Integritetsskyddsmyndigheten

Regeringskansliet, Socialdepartementet

Diarienummer:
IMY-2022-680

Ert diarienummer:
S2022/00436

Datum:
2022-06-22

Yttrande över slutbetänkandet Träffsäkert (SOU 2021:101)

Integritetsskyddsmyndigheten (IMY) har granskat förslaget huvudsakligen utifrån myndighetens uppgift att arbeta för att människors grundläggande fri- och rättigheter skyddas i samband med behandling av personuppgifter.

IMY lämnar följande synpunkter.

IMY anser att analysen om förslagens inverkan på den enskildes personliga integritet är kortfattad. Utredningen konstaterar att förslagen innebär en utökad behandling av personuppgifter och ”att de personuppgifter som omfattas av direktåtkomst inte är utan integritetskänslighet, men är inte heller av det särskilt känsliga slaget”.[1] Utredningen för också ett resonemang om vilken skillnad som finns mellan direktåtkomst och så kallade ”fråga/svar-tjänster”. Utredningen påpekar i det sammanhanget att det finns en rättslig skillnad mellan direktåtkomst och andra former av elektroniskt utlämnande.

IMY vill i detta sammanhang framhålla att användning av så kallade ”fråga/svar-tjänster” kan innebära samma typ av problematik som direktåtkomst utifrån ett integritetsperspektiv, eftersom den utlämnande myndigheten inte i varje enskilt fall tar ställning till utlämnandet av personuppgifterna. IMY påpekade denna problematik i remissyttrandet avseende betänkandet Myndighetsdatalag (SOU 2015:39). Yttrandet bifogas.

Oavsett vad man väljer att kalla möjligheten för en myndighet att bereda sig tillgång till personuppgifter hos en annan myndighet behöver en integritetsanalys av behandlingen göras. I samband med detta kan exempelvis de risker som tillgången till personuppgifter medför reduceras med skydds- och säkerhetsåtgärder reglerade i författning, såsom sökbegränsningar och skydd mot massuthämtningar. IMY efterfrågar därför en djupare analys i det fortsatta beredningsarbetet av de risker som den föreslagna behandlingen kan komma att innebära och de eventuella åtgärder som behöver vidtas i författning för att säkerställa skyddet för de registrerades grundläggande fri- och rättigheter.

Detta yttrande har beslutats av den tillförordnade enhetschefen Linn Sandmark efter föredragning av juristen Mattias Sandström. Vid den slutliga handläggningen har även juristen Ulrika Harnesk medverkat.

Linn Sandmark, 2022-06-22 (Det här är en elektronisk signatur)

[1] SOU 2021:101 s. 279.

Postadress:
Box 8114
104 20 Stockholm

Webbplats:
www.imy.se

E-post:
imy@imy.se

Telefon:
08-657 61 00

Justitiedepartementet
Grundlagsenheten
103 33 STOCKHOLM

Betänkandet Myndighetsdatalag (SOU 2015:39)

Datainspektionen har granskat remissen huvudsakligen utifrån sin uppgift att verka för att människor skyddas mot att deras personliga integritet kränks genom behandling av personuppgifter.

Inspektionen lämnar följande synpunkter.

Inledning

Utredningen har på ett ambitiöst, noggrant och överlag pedagogiskt sätt utfört sitt omfattande uppdrag. Datainspektionen vill bland annat framhålla den förtjänstfulla genomgång av registerlagstiftningsområdet som utredningen gjort i avsnitt 4 och på det hela taget avsnitt 5, där utredningen behandlar det inom e-förvaltningen centrala begreppet direktåtkomst. Även avsnitten som berör de materiella bestämmelserna i den föreslagna myndighetsdatalagen är, som helhet, omsorgsfullt hanterade.

Datainspektionen har dock synpunkter och invändningar, både av principiell och mer praktisk natur, mot delar av utredningens bedömningar och förslag. I vissa väsentliga delar avstyrker inspektionen de förslag som lämnas.

Enskilda individer ges enligt artikel 8 i Europakonventionen rätt till skydd för sitt privatliv och i artikel 8 i EU:s rättighetsstadga anges att var och en har rätt till skydd av de personuppgifter som rör honom eller henne. Inom EU skyddas denna rätt genom bland annat dataskyddsdirektivet (95/46/EG), som syftar till att garantera en hög och i alla medlemsstater likvärdig nivå när det gäller enskildas personliga fri- och rättigheter med avseende på behandling av personuppgifter. Direktivet har i svensk rätt i första hand införts genom personuppgiftslagen.

Den föreslagna myndighetsdatalagen ska i stor utsträckning ersätta personuppgiftslagen och den kan sägas bygga på principen att myndigheters personuppgiftsbehandling är tillåten om den behövs för verksamheten, men att det ska vara möjligt att i lag eller förordning förbjuda eller begränsa när det bedöms vara motiverat.

Fokus ligger i detta fall inte på enskildas fri- och rättigheter i form av rätt till personlig integritet. Betänkandet har istället ett tydligt effektivitets- och verksamhetsperspektiv. Naturligtvis måste ambitionen vara att den offentliga verksamheten ska bedrivas så effektivt och ändamålsenligt som möjligt. Det får dock inte ske på ett sätt som sätter grundläggande integritetsskyddsmekanismer ur spel.

Rätten till skydd för den personliga integriteten gäller även offentlig verksamhet och dataskyddsdirektivet anger den nivå på skyddet som länderna inom EU måste hålla. I andra kapitlet i direktivet anges under vilka förutsättningar behandling av personuppgifter är tillåten. Datainspektionen anser att det inte är förenligt med direktivet att utgångspunkten är tillåtlighet och att inskränkningarna utgör undantag.

Den enskildes privatliv skyddas i Sverige även genom regeringsformens bestämmelser om grundläggande fri- och rättigheter. Här kan särskilt framhållas bestämmelsen i 2 kap. 6 § andra stycket regeringsformen. Enskilda är enligt bestämmelsen skyddade mot åtgärder från det allmännas sida som innefattar betydande intrång i den personliga integriteten, om intrånget sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Den rättigheten kan enligt 2 kap. 20 § första stycket andra punkten regeringsformen endast begränsas genom lag.

I utredningens uppdrag har inte ingått att föreslå några betydande förändringar vad gäller om och hur myndigheter får behandla personuppgifter. Utredningen har inte heller haft i uppdrag att ompröva tidigare avvägningar mellan effektivitetssträvanden och skyddet för enskildas personliga integritet. Utredningens förslag innebär dock flera väsentliga avsteg från de bestämmelser och principer som idag styr myndigheters personuppgiftsbehandling. Förslaget innebär också en principiell försvagning av skyddet för enskildas personliga integritet.

Villkoren för hur uppgifter får hanteras föreslås nu i hög utsträckning överlåtas åt regeringen att besluta om i förordningsform. Dessutom får myndigheterna stor frihet att själva bestämma villkoren för behandling av personuppgifter, exempelvis vid direktåtkomst. Risken ökar då att uppgifter behandlas oreflekterat på det sätt som kanske är snabbast, billigast och mest effektivt och att hänsyn inte tas till enskildas berättigade anspråk på skydd för den personliga integriteten. Genom att i högre utsträckning ställa krav på lagstöd garanteras – åtminstone i princip – att det sker en noggrann och utförlig integritetsanalys, där behovet av och vinsten med ett förslag vägs mot de integritetsintrång som kan uppstå.

Utredningen har bedömt att det från normgivningssynpunkt finns få hinder mot att i förordningsform avvika från eller komplettera bestämmelserna i den föreslagna myndighetsdatalagen. Enligt utredningen torde det vara endast i rena undantagsfall som behandling av personuppgifter hos myndigheter innehåller moment som medför att behandlingen måste ha stöd i lag. Till grund för detta ställningstagande ligger en tolkning av grundlagsbestämmelsen i 2 kap. 6 § andra stycket regeringsformen som Datainspektionen inte delar.

Bedömningen av vilket utrymme det finns att i nu aktuella lagstiftningsärende reglera frågor om hanteringen av personuppgifter i förordningsform måste ske genom en tolkning av 2 kap. 6 § andra stycket regeringsformen och i likhet med vad som gäller för all rättighetsbegränsande lagstiftning måste det då bli fråga om en restriktiv tolkning. Utrymmet för att i förordningsform avvika från eller komplettera bestämmelserna i myndighetsdatalagen är enligt inspektionen mindre än vad utredningen förespeglar. I det fortsatta lagstiftningsärendet bör denna fråga bli föremål för ytterligare analys.

De myndigheter som omfattas av tillämpningsområdet för myndighetsdatalagen måste, utöver bestämmelserna i den lagen, även beakta många bestämmelser i personuppgiftslagen och den särreglering som ges i bilagor till lagen samt den anslutande förordningen. Den föreslagna lagen förutsätter att myndigheterna har god kunskap om såväl de grundläggande kraven på dataskydd som de nationella regelverken och dess förhållande till varandra. Eftersom den föreslagna lagen inte är anpassad till de olika myndigheternas verksamheter måste myndigheterna också förstå hur reglerna ska tillämpas i deras verksamhet. Datainspektionen ifrågasätter därför om den föreslagna regleringen i praktiken innebär ett tydligare regelverk som är lättare att tillämpa.

Datainspektionen anser också att det är viktigt att avvakta med en nationell reglering till dess att man på EU-nivå beslutat om en dataskyddsförordning. Det är först då som det står klart vilket utrymme det finns att på nationell nivå besluta om regler.

Utöver dessa mer principiella invändningar mot förslaget har Datainspektionen synpunkter på utredningens förslag och bedömningar i fråga om bland annat tolkningen av finalitetsprincipen, ändamålsbestämning, reglering av känsliga personuppgifter, personuppgiftsansvar, direktåtkomst, befogenhet att besluta om vite och straffbestämmelser.

Avsnitt 7.1 Allmänna utgångspunkter

Utredningen har föreslagit en lag som ska innehålla bestämmelser som gäller generellt för alla statliga och kommunala myndigheters personuppgiftsbehandling, frånsett den brottsbekämpande verksamheten. Utredningen bedömer att en samlad reglering gör det möjligt att åstadkomma ett tydligt regelverk som är lättare att tillämpa och som är bättre anpassat till övrig reglering av betydelse för myndigheters personuppgiftsbehandling.

Registerförfattningsområdet är omfattande, brokigt och svårgenomträngligt. Det är därför en tilltalande tanke att i möjligaste mån samla regleringen i en egen lagstiftning. Det skulle kunna innebära en mer lättillgänglig och tydlig reglering, vilket i förlängningen skulle gagna såväl myndigheternas verksamheter som skyddet för enskildas personliga integritet. Datainspektionen är emellertid tveksam till om den föreslagna regleringen i praktiken får dessa effekter.

Den föreslagna lagen ska i första hand gälla för myndigheter som idag inte omfattas av någon särskild registerförfattning. Ambitionen på sikt är dock att mycket av den myndighetsbaserade personuppgiftsbehandling som idag omfattas av särreglering ska regleras i myndighetsdatalagen. Utredningen har tänkt sig att denna reglering ska kunna ske i särskilda bilagor som tillfogas lagen samt genom en anslutande förordning.

Utredningen har också bedömt att behovet av fortsatt på särreglering på sikt kommer att minska betydligt. Någon närmare analys till stöd för denna bedömning lämnas dock inte i betänkandet. Vilka praktiska och rättsliga möjligheter det finns att få till en samlad reglering och vilka behov det fortsatt

kommer att finnas av särreglering utanför myndighetsdatalagen får därför sammanfattningsvis betecknas som mycket osäkert.

De myndigheter som omfattas av tillämpningsområdet för den föreslagna myndighetsdatalagen måste, utöver bestämmelserna i den lagen, även beakta många bestämmelser i personuppgiftslagen och den särreglering som ges i bilagor till lagen samt den anslutande förordningen. Dessutom krävs det att myndigheterna känner till de grundläggande dataskyddsbestämmelserna och hur dessa är avsedda att tillämpas. Det är förutsättningen för att myndigheterna ska kunna uppfylla exempelvis kraven om tillåten behandling enligt artikel 7 i dataskyddsdirektivet.

Datainspektionen ifrågasätter i vilken mån detta innebär ett tydligare och mer lättillämpat regelverk för myndigheterna. Genom att lägga ett så stort ansvar på myndigheterna att uppfylla de krav som ställs på att värna den enskildes integritet vid behandling av personuppgifter skapas betydande integritetsrisker.

Utredningen har också bedömt att en samlad reglering är mer ändamålsenlig för att möta den förändring som förväntas ske genom EU:s dataskyddsförordning. Datainspektionen vill framhålla att det idag är svårt att förutspå den närmare utformningen av denna förordning och vilket utrymme det i slutänden kommer att finnas att inom myndighetsområdet införa en särreglering.

Med hänsyn till de betydande oklarheter som faktiskt gäller i detta avseende anser Datainspektionen att det är viktigt att vänta med en nationell reglering till dess att EU beslutat om en dataskyddsförordning.

Avsnitt 7.3 Normgivningsnivå för särreglering

Utredningen har bedömt att det från normgivningssynpunkt som huvudregel inte finns några hinder mot att i förordningsform avvika från eller komplettera bestämmelserna i den föreslagna myndighetsdatalagen. Utredningen gör vidare bedömningen att det bortsett från de brottsbekämpande myndigheterna torde vara i rena undantagsfall som behandling av personuppgifter hos myndigheter kan anses innehålla några sådana särskilda moment som innebär att behandlingen måste ha stöd i sådan lag som endast får beslutas enligt reglerna i 2 kap regeringsformen.

Det resonemang som ligger till grund för utredningens ställningstagande utmynnar i bedömningen att bestämmelsen i 2 kap. 6 § andra stycket regeringsformen inte syftar till att ange vilka bestämmelser om exempelvis behandling av personuppgifter som ska ha form av lag istället för förordning. Enligt utredningen har bestämmelsen i stället primärt funktionen att bland sådana intrång som omfattas av lagkravet i 8 kap. 2 § första stycket regeringsformen skilja ut de intrång som är så kvalificerade att de ska omfattas av de särskilda begränsningar som enligt 2 kap. 20-22 §§ gäller för riksdagens möjligheter att besluta om en rättighetsinskränkande lag.

Datainspektionen delar inte utredningens bedömningar ovan. Enligt inspektionen råder det inga tvivel om att bestämmelsen i 2 kap. 6 § andra stycket regeringsformen utgör en från 8 kap. regeringsformen fristående bestämmelse, som ställer krav på lagform.

Bestämmelsen i 2 kap. 6 § andra stycket regeringsformen har utformats med utgångspunkt i den uppbyggnad och systematik som gäller för fri- och rättighetsskyddet i regeringsformen. Bestämmelsen reglerar förhållandet mellan den enskilde och det allmänna och utgör en begränsning av statsmakternas normgivningsbefogenheter inom ramen för rättighetsskyddet. Enskilda är enligt bestämmelsen skyddade mot åtgärder från det allmännas sida som innefattar betydande intrång i den personliga integriteten, om intrånget sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Den rättigheten kan enligt 2 kap. 20 § första stycket andra punkten regeringsformen endast begränsas genom lag.

Det har förutsatts att bestämmelsen i 2 kap. 6 § andra stycket regeringsformen kommer att leda till att ett antal registerförfattningar som för närvarande har förordningsform kommer att behöva ges lagform. Med anledning av detta har det införts övergångsbestämmelser i regeringsformen, med innebörden att äldre föreskrifter som innebär betydande intrång i enskildas personliga integritet, äger fortsatt giltighet längst fram till och med december 2015 (prop. 2009/10:80 s. 243).

Det förstärkta integritetsskyddet i 2 kap. 6 § andra stycket regeringsformen innebär sammanfattningsvis att regler om det allmännas personuppgiftsbehandling som är av särskilt integritetskänsligt slag numera hör till det obligatoriska lagområdet. Det innebär att utrymmet för att i

förordningsform reglera personuppgiftsbehandlingen i motsvarande mån har minskat.

I förarbeten till den aktuella bestämmelsen framhålls att flera omständigheter bör vägas in vid bedömningen av vad som kan anses utgöra betydande intrång i enskildas personliga integritet. Det betonas att uppgifternas karaktär och omfattning endast utgör två faktorer att beakta. Därutöver kan det också behöva beaktas till exempel ändamålet med behandlingen av uppgifterna och omfattningen av utlämnandet av uppgifter till andra som sker utan omedelbart stöd av offentlighetsprincipen (prop. 2009/10:80 s. 184).

I sitt slutbetänkande framhöll integritetsskyddskommittén att när det gäller hantering av personuppgifter i de informationssamlingar som kommer att omfattas av det utvidgade grundlagsskyddet är det självfallet så att inte alla led i hanteringen är att betrakta som sådana intrång som träffas av skyddet. Som exempel på sådana moment som träffades av det skyddet angav kommittén bland annat hur uppgifter om enskilda får samlas in, ändamålet med behandlingen och i vilken utsträckning uppgifter på grund av uppgiftsskyldighet, som alltså bryter sekretess som gäller för uppgifterna, ska lämnas ut till andra för samkörning med uppgifter i andra myndighetsregister eller av andra skäl. (SOU 2008:3, s. 272).

Det utrymme som i praktiken finns att i nu aktuella lagstiftningsärende reglera frågor om hanteringen av personuppgifter i förordningsform måste ske genom en tolkning av 2 kap. 6 § andra stycket regeringsformen och i likhet med vad som gäller för all rättighetsbegränsande lagstiftning måste det bli fråga om en restriktiv tolkning.

Datainspektionen ifrågasätter också utredningens bedömning att personuppgifter hos de brottsbekämpande myndigheterna på detta område skulle skilja sig från exempelvis behandling av större samlingar av känsliga personuppgifter. Det finns utifrån dataskyddsbestämmelserna inte någon grund för att göra en sådan särskiljning.

Mot bakgrund av vad som anförts ovan är inspektionen kritisk till utredningens bedömning att det endast är i rena undantagsfall som behandling av personuppgifter hos myndigheter kan anses innehålla några sådana särskilda moment som medför krav på lagstiftning. Med hänsyn till de stora informationsmängder det rör sig om kan det bland annat ifrågasättas om

till exempel ändamålsbestämmelser, villkor för direktåtkomst och behandling av känsliga personuppgifter i detta fall kan regleras i förordningsform.

Avsnitt 8.2.2 Undantagen från den föreslagna lagen

Utredningen har föreslagit en bestämmelse i 3 § enligt vilken administrativ verksamhet ska undantas från lagens tillämpningsområde.

Av betänkandet framgår att myndighetsdatalagen är tänkt att gälla för den personuppgiftsbehandling som sker i myndigheternas sakverksamhet, det vill säga den personuppgiftsbehandling som sker då myndigheterna utför de uppgifter de är ålagda att utföra inom ramen för deras verksamheter. I betänkandet betonas att det är myndigheters rent administrativa verksamhet, som exempelvis personal- och lokalfrågor, som är tänkt att undantas.

Enligt Datainspektionen hade det underlättat tillämpningen om lagtexten gavs en mer precis utformning, där det tydligare framgår vad som omfattas av undantaget. Inspektionen efterlyser också fler exempel på när undantaget för myndigheters administrativa verksamhet är tillämpligt. Ska till exempel schemaläggning i kommunal skolverksamhet omfattas? Omfattas loggning och logguppföljning av personalens aktiviteter i verksamhetssystemen av undantaget?

Det kan också ifrågasättas om det överhuvudtaget är motiverat att undanta administrativ verksamhet från lagens tillämpningsområde. På registerlagstiftningsområdet gäller generellt att den verksamhet som avser myndighetens interna administration faller utanför registerförfattningarnas tillämpningsområde. Det är naturligt eftersom registerförfattningarna syftar till att särreglera personuppgiftsbehandlingen inom vissa utpekade verksamheter och myndigheter. Bestämmelserna i dessa författningar är därför ofta illa anpassade att reglera den behandling av personuppgifter som sker i myndigheternas administrativa verksamhet.

Myndighetsdatalagen är däremot tänkt att gälla generellt för alla statliga och kommunala myndigheters personuppgiftsbehandling, frånsett den brottsbekämpande verksamheten och föreslås därför få en generell utformning som i många delar överensstämmer med regleringen i personuppgiftslagen. Mot den bakgrunden, och på grund av de tillämpningssvårigheter som bestämmelsen kan ge upphov till, kan det ifrågasättas om myndigheters administrativa verksamhet bör undantas från

lagens tillämpningsområde. Datainspektionen utesluter inte att så kan vara fallet, men efterlyser en närmare analys.

Utredningen har också valt att undanta en myndighets verksamhet som personuppgiftsbiträde från myndighetsdatalagens tillämpningsområde. Därmed tydliggörs enligt utredningen att det är den personuppgiftsansvarige myndigheten som är skyldig att följa lagen och se till att bestämmelserna i den följs. Enligt Datainspektionen innebär förslaget om att undanta verksamheten som personuppgiftsbiträde från tillämpningsområdet snarare att tydligheten minskar.

Som utredningen själv uttryckt blir myndighetsdatalagen indirekt tillämplig hos en myndighet som är personuppgiftsbiträde när den personuppgiftsansvarige uppdragsgivarens personuppgiftsbehandling omfattas av lagen. Att uttryckligen ange att lagen inte ska tillämpas i en myndighets verksamhet som personuppgiftsbiträde kan ge upphov till tveksamhet huruvida en myndighet som agerar i egenskap av personuppgiftsbiträde överhuvudtaget, det vill säga även indirekt, träffas av regleringen i myndighetsdatalagen.

Dessutom anges i 19 § i förslaget att ett personuppgiftsbiträde eller den som arbetar under biträdets ledning bara får behandla personuppgifter i enlighet med instruktioner från den personuppgiftsansvariga myndigheten. Det ökar otydligheten ytterligare.

Avsnitt 9.2.4 Behandling av insamlade personuppgifter för nya ändamål

Utredaren har bedömt att finalitetsprincipen ska gälla då myndigheter behandlar personuppgifter med stöd av myndighetsdatalagen.

Som utredningen uppmärksammat är det inom registerlagstiftningsområdet ibland otydligt om finalitetsprincipen ska tillämpas eller inte då myndigheter lämnar ut personuppgifter till utomstående. Därför är det positivt att det nu klargörs att denna princip ska gälla. Datainspektionen ställer sig dock kritisk till den tolkning av principen som utredningen ger uttryck för.

Utredningen har bedömt att utlämnanden är förenliga med finalitetsprincipen om de sker med stöd av någon sekretessbrytande bestämmelse. Genom att sekretessreglera ett uppgiftsutlämnande får, enligt

utredningen, lagstiftaren anses ha tagit ställning till att sådana utlämnanden som ska eller får ske inte är oförenliga med de ursprungliga ändamålen. Utredningen har därmed anslutit sig till den tolkning av finalitetsprincipen som Offentlighets- och sekretesskommittén tidigare har gett utryck för (SOU 2003:99 s. 236). I remissyttrande över det betänkandet var Datainspektionen mycket kritisk till denna tolkning och framhöll att den innebar en synnerligen liberal tolkning av finalitetsprincipen. Inspektionen vidhåller denna uppfattning och vill samtidigt tillägga följande.

Finalitetsprincipen är en av de mest centrala integritetsskyddande principerna i personuppgiftslagen och det underliggande dataskyddsdirektivet. Principen begränsar på ett påtagligt sätt möjligheterna för personuppgiftsansvariga att utbyta personuppgifter. Vid den oförenlighetsprövning som principen påkallar, utgår man hypotetisk från hur en registrerad typiskt sett skulle se på saken. Kommer man vid en sådan bedömning fram till att den registrerade rimligen har att räkna med att de insamlade personuppgifterna också får behandlas för det nya ändamålet, kan detta inte anses vara oförenligt med det ursprungliga.

Utredningens tolkning innebär att myndigheter i princip fritt ska kunna utbyta personuppgifter så länge det inte hindras av bestämmelser om sekretess. Det är en mycket tillåtande tolkning av finalitetsprincipen. De faktiska konsekvenserna som denna tolkning medför är svåra att överblicka. Personuppgifter kan vara integritetskänsliga trots att de inte omfattas av sekretess till skydd för enskilda. Så är till exempel fallet i fråga om uppgifter i domar och beslut, som i regel är offentliga. Förhållandevis integritetskänsliga personuppgifter kan dessutom, om de läggs samman med varandra, skapa ett integritetsintrång som är betydande.

Att reducera finalitetsprincipen till en renodlad sekretessprövning är visserligen praktiskt tilltalande men riskerar att leda till en egen svensk tolkning av finalitetsprincipen utifrån offentlighetsprincipen och inte utifrån principen om rätten till privatliv.

Dataskyddsbestämmelserna måste idag införliva dataskyddsdirektivet och framöver stämma överens med den kommande förordningen. Det skulle därför vara problematiskt, om ens möjligt, att införa en finalitetsprincip som i grunden har ett motsatt intresse än att värna den personliga integriteten.

Datainspektionen motsätter sig följaktligen den tolkning av finalitetsprincipen som utredningen gjort.

Avsnitt 9.2.4 En allmän och heltäckande rättslig grund för myndigheternas behandling av personuppgifter

Utredningen har föreslagit en generell bestämmelse i 8 § enligt vilken en myndighet ska få behandla personuppgifter om det är nödvändigt för att myndigheten ska kunna utföra sin verksamhet. Bestämmelsen innebär att det är respektive personuppgiftsansvarig myndighet som, inom ramen för de uppgifter som myndigheten ålagts genom företrädesvis författning, regleringsbrev eller särskilda beslut, har att närmare specificera för vilket eller vilka ändamål personuppgifter behandlas i verksamheten.

Det aktuella förslaget har en uttalad ambition att förenkla för myndigheterna och att främja effektiviteten inom den offentliga verksamheten. Det är naturligtvis viktigt att den offentliga förvaltningen bedrivs effektivt och att onödiga hinder för en väl fungerande offentlig förvaltning undanröjs. Detta får dock inte ske på ett sätt som äventyrar enskildas rätt till skydd för den personliga integriteten.

Som Datainspektionen framhållit tidigare i detta yttrande (avsnitt 7.3) är frågor om ändamålsreglering i omfattande myndighetsbaserade databaser ett typexempel på sådant som omfattas av det förstärkta grundlagsskyddet i 2 kap. 6 § andra stycket regeringsformen. Förslaget innebär att den från integritetssynpunkt viktiga frågan om för vilka ändamål personuppgifter får hanteras i myndigheternas verksamheter delvis överlåts åt myndigheterna och regeringen att besluta om. Detta strider enligt Datainspektionen mot grundlagsbestämmelsen i 2 kap. 6 § andra stycket regeringsformen. Datainspektionen avstyrker av detta skäl det aktuella förslaget.

Utredningens förslag till ändamålsreglering kan ifrågasättas även av andra skäl. Personuppgiftslagen och det underliggande dataskyddsdirektivet innehåller skyddsbestämmelser som syftar till att förhindra intrång i enskildas personliga integritet från det allmännas sida. I artikel 7 i dataskyddsdirektivet anges till exempel för vilka ändamål personuppgifter får behandlas utan stöd av samtycke från de registrerade. Bestämmelsen har genomförts i svensk rätt i 10 § personuppgiftslagen.

Utredningen bedömer, utan någon närmare fördjupning eller analys, att en generell ändamålsbestämmelse av nu angivet slag är förenlig med artikel 7 i dataskyddsdirektivet. Datainspektionen ifrågasätter denna slutsats. De författningar och andra styrande regelverk som omgärdar myndigheternas verksamhet tar sällan sikte på behandling av personuppgifter. Den föreslagna bestämmelsen lämnar därför ett mycket stort utrymme åt myndigheterna att självständigt avgöra vilken behandling av personuppgifter som verksamheten kräver. Det finns därför ingen garanti att myndigheternas behandling av personuppgifter i slutänden sker för de ändamål som anges i artikel 7 i dataskyddsdirektivet.

Vid en intresseavvägning enligt 10 § personuppgiftslagen ska den registrerades inställning till en personuppgiftsbehandling tillmätas betydelse. Det är oklart i vilken mån detta fortsatt ska gälla då myndigheter behandlar personuppgifter med stöd av den föreslagna myndighetsdatalagen.

Den registrerades inställning tillmäts också betydelse vid tillämpningen av finalitetsprincipen, eftersom den registrerades befogade förväntningar påverkar oförenlighetsbedömningen (se avsnittet ovan). Det är oklart vilka konsekvenser det aktuella förslaget kan få i detta avseende.

Datainspektionen bedömer att det aktuella förslaget innebär en principiellt väsentlig försvagning av skyddet för enskildas personliga integritet. Det är enligt inspektionen mycket tveksamt om förslaget är förenligt med dataskyddsdirektivet. Inspektionen avstyrker därför även av detta skäl förslaget och förordar istället att 10 § personuppgiftslagen görs tillämplig.

Avsnitt 9.3 Tillåten behandling av särskilda kategorier av personuppgifter

Utredningen har föreslagit en bestämmelse i 10 § enligt vilken myndigheter bland annat ska få behandla känsliga personuppgifter om uppgifterna har lämnats i ett ärende eller är nödvändiga för handläggningen av det. Undantaget motsvaras inte av något av de undantag som anges i 15-19 §§ personuppgiftslagen och som i sak motsvaras av uppräkningen i artikel 8.2 i dataskyddsdirektivet.

Med stöd av artikel 8.4 i dataskyddsdirektivet är det möjligt för medlemsstaterna att i sin nationella lagstiftning besluta om andra undantag än de som anges i artikel 8.2 i dataskyddsdirektivet, under förutsättning att

det sker av hänsyn till ett viktigt allmänt intresse. Som utredningen själv uppmärksammat indikerar direktivets krav på att det ska vara fråga om ett viktigt allmänt intresse att en tillåtande bestämmelse ska ges en restriktiv utformning. Utgångspunkten är dessutom att kravet på nödvändighet bör vara större än vad som gäller i fråga personuppgifter som inte är känsliga.

Det kan visserligen anses utgöra ett viktigt allmänt intresse att myndigheter ska kunna ha en fungerande elektronisk ärendehantering som inbegriper behandling av känsliga personuppgifter. Datainspektionen anser dock att begränsningen till vad som är ”nödvändigt” för handläggningen av ett ärende inte innebär en sådan tillräckligt restriktiv utformning av bestämmelsen som kan godtas enligt artikel 8.4 dataskyddsdirektivet.

Inspektionen konstaterar i detta sammanhang att det redan följer av det grundläggande kravet i 9 § punkten f) personuppgiftslagen, som föreslås vara tillämplig på myndigheternas personuppgiftsbehandling, att det inte är tillåtet att behandla fler personuppgifter än vad som är nödvändigt med hänsyn till ändamålen med behandlingen. Det är oklart hur den nödvändighetsbedömning som ska göras avseende känsliga personuppgifter förhåller sig till den nödvändighetsbedömning som den personuppgiftsansvarige myndigheten ändå är skyldig att göra enligt 9 § punkten f) personuppgiftslagen.

Datainspektionen vill också framhålla följande. Det föreslagna undantaget i 10 § myndighetsdatalagen är begränsat till behandling av personuppgifter i enskilda ärenden. Vid en första anblick förefaller möjligheten att behandla personuppgifter därmed ha avgränsats på ett sätt som är rimligt ur integritetssynpunkt. Beroende på hur myndigheterna väljer att avgränsa sina ärenden kan dock omfattningen av ärendena och därmed det potentiella integritetsintrånget skilja sig åt väsentligt. Detta berörs inte i betänkandet.

Personuppgifter får enligt 8 § personuppgiftsförordningen behandlas av en myndighet i löpande text om uppgifterna har lämnats i ett ärende eller är nödvändiga för handläggningen av det. Utredningens förslag innebär att begränsningen till löpande text tas bort och att känsliga personuppgifter således ska kunna behandlas i större omfattning än vad som gäller enligt personuppgiftslagen med tillhörande förordning. Mot den bakgrunden och på grund av de skäl som redovisats ovan i detta avsnitt avstyrker Datainspektionen förslaget.

Avsnitt 10.1 Personuppgiftsansvar

Utredningen har föreslagit en generell bestämmelse i 7 § första stycket, enligt vilken en myndighet är personuppgiftsansvarig för den behandling som myndigheten utför. Bestämmelsen är tänkt att komplettera definitionen i 3 § personuppgiftslagen av begreppet personuppgiftsansvarig. Avsikten är att klargöra att det är den faktiska informationshantering som sker i en viss myndighets verksamhet som ska vara utgångspunkten för bedömningen av när ett personuppgiftsansvar aktualiseras.

Av definitionen i 3 § personuppgiftslagen som i sak överensstämmer med definitionen av begreppet registeransvarig i artikel 2 punkten d) i dataskyddsdirektivet, framgår att det är den som ensam eller tillsammans med andra bestämmer över ändamålen med eller medlen för behandlingen av personuppgifter som är personuppgiftsansvarig.

Den föreslagna bestämmelsen innebär att det i förhållande till personuppgiftslagen införs ett nytt element i begreppsbildningen - vad en myndighet ”utför”. Det ger upphov till frågor om vilka omständigheter som i praktiken aktualiserar ett personuppgiftsansvar. Att ”utföra” någonting, leder till exempel tanken till att det krävs att myndigheten rent faktiskt utför en viss behandling för att ett personuppgiftsansvar ska komma i fråga. En sådan tolkning ligger dock inte i linje med definitionen av personuppgiftsansvar i vare sig personuppgiftslagen eller det underliggande dataskyddsdirektivet.

Att personuppgiftsansvaret uttryckligen knyts till vad en myndighet utför riskerar att medföra att personuppgiftsansvarsfrågan i den praktiska tillämpningen kan komma att bedömas på ett sätt som varken överensstämmer med personuppgiftslagen eller det underliggande dataskyddsdirektivet. Enligt Datainspektionen bidrar det inte till att göra den redan nu komplexa begreppsbildningen på området tydligare. Effekten riskerar istället att bli att lagen tillämpas i strid med dataskyddsdirektivet och den kommande dataskyddsförordningen. Datainspektionen avstyrker därför förslaget.

Utredningen föreslår vidare i 7 § andra stycket en bestämmelse som syftar till att klargöra att personuppgiftsansvaret för behandling av personuppgifter som en myndighet utför även omfattar sådan behandling som utförs när myndigheten via direktåtkomst hos en annan myndighet eller enskild behandlar en tillgängliggjord personuppgift.

Det är i och för sig positivt att utredningen har försökt klargöra hur personuppgiftsansvaret ska fördelas vid direktåtkomst. Enligt Datainspektionen finns det dock även fortsättningsvis oklarheter.

I betänkandet uttalas å ena sidan att en myndighet som har tillgång till en annan myndighets personuppgifter via direktåtkomst blir personuppgiftsansvarig för den behandling som utförs då direktåtkomsten används, exempelvis när en sökning hos den utlämnande myndigheten sker. Å andra sidan uttalas att den utlämnande myndigheten har ett personuppgiftsansvar för den *fortsatta lagringen* och det kontinuerliga tillgängliggörandet för externa mottagare. Det är oklart vad utredningen faktiskt åsyftat med det kursiverade. Är tanken att även den utlämnande myndigheten ska ha ett personuppgiftsansvar för det som den mottagande myndigheten gör med uppgifterna i fråga, trots att den utlämnande myndigheten i detta fall inte utför någon egentlig behandling?

En annan fråga är hur man i förekommande fall ska se på obehörig åtkomst till personuppgifter, till exempel av anställd eller personuppgiftsbiträde, som sker inom ett system för direktåtkomst hos en mottagande myndighet. Ska denna behandling anses ha utförts av den mottagande myndigheten, trots att behandlingen kanske utförts i strid med den mottagande myndighetens uttryckliga rutiner och regelverk? Eller är det den utlämnande myndigheten som ansvarar för eventuellt bristande säkerhetsrutiner i samband med att direktåtkomsten tillåts?

Begreppet behandling innefattar enligt personuppgiftslagens definition väldigt många olika aktiviteter. När en mottagande myndighet genom direktåtkomst söker och eventuellt hämtar uppgifter i en utlämnande myndighets uppgiftssamling sker många olika typer av behandlingar. För att kunna bedöma hur ansvaret ska fördelas krävs därför god kännedom om vad som faktiskt sker i befintliga system och det ska sedan ställas i relation till den som utför detta. Datainspektionen anser att det kommer bli problematiskt för de inblandade myndigheterna att få klarhet i det och det blir då givetvis än svårare för den enskilde att förstå vilken myndighet som är personuppgiftsansvarig.

I det fortsatta lagstiftningsärendet är det enligt Datainspektionen angeläget att personuppgiftsansvarsfrågan vid direktåtkomst blir ytterligare analyserad och tydligare reglerad.

Avsnitt 11.1.1 Definition av begreppet direktåtkomst

Utredningen har bedömt att begreppet direktåtkomst bör definieras på så sätt att en direktåtkomst föreligger om en myndighet hos en annan myndighet har sådan teknisk tillgång till upptagningar som avses i 2 kap. 3 § andra stycket TF.

I likhet med utredningen anser Datainspektionen att det finns anledning att även fortsättningsvis behålla en rättslig åtskillnad mellan å ena sidan direktåtkomst och å andra sidan annat utlämnande i elektronisk form. Utan denna skiljelinje blir myndigheters ansvarsroller i olika hänseenden, inte minst i fråga om behandling av personuppgifter, mycket otydlig. För att denna skiljelinje ska vara meningsfull får det dock inte finnas några oklarheter om vad som faktiskt utgör direktåtkomst respektive annat elektroniskt utlämnande.

Att en direktåtkomst ska anses föreligga när förutsättningarna enligt 2 kap. 3 § andra stycket TF är uppfyllda innebär att det även fortsättningsvis kommer att finnas en stor otydlighet om när direktåtkomst föreligger, eftersom inte heller TF innehåller någon egentlig definition. Denna otydlighet har blivit uppenbar i Högsta förvaltningsdomstolens avgörande den 29 oktober 2015 (mål nr 1356-14), som rör tolkningen av begreppet direktåtkomst inom ramen för det uppgiftsutbyte mellan Försäkringskassan och kommunala nämnder som sker i systemet LEFI Online.

I avgörandet utgår Högsta förvaltningsdomstolen från den i betänkandet beskrivna definitionen på direktåtkomst och utgår således från 2 kap. 3 § andra stycket TF. Högsta förvaltningsdomstolen konstaterar att socialnämnderna inte på egen hand kan söka information i socialförsäkringsbalken, utan att ett utlämnande genom LEFI Online förutsätter att Försäkringskassan reagerar på en begäran om att de efterfrågade uppgifterna ska lämnas ut. Enligt domstolen får därför Försäkringskassan anses förfoga över frågan om och i så fall vilka uppgifter som ska lämnas ut. Någon teknisk tillgång till upptagningar som avses i 2 kap. 3 § andra stycket TF kan socialnämnderna, enligt domstolen, således inte ha.

Högsta förvaltningsdomstolen har visserligen endast tagit ställning till frågan om direktåtkomst utifrån de specifika förutsättningar som förelegat i det aktuella målet. Utifrån domstolens resonemang är det dock oklart vilket utrymme det finns att beteckna ett elektroniskt utbyte som direktåtkomst. Den idag helt dominerande systemmodellen för elektroniska informationssystem fungerar så att en komponent (klient) ställer en fråga till en resurs (server) som sedan utformar och levererar ett svar tillbaka. Det gäller oavsett om informationen ska hanteras internt eller externt, om det är frågan om stora uppgiftssamlingar eller små, om frågemöjligheterna är vida eller begränsade. Att Försäkringskassans system reagerar på den fråga som ställs är därför nödvändigt för att information överhuvudtaget ska kunna erhållas från systemet.

Datainspektionen anser att domen dels visar att det inte är klargörande att koppla begreppet direktåtkomst till kriterierna för förvaring av upptagningar i 2 kap. 3 § andra stycket TF, dels att det behövs en tydlig definition som tar sikte på det som är skyddsbehovet - det vill säga att särskilt reglera situationen då myndigheter inte manuellt tar ställning till ett utlämnande avseende den konkreta handlingen.

Juridiska fakulteten vid Stockholms universitet har i sitt remissyttrande över det aktuella betänkandet anfört att det skulle vara till fördel för rättstillämpningen om det i förarbetsuttalandena kunde sägas att direktåtkomst föreligger i de situationer då en utlämnande maskin gör det på maskinell väg efterfrågade elektroniska utlämnandet utan mänsklig inblandning i det enskilda fallet. På det sättet skulle man väsentligt öka tydligheten och slippa försök att undkomma restriktioner i fråga om direktåtkomst exempelvis genom att den utlämnande maskinen fattar någon form av automatiserat beslut före utlämnandet. Datainspektionen delar Juridiska fakultetens bedömning.

Direktåtkomst är ett centralt begrepp inom e-förvaltningen och bestämmelser om direktåtkomst finns i åtskilliga registerförfattningar. De oklarheter som nu finns om begreppets närmare innebörd får följaktligen konsekvenser inte bara vid tillämpningen av myndighetsdatalagen. Att begreppet direktåtkomst ges en tydlig definition som på ett väl avvägt sätt balanserar effektivitetsbehov med enskildas behov av skydd för den personliga integriteten är ett nålsöga som måste passeras inom registerförfattningsområdet och e-förvaltningen som helhet.

Utöver ett klargörande i förarbetena av vad som ligger i begreppet direktåtkomst bör det i det fortsatta lagstiftningsarbetet också övervägas en legaldefinition av begreppet direktåtkomst i linje med detta resonemang.

Avsnitt 11.1.5 Finns det anledning att begränsa en myndighets möjlighet att medge direktåtkomst till offentliga uppgifter?

Utredningen har föreslagit en bestämmelse i 13 § som innebär att direktåtkomst till sekretessreglerade personuppgifter kräver stöd i lag eller förordning för att vara tillåten. Däremot saknas det enligt utredningen behov av en särskild bestämmelse som begränsar myndigheters möjligheter att medge direktåtkomst till offentliga uppgifter som förekommer i deras verksamheter.

Datainspektionen avstyrker utredningens förslag. Inspektionen anser att direktåtkomst till personuppgifter, oavsett om de omfattas av sekretess, ska kräva särskilt lagstöd för att vara tillåten.

Visserligen kan uppgifter som är sekretessreglerade typiskt sett anses vara mer integritetskänsliga än uppgifter som inte är det. Även för den senare kategorin uppgifter kan dock integritetsaspekten göra sig starkt gällande. Uppgifterna kan i sig vara integritetskänsliga, som exempelvis uppgifter om enskilda i domar och beslut. Även uppgifter som var för sig är att beteckna som förhållandevis harmlösa kan tillsammans medföra ett integritetsintrång som blir betydande.

Myndighetsdatalagen är tänkt att omfatta personuppgiftsbehandlingen inom stora delar av den offentliga förvaltningen. Det är inte lämpligt att villkoren för hur uppgifter får hanteras, till exempel genom direktåtkomst, överlåts åt myndigheterna själva att bestämma. Då ökar risken att uppgifter tillhandahålls oreflekterat på det sätt som kanske är snabbast, billigast och mest effektivt och att hänsyn inte tas till enskildas berättigade anspråk på skydd för den enskilda integriteten. Genom att ställa krav på lagstöd för att direktåtkomst ska beviljas säkerställs - åtminstone i princip - att det sker en noggrann och utförlig integritetsanalys, där behovet av och vinsten med direktåtkomsten vägs mot de integritetsintrång som kan uppstå.

Inspektionen anser följaktligen att direktåtkomst med hänsyn till de principiella integritetsrisker som är förknippade med sådan åtkomst, av

lämplighetsskäl, bör medföra krav på lagstöd. Som Datainspektionen framhållit i avsnitt 7.3 kan emellertid frågan om villkor för direktåtkomst eventuellt också omfattas av grundlagsbestämmelsen i 2 kap. 6 § andra stycket regeringsformen, vilket i så fall innebär krav på lagreglering. I det fortsatta lagstiftningsärendet bör denna fråga närmare analyseras.

Avsnitt 11.2.3 Bör utlämnanden i elektronisk form kräva stöd i lag eller förordning?

Utredningen bedömer att det saknas skäl att införa ett grundläggande krav på att utlämnanden av personuppgifter i elektronisk form ska ha stöd i lag eller förordning.

Datainspektionen vill återigen framhålla att uppgifter kan vara integritetskänsliga även i de fall då de inte omfattas av sekretess. Det kan därför ifrågasättas om inte utgångspunkten i detta fall istället bör vara att utlämnanden ska ha stöd i lag eller förordning för att vara tillåtna. I det fortsatta lagstiftningsärendet bör denna fråga bli föremål för en fördjupad analys, där behovet av en flexibel lagstiftning noggrant vägs mot intrånget i enskildas personliga integritet.

Avsnitt 12.5 Behov av ytterligare undantag

Utredningen har föreslagit en bestämmelse i 16 § enligt vilken myndigheter ska kunna överföra personuppgifter till tredje land som saknar en adekvat skyddsnivå om överföringen krävs för handläggningen av ett visst ärende. I betänkandet lämnas en mycket knapphändig redogörelse för undantaget, vilket gör det svårt att närmare avgöra vilka situationer som det avser att täcka.

I betänkandet framhåller utredningen att myndigheter på ett rättssäkert och effektivt sätt måste kunna handlägga ärenden med användning av modern teknik för att kommunicera och kunna förmedla information även till enskilda som befinner sig i avlägsna länder. Den faktiska utformningen av bestämmelsen i fråga tycks dock möjliggöra utlämnanden inte bara till enskilda utan också till myndigheter.

Datainspektionen ställer sig frågande till hur det aktuella undantaget förhåller sig till artikel 26.1 punkten d) i dataskyddsdirektivet. Enligt den artikeln får medlemsstaterna föreskriva undantag från förbudet att föra över personuppgifter till tredje land som inte har en adekvat skyddsnivå under förutsättning att överföringen är nödvändig eller bindande enligt författning

av skäl som rör viktiga allmänna intressen eller för att fastslå, göra gällande eller försvara rättsliga anspråk.

Utredningen har i en mening bedömt att det aktuella undantaget uppfyller direktivets krav på att utgöra ett viktigt allmänt intresse. Mot bakgrund av de oklarheter som finns om förlagets förenlighet med dataskyddsdirektivet avstyrker Datainspektionen i nuläget förslaget.

Avsnitt 13.4.1 Information som ska lämnas självmant

Utredningen har bedömt att det inte behövs någon bestämmelse om att information ska ges då uppgifter samlas in från någon annan källa än den registrerade. Skälet till detta är att det enligt utredningen alltid kan antas finnas bestämmelser om myndighetens registrerande och utlämnande av personuppgifter i författning. Utredningen anser följaktligen att myndighetsdatalagen inte bör innehålla någon hänvisning till 24 § personuppgiftslagen.

24 § personuppgiftslagen ålägger den personuppgiftsansvarige att på eget initiativ lämna information om behandling av personuppgifter till de registrerade när personuppgifter samlas in från någon annan källa än den registrerade. Paragrafen är avsedd att ha samma innebörd som artikel 11 i dataskyddsdirektivet. Enligt artikel 11.1 i dataskyddsdirektivet är den registeransvarige skyldig att informera den registrerade om behandlingen av personuppgifter i de situationer som anges i bestämmelsen. Enligt artikel 11.2 i samma artikel är det möjligt att avvika från skyldigheten att informera bland annat om registrering eller utlämnande uttryckligen föreskrivs i författning.

EU-domstolen har i ett förhandsavgörande från den 1 oktober 2015 (C-201/14) bland annat tagit ställning till innebörden av artikel 11 i dataskyddsdirektivet. Bakgrunden till avgörandet var att den rumänska skattemyndigheten (ANAF) med stöd av bestämmelser i nationell lag överfört personuppgifter till den rumänska myndigheten för sjukförsäkringar (CNAS) i syfte att bedöma om de berörda personerna hade rätt till sjukförsäkring. EU-domstolen bedömde att författningsbestämmelserna som reglerade överföringen av personuppgifter från ANAF till CNAS inte utgjorde sådana uttryckliga föreskrifter som avses i 11.2 dataskyddsdirektivet. Domstolen fäste bland annat vikt vid att den aktuella lagen vare sig definierade de uppgifter som skulle överföras eller de närmare villkoren för överföring av dessa uppgifter, utan att detta endast framgick av ett protokoll som överenskommits mellan ANAF och CNAS.

Myndighetsdatalagen är tänkt att gälla för en stor del av den statliga och kommunala förvaltningen och saknar bestämmelser som uttryckligen anger för vilka ändamål personuppgifter får hanteras. Det rör sig om vitt skilda verksamheter, där styrningen av verksamheterna i form av författningsreglering, instruktioner och särskilda regeringsuppdrag skiljer sig åt väsentligt. I ena änden av spannet finns myndigheter med avgränsade uppdrag och med en författningsreglering som är lättare att överblicka. I andra änden finns kommunerna vars uppdrag spänner över många och väsensskilda områden och som dessutom, genom den allmänna kommunala kompetensen i 2 kap. 1 § kommunallagen, saknar en tydlig avgränsning.

För vissa myndigheter med tydligt författningsreglerade verksamheter kan kravet på sådana uttryckliga föreskrifter i författning som avses i artikel 11.2 i dataskyddsdirektivet möjligen vara uppfyllt. Sett som en helhet, med beaktande av ovan angivna avgörande från EU-domstolen, kan kravet på uttryckliga föreskrifter dock knappast anses uppfyllt. Datainspektionen motsätter sig därför utredningens förslag och anser att 24 § personuppgiftslagen görs tillämplig.

Avsnitt 17.3.4. Föreläggande att åtgärda en behandling som inte uppfyller gällande krav

Utredningen har föreslagit en bestämmelse i 28 § andra stycket, enligt vilken det av tillsynsmyndighetens föreläggande ska framgå vad tillsynsmyndigheten anser är nödvändigt för att avhjälpa påtalade brister.

Datainspektionen avstyrker förslaget. Inspektionen har generellt en restriktiv inställning till att i tillsynsbeslut föreskriva vilka närmare åtgärder en personuppgiftsansvarig ska vidta. Anledningen till det är att det ofta finns flera tänkbara sätt att avhjälpa konstaterade brister i en personuppgiftsbehandling. I dessa fall är det den personuppgiftsansvarige, med särskild kännedom om sin verksamhet och de behov och resurser som finns, som är bäst lämpad att avgöra vilka åtgärder som bör vidtas för att komma tillrätta med påtalade brister. Det får heller inte råda något tvivel om att det är den personuppgiftsansvarige som har ansvar att följa gällande regelverk.

Enligt Datainspektionen bör det vara tillräckligt att det av inspektionens beslut tydligt framgår i vilket eller vilka avseenden som en behandling brister.

Det är därefter den personuppgiftsansvarige myndigheten som ska vidta de åtgärder som är nödvändiga för att komma tillrätta med bristen. Naturligtvis kan Datainspektionen, om myndigheten anser att det lämpligt, på ett icke bindande sätt ge förslag på hur en brist kan åtgärdas. Det är inte ovanligt att inspektionen lämnar sådan vägledning. Det finns inte heller någonting som hindrar att Datainspektionen, om det är lämpligt, uttryckligt föreskriver vilka åtgärder som den personuppgiftsansvarige ska vidta.

Avsnitt 17.3.4 Förbud mot att fortsätta en behandling

Utredningen har föreslagit en bestämmelse i 29 § enligt vilken tillsynsmyndigheten ska kunna förbjuda en myndighet att fortsätta en behandling av personuppgifter på annat sätt än att uppgifterna lagras, under förutsättning att myndigheten allvarligt brustit i sina skyldigheter enligt den föreslagna myndighetsdatalagen.

I betänkandet anges som exempel på sådana allvarliga brister som innebär att bestämmelsen blir tillämplig bland annat att en myndighet i en inte obetydlig omfattning behandlar känsliga personuppgifter trots att myndigheten saknar stöd för det. Ett annat exempel som anges i betänkandet är då en myndighet på ett allvarligt sätt åsidosätter sin skyldighet att vidta åtgärder för att upprätthålla en tillräckligt hög säkerhetsnivå för en stor mängd känsliga personuppgifter.

De ovan angivna exemplen tar sikte på situationer där känsliga personuppgifter behandlas i viss omfattning. Det kan dock uppstå betydande integritetsintrång även då endast enstaka personuppgifter av mycket känslig natur hanteras i strid med myndighetslagen. Är tanken att också sådana situationer ska omfattas? Det sistnämnda exemplet ovan förutsätter dessutom att myndigheter på ett ”allvarligt sätt” åsidosatt sina skyldigheter. Utgör inte i princip varje form av åsidosättande från myndighetens sida av sina skyldigheter i dessa fall sådana allvarliga brister som avses i den föreslagna bestämmelsen?

Datainspektionen anser att det till ledning för tillämpningen av bestämmelsen bör lämnas fler, tydligare och utförligare exempel på när det föreligger sådana allvarliga brister som avses i bestämmelsen.

Avsnitt 17.3.5 Befogenhet att besluta om vite

Utredningen har bedömt att tillsynsmyndigheten inte bör ha befogenhet att rikta vitesförelägganden mot de myndigheter som behandlar personuppgifter enligt myndighetsdatalagen.

Datainspektionen har inga synpunkter på att tillsynsmyndigheten som utgångspunkt inte ska ha möjlighet att vitesförelägga statliga myndigheter. Däremot är inspektionen inte övertygad om det riktiga i att inte ge tillsynsmyndigheten möjlighet att vitesförelägga kommunala myndigheter. Det gäller även med beaktande av vad som anges om särregleringen av hälso- och sjukvårdsområdet och socialtjänsten. Inspektionen utesluter inte att den kommunala efterlevnaden också på andra områden är sådan att tillsynsmyndigheten behöver kunna ha ett kraftfullt verktyg i form av vite.

Utformningen bör vara sådan att tillsynsmyndigheten bör kunna förena beslut om både förelägganden och förbud med vite. Att Datainspektionen hittills inte använt sig av vite beror inte på att myndigheten inte sett behov av det utan närmast på att utformningen idag är för trubbig – myndigheten har ju inte kunna förena ett föreläggande om att vidta en viss åtgärd med vite utan endast haft möjlighet att använda det i samband med att helt förbjuda och därmed stoppa all behandling än lagring av personuppgifter.

Avsnitt 18.1 Skadestånd och straff

Utredningen har bedömt att det inte finns något behov av att införa särskilda straffbestämmelser i myndighetsdatalagen. Det föreslås inte heller göras någon hänvisning till straffbestämmelserna i 49 § personuppgiftslagen. Det innebär sammantaget att det inte kommer att finnas några överträdelser av lagen som är straffsanktionerade.

Som anges i betänkandet kan straffansvar aktualiseras enligt andra straffbestämmelser än dem i personuppgiftslagen, såsom tjänstefel, brott mot tystnadsplikt eller dataintrång. Även om dessa lagöverträdelser i vissa fall kan sammanfalla med brott mot personuppgiftslagen, så är det dock långt ifrån alltid som det föreligger en sådan överensstämmelse.

Det är straffbart enligt 49 § personuppgiftslagen att uppsåtligen eller av grov oaktsamhet behandla personuppgifter i strid med 13 – 21 § personuppgiftslagen. Att skapa en uppgiftssamling med känsliga personuppgifter utan lagligt stöd är således straffbart enligt

personuppgiftslagen, men det handlar inte om brott mot tystnadsplikten eller dataintrång. Att skapa en dylik uppgiftssamling skulle kunna ha samband med myndighetsutövning, det vill säga ske i samband med beslut eller faktiska åtgärder som myndigheten vidtar gentemot enskilda och som grundas på samhällets maktbefogenheter. Oftast rör det sig dock om generella förvaltningsrättsliga åtgärder som inte genererar ansvar för tjänstefel.

Datainspektionen anser inte att det generellt bör anses mindre straffvärt att exempelvis skapa en uppgiftssamling med känsliga personuppgifter utan lagligt stöd, än att en tjänsteman vid myndighetsutövning åsidosätter sina åligganden eller röjer sekretessbelagda uppgifter.

Dessutom innebär förslaget att det uppstår en principiellt stor skillnad i fråga om straffansvar i privat och offentlig verksamhet. Varför ska det anses mindre straffvärt att skapa en uppgiftssamling med känsliga personuppgifter utan lagligt stöd i offentlig verksamhet än i privat? Ett annat exempel är då någon lämnar osanna uppgifter till Datainspektionen vid tillsyn eller överför uppgifter till tredje land utan rättsligt stöd, vilket i princip är straffbart enligt personuppgiftslagen. Varför ska dessa situationer bedömas olika beroende på om det rör sig om offentlig eller privat verksamhet?

I betänkandet anges som ett argument för denna skillnad att myndigheter inte kan begå brott. I Sverige gäller dock generellt att juridiska personer inte kan begå brott och att straffansvaret bärs av dess företrädare. Det är således inte något skäl till att särbehandla myndigheter.

Datainspektionen ifrågasätter sammanfattningsvis förslaget att undanta överträdelse av myndighetsdatalagen från straffsanktioner och efterlyser en närmare analys av de konsekvenser för den personliga integriteten som förslaget kan komma att medföra.

Detta yttrande har beslutats av generaldirektören Kristina Svahn Starrsjö efter föredragning av juristen Oskar Öhrström. Vid den slutliga handläggningen har även chefsjuristen Hans-Olof Lindblom, enhetschefen Katarina Tullstedt och it-säkerhetsspecialisten Magnus Bergström deltagit.

Kristina Svahn Starrsjö

Oskar Öhrström