieras i 1 kap. 6 § brottsdatalagen (2018:000).

Att lagen gäller utöver brottsdatalagen innebär bl.a. att lagen enligt 1 kap. 3 § brottsdatalagen bara gäller för sådan behandling av personuppgifter som är helt eller delvis automatiserad och för annan behandling av personuppgifter som ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

I brottsdatalagen finns alla de grundläggande bestämmelserna om hur personuppgifter får behandlas. Den nu aktuella lagen innehåller bestämmelser som innebär preciseringar, undantag eller avvikelser från bestämmelser i brottsdatalagen. Det innebär att bestämmelserna i lagen ska läsas tillsammans med regleringen i brottsdatalagen och tolkas i ljuset av den regleringen.

Enligt *punkten 1* gäller lagen för Polismyndigheten om personuppgifter behandlas i syfte att bekämpa eller lagföra brott eller upprätthålla allmän ordning och säkerhet. Vad det närmare innebär utvecklas i kommentaren till 2 kap. 1 §.

För Ekobrottsmyndigheten gäller lagen enligt *punkten 2* om syftet med personuppgiftsbehandlingen är att utreda brott och det inte är fråga om åklagarverksamhet. I sådan verksamhet gäller i stället åklagarväsendets brottsdatalag. Vad som avses med åklagarverksamhet utvecklas i avsnitt 7.2.1. Polisens brottsdatalag ska tillämpas i myndighetens övriga verksamhet för att utreda brott. Att lagen även ska tillämpas i den underrättelseverksamhet som förekommer vid Ekobrottsmyndigheten följer av punkten 1, eftersom det är Polismyndigheten som bedriver den verksamheten.

För Säkerhetspolisen gäller lagen enligt *punkten 3* enbart när myndigheten agerar som behörig myndighet enligt brottsdatalagen i frågor som inte rör nationell säkerhet och syftet med personuppgiftsbehandlingen är att bekämpa och lagföra brott. Det handlar om ett fåtal situationer där Säkerhetspolisen övertar en arbetsuppgift från Polismyndigheten eller där Säkerhetspolisen biträder Polismyndigheten. I Säkerhetspolisens brottsbekämpning och lagföring som rör nationell säkerhet gäller Säkerhetspolisens datalag.

I *andra stycket* tydliggörs att det är endast är vissa kapitel i lagen som gäller för Ekobrottsmyndigheten och Säkerhetspolisen. Kapitel 5 om särskilda register och kapitel 6 om behandling av personuppgifter vid Polismyndigheten för forensiska ändamål ska således bara tillämpas av Polismyndigheten.

2 §

I paragrafen, som motsvarar nuvarande 1 kap. 3 §, föreskrivs att lagen inte gäller vid behandling av personuppgifter enligt fem uppräknade lagar. Dessa lagar innehåller särregler inom brottsdatalagens tillämpningsområde. Paragrafen behandlas i avsnitt 7.2.1.

3 §

Paragrafen, som motsvarar nuvarande 1 kap. 4 §, anger hur regleringen i lagen förhåller sig till regleringen i lagen (2017:496) om internationellt polisiärt samarbete. Frågan behandlas i avsnitt 17.3.

Personuppgiftsansvar

4 §

I paragrafen, som behandlas i avsnitt 7.2.2 och motsvarar nuvarande 2 kap. 4 §, regleras personuppgiftsansvaret. Personuppgiftsansvarig definieras i 1 kap. 6 § brottsdatalagen (2018:000). Personuppgiftsansvarigas skyldigheter regleras i 3 kap. brottsdatalagen.

Regleringen i *första stycket* av Polismyndighetens personuppgiftsansvar anpassas till den terminologi som används i lagen i övrigt. Ansvaret omfattar dels all behandling av personuppgifter

enligt lagen vid Polismyndigheten, dels den behandling av personuppgifter som myndigheten utför vid Ekobrottsmyndigheten. Det sistnämnda avser behandling av personuppgifter i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet.

Av *andra stycket* framgår att Ekobrottsmyndigheten är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför enligt lagen i syfte att utreda brott.

Säkerhetspolisens personuppgiftsansvar, som regleras i *tredje stycket*, omfattar behandling av personuppgifter som myndigheten utför enligt lagen.

Uttryck i lagen

5 §

Paragrafen, som motsvarar nuvarande 2 kap. 3 §, innehåller definitioner av vissa uttryck som används i lagen. I paragrafen görs endast språkliga ändringar.

Lagens tillämpning på uppgifter om juridiska personer

6 §

I paragrafen, som motsvarar nuvarande 1 kap. 6 §, anges vilka bestämmelser i lagen och i brottsdatalagen som gäller för behandling av uppgifter om juridiska personer. Frågan behandlas i avsnitt 5.4.1.

Uppräkningen av bestämmelser som gäller vid behandling av uppgifter om juridiska personer motsvarar nuvarande reglering.

Lagens uppbyggnad

7 §

Paragrafen, som motsvarar nuvarande 1 kap. 7 § och behandlas i avsnitt 7.2.3, anger hur lagen är uppbyggd.

Enligt *första stycket* gäller 1 kap., som innehåller allmänna bestämmelser, för all behandling enligt lagen. Detsamma gäller 7 kap., som innehåller bestämmelser om administrativa sanktionsavgifter och rättsmedel. I 2 kap. finns det grundläggande bestämmelser om

behandling. Det gäller också för all behandling enligt lagen, med undantag för behandling enligt 6 kap. I 4 kap., som reglerar längsta tid för behandling av personuppgifter, finns det också generella regler, men de är inte tillämpliga på behandling i de särskilda register som regleras i 5 kap. De ska inte heller tillämpas vid behandling av personuppgifter i Polismyndighetens forensiska verksamhet, som regleras i 6 kap.

Av *andra stycket* framgår att 3 kap. enbart gäller för uppgifter som görs eller har gjorts gemensamt tillgängliga.

I 5 kap. särregleras vissa register. Av *tredje stycket* framgår att det kapitlet gäller i stället för 3 och 4 kap.

I *fjärde stycket* anges vad som gäller för behandling av personuppgifter i den forensiska verksamheten, som regleras i 6 kap. Då gäller det kapitlet i stället för 2–4 kap.

2 kap. Grundläggande bestämmelser om behandling

Tillåtna rättsliga grunder för behandling av personuppgifter

1 §

Paragrafen reglerar de tillåtna rättsliga grunderna för behandling av personuppgifter. Den behandlas i avsnitt 6.1, 6.3 och 7.3.1.

Paragrafen, som är anpassad till hur de rättsliga grunderna för behandling av personuppgifter anges i 2 kap. 1 § brottsdatalagen (2018:000), ersätter den bestämmelsen. Regleringen i 2 kap. 2 § brottsdatalagen ger myndigheterna rättsligt stöd för att i vissa fall behandla personuppgifter enbart för diarieföring och nödvändig handläggning, trots brist på stöd i denna paragraf.

Personuppgifter får enligt *första stycket* behandlas om det är nödvändigt för att utföra en arbetsuppgift i vissa särskilt angivna syften inom lagens tillämpningsområde. Bestämmelsen bildar den yttre ramen för när behandling av personuppgifter är tillåten. Eftersom lagen tillämpas av flera myndigheter måste bestämmelsen läsas tillsammans med regleringen i 1 kap. 1 § av tillämpningsområdet för att det ska kunna avgöras vilka punkter som är relevanta för respektive myndighet.

Enligt *punkten 1* får personuppgifter behandlas i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet. Det är fram-

för allt underrättelseverksamhet som regleras i punkten. Med det avses arbete med insamling, bearbetning och analys av information i syfte att förhindra eller upptäcka brottslig verksamhet när det ännu inte finns misstankar om att något konkret brott har begåtts (se prop. 2009/10:85 s. 318). Även behandling av överskottsinformation med stöd av 27 kap. 23 a § rättegångsbalken omfattas, om syftet är att förhindra brott. Personuppgiftsbehandling vid annan brottsförebyggande verksamhet omfattas också.

Enligt *punkten 2* får personuppgifter behandlas i syfte att utreda eller lagföra brott. Med utreda brott avses framför allt att genomföra förundersökning enligt 23 kap. rättegångsbalken, oavsett om det är Polismyndigheten eller åklagare som leder förundersökningen. Med brott avses konkreta brott, men det kan vara fråga om både brott som bevisligen har begåtts och brott som det enbart finns misstankar om. Misstankarna behöver inte vara riktade mot någon bestämd person. Är det fråga om undersökning av icke konkretiserad brottslig verksamhet tillämpas punkten 1 (se prop. 2009/10:85 s. 318).

Även personuppgiftsbehandling inom ramen för den form av förenklat utredningsförfarande som regleras i 23 kap. 22 § rättegångsbalken och vid åtgärder som vidtas med stöd av 23 kap. 3 och 8 §§ rättegångsbalken omfattas. Punkten omfattar även annan utredning som görs enligt bestämmelserna i 23 kap. rättegångsbalken (se prop. 2009/10:85 s. 319).

Med lagföra brott avses att utfärda förelägganden av ordningsbot. I tidigare förarbeten utvecklas närmare vad det innebär (se prop. 2009/10:85 s. 318 f.).

Enligt *punkten 3* får personuppgifter behandlas i syfte att upprätthålla allmän ordning och säkerhet. Det är endast Polismyndigheten som har sådana arbetsuppgifter att personuppgiftsbehandling enligt denna punkt kan bli aktuell. Vilka arbetsuppgifter det kan vara fråga om utvecklas i SOU 2017:29 s. 227 f.

Personuppgifter får enligt *punkten 4* också behandlas i syfte att fullgöra förpliktelser som följer av internationella åtaganden. Behandling enligt denna punkt tar sikte på sådana förpliktelser som syftar till att gagna utländsk brottsbekämpande verksamhet (se prop. 2009/10:85 s. 319).

I *andra stycket* anges att det ska vara fråga om en arbetsuppgift som framgår av en bindande unionsrättsakt eller av en lag, en för-

ordning eller ett särskilt beslut i vilket regeringen uppdragit åt myndigheten att ansvara för en sådan uppgift. Motsvarande bestämmelse finns i 2 kap. 1 § brottsdatalagen. Vad den innebär utvecklas i SOU 2017:29 s. 238 f.

2 §

I paragrafen, som behandlas i avsnitt 7.3.1, upplyses om att förutsättningarna för att personuppgifter ska få behandlas för nya ändamål regleras i 2 kap. 4 och 22 §§ brottsdatalagen (2018:000). Innan personuppgifter får behandlas för ett nytt ändamål inom eller utanför brottsdatalagens tillämpningsområde krävs det en prövning enligt någon av paragraferna. Vad prövningen innebär utvecklas i SOU 2017:29 s. 249 f. och avsnitt 6.4.3.

Särskilda upplysningar

3 §

I paragrafen, som behandlas i avsnitt 5.3.10, görs det undantag från bestämmelserna om särskilda upplysningar i 2 kap. 3 § andra stycket, 9 och 10 §§ brottsdatalagen (2018:000). Det är endast personuppgifter som har gjorts gemensamt tillgängliga med stöd av 3 kap. 2 § som i vissa fall ska förses med särskilda upplysningar. Det innebär att när personuppgifter behandlas bara av ett fåtal personer behöver särskilda upplysningar inte lämnas.

Känsliga personuppgifter

4 §

I paragrafen, som behandlas i avsnitt 7.3.2, regleras när biometriska uppgifter får behandlas. Biometriska uppgifter definieras i 1 kap. 6 § brottsdatalagen (2018:000). Att biometriska uppgifter också får behandlas i den forensiska verksamheten framgår av 6 kap. 4 §.

Paragrafen möjliggör användning av särskild teknisk behandling för att bekräfta unik identifiering av en person. Det innebär att

t.ex. fingeravtryck, ansiktsgeometri, röstigenkänning eller rörelsemönster får användas för att identifiera en person.

Biometriska uppgifter får behandlas av Polismyndigheten och Säkerhetspolisen enligt de förutsättningar som anges i 2 kap. 12 § brottsdatalagen. Behandlingen av de biometriska uppgifterna ska vara absolut nödvändig för ändamålet med behandlingen. Det innebär att behovet av att behandla sådana uppgifter måste prövas noga.

5 §

I paragrafen, som tillsammans med 6 § reglerar när det är tillåtet att använda känsliga personuppgifter vid sökning, görs det undantag från sökförbudet i 2 kap. 14 § brottsdatalagen (2018:000). Paragrafen behandlas i avsnitt 7.3.3.

Undantaget gäller vid sökning i alla slags uppgifter, dvs. såväl personuppgifter som har gjorts gemensamt tillgängliga som personuppgifter som inte har det. Sökförbudet hindrar inte att brottsrubriceringar, uppgifter om tillvägagångssätt vid brott, uppgifter om verkställighet av påföljd eller uppgifter som beskriver en persons utseende används vid sökning, även om det skulle leda till ett personurval grundat på känsliga personuppgifter.

Med uppgifter som beskriver en persons utseende avses signalementsuppgifter som t.ex. kroppsbyggnad, ansiktsform, hår- och hudfärg, klädsel och fysiska kännetecken som födelsemärken, blindhet och tatueringar (jfr prop. 2011/12:45 s. 124). En sökning på ett fysiskt särdrag kan ge ett personurval grundat på uppgifter som rör hälsa.

Sökning på t.ex. vissa sexualbrott eller tillvägagångssätt vid brott kan resultera i ett personurval grundat på sexualliv eller sexuell läggning. Ett personurval grundat på uppgifter om hälsa kan även bli resultatet vid sökning på exempelvis olika vårdpåföljder. Sökning på uppgifter om en persons utseende kan avse exempelvis fysiska skador eller särdrag som kan avslöja uppgifter om hälsa. Uppgifter om tatueringar kan t.ex. avslöja viss politisk åsikt eller religiös övertygelse.

I vilken utsträckning det är tillåtet att behandla någon eller några av personuppgifterna i en sammanställning av sådana uppgifter som sökningen resulterat i får prövas mot huvudregeln om

behandling av känsliga personuppgifter i 2 kap. 11 § brottsdatalagen. Rätten att göra sökning enligt denna paragraf medför således inte en generell rätt att fortsätta att behandla uppgifterna.

6 §

I paragrafen, som tillsammans med 5 § reglerar när det är tillåtet att använda känsliga personuppgifter vid sökning, görs det undantag från sökförbudet i 2 kap. 14 § brottsdatalagen (2018:000). Paragrafen behandlas i avsnitt 7.3.3.

Undantaget gäller enbart vid sökning i personuppgifter som inte har gjorts gemensamt tillgängliga, dvs. personuppgifter som endast ett fåtal har tillgång till. Sökning i sådana uppgifter får göras i syfte att få fram ett personurval grundat på etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening eller uppgifter som rör hälsa, sexualliv eller sexuell läggning. Sådana sökningar kan aktualiseras bl.a. vid utredning av brott som kan ha etniska, politiska eller religiösa motiv. Sökning kan också vara motiverad för att kartlägga sambandet mellan personer i kriminella nätverk som hålls samman av etniskt ursprung eller personer som begår vissa brott på grund av sin ideologiska övertygelse. Vid vissa brottstyper, exempelvis sexualbrott, kan återfall i brott vara vanligt och motivera att sökning görs som kan avslöja sexualliv eller sexuell läggning vid brott med okänd gärningsman.

Rätten att söka på känsliga personuppgifter gäller dock inte sökning på ras. Sökning i genetiska eller biometriska uppgifter är enligt 6 kap. 4 § enbart tillåtet i den forensiska verksamheten.

I vilken utsträckning det är tillåtet att behandla någon eller några av personuppgifterna i en sammanställning av sådana uppgifter som sökningen resulterat i får prövas mot huvudregeln om behandling av känsliga personuppgifter i 2 kap. 11 § brottsdatalagen. Rätten att göra sökning enligt denna paragraf medför således inte en generell rätt att fortsätta att behandla uppgifterna.

Utlämnande av personuppgifter

7 §

Paragrafen innehåller sekretessbrytande bestämmelser om utlämnande av personuppgifter till utländska myndigheter och mellanfolkliga organisationer. Den motsvarar nuvarande 2 kap. 15 §.

Första stycket ändras endast redaktionellt.

Ändringen i *andra stycket* är en följd av att uttrycket brottsbekämpande verksamhet utmönstras ur lagen, vilket behandlas i avsnitt 4.4.1. Sekretessen bryts och personuppgifter får lämnas ut om mottagaren behöver dem för något av de syften som räknas upp i 1 §. Det innebär att möjligheterna till utlämnande vidgas något, eftersom lagen även gäller vid upprätthållande av allmän ordning och säkerhet. När det gäller mottagare i tredjeland ska regleringen i 8 kap. 1 § brottsdatalagen (2018:000) också beaktas.

I *tredje stycket* görs en redaktionell ändring.

8 §

Genom paragrafen bryts viss sekretess som annars skulle ha gällt gentemot andra brottsbekämpande myndigheter. Den motsvarar nuvarande 2 kap. 16 §.

I *första stycket* läggs Polismyndigheten till i uppräknningen av myndigheter i förhållande till vilka sekretessen bryts. Det tydliggörs också att sekretessen bryts om den mottagande myndigheten behöver uppgifterna för något av de syften som anges i 1 kap. 2 § brottsdatalagen (2018:000). Ändringen är en följd av att uttrycket brottsbekämpande verksamhet utmönstras ur lagen, vilket behandlas i avsnitt 4.4.1.

I *andra stycket* görs en redaktionell ändring.

9 §

Paragrafen innehåller en bestämmelse som i fråga om uppgifter i dna-register bryter viss sekretess som annars skulle ha gällt gentemot andra brottsbekämpande myndigheter. Den motsvarar nuvarande 2 kap. 17 §. Det tydliggörs att sekretessen bryts om den mottagande myndigheten behöver uppgifterna för något av de syf-

ten som anges i 1 kap. 2 § brottsdatalagen (2018:000). Ändringen är en följd av att uttrycket brottsbekämpande verksamhet utmönstras ur lagen, vilket behandlas i avsnitt 4.4.1. Paragrafen ändras också redaktionellt.

10 §

Paragrafen innehåller en bestämmelse som i fråga om uppgifter i fingeravtrycks- och signalementsregister bryter viss sekretess som annars skulle ha gällt gentemot andra brottsbekämpande myndigheter. Den motsvarar nuvarande 2 kap. 18 §. Det tydliggörs att sekretessen bryts om den mottagande myndigheten behöver uppgifterna för något av de syften som anges i 1 kap. 2 § brottsdatalagen (2018:000). Ändringen är en följd av att uttrycket brottsbekämpande verksamhet utmönstras ur lagen, vilket behandlas i avsnitt 4.4.1. Paragrafen ändras även redaktionellt.

11 §

Paragrafen innehåller en sekretessbrytande bestämmelse som motsvarar nuvarande 9 § lagen (2015:51) om register över tillträdesförbud vid idrottsarrangemang. Tillträdesförbudsregistret regleras i 5 kap. 23–26 §§. Paragrafen behandlas i avsnitt 16.3.

12 §

Paragrafen reglerar när personuppgifter får lämnas ut elektroniskt.

I *första stycket* föreskrivs att personuppgifter får lämnas ut elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt. Med sådant utlämnande avses bl.a. utlämnande genom e-post eller annan elektronisk överföring eller på ett usb-minne eller annat motsvarande medium. Frågan behandlas i avsnitt 5.6.4.

Det har betydelse vem mottagaren är för frågan om det är olämpligt att lämna ut uppgifter elektroniskt. Som regel kan det inte anses vara olämpligt att lämna ut uppgifter på det sättet till en myndighet (se prop. 2014/15:148 s. 113, jfr SOU 2015:39 s. 447 f.).

När det gäller utlämnande till enskilda krävs en mer nyanserad bedömning. Om det finns en författningsreglerad skyldighet att sända en handling till en viss person får det avgöras om elektroniskt utlämnande är olämpligt med hänsyn till bl.a. innehållet i handlingen, vem som är mottagare, behovet av att kunna visa att personen i fråga har tagit del av handlingen och andra omständigheter. Är det fråga om processmaterial som översänds till parter eller ombud bör även principen om equality of arms beaktas.

Frågan är särskilt svårbedömd när uppgifter ska lämnas ut till enskilda och det på grund av uppgifternas art, struktur, antal eller någon annan särskild omständighet finns anledning att befara att utlämnandet kan leda till integritetsrisker (jfr prop. 2014/15:148 s. 114). Bedömer myndigheten att det finns risk för att personuppgifterna kan komma att missbrukas om de lämnas ut elektroniskt gäller sekretess enligt 21 kap. 7 § offentlighets- och sekretesslagen (2009:400). De får då inte lämnas ut till följd av sekretess.

Det kan också finnas särskild anledning att iaktta försiktighet när det gäller utlämnande av bild- och ljudupptagningar (jfr prop. 2016/17:68 s. 51 f.).

Vid prövningen av om personuppgifter bör lämnas ut elektroniskt bör även informationssäkerheten vägas in.

Om någon begär att få tillgång till en allmän handling med stöd av tryckfrihetsförordningen får den utlämnande myndigheten inte efterforska syftet med begäran. Det kan ha betydelse för möjligheten att få underlag för att bedöma om det i ett enskilt fall är lämpligt att lämna ut en handling med personuppgifter elektroniskt (se JO dnr 4171-2011).

Elektroniskt utlämnande genom direktåtkomst regleras i *andra stycket*, som motsvarar nuvarande 2 kap. 21 §. Det är tillåtet endast i den utsträckning som anges i lagen.

Personuppgifter från transportföretag

13 §

Paragrafen reglerar, tillsammans med 14 och 15 §§, hur personuppgifter som ett transportföretag tillhandahåller enligt 25 § polislagen (1984:387) får behandlas. Regleringen avser uppgifter om ankommande eller avgående transporter av bl.a. passagerare och fordon

som transportföretag befordrar till och från Sverige. Det rör sig alltså om bokningsuppgifter i framför allt flyg- och färjetrafik. Paragrafen behandlas i avsnitt 7.4.1 och 7.4.2. Transportföretagens skyldighet att tillhandahålla uppgifter regleras alltså i polislagen.

I *första stycket* tydliggörs att uppgifter från transportföretag endast får behandlas i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott. Möjligheten att söka i sådana uppgifter med hjälp av personnummer och andra liknande identitetsbeteckningar regleras i 15 §.

Om det vid den behandling som görs, eller vid kontroll vid ankomsten till Sverige, framkommer skäl att behandla personuppgifterna för ett nytt ändamål får det enligt *andra stycket* bara göras om förutsättningarna för behandling för nya ändamål i 2 kap. 4 eller 22 § brottsdatalogen (2018:000) är uppfyllda i det enskilda fallet. Ett typiskt exempel är att ett brott upptäcks och att uppgifterna behövs för att utreda och lagföra brottet. Det kan också visa sig att vissa av uppgifterna behövs i ett underrättelseärende.

Det framgår av 3 kap. 2 § i vilken utsträckning som personuppgifter från transportföretag får göras gemensamt tillgängliga

14 §

I paragrafen anges hur uppgifter från transportföretag som tillhandahålls genom terminalåtkomst får behandlas. Paragrafen, som motsvarar nuvarande 26 § andra stycket polislagen (1984:387), behandlas i avsnitt 7.4.1.

Paragrafen reglerar enbart behandling vid terminalåtkomst till personuppgifter hos transportföretag, medan 13 och 15 §§ anger vad som gäller i fråga om personuppgifter som förs över till myndighetens it-system eller behandlas strukturerat på annat sätt.

Genom terminalåtkomsten till företagens it-system får polisen tillgång till omfattande överskottsinformation om resande. Myndigheten får inte ändra eller på annat sätt bearbeta uppgifter i sådana system. Syftet med regleringen är att myndigheten inte heller ska kunna föra över en hel sådan uppgiftssamling till sina egna it-system för att bearbeta, ändra och lagra personuppgifterna där. Som framgår av 13 § får uppgifter däremot föras över i enskilda fall om förutsättningarna för det är uppfyllda.

15 §

I paragrafen, som behandlas i avsnitt 7.4.2, regleras i vilken utsträckning direkta personuppgifter får användas vid sökning i uppgifter som tillhandahålls av transportföretag.

I paragrafen begränsas möjligheten att söka i personuppgifter som avses i 13 § första stycket. När sökning görs med hjälp av personnummer, samordningsnummer och liknande identitetsbeteckningar får sökningen enbart avse personer som är eller har varit misstänkta för brott, är misstänkta för att utöva eller komma att utöva brottslig verksamhet avseende brott för vilket är föreskrivet fängelse i ett år eller mer eller personer som övervakas enligt 3 kap. 2 § första stycket 2. Det förhållandet att en person reser under annat namn eller använder ett känt alias hindrar inte sökning som görs på det eller de namnen under de förutsättningar som nu nämnts. Eftersom begränsningen bara gäller vid sökning med användande av direkta personuppgifter är sökning där sådana uppgifter inte används tillåtna, t.ex. för att ta fram resandeprofiler.

Föreskrifter

17 §

I paragrafen, där bestämmelser om föreskrifter samlas, upplyses om att regeringen kan meddela föreskrifter om att personuppgifter får lämnas ut i andra fall än som anges i 7–11 §§ (vilket motsvarar nuvarande 2 kap. 19 § första stycket) och om begränsning av möjligheterna att lämna ut personuppgifter elektroniskt på annat sätt än genom direktåtkomst. Frågan behandlas i avsnitt 5.6.4.

3 kap.

1 §

Av paragrafen framgår att kapitlet innehåller särskilda bestämmelser om behandling av personuppgifter som görs eller har gjorts gemensamt tillgängliga. Vad som avses med att uppgifter görs gemensamt tillgängliga utvecklas i prop. 2009/10:85 s. 334 f.

I *första stycket* anpassas regleringen till att uttrycket brottsbekämpande verksamhet utmönstras ur lagen, vilket behandlas i avsnitt 4.4.1.

Av *andra stycket* framgår att kapitlet inte gäller när personuppgifter behandlas med stöd av den särskilda bestämmelsen i 2 kap. 2 § brottsdatalagen (2018:000) om behandling av personuppgifter för diarieföring eller för att utföra andra nödvändiga handläggningsuppgifter.

2 §

I paragrafen anges vilka personuppgifter som får göras gemensamt tillgängliga.

I *första stycket* finns två nya punkter som anger ytterligare uppgifter som får göras gemensamt tillgängliga. Ändringarna behandlas i avsnitt 7.5.1.

Enligt *punkten 4* får personuppgifter som förekommer i ett ärende om kontaktförbud eller ett ärende om personskydd göras gemensamt tillgängliga. Utöver de uppgifter som registreras i belastningsregistret om den som meddelas kontaktförbud, finns det andra uppgifter som ligger till grund för sådana beslut som kan behöva göras gemensamt tillgängliga. Det kan t.ex. vara fråga om uppgifter om närstående till en person som skyddas av ett kontaktförbud, där det antingen kan vara viktigt att personens adressuppgifter inte röjs i andra sammanhang eller att det finns tillgång till uppgifter om närstående som också kan komma att utsättas för trakasserier eller brott. Genom formuleringen "berörs av" tydliggörs att om t.ex. en person som skyddas av ett kontaktförbud har barn som bor på samma adress och som inte själva skyddas av kontaktförbud, får uppgifter om barnen också göras gemensamt tillgängliga om det behövs för skyddet.

Det kan i vissa fall vara viktigt att kunna göra uppgifter om en person som har begärt kontaktförbud gemensamt tillgängliga trots att frågan om kontaktförbud ännu inte är slutligt avgjord, om det bedöms finnas akut risk för att personen utsätts för brott. Även uppgifter i ärenden där någon ansökt om kontaktförbud, men där underlaget inte har bedömts räcka till för ett sådant förbud, kan i

vissa fall vara viktiga att kunna göra gemensamt tillgängliga i syfte att uppmärksamma risken för brott mot personen i fråga.

På motsvarande sätt kan uppgifter som förekommer i ärenden om personskydd och om närstående till den som har personskydd i vissa fall behöva göras gemensamt tillgängliga, för att det inom myndigheten ska finnas allmän kännedom om att en viss person är i behov av sådant skydd.

Enligt *punkten 6* får uppgifter som behandlas i syfte att upprätthålla allmän ordning och säkerhet också göras gemensamt tillgängliga. Det kan t.ex. vara fråga om uppgifter om personer som bedöms kunna utgöra hot mot allmän ordning och säkerhet i samband med ett planerat idrottsarrangemang, en demonstration eller en politisk sammankomst. Sådana uppgifter torde i många fall kunna göras gemensamt tillgängliga med stöd av andra punkter i paragrafen. Denna punkt ger emellertid generell möjlighet att göra sådana personuppgifter tillgängliga utan någon kontroll av om den som personuppgiften rör är registrerad i underrättelseverksamheten, är misstänkt för brott eller förekommer i något annat sammanhang som ger möjlighet att göra personuppgifterna gemensamt tillgängliga.

Punkterna 1–3 ändras endast redaktionellt och *punkten 5* är oförändrad. *Punkten 7* motsvarar nuvarande punkten 4.

I *andra stycket* görs endast redaktionella ändringar.

Tredje stycket är oförändrat.

3 §

I paragrafen föreskrivs att personuppgifter som har gjorts gemensamt tillgängliga med stöd av 2 § första stycket 2 eller 5 ska förse med en särskild upplysning. Att det ska framgå för vilket närmare ändamål personuppgifterna behandlas följer av 2 kap. 3 § brottsdatalogen (2018:000). Paragrafen ändras också redaktionellt.

4 §

I paragrafen, som behandlas i avsnitt 5.3.10, regleras i vilken utsträckning uppgifter i underrättelseverksamhet som är gemensamt tillgängliga ska förse med särskilda upplysningar.

Enligt *första stycket* ska det framgå av uppgifter i underrättelseverksamhet att en person inte är misstänkt för att utöva brottslig verksamhet. Det ska alltså gå att skilja mellan personer som är föremål för polisens intresse på grund av inblandning i brottslig verksamhet och personer som inte är misstänkta för det. Att det ska framgå om en person är misstänkt för brott eller är ett brottsoffer regleras i 2 kap. 9 § brottsdatalagen (2018:000).

Enligt *andra stycket* ska uppgifter om personer som kan antas ha samband med misstänkt brottslig verksamhet eller som övervakas på visst sätt förses med upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak. Det tydliggörs att kravet på särskild upplysning bara gäller uppgifter om en person som kan antas ha direkt samband med misstänkt brottslig verksamhet. Kravet på samband är lågt ställt. Så snart det finns något som stöder ett antagande om att en person har ett direkt samband med brottslig verksamhet och det är fråga om uppgifter som görs gemensamt tillgängliga ska det framgå på vilket sätt personen har anknytning till den brottsliga verksamheten. Sambandet kan t.ex. bestå i att en person ofta träffar eller har annan kontakt med andra personer som är misstänkta för att utöva brottslig verksamhet eller ofta rör sig i miljöer där brottslighet förekommer, utan att ha naturliga skäl att befinna sig där. Uppgifter om den som är anhörig till en person som kan antas ha samband med misstänkt brottslig verksamhet faller alltså utanför, utom i de fall där båda kan antas ha direkt samband med brottslig verksamhet.

Det är bara uppgifter som rör en person som är misstänkt för att utöva eller komma att utöva brottslig verksamhet som behöver förses med upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak. De uppgifter som är av intresse är, förutom uppgifter om på vilket sätt personen är knuten till den brottsliga verksamheten, framför allt uppgifter som belyser brottslighetens art och omfattning. Uppgifter av det slaget kan behöva förses med särskilda upplysningar för att personens anknytning till brottsligheten ska kunna bedömas.

Utrymmet för att underlåta att förse uppgifter med upplysning om trovärdighet och riktighet vidgas något genom att det inte längre krävs särskilda omständigheter för att upplysningskravet inte ska gälla. Det är tillräckligt att det på grund av de samlade omständigheterna är onödigt att förse uppgifterna med en upplysning.

5 §

Paragrafen, som motsvarar nuvarande 3 kap. 6 §, innehåller en allmän begränsning av vilka uppgifter som får tas fram vid sökning i gemensamt tillgängliga uppgifter på namn, personnummer, samordningsnummer eller liknande identitetsbeteckningar. Den behandlas i avsnitt 7.5.2.

Genom ett tillägg tydliggörs att paragrafen endast gäller vid sökning i automatiserade behandlingssystem. Vad som avses med automatiserade behandlingssystem anges i SOU 2017:29 s. 306 f.

Punkterna 1–6 är oförändrade.

Enligt *punkten 7*, som är ny, får uppgifter om att en person berörs av ett kontaktförbud eller av åtgärder i ett personskyddsärende tas fram vid sökning.

I *punkterna 8–12* görs enbart redaktionella ändringar.

6 §

Paragrafen, som behandlas i avsnitt 7.5.2, innehåller undantag från begränsningarna i 5 §.

Enligt *första stycket*, som motsvarar nuvarande 3 kap. 7 § första stycket 1, gäller inga begränsningar vid sökning i en viss handling eller i ett visst ärende.

Enligt *andra stycket* gäller begränsningarna i 5 § inte vid vissa sökningar som utförs av särskilt angivna tjänstemän. Det gäller enligt *punkten 1*, som motsvarar nuvarande 6 § i polisdataförordningen (2010:1155), när de utför beredningsuppgifter och arbetet befinner sig i ett inledande skede i underrättelseverksamheten. Syftet med bestämmelsen är att tjänstemännen inledningsvis ska ha större möjligheter att göra sökningar för att kunna finna samband mellan nya och befintliga underrättelseuppgifter. Det är således bara under en begränsad tid efter det att uppgifterna kom in som punkten är tillämplig. Så snart beredningsarbetet har avslutats upphör möjligheten att göra sökningar med stöd av den nu aktuella punkten.

Enligt *punkten 2*, som motsvarar nuvarande 3 kap. 7 § första stycket 2 och andra stycket 1, är sökningar i syfte att bearbeta och analysera personuppgifter som har gjorts gemensamt tillgängliga i underrättelseverksamhet eller för övervakningen av en allvarligt

kriminellt belastad person tillåtna, om det endast är de tjänstemän som får göra sökningen som också har tillgång till uppgifterna.

Punkten 3, som motsvarar nuvarande 3 kap. 7 § andra stycket 2, ändras endast redaktionellt.

Enligt *punkten 4*, som är ny, gäller inte begränsningarna i 5 § vid sökning i syfte att samordna utredningar av brott som kan vara systematiska och för vilka det är föreskrivet fängelse i två år eller däröver. Sådana sökningar kan krävas för att finna samband mellan brott som kan ha begåtts i organiserad form eller i olika delar av landet eller där det annars finns inslag av systematik.

Undantaget i *tredje stycket* är nytt. Det innebär att begränsningarna i 5 § inte gäller när en tjänsteman i någon av Polismyndighetens ledningscentraler utför sökning på begäran av en polisman som verkställer ett ingripande eller vidtar en åtgärd som rör en enskild.

7 §

I paragrafen, som motsvarar nuvarande 3 kap. 8 § första stycket, anges vilka myndigheter som får medges direktåtkomst till uppgifter som har gjorts gemensamt tillgängliga och för vilka syften. Polismyndigheten läggs till i uppräkningslistan. Paragrafen ändras med anledning av att uttrycket brottsbekämpande verksamhet utmönstras ur lagen, vilket behandlas i avsnitt 4.4.1. Den ändras också redaktionellt.

8 §

I paragrafen, som motsvarar nuvarande 3 kap. 7 § fjärde stycket, upplyses om att regeringen kan meddela föreskrifter om ytterligare undantag från bestämmelserna om sökning i 5 §.

9 §

I paragrafen, där övriga bestämmelser om föreskrifter samlas, upplyses om att regeringen, eller den myndighet som regeringen bestämmer, kan meddela föreskrifter om begränsning av tillgången

till sådana uppgifter som anges i 5 § (vilket motsvarar nuvarande 3 kap. 6 § andra stycket), under vilka förutsättningar sökning får utföras med stöd av 6 § (vilket motsvarar nuvarande 3 kap. 7 § tredje stycket) och omfattningen av direktåtkomst och om behörighet och säkerhet vid sådan åtkomst (vilket motsvarar nuvarande 3 kap. 8 § tredje stycket).

4 kap. Längsta tid som personuppgifter får behandlas

Allmän bestämmelse

1 §

Flertalet av bestämmelserna som anger hur länge personuppgifter får behandlas samlas i detta kapitel. Frågan behandlas i avsnitt 5.5.1. Bestämmelser om hur länge personuppgifter får behandlas i de register som regleras i 5 kap. och i den forensiska verksamheten som regleras i 6 kap. finns dock alltså i de kapitlen.

I *första stycket* föreskrivs att bestämmelserna i kapitlet endast gäller för uppgifter som behandlas automatiserat.

Andra stycket upplyser om att den grundläggande bestämmelsen om att personuppgifter inte får behandlas längre än vad som är nödvändigt med hänsyn till ändamålet med behandlingen finns i 2 kap. 17 § första stycket brottsdatalogen (2018:000). I övriga paragrafer i kapitlet anges hur länge vissa typer av personuppgifter får behandlas inom den ram som sätts av denna huvudregel. Oavsett vilken bedömning som görs av nyttan med behandlingen av en viss personuppgift får den inte behandlas längre än vad som anges i respektive paragraf.

Tredje stycket innehåller en uppräkningslista av de bestämmelser om hur länge personuppgifter får behandlas som finns i 5 och 6 kap.

Personuppgifter som inte har gjorts gemensamt tillgängliga

2 §

I paragrafen, som motsvarar nuvarande 2 kap. 13 §, anges hur länge uppgifter som inte har gjorts gemensamt tillgängliga får behandlas. Regleringen behandlas i avsnitt 5.5.2. Någon ändring av hur länge sådana personuppgifter får behandlas görs inte.

I *första stycket* klargörs att uppgifterna, trots det som sägs i 2 kap. 17 § andra stycket brottsdatalagen (2018:000) om att arkivlagstiftningen har företräde, inte får arkiveras digitalt. Utgångspunkten är alltså att all automatiserad behandling av personuppgifterna ska upphöra när den tid som anges i paragrafen har löpt ut, vilket innebär att de ska tas bort. Endast om det har meddelats uttryckliga föreskrifter som innebär att uppgifterna i fråga får behandlas för arkivändamål av allmänt intresse eller för vetenskapliga, statistiska eller historiska ändamål får de behandlas automatiserat längre än vad som anges i denna paragraf (jfr 12 § 1).

Andra stycket klargör att paragrafen inte ska tillämpas på ärenden om utredning av eller lagföring för brott.

Gemensamt tillgängliga uppgifter i ärenden om utredning av eller lagföring för brott

3 §

Paragrafen, som motsvarar nuvarande 3 kap. 10 §, reglerar hur länge personuppgifter i en anmälan om brott får behandlas. Terminologin anpassas till den som används i lagen i övrigt och till att uttrycket brottsbekämpande verksamhet utmönstras ur lagen, vilket behandlas i avsnitt 4.4.1.

Enligt paragrafen inskränks enbart behandlingen av personuppgifter för de ändamål som regleras i lagen, vilket innebär att uppgifterna får fortsätta att behandlas automatiserat för bl.a. arkivändamål efter de tidpunkter som anges i paragrafen. Frågan behandlas i avsnitt 5.5.3.

4 §

Paragrafen, som motsvarar nuvarande 3 kap. 11 §, reglerar hur länge personuppgifter i förundersökningar och andra utredningar som handläggs enligt bestämmelserna i 23 kap. rättegångsbalken får behandlas.

Enligt paragrafen inskränks enbart behandlingen av personuppgifter för de ändamål som regleras i lagen, vilket innebär att uppgifterna får fortsätta att behandlas automatiserat för bl.a. arkivändamål efter de tidpunkter som anges i paragrafen. Frågan behandlas i avsnitt 5.5.3.

Terminologin i *första stycket* anpassas till den som används i lagen i övrigt. Vissa redaktionella ändringar görs också. Terminologin anpassas även i *andra stycket*.

Tredje stycket är oförändrat.

5 §

Paragrafen, som motsvarar nuvarande 3 kap. 13 §, reglerar vad som gäller i fråga om personuppgifter som rör någon som har varit misstänkt i en förundersökning som har lagts ner eller där åtal har lagts ner eller frikännande dom har meddelats och fått laga kraft. Paragrafen ändras endast redaktionellt.

Övriga gemensamt tillgängliga uppgifter

6 §

I paragrafen anges att det i de följande paragraferna finns bestämmelser om hur länge vissa typer av gemensamt tillgängliga uppgifter, som inte förekommer i ärenden om utredning av eller lagföring för brott, får behandlas. Det klargörs att uppgifterna, trots det som sägs i 2 kap. 17 § andra stycket brottsdatalogen (2018:000) om att arkivlagstiftningen har företräde, inte får arkiveras digitalt. Utgångspunkten är alltså att all automatiserad behandling av personuppgifterna ska upphöra när den tid som anges i 7–10 §§ har löpt ut, vilket innebär att uppgifterna ska tas bort. Endast om det har meddelats uttryckliga föreskrifter som innebär att uppgifterna i fråga får behandlas för arkivändamål av allmänt intresse eller för

vetenskapliga, statistiska eller historiska ändamål får de behandlas automatiserat längre än vad som anges i de följande paragraferna (jfr 12 §). Frågan behandlas i avsnitt 5.5.2.

7 §

Paragrafen, som motsvarar nuvarande 3 kap. 14 § andra och sjätte styckena, reglerar hur länge personuppgifter får behandlas i under rättelseverksamhet.

Enligt *första stycket*, som är nytt och behandlas i avsnitt 7.6, får personuppgifter som kan antas ha samband med sådan brottslig verksamhet som anges i 3 kap. 2 § första stycket 1 och som behandlas i ett ärende inte behandlas längre än ett år efter det att ärendet avslutades.

I *andra stycket* görs ingen ändring i fråga om hur länge personuppgifterna får behandlas men stycket anpassas till den terminologi som används i lagen i övrigt. Det tydliggörs att fristen för hur länge personuppgifter får behandlas endast ska påverkas av om det görs en ny registrering beträffande personens anknytning till brottslig verksamhet. Andra uppgifter som tillförs, t.ex. uppgifter om ändrade bostadsförhållanden eller annat som inte har betydelse för anknytningen till den brottsliga verksamheten, påverkar alltså inte hur länge personuppgifterna får behandlas. Frågan behandlas i avsnitt 5.5.4.

Tredje stycket ändras endast redaktionellt.

8 §

Paragrafen, som motsvarar nuvarande 3 kap. 14 § tredje och sjätte styckena, reglerar hur länge uppgifter om en person som är föremål för övervakning enligt 3 kap. 2 § första stycket 2 får behandlas. *Första och andra styckena* anpassas till den terminologi som används i lagen i övrigt.

9 §

Paragrafen reglerar hur länge personuppgifter som behandlas i ärenden om kontaktförbud eller personskydd eller som behandlas i syfte att fullgöra internationella åtaganden får behandlas.

Första stycket, som är nytt, reglerar hur länge uppgifter i ärenden om kontaktförbud eller personskydd får behandlas, vilket behandlas i avsnitt 7.5.1. Sådana personuppgifter får inte behandlas längre än ett år efter det att ärendet som uppgifterna behandlades i avslutades.

I *andra stycket*, som motsvarar nuvarande 3 kap. 14 § fjärde stycket, anges hur länge personuppgifter som behandlas i syfte att fullgöra internationella åtaganden får behandlas. Sådana uppgifter får inte behandlas längre än ett år efter utgången av det kalenderår då ärendet som uppgifterna behandlades i avslutades.

Paragrafen anpassas till den terminologi som används i lagen i övrigt.

10 §

Paragrafen reglerar hur länge personuppgifter som har rapporterats till Polismyndighetens ledningscentraler och uppgifter som har gjorts gemensamt tillgängliga i syfte att upprätthålla allmän ordning och säkerhet får behandlas.

Den frist som gäller för hur länge uppgifter som har rapporterats till Polismyndighetens ledningscentraler får behandlas, som motsvarar nuvarande 3 kap. 14 § femte stycket, ändras inte. Samma frist gäller för personuppgifter som har gjorts gemensamt tillgängliga i syfte att upprätthålla allmän och säkerhet, vilket behandlas i avsnitt 7.5.1. Sådana personuppgifter får inte behandlas längre än ett år efter utgången av det kalenderår då de behandlades automatiserat första gången.

Paragrafen anpassas till den terminologi som används i lagen i övrigt.

Föreskrifter

11 §

I paragrafen, som motsvarar nuvarande 3 kap. 12 § och 15 § första stycket, upplyses om att regeringen kan meddela föreskrifter om att vissa kategorier av personuppgifter får fortsätta att behandlas för ändamål inom lagens tillämpningsområde under längre tid än vad som anges i 3, 4 och 7–10 §§.

12 §

I paragrafen upplyses om att regeringen, eller den myndighet som regeringen bestämmer, kan meddela föreskrifter dels om att personuppgifter, trots att den tillåtna tiden för behandling har löpt ut, får fortsätta att behandlas för arkivändamål av allmänt intresse och vetenskapliga, statistiska eller historiska ändamål (vilket motsvarar nuvarande 2 kap. 12 § andra stycket och 13 § tredje stycket och 3 kap. 15 § andra stycket), dels om begränsning av behandlingen av personuppgifter för ändamål inom lagens tillämpningsområde vid digital arkivering (vilket motsvarar motsvarande 2 kap. 12 § tredje stycket). Frågan behandlas i avsnitt 5.5.2 och 5.5.3.

5 kap.

Register över dna-profiler

Rätten att föra register

1 §

Paragrafen, som motsvarar nuvarande 4 kap. 1 §, reglerar Polismyndighetens rätt att föra dna-register (dna-registret, utredningsregistret och spårregistret).

I *första stycket* förtydligas i vilka syften dna-registren får föras, vilket behandlas i avsnitt 7.7.1. Någon ändring i sak är inte avsedd. Stycket ändras också redaktionellt.

Andra stycket är oförändrat.

Dna-registret

2 §

Paragrafen, som motsvarar nuvarande 4 kap. 2 §, är oförändrad frånsett språkliga justeringar.

3 §

Paragrafen, som motsvarar nuvarande 4 kap. 3 §, är oförändrad frånsett en språklig justering.

Utredningsregistret

4 §

Paragrafen, som motsvarar nuvarande 4 kap. 4 §, är oförändrad frånsett språkliga justeringar.

Spårregistret

5 §

Paragrafen, som motsvarar nuvarande 4 kap. 5 §, är oförändrad frånsett en språklig justering.

6 §

Paragrafen, som motsvarar nuvarande 4 kap. 6 §, är oförändrad frånsett språkliga justeringar.

Längsta tid som personuppgifter får behandlas

7 §

Paragrafen, som motsvarar nuvarande 4 kap. 7 §, anger den längsta tid under vilken uppgifter om en person får behandlas i dna-registren. Regleringen behandlas i avsnitt 5.5.2. Någon ändring i fråga om hur länge uppgifterna får behandlas görs inte.

I *första stycket* klargörs att personuppgifter av nu aktuellt slag, trots det som sägs i 2 kap. 17 § andra stycket brottsdatalagen (2018:000) om att arkivlagstiftningen har företräde, inte får arkiveras digitalt. Behandlingen av personuppgifterna ska upphöra när den tid som anges i paragrafen har löpt ut. Terminologin anpassas till den som används i lagen i övrigt.

Andra och tredje styckena anpassas till den terminologi som används i lagen i övrigt.

I *fjärde stycket* ersätts uppräknningen av vissa brott med en hänvisning till 35 kap. 2 § första stycket brottsbalken. Det innebär ingen ändring i sak.

Prover för dna-analys

8 §

Paragrafen, som motsvarar nuvarande 4 kap. 8 §, är oförändrad fränsett språkliga justeringar.

9 §

Paragrafen, som motsvarar nuvarande 4 kap. 9 §, är oförändrad fränsett språkliga justeringar.

Direktåtkomst

10 §

I paragrafen, som motsvarar nuvarande 4 kap. 10 § första stycket, anges förutsättningarna för att medge direktåtkomst till dna-registren. Direktåtkomst får bara medges för något av de syften som

anges i 1 kap. 2 § brottsdatalagen (2018:000). Ändringen är en följd av att uttrycket brottsbekämpande verksamhet utmönstras ur lagen, vilket behandlas i avsnitt 4.4.1.

Fingeravtrycks- och signalementsregister

Rätten att föra register

11 §

Paragrafen, som motsvarar nuvarande 4 kap. 11 § och 12 § tredje stycket och behandlas i avsnitt 7.7.2, reglerar Polismyndighetens rätt att föra fingeravtrycks- och signalementsregister.

I en uppräkningslista anges i vilka syften fingeravtrycks- och signalementsregister får föras. Genom ett tillägg, som motsvarar nuvarande 2 kap. 8 § första stycket punkten 6, tydliggörs att registret också får föras för att kontrollera fingeravtryck som Migrationsverket har tagit enligt 9 kap. 8 § utlänningslagen (2005:716). Någon ändring i sak är inte avsedd.

Innehåll

12 §

I paragrafen, som motsvarar nuvarande 4 kap. 12 §, regleras vilka personer som fingeravtrycks- och signalementsregister får innehålla uppgifter om. *Första och andra styckena* är oförändrade. I *tredje stycket* görs en redaktionell ändring.

13 §

Paragrafen, som motsvarar nuvarande 4 kap. 12 a §, reglerar behandling av fingeravtrycks- och signalementsuppgifter som överförts till Sverige med stöd av det s.k. Ecris-beslutet. Den är oförändrad.

14 §

Paragrafen, som motsvarar nuvarande 4 kap. 13 § och anger vilka uppgifter fingeravtrycks- och signalementsregister får innehålla, är oförändrad.

Längsta tid som personuppgifter får behandlas

15 §

Paragrafen, som motsvarar nuvarande 4 kap. 14 §, anger tillsammans med 16 § den längsta tid under vilken uppgifter om en person får behandlas i fingeravtrycks- och signalementsregister. Terminologin anpassas till den som används i lagen i övrigt.

I paragrafen klargörs att personuppgifterna, trots det som sägs i 2 kap. 17 § andra stycket brottsdatalagen (2018:000) om att arkivlagstiftningen har företräde, inte får arkiveras digitalt. Utgångspunkten är alltså att all automatiserad behandling ska upphöra när den tid som anges i paragrafen har löpt ut, vilket innebär att uppgifterna ska tas bort. Endast om det har meddelats uttryckliga föreskrifter som innebär att uppgifterna i fråga får behandlas för arkivändamål av allmänt intresse eller för vetenskapliga, statistiska eller historiska ändamål får de behandlas automatiserat längre än vad som anges i paragrafen (jfr 27 §). Frågan behandlas i avsnitt 5.5.2.

16 §

Paragrafen, som motsvarar nuvarande 4 kap. 15 §, anger tillsammans med 15 § den längsta tid under vilken uppgifter om en person får behandlas i fingeravtrycks- och signalementsregister. Ändringarna är av samma slag som i 15 § och behandlas i avsnitt 5.5.2.

Direktåtkomst

17 §

I paragrafen, som motsvarar nuvarande 4 kap. 17 § första stycket, regleras förutsättningarna för att medge direktåtkomst. Direktåtkomst får bara medges för något av de syften som anges i 1 kap. 2 §

brottsdatalagen (2018:000). Ändringen beror på att uttrycket brottsbekämpande verksamhet utmönstras ur lagen, vilket behandlas i avsnitt 4.4.1.

Penningtvätsregister

Rätten att föra register

18 §

I paragrafen, som motsvarar nuvarande 4 kap. 18 § första stycket, regleras Polismyndighetens rätt att föra penningtvätsregister. Den är oförändrad.

19 §

I paragrafen, som motsvarar nuvarande 4 kap. 19 §, regleras vilka personuppgifter som får behandlas i penningtvätsregister. Den ändras endast redaktionellt.

Längsta tid som personuppgifter får behandlas

20 §

Paragrafen, som motsvarar nuvarande 4 kap. 20 § första stycket, anger den längsta tid under vilken uppgifter om en person får behandlas i penningtvätsregister. Fristen för hur länge personuppgifter får behandlas ska endast påverkas av om det görs en ny registrering beträffande personens anknytning till brottslig verksamhet. Andra uppgifter som tillförs, t.ex. uppgifter om ändrade bostadsförhållanden eller annat som inte har betydelse för anknytningen till den brottsliga verksamheten, påverkar alltså inte hur länge personuppgifterna får behandlas. Övriga ändringar är av samma slag som i 15 §. Frågan behandlas i avsnitt 5.5.2 och 5.5.4.

Det internationella registret

Rätten att föra register

21 §

I paragrafen, som motsvarar nuvarande 4 kap. 21 § första och andra styckena, regleras Polismyndighetens rätt att föra ett internationellt register. Den är oförändrad.

Längsta tid som personuppgifter får behandlas

22 §

Paragrafen, som motsvarar nuvarande 4 kap. 22 § första stycket, anger den längsta tid under vilken uppgifter om en person får behandlas i det internationella registret. Ändringarna är av samma slag som i 15 §. Frågan behandlas i avsnitt 5.5.2.

Tillträdesförbudsregistret

Rätten att föra register

23 §

Paragrafen reglerar Polismyndighetens rätt att föra ett särskilt register över tillträdesförbud vid idrottsarrangemang, tillträdesförbudsregistret. Paragrafen, som behandlas i avsnitt 16.3, motsvarar nuvarande 2 § och 6 § första stycket lagen (2015:51) om register över tillträdesförbud vid idrottsarrangemang.

Innehåll

24 §

Paragrafen, som reglerar vilka uppgifter som tillträdesförbudsregistret får innehålla, motsvarar nuvarande 8 § lagen (2015:51) om register över tillträdesförbud vid idrottsarrangemang. Den behandlas i avsnitt 16.3.

25 §

Paragrafen, som behandlas i avsnitt 16.3, ger Polismyndigheten rätt att behandla personuppgifter i syfte att tillgodose idrottsorganisationernas behov av att få tillgång till uppgifter om gällande tillträdesförbud.

Paragrafen motsvarar nuvarande 6 § andra stycket lagen (2015:51) om register över tillträdesförbud vid idrottsarrangemang, men anpassas till den terminologi som används i lagen i övrigt. Någon ändring i sak är inte avsedd.

I 2 kap. 11 § finns en sekretessbrytande regel som ger idrottsorganisationer rätt att ta del av nu aktuella uppgifter utan hinder av den sekretess som gäller enligt 35 kap. 4 a § offentlighets- och sekretesslagen (2009:400).

Längsta tid som personuppgifter får behandlas

26 §

Paragrafen, som anger hur länge uppgifter får behandlas i tillträdesförbudsregistret, motsvarar nuvarande 12 § lagen (2015:51) om register över tillträdesförbud vid idrottsarrangemang. Ändringarna är av samma slag som i 15 §. Paragrafen behandlas i avsnitt 16.3.

Föreskrifter

27 §

I paragrafen, där bestämmelser om föreskrifter samlas, upplyses om att regeringen, eller den myndighet som regeringen bestämmer, kan meddela föreskrifter om omfattningen av direktåtkomsten till dna-register och fingeravtrycks- och signalementsregister och om behörighet och säkerhet vid direktåtkomst (vilket motsvarar nuvarande 4 kap. 10 § tredje stycket och 17 § tredje stycket), tillgången till personuppgifter i penningtvättsregister och det internationella registret (vilket motsvarar nuvarande 4 kap. 18 § andra stycket och 21 § tredje stycket) och att personuppgifter i fingeravtrycks- och signalementsregister, penningtvättsregister, det internationella registret och tillträdesförbudsregistret får behandlas under längre

tid för arkivändamål av allmänt intresse och vetenskapliga, statistiska eller historiska ändamål (vilket motsvarar nuvarande 4 kap. 16 §, 20 § andra stycket och 22 § andra stycket).

6 kap.

3 §

I paragrafen anges vad som gäller när personuppgifter som behandlas för forensiska ändamål ska behandlas för nya ändamål. Paragrafen behandlas i avsnitt 7.8.3.

Förutsättningarna för behandling för nya ändamål regleras i 2 kap. 4 och 22 §§ brottsdatalagen (2018:000). Möjligheten att behandla sådana uppgifter för nya ändamål utanför den forensiska verksamheten begränsas till vissa typer av uppgifter och till att det ska vara fråga om behandling i enskilda fall. Paragrafen ändras också till följd av att uttrycket brottsbekämpande verksamhet utmönstras ur lagen, vilket behandlas i avsnitt 4.4.1.

4 §

Paragrafen, som är ny, anger förutsättningarna för att behandla biometriska och genetiska uppgifter i den forensiska verksamheten. Paragrafen behandlas i avsnitt 7.8.4. Biometriska respektive genetiska uppgifter definieras i 1 kap. 6 § brottsdatalagen (2018:000).

Biometriska och genetiska uppgifter får behandlas enligt de förutsättningar som anges i 2 kap. 12 § brottsdatalagen. Det innebär att de bara får behandlas om det är absolut nödvändigt för ändamålet med behandlingen. Om material har samlats in på en brottsplats eller annars tagits om hand inom ramen för en brottsutredning och materialet behöver analyseras forensiskt, får det anses vara absolut nödvändigt att behandla personuppgifterna i fråga.

5 §

I paragrafen, som är ny och behandlas i avsnitt 7.8.4, görs undantag från sökförbudet i 2 kap. 14 § brottsdatalagen (2018:000).

Undantaget innebär att det i forensisk verksamhet är tillåtet att göra sökningar i dna-register och fingeravtrycks- och signalementsregister i syfte att få fram ett personurval grundat på uppgifter som rör hälsa eller biometriska eller genetiska uppgifter. Dna-registren och fingeravtrycksregister består till stor del av biometriska uppgifter. Sökning på uppgifter i dessa register leder därmed till personurval grundade på biometriska uppgifter. I fingeravtrycksregister kan det t.ex. behöva göras sökningar för att få fram uppgifter om personer som saknar en eller flera fingrar, vilket förutom att vara en biometrisk uppgift också kan vara en uppgift om hälsa.

6 §

Paragrafen, som motsvarar nuvarande 5 kap. 7 §, anger den längsta tid under vilken uppgifter om en person får behandlas för forensiska uppslag. Någon ändring i fråga om hur länge personuppgifterna får behandlas görs inte. Paragrafen anpassas till den terminologi som används i lagen i övrigt.

7 §

Paragrafen, som motsvarar nuvarande 5 kap. 8 §, innehåller en sekretessbrytande bestämmelse.

Första stycket ändras till följd av att uttrycket brottsbekämpande verksamhet utmönstras ur lagen, vilket behandlas i avsnitt 4.4.1. I *andra stycket* görs endast en redaktionell ändring.

8 §

I paragrafen, som är ny, föreskrivs att personuppgifter får lämnas ut elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt. Vilka omständigheter som kan påverka den bedömningen framgår av kommentaren till 2 kap. 12 §. Frågan behandlas i avsnitt 5.6.4.

9 §

I paragrafen, som är ny, upplyses om att regeringen kan meddela föreskrifter om begränsning av möjligheten att lämna ut personuppgifter elektroniskt på annat sätt än genom direktåtkomst. Frågan behandlas i avsnitt 5.6.4.

10 §

I paragrafen, som motsvarar nuvarande 5 kap. 6 § andra stycket, upplyses om att regeringen, eller den myndighet som regeringen bestämmer, kan meddela föreskrifter som begränsar behandlingen av personuppgifter vid digital arkivering.

7 kap. Administrativa sanktionsavgifter och rättsmedel

Administrativa sanktionsavgifter

1 §

Paragrafen, som är ny, reglerar vid vilka överträdelser sanktionsavgift får tas ut. Frågan behandlas i avsnitt 5.4.2.

I *första stycket* anges vid vilka överträdelser sanktionsavgift får tas ut av den personuppgiftsansvarige. Tillsynsmyndigheten avgör i det enskilda fallet om det är påkallat att ta ut sanktionsavgift, vilket framgår av formuleringen att avgift får tas ut. Uppräkningen av vilka överträdelser som kan föranleda sanktionsavgift är uttömmande. Sanktionsavgift kan tas ut för överträdelse av bestämmelserna om tillåtna rättsliga grunder, särskilda upplysningar och längsta tid som personuppgifter får behandlas. Brottsdatalogens förfaranderegler när det gäller sanktionsavgifter tillämpas även vid överträdelser enligt denna lag. I brottsdatalogen med tillhörande förordning regleras också handläggningen av frågor om sanktionsavgift.

I *andra stycket* anges storleken på de sanktionsavgifter som kan komma i fråga. De överträdelser som enligt lagen kan föranleda sanktionsavgift är alla av allvarligt slag. Lägsta sanktionsavgift är därför 50 000 kronor.

Skadestånd

2 §

I paragrafen regleras den registrerades rätt till skadestånd för behandling av personuppgifter i strid med regelverket. Paragrafen behandlas i avsnitt 5.4.3.

Paragrafen hänvisar till 7 kap. 1 § brottsdatalagen (2018:000), som ska tillämpas på motsvarande sätt när det har förekommit felaktig behandling av personuppgifter enligt förevarande lag eller föreskrifter som har meddelats i anslutning till den. Det innebär att den personuppgiftsansvarige ska ersätta den registrerade för den skada och kränkning av den personliga integriteten som behandlingen av personuppgifter har orsakat. Med skada avses personskada, sakskada eller ren förmögenhetsskada. Med kränkning avses ideell skada som består i att den enskildes integritet kränkts genom behandlingen. Någon möjlighet till jämkning av skadeståndet finns inte.

Överklagande

3 §

I paragrafen, som behandlas i avsnitt 5.4.4, upplyses om att det i 7 kap. brottsdatalagen (2018:000) finns bestämmelser om överklagande och om vilka beslut som får överklagas.

Övergångsbestämmelser

Ikraftträdande- och övergångsbestämmelserna tas upp i avsnitt 18.1 och 18.2.

Punkten 1 föreskriver när lagen ska träda i kraft.

Sanktionsavgift får enligt *punkten 2* beslutas endast för överträdelser som har begåtts efter ikraftträdandet.

Punkten 3 innebär att bestämmelsen om skadestånd i 48 § personuppgiftslagen fortfarande ska gälla för skada som har orsakats före ikraftträdandet vid behandling av personuppgifter enligt lagen eller föreskrifter som har meddelats i anslutning till den.

20.14 Förslaget till lag om ändring i kustbevakningsdatalagen (2012:145)

Lagen renodlas så att den enbart omfattar personuppgiftsbehandling inom brottsdatalagens tillämpningsområde. Det innebär bl.a. att ett av kapitlen upphävs.

Lagen anpassas till bestämmelserna i brottsdatalagen, vilket leder till en kraftig omarbetning av den. Ytterligare tre kapitel upphävs och fyra nya införs. Bestämmelserna om föreskrifter, som nu är utspridda, samlas i slutet av varje kapitel. Dessa förändringar föranleder omnumreringar av vissa paragrafer.

Bestämmelserna om längsta tid för behandling av personuppgifter samlas i ett särskilt kapitel. Som en anpassning till brottsdatalagen tillkommer ett nytt kapitel om administrativa sanktionsavgifter och rättsmedel.

De generella ändringarna i lagen behandlas i kapitel 4, 5 och 6 och övriga ändringar i kapitel 9.

Lagen får också ett nytt namn, Kustbevakningens brottsdatalag.

1 kap. Allmänna bestämmelser

Lagens tillämpningsområde

1 §

I paragrafen, som behandlas i avsnitt 9.2, anges lagens tillämpningsområde.

Lagen gäller utöver brottsdatalagen när Kustbevakningen i egenskap av behörig myndighet enligt den lagen behandlar personuppgifter för vissa syften. Behörig myndighet, personuppgift och behandling av personuppgifter definieras i 1 kap. 6 § brottsdatalagen (2018:000).

Att lagen gäller utöver brottsdatalagen innebär bl.a. att lagen enligt 1 kap. 3 § brottsdatalagen bara gäller för sådan behandling av personuppgifter som är helt eller delvis automatiserad och för annan behandling av personuppgifter som ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

I brottsdatalagen finns alla de grundläggande bestämmelserna om hur personuppgifter får behandlas. Den nu aktuella lagen innehåller bestämmelser som innebär preciseringar, undantag eller avvikelser från bestämmelser i brottsdatalagen. Det innebär att bestämmelserna i lagen ska läsas tillsammans med regleringen i brottsdatalagen och tolkas i ljuset av den regleringen.

Lagen gäller om syftet med personuppgiftsbehandlingen är att bekämpa eller lagföra brott eller upprätthålla allmän ordning och säkerhet. Vad det innebär utvecklas i kommentaren till 2 kap. 1 §.

2 §

Paragrafen, som motsvarar nuvarande 1 kap. 2 § tredje stycket, anger hur regleringen i lagen förhåller sig till regleringen i lagen (2017:496) om internationellt polisiärt samarbete. Frågan behandlas i avsnitt 17.3.

Personuppgiftsansvar

3 §

Paragrafen, som motsvarar nuvarande 2 kap. 4 §, reglerar personuppgiftsansvaret. Personuppgiftsansvarig definieras i 1 kap. 6 § brottsdatalagen (2018:000). Personuppgiftsansvarigas skyldigheter regleras i 3 kap. brottsdatalagen.

Lagens tillämpning på uppgifter om juridiska personer

4 §

I paragrafen, som motsvarar nuvarande 1 kap. 3 §, anges vilka bestämmelser i lagen och i brottsdatalagen som gäller för behandling av uppgifter om juridiska personer. Frågan behandlas i avsnitt 5.4.1.

Uppräkningen i paragrafen av bestämmelser som gäller vid behandling av uppgifter om juridiska personer motsvarar nuvarande reglering.

2 kap. Grundläggande bestämmelser om behandling

Tillåtna rättsliga grunder för behandling av personuppgifter

1 §

Paragrafen reglerar de tillåtna rättsliga grunderna för behandling av personuppgifter. Den behandlas i avsnitt 6.1, 6.3 och 9.3.1.

Paragrafen, som är anpassad till hur de rättsliga grunderna för behandling av personuppgifter anges i 2 kap. 1 § brottsdatalagen (2018:000), ersätter den bestämmelsen. Regleringen i 2 kap. 2 § brottsdatalagen ger myndigheten rättsligt stöd för att i vissa fall behandla personuppgifter för diarieföring eller för att utföra andra nödvändiga handläggningsuppgifter, trots brist på stöd i denna paragraf.

Kustbevakningen får enligt *första stycket* behandla personuppgifter om det är nödvändigt för att utföra en arbetsuppgift i vissa särskilt angivna syften inom lagens tillämpningsområde. Bestämmelsen bildar den yttre ramen för när behandling av personuppgifter är tillåten.

Enligt *punkten 1* får personuppgifter behandlas i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet. Det är framför allt Kustbevakningens underrättelseverksamhet som avses. Med underrättelseverksamhet avses arbete med insamling, bearbetning och analys av information i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet när det ännu inte finns misstankar om att något konkret brott har begåtts (se prop. 2011/12:45 s. 203). Även behandling av överskottsinformation med stöd av 27 kap. 23 a § rättegångsbalken omfattas, om syftet är att förhindra brott. Personuppgiftsbehandling vid annan brottsförebyggande verksamhet omfattas också.

Enligt *punkten 2* får personuppgifter behandlas i syfte att utreda eller lagföra brott. Att utreda brott innebär framför allt att genomföra förundersökning enligt 23 kap. rättegångsbalken. Med brott avses konkreta brott, men det kan vara fråga om både brott som bevisligen har begåtts och brott som det enbart finns misstankar om. Misstankarna behöver inte vara riktade mot någon bestämd person. Även personuppgiftsbehandling inom ramen för den form av förenklat utredningsförfarande som regleras i 23 kap. 22 § rätte-

gångsbalken och vid åtgärder som vidtas med stöd av 23 kap. 3 och 8 §§ rättegångsbalken omfattas.

Med lagföra brott avses att utfärda förelägganden av ordningsbot.

Kustbevakningen får enligt *punkten 3* behandla personuppgifter i syfte att upprätthålla allmän ordning och säkerhet. När en kustbevakningstjänsteman ingriper vid en konkret ordningsstörning, eller en potentiell sådan störning vid en specifik händelse, är det fråga om att upprätthålla allmän ordning och säkerhet. Detsamma gäller vid ingripande eller andra åtgärder för att avvärja brott. Det kan t.ex. vara fråga om åtgärder enligt 13 § polislagen (1984:387) eller enligt lagstiftningen om sjöfartsskydd eller hamnskydd.

Kustbevakningen får enligt *punkten 4* behandla personuppgifter i syfte att fullgöra förpliktelser som följer av internationella åtaganden. Behandling enligt denna punkt tar sikte på förpliktelser som syftar till att gagna utländsk brottsbekämpande verksamhet (se prop. 2011/12:45 s. 204).

I *andra stycket* anges att det ska vara fråga om en arbetsuppgift som framgår av en bindande unionsrättsakt eller av en lag, en förordning eller ett särskilt beslut i vilket regeringen uppdragit åt myndigheten att ansvara för en sådan uppgift. Motsvarande bestämmelse finns i 2 kap. 1 § brottsdatalagen. Vad den innebär utvecklas i SOU 2017:29 s. 238 f.

2 §

I paragrafen, som behandlas i avsnitt 9.3.1, upplyses om att förutsättningarna för att personuppgifter ska få behandlas för nya ändamål regleras i 2 kap. 4 och 22 §§ brottsdatalagen (2018:000). Innan personuppgifter får behandlas för ett nytt ändamål inom eller utanför brottsdatalagens tillämpningsområde krävs det en prövning enligt någon av paragraferna. Vad prövningen innebär utvecklas i SOU 2017:29 s. 249 f. och avsnitt 6.4.3.

Särskilda upplysningar

3 §

I paragrafen, som behandlas i avsnitt 5.3.10, görs det undantag från bestämmelserna om särskilda upplysningar i 2 kap. 3 § andra stycket, 9 och 10 §§ brottsdatalagen (2018:000). Det är endast personuppgifter som har gjorts gemensamt tillgängliga med stöd av 3 kap. 2 § som i vissa fall ska förses med särskilda upplysningar. Det innebär att när personuppgifter behandlas av bara ett fåtal personer behöver särskilda upplysningar inte lämnas.

Känsliga personuppgifter

4 §

I paragrafen, som tillsammans med 5 § reglerar när det är tillåtet att använda känsliga personuppgifter vid sökning, görs det undantag från sökförbudet i 2 kap. 14 § brottsdatalagen (2018:000). Paragrafen behandlas i avsnitt 9.3.3 och motsvarar nuvarande 4 kap. 4 § andra stycket.

Undantaget gäller vid sökning i alla slags personuppgifter, dvs. i såväl personuppgifter som har gjorts gemensamt tillgängliga som personuppgifter som inte har det. Sökförbudet hindrar inte att brottsrubriceringar, uppgifter om tillvägagångssätt vid brott eller uppgifter som beskriver en persons utseende används vid sökning, även om det skulle leda till ett personurval grundat på känsliga personuppgifter. Att uppgifter om tillvägagångssätt vid brott får användas vid sökning är nytt. Sådan sökning kan aktualiseras bl.a. vid vissa smugglingsbrott.

Med uppgifter som beskriver en persons utseende avses signalementsuppgifter som t.ex. kroppsbyggnad, ansiktsform, hår- och hudfärg, klädsel och fysiska kännetecken som födelsemärken, blindhet och tatueringar (se prop. 2011/12:45 s. 124). En sökning på ett fysiskt särdrag kan ge ett personurval grundat på uppgifter som rör hälsa.

I vilken utsträckning det är tillåtet att behandla någon eller några av personuppgifterna i en sammanställning av sådana uppgifter som sökningen resulterat i får prövas mot huvudregeln om behandling av känsliga personuppgifter i 2 kap. 11 § brottsdata-

lagen. Rätten att göra sökning enligt denna paragraf medför således inte en generell rätt att fortsätta att behandla uppgifterna.

5 §

I paragrafen, som tillsammans med 4 § reglerar när det är tillåtet att använda känsliga personuppgifter vid sökning, görs det undantag från sökförbudet i 2 kap. 14 § brottsdatalagen (2018:000). Paragrafen behandlas i avsnitt 9.3.3.

Undantaget gäller enbart vid sökning i personuppgifter som inte har gjorts gemensamt tillgängliga, dvs. personuppgifter som enbart ett fåtal har tillgång till. Sökning i sådana uppgifter får göras i syfte att få fram ett personurval grundat på etniskt ursprung, religiös eller filosofisk övertygelse eller uppgifter som rör hälsa. Sådana sökningar kan aktualiseras bl.a. vid utredning av brott som kan ha anknytning till etniska grupper eller ha religiösa motiv.

Rätten att söka på känsliga personuppgifter gäller dock inte sökning på ras, politiska åsikter, medlemskap i fackförening, sexualliv eller sexuell läggning eller sökning i genetiska eller biometriska uppgifter. Sökningar som syftar till att få fram ett personurval grundat på sådana uppgifter är alltså inte tillåtna.

I vilken utsträckning det är tillåtet att behandla någon eller några av personuppgifterna i en sammanställning av sådana uppgifter som sökningen resulterat i får prövas mot huvudregeln om behandling av känsliga personuppgifter i 2 kap. 11 § brottsdatalagen. Rätten att göra sökning enligt denna paragraf medför således inte en generell rätt att fortsätta att behandla uppgifterna.

Utlämnande av personuppgifter

6 §

Paragrafen innehåller sekretessbrytande bestämmelser om utlämnande av personuppgifter till utländska myndigheter och mellanfolkliga organisationer. Den motsvarar nuvarande 3 kap. 6 §.

I första stycket görs endast en redaktionell ändring.

Av *andra stycket* framgår att personuppgifter får lämnas ut bara om mottagaren behöver dem för något av de syften som anges i 1 §.

Det innebär att möjligheterna till utlämnande vidgas något, eftersom lagen även gäller vid upprätthållande av allmän ordning och säkerhet. När det gäller mottagare i tredjeländ ska regleringen i 8 kap. 1 § brottsdatalagen (2018:000) också beaktas.

I *tredje stycket* görs endast en redaktionell ändring.

7 §

Paragrafen innehåller en bestämmelse som bryter viss sekretess som annars skulle ha gällt gentemot andra brottsbekämpande myndigheter. Den motsvarar nuvarande 3 kap. 7 §.

Det tydliggörs att sekretessen bryts om den mottagande myndigheten behöver uppgifterna för något av de syften som anges i 1 kap. 2 § brottsdatalagen (2018:000). Ändringen, som är en följd av att uttrycket brottsbekämpande verksamhet utmönstras ur lagen, behandlas i avsnitt 4.4.1.

8 §

Paragrafen reglerar när personuppgifter får lämnas ut elektroniskt.

I *första stycket* föreskrivs att personuppgifter får lämnas ut elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt. Med sådant utlämnande avses bl.a. utlämnande genom e-post eller annan elektronisk överföring eller på ett usb-minne eller annat motsvarande medium. Frågan behandlas i avsnitt 5.6.4.

Det har betydelse vem mottagaren är för frågan om det är olämpligt att lämna ut uppgifter elektroniskt. Som regel kan det inte anses vara olämpligt att lämna ut uppgifter på det sättet till en myndighet (se prop. 2014/15:148 s. 113, jfr SOU 2015:39 s. 447 f.).

När det gäller utlämnande till enskilda krävs en mer nyanserad bedömning. Om det finns en författningsreglerad skyldighet att sända en handling till en viss person får det avgöras om elektroniskt utlämnande är olämpligt med hänsyn till bl.a. innehållet i handlingen, vem som är mottagare, behovet av att kunna visa att personen i fråga har tagit del av handlingen och andra omständigheter.

Frågan är särskilt svårbedömd när uppgifter ska lämnas ut till enskilda och det på grund av uppgifternas art, struktur, antal eller någon annan särskild omständighet finns anledning att befara att

utlämnandet kan leda till integritetsrisker (jfr prop. 2014/15:148 s. 114). Bedömer myndigheten att det finns risk för att personuppgifterna kan komma att missbrukas om de lämnas ut elektroniskt gäller sekretess enligt 21 kap. 7 § offentlighets- och sekretesslagen (2009:400). De får då inte lämnas ut till följd av sekretess.

Det kan också finnas särskild anledning att iaktta försiktighet när det gäller utlämnande av bild- och ljudupptagningar (jfr prop. 2016/17:68 s. 51 f.).

Vid prövningen av om personuppgifter bör lämnas ut elektroniskt bör givetvis även informationssäkerheten vägas in.

Om någon begär att få tillgång till en allmän handling med stöd av tryckfrihetsförordningen får den utlämnande myndigheten inte efterforska syftet med begäran. Det kan ha betydelse för möjligheten att få underlag för att bedöma om det i ett enskilt fall är lämpligt att lämna ut en handling med personuppgifter elektroniskt (se JO dnr 4171-2011).

Elektroniskt utlämnande genom direktåtkomst regleras i *andra stycket*, som motsvarar nuvarande 2 kap. 9 §. Det är tillåtet bara i den utsträckning som anges i lagen.

Föreskrifter

9 §

I paragrafen upplyses om att regeringen kan meddela föreskrifter om att personuppgifter får lämnas ut även i andra fall än som anges i 6 och 7 §§ (vilket motsvarar nuvarande 3 kap. 8 § första stycket) och om begränsning av möjligheten att lämna ut personuppgifter elektroniskt på annat sätt än genom direktåtkomst, vilket behandlas i avsnitt 5.6.4.

3 kap.

1 §

Av paragrafen framgår att kapitlet innehåller bestämmelser om behandling av personuppgifter som görs eller har gjorts gemensamt tillgängliga.

I *första stycket* anges vad kapitlet innehåller. Vidare anges vad som avses med uttrycket gemensamt tillgängliga uppgifter, vilket motsvarar nuvarande 1 kap. 4 §. Vad det innebär utvecklas i prop. 2011/12:145 s. 210 f.

Av *andra stycket* framgår att kapitlet inte gäller när personuppgifter behandlas med stöd av den särskilda bestämmelsen i 2 kap. 2 § brottsdatalagen (2018:000) om behandling av personuppgifter för diarieföring eller för att utföra andra nödvändiga handläggningsuppgifter.

2 §

I paragrafen, som motsvarar nuvarande 4 kap. 1 § och behandlas i avsnitt 9.4.2, anges vilka personuppgifter som får göras gemensamt tillgängliga. Regleringen anpassas till att uttrycket brottsbekämpande verksamhet utmönstras ur lagen, vilket behandlas i avsnitt 4.4.1.

I *punkten 1* görs endast en redaktionell ändring.

I *punkten 2* anpassas terminologin till den som används i lagen i övrigt.

Enligt *punkten 3*, som är ny, får personuppgifter som behandlas i syfte att upprätthålla allmän ordning och säkerhet göras gemensamt tillgängliga. Det kan t.ex. vara fråga om uppgifter om personer som bedöms kunna utgöra ett hot mot allmän ordning och säkerhet. Inför förväntade ordningsstörningar riktade mot sjötrafiken eller enskilda fartyg kan Kustbevakningen behöva göra uppgifter gemensamt tillgängliga om personer som vid tidigare tillfällen gjort sig skyldiga till ordningsstörningar.

Punkten 4 är oförändrad.

Punkten 5 motsvarar nuvarande punkten 3.

3 §

I paragrafen, som behandlas i avsnitt 5.3.10 och motsvarar nuvarande 4 kap. 3 §, föreskrivs att uppgifter i underrättelseverksamhet som är gemensamt tillgängliga ska föras med särskilda upplysningar.

Enligt *första stycket* ska det framgå av uppgifter i underrättelseverksamhet att en person inte är misstänkt för att utöva brottslig

verksamhet. Det ska alltså gå att skilja mellan personer som är föremål för myndighetens intresse på grund av inblandning i brottslig verksamhet och personer som inte är misstänkta för det. Att det ska framgå om en person är misstänkt för brott eller är ett brotts-offer, regleras i 2 kap. 9 § brottsdatalagen (2018:000).

Enligt *andra stycket* ska uppgifter om personer som kan antas ha samband med misstänkt brottslig verksamhet förse med upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak. Det tydliggörs att kravet på särskild upplysning bara gäller uppgifter om en person som kan antas ha direkt samband med misstänkt brottslig verksamhet. Kravet på samband är lågt ställt. Så snart det finns något som stöder ett antagande om att en person har ett direkt samband med brottslig verksamhet och det är fråga om uppgifter som görs gemensamt tillgängliga ska det framgå på vilket sätt personen har anknytning till den brottsliga verksamheten. Sambandet kan t.ex. bestå i att en person ofta träffar eller har annan kontakt med andra personer som är misstänkta för att utöva brottslig verksamhet eller ofta rör sig i miljöer där brottslighet förekommer, utan att ha naturliga skäl att befinna sig där. Uppgifter om den som är anhörig till en person som kan antas ha samband med misstänkt brottslig verksamhet faller alltså utanför, utom i de fall där båda kan antas ha direkt samband med brottslig verksamhet.

Det är bara uppgifter som rör en person som är misstänkt för att utöva eller komma att utöva brottslig verksamhet som behöver förse med upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak. De uppgifter som är av intresse är, förutom uppgifter om på vilket sätt personen är knuten till den brottsliga verksamheten, framför allt uppgifter som belyser brottslighetens art och omfattning. Uppgifter av det slaget kan behöva förse med särskilda upplysningar för att personens anknytning till brottsligheten ska kunna bedömas.

Utrymmet för att underlåta att förse uppgifter med upplysning om trovärdighet och riktighet vidgas något genom att det inte längre krävs särskilda omständigheter för att upplysningskravet inte ska gälla. Det är tillräckligt att det på grund av de samlade omständigheterna är onödigt att förse uppgifterna med en upplysning.

4 §

Paragrafen, som behandlas i avsnitt 9.4.3 och motsvarar nuvarande 4 kap. 5 § första stycket, innehåller en allmän begränsning av vilka uppgifter som får tas fram vid sökning i gemensamt tillgängliga uppgifter på namn, personnummer, samordningsnummer eller liknande identitetsbeteckningar.

Genom ett tillägg tydliggörs att paragrafen endast gäller vid sökning i automatiserade behandlingssystem. Vad som avses med automatiserade behandlingssystem anges i SOU 2017:29 s. 306 f. Paragrafen ändras i övrigt endast redaktionellt.

5 §

Paragrafen, som behandlas i avsnitt 9.4.3 och motsvarar nuvarande 4 kap. 6 § första stycket, gör undantag från begränsningarna i 4 §.

Enligt *första stycket* gäller inga begränsningar vid sökning i en viss handling eller i ett visst ärende.

Enligt *andra stycket* gäller begränsningarna i 4 § inte vid vissa sökningar som utförs av särskilt angivna tjänstemän i syfte att bearbeta och analysera personuppgifter som har gjorts gemensamt tillgängliga i underrättelseverksamhet, om det endast är de tjänstemän som får göra sökningen som har tillgång till informationen.

6 §

I paragrafen, som motsvarar nuvarande 4 kap. 7 § första stycket, anges vilka myndigheter som får medges direktåtkomst till uppgifter som har gjorts gemensamt tillgängliga och för vilka syften. Paragrafen ändras som en följd av att uttrycket brottsbekämpande verksamhet utmönstras ur lagen, vilket behandlas i avsnitt 4.4.1. Den ändras också redaktionellt.

7 §

I paragrafen, som motsvarar nuvarande 4 kap. 6 § tredje stycket, upplyses om att regeringen kan meddela föreskrifter om ytterligare undantag från bestämmelserna om sökning i 4 §.

8 §

I paragrafen, där övriga bestämmelser om föreskrifter samlas, upplyses om att regeringen, eller den myndighet som regeringen bestämmer, kan meddela föreskrifter om begränsning av tillgången till sådana uppgifter som avses i 4 § (vilket motsvarar nuvarande 4 kap. 5 § andra stycket), under vilka förutsättningar sökning får utföras med stöd av 5 § (vilket motsvarar nuvarande 4 kap. 6 § andra stycket) och omfattningen av direktåtkomsten och om behörighet och säkerhet vid sådan åtkomst (vilket motsvarar nuvarande 4 kap. 7 § tredje stycket).

4 kap. Längsta tid som personuppgifter får behandlas

Allmän bestämmelse

1 §

De bestämmelser som anger hur länge personuppgifter får behandlas samlas i detta kapitel. Frågan behandlas i avsnitt 5.5.1.

I *första stycket* föreskrivs att bestämmelserna i kapitlet endast gäller för personuppgifter som behandlas automatiserat.

Andra stycket upplyser om att den grundläggande bestämmelsen om att personuppgifter inte får behandlas längre än vad som är nödvändigt med hänsyn till ändamålet med behandlingen finns i 2 kap. 17 § första stycket brottsdatalagen (2018:000). I övriga paragrafer i kapitlet anges hur länge vissa typer av personuppgifter får behandlas inom den ram som sätts av denna huvudregel. Oavsett vilken bedömning som görs av nyttan med behandlingen av en viss personuppgift får den dock inte behandlas längre än vad som anges i respektive paragraf.

Personuppgifter som inte har gjorts gemensamt tillgängliga

2 §

I paragrafen, som motsvarar nuvarande 3 kap. 5 §, anges hur länge personuppgifter som inte har gjorts gemensamt tillgängliga får behandlas. Regleringen behandlas i avsnitt 5.5.2. Någon ändring av hur länge sådana personuppgifter får behandlas görs inte.

I *första stycket* klargörs att uppgifterna, trots det som sägs i 2 kap. 17 § andra stycket brottsdatalagen om att arkivlagstiftningen har företräde, inte får arkiveras digitalt. Utgångspunkten är alltså att all automatiserad behandling av personuppgifterna ska upphöra när den tid som anges i paragrafen har löpt ut, vilket innebär att de ska tas bort. Endast om det har meddelats uttryckliga föreskrifter som innebär att uppgifterna i fråga får behandlas för arkivändamål av allmänt intresse eller för vetenskapliga, statistiska eller historiska ändamål får de behandlas automatiserat längre än vad som anges i förevarande paragraf (jfr 11 §).

Andra stycket klargör att paragrafen inte ska tillämpas på ärenden om utredning av eller lagföring för brott.

Gemensamt tillgängliga uppgifter i ärenden om utredning av eller lagföring för brott

3 §

Paragrafen, som motsvarar nuvarande 4 kap. 9 §, reglerar hur länge personuppgifter i en anmälan om brott får behandlas. Terminologin anpassas till den som används i lagen i övrigt och till att uttrycket brottsbekämpande verksamhet utmönstras ur lagen, vilket behandlas i avsnitt 4.4.1.

Enligt paragrafen inskränks enbart behandlingen av personuppgifter för de ändamål som regleras i lagen, vilket innebär att uppgifterna får fortsätta att behandlas automatiserat för bl.a. arkivändamål efter de tidpunkter som anges i paragrafen. Frågan behandlas i avsnitt 5.5.3.

4 §

Paragrafen, som motsvarar nuvarande 4 kap. 10 §, reglerar hur länge personuppgifter i förundersökningar och andra utredningar som handläggs enligt bestämmelserna i 23 kap. rättegångsbalken får behandlas.

Enligt paragrafen inskränks enbart behandlingen av personuppgifter för de ändamål som regleras i lagen, vilket innebär att uppgifterna får fortsätta att behandlas automatiserat bl.a. för arkivändamål efter de tidpunkter som anges i paragrafen. Frågan behandlas i avsnitt 5.5.3.

Terminologin i *första och andra styckena* anpassas till den som används i lagen i övrigt och till att uttrycket brottsbekämpande verksamhet utmönstras ur lagen, vilket behandlas i avsnitt 4.4.1. Vissa redaktionella ändringar görs också.

Tredje stycket är oförändrat.

5 §

Paragrafen, som motsvarar nuvarande 4 kap. 12 §, reglerar vad som gäller i fråga om personuppgifter som rör någon som har varit misstänkt i en förundersökning som har lagts ner eller där åtal har lagts ner eller frikännande dom har meddelats och fått laga kraft. I paragrafen görs endast en redaktionell ändring.

Övriga gemensamt tillgängliga uppgifter

6 §

I paragrafen anges att det i de följande paragraferna finns bestämmelser om hur länge vissa typer av gemensamt tillgängliga uppgifter, som inte förekommer i ärenden om utredning av eller lagföring för brott, får behandlas. Det klargörs att uppgifterna, trots det som sägs i 2 kap. 17 § andra stycket brottsdatalagen (2018:000) om att arkivlagstiftningen har företräde, inte får arkiveras digitalt. Utgångspunkten är alltså att all automatiserad behandling av personuppgifterna ska upphöra när den tid som anges i 7–9 §§ har löpt ut, vilket innebär att uppgifterna ska tas bort. Endast om det har meddelats uttryckliga föreskrifter som innebär att uppgifterna i fråga

får behandlas för arkivändamål av allmänt intresse eller för vetenskapliga, statistiska eller historiska ändamål får de behandlas automatiserat längre än vad som anges i de följande paragraferna (jfr 11 §). Frågan behandlas i avsnitt 5.5.2.

7 §

Paragrafen, som motsvarar nuvarande 4 kap. 13 § andra stycket, reglerar hur länge personuppgifter får behandlas i underrättelseverksamhet. Någon ändring görs inte i fråga om hur länge personuppgifterna får behandlas. Det tydliggörs att fristen för hur länge personuppgifter får behandlas endast ska påverkas av om det görs en ny registrering beträffande personens anknytning till brottslig verksamhet. Andra uppgifter som tillförs, t.ex. uppgifter om ändrade bostadsförhållanden eller annat som inte har betydelse för anknytningen till den brottsliga verksamheten, påverkar alltså inte hur länge personuppgifterna får behandlas. Frågan behandlas i avsnitt 5.5.4.

Paragrafen anpassas också till den terminologi som används i lagen i övrigt.

8 §

Paragrafen, som motsvarar nuvarande 4 kap. 13 § fjärde stycket, reglerar hur länge personuppgifter som behandlas i syfte att upprätthålla allmän ordning och säkerhet och personuppgifter som har rapporterats till Kustbevakningens ledningscentraler får behandlas.

Den frist som gäller för hur länge uppgifter som har rapporterats till Kustbevakningens ledningscentraler får behandlas, som motsvarar nuvarande 4 kap. 13 § tredje stycket, ändras inte. Samma frist gäller för personuppgifter som har gjorts gemensamt tillgängliga i syfte att upprätthålla allmän ordning och säkerhet, vilket behandlas i avsnitt 9.4.2. Sådana personuppgifter får inte behandlas längre än ett år efter utgången av det kalenderår då de behandlades automatiserat första gången.

Paragrafen anpassas till den terminologi som används i lagen i övrigt.

9 §

Paragrafen, som motsvarar nuvarande 4 kap. 13 § tredje stycket, reglerar hur länge personuppgifter som behandlas i syfte att fullgöra internationella åtaganden får behandlas. Paragrafen anpassas till den terminologi som används i lagen i övrigt.

Föreskrifter

10 §

I paragrafen upplyses om att regeringen kan meddela föreskrifter om att vissa kategorier av personuppgifter får fortsätta att behandlas för ändamål inom lagens tillämpningsområde under längre tid än vad som anges i 3, 4 och 7–9 §§ (vilket motsvarar nuvarande 4 kap. 11 § och 14 § första stycket) och om begränsning av behandlingen av personuppgifter för ändamål inom lagens tillämpningsområde vid digital arkivering (vilket motsvarar nuvarande 3 kap. 4 § tredje stycket). Frågan behandlas i avsnitt 5.5.3. Paragrafen anpassas till den terminologi som används i lagen i övrigt.

11 §

I paragrafen, som motsvarar nuvarande 3 kap. 5 § tredje stycket och 4 kap. 14 § andra stycket, upplyses om att regeringen, eller den myndighet som regeringen bestämmer, kan meddela föreskrifter om att personuppgifter, trots att den tillåtna tiden för behandling har löpt ut, får fortsätta att behandlas för arkivändamål av allmänt intresse och vetenskapliga, statistiska eller historiska ändamål. Frågan behandlas i avsnitt 5.5.2. Paragrafen anpassas till den terminologi som används i lagen i övrigt och ändras också redaktionellt.

5 kap. Administrativa sanktionsavgifter och rättsmedel

Administrativa sanktionsavgifter

1 §

Paragrafen, som är ny, reglerar vid vilka överträdelser sanktionsavgift får tas ut. Frågan behandlas i avsnitt 5.4.2.

I *första stycket* anges vid vilka överträdelser sanktionsavgift får tas ut av den personuppgiftsansvarige. Tillsynsmyndigheten avgör i det enskilda fallet om det är påkallat att ta ut sanktionsavgift, vilket framgår av formuleringen att avgift får tas ut. Uppräkningen av vilka överträdelser som kan föranleda sanktionsavgift är uttömmande. Sanktionsavgift kan tas ut för överträdelse av bestämmelserna om tillåtna rättsliga grunder, särskilda upplysningar och längsta tid som personuppgifter får behandlas. Brottsdatalogens förfaranderegler när det gäller sanktionsavgift tillämpas även vid överträdelser enligt denna lag. I brottsdatalogen med tillhörande förordning regleras också handläggningen av frågor om sanktionsavgift.

I *andra stycket* anges storleken på de sanktionsavgifter som kan komma i fråga. De överträdelser som enligt lagen kan föranleda sanktionsavgift är alla av allvarligt slag. Lägsta sanktionsavgift är därför 50 000 kronor.

Skadestånd

2 §

I paragrafen regleras den registrerades rätt till skadestånd för behandling av personuppgifter i strid med regelverket. Paragrafen behandlas i avsnitt 5.4.3.

Paragrafen hänvisar till 7 kap. 1 § brottsdatalogen (2018:000), som ska tillämpas på motsvarande sätt när det har förekommit felaktig behandling av personuppgifter enligt förevarande lag eller föreskrifter som har meddelats i anslutning till den. Det innebär att den personuppgiftsansvarige ska ersätta den registrerade för den skada och kränkning av den personliga integriteten som behandlingen av personuppgifter har orsakat. Med skada avses personskada, sakskada eller ren förmögenhetsskada. Med kränkning avses

ideell skada som består i att den enskildes integritet kränkts genom behandlingen. Någon möjlighet till jämkning av skadeståndet finns inte.

Överklagande

3 §

I paragrafen, som behandlas i avsnitt 5.4.4, upplyses om att det i 7 kap. brottsdatalogen (2018:000) finns bestämmelser om överklagande och om vilka beslut som får överklagas.

Övergångsbestämmelser

Ikraftträdande- och övergångsbestämmelserna tas upp i avsnitt 18.1 och 18.2.

Punkten 1 föreskriver när lagen ska träda i kraft.

Sanktionsavgift får enligt *punkten 2* beslutas endast för överträdelser som har begåtts efter ikraftträdandet.

Punkten 3 innebär att bestämmelsen om skadestånd i 48 § personuppgiftslagen fortfarande ska gälla för skada som har orsakats före ikraftträdandet vid behandling av personuppgifter enligt lagen eller föreskrifter som har meddelats i anslutning till den.

20.15 Förslaget till lag om ändring i lagen (2014:400) om Polismyndighetens elimineringsdatabas

1 §

Paragrafen reglerar Polismyndighetens rätt att föra register över dna-profiler.

I *första och andra styckena* görs endast redaktionella ändringar.

I *tredje stycket* ändras en hänvisning till en lag som byter namn, vilket behandlas i avsnitt 7.2.1.

2 §

Paragrafen reglerar förhållandet till annan personuppgiftsreglering. I paragrafen, som behandlas i avsnitt 17.4, föreskrivs att lagen gäller utöver brottsdatalagen (2018:000). Vad det innebär utvecklas i kommentaren till 1 kap. 1 § polisens brottsdatalag (2010:361).

4 §

Av paragrafen framgår vilka jämförelser som får göras med dna-profiler i elimineringsdatabasen.

I *första och andra styckena* ändras hänvisningar till en lag som byter namn, vilket behandlas i avsnitt 7.2.1. Vidare görs redaktionella ändringar.

I *tredje stycket* görs endast redaktionella ändringar.

11 §

Paragrafen reglerar hur länge uppgifter får behandlas i elimineringsdatabasen.

I *första stycket*, som är nytt, klargörs att uppgifterna, trots det som sägs i 2 kap. 17 § andra stycket brottsdatalagen (2018:000) om att arkivlagstiftningen har företräde, inte får arkiveras digitalt. Det innebär att all automatiserad behandling av personuppgifterna ska upphöra när de tider som anges i paragrafen har löpt ut.

Ändringarna i *andra–femte styckena* består enbart i anpassningar till brottsdatalagen (2018:000) och den terminologi som används i den lagen. Ändringarna behandlas i avsnitt 17.4.

12 §

Paragrafen, som behandlas i avsnitt 17.4, hänvisar till bestämmelsen om skadestånd 7 kap. 1 § brottsdatalagen (2018:000), som ska tillämpas på motsvarande sätt när det har förekommit felaktig behandling av personuppgifter enligt förevarande lag. Vad hänvisningen innebär utvecklas i kommentaren till 7 kap. 2 § polisens brottsdatalag (2010:361).

20.16 Förslaget till lag om ändring i lagen (2015:51) om register över tillträdesförbud vid idrottsarrangemang

Bestämmelserna om Polismyndighetens behandling av personuppgifter flyttas, av de skäl som anges i avsnitt 16.2, till polisens brottsdatalag (2010:361). Till följd av det upphävs ett flertal paragrafer i lagen och de återstående paragraferna numreras om och ändras redaktionellt. Lagen ges också nytt namn.

Dataskyddsförordningen och lagen med kompletterande bestämmelser till EU:s dataskyddsförordning gäller för idrottsorganisationernas behandling av personuppgifter. Lagen anger, tillsammans med regleringen i lagen (2005:321) om tillträdesförbud vid idrottsarrangemang, den rättsliga grunden för att idrottsorganisationer får behandla personuppgifter från tillträdesförbudsregistret.

1 §

I paragrafen anges syftet med lagen. Regleringen omfattar numera enbart idrottsorganisationernas behandling av personuppgifter för att upprätthålla gällande tillträdesförbud. Det förtydligas att behandlingen rör tillträdesförbud som avses i 1 § lagen (2005:321) om tillträdesförbud vid idrottsarrangemang.

Ändringarna behandlas i avsnitt 16.3 och 16.4.

2 §

Paragrafen, som behandlas i avsnitt 16.3 och 16.4 och motsvarar nuvarande 3 §, anger lagens tillämpningsområde.

I *första stycket* regleras numera endast idrottsorganisationernas behandling av personuppgifter.

I *andra stycket* görs enbart redaktionella ändringar.

3 §

Paragrafen, som är ny och behandlas i avsnitt 16.4, anger hur lagen förhåller sig till annan reglering om personuppgiftsbehandling.

Av paragrafen framgår att dataskyddsförordningen gäller vid idrottsorganisationernas behandling av personuppgifter. Lagen med kompletterande bestämmelser till EU:s dataskyddsförordning gäller om det inte finns avvikande bestämmelser i denna lag eller föreskrifter som har meddelats i anslutning till den. Det framgår av hänvisningen i paragrafen.

4 §

I paragrafen, som motsvarar nuvarande 5 § andra stycket och behandlas i avsnitt 16.3 och 16.4, regleras numera endast idrottsorganisationernas personuppgiftsansvar.

6 §

Paragrafen, som motsvarar nuvarande 11 §, reglerar tillgången till personuppgifter. Regleringen i *första stycket* omfattar numera enbart idrottsorganisationernas behandling av personuppgifter. Ändringen behandlas i avsnitt 16.3 och 16.4. *Andra stycket* ändras inte.

7 §

Paragrafen, som motsvarar nuvarande 13 §, reglerar hur länge en idrottsorganisation får behandla personuppgifter som rör tillträdesförbud. I paragrafen, som behandlas i avsnitt 16.4, tydliggörs när behandlingen av personuppgifter senast måste upphöra.

Övergångsbestämmelser

Ikraftträdande- och övergångsbestämmelserna tas upp i avsnitt 18.1 och 18.3.

Punkten 1 föreskriver när lagen ska träda i kraft.

Enligt *punkten 2* ska vissa äldre bestämmelser fortsätta att gälla fram till dess att dataskyddsförordningen börjar tillämpas.

Enligt *punkten 3* ska 3 §, som reglerar förhållandet till dataskyddsförordningen med kompletterande lagstiftning, inte tillämpas förrän den 25 maj 2018.

20.17 Förslaget till lag om ändring i åklagardatalagen (2015:433)

Lagen renodlas så att den enbart omfattar personuppgiftsbehandling inom brottsdatalagens tillämpningsområde. Det leder bara till en mindre ändring.

Lagen anpassas till bestämmelserna i brottsdatalagen, vilket leder till en kraftig omarbetning av den och att två kapitel upphävs och ersätts med nya. Även i de övriga kapitlen upphävs vissa paragrafer, samtidigt som nya paragrafer tillkommer. Bestämmelserna om föreskrifter, som nu är utspridda, samlas i slutet av varje kapitel. Dessa förändringar föranleder bl.a. omnumreringar av vissa paragrafer.

Bestämmelserna om längsta tid för behandling av personuppgifter samlas i ett särskilt kapitel. Som en anpassning till brottsdatalagen tillkommer ett nytt kapitel om administrativa sanktionsavgifter och rättsmedel.

De generella ändringarna i lagen behandlas i kapitel 4, 5 och 6 och övriga ändringar i kapitel 11.

Lagen får också ett nytt namn, åklagarväsendets brottsdatalag.

1 kap. Allmänna bestämmelser

Lagens tillämpningsområde

1 §

I paragrafen, som behandlas i avsnitt 11.2 anges lagens tillämpningsområde.

Lagen gäller enligt *första stycket* utöver brottsdatalagen när Åklagarmyndigheten eller Ekobrottsmyndigheten, som tillsammans utgör åklagarväsendet, i egenskap av behörig myndighet enligt brotts-

datalagen behandlar personuppgifter i åklagarverksamhet för vissa syften. Behörig myndighet, personuppgift och behandling av personuppgifter definieras i 1 kap. 6 § brottsdatalagen (2018:000).

Att lagen gäller utöver brottsdatalagen innebär bl.a. att lagen enligt 1 kap. 3 § brottsdatalagen bara gäller för sådan behandling av personuppgifter som är helt eller delvis automatiserad och för annan behandling av personuppgifter som ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

I brottsdatalagen finns alla de grundläggande bestämmelserna om hur personuppgifter får behandlas. Den nu aktuella lagen innehåller bestämmelser som innebär preciseringar, undantag eller avvikelser från bestämmelser i brottsdatalagen. Det innebär att bestämmelserna i lagen ska läsas tillsammans med regleringen i brottsdatalagen och tolkas i ljuset av den regleringen.

Lagen gäller när Åklagarmyndigheten eller Ekobrottsmyndigheten behandlar personuppgifter om syftet med behandlingen är att bekämpa eller lagföra brott eller handlägga frågor om ändring eller verkställighet av straffrättsliga påföljder eller upprätthållande av allmän ordning och säkerhet. Vad det innebär utvecklas i kommentaren till 2 kap. 1 §.

En förutsättning för att lagen ska gälla är att personuppgiftsbehandlingen utförs i åklagarverksamhet. Med det avses behandling av personuppgifter i samband med att åklagare fullgör åklagaruppgifter t.ex. som förundersökningsledare eller fattar beslut i fråga om lagförelse. Vad det innebär utvecklas i avsnitt 7.2.1 och kommentaren till 2 kap. 1 §.

För Ekobrottsmyndighetens del gäller lagen när myndigheten behandlar personuppgifter i sin åklagarverksamhet i syfte att utreda eller lagföra brott eller handlägga frågor om ändring eller verkställighet av straffrättsliga påföljder. Om Ekobrottsmyndigheten däremot behandlar personuppgifter i syfte att utreda brott och det inte är fråga om åklagarverksamhet gäller i stället polisens brottsdatalag.

Lagen gäller inte när åklagaruppgifter utförs för andra syften än de som anges i paragrafen, t.ex. när åklagare fattar beslut enligt lagen (2011:111) om förstörande av vissa hälsofarliga missbrukssubstanter (se SOU 2017:29 s. 232 f.).

I *andra stycket* upplyses om att det även finns bestämmelser om personuppgiftsbehandling vid Ekobrottsmyndigheten i polisens brottsdatalag.

Personuppgiftsansvar

2 §

Paragrafen, som motsvarar nuvarande 2 kap. 3 §, reglerar personuppgiftsansvaret. Personuppgiftsansvarig definieras i 1 kap. 6 § brottsdatalagen (2018:000). Personuppgiftsansvarigas skyldigheter regleras i 3 kap. brottsdatalagen.

Lagens tillämpning på uppgifter om juridiska personer

3 §

I paragrafen anges vilka bestämmelser i lagen och i brottsdatalagen (2018:000) som gäller för behandling av uppgifter om juridiska personer. Paragrafen behandlas i avsnitt 5.4.1.

Uppräkningen i paragrafen av bestämmelser som gäller vid behandling av uppgifter om juridiska personer motsvarar nuvarande 1 kap. 4 §.

2 kap. Grundläggande bestämmelser om behandling

Tillåtna rättsliga grunder för behandling av personuppgifter

1 §

Paragrafen reglerar de tillåtna rättsliga grunderna för behandling av personuppgifter. Den behandlas i avsnitt 6.1, 6.3 och 11.3.1.

Paragrafen, som är anpassad till hur de rättsliga grunderna för behandling av personuppgifter är utformade i 2 kap. 1 § brottsdatalagen (2018:000), ersätter den bestämmelsen. Regleringen i 2 kap. 2 § brottsdatalagen ger myndigheterna rättsligt stöd för att i vissa fall behandla personuppgifter enbart för diarieföring och nödvändig handläggning, trots brist på stöd i denna paragraf.

Åklagarväsendet får enligt *första stycket* behandla personuppgifter om det är nödvändigt för att utföra en arbetsuppgift i vissa särskilt angivna syften inom lagens tillämpningsområde. Bestämmelsen bildar den yttre ramen för när behandling av personuppgifter är tillåten.

Enligt *punkten 1* får personuppgifter behandlas i syfte att förebygga eller förhindra brottslig verksamhet. Med förebygga brottslig verksamhet avses Ekobrottsmyndighetens brottsförebyggande arbete. I det ingår att lämna information om ekonomisk brottslighet till andra myndigheter, kommuner, näringsliv, organisationer och allmänheten. Det brottsförebyggande arbete som utförs vid Ekobrottsmyndigheten är inte något underrättelsearbete, utan ett strategiskt förebyggande arbete där personuppgifter normalt inte förekommer, men det kan inte uteslutas (se prop. 2014/15:63 s. 64). Underrättelseverksamheten regleras i polisens brottsdatalog.

Med förhindra brottslig verksamhet avses bl.a. de uppgifter som åklagare vid Åklagarmyndigheten utför enligt lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott, t.ex. att ansöka om tillstånd till hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation. Även behandling av överskottsinformation med stöd av 27 kap. 23 a § rättegångsbalken omfattas, om syftet är att förhindra brott.

Åklagarväsendet får enligt *punkten 2* behandla personuppgifter i syfte att utreda eller lagföra brott, vilket utgör huvuddelen av verksamheten. Med utreda brott avses framför allt att besluta om förundersökningsbegränsning och leda förundersökning enligt 23 kap. rättegångsbalken. Termen brott avser konkreta brott, men det kan vara fråga om både brott som bevisligen har begåtts och brott som det enbart finns misstankar om. Misstankarna behöver inte vara riktade mot någon bestämd person. Personuppgiftsbehandling inom ramen för den form av förenklat utredningsförfarande som regleras i 23 kap. 22 § rättegångsbalken omfattas också. Den gäller även för andra utredningar som genomförs enligt bestämmelserna i 23 kap. rättegångsbalken. Vad bestämmelsen innebär utvecklas i prop. 2014/15:63 s. 140.

Med lagföra brott avses främst beslut i fråga om åtal eller annan talan vid domstol, t.ex. särskild förverkandetalan, och att utfärda strafföreläggande (se prop. 2014/15:63 s. 140). Beslut i fråga om åtalsunderlåtelse och om särskild åtalsprövning är andra exempel.

Hit hör också att föra talan om eller vara motpart i fråga om resning och andra extraordinära rättsmedel.

Enligt *punkten 3* får åklagarväsendet behandla personuppgifter i syfte att handlägga frågor om ändring eller verkställighet av straffrättsliga påföljder. Till *punkten* hör ärenden om ändring eller undanröjande av påföljd. Exempel på handläggning av frågor om verkställighet av straffrättsliga påföljder är yttranden om rättspsykiatrisk vård eller utfärdande av arresteringsorder som rör straffverksställighet. Frågor om resning kan, om de inte hör under *punkten 2*, också höra hit.

Personuppgifter får enligt *punkten 4* också behandlas i syfte att handlägga frågor som rör upprätthållande av allmän ordning och säkerhet. *Punkten* är tillämplig när åklagare utreder och prövar frågor om tillträdesförbud vid idrottsarrangemang.

Åklagarväsendet får enligt *punkten 5* behandla personuppgifter i syfte att fullgöra förpliktelser som följer av internationella åtaganden. Den tar sikte på förpliktelser i syfte att gagna utländsk brottsbekämpande verksamhet. Sverige har exempelvis åtaganden enligt ett flertal konventioner där åklagare har vissa uppgifter (se prop. 2014/15:63 s. 140 f.). Handläggning av frågor som rör internationell rättslig hjälp i brottmål kan som regel hänföras till *punkterna 2* eller *3* men ligger i övrigt under denna punkt.

I *andra stycket* anges att det ska vara fråga om en arbetsuppgift som framgår av en bindande unionsrättsakt eller av en lag, en förordning eller ett särskilt beslut i vilket regeringen uppdragit åt myndigheten att ansvara för en sådan uppgift. Motsvarande bestämmelse finns i 2 kap. 1 § brottsdatalagen. Vad den innebär utvecklas i SOU 2017:29 s. 238 f.

2 §

I paragrafen, som behandlas i avsnitt 11.3.1, upplyses om att förutsättningarna för att personuppgifter ska få behandlas för nya ändamål regleras i 2 kap. 4 och 22 §§ brottsdatalagen (2018:000). Innan personuppgifter får behandlas för ett nytt ändamål inom eller utanför brottsdatalagens tillämpningsområde krävs det en prövning enligt någon av paragraferna. Vad prövningen innebär utvecklas i SOU 2017:29 s. 249 f. och avsnitt 6.4.3.

Särskilda upplysningar

3 §

I paragrafen, som behandlas i avsnitt 5.3.10, görs det undantag från bestämmelserna om särskilda upplysningar i 2 kap. 3 § andra stycket, 9 och 10 §§ brottsdatalagen (2018:000). Endast personuppgifter som har gjorts gemensamt tillgängliga med stöd av 3 kap. 2 § ska i vissa fall förses med särskilda upplysningar. Det innebär att när personuppgifter behandlas av bara ett fåtal personer behöver särskilda upplysningar inte lämnas. Eftersom åklagare normalt biträds av polisen vid förundersökningar och samma reglering gäller för polisen, framgår de upplysningar som ska lämnas enligt paragrafen normalt av sammanhanget och någon särskilt upplysning behövs i så fall inte heller när det gäller uppgifter som har gjorts gemensamt tillgängliga.

Känsliga personuppgifter

4 §

I paragrafen, som reglerar när det är tillåtet att använda känsliga personuppgifter vid sökning, görs det undantag från det generella sökförbudet i 2 kap. 14 § brottsdatalagen (2018:000). Paragrafen behandlas i avsnitt 11.3.3.

Undantaget gäller vid sökning i alla slags personuppgifter, dvs. både personuppgifter som har gjorts gemensamt tillgängliga och personuppgifter som inte har det. Sökförbudet hindrar inte att brottsrubriceringar eller uppgifter som beskriver en persons utseende får användas vid sökning, även om det skulle leda till ett personurval grundat på känsliga personuppgifter. Med uppgifter som beskriver en persons utseende avses signalementsuppgifter om t.ex. kroppsbyggnad, ansiktsform, hår- och hudfärg, klädsel och fysiska kännetecken som födelsemärken, blindhet och tatueringar (jfr prop. 2011/12:45 s. 124). Sökning på sådana uppgifter kan resultera i personurval grundat på uppgifter om hälsa. Sökning på vissa sexualbrott kan resultera i ett personurval grundat på sexualliv eller sexuell läggning. En sökning på påföljder för vissa typer av brott kan ge ett urval grundat på uppgifter om hälsa.

I vilken utsträckning det är tillåtet att behandla någon eller några av personuppgifterna i en sammanställning av sådana uppgifter som sökningen resulterat i får prövas mot huvudregeln om behandling av känsliga personuppgifter i 2 kap. 11 § brottsdatalagen. Rätten att göra sökning enligt denna paragraf medför således inte en generell rätt att fortsätta att behandla uppgifterna.

Utlämnande av personuppgifter

5 §

Paragrafen innehåller sekretessbrytande bestämmelser om utlämnande av personuppgifter till utländska myndigheter och mellanfolkliga organisationer. Den motsvarar nuvarande 2 kap. 13 §.

Första stycket ändras endast redaktionellt.

Ändringen i *andra stycket* är en följd av att uttrycket brottsbekämpande verksamhet utmönstras ur lagen, vilket behandlas i avsnitt 4.4.1. Sekretessen bryts och personuppgifter får lämnas ut om mottagaren behöver dem för något av de syften som räknas upp i 1 §. Det innebär att möjligheterna till utlämnande vidgas något. När det gäller mottagare i tredjeland ska regleringen i 8 kap. 1 § brottsdatalagen (2018:000) också beaktas.

I tredje stycket görs endast en redaktionell ändring.

6 §

Paragrafen innehåller en bestämmelse som bryter viss sekretess som annars skulle ha gällt gentemot andra brottsbekämpande myndigheter. Den motsvarar nuvarande 2 kap. 14 §.

Det tydliggörs att sekretessen bryts om den mottagande myndigheten behöver uppgifterna för något av de syften som anges i 1 kap. 2 § brottsdatalagen (2018:000). Ändringen är en följd av att uttrycket brottsbekämpande verksamhet utmönstras ur lagen, vilket behandlas i avsnitt 4.4.1.

7 §

Paragrafen reglerar när personuppgifter får lämnas ut elektroniskt.

I *första stycket* föreskrivs att personuppgifter får lämnas ut elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt. Med sådant utlämnande avses bl.a. utlämnande genom e-post eller annan elektronisk överföring eller på ett usb-minne eller annat motsvarande medium. Frågan behandlas i avsnitt 5.6.4.

Det har betydelse vem mottagaren är för frågan om det är olämpligt att lämna ut uppgifter elektroniskt. Som regel kan det inte anses vara olämpligt att lämna ut uppgifter på det sättet till en myndighet (se prop. 2014/15:148 s. 113, jfr SOU 2015:39 s. 447 f.).

När det gäller utlämnande till enskilda krävs en mer nyanserad bedömning. Om det finns en författningsreglerad skyldighet att sända en handling till en viss person får det avgöras om elektroniskt utlämnande är olämpligt med hänsyn till bl.a. innehållet i handlingen, vem som är mottagare, behovet av att kunna visa att personen i fråga har tagit del av handlingen och andra omständigheter. Är det fråga om processmaterial som översänds till parter eller ombud bör även principen om equality of arms beaktas.

Frågan är särskilt svårbedömd när uppgifter ska lämnas ut till enskilda och det på grund av uppgifternas art, struktur, antal eller någon annan särskild omständighet finns anledning att befara att utlämnandet kan leda till integritetsrisker (jfr prop. 2014/15:148 s. 114). Bedömer den utlämnande myndigheten att det finns risk för att personuppgifterna kan komma att missbrukas om de lämnas ut elektroniskt gäller sekretess enligt 21 kap. 7 § offentlighets- och sekretesslagen (2009:400). De får då inte lämnas ut till följd av sekretess.

Det kan också finnas särskild anledning att iaktta försiktighet när det gäller utlämnande av bild- och ljudupptagningar (jfr prop. 2016/17:68 s. 51 f.).

Vid prövningen av om personuppgifter bör lämnas ut elektroniskt bör givetvis även informationssäkerheten vägas in.

Om någon begär att få tillgång till en allmän handling med stöd av tryckfrihetsförordningen får myndigheten inte efterforska syftet med begäran. Det kan ha betydelse för möjligheten att få underlag för att bedöma om det i ett enskilt fall är lämpligt att lämna ut en handling med personuppgifter elektroniskt (se JO dnr 4171-2011).

Elektroniskt utlämnande genom direktåtkomst regleras i *andra stycket*, som motsvarar nuvarande 2 kap. 17 §. Det är tillåtet bara i den utsträckning som anges i lagen.

Föreskrifter

8 §

I paragrafen upplyses om att regeringen kan meddela föreskrifter om utlämnande av personuppgifter. Det gäller föreskrifter om dels att personuppgifter får lämnas ut även i andra fall än som anges i 5 och 6 §§ (vilket motsvarar nuvarande 2 kap. 15 § första stycket), dels begränsning av möjligheten att lämna ut personuppgifter elektroniskt på annat sätt än genom direktåtkomst, vilket behandlas i avsnitt 5.6.4.

3 kap. Gemensamt tillgängliga uppgifter

1 §

Av paragrafen framgår att kapitlet innehåller särskilda bestämmelser för behandling av personuppgifter som görs eller har gjorts gemensamt tillgängliga. Vad som avses med att uppgifter görs gemensamt tillgängliga utvecklas i prop. 2014/15:63 s. 151 f.

I *första stycket* ändras regleringen på grund av att lagen endast omfattar åklagarverksamhet inom brottsdatalagens tillämpningsområde, vilket behandlas i avsnitt 11.2.

Av *andra stycket* framgår att kapitlet inte gäller när personuppgifter behandlas med stöd av den särskilda bestämmelsen i 2 kap. 2 § brottsdatalagen (2018:000) om behandling av personuppgifter för diarieföring eller för att utföra andra nödvändiga handläggningsuppgifter.

2 §

I paragrafen anges vilka personuppgifter som får göras gemensamt tillgängliga. Regleringen anpassas till att lagen har ett något annorlunda utformat tillämpningsområde än tidigare.

3 §

Paragrafen, som behandlas i avsnitt 11.4, innehåller en allmän begränsning av vilka uppgifter som får tas fram vid sökning i gemensamt tillgängliga uppgifter på namn, personnummer, samordningsnummer och liknande identitetsbeteckningar.

Genom ett tillägg tydliggörs det att paragrafen endast gäller vid sökning i automatiserade behandlingssystem. Vad som avses med automatiserade behandlingssystem anges i SOU 2017:29 s. 306 f.

Punkten 1, som är ny och behandlas i avsnitt 11.4, innebär att uppgifter om att någon är anmäld för brott får tas fram vid sökning. *Punkterna 2–9* ändras endast redaktionellt.

4 §

I paragrafen görs undantag från begränsningarna i 3 §. Den ändras enbart redaktionellt.

5 §

Paragrafen innehåller en uppräknning av vilka myndigheter som får medges direktåtkomst till uppgifter som har gjorts gemensamt tillgängliga och för vilka syften. Ändringen är en följd av att uttrycket brottsbekämpande verksamhet utmönstras ur lagen, vilket behandlas i avsnitt 4.4.1. Den ändras också redaktionellt.

6 §

I paragrafen upplyses om att regeringen kan meddela föreskrifter om ytterligare undantag från bestämmelserna om sökning i 3 §.

7 §

I paragrafen, där kapitlets övriga bestämmelser om föreskrifter samlas, upplyses om att regeringen, eller den myndighet som regeringen bestämmer, kan meddela föreskrifter om gemensamt tillgängliga uppgifter (vilket motsvarar nuvarande 3 kap. 2 § andra

stycket) och omfattningen av direktåtkomsten och om behörighet och säkerhet vid sådan åtkomst (vilket motsvarar nuvarande 3 kap. 8 § tredje stycket).

4 kap. Längsta tid som personuppgifter får behandlas

Allmän bestämmelse

1 §

De bestämmelser som anger hur länge personuppgifter får behandlas samlas i detta kapitel. Frågan behandlas i avsnitt 5.5.1.

I *första stycket* föreskrivs att bestämmelserna i kapitlet endast gäller personuppgifter som behandlas automatiserat.

Andra stycket upplyser om att den grundläggande bestämmelsen om att personuppgifter inte får behandlas längre än vad som är nödvändigt med hänsyn till ändamålet med behandlingen finns i 2 kap. 17 § första stycket brottsdatalagen (2018:000). I övriga paragrafer i kapitlet anges hur länge vissa typer av personuppgifter får behandlas inom den ram som sätts av denna huvudregel. Oavsett vilken bedömning som görs av nyttan med behandlingen av en viss personuppgift får den dock inte behandlas längre än vad som anges i respektive paragraf.

Personuppgifter i ärenden

2 §

Paragrafen, som motsvarar nuvarande 2 kap. 10 § andra stycket och behandlas i avsnitt 5.5.3, reglerar hur länge personuppgifter i ett ärende får behandlas. Någon ändring av hur länge sådana personuppgifter får behandlas görs inte. Terminologin anpassas till den som används i lagen i övrigt. Vidare görs redaktionella ändringar.

Enligt paragrafen inskränks enbart behandlingen av personuppgifter för de ändamål som regleras i lagen, vilket innebär att uppgifterna får fortsätta att behandlas automatiserat för bl.a. arkivändamål efter de tidpunkter som anges i paragrafen.

3 §

Paragrafen, som motsvarar nuvarande 3 kap. 7 §, reglerar vad som gäller i fråga om personuppgifter när förundersökning inte har inletts eller har lagts ner eller där åtal har lagts ner eller frikännande dom har meddelats och fått laga kraft. Terminologin anpassas till den som används i lagen i övrigt. Vidare görs redaktionella ändringar.

Enligt paragrafen inskränks enbart behandlingen av personuppgifter för de ändamål som regleras i lagen, vilket innebär att uppgifterna får fortsätta att behandlas automatiserat för bl.a. arkivändamål efter de tidpunkter som anges i paragrafen. Frågan behandlas i avsnitt 5.5.3.

Övriga personuppgifter

4 §

Paragrafen, som motsvarar nuvarande 2 kap. 10 § tredje stycket och behandlas i avsnitt 5.5.2, reglerar hur länge personuppgifter som inte kan hänföras till ett ärende får behandlas. Någon ändring av hur länge personuppgifter får behandlas görs inte. Terminologin anpassas till den som används i lagen i övrigt och vissa redaktionella ändringar görs.

Det klargör att uppgifterna, trots det som sägs i 2 kap. 17 § andra stycket brottsdatalogen (2018:000) om att arkivlagstiftningen har företräde, inte får arkiveras digitalt. Utgångspunkten är alltså att all automatiserad behandling av personuppgifterna ska upphöra när den tid som anges i paragrafen har löpt ut, vilket innebär att uppgifterna ska tas bort. Endast om det har meddelats uttryckliga föreskrifter som innebär att uppgifterna får behandlas för arkivändamål av allmänt intresse eller för vetenskapliga, statistiska eller historiska ändamål får de behandlas automatiserat längre än vad som anges i denna paragraf (jfr 5 §).

Föreskrifter

5 §

I paragrafen, som motsvarar nuvarande 2 kap. 11 §, upplyses om att regeringen, eller den myndighet som regeringen bestämmer, kan meddela föreskrifter om att uppgifter i vissa ärendetyper eller vissa kategorier av personuppgifter får fortsätta att behandlas för ändamål inom lagens tillämpningsområde under längre tid än vad som anges i 2 §, om att personuppgifter som inte kan hänföras till ett ärende, trots att den tillåtna tiden för behandling har löpt ut, får fortsätta att behandlas för arkivändamål av allmänt intresse och vetenskapliga, statistiska eller historiska ändamål och om begränsning av behandlingen av personuppgifter för ändamål inom lagens tillämpningsområde vid digital arkivering. Frågorna behandlas i avsnitt 5.5.2 och 5.5.3.

5 kap. Administrativa sanktionsavgifter och rättsmedel

Administrativa sanktionsavgifter

1 §

Paragrafen, som är ny, reglerar vid vilka överträdelser sanktionsavgift får tas ut. Frågan behandlas i avsnitt 5.4.2.

I *första stycket* anges vid vilka överträdelser sanktionsavgift får tas ut av den personuppgiftsansvarige. Tillsynsmyndigheten avgör i det enskilda fallet om det är påkallat att ta ut sanktionsavgift, vilket framgår av formuleringen att avgift får tas ut. Uppräkningen av vilka överträdelser som kan föranleda sanktionsavgift är uttömmande. Sanktionsavgift kan tas ut för överträdelse av bestämmelserna om tillåtna rättsliga grunder och längsta tid som personuppgifter får behandlas. Brottsdatalagens förfaranderegler när det gäller sanktionsavgift tillämpas även vid överträdelser enligt denna lag. I brottsdatalagen med tillhörande förordning regleras också handläggningen av frågor om sanktionsavgift.

I *andra stycket* anges storleken på de sanktionsavgifter som kan komma i fråga. De överträdelser som enligt lagen kan föranleda sanktionsavgift är alla av allvarligt slag. Lägsta sanktionsavgift är därför 50 000 kronor.

Skadestånd

2 §

I paragrafen regleras den registrerades rätt till skadestånd för behandling av personuppgifter i strid med regelverket. Paragrafen behandlas i avsnitt 5.4.3.

Paragrafen hänvisar till 7 kap. 1 § brottsdatalagen (2018:000), som ska tillämpas på motsvarande sätt när det har förekommit felaktig behandling av personuppgifter enligt förevarande lag eller föreskrifter som har meddelats i anslutning till den. Det innebär att den personuppgiftsansvarige ska ersätta den registrerade för den skada och kränkning av den personliga integriteten som behandlingen av personuppgifter har orsakat. Med skada avses personskada, sakskada eller ren förmögensskada. Med kränkning avses ideell skada som består i att den enskildes integritet kränkts genom behandlingen. Någon möjlighet till jämkning av skadeståndet finns inte.

Överklagande

3 §

I paragrafen, som behandlas i avsnitt 5.4.4, upplyses om att det i 7 kap. brottsdatalagen (2018:000) finns bestämmelser om överklagande och om vilka beslut som får överklagas.

Övergångsbestämmelser

Ikraftträdande- och övergångsbestämmelserna tas upp i avsnitt 18.1 och 18.2.

Punkten 1 föreskriver när lagen ska träda i kraft.

Sanktionsavgift får enligt *punkten 2* beslutas endast för överträdelser som har begåtts efter ikraftträdandet.

Punkten 3 innebär att bestämmelsen om skadestånd i 48 § personuppgiftslagen fortfarande ska gälla för skada som har orsakats före ikraftträdandet vid behandling av personuppgifter enligt lagen eller föreskrifter som har meddelats i anslutning till den.

20.18 Förslaget till lag om ändring i utlänningsdatalagen (2016:27)

14 §

Paragrafen reglerar Migrationsverkets rätt att föra register över fingeravtryck och för vilka ändamål registret får användas. En hänvisning i *andra stycket* till en lag som byter namn ändras, vilket behandlas i avsnitt 7.1.2. Stycket ändras också redaktionellt.

Första och tredje styckena är oförändrade.

20.19 Förslaget till lag om ändring i tullagen (2016:253)

4 kap.

8 §

I paragrafen, som behandlas i avsnitt 8.4.2, regleras på vilket sätt Tullverket får ta del av uppgifter som lämnas av transportföretag med stöd av 6 §.

Första stycket är oförändrat.

I *andra stycket* regleras numera endast i vilken omfattning Tullverket får ta del av uppgifter genom terminalåtkomst. Myndighetens behandling av sådana personuppgifter regleras i Tullverkets brottsdatalag (2017:447).

20.20 Förslaget till lag om ändring i tullbrottsdatalagen (2017:447)

Lagen anpassas till bestämmelserna i brottsdatalagen, vilket leder till omarbetning av den och att två kapitel upphävs och ersätts med nya. Vissa paragrafer upphävs, samtidigt som nya paragrafer tillkommer. Bestämmelserna om föreskrifter samlas i slutet av varje kapitel. Dessa förändringar föranleder omnumreringar av vissa paragrafer.

Vidare flyttas bestämmelserna om Tullverkets behandling av personuppgifter som transportföretag tillhandahåller myndigheten enligt bestämmelser i lagen (1996:701) om Tullverkets befogen-

heter vid Sveriges gräns mot ett annat land inom Europeiska unionen och tullagen (2016:253) till den nu aktuella lagen.

Som en anpassning till brottsdatalagen införs ett nytt kapitel om administrativa sanktionsavgifter och rättsmedel.

De generella ändringarna i lagen behandlas i kapitel 4, 5 och 6 och övriga ändringar i kapitel 8.

Lagen får också ett nytt namn, Tullverkets brottsdatalag.

1 kap. Allmänna bestämmelser

Lagens tillämpningsområde

1 §

I paragrafen, som behandlas i avsnitt 8.2, anges lagens tillämpningsområde.

Lagen gäller utöver brottsdatalagen när Tullverket i egenskap av behörig myndighet enligt den lagen behandlar personuppgifter för vissa syften. Behörig myndighet, personuppgift och behandling av personuppgifter definieras i 1 kap. 6 § brottsdatalagen (2018:000).

Att lagen gäller utöver brottsdatalagen innebär bl.a. att lagen enligt 1 kap. 3 § brottsdatalagen bara gäller för sådan behandling av personuppgifter som är helt eller delvis automatiserad och för annan behandling av personuppgifter som ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

I brottsdatalagen finns alla de grundläggande bestämmelserna om hur personuppgifter får behandlas. Den nu aktuella lagen innehåller bestämmelser som innebär preciseringar, undantag eller avvikelser från bestämmelser i brottsdatalagen. Det innebär att bestämmelserna i lagen ska läsas tillsammans med regleringen i brottsdatalagen och tolkas i ljuset av den regleringen.

Lagen gäller när Tullverket behandlar personuppgifter om syftet med behandlingen är att bekämpa eller lagföra brott. Vad det innebär utvecklas i kommentaren till 2 kap. 1 §.

2 §

Paragrafen, som motsvarar nuvarande 1 kap. 3 § första och tredje styckena, anger hur regleringen i lagen förhåller sig till regleringen i lagen (2017:496) om internationellt polisiärt samarbete. Frågan behandlas i avsnitt 17.3.

Personuppgiftsansvar

3 §

I paragrafen, som motsvarar nuvarande 2 kap. 3 §, regleras personuppgiftsansvaret. Personuppgiftsansvarig definieras i 1 kap. 6 § brottsdatalagen (2018:000). Personuppgiftsansvarigas skyldigheter regleras i 3 kap. brottsdatalagen.

Lagens tillämpning på uppgifter om juridiska personer

4 §

I paragrafen, som motsvarar nuvarande 1 kap. 4 §, anges vilka bestämmelser i lagen och i brottsdatalagen som gäller för behandling av uppgifter om juridiska personer. Frågan behandlas i avsnitt 5.4.1.

Uppräkningen i paragrafen av bestämmelser som ska gälla vid behandling av uppgifter om juridiska personer motsvarar nuvarande reglering.

2 kap. Grundläggande bestämmelser om behandling

Tillåtna rättsliga grunder för behandling av personuppgifter

1 §

Paragrafen reglerar de tillåtna rättsliga grunderna för behandling av personuppgifter. Den behandlas i avsnitt 6.1, 6.3 och 8.3.1.

Paragrafen, som är anpassad till hur de rättsliga grunderna för behandling av personuppgifter är utformade i 2 kap. 1 § brottsdatalagen (2018:000), ersätter den bestämmelsen. Regleringen i 2 kap. 2 § brottsdatalagen ger myndigheten rättsligt stöd för att i vissa fall

behandla personuppgifter enbart för diarieföring och nödvändig handläggning, trots brist på stöd i denna paragraf.

Personuppgifter får enligt *första stycket* behandlas om det är nödvändigt för att utföra en arbetsuppgift i vissa särskilt angivna syften inom lagens tillämpningsområde. Bestämmelsen bildar den yttre ramen för när behandling av personuppgifter är tillåten.

Enligt *punkten 1* får personuppgifter behandlas i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet. Det är framför allt Tullverkets underrättelseverksamhet som regleras i punkten. Med det avses arbete med insamling, bearbetning och analys av information i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet när det ännu inte finns konkreta misstankar om att något konkret brott har begåtts (se prop. 2016/17:91 s. 198 f.). Personuppgiftsbehandling i Tullverkets brottsförebyggande arbete som rör införsel av varor, liksom kartläggning och spaning som inte är hänförlig till en förundersökning men utförs i syfte att upptäcka brottslig verksamhet, omfattas också.

Behandling av uppgifter om vilka personer som kommer med en viss transport, t.ex. en viss färja, går i stor utsträckning ut på att förebygga, förhindra och upptäcka smuggling av framför allt narkotika genom att studera resmönster, betalningssätt, vilka som reser i sällskap och liknande. När uppslag om kontrollobjekt som är intressanta ur brottsbekämpningssynpunkt vidarebefordras till myndighetens kontrollverksamhet görs det i syfte att förhindra och upptäcka brottslig verksamhet. Viss personuppgiftsbehandling som är nödvändig för att planera kontroller, välja ut kontrollobjekt och utföra begärda kontroller i Tullverkets brottsbekämpande verksamhet ryms därför under punkten. Om personuppgiftsbehandling i samband med kontroller omfattas av lagen avgörs av om kontrollen görs i syfte att upptäcka, förebygga eller förhindra brottslig verksamhet eller inte.

Enligt *punkten 2* får personuppgifter behandlas i syfte att utreda eller lagföra brott. Att utreda brott innebär framför allt att genomföra förundersökning enligt 23 kap. rättegångsbalken. Med brott avses konkreta brott, men det kan vara fråga om både brott som bevisligen har begåtts och brott som det enbart finns misstankar om. Misstankarna behöver inte vara riktade mot någon bestämd person. Även personuppgiftsbehandling inom ramen för den form av förenklat utredningsförfarande som regleras i 23 kap. 22 § rätte-

gångsbalken och vid åtgärder som vidtas med stöd av 23 kap. 3 och 8 §§ rättegångsbalken omfattas.

Med lagföra brott avses framför allt att utfärda strafförelägganden och förelägganden av ordningsbot. Tullverkets åklagare får även väcka åtal och föra talan vid domstol i vissa typer av mål. Den personuppgiftsbehandling som är nödvändig för dessa åklagaruppgifter har stöd i denna punkt.

Personuppgifter får enligt *punkten 3* också behandlas i syfte att fullgöra förpliktelser som följer av internationella åtaganden. Punkten tar sikte på förpliktelser som syftar till att gagna utländsk brottsbekämpande verksamhet (se prop. 2016/17:91 s. 199).

I *andra stycket* anges att det ska vara fråga om en arbetsuppgift som framgår av en bindande unionsrättsakt eller av en lag, en förordning eller ett särskilt beslut i vilket regeringen uppdragit åt myndigheten att ansvara för en sådan uppgift. Motsvarande bestämmelse finns i 2 kap. 1 § brottsdatalagen. Vad den innebär utvecklas i SOU 2017:29 s. 238.

2 §

I paragrafen, som behandlas i avsnitt 8.3.1, upplyses om att förutsättningarna för att personuppgifter ska få behandlas för nya ändamål regleras i 2 kap. 4 och 22 §§ brottsdatalagen (2018:000). Innan personuppgifter får behandlas för ett nytt ändamål inom eller utanför brottsdatalagens tillämpningsområde krävs det en prövning enligt någon av paragraferna. Vad prövningen innebär utvecklas i SOU 2017:29 s. 249 f. och avsnitt 6.4.3.

Särskilda upplysningar

3 §

I paragrafen, som behandlas i avsnitt 5.3.10, görs det undantag från bestämmelserna om särskilda upplysningar i 2 kap. 3 § andra stycket, 9 och 10 §§ brottsdatalagen (2018:000). Det är endast personuppgifter som har gjorts gemensamt tillgängliga med stöd av 3 kap. 2 § som i vissa fall ska förses med särskilda upplysningar.

Det innebär att när personuppgifter behandlas bara av ett fåtal personer behöver särskilda upplysningar inte lämnas.

Känsliga personuppgifter

4 §

I paragrafen, som behandlas i avsnitt 8.3.2, regleras när Tullverket får behandla biometriska uppgifter. Biometriska uppgifter definieras i 1 kap. 6 § brottsdatalagen (2018:000).

Bestämmelsen möjliggör användning av särskild teknisk behandling för att bekräfta unik identifiering av en person. Regleringen innebär att t.ex. fingeravtryck, ansiktsgeometri, röstigenkänning eller rörelsemönster kan användas för att identifiera en person.

Biometriska uppgifter får behandlas enligt de förutsättningar som anges i 2 kap. 12 § brottsdatalagen. Behandlingen ska vara absolut nödvändig för ändamålet med behandlingen. Det innebär att behovet av att behandla biometriska uppgifter måste prövas noga i det enskilda fallet.

5 §

I paragrafen, som tillsammans med 6 § reglerar när det är tillåtet att använda känsliga personuppgifter vid sökning, görs undantag från det generella sökförbudet i 2 kap. 14 § brottsdatalagen (2018:000). Paragrafen behandlas i avsnitt 8.3.3.

Undantaget gäller vid sökning i alla slags personuppgifter, dvs. såväl personuppgifter som har gjorts gemensamt tillgängliga som personuppgifter som inte har det.

Sökförbudet hindrar inte att brottsrubriceringar, uppgifter om tillvägagångssätt vid brott eller uppgifter som beskriver en persons utseende används vid sökning, även om det skulle leda till ett personurval grundat på känsliga personuppgifter.

Med uppgifter som beskriver en persons utseende avses signalementsuppgifter som t.ex. kroppsbyggnad, ansiktsform, hår- och hudfärg, klädsel och fysiska kännetecken som födelsemärken, blindhet och tatueringar (jfr prop. 2011/12:45 s. 124). En sökning på ett fysiskt särdrag kan ge ett personurval grundat på uppgifter

som rör hälsa. Med uppgifter om tillvägagångssätt vid brott avses t.ex. uppgifter om smugglingsmetoder eller särskilda föremål som kan användas som brottsverktyg. Vid exempelvis kontroll av förbud mot införsel och utförsel av barnpornografi kan sökning på brottsrubricering och särskilda föremål avslöja en persons sexualliv eller sexuella läggning.

Sökning på tillvägagångssätt vid brott kan t.ex. resultera i ett personurval grundat på hälsa. Det gäller exempelvis sökning på s.k. sväljare. Sökning på uppgifter om en persons utseende kan avse exempelvis fysiska skador eller särdrag som kan avslöja uppgifter om hälsa eller uppgifter om tatueringar som kan avslöja viss politisk åsikt eller religiös övertygelse.

I vilken utsträckning det är tillåtet att behandla någon eller några av personuppgifterna i en sammanställning av sådana uppgifter som sökningen resulterat i får prövas mot huvudregeln om behandling av känsliga personuppgifter i 2 kap. 11 § brottsdatalagen. Rätten enligt denna paragraf att göra sökning medför således inte en generell rätt att fortsätta att behandla uppgifterna.

6 §

I paragrafen, som tillsammans med 5 § reglerar när det är tillåtet att använda känsliga personuppgifter vid sökning, görs undantag från sökförbudet i 2 kap. 14 § brottsdatalagen (2018:000). Paragrafen behandlas i avsnitt 8.3.3.

Undantaget gäller enbart vid sökning i personuppgifter som inte har gjorts gemensamt tillgängliga, dvs. personuppgifter som enbart ett fåtal har tillgång till. Sökning i sådana uppgifter får göras i syfte att få fram ett personurval grundat på etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller uppgifter som rör hälsa, sexualliv eller sexuell läggning. Sådana sökningar kan aktualiseras bl.a. om det är känt att en viss narkotikasort används av en grupp med visst etniskt ursprung eller religiös övertygelse. Drogen kat som endast odlas utomlands är ett exempel på det. Tullverket kan även behöva göra sökningar i syfte att få fram uppgifter om ideologiskt motiverade grupperingar som är kända för att finansiera sin verksamhet genom smuggling av narkotika eller andra otillåtna föremål. Tullverket kan även ha skäl att söka på ordet pedofil eller

vissa typer av föremål i syfte att förebygga, förhindra eller upptäcka smuggling av barnpornografi.

Rätten att söka på känsliga personuppgifter gäller dock inte sökning på ras eller medlemskap i fackförening eller sökning i genetiska eller biometriska uppgifter. Sökning som syftar till att få fram ett personurval grundat på sådana uppgifter är alltså inte tillåten.

I vilken utsträckning det är tillåtet att behandla någon eller några av personuppgifterna i en sammanställning av sådana uppgifter som sökningen resulterat i får prövas mot huvudregeln om behandling av känsliga personuppgifter i 2 kap. 11 § brottsdatalagen. Rätten att göra sökning enligt denna paragraf medför således inte en generell rätt att fortsätta att behandla uppgifterna.

Utlämnande av personuppgifter

7 §

Paragrafen innehåller sekretessbrytande bestämmelser om utlämnande till utländska myndigheter och mellanfolkliga organisationer. Den motsvarar nuvarande 2 kap. 12 §.

I första stycket görs endast en redaktionell ändring.

Av andra stycket framgår att personuppgifter får lämnas ut bara om mottagaren behöver dem för något av de syften som räknas upp i 1 §. När det gäller mottagare i tredjeland ska regleringen i 8 kap. 1 § brottsdatalagen (2018:000) också beaktas.

Tredje stycket ändras endast redaktionellt.

8 §

Paragrafen innehåller en bestämmelse som bryter viss sekretess som annars skulle ha gällt gentemot andra brottsbekämpande myndigheter. Den motsvarar nuvarande 2 kap. 13 §.

I paragrafen tydliggörs att sekretessen bryts om den mottagande myndigheten behöver uppgifterna för något av de syften som anges i 1 kap. 2 § brottsdatalagen (2018:000). Ändringen är en följd av att uttrycket brottsbekämpande verksamhet utmönstras ur lagen, vilket behandlas i avsnitt 4.4.1.

9 §

Paragrafen reglerar när personuppgifter får lämnas ut elektroniskt.

I *första stycket* föreskrivs att personuppgifter får lämnas ut elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt. Med sådant utlämnande avses bl.a. utlämnande genom e-post eller annan elektronisk överföring eller på ett usb-minne eller annat motsvarande medium. Frågan behandlas i avsnitt 5.6.4.

Det har betydelse vem mottagaren är för frågan om det är olämpligt att lämna ut uppgifter elektroniskt. Som regel kan det inte anses vara olämpligt att lämna ut uppgifter på det sättet till en myndighet (se prop. 2014/15:148 s. 113, jfr SOU 2015:39 s. 447 f.).

När det gäller utlämnande till enskilda krävs en mer nyanserad bedömning. Om det finns en författningsreglerad skyldighet att sända en handling till en viss person får det avgöras om elektroniskt utlämnande är olämpligt med hänsyn till bl.a. innehållet i handlingen, vem som är mottagare, behovet av att kunna visa att personen i fråga har tagit del av handlingen och andra omständigheter. Är det fråga om processmaterial som översänds till parter eller ombud bör även principen om equality of arms beaktas.

Frågan är särskilt svårbedömd när uppgifter ska lämnas ut till enskilda och det på grund av uppgifternas art, struktur, antal eller någon annan särskild omständighet finns anledning att befara att utlämnandet kan leda till integritetsrisker (jfr prop. 2014/15:148 s. 114). Bedömer myndigheten att det finns risk för att personuppgifterna kan komma att missbrukas om de lämnas ut elektroniskt gäller sekretess enligt 21 kap. 7 § offentlighets- och sekretesslagen (2009:400). De får då inte lämnas ut till följd av sekretess.

Det kan också finnas särskild anledning att iaktta försiktighet när det gäller utlämnande av bild- och ljudupptagningar (jfr prop. 2016/17:68 s. 51 f.).

Vid prövningen av om personuppgifter bör lämnas ut elektroniskt bör givetvis även informationssäkerheten vägas in.

Om någon begär att få tillgång till en allmän handling med stöd av tryckfrihetsförordningen får den utlämnande myndigheten inte efterforska syftet med begäran. Det kan ha betydelse för möjligheten att få underlag för att bedöma om det i ett enskilt fall är lämpligt att lämna ut en handling med personuppgifter elektroniskt (se JO dnr 4171-2011).

Elektroniskt utlämnande genom direktåtkomst regleras i *andra stycket*, som motsvarar nuvarande 2 kap. 17 §. Det är tillåtet bara i den utsträckning som anges i lagen.

Personuppgifter från transportföretag

10 §

Paragrafen, som motsvarar nuvarande 2 kap. 8 § första stycket och behandlas i avsnitt 8.4.1 och 8.4.2, reglerar hur personuppgifter som transportföretag tillhandahåller Tullverket får behandlas. Det är fråga om uppgifter om ankommande eller avgående transporter av varor, passagerare eller fordon som företagen befordrar till och från Sverige. Det rör sig om bokningsuppgifter i framför allt flyg- och färjetrafik. Transportföretagens skyldighet att tillhandahålla uppgifter regleras alltså i lagen (1996:701) om Tullverkets befogenheter vid Sveriges gräns mot ett annat land inom Europeiska unionen och tullagen (2016:253).

Personuppgifter från transportföretag får enligt *första stycket* behandlas för att planera kontroller och välja ut kontrollobjekt i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet. Det innebär att arbetet inriktas på att få fram kontrollobjekt för vilka det råder förhöjd risk för smuggling eller andra brott. Sådana uppgifter får också behandlas i syfte att utreda eller lagföra brott. Möjligheten att söka i sådana personuppgifter med hjälp av personnummer och andra identitetsbeteckningar regleras i 12 §.

Om det vid den behandling som görs, eller vid kontroll vid ankomsten till Sverige, uppkommer skäl att behandla personuppgifterna för ett nytt ändamål inom lagens tillämpningsområde får det enligt *andra stycket* bara göras om förutsättningarna för behandling för nya ändamål i 2 kap. 4 § brottsdatalagen (2018:000) är uppfyllda i det enskilda fallet. Ett typiskt exempel är att ett brott upptäcks när någon har tagits ut för kontroll och att uppgifterna behövs för att utreda och lagföra brottet. Det kan också visa sig att vissa av uppgifterna behövs i ett underrättelseärende, t.ex. för kartläggning av nya smugglingsmetoder. Det kan inte uteslutas att personuppgifterna behöver behandlas för ett nytt ändamål utanför lagens tillämpningsområde, t.ex. för att lämnas ut enligt tryckfrihetsförord-

ningen. Hänvisning görs därför även till provningen i 2 kap. 22 § brottsdatalagen.

Av 3 kap. 2 § andra stycket framgår i vilken utsträckning personuppgifter som transportföretag tillhandahåller får göras gemensamt tillgängliga.

11 §

I paragrafen anges hur personuppgifter som Tullverket får del av genom terminalåtkomst får behandlas. Bestämmelsen motsvarar nuvarande 16 § andra stycket lagen (1996:701) om Tullverkets befogenheter vid Sveriges gräns mot ett annat land inom Europeiska unionen och 4 kap. 8 § andra stycket tullagen (2016:253). Paragrafen behandlas i avsnitt 8.4.2.

Paragrafen reglerar enbart behandling vid terminalåtkomst till personuppgifter hos transportföretag, medan 10 och 12 §§ anger vad som gäller i fråga om personuppgifter som förs över till myndighetens it-system eller behandlas strukturerat på annat sätt.

Genom terminalåtkomsten till företagens it-system får Tullverket tillgång till omfattande överskottsinformation om resande. Myndigheten får inte ändra eller på annat sätt bearbeta uppgifter i sådana system. Syftet med regleringen är att myndigheten inte heller ska kunna föra över en hel sådan uppgiftssamling till sina egna it-system för att bearbeta, ändra och lagra personuppgifterna där. Som framgår av 10 § får däremot uppgifter föras över i enskilda fall om förutsättningarna för det är uppfyllda.

12 §

I paragrafen, som motsvarar nuvarande 2 kap. 9 § första stycket och behandlas i avsnitt 8.4.2, regleras i vilken utsträckning direkta personuppgifter får användas vid sökning i uppgifter som transportföretag tillhandahåller. Paragrafen ändras endast redaktionellt.

Föreskrifter

13 §

Paragrafen upplyser om att regeringen kan meddela föreskrifter om att personuppgifter får lämnas ut i andra fall än som anges i 7 och 8 §§ (vilket motsvarar nuvarande 2 kap. 14 § första stycket) och om att begränsa möjligheten att lämna ut uppgifter elektroniskt på annat sätt än genom direktåtkomst, vilket behandlas i avsnitt 5.6.4.

3 kap.

1 §

Av paragrafen framgår att kapitlet innehåller bestämmelser om behandling av personuppgifter som görs eller har gjorts gemensamt tillgängliga. Vad som avses med att uppgifter görs gemensamt tillgängliga utvecklas i prop. 2016/17:91 s. 208 f.

I *första stycket* anpassas regleringen till att uttrycket brottsbekämpande verksamhet utmönstras ur lagen, vilket behandlas i avsnitt 4.4.1. Av *andra stycket* framgår att kapitlet inte gäller när personuppgifter behandlas med stöd av den särskilda bestämmelsen i 2 kap. 2 § brottsdatalagen (2018:000) om behandling av personuppgifter för diarieföring eller för att utföra andra nödvändiga handläggningsuppgifter.

2 §

I paragrafen anges vilka personuppgifter som får göras gemensamt tillgängliga.

I *första stycket* anpassas terminologin till den som används i lagen i övrigt och görs redaktionella ändringar.

Av *andra stycket*, som är nytt och motsvarar nuvarande 2 kap. 8 § andra stycket, framgår att personuppgifter från transportföretag endast får göras gemensamt tillgängliga om det behövs i ett enskilt fall. Ändringen behandlas i avsnitt 8.5.2. Regleringen gör det möjligt för Tullverket att göra personuppgifter om utvalda kontrollobjekt gemensamt tillgängliga t.ex. för att kontrollverksamheten ska få kännedom om att det för vissa resande eller varusändningar

kan finnas en förhöjd risk för smuggling. Uppgifterna kan också göras gemensamt tillgängliga i underrättelseverksamheten eller för att utreda eller lagföra brott.

Tredje stycket motsvarar nuvarande andra stycket och är oförändrat.

3 §

I paragrafen, som behandlas i avsnitt 5.3.10, föreskrivs att det ska framgå om personuppgifter har gjorts gemensamt tillgängliga med stöd av 2 § första stycket 2. Att det ska framgå för vilket närmare ändamål personuppgifterna behandlas följer av 2 kap. 3 § brottsdatalagen (2018:000). Paragrafen ändras också redaktionellt.

4 §

I paragrafen, som behandlas i avsnitt 5.3.10, ställs det krav på att uppgifter som är gemensamt tillgängliga i underrättelseverksamhet i vissa fall ska förses med särskilda upplysningar.

Enligt *första stycket* ska det framgå av uppgifter i underrättelseverksamhet att en person inte är misstänkt för att utöva brottslig verksamhet. Det ska alltså gå att skilja mellan personer som är föremål för myndighetens intresse på grund av inblandning i brottslig verksamhet och personer som inte är misstänkta för det. Att det ska framgå om en person är misstänkt för brott eller är ett brottsoffer regleras i 2 kap. 9 § brottsdatalagen (2018:000).

Enligt *andra stycket* ska uppgifter om personer som kan antas ha samband med misstänkt brottslig verksamhet eller som övervakas på visst sätt förses med upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak. Det tydliggörs att kravet på särskild upplysning bara gäller uppgifter om en person som kan antas ha direkt samband med misstänkt brottslig verksamhet. Kravet på samband är lågt ställt. Så snart det finns något som stöder ett antagande om att en person har ett direkt samband med brottslig verksamhet och det är fråga om uppgifter som görs gemensamt tillgängliga ska det framgå på vilket sätt personen har anknytning till den brottsliga verksamheten. Sambandet kan t.ex. bestå i att en person ofta träffar eller har annan kontakt med andra personer som

är misstänkta för att utöva brottslig verksamhet eller ofta rör sig i miljöer där brottslighet förekommer, utan att ha naturliga skäl att befinna sig där. Uppgifter om den som är anhörig till en person som kan antas ha samband med misstänkt brottslig verksamhet faller alltså utanför, utom i de fall där båda kan antas ha direkt samband med brottslig verksamhet.

Det är bara uppgifter som rör en person som är misstänkt för att utöva eller komma att utöva brottslig verksamhet som behöver förse med upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak. De uppgifter som är av intresse är, förutom uppgifter om på vilket sätt personen är knuten till den brottsliga verksamheten, framför allt uppgifter som belyser brottslighetens art och omfattning. Uppgifter av det slaget kan behöva förse med särskilda upplysningar för att personens anknytning till brottsligheten ska kunna bedömas.

Utrymmet för att underlåta att förse uppgifter med upplysning om trovärdighet och riktighet vidgas något genom att det inte längre krävs särskilda omständigheter för att upplysningskravet inte ska gälla. Det är tillräckligt att det på grund av de samlade omständigheterna är onödigt att förse uppgifterna med en upplysning.

5 §

Paragrafen, som behandlas i avsnitt 8.5.1, innehåller en allmän begränsning av vilka uppgifter som får tas fram vid sökning i gemensamt tillgängliga uppgifter på namn, personnummer eller liknande identitetsbeteckningar.

Genom ett tillägg tydliggörs att bestämmelsen endast gäller vid sökning i automatiserade behandlingssystem. Vad som avses med automatiserade behandlingssystem anges i SOU 2017:29 s. 306 f.

6 §

Paragrafen, som behandlas i avsnitt 8.5.1, innehåller undantag från begränsningarna i 5 §.

Enligt *första stycket* gäller inga begränsningar vid sökning i en viss handling eller ett visst ärende.

Enligt *andra stycket* gäller begränsningarna i 5 § inte vid vissa sökningar som utförs av särskilt angivna tjänstemän. Det gäller enligt *punkten 1*, som är ny, när de utför beredningsuppgifter i underrättelseverksamhet och arbetet befinner sig i ett inledande skede. Syftet med bestämmelsen är att tjänstemännen inledningsvis ska ha större möjligheter att göra sökningar för att kunna finna samband med befintliga underrättelseuppgifter. Det kan t.ex. vara fråga om tips från allmänheten om smuggling. Det är bara under en begränsad tid efter det att uppgifterna kom in som punkten är tillämplig. Så snart beredningsarbetet har avslutats upphör möjligheten att göra sökningar med stöd av den nu aktuella punkten.

I *punkten 2*, som motsvarar nuvarande 3 kap. 7 § första stycket 2 och andra stycket 1, undantas sökning som utförs i syfte att bearbeta och analysera personuppgifter som har gjorts gemensamt tillgängliga i underrättelseverksamhet eller för övervakningen av en allvarligt kriminellt belastad person, om endast vissa tjänstemän har tillgång till uppgifterna.

Punkten 3, som motsvarar nuvarande 3 kap. 7 § andra stycket 2, ändras endast redaktionellt.

Enligt *punkten 4*, som är ny, gäller inte begränsningarna i 5 § vid sökningar i syfte att samordna utredningar av brott som kan vara systematiska och för vilka det är föreskrivet fängelse i två år eller däröver.

Undantaget i *tredje stycket* är nytt och innebär att begränsningarna i 5 § inte gäller när en tjänsteman vid någon av Tullverkets ledningscentraler utför sökningar på begäran av en tulltjänsteman som verkställer ett ingripande eller vidtar en åtgärd som rör en enskild.

7 §

I paragrafen anges vilka myndigheter som får medges direktåtkomst till uppgifter som har gjorts gemensamt tillgängliga och för vilka syften. Ändringen är en följd av att uttrycket brottsbekämpande verksamhet utmönstras ur lagen, vilket behandlas i avsnitt 4.4.1. Paragrafen ändras också redaktionellt.

8 §

I paragrafen upplyses om att regeringen kan meddela föreskrifter om ytterligare undantag från bestämmelserna om sökning i 5 §. Paragrafen, som motsvarar nuvarande 3 kap. 7 § tredje stycket, ändras endast redaktionellt.

9 §

I paragrafen, där övriga bestämmelser om föreskrifter som rör gemensamt tillgängliga uppgifter samlas, upplyses om att regeringen, eller den myndighet som regeringen bestämmer, kan meddela föreskrifter om begränsning av tillgången till personuppgifter som avses i 5 § (vilket motsvarar nuvarande 3 kap. 6 § andra stycket), under vilka förutsättningar sökning får utföras med stöd av 6 § (vilket motsvarar nuvarande 3 kap. 7 § tredje stycket) och omfattningen av direktåtkomst och behörighet och säkerhet vid sådan åtkomst (vilket motsvarar nuvarande 3 kap. 8 § tredje stycket).

4 kap.

1 §

Regleringen av hur länge personuppgifter får behandlas är samlad i detta kapitel. I *första stycket*, som är nytt, föreskrivs att kapitlet endast gäller för uppgifter som behandlas automatiserat, om inget annat sägs. I 3 § finns en bestämmelse som även är tillämplig på viss annan behandling.

Andra stycket upplyser om att den grundläggande bestämmelsen om att personuppgifter inte får behandlas längre än vad som är nödvändigt med hänsyn till ändamålet med behandlingen finns i 2 kap. 17 § första stycket brottsdatalagen (2018:000). I övriga paragrafer i kapitlet anges hur länge vissa typer av personuppgifter får behandlas inom den ram som sätts av denna huvudregel. Oavsett vilken bedömning som görs av nyttan med behandlingen av en viss personuppgift får den dock inte behandlas längre än vad som anges i respektive paragraf.

2 §

I paragrafen anges hur länge uppgifter som inte har gjorts gemensamt tillgängliga får behandlas. Frågan behandlas i avsnitt 5.5.2. Någon ändring av hur länge personuppgifterna får behandlas görs inte.

I *första stycket* klargörs att uppgifterna, trots det som sägs i 2 kap. 17 § andra stycket brottsdatalagen (2018:000) om att arkivlagstiftningen har företräde, inte får arkiveras digitalt. Utgångspunkten är alltså att all automatiserad behandling av personuppgifterna ska upphöra när den tid som anges i paragrafen har löpt ut, vilket innebär att uppgifterna ska tas bort. Endast om det har meddelats uttryckliga föreskrifter som innebär att uppgifterna i fråga får behandlas för arkivändamål av allmänt intresse eller för vetenskapliga, statistiska eller historiska ändamål får de behandlas automatiserat längre än vad som anges i denna paragraf (se 12 §). Stycket ändras även redaktionellt.

Andra stycket ändras endast redaktionellt.

3 §

Paragrafen, som är ny och behandlas i avsnitt 8.4.2, reglerar när personuppgifter från transportföretag ska förstöras. Den motsvarar 16 § tredje stycket lagen (1996:701) om Tullverkets befogenheter vid Sveriges gräns mot ett annat land inom Europeiska unionen och 4 kap. 8 § tredje stycket tullagen (2016:253).

Transportföretagens uppgiftsskyldighet kan fullgöras på det sätt transportföretagen finner lämpligt. Av 15 § lagen om Tullverkets befogenheter vid Sveriges gräns mot ett annat land inom Europeiska unionen och 4 kap. 6 § tullagen framgår att terminalåtkomst bara tillåts i den omfattning och under den tid som behövs för att kontrollera aktuella transporter (se prop. 1995/96:166 s. 81 f.). Personuppgifter som Tullverket får tillgång till på annat sätt än genom terminalåtkomst ska enligt *första stycket* förstöras omedelbart om de saknar betydelse för brottsbekämpning och lagföring. Eftersom flertalet uppgifter rör personer som varken är misstänkta för brott eller att utöva brottslig verksamhet, ska personuppgifterna omedelbart tas bort när Tullverket har gjort profilsökning och riskanalys och inte längre behöver dem.

Enligt 2 kap. 10 § andra stycket får uppgifter från transportföretag i ett enskilt fall behandlas för nya ändamål om förutsättningarna för det är uppfyllda. Det kan t.ex. vara fallet om uppgifterna är nödvändiga för att Tullverket ska kunna utreda eller lagföra ett visst brott i samband med in- eller utförsel av varor (jfr prop. 1995/96:166 s. 99 f.). Sådana personuppgifter behöver då inte förstöras. För dem gäller i stället bestämmelserna i 4–6 §§.

I *andra stycket* föreskrivs att paragrafen även gäller för behandling som inte är automatiserad när uppgifter från transportföretag ingår i en strukturerad samling personuppgifter. Det innebär att paragrafen är tillämplig t.ex. på personuppgifter som lämnas i pappersform.

4 §

Paragrafen reglerar hur länge personuppgifter i en anmälan om brott får behandlas. Terminologin anpassas till den som används i lagen i övrigt och till att uttrycket brottsbekämpande verksamhet utmönstras ur lagen, vilket behandlas i avsnitt 4.4.1.

Enligt paragrafen inskränks enbart behandlingen av personuppgifter för de ändamål som regleras i lagen, vilket innebär att uppgifterna får fortsätta att behandlas automatiserat för bl.a. arkivändamål efter de tidpunkter som anges i paragrafen. Frågan behandlas i avsnitt 5.5.3.

5 §

Paragrafen reglerar hur länge personuppgifter i förundersökningar och andra utredningar som handläggs enligt bestämmelserna i 23 kap. rättegångsbalken får behandlas.

Enligt paragrafen inskränks enbart behandlingen av personuppgifter för de ändamål som regleras i lagen, vilket innebär att uppgifterna får fortsätta att behandlas automatiserat för bl.a. arkivändamål efter de tidpunkter som anges i paragrafen. Frågan behandlas i avsnitt 5.5.3.

Terminologin i *första och andra styckena* anpassas till den som används i lagen i övrigt och till att uttrycket brottsbekämpande verksamhet utmönstras ur lagen, vilket behandlas i avsnitt 4.4.1.

Tredje stycket är oförändrat.

7 §

I paragrafen anges att det i de följande paragraferna finns bestämmelser om hur länge vissa typer av gemensamt tillgängliga uppgifter, som inte förekommer i ärenden om utredning av eller lagföring för brott, får behandlas. Det klargörs att uppgifterna, trots det som sägs i 2 kap. 17 § andra stycket brottsdatalagen (2018:000) om att arkivlagstiftningen har företräde, inte får arkiveras digitalt. Utgångspunkten är alltså att all automatiserad behandling av personuppgifterna ska upphöra när den tid som anges i 8–11 §§ har löpt ut, vilket innebär att uppgifterna ska tas bort. Endast om det har meddelats uttryckliga föreskrifter som innebär att uppgifterna i fråga får behandlas för arkivändamål av allmänt intresse eller för vetenskapliga, statistiska eller historiska ändamål får de behandlas automatiserat längre än vad som anges i de följande paragraferna (jfr 12 §). Frågan behandlas i avsnitt 5.5.2.

8 §

Paragrafen reglerar hur länge personuppgifter får behandlas i underrättelseverksamhet. Paragrafen anpassas till den terminologi som används i lagen i övrigt.

Enligt *första stycket*, som är nytt och behandlas i avsnitt 8.6, får personuppgifter som kan antas ha samband med sådan brottslig verksamhet som anges i 3 kap. 2 § första stycket 1 och som behandlas i ett ärende inte behandlas längre än ett år efter det att ärendet avslutades.

I *andra stycket*, som motsvarar 9 § andra stycket, görs ingen ändring i fråga om hur länge personuppgifterna får behandlas men stycket anpassas till den terminologi som används i lagen i övrigt. Det tydliggörs att fristen för hur länge personuppgifter får behandlas endast ska påverkas av om det görs en ny registrering beträffande personens anknytning till brottslig verksamhet. Andra uppgifter som tillförs, t.ex. uppgifter om ändrade bostadsförhållanden eller annat som inte har betydelse för anknytningen till den brotts-

liga verksamheten, påverkar alltså inte hur länge personuppgifterna får behandlas. Frågan behandlas i avsnitt 5.5.4.

Tredje stycket ändras endast redaktionellt.

9 §

Paragrafen, som motsvarar nuvarande 9 § tredje och fjärde styckena, reglerar hur länge uppgifter om en person som är föremål för övervakning enligt 3 kap. 2 § första stycket 2 får behandlas. I *första stycket* anpassas regleringen till den terminologi som används i lagen i övrigt. Frågan behandlas i avsnitt 5.5.2. *Andra stycket* är oförändrat.

10 §

I paragrafen, som motsvarar nuvarande 10 § tredje stycket, regleras hur länge uppgifter som har rapporterats till Tullverkets ledningscentraler får behandlas. Regleringen, som behandlas i avsnitt 5.5.2, anpassas till den terminologi som används i lagen i övrigt.

11 §

Paragrafen, som motsvarar nuvarande 10 § andra stycket, reglerar hur länge uppgifter som behandlas för att fullgöra internationella åtaganden får behandlas. Regleringen, som behandlas i avsnitt 5.5.2, anpassas till den terminologi som används i lagen i övrigt.

12 §

I paragrafen upplyses om att regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om att vissa kategorier av personuppgifter får behandlas längre än vad som anges i 4, 5 och 8–11 §§ (vilket motsvarar nuvarande 2 § 1), om att personuppgifter, trots att den tillåtna tiden för behandling har löpt ut, får fortsätta att behandlas för arkivändamål av allmänt intresse och vetenskapliga, statistiska eller historiska ändamål under längre tid än vad som anges i 2 § första stycket och 8–11 §§ (vilket motsvarar

nuvarande 2 § 2) och om digital arkivering inom lagens tillämpningsområde (vilket motsvarar nuvarande 2 § 3).

5 kap.

Administrativa sanktionsavgifter

1 §

Paragrafen, som är ny, reglerar vilka överträdelser som kan föranleda sanktionsavgift. Frågan behandlas i avsnitt 5.4.2.

I *första stycket* anges vid vilka överträdelser sanktionsavgift får tas ut av den personuppgiftsansvarige. Tillsynsmyndigheten avgör i det enskilda fallet om det är påkallat att ta ut sanktionsavgift, vilket framgår av formuleringen att avgift får tas ut. Uppräkningen av vilka överträdelser som kan föranleda sanktionsavgift är uttömmande. Sanktionsavgift kan tas ut för överträdelse av bestämmelserna om tillåtna rättsliga grunder, särskilda upplysningar och längsta tid som personuppgifter får behandlas. Brottsdatalagens förfaranderegler när det gäller sanktionsavgift tillämpas även vid överträdelser enligt denna lag. I brottsdatalagen med tillhörande förordning regleras också handläggningen av frågor om sanktionsavgift.

I *andra stycket* anges storleken på de sanktionsavgifter som kan komma i fråga. De överträdelser som enligt lagen kan föranleda sanktionsavgift är alla av allvarligt slag. Lägsta sanktionsavgift är därför 50 000 kronor.

Skadestånd

2 §

I paragrafen regleras den registrerades rätt till skadestånd för behandling av personuppgifter i strid med regelverket. Paragrafen behandlas i avsnitt 5.4.3.

Paragrafen hänvisar till 7 kap. 1 § brottsdatalagen (2018:000), som ska tillämpas på motsvarande sätt när det har förekommit felaktig behandling av personuppgifter enligt förevarande lag eller föreskrifter som har meddelats i anslutning till den. Det innebär att

den personuppgiftsansvarige ska ersätta den registrerade för den skada och kränkning av den personliga integriteten som behandlingen av personuppgifter har orsakat. Med skada avses personskada, sakskada eller ren förmögenhetsskada. Med kränkning avses ideell skada som består i att den enskildes integritet kränkts genom behandlingen. Någon möjlighet till jämkning av skadeståndet finns inte.

Överklagande

3 §

I paragrafen, som behandlas i avsnitt 5.4.4, upplyses om att det i 7 kap. brottsdatalagen (2018:000) finns bestämmelser om överklagande och om vilka beslut som får överklagas.

Övergångsbestämmelser

Ikraftträdande- och övergångsbestämmelserna tas upp i avsnitt 18.1 och 18.2.

Punkten 1 föreskriver när lagen ska träda i kraft.

Sanktionsavgift får enligt *punkten 2* beslutas endast för överträdelser som har begåtts efter ikraftträdandet.

Punkten 3 innebär att bestämmelsen om skadestånd i 48 § personuppgiftslagen fortfarande ska gälla för skada som har orsakats före ikraftträdandet vid behandling av personuppgifter enligt lagen eller föreskrifter som har meddelats i anslutning till den.

20.21 Förslaget till lag om ändring i skattebrottsdatalagen (2017:452)

Lagen anpassas till bestämmelserna i brottsdatalagen, vilket leder till omarbetning av den och att två kapitel upphävs och ersätts med nya. Vissa paragrafer i de övriga kapitlen upphävs, samtidigt som nya paragrafer tillkommer. Bestämmelserna om föreskrifter, samlas i slutet av varje kapitel. Dessa förändringar föranleder omnumreringar av vissa paragrafer.

Som en anpassning till brottsdatalagen tillkommer ett nytt kapitel om administrativa sanktionsavgifter och rättsmedel.

De generella ändringarna i lagen behandlas i kapitel 4, 5 och 6 och övriga ändringar i kapitel 10.

Lagen får också ett nytt namn, Skatteverkets brottsdatalag.

1 kap. Allmänna bestämmelser

Lagens tillämpningsområde

1 §

I paragrafen, som behandlas i avsnitt 10.2, anges lagens tillämpningsområde.

Lagen gäller utöver brottsdatalagen när Skatteverket i egenskap av behörig myndighet enligt brottsdatalagen behandlar personuppgifter för vissa syften. Behörig myndighet, personuppgift och behandling av personuppgifter definieras i 1 kap. 6 § brottsdatalagen (2018:000).

Att lagen gäller utöver brottsdatalagen innebär bl.a. att lagen enligt 1 kap. 3 § brottsdatalagen bara gäller för sådan behandling av personuppgifter som är helt eller delvis automatiserad och för annan behandling av personuppgifter som ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

I brottsdatalagen finns alla de grundläggande bestämmelserna om hur personuppgifter får behandlas. Den nu aktuella lagen innehåller bestämmelser som innebär preciseringar, undantag eller avvikelser från bestämmelser i brottsdatalagen. Det innebär att bestämmelserna i lagen ska läsas tillsammans med regleringen i brottsdatalagen och tolkas i ljuset av den regleringen.

Lagen gäller när Skatteverket behandlar personuppgifter om syftet med behandlingen är att bekämpa brott. Vad det innebär utvecklas i kommentaren till 2 kap. 1 §.

Personuppgiftsansvar

2 §

Paragrafen, som motsvarar nuvarande 2 kap. 3 §, reglerar personuppgiftsansvaret. Personuppgiftsansvarig definieras i 1 kap. 6 § brottsdatalagen (2018:000). Personuppgiftsansvarigas skyldigheter regleras i 3 kap. brottsdatalagen.

Lagens tillämpning på uppgifter om juridiska personer

3 §

I paragrafen anges vilka bestämmelser i lagen och i brottsdatalagen som gäller för behandling av uppgifter om juridiska personer. Frågan behandlas i avsnitt 5.4.1.

Uppräkningen i paragrafen av bestämmelser som ska gälla vid behandling av uppgifter om juridiska personer motsvarar nuvarande reglering.

2 kap. Grundläggande bestämmelser om behandling

Tillåtna rättsliga grunder för behandling av personuppgifter

1 §

Paragrafen reglerar de tillåtna rättsliga grunderna för behandling av personuppgifter. Den behandlas i avsnitt 6.1, 6.3 och 10.3.1.

Paragrafen, som är anpassad till hur de rättsliga grunderna för behandling av personuppgifter anges i 2 kap. 1 § brottsdatalagen (2018:000), ersätter den bestämmelsen. Regleringen i 2 kap. 2 § brottsdatalagen ger myndigheten rättsligt stöd för att i vissa fall behandla personuppgifter för diarieföring eller för att utföra andra nödvändiga handläggningsuppgifter, trots brist på stöd i denna paragraf.

Personuppgifter får enligt *första stycket* behandlas om det är nödvändigt för att utföra en arbetsuppgift i vissa särskilt angivna syften inom lagens tillämpningsområde. Bestämmelsen bildar den yttre ramen för när behandling av personuppgifter är tillåten.

Enligt *punkten 1* får Skatteverket behandla personuppgifter i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet. Det är framför allt myndighetens underrättelseverksamhet som avses (se prop. 2016/17:89 s. 139).

Enligt *punkten 2* får personuppgifter behandlas i syfte att utreda brott. Vad det innebär utvecklas i prop. 2016/17:89 s. 139.

Personuppgifter får enligt *punkten 3* också behandlas i syfte att fullgöra förpliktelser som följer av internationella åtaganden, vilket tar sikte på förpliktelser som syftar till att gagna utländsk brottsbekämpande verksamhet (se prop. 2016/17:89 s. 139).

I *andra stycket* anges att det ska vara fråga om en arbetsuppgift som framgår av en bindande unionsrättsakt eller av en lag, en förordning eller ett särskilt beslut i vilket regeringen uppdragit åt den behöriga myndigheten att ansvara för en sådan uppgift. Motsvarande bestämmelse finns i 2 kap. 1 § brottsdatalagen. Vad den innebär utvecklas i SOU 2017:29 s. 238 f.

2 §

I paragrafen, som behandlas i avsnitt 10.3.1, upplyses om att förutsättningarna för att personuppgifter ska få behandlas för nya ändamål regleras i 2 kap. 4 och 22 §§ brottsdatalagen (2018:000). Innan personuppgifter får behandlas för ett nytt ändamål inom eller utanför brottsdatalagens tillämpningsområde krävs det en prövning enligt någon av paragraferna. Vad prövningen innebär utvecklas i SOU 2017:29 s. 249 f. och avsnitt 6.4.3.

Särskilda upplysningar

3 §

I paragrafen, som behandlas i avsnitt 5.3.10, görs det undantag från bestämmelserna om särskilda upplysningar i 2 kap. 3 § andra stycket, 9 och 10 §§ brottsdatalagen (2018:000). Det är endast personuppgifter som har gjorts gemensamt tillgängliga med stöd av 3 kap. 2 § som i vissa fall ska förses med särskilda upplysningar. Det innebär att när personuppgifter behandlas bara av ett fåtal personer behöver särskilda upplysningar inte lämnas.

Sökning

Känsliga personuppgifter

4 §

I paragrafen, som tillsammans med 5 § reglerar när det är tillåtet att använda känsliga personuppgifter vid sökning, görs det undantag från sökförbudet i 2 kap. 14 § brottsdatalagen (2018:000). Paragrafen behandlas i avsnitt 10.3.3.

Undantaget gäller vid sökning i alla slags personuppgifter, dvs. såväl personuppgifter som har gjorts gemensamt tillgängliga som personuppgifter som inte har det. Sökförbudet hindrar inte att uppgifter som beskriver en persons utseende får användas vid sökning, även om det skulle leda till ett personurval grundat på känsliga personuppgifter. Med uppgifter som beskriver en persons utseende avses bl.a. uppgifter om hudfärg eller tatueringar. Sökning på sådana uppgifter kan t.ex. ge ett personurval grundat på uppgifter om etniskt ursprung, politisk åskådning eller religiös övertygelse.

I vilken utsträckning det är tillåtet att behandla någon eller några av personuppgifterna i en sammanställning av sådana uppgifter som sökningen resulterat i får prövas mot huvudregeln om behandling av känsliga personuppgifter i 2 kap. 11 §§ brottsdatalagen. Rätten att göra sökning enligt denna paragraf medför således inte en generell rätt att fortsätta att behandla uppgifterna.

5 §

I paragrafen, som tillsammans med 4 § reglerar när det är tillåtet att använda känsliga personuppgifter vid sökning, görs det undantag från sökförbudet i 2 kap. 14 § brottsdatalagen (2018:000). Paragrafen behandlas i avsnitt 10.3.3.

Undantaget gäller enbart vid sökning i personuppgifter som inte har gjorts gemensamt tillgängliga, dvs. personuppgifter som enbart ett fåtal har tillgång till. Sökning i sådana uppgifter får göras i syfte att få fram ett personurval grundat på etniskt ursprung. Sökning av det slaget kan behövas för att förebygga, förhindra eller upptäcka brottslig verksamhet som begås av flera som förenas av sitt etniska ursprung. I t.ex. ärenden om falska identitetshandlingar eller ärenden om gränsöverskridande ekonomisk brottslighet kan etniskt

ursprung vara en gemensam faktor som knyter samman personerna i ett nätverk.

I vilken utsträckning det är tillåtet att behandla någon eller några av personuppgifterna i en sammanställning av sådana uppgifter som sökningen resulterat i får prövas mot huvudregeln om behandling av känsliga personuppgifter i 2 kap. 11 § brottsdatalagen. Rätten att göra sökning enligt denna paragraf medför således inte en generell rätt att fortsätta att behandla uppgifterna.

Beskattningsdatabasen

6 §

I paragrafen, som motsvarar nuvarande 2 kap. 9 §, regleras vilka uppgifter Skatteverket får använda vid sökning i beskattningsdatabasen i syfte att bekämpa brott. Ändringen är en följd av att uttrycket brottsbekämpande verksamhet utmönstras ur lagen, vilket behandlas i avsnitt 4.4.1.

Utlämnande av personuppgifter

7 §

Paragrafen innehåller en sekretessbrytande bestämmelse om utlämnande till utländska myndigheter och mellanfolkliga organisationer. Den motsvarar nuvarande 2 kap. 11 §.

8 §

Paragrafen innehåller en bestämmelse som bryter viss sekretess som annars skulle ha gällt gentemot andra brottsbekämpande myndigheter. Den motsvarar nuvarande 2 kap. 12 §.

Det tydliggörs att sekretessen bryts om den mottagande myndigheten behöver uppgifterna för något av de syften som anges i 1 kap. 2 § brottsdatalagen. Ändringen, som är en följd av att uttrycket brottsbekämpande verksamhet utmönstras ur lagen, behandlas i avsnitt 4.4.1.

9 §

Paragrafen reglerar när personuppgifter får lämnas ut elektroniskt.

I *första stycket* föreskrivs att personuppgifter får lämnas ut elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt. Med sådant utlämnande avses bl.a. utlämnande genom e-post eller annan elektronisk överföring eller på ett usb-minne eller annat motsvarande medium. Frågan behandlas i avsnitt 5.6.4.

Det har betydelse vem mottagaren är för frågan om det är olämpligt att lämna ut uppgifter elektroniskt. Som regel kan det inte anses vara olämpligt att lämna ut uppgifter på det sättet till en myndighet (se prop. 2014/15:148 s. 113, jfr SOU 2015:39 s. 447 f.).

När det gäller utlämnande till enskilda krävs en mer nyanserad bedömning. Om det finns en författningsreglerad skyldighet att sända en handling till en viss person får det avgöras om elektroniskt utlämnande är olämpligt med hänsyn till bl.a. innehållet i handlingen, vem som är mottagare, behovet av att kunna visa att personen i fråga har tagit del av handlingen och andra omständigheter.

Frågan är särskilt svårbedömd när uppgifter ska lämnas ut till enskilda och det på grund av uppgifternas art, struktur, antal eller någon annan särskild omständighet finns anledning att befara att utlämnandet kan leda till integritetsrisker (jfr prop. 2014/15:148 s. 114). Bedömer myndigheten att det finns risk för att personuppgifterna kan komma att missbrukas om de lämnas ut elektroniskt gäller sekretess enligt 21 kap. 7 § offentlighets- och sekretesslagen (2009:400). De får då inte lämnas ut till följd av sekretess.

Det kan också finnas särskild anledning att iaktta försiktighet när det gäller utlämnande av bild- och ljudupptagningar (jfr prop. 2016/17:68 s. 51 f.).

Vid prövningen av om personuppgifter bör lämnas ut elektroniskt bör givetvis även informationssäkerheten vägas in.

Om någon begär att få tillgång till en allmän handling med stöd av tryckfrihetsförordningen får den utlämnande myndigheten inte efterforska syftet med begäran. Det kan ha betydelse för möjligheten att få underlag för att bedöma om det i ett enskilt fall är lämpligt att lämna ut en handling med personuppgifter elektroniskt (se JO dnr 4171-2011).

Elektroniskt utlämnande genom direktåtkomst regleras i *andra stycket*, som motsvarar nuvarande 2 kap. 16 §. Det är tillåtet endast i den utsträckning som anges i lagen.

Föreskrifter

10 §

I paragrafen upplyses om att regeringen kan meddela föreskrifter om att personuppgifter får lämnas ut även i andra fall än som anges i 7 och 8 §§ (vilket motsvarar nuvarande 2 kap. 13 § första stycket) och om begränsning av möjligheterna att lämna ut personuppgifter elektroniskt på annat sätt än genom direktåtkomst. Frågan behandlas i avsnitt 5.6.4.

3 kap.

1 §

Av paragrafen framgår att kapitlet innehåller bestämmelser om behandling av personuppgifter som görs eller har gjorts gemensamt tillgängliga. Vad som avses med att uppgifter görs gemensamt tillgängliga utvecklas i prop. 2016/17:89 s. 147 f.

I *första stycket* anpassas regleringen till att uttrycket brottsbekämpande verksamhet utmönstras ur lagen, vilket behandlas i avsnitt 4.4.1.

Av *andra stycket* framgår att kapitlet inte gäller när personuppgifter behandlas med stöd av den särskilda bestämmelsen i 2 kap. 2 § brottsdatalagen (2018:000) om behandling av personuppgifter för diarieföring eller för att utföra andra nödvändiga handläggningsuppgifter.

2 §

I paragrafen anges vilka personuppgifter som får göras gemensamt tillgängliga. Regleringen anpassas till den terminologi som används i lagen i övrigt.

3 §

I paragrafen ställs det krav på att uppgifter som är gemensamt tillgängliga i underrättelseverksamhet ska förse med särskilda upplysningar. Frågan behandlas i avsnitt 5.3.10.

Enligt *första stycket* ska det framgå av uppgifter i underrättelseverksamhet att en person inte är misstänkt för att utöva brottslig verksamhet. Det ska alltså gå att skilja mellan personer som är föremål för myndighetens intresse på grund av inblandning i brottslig verksamhet och personer som inte är misstänkta för det. Att det ska framgå om en person är misstänkt för brott eller är ett brottsoffer, regleras i 2 kap. 9 § brottsdatalagen (2018:000).

Enligt *andra stycket* ska uppgifter om personer som kan antas ha samband med misstänkt brottslig verksamhet förse med upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak. Det tydliggörs att kravet på särskild upplysning bara gäller uppgifter om en person som kan antas ha direkt samband med misstänkt brottslig verksamhet. Kravet på samband är lågt ställt. Så snart det finns något som stöder ett antagande om att en person har ett direkt samband med brottslig verksamhet och det är fråga om uppgifter som görs gemensamt tillgängliga ska det framgå på vilket sätt personen har anknytning till den brottsliga verksamheten. Sambandet kan t.ex. bestå i att en person ofta träffar eller har annan kontakt med andra personer som är misstänkta för att utöva brottslig verksamhet eller ofta rör sig i miljöer där brottslighet förekommer, utan att ha naturliga skäl att befinna sig där. Uppgifter om den som är anhörig till en person som kan antas ha samband med misstänkt brottslig verksamhet faller alltså utanför, utom i de fall där båda kan antas ha direkt samband med brottslig verksamhet.

Det är bara uppgifter som rör en person som är misstänkt för att utöva eller komma att utöva brottslig verksamhet som behöver förse med upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak. De uppgifter som är av intresse är, förutom uppgifter om på vilket sätt personen är knuten till den brottsliga verksamheten, framför allt uppgifter som belyser brottslighetens art och omfattning. Uppgifter av det slaget kan behöva förse med särskilda upplysningar för att personens anknytning till brottsligheten ska kunna bedömas.

Utrymmet för att underlåta att förse uppgifter med upplysning om trovärdighet och riktighet vidgas något genom att det inte längre krävs särskilda omständigheter för att upplysningskravet inte ska gälla. Det är tillräckligt att det på grund av de samlade omständigheterna är onödigt att förse uppgifterna med en upplysning.

4 §

Paragrafen, som behandlas i avsnitt 10.4, innehåller en allmän begränsning av vilka uppgifter som får tas fram vid sökning i gemensamt tillgängliga uppgifter på namn, personnummer eller liknande identitetsbeteckningar.

Genom ett tillägg tydliggörs det att bestämmelsen endast gäller vid sökning i automatiserade behandlingssystem. Vad som avses med automatiserade behandlingssystem utvecklas i SOU 2017:29 s. 306 f. I övrigt ändras paragrafen endast redaktionellt.

5 §

Paragrafen, som behandlas i avsnitt 10.4, innehåller undantag från begränsningarna i 4 §.

Enligt *första stycket* gäller inga begränsningar vid sökning i en viss handling eller ett visst ärende.

Enligt *andra stycket* gäller begränsningarna i 4 § inte vid vissa sökningar som utförs av särskilt angivna tjänstemän. Det gäller enligt *punkten 1*, som är ny, när de utför beredningsuppgifter i underrättelseverksamhet och arbetet befinner sig i ett inledande skede. Syftet med bestämmelsen är att tjänstemännen inledningsvis ska ha större möjligheter att göra sökningar för att kunna finna samband med befintliga underrättelseuppgifter. Det är således bara under en begränsad tid från det att uppgifterna kommit in som punkten är tillämplig. Så snart beredningsarbetet har avslutats upphör möjligheten att göra sökningar med stöd av den nu aktuella punkten.

I *punkten 2*, som motsvarar nuvarande 3 kap. 7 § första stycket 2 och andra stycket 1, undantas sökningar som utförs i syfte att bearbeta och analysera personuppgifter som har gjorts gemensamt

tillgängliga i underrättelseverksamhet, om det endast är de tjänstemän som får göra sökningen som också har tillgång till uppgifterna.

Punkten 3, som motsvarar nuvarande 3 kap. 7 § andra stycket 2, ändras endast redaktionellt.

6 §

I paragrafen anges vilka myndigheter som får medges direktåtkomst till uppgifter som har gjorts gemensamt tillgängliga och för vilka syften. Ändringen är en följd av att uttrycket brottslig verksamhet utmönstras ur lagen, vilket behandlas i avsnitt 4.4.1. Vidare görs redaktionella ändringar.

7 §

I paragrafen upplyses om att regeringen kan meddela föreskrifter om ytterligare undantag från bestämmelserna om sökning i 4 §.

8 §

I paragrafen, där övriga bestämmelser om föreskrifter samlas, upplyses om att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter om begränsning av tillgången till sådana personuppgifter som avses i 4 § (vilket motsvarar nuvarande 6 § andra stycket), under vilka förutsättningar sökning får utföras med stöd av 5 § (vilket motsvarar nuvarande 7 § tredje stycket) och omfattningen av direktåtkomst och behörighet och säkerhet vid sådan åtkomst (vilket motsvarar nuvarande 8 § tredje stycket).

4 kap.

1 §

De bestämmelser som anger hur länge personuppgifter som behandlas enligt lagen får behandlas är samlade i detta kapitel.

I *första stycket*, som är nytt, föreskrivs att bestämmelserna i kapitlet endast gäller för uppgifter som behandlas automatiserat.

Andra stycket upplyser om att den grundläggande bestämmelsen om att personuppgifter inte får behandlas längre än vad som är nödvändigt med hänsyn till ändamålet med behandlingen finns i 2 kap. 17 § första stycket brottsdatalagen (2018:000). I övriga paragrafer i kapitlet anges hur länge vissa typer av personuppgifter får behandlas inom den ram som sätts av denna huvudregel. Oavsett vilken bedömning som görs av nyttan med behandlingen av en viss personuppgift får den dock inte behandlas längre än vad som anges i respektive paragraf.

2 §

I paragrafen anges hur länge uppgifter som inte har gjorts gemensamt tillgängliga får behandlas. Frågan behandlas i avsnitt 5.5.2. Någon ändring av ur länge personuppgifterna får behandlas görs inte.

I *första stycket* klargörs att uppgifterna, trots det som sägs i 2 kap. 17 § andra stycket brottsdatalagen (2018:000) om att arkivlagstiftningen har företräde, inte får arkiveras digitalt. Utgångspunkten är alltså att all automatiserad behandling av personuppgifterna ska upphöra när den tid som anges i paragrafen har löpt ut, vilket innebär att uppgifterna ska tas bort. Endast om det har meddelats uttryckliga föreskrifter som innebär att uppgifterna i fråga får behandlas för arkivändamål av allmänt intresse eller för vetenskapliga, statistiska eller historiska ändamål får de behandlas automatiserat längre än vad som anges i denna paragraf (jfr 9 §).

Andra stycket är oförändrat.

3 §

I paragrafen anges hur länge personuppgifter i en anmälan om brott får behandlas. Paragrafen ändras till följd av att uttrycket brottsbekämpande verksamhet utmönstras ur lagen, vilket behandlas i avsnitt 4.4.1.

Enligt paragrafen inskränks enbart behandlingen av personuppgifter för de ändamål som regleras i lagen, vilket innebär att uppgifterna får fortsätta att behandlas automatiserat för bl.a. arkivända-

mål efter de tidpunkter som anges i paragrafen. Frågan behandlas i avsnitt 5.5.3.

4 §

Paragrafen reglerar hur länge personuppgifter i förundersökningar och andra utredningar som handläggs enligt bestämmelser i 23 kap. rättegångsbalken får behandlas.

Enligt paragrafen inskränks enbart behandlingen av personuppgifter för de ändamål som regleras i lagen, vilket innebär att uppgifterna får fortsätta att behandlas automatiserat för bl.a. arkivändamål efter de tidpunkter som anges i paragrafen. Frågan behandlas i avsnitt 5.5.3.

Första och andra styckena ändras till följd av att uttrycket brottsbekämpande verksamhet utmönstras ur lagen. Vidare anpassas terminologin till den som används i lagen i övrigt och vissa redaktionella ändringar görs. Frågorna behandlas i avsnitt 4.4.1 och 5.5.2.

Tredje stycket är oförändrat.

6 §

I paragrafen anges att det i de följande paragraferna finns bestämmelser om hur länge vissa typer av gemensamt tillgängliga uppgifter, som inte förekommer i ärenden om utredning av eller lagföring för brott, får behandlas. Det klargörs att uppgifterna, trots det som sägs i 2 kap. 17 § andra stycket brottsdatalagen (2018:000) om att arkivlagstiftningen har företräde, inte får arkiveras digitalt. Utgångspunkten är alltså att all automatiserad behandling av personuppgifterna ska upphöra när den tid som anges i 7 och 8 §§ har löpt ut, vilket innebär att uppgifterna ska tas bort. Endast om det har meddelats uttryckliga föreskrifter som innebär att uppgifterna i fråga får behandlas för arkivändamål av allmänt intresse eller för vetenskapliga, statistiska eller historiska ändamål får de behandlas automatiserat längre än vad som anges i de följande paragraferna (jfr 9 §). Frågan behandlas i avsnitt 5.5.2.

7 §

Paragrafen reglerar hur länge personuppgifter får behandlas i underrättelseverksamhet. Någon ändring i fråga om hur länge personuppgifterna får behandlas görs inte. Paragrafen anpassas till den terminologi som används i lagen i övrigt.

Det tydliggörs att fristen för hur länge personuppgifter får behandlas endast ska påverkas av om det görs en ny registrering beträffande personens anknytning till brottslig verksamhet. Andra uppgifter som tillförs, t.ex. uppgifter om ändrade bostadsförhållanden eller annat som inte har betydelse för anknytningen till den brottsliga verksamheten, påverkar alltså inte hur länge personuppgifterna får behandlas. Frågan behandlas i avsnitt 5.5.4.

8 §

Paragrafen, som motsvarar nuvarande 8 § tredje stycket, reglerar hur länge uppgifter som behövs för att fullgöra internationella åtaganden får behandlas. Paragrafen anpassas till den terminologi som används i lagen i övrigt.

9 §

I paragrafen, som motsvarar nuvarande 2 §, upplyses om att regeringen, eller den myndighet som regeringen bestämmer, kan meddela föreskrifter om att vissa kategorier av personuppgifter får behandlas längre än vad som anges i 3, 4, 7 och 8 §§, om att personuppgifter, trots att den tillåtna tiden för behandling har löpt ut, får fortsätta att behandlas för arkivändamål av allmänt intresse och vetenskapliga, statistiska eller historiska ändamål och om begränsning av behandlingen av personuppgifter för ändamål inom lagens tillämpningsområde för digital arkivering.

5 kap. Administrativa sanktionsavgifter och rättsmedel

Administrativa sanktionsavgifter

1 §

Paragrafen, som är ny, reglerar vilka överträdelser som kan föranleda sanktionsavgift. Frågan behandlas i avsnitt 5.4.2.

I *första stycket* anges vid vilka överträdelser sanktionsavgift får tas ut av den personuppgiftsansvarige. Tillsynsmyndigheten avgör i det enskilda fallet om det är påkallat att ta ut sanktionsavgift, vilket framgår av formuleringen att avgift får tas ut. Uppräkningen av vilka överträdelser som kan föranleda sanktionsavgift är uttömmande. Sanktionsavgift kan tas ut för överträdelse av bestämmelserna om tillåtna rättsliga grunder, särskilda upplysningar och längsta tid som personuppgifter får behandlas. Brottsdatalogens förfaranderegler när det gäller sanktionsavgift tillämpas även vid överträdelser enligt denna lag. I brottsdatalogen med tillhörande förordning regleras också handläggningen av frågor om sanktionsavgift.

I *andra stycket* anges storleken på de sanktionsavgifter som kan komma i fråga. De överträdelser som enligt lagen kan föranleda sanktionsavgift är alla av allvarligt slag. Lägsta sanktionsavgift är därför 50 000 kronor.

Skadestånd

2 §

I paragrafen regleras den registrerades rätt till skadestånd för behandling av personuppgifter i strid med regelverket. Paragrafen behandlas i avsnitt 5.4.3.

Paragrafen hänvisar till 7 kap. 1 § brottsdatalogen (2018:000), som ska tillämpas på motsvarande sätt när det har förekommit felaktig behandling av personuppgifter enligt förevarande lag eller föreskrifter som har meddelats i anslutning till den. Det innebär att den personuppgiftsansvarige ska ersätta den registrerade för den skada och kränkning av den personliga integriteten som behandlingen av personuppgifter har orsakat. Med skada avses personskada, sakskada eller ren förmögenhetsskada. Med kränkning avses

ideell skada som består i att den enskildes integritet kränkts genom behandlingen. Någon möjlighet till jämkning av skadeståndet finns inte.

Överklagande

3 §

I paragrafen, som behandlas i avsnitt 5.4.4, upplyses om att det i 7 kap. brottsdatalogen (2018:000) finns bestämmelser om överklagande och om vilka beslut som får överklagas.

Övergångsbestämmelser

Ikraftträdande- och övergångsbestämmelserna tas upp i avsnitt 18.1 och 18.2.

Punkten 1 föreskriver när lagen ska träda i kraft.

Sanktionsavgift får enligt *punkten 2* beslutas endast för överträdelser som har begåtts efter ikraftträdandet.

Punkten 3 innebär att bestämmelsen om skadestånd i 48 § personuppgiftslagen fortfarande ska gälla för skada som har orsakats före ikraftträdandet vid behandling av personuppgifter enligt lagen eller föreskrifter som har meddelats i anslutning till den.

20.22 Förslaget till lag om ändring i lagen (2017:496) om internationellt polisiärt samarbete

6 kap.

1 §

I paragrafen regleras hur bestämmelserna i lagen förhåller sig till andra bestämmelser om behandling av personuppgifter. Frågan behandlas i avsnitt 17.3.

Av paragrafen framgår att brottsdatalogen och de registerförfattningar som gäller för Polismyndigheten, Säkerhetspolisen, Kustbevakningen respektive Tullverket gäller vid behandling av personuppgifter i internationellt polisiärt samarbete, om det inte

finns avvikande bestämmelser i förevarande lag eller föreskrifter som regeringen har meddelat i anslutning till den. Vidare ändras hänvisningarna till de lagar som byter namn, vilket behandlas i avsnitt 7.1.2, 8.1.2, 9.1.2 och 14.2.2.

7 kap.

1 §

Paragrafen reglerar direktåtkomst till och sökning i referensuppgifter i dna-register. I *tredje stycket* ändras en hänvisning till en lag som byter namn, vilket behandlas i avsnitt 7.1.2. I övrigt är paragrafen oförändrad.

3 §

Paragrafen reglerar direktåtkomst till referensuppgifter i fingeravtrycksregister. Ändringen är av samma slag som i 1 §.

4 §

Paragrafen reglerar sökning i fingeravtrycksregister. Ändringen är av samma slag som i 1 §.

7 §

Paragrafen hänvisar i fråga om skadestånd till bestämmelsen i 7 kap. 1 § brottsdatalagen (2018:000). Den behandlas i avsnitt 17.3. Vad hänvisningen innebär utvecklas i kommentaren till 7 kap. 2 § polisens brottsdatalag (2010:361). Vidare görs en redaktionell ändring.

8 kap.

3 §

Paragrafen hänvisar i fråga om skadestånd till bestämmelsen i 7 kap. 1 § brottsdatalagen (2018:000). Ändringen är av samma slag som i 7 kap. 7 §.

9 kap.

4 §

Paragrafen, som behandlas i avsnitt 17.3, reglerar överföring av personuppgifter som hämtats från VIS till tredjeland eller en internationell organisation.

Första stycket är oförändrat.

Av *andra stycket punkten 4* framgår att bestämmelserna i 8 kap. 1 § brottsdatalagen (2018:000) om överföring av personuppgifter till tredjeland eller internationella organisationer ska vara uppfyllda.

5 §

Paragrafen hänvisar i fråga om skadestånd till bestämmelsen i 7 kap. 2 § brottsdatalagen (2018:000). Ändringen är av samma slag som i 7 kap. 7 §.

10 kap.

1 §

Paragrafen reglerar direktåtkomst till referensuppgifter i fingeravtrycksregistret. Hänvisningen till personuppgiftslagen (1998:204) tas bort och hänvisningen till en lag som byter namn ändras, vilket behandlas i avsnitt 7.1.2.

2 §

Paragrafen reglerar det svenska kontaktställets sökning i amerikanska fingeravtrycksregister och i vilken utsträckning behandling är tillåten. En hänvisning till en lag som byter namn ändras, vilket behandlas i avsnitt 7.1.2.

3 §

Paragrafen hänvisar i fråga om skadestånd till bestämmelsen i 7 kap. 2 § brottsdatalagen (2018:000). Ändringen är av samma slag som i 7 kap. 7 §.

Övergångsbestämmelser

Ikraftträdande- och övergångsbestämmelserna tas upp i avsnitt 18.1 och 18.2.

Punkten 1 föreskriver när lagen ska träda i kraft.

Punkten 2 innebär att bestämmelsen om skadestånd i 48 § personuppgiftslagen fortfarande ska gälla för skada som har orsakats före ikraftträdandet vid behandling av personuppgifter med stöd lagen eller föreskrifter som har meddelats i anslutning till den.

20.23 Förslaget till lag om ändring i brottsdatalagen (2018:000)

2 kap.

4 §

I paragrafen regleras förutsättningarna för att personuppgifter ska få behandlas för ett nytt ändamål inom lagens tillämpningsområde.

I *första stycket* görs endast en redaktionell ändring.

I *andra stycket*, som är nytt och behandlas i avsnitt 6.5, föreskrivs att någon prövning enligt första stycket inte behöver göras i den utsträckning skyldighet att lämna uppgifter följer av lag eller förordning. I de fall där det i lag eller förordning bara föreskrivs en möjlighet, men ingen skyldighet, att lämna personuppgifter ska det

däremot prövas om uppgiftslämnandet är nödvändigt och proportionerligt. En prövning ska också göras innan uppgifter lämnas med stöd av 6 kap. 5 § offentlighets- och sekretesslagen (2009:400).

13 §

Av paragrafen framgår vad som är känsliga personuppgifter. Det tydliggörs att vad som betecknas som känsliga personuppgifter inte enbart gäller enligt lagen, utan även för författningar som gäller utöver brottsdatalagen.

18 §

Den personuppgiftsansvarige är enligt paragrafen skyldig att årligen se över behovet av att fortsätta att behandla personuppgifter för vilka det inte i lag eller författning är föreskrivet hur länge de får behandlas. I paragrafen, som behandlas i avsnitt 5.5.3, tydliggörs att regleringen enbart avser behandling för ändamål inom lagens tillämpningsområde. Det innebär att personuppgifterna får behandlas automatiserat för bl.a. arkivändamål.

21 §

Paragrafen, som är ny och behandlas i avsnitt 5.4.5, reglerar behandling av personuppgifter som är nödvändiga för att framställa rättsstatistiken. Sådana uppgifter ska enligt paragrafen lämnas till den som ansvarar för att framställa sådan statistik. Enligt 2 § förordningen (2016:1201) med instruktion för Brottsförebyggande rådet ansvarar myndigheten för kriminalstatistiken. I 24 kap. 8 § första stycket offentlighets- och sekretesslagen (2009:400) föreskrivs att absolut sekretess gäller för uppgifter om enskilda personliga eller ekonomiska förhållanden i sådan särskild verksamhet hos en myndighet som avser framställning av statistik.

22 §

Paragrafen anger vad som gäller när fråga uppkommer om att behandla personuppgifter, som behandlas med stöd av lagen, för nya ändamål utanför lagens tillämpningsområde.

I *första stycket* ändras hänvisningen till artikel 2.2 d i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning). Av regleringen framgår att dataskyddsförordningen ska tillämpas när en behörig myndighet behandlar personuppgifter för ändamål utanför lagens tillämpningsområde. Det innebär att de förutsättningar för behandling av personuppgifter som anges där, t.ex. att det finns en rättslig grund för behandling enligt artikel 6.1, måste vara uppfyllda för att personuppgifterna ska få behandlas.

Innan personuppgifter som behandlas med stöd av lagen behandlas för ett nytt ändamål utanför lagens tillämpningsområde ska det enligt *andra stycket*, som är nytt, säkerställas att behandlingen är nödvändig och proportionerlig för det ändamålet. I kravet på proportionalitet ligger att skälen för den nya behandlingen ska väga tyngre än det intrång som behandlingen innebär för den enskilde. Det som står att vinna med behandlingen ska alltså vägas mot intrånget i enskildas integritet. Det har också betydelse vilka personuppgifter det är fråga om och för vilket syfte de ska användas. Någon prövning av om behandlingen för det nya ändamålet är förenlig med det ändamål för vilket uppgifterna ursprungligen behandlades behöver däremot inte göras. Ändringen behandlas i avsnitt 6.4.2 och 6.4.3.

I *tredje stycket*, som är nytt och behandlas i avsnitt 6.5, föreskrivs att någon prövning enligt andra stycket inte behöver göras i den utsträckning skyldighet att lämna uppgifter följer av lag eller förordning. I de fall där det i lag eller förordning bara föreskrivs en möjlighet, men ingen skyldighet, att lämna personuppgifter ska det däremot prövas om uppgiftslämnandet är nödvändigt och proportionerligt. En prövning ska också göras i de fall där uppgifter lämnas med stöd av 6 kap. 5 § offentlighets- och sekretesslagen (2009:400).

3 kap.

16 §

I paragrafen, som är ny och behandlas i avsnitt 17.1, regleras dataskyddsbudens tystnadsplikt.

I *första stycket* föreskrivs att ett dataskyddsbud inte obehörigen får röja eller utnyttja det som han eller hon i den rollen har fått veta om enskilds personliga eller ekonomiska förhållanden. Bestämmelsen är tillämplig på den som har utsetts till dataskyddsbud av någon annan aktör än en myndighet eller annat organ som tillämpar offentlighets- och sekretesslagen.

Om dataskyddsbudet har en sådan anställning eller uppdrag som avses i 2 kap. 1 § offentlighets- och sekretesslagen tillämpas i stället den lagen, vilket framgår av *andra stycket*.

6 kap.

1 §

Paragrafen reglerar vid vilka överträdelser sanktionsavgift får tas ut av en personuppgiftsansvarig.

I *första stycket punkten 1* läggs 2 kap. 22 § andra stycket till i uppräkningsen av vilka överträdelser som kan föranleda sanktionsavgift. Ändringen behandlas i avsnitt 6.4.3. Stycket är i övrigt oförändrat.

Andra stycket är oförändrat.

Kommittédirektiv 2016:21

Genomförande av EU:s direktiv om skydd av personuppgifter vid brottsbekämpning, brottmålshandling och straffverkställighet

Beslut vid regeringssammanträde den 17 mars 2016

Sammanfattning

Inom kort förväntas EU besluta om ett direktiv med regler om skydd av personuppgifter när behöriga myndigheter behandlar sådana uppgifter vid brottsbekämpning, brottmålshandling eller straffverkställighet. En särskild utredare ska föreslå hur EU-direktivet ska genomföras i svensk rätt. Utredaren ska bl.a.

- lämna förslag till en ny ramlagstiftning med bestämmelser om skydd av personuppgifter inom direktivets tillämpningsområde,
- lämna de förslag till författningsändringar som krävs för att anpassa vissa centrala författningar om rättsväsendets behandling av personuppgifter till de nya förutsättningarna,
- bedöma om direktivet ger anledning till ny eller ändrad reglering om tillsyn och vid behov lämna författningsförslag,
- bedöma om det finns anledning att reglera Säkerhetspolisens personuppgiftsbehandling separat från den lagstiftning som gäller för Polismyndigheten och vid behov lämna författningsförslag.

Utredaren ska senast den 1 april 2017 i ett delbetänkande redovisa uppdraget i den del det rör dels en ny ramlagstiftning, dels tillsyn inom direktivets tillämpningsområde. Uppdraget ska slutredovisas senast den 30 september 2017.

Den nuvarande regleringen och EU:s dataskyddsreform

Några grundläggande bestämmelser om skydd av personuppgifter vid brottsbekämpning

Grundläggande bestämmelser till skydd för den personliga integriteten finns i regeringsformen. I 1 kap. 2 § första stycket slås det fast att den offentliga makten ska utövas med respekt bl.a. för den enskilda människans frihet och i fjärde stycket anges bl.a. att det allmänna ska värna den enskildes privatliv och familjeliv. Enligt 2 kap. 6 § andra stycket är var och en gentemot det allmänna skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Behandling av personuppgifter i brottsbekämpande myndigheters verksamhet kan typiskt sett falla under bestämmelsen. Inskränkningar i det grundlagsfästa skyddet kan endast göras genom lag och bara under de förutsättningar som anges i 2 kap. regeringsformen.

I EU:s stadga om de grundläggande rättigheterna (EUT C 83, 30.3.2010, s. 389) bekräftas de rättigheter som har sin grund i medlemsstaternas gemensamma författningstraditioner och internationella förpliktelser, Europakonventionen, unionens och Europarådets sociala stadgor samt rättspraxis vid Europeiska unionens domstol och Europeiska domstolen för de mänskliga rättigheterna. Artikel 8 i stadgan reglerar skydd av personuppgifter. Enligt artikeln har var och en rätt till skydd av de personuppgifter som rör honom eller henne. Sådana uppgifter ska behandlas lagenligt för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund. Var och en har rätt att få tillgång till insamlade uppgifter som rör honom eller henne och att få dem rättade. En oberoende myndighet ska kontrollera att reglerna efterlevs.

I detta sammanhang bör även artikel 8 i Europakonventionen nämnas. Enligt artikeln har var och en rätt till respekt för sitt

privat- och familjeliv, sitt hem och sin korrespondens. Med detta avses bl.a. skyddet av personuppgifter. Rättigheten är dock inte absolut. Inskränkningar får göras med stöd av lag och om det är nödvändigt och proportionerligt i ett demokratiskt samhälle med hänsyn till vissa särskilt angivna ändamål, bl.a. förebyggande av oordning och brott.

Den nuvarande EU-regleringen

Den allmänna regleringen om behandling av personuppgifter inom EU finns i dag i Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (dataskyddsdirektivet). Direktivet gäller inte på området för polissamarbete och straffrättsligt samarbete och inte heller på området för nationell säkerhet.

Den nuvarande EU-regleringen i rådets rambeslut 2008/977/RIF av den 27 november 2008 om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete (dataskyddsrambeslutet) är tillämplig på informationsutbyte över gränserna. Dataskyddsrambeslutet är alltså tillämpligt på uppgifter som överförs eller görs tillgängliga mellan medlemsstater eller mellan medlemsstater och EU-organ och vissa informationssystem. Dataskyddsrambeslutet gäller däremot inte för rent nationell personuppgiftsbehandling. Från tillämpningsområdet undantas också personuppgiftsbehandling inom området nationell säkerhet.

Den nuvarande svenska regleringen

Dataskyddsdirektivet har genomförts i svensk rätt huvudsakligen genom personuppgiftslagen (1998:204). Personuppgiftslagen har gjorts generellt tillämplig vilket innebär att den gäller även utanför EU-rättens tillämpningsområde och alltså reglerar behandling av personuppgifter oavsett ändamålet med behandlingen. Personuppgiftslagen är dock subsidiär i förhållande till andra lagar och förordningar. Inom flera områden, bl.a. när det gäller brottsbekämpning, finns särlagstiftning i s.k. registerförfattningar som helt eller delvis ersätter personuppgiftslagen. När särregleringen helt ersätter

personuppgiftslagen, görs som regel hänvisningar till vissa paragrafer i lagen som ändå ska gälla. Sådana hänvisningar görs ofta till personuppgiftslagens bestämmelser om bl.a. information till den registrerade, rättelser, säkerheten vid behandling, överföring av personuppgifter till tredjeland, tillsynsmyndighetens befogenheter och skadestånd.

Vid genomförandet av dataskyddsrambeslutet bedömdes merparten av rambeslutets artiklar motsvaras av bestämmelser i svensk rätt, dels i personuppgiftslagen, dels i berörda myndigheters registerförfattningar. De kompletterande bestämmelser som krävdes genomfördes i en särskild lag, lagen (2013:329) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen.

EU:s dataskyddsreform

Inom kort väntas en ny EU-förordning antas om skydd för enskilda personer med avseende på behandling av personuppgifter och det fria flödet av sådana uppgifter (nedan dataskyddsförordningen).¹ Samtidigt väntas ett nytt EU-direktiv antas om skydd för enskilda personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, utreda, upptäcka eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter (nedan det nya dataskyddsdirektivet).²

Dataskyddsförordningen utgör en ny generell reglering för personuppgiftsbehandling inom EU och kommer att ersätta dataskyddsdirektivet från år 1995. Den börjar tillämpas två år räknat från den tjugonde dagen efter publicering i Europeiska unionens officiella tidning. Det huvudsakliga syftet med förordningen är att ytterligare harmonisera och effektivisera skyddet för personuppgifter för att förbättra den inre marknadens funktion och öka enskildas kontroll över sina personuppgifter.

Från dataskyddsförordningens tillämpningsområde undantas bl.a. personuppgiftsbehandling som utförs av behöriga myndig-

¹ Kommittédirektiven utgår från den version av förslaget som finns i dok 5455/16 av den 28 januari 2016.

² Kommittédirektiven utgår från den version av förslaget som finns i dok 5463/16 av den 28 januari 2016.

heter i syfte att förebygga, utreda, upptäcka eller lagföra brott eller verkställa straff, inkluderande skydd mot samt förebyggande av hot mot den allmänna säkerheten. Den personuppgiftsbehandling som görs för dessa syften faller i stället under det nya dataskyddsdirektivets tillämpningsområde. Direktivet ska dels skydda fysiska personers grundläggande fri- och rättigheter, särskilt deras rätt till skydd av personuppgifter, dels underlätta det informationsutbyte mellan behöriga myndigheter som är nödvändigt enligt unionsrätt eller nationell rätt.

Från både förordningens och direktivets tillämpningsområden undantas personuppgiftsbehandling i verksamhet som inte omfattas av unionsrätten, däribland området nationell säkerhet.

EU:s dataskyddsreform kommer att kräva en bred översyn av svenska författningar om personuppgiftsbehandling. Bland övrigt utredningsarbete bör nämnas att en särskild utredare har i uppdrag att föreslå de anpassningar och kompletterande författningsbestämmelser på generell nivå som dataskyddsförordningen ger anledning till (dir. 2016:15). Den utredningen syftar till att säkerställa att det finns en ändamålsenlig och välbalanserad kompletterande nationell reglering om personuppgiftsbehandling när förordningen börjar tillämpas.

Uppdraget att föreslå hur EU-direktivet ska genomföras i svensk rätt

En väl avvägd balans är nödvändig mellan å ena sidan skyddet för den personliga integriteten och å andra sidan samhällets krav på att brott förebyggs och förhindras, att brott utreds och att personer som begår brott lagförs. Den svenska regleringen om skydd av personuppgifter inom direktivets tillämpningsområde har i stor utsträckning nyligen moderniserats och bedömts ändamålsenlig. En avvägning mellan olika intressen har då gjorts. En allmän utgångspunkt för uppdraget är därför att utredaren ska sträva efter principiella lösningar som ansluter till nuvarande systematik i bl.a. polisdatlagen (2010:361), åklagardatalagen (2015:433) och domstolsdatalagen (2015:728). Även i övrigt ska utredaren så långt det är lämpligt och möjligt sträva efter principiella lösningar som är förenliga med gällande författningar och systematik. Vid utformningen av de författningsförslag som lämnas ska utredaren beakta EU:s

stadga om de grundläggande rättigheterna och de internationella konventioner på området som Sverige är förpliktat att följa. Liksom vid all lagstiftning ska enkelhet, överskådlighet och konsekvens eftersträvas för det samlade regelverket om skydd av personuppgifter. I detta ligger också att förslagen så långt som möjligt ska vara kostnadseffektiva.

Direktivet kommer att vara ett resultat av förhandlingar och kompromisser i och mellan kommissionen, rådet och Europaparlamentet, vilket kan medföra oklarheter och otydligheter i text och systematik. Utredaren ska därför eftersträva att innebörden av direktivet vid behov förklaras och tydliggörs.

En ny ramlagstiftning för skydd av personuppgifter vid brottbekämpning, brottmålshantering och straffverkställighet

Det nya dataskyddsdirektivet innehåller ett antal bestämmelser som innebär förpliktelser för medlemsstaterna. Medlemsstaterna ska vidta de åtgärder som är nödvändiga för att följa bestämmelserna i direktivet.

I förhållande till nuvarande svensk reglering innehåller direktivet en delvis ny eller mer detaljerad reglering om rättigheter för enskilda och om skyldigheter för personuppgiftsansvariga eller biträden när det gäller bl.a. datasäkerhet, dokumentation och loggning, konsekvensanalyser och förhandssamråd med tillsynsmyndighet och regler om underrättelser vid s.k. personuppgiftsincidenter.

Direktivet innehåller också regler som anpassats för rättsaktens tillämpningsområde om överföring av personuppgifter till tredjeland och internationella organisationer. Även när det gäller uppgifter och befogenheter för en tillsynsmyndighet innehåller direktivet särskilt anpassade bestämmelser.

Enligt direktivet har enskilda vissa rättigheter, bl.a. att vända sig till en tillsynsmyndighet med klagomål, att få tillgång till rättsmedel både mot tillsynsmyndighetens beslut och mot åtgärder av en personuppgiftsansvarig eller biträde samt att få ersättning av ansvariga som inte lever upp till direktivets krav. Direktivet förpliktar även medlemsstater att föreskriva regler om påföljder eller sanktioner vid överträdelser av bestämmelser som genomför direktivet.

Direktivets tillämpningsområde omfattar personuppgiftsbehandling som utförs av behöriga myndigheter i syfte att förebygga,

utreda, upptäcka eller lagföra brott eller verkställa straff, inkluderande skydd mot samt förebyggande av hot mot den allmänna säkerheten. Det finns behov av att utifrån svenska förhållanden analysera och beskriva direktivets tillämpningsområde. Det behöver bl.a. analyseras i vilken utsträckning även personuppgiftsbehandling vid andra myndigheter än dem som ingår i rättskedjan, exempelvis Statens institutionsstyrelse och Rättsmedicinalverket, omfattas av direktivets förpliktelser.

Som framgått är det personuppgiftslagen som i dag i huvudsak innehåller reglering av motsvarande slag som det nya dataskyddsdirektivet kräver. När den nya dataskyddsförordningen börjar tillämpas kommer dock personuppgiftslagen och föreskrifter i anslutning till den lagen att behöva upphävas. Det regelverk som ersätter personuppgiftslagen – förordningen och kompletterande nationella bestämmelser – är inte anpassat till de särskilda förutsättningar som gäller för personuppgiftsbehandling inom området för brottsbekämpning, brottmålshantering och straffverkställighet. Det bedöms emellertid fortfarande vara lämpligt med ett så långt som möjligt gemensamt regelverk om behandling av personuppgifter för de myndigheter som bedriver verksamhet inom det aktuella området. Det behövs därför en ny svensk ramlagstiftning för skydd av personuppgifter inom direktivets tillämpningsområde och att utredaren utgår från detta vid analyser, bedömningar och förslag.

Efter en analys av direktivets tillämpningsområde är det möjligt att utredaren bedömer att myndigheter som för närvarande inte omfattas av särreglering i registerförfattningar kommer att omfattas av direktivets krav. Det finns därför anledning att i första hand undersöka om den nya ramlagstiftningen kan utformas på ett sätt som inte förutsätter att det tas fram nya, kompletterande, registerförfattningar för sådana myndigheter.

Det behöver analyseras hur direktivets förpliktelser förhåller sig till svensk rätt. Förutom en övergripande analys avseende förhållandet till svensk reglering av personuppgiftsbehandling inom direktivets tillämpningsområde, behöver analysen omfatta förhållandet till nationell reglering avseende sekretess och arkiv liksom förvaltningsrätt, processrätt och skadeståndsrätt. Behovet av analys omfattar exempelvis frågan om hur direktivets utrymme för begränsningar av enskildas rätt till information eller tillgång till sina

egna personuppgifter förhåller sig till svensk sekretessreglering och hur möjligheterna att anpassa tidpunkten för den enskildes utövande av rätten till insyn förhåller sig till nationella straff-processuella bestämmelser.

Direktivet innehåller en bestämmelse om att dataskyddsrambeslutet ska upphävas. Frågan är vilka konsekvenser det får för den svenska lagstiftning som delvis genomförde rambeslutet, lagen med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen.

Utredaren ska alltså

- analysera och beskriva direktivets tillämpningsområde,
- analysera hur svensk rätt förhåller sig till direktivets förpliktelser,
- bedöma i vilka avseenden ny eller ändrad författningsreglering krävs för att Sverige ska leva upp till förpliktelserna,
- lämna förslag till en ny ramlagstiftning för skydd av personuppgifter inom direktivets tillämpningsområde,
- ta ställning till om lagen med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen bör upphävas och vid behov lämna förslag till författningsändringar, och
- om det behövs, lämna förslag till författningsändringar även på andra områden än den reglering som närmast rör personuppgiftsbehandling.

Hur behöver centrala författningar om rättsväsendets personuppgiftsbehandling anpassas?

Inom det nya dataskyddsdirektivets tillämpningsområde hanterar rättsväsendet en stor mängd information som innebär behandling av personuppgifter. Ett antal författningar är i detta avseende av central betydelse. Det gäller polisdatalagen, lagen (1999:90) om behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar, lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet, kustbevakningsdatalagen (2012:145), åklagardatalagen, domstolsdatalagen och lagen (2001:617) om

behandling av personuppgifter inom kriminalvården. De berörda lagarna kompletteras av förordningar.

Det krävs en närmare analys och bedömning av i vilken utsträckning direktivets förpliktelser medför behov av ändringar av de angivna lagarna och de tillhörande förordningarna. Det kommer också att krävas en anpassning av de angivna författningarna med anledning av en ny ramlagstiftning för skydd av personuppgifter inom direktivets tillämpningsområde när personuppgiftslagen upphävs.

Utredaren ska därför

- analysera och bedöma behovet av författningsändringar för att anpassa de angivna författningarna till direktivets förpliktelser och de nya förutsättningarna för regleringen, och
- lämna förslag till författningsändringar.

Inom direktivets tillämpningsområde berörs, utöver de angivna lagarna och förordningarna, även andra författningar av direktivets förpliktelser eller andra delar av EU:s dataskyddsreform. Det gäller t.ex. lagen (1998:620) om belastningsregister och lagen (1998:621) om misstankeregister. Det ligger dock inte inom ramen för utredarens uppdrag att se över behovet av ändringar när det gäller de lagarna eller andra författningar som inte har angetts här.

Personuppgiftsbehandling vid tillhandahållande av information – bör även dataskyddsförordningens reglering kompletteras?

Polismyndigheten, Skatteverket, Tullverket, Kustbevakningen, åklagarväsendet, domstolsväsendet och Kriminalvården kommer att tillämpa regleringen i dataskyddsförordningen när de behandlar personuppgifter i verksamhet som utförs i annat syfte än att bekämpa brott, hantera brottmål eller verkställa straff. Som en utgångspunkt ingår det inte i utredarens uppdrag att se över eller lämna förslag till förändringar av författningar inom förordningens tillämpningsområde. Det gäller även i den utsträckning t.ex. kustbevakningsdatalagen eller domstolsdatalagen reglerar behandling av personuppgifter inom förordningens tillämpningsområde.

Enligt det nya dataskyddsdirektivets artikel 7a ska personuppgifter som samlas in av behöriga myndigheter i syfte att

bekämpa brott, hantera brottmål eller verkställa straff inte därefter behandlas för andra ändamål än de som ryms inom direktivets tillämpningsområde, om inte sådan behandling är tillåten enligt unionsrätten eller nationell rätt. I sådana fall ska dataskyddsförordningen tillämpas på denna behandling, om inte behandlingen utförs som ett led i en verksamhet som inte omfattas av unionsrätten. Förordningens reglering tillämpas alltså redan vid tillhandahållandet när t.ex. uppgifter som samlats in under en förundersökning överförs för ändamål som faller utanför direktivets tillämpningsområde. Enligt den nuvarande svenska regleringen finns bestämmelser som reglerar tillåtligheten av behandling för sådant tillhandahållande, s.k. sekundära ändamål, i den författning som reglerar myndighetens behandling av personuppgifter för brottsbekämpande ändamål (se t.ex. 2 kap. 8 § polisdatalagen).

Förordningen ger ett visst utrymme för medlemsstaterna att behålla eller införa mer specifika bestämmelser om hur bestämmelserna i förordningen ska tillämpas (förordningens artikel 6.2 a). Det krävs en analys och bedömning av i vilken utsträckning det är möjligt och lämpligt att utnyttja förordningens utrymme att behålla eller införa specifik reglering i svensk rätt som tar sikte på den typ av situation som beskrivits.

Utredaren ska därför

- analysera om det finns utrymme för och behov av att inom förordningens tillämpningsområde införa eller behålla specifik reglering i svensk rätt om behandling av personuppgifter för tillhandahållande av information, och
- vid behov föreslå författningsändringar.

Hur behöver reglerna om tillsyn anpassas?

Tillsyn över behandling av personuppgifter inom det nya dataskyddsdirektivets tillämpningsområde utövas i dag av Datainspektionen. Säkerhets- och integritetsskyddsnämnden har också ett tillsynsuppdrag och granskar bl.a. brottsbekämpande myndigheters användning av hemliga tvångsmedel och polisens personuppgiftsbehandling. Att Datainspektionens tillsyn kompletteras med tillsyn av en myndighet med särskild uppgift att utöva tillsyn över personuppgiftsbehandling i bl.a. polisens brottsbekämpande verksamhet

har ansetts innebära möjligheter att inrikta tillsynen på de områden som kan ge upphov till särskilda risker från integritetssynpunkt (prop. 2009/10:85 s. 273 f.).

Det nya dataskyddsdirektivet innehåller flera bestämmelser som rör tillsyn, bl.a. tillsynsmyndighetens befogenheter. Det ligger i utredarens uppdrag att föreslå hur direktivets förpliktelser ska genomföras även när det gäller bestämmelserna om tillsyn. Det finns dock några frågor om tillsyn som inte ingår i uppdraget på grund av att de omhändertas av andra utredningar.

Utredningen om tillsynen över den personliga integriteten (Ju 2015:02), som ska redovisa sitt uppdrag senast den 30 september 2016, ska bl.a. lämna de förslag som behövs för att den myndighet för tillsyn som utredningen kommer att föreslå ska kunna fullgöra de uppgifter som den nu aktuella EU-reformen medför. Det får därför anses ligga inom ramen för det uppdraget att omhänderta vissa frågor om genomförandet av direktivet. Hit hör frågor om anpassning till direktivets förpliktelser avseende organisation, utnämningen respektive avsättandet av medlemmar samt resurser och anknytande frågor för den myndigheten. Dessa frågor ingår alltså inte i utredarens uppdrag.

Det ligger vidare inom ramen för uppdraget för den särskilda utredare som har i uppdrag att föreslå anpassningar på generell nivå som förordningen ger anledning till att bl.a. analysera om det finns behov av författningsändringar med avseende på tystnadsplikt hos tillsynsmyndigheten till skydd för enskild. Eftersom direktivets krav i denna del överensstämmer med förordningens ingår inte heller denna fråga i utredarens uppdrag.

Med en utgångspunkt i att Säkerhets- och integritetsskyddsnämnden även i fortsättningen utövar tillsyn inom direktivets tillämpningsområde finns det behov av att också med avseende på nämnden se över om och i vilken utsträckning en ny reglering eller ändringar i svensk rätt krävs med anledning av direktivets förpliktelser. Detta ingår i sin helhet i utredarens uppdrag.

Utredaren ska alltså, med undantag för de frågor som angetts ingå i andra utredningars uppdrag,

- analysera och bedöma om direktivet föranleder behov av ny eller ändrad reglering om tillsyn, och
- vid behov föreslå författningsändringar.

Uppdraget att bedöma hur Säkerhetspolisens personuppgiftsbehandling bör regleras

Den 1 januari 2015 ombildades Säkerhetspolisen till en fristående myndighet. Regleringen av Säkerhetspolisens behandling av personuppgifter har anpassats till de nya förhållandena (se prop. 2014/15:94), men myndighetens behandling av personuppgifter regleras fortfarande i polisdatalagen med tillhörande förordning.

EU:s dataskyddsreform kommer att medföra ett förändrat regelverk för nationell personuppgiftsbehandling. Samtidigt är centrala delar av Säkerhetspolisens verksamhet av sådant slag att unionsrätten inte är tillämplig.

De förändringar i nationell rätt som föranleds av EU:s dataskyddsreform innebär att det behövs en analys och bedömning av på vilket sätt Säkerhetspolisens personuppgiftsbehandling bör regleras och om det finns skäl att separera den regleringen från polisdatalagstiftningen. En utgångspunkt för utredarens analys och bedömning ska vara att regleringen av Säkerhetspolisens personuppgiftsbehandling nyligen har moderniserats och bedömts ändamålsenlig. Så långt det är lämpligt och möjligt ska principiella lösningar som är förenliga med gällande författningar och systematik eftersträvas om författningsförslag lämnas.

Utredaren ska

- analysera och bedöma hur Säkerhetspolisens personuppgiftsbehandling bör regleras och om regleringen bör separeras från den lagstiftning som gäller för Polismyndigheten, och
- vid behov föreslå författningsändringar.

Konsekvensbeskrivningar

Utredaren ska bedöma de ekonomiska konsekvenserna av förslagen. Om förslagen kan förväntas leda till kostnadsökningar för det allmänna ska utredaren föreslå hur dessa ska finansieras. Utredaren ska också redovisa förslagets konsekvenser för brottsbekämpningen och för den personliga integriteten.

Samråd och redovisning av uppdraget

Utredaren ska hålla sig väl informerad om och beakta relevant arbete som bedrivs inom Regeringskansliet, utredningsväsendet och EU. Vid anpassningen av svensk rätt till den nya EU-regleringen bör en enhetlig tolkning av regelverket eftersträvas. Utredaren ska därför följa och i lämplig omfattning samråda med utredningen som har i uppdrag att föreslå anpassningar på generell nivå som dataskyddsförordningen ger anledning till och Utredningen om tillsynen över den personliga integriteten.

Samråd är särskilt viktigt i processuella frågor och frågor som rör sanktioner, tillsynsmyndigheten och arkivering. Utredaren ska också, i den utsträckning det bedöms lämpligt, hålla sig informerad om och samråda med övriga utredningar som har i uppdrag att anpassa svensk rätt till reformen av EU:s dataskyddsregelverk. Under genomförandet av uppdraget ska utredaren även ha en dialog med och inhämta upplysningar från de myndigheter som kan vara berörda av aktuella frågor.

Utredaren är fri att ta upp och lämna förslag i näraliggande frågor som aktualiseras under utredningsuppdraget men som inte rör genomförandet av eller anpassningen av svensk rätt till EU:s dataskyddsreform.

Uppdraget att föreslå hur direktivet ska genomföras ska redovisas genom ett delbetänkande senast den 1 april 2017 i den del det rör dels en ny ramlagstiftning för skydd av personuppgifter vid brottsbekämpning, brottmålshantering och straffverkställighet, dels tillsyn inom direktivets tillämpningsområde. Uppdraget ska slutredovisas senast den 30 september 2017.

(Justitiedepartementet)

Statens offentliga utredningar 2017

Kronologisk förteckning

1. För Sveriges landsbygder
– en sammanhållen politik för
arbete, hållbar tillväxt och välfärd. N.
2. Kraftsamling för framtidens energi. M.
3. Karens för statsråd och statssekreterare.
Fi.
4. För en god och jämlik hälsa.
En utveckling av det
folkhälsopolitiska ramverket. S.
5. Svensk social trygghet i en
globaliserad värld. Del 1 och 2. S.
6. Se barnet! Ju.
7. Straffprocessens ramar och
domstolens beslutsunderlag
i brottmål – en bättre hantering av
stora mål. Ju.
8. Kunskapsläget på kärnavfallsområdet 2017.
Kärnavfallet – en fråga i ständig
förändring. M.
9. Det handlar om oss.
– unga som varken arbetar eller studerar. U.
10. Ny ordning för att främja god sed
och hantera oredlighet i forskning. U.
11. Vägs katt. Volym 1 och 2. Fi.
12. Att ta emot människor på flykt.
Sverige hösten 2015. Ju.
13. Finansiering av infrastruktur med
privat kapital? Fi.
14. Migrationsärendena
vid utlandsmyndigheterna. Ju.
15. Kvalitet och säkerhet
på apoteksmarknaden. S.
16. Sverige i Afghanistan 2002–2014. UD.
17. Om oskuldspresumtionen och rätten att
närvara vid rättegången. Genomförande
av EU:s oskuldspresumtionsdirektiv. Ju.
18. En nationell strategi för validering. U.
19. Uppdrag: Samverkan. Steg på vägen
mot fördjupad lokal samverkan
för unga arbetslösa. A.
20. Tillträde för nybörjare – ett öppnare
och enklare system för tillträde till
högskoleutbildning. U.
21. Läs mig! Nationell kvalitetsplan för
vård och omsorg om äldre personer.
Del 1 och 2. S.
22. Från värdekedja till värdecykel – så får
Sverige en mer cirkulär ekonomi. M.
23. digitalforvaltning.nu. Fi.
24. Ett arbetsliv i förändring – hur
påverkas ansvaret för arbetsmiljön? A.
25. Samlad kunskap – stärkt
handläggning. S.
26. Delningsekonomi. På användarnas
villkor. Fi.
27. Vissa frågor inom fastighets- och
stämpelskatteområdet. Fi.
28. Ett nationellt centrum för kunskap
om och utvärdering av arbetsmiljö. A.
29. Brottstatalag. Ju
30. En omreglerad spelmarknad.
Del 1 och 2. Fi.
31. Stärkt konsumentskydd
på bostadsrättsmarknaden. Ju.
32. Substitution i Centrum
– stärkt konkurrenskraft med
kemikaliesmarta lösningar. M.
33. Stärkt ställning för hyresgäster. Ju.
34. Ekologisk kompensation – Åtgärder
för att motverka nettoförluster av
biologisk mångfald och ekosystem-
tjänster, samtidigt som behovet av
markexploatering tillgodoses. M.
35. Samling för skolan. Nationell strategi
för kunskap och likvärdighet. U.
36. Informationssäkerhet för samhälls-
viktiga och digitala tjänster. Ju.
37. Kvalificerad välfärdsbrottslighet
– förebygga, förhindra, upptäcka och
beivra. Ju.

38. Kvalitet i välfärden – bättre upphandling och uppföljning. Fi.
39. Ny dataskyddslag. Kompletterande bestämmelser till EU:s dataskyddsförordning. Ju.
40. För dig och för alla. S.
41. Meddelarskyddslagen – fler verksamheter med stärkt meddelarskydd. Ju.
42. Vem har ansvaret? M.
43. På lika villkor! Delaktighet, jämlikhet och effektivitet i hjälpmedelsförsörjningen. S.
44. Entreprenad, fjärrundervisning och distansundervisning. U.
45. Ny lag om företagsshemligheter. Ju.
46. Stärkt ordning och säkerhet i domstol. Ju.
47. Nästa steg på vägen mot en mer jämlik hälsa. Förslag för ett långsiktigt arbete för en god och jämlik hälsa. S.
48. Kunskapsbaserad och jämlik vård. Företsättningar för en lärande hälso- och sjukvård. S.
49. EU:s dataskyddsförordning och utbildningsområdet. U.
50. Personuppgiftsbehandling för forskningsändamål. U.
51. Utbildning, undervisning och ledning – reformvård till stöd för en bättre skola. U.
52. Så stärker vi den personliga integriteten. Ju.
53. God och nära vård. En gemensam färdplan och målbild. S.
54. Fler nyanlända elever ska uppnå behörighet till gymnasiet. U.
55. En ny kamerabevakningslag. Ju.
56. Jakten på den perfekta ersättningsmodellen. Vad händer med medarbetarnas handlingsutrymme? Fi.
57. Lag om flygpassageraruppgifter i brottsbekämpningen. Ju.
58. Amerikansk inresekontroll vid utresa från Sverige – så kan avtalen genomföras. Ju.
59. Reglering av alkoglass m.fl. produkter. S.
60. Nästa steg? Förslag för en stärkt minoritetspolitik. Ku.
61. Villkorlig frigivning – förstärkta åtgärder mot återfall i brott. Ju.
62. Kärnavfallsrådets yttrande över SKB:s Fud-program 2016. M.
63. Miljötillsyn och sanktioner – en tillsyn präglad av ansvar, respekt och enkelhet. M.
64. Detaljplanekravet. N.
65. Hyran vid nyproduktion – en utvärdering och utveckling av modellen med presumtionshyra. Ju.
66. Dataskydd inom Socialdepartementets verksamhetsområde – en anpassning till EU:s dataskyddsförordning. S.
67. Våldsbejakande extremism. En forskarantologi. Ku.
68. Barnets rättigheter i ett straffrättsligt förfarande m.m. Genomförande av EU:s barnrättsdirektiv och två andra straffprocessuella frågor. Ju.
69. Marknadskontrollmyndigheter – befogenheter och sanktionsmöjligheter. UD.
70. Förstärkt skydd för uppgifter av betydelse för ett internationellt samarbete för fred och säkerhet som Sverige deltar i. Ju.
71. Bostäder på statens mark – en möjlighet? N.
72. Genomförande av vissa straffrättsliga åtaganden för att förhindra och bekämpa terrorism. Ju.
73. En gemensam bild av bostadsbyggnadsbehovet. N.
74. Brottsdatalag – kompletterande lagstiftning. Ju.

Statens offentliga utredningar 2017

Systematisk förteckning

Arbetsmarknadsdepartementet

- Uppdrag: Samverkan. Steg på vägen mot fördjupad lokal samverkan för unga arbetslösa. [19]
- Ett arbetsliv i förändring – hur påverkas ansvaret för arbetsmiljön? [24]
- Ett nationellt centrum för kunskap om och utvärdering av arbetsmiljö. [28]

Finansdepartementet

- Karens för statsråd och statssekreterare. [3]
- Vägs katt. Volym 1 och 2. [11]
- Finansiering av infrastruktur med privat kapital? [13]
- digitalforvaltning.nu. [23]
- Delningsekonomi. På användarnas villkor. [26]
- Vissa frågor inom fastighets- och stämpel-skatteområdet. [27]
- En omreglerad spelmarknad. Del 1 och 2. [30]
- Kvalitet i välfärden – bättre upphandling och uppföljning. [38]
- Jakten på den perfekta ersättningsmodellen. Vad händer med medarbetarnas handlingsutrymme? [56]

Justitiedepartementet

- Se barnet! [6]
- Straffprocessens ramar och domstolens beslutsunderlag i brottmål – en bättre hantering av stora mål. [7]
- Att ta emot människor på flykt. Sverige hösten 2015. [12]
- Migrationsärenden vid utlandsmyndigheterna. [14]
- Om oskuldspresumtionen och rätten att närvara vid rättegången. Genomförande av EU:s oskuldspresumtionsdirektiv. [17]

- Brottsdatalag. [29]
- Stärkt konsumentskydd på bostadsrättsmarknaden. [31]
- Stärkt ställning för hyresgäster. [33]
- Informationssäkerhet för samhällsviktiga och digitala tjänster. [36]
- Kvalificerad välfärdsbrottslighet – förebygga, förhindra, upptäcka och beivra. [37]
- Ny dataskyddslag. Kompletterande bestämmelser till EU:s dataskyddsförordning. [39]
- Meddelarskyddslagen – fler verksamheter med stärkt meddelarskydd. [41]
- Ny lag om företagshemligheter. [45]
- Stärkt ordning och säkerhet i domstol. [46]
- Så stärker vi den personliga integriteten. [52]
- En ny kamerabevakningslag. [55]
- Lag om flygpassageraruppgifter i brottsbekämpningen. [57]
- Amerikansk inresekontroll vid utresa från Sverige – så kan avtalen genomföras. [58]
- Villkorlig frigivning – förstärkta åtgärder mot återfall i brott. [61]
- Hyran vid nyproduktion – en utvärdering och utveckling av modellen med presumtionshyra. [65]
- Barnets rättigheter i ett straffrättsligt förfarande m.m. Genomförande av EU:s barnrättsdirektiv och två andra straffprocessuella frågor. [68]
- Förstärkt skydd för uppgifter av betydelse för ett internationellt samarbete för fred och säkerhet som Sverige deltar i. [70]
- Genomförande av vissa straffrättsliga åtaganden för att förhindra och bekämpa terrorism. [72]

Brottsdatalog – kompletterande lagstiftning. [74]

Kulturdepartementet

Nästa steg? Förslag för en stärkt minoritetspolitik. [60]

Våldsbejakande extremism.
En forskarantologi. [67]

Miljö- och energidepartementet

Kraftsamling för framtidens energi. [2]

Kunskapsläget på kärnavfallsområdet 2017.
Kärnavfallet – en fråga i ständig förändring. [8]

Från värdekedja till värdecykel – så får Sverige en mer cirkulär ekonomi. [22]

Substitution i Centrum
– stärkt konkurrenskraft med kemikaliesmarta lösningar. [32]

Ekologisk kompensation – Åtgärder för att motverka nettoförluster av biologisk mångfald och ekosystemtjänster, samtidigt som behovet av markexploatering tillgodoses. [34]

Vem har ansvaret? [42]

Kärnavfallsrådets yttrande över SKB:s Fud-program 2016. [62]

Miljötillsyn och sanktioner
– en tillsyn präglad av ansvar, respekt och enkelhet. [63]

Näringsdepartementet

För Sveriges landsbygder
– en sammanhållen politik för arbete, hållbar tillväxt och välfärd. [1]

Detaljplanekravet. [64]

Bostäder på statens mark
– en möjlighet? [71]

En gemensam bild av bostadsbyggnadsbehovet. [73]

Socialdepartementet

För en god och jämlik hälsa.
En utveckling av det folkhälsopolitiska ramverket. [4]

Svensk social trygghet i en globaliserad värld. Del 1 och 2. [5]

Kvalitet och säkerhet
på apoteksmarknaden. [15]

Läs mig! Nationell kvalitetsplan
för vård och omsorg om äldre personer.
Del 1 och 2. [21]

Samlad kunskap – stärkt handläggning. [25]
För dig och för alla. [40]

På lika villkor! Delaktighet, jämlikhet och effektivitet i hjälpmedelsförsörjningen. [43]

Nästa steg på vägen mot en mer jämlik hälsa.
Förslag för ett långsiktigt arbete för en god och jämlik hälsa. [47]

Kunskapsbaserad och jämlik vård.
Förutsättningar för en lärande hälso- och sjukvård. [48]

God och nära vård. En gemensam färdplan och målbild. [53]

Reglering av alkoglass m.fl. produkter. [59]

Dataskydd inom Socialdepartementets verksamhetsområde – en anpassning till EU:s dataskyddsförordning. [66]

Utbildningsdepartementet

Det handlar om oss.
– unga som varken arbetar eller studerar. [9]

Ny ordning för att främja god sed och hantera oredlighet i forskning. [10]

En nationell strategi för validering [18]

Tillträde för nybörjare – ett öppnare och enklare system för tillträde till högskoleutbildning. [20]

Samling för skolan.
Nationell strategi för kunskap och likvärdighet. [35]

Entreprenad, fjärrundervisning och distansundervisning. [44]

EU:s dataskyddsförordning och utbildningsområdet. [49]

Personuppgiftsbehandling
för forskningsändamål. [50]

Utbildning, undervisning och ledning
– reformvård till stöd för en bättre skola. [51]

Fler nyanlända elever ska uppnå behörighet
till gymnasiet. [54]

Utrikesdepartementet

Sverige i Afghanistan 2002–2014. [16]

Marknadskontrollmyndigheter
– befogenheter och
sanktionsmöjligheter. UD. [69]