

Regeringskansliet,
Finansdepartementet

Diarienummer:
DI-2020-12475

Ert diarienummer:
Fi2020/05128

Datum:
2021-02-22

Yttrande över departements- promemorian En utvecklad organisation för lokal statlig service – slutredovisning (Ds 2020:29)

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

IMY är positiv till ambitionen att utöka tillgängligheten till den statliga servicen i landet, men vill lämna följande synpunkter gällande dataskyddet.

När flera aktörer ska samverka är det gällande dataskyddet viktigt att respektive aktörs ansvar är utrett och klarlagt innan samverkan påbörjas. Det behöver därför göras en kartläggning av om aktuell samverkan innebär behandling av personuppgifter. Det gäller exempelvis myndigheters samverkan kring lokaler som t.ex. omfattar en gemensam reception eller tillhandahållande av IT-system, men även vid sådan samverkan inom kommuner som bl.a. kallas kontaktcenter och som omnämns i departementspromemorian. Detta är avgörande för att de aktörer som har ett ansvar enligt dataskyddsbestämmelserna ska kunna ta sitt ansvar och fullgöra sina skyldigheter (jfr ansvarsskyldigheten i artikel 5.2 i dataskyddsförordningen).

Bedömningen av personuppgiftsansvaret ska göras utifrån dataskyddsförordningens bestämmelser och eventuell kompletterande nationell lagstiftning på det aktuella området. Om det uppstår en sådan roll att en aktör behandlar personuppgifter för den personuppgiftsansvariges räkning, och aktören därigenom är att betrakta som ett personuppgiftsbiträde, ska behandlingen regleras genom ett avtal eller en annan rättsakt som är bindande för personuppgiftsbiträdet (se artiklarna 4.7, 4.8 och 28.3 i dataskyddsförordningen). Det är dock inte förenligt med bestämmelserna i dataskyddsförordningen att föreskriva någon annan ordning än den som anges i förordningen vad gäller ansvaret mellan den som är personuppgiftsansvarig och personuppgiftsbiträde. Personuppgiftsbiträdet får endast behandla personuppgifter i enlighet med dokumenterade instruktioner från den som är personuppgiftsansvarig såvida inte denne är skyldig att göra det enligt unionsrätten eller medlemsstaternas nationella rätt (artikel 29). Av dataskyddsförordningen följer dock att personuppgiftsbiträdet har egna skyldigheter i vissa avseenden, t.ex. i fråga om säkerhetsåtgärder (artikel 32).

Postadress:
Box 8114
104 20 Stockholm

Webbplats:
www.imy.se

E-post:
imy@imy.se

Telefon:
08-657 61 00

En absolut förutsättning vid samverkan som innebär personuppgiftsbehandling är öppenheten och att de registrerade ges tydlig information om hur ansvaret ser ut och vart hon eller han kan vända sig för att kunna ta tillvara sina rättigheter enligt dataskyddsförordningen (artiklarna 5.1a och 12-15).

Som anges i departementspromemorian ställer dataskyddsförordningen krav på säkerhet i samband med behandling av personuppgifter. Detta gäller exempelvis vid användning av mobila kontor för servicetjänster med portabel IT-utrustning och användningen av fjärrskrivbord för att möjliggöra åtkomst till personuppgifter (se avsnitten 4.6 och 9.3). Användningen av sådana lösningar kan innebära säkerhetsrisker. I detta sammanhang behöver särskilt artiklarna 5.1f, 24, 25 och 32 i dataskyddsförordningen beaktas. Säkerhetsåtgärderna ska bedömas utifrån skyddet för den enskildes rättigheter och friheter. Att integrera nödvändiga skyddsåtgärder är ett sätt att säkerställa att kraven i dataskyddsförordningen uppfylls och att de registrerades rättigheter skyddas.

När det gäller artikel 32 i dataskyddsförordningen, vill IMY framhålla att enligt bestämmelsen ska den personuppgiftsansvarige, och i förekommande fall även ett personuppgiftsbiträde, vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken. Vid bedömningen ska beaktas den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna för fysiska personers rättigheter och friheter som kan vara av varierande sannolikhetsgrad och allvar. Särskild hänsyn ska tas till de risker som behandlingen medför, i synnerhet för oavsiktlig eller olaglig förstöring, förlust eller ändring eller för obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

Det finns flera olika sätt att analysera risker, exempelvis genom en riskanalys där hot och oönskade händelser identifieras som kan leda till negativa konsekvenser. Genom en riskanalys får den personuppgiftsansvarige ett underlag för att ta beslut om vilka säkerhetsåtgärder som ska införas. Nästa skede kan vara att genomföra en gapanalys för att balansera säkerhetsåtgärderna mot säkerhetsbehoven där syftet är att identifiera den önskvärda nivån på informationssäkerheten och den faktiska nivån för att överbrygga gapet. Som ett stöd i arbetet finns ett flertal vedertagna standarder, metoder och vägledningar att utgå ifrån.

Det kan framhållas att kraven på säkerhet är högre om det är fråga om en omfattande behandling av personuppgifter där en stor del är känsliga eller integritetskänsliga personuppgifter. Det är fallet vid servicesamverkan mellan Statens servicecenter och aktuella samverkansmyndigheter. Som anges i departementspromemorian kan den personuppgiftsansvarige vid en bedömning av vad som är lämplig säkerhet även behöva beakta vilka övriga uppgifter som servicehandläggaren vid Statens servicecenter tar del av.

Mot bakgrund av detta är det en förutsättning för att servicehandläggarna vid Statens servicecenter ska ges tillgång till samverkansmyndigheternas verksamhetssystem från respektive myndighets fjärrskrivbord att alla åtgärder som typiskt sett är lämpliga enligt artikel 32 i dataskyddsförordningen har vidtagits. Det gäller bl.a. i fråga om kryptering och autentisering.

När det gäller förslagen om utökning av servicekontorsverksamheten med service för ytterligare myndigheters räkning, anser IMY att det är positivt att departementspromemorian belyser de integritetsrisker som kan aktualiseras om handläggare vid Statens servicecenter får tillgång till en ökad mängd personuppgifter i flera verksamhetssystem samtidigt. Det kan bl.a. innebära att en servicehandläggare får en oönskat sammansatt bild av en enskilds personliga förhållanden. IMY instämmer därför i att samverkansmyndigheterna innan avtal ingås, men även under samarbetets gång, noga bör överväga vilka arbetsuppgifter som ska utföras vid servicekontoren och vilka personuppgifter som en servicehandläggare får ges tillgång till inom ramen för den aktuella verksamheten.

IMY vill i detta sammanhang på nytt understryka vikten av att samverkansmyndigheterna ger tydliga instruktioner till servicehandläggarna hur personuppgifter får behandlas i myndighetens verksamhet och säkerställer att det utförs behörighetskontroller (se artiklarna 29 och 32.4 i dataskyddsförordningen).

Avslutningsvis vill IMY lyfta fram att en utökning av servicesamverkan av ovan nämnt slag innebär att en servicehandläggare kan få ytterligare instruktioner från en personuppgiftsansvarig myndighet att förhålla sig till. Det ställer stora krav på den enskilde handläggaren att hålla isär uppgifterna. En sådan utökning innebär även ökade krav på servicehandläggarnas kunskaper om gällande bestämmelser om bl.a. personuppgiftsbehandling och sekretess avseende flera myndigheter. Handläggarna kan alltså komma att ställas inför komplicerade frågeställningar i fråga om dataskydd och sekretess. IMY noterar att Statens servicecenter och samverkansmyndigheterna har ingått överenskommelser som gäller samverkan på servicekontoren i fråga om bl.a. utbildning för att säkerställa att personalen har den utbildning som krävs för att utföra de specifika uppgifterna vilket i sig är positivt. Som konstateras i departementspromemorian behöver dock utbildningsinsatserna öka i och med att komplexiteten i verksamheten ökar med en större bredd av frågor som en enskild handläggare behöver behärska.

Detta yttrande har beslutats av enhetschefen Malin Blixt efter föredragning av juristen Nina Hubendick. I den slutliga handläggningen har även avdelningsdirektören Suzanne Isberg deltagit.

Malin Blixt, 2021-02-22 (Det här är en elektronisk signatur)