

Regeringskansliet,
Finansdepartementet

Juridik som stöd för förvaltningens digitalisering (SOU 2018:25)

Datainspektionen har granskat betänkandet huvudsakligen utifrån myndighetens uppgift att arbeta för att människors grundläggande fri- och rättigheter skyddas i samband med behandling av personuppgifter.

Sammanfattning

Datainspektionen tillstyrker förslaget till ny lag om tystnadsplikt för privata leverantörer. Inspektionen finner dock anledning att ifrågasätta utredningens bedömning rörande automation i förvaltningen, digital kommunikation samt avstyrker utredningens förslag rörande Datainspektionens uppdrag. Inspektionen lämnar följande synpunkter.

Inledning

Datainspektionen noterar att det är fråga om ett mycket viktigt och omfattande betänkande som i stora delar är välskrivet, med välgrundade förslag. Det finns dock anledning att peka på några områden där utredningens bedömningar kan ifrågasättas. Yttrandet följer betänkandets struktur.

7. Automation i förvaltningen

Enligt artikel 22 dataskyddsförordningen har den enskilde rätt att inte bli föremål för beslut som enbart grundar sig på automatiserad behandling, inbegripet profilering, om beslutet kan ha rättsliga följder för den enskilde eller på liknande sätt i betydande grad påverkar honom eller henne. Sådant automatiserat beslutsfattande kan dock vara tillåtet, t.ex. enligt unionsrätten eller nationell rätt som fastställer lämpliga åtgärder till skydd för den registrerades rättigheter, friheter och berättigade intressen.

Utredningen konstaterar att det saknas förarbetsuttalanden som anger hur bestämmelsen i förvaltningslagen, om att beslut kan fattas automatiserat, förhåller sig till dataskyddsförordningen. Utredningen gör dock bedömningen att det mot bakgrund av regeringens tydliga avsikt att skapa bättre förutsättningar för en fortsatt utveckling av den digitala förvaltningen och det uttalade stödet för automatiserat beslutsfattande i förvaltningslagen, som utgångspunkt borde innebära att automatiserat beslutsfattande inom förvaltningen även ska anses vara tillåtet enligt dataskyddsförordningen.

Utredningen konstaterar vidare att några särskilda åtgärder till skydd för den registrerades rättigheter, friheter och berättigade intressen med avseende på automatiserade beslut emellertid inte har införts i förvaltningslagen. Utredningen lyfter dock fram att förvaltningslagen innehåller generellt tillämpliga bestämmelser om bl.a. rätt att lämna uppgifter muntligt i ett ärende, om det inte framstår som obehövt, och bestämmelser om omprövning samt rätt att överklaga beslut. Utredningen för vidare ett resonemang om på vilket sätt reglering i den materiella rätt som ska tillämpas vid beslutsfattande, kan inverka på frågan om det är tillåtet eller lämpligt att beslut fattas automatiserat i kapitel 7.9.1.

Datainspektionen delar inte utredningens bedömning. Artikel 22.2 b i dataskyddsförordningen kräver att det finns ett rättsligt stöd i den nationella rätten som fastställer lämpliga åtgärder till skydd för den registrerades rättigheter, friheter och berättigade intressen. Mot bakgrund av att det inte finns någon sådan reglering i förvaltningslagen anser Datainspektionen att förvaltningslagens bestämmelser inte uppfyller de krav som artikel 22.2 b ställer på nationell rätt. Inspektionen ifrågasätter även utredningens resonemang angående att generellt tillämpliga bestämmelser visar att kraven enligt artikel 22.2 b är uppfyllda. Inspektionen anser att detta innebär att registrerade har rätt att inte bli föremål för beslut som enbart grundas på automatiserad behandling, inbegripet profilering, som har rättsliga följder för honom eller henne eller på liknande sätt i betydande grad påverkar honom eller henne. En förutsättning för förvaltningslagens bestämmelser ska kunna utgöra nationell rätt som tillåter automatiserade beslut är att förvaltningslagen kompletteras med bestämmelser som uppfyller förordningens krav enligt artikel 22.2 b.

Bedömningen ovan påverkar även förslaget i kapitel 7.9.2 om att upphäva särreglering av automatiserat beslutsfattande. Om förvaltningslagens bestämmelser inte medför att automatiserat beslutsfattande inom förvaltningen är tillåtet enligt dataskyddsförordningen, så saknas anledning att upphäva särregleringen på så sätt som föreslås. Datainspektionen anser

att det finns två alternativ för att möjliggöra automatiserat beslutsfattande. Antingen kompletteras förvaltningslagen på så sätt som beskrivs ovan, eller så får befintlig särreglering av automatiserat beslutsfattande analyseras och kompletteras så att bestämmelserna uppfyller kraven enligt artikel 22.2 b.

8. Digital kommunikation

8.3.3 Ny huvudregel om digital tillgänglighet, 8.3.6 Ny huvudregel om digital kommunikation till enskilda

Utredningen föreslår att myndigheter ska vara skyldiga att tillhandahålla, och på lämpligt sätt anvisa, en eller flera digitala mottagningsfunktioner dit handlingar kan förmedlas, om det inte är olämpligt av säkerhetsskäl eller av andra skäl. Utredningen föreslår även att myndigheter ska vara skyldiga att förmedla skriftliga underrättelser eller andra handlingar till enskilda digitalt, om det inte är olämpligt av säkerhetsskäl eller av andra skäl.

I detta sammanhang vill Datainspektionen påtala att den övervägande majoriteten av handlingar som kommer att behandlas i digitala mottagningsfunktioner kommer att innehålla personuppgifter, vilket innebär att kraven i dataskyddsförordningen alternativt brottsdatalagen samt i många fall även kompletterande registerförfattningar måste uppfyllas. Dessa regelverk är *den primära rättskällan vid behandling av personuppgifter*. En av förutsättningarna för att få behandla personuppgifter är, enligt artikel 32 dataskyddsförordningen, att den personuppgiftsansvarige vidtar lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken. Den personuppgiftsansvarige måste således aktivt säkerställa tillräcklig säkerhet för behandlingen.

Då de föreslagna bestämmelserna anger rekvisitet, *inte olämpligt av säkerhetsskäl eller av andra skäl*, kan bestämmelserna tolkas som att det är upp till verksamhetsutövarna att göra en lämplighetsbedömning som inte knyter an till kravet på säkerhetsåtgärder i tillämpliga dataskyddsbestämmelser. Datainspektionen anser att de föreslagna bestämmelserna ska ändras så att det klart framgår att en tillräcklig säkerhetsnivå är en förutsättning för att verksamhetsutövare ska få använda digitala mottagningsfunktioner och kommunicera digitalt med registrerade.

När det gäller skyldigheten att kommunicera digitalt föreslår utredningen att enskilda ska kunna meddela att de inte önskar ta emot skriftliga underrättelser eller andra handlingar från myndigheten i digital form. Att en enskild tyst accepterar digital kommunikation innebär inte att den tysta acceptansen samtidigt medför ett godkännande av att uppgifterna anses vara skyddade av en tillräcklig säkerhetsnivå. Personuppgiftsansvariga alltid är

skyldiga att uppnå en tillräcklig säkerhetsnivå. Dataskyddsförordningen lämnar inte något utrymme för enskilda att direkt eller indirekt "godkänna" otillräcklig säkerhet.

Egna utrymmen - personuppgiftsansvar

Utredningen har analyserat de digitala tjänster som brukar kallas egna utrymmen. De beskrivs som att de innehåller ett så kallat eget utrymme där användaren exempelvis kan registrera och lagra uppgifter utan att myndigheten som tillhandahåller det egna utrymmet har insyn i eller tar del av uppgifterna i fråga. Ett ytterligare kännetecken för denna typ av tjänster anges vara att den myndighet som tillhandahåller det egna utrymmet enbart tekniskt bearbetar eller tekniskt lagrar uppgifterna för annans räkning fram till dess användaren aktivt förmedlat uppgifterna i fråga till myndigheten. Utredningen framhåller att begreppet inte tillkommit enbart utifrån tekniska aspekter, utan snarare som en rättsfigur, mot bakgrund av att förvaltningens digitala utveckling har förutsatt att myndigheterna svarat upp mot de förväntningar som privatpersoner och företag har på att handlingar inte är att anse som inkomna till myndigheten i ett för tidigt skede, dvs. innan avsikten varit att ge in dem till myndigheten.

Utredningen har genomfört en analys av hur personuppgiftsansvaret är fördelat när myndigheter använder egna utrymmen och konstaterar att för varje personuppgiftsbehandling som utförs i den offentliga förvaltningen finns en eller flera myndigheter som bär personuppgiftsansvaret för behandlingen ifråga. Hur ansvaret fördelas ska utredas av de parter som har del i personuppgiftsbehandlingen innan behandlingen påbörjas. Utredningen lyfter dock fram ett antal frågeställningar och gör bedömningen att det kan vara förenat med avsevärda svårigheter att med en hög grad av exakthet fastställa ramarna för respektive aktörs personuppgiftsansvar i myndighetsgemensamma digitala tjänster med eget utrymme. Utredningen anser att det finns avsevärda svårigheter att med en hög grad av exakthet fastställa ramarna för respektive aktörs personuppgiftsansvar i myndighetsgemensamma digitala tjänster med eget utrymme. Datainspektionen vill i detta sammanhang påpeka att frågan om myndigheter kan behandla personuppgifter gemensamt, egentligen inte är en fråga som rör egna utrymmen, även om frågeställningen aktualiseras i samband med dessa.

Att personuppgiftsansvaret uppfattas korrekt av en verksamhetsutövare är avgörande för att skyddet för den enskildes integritet ska fungera. Ett utrymmes karaktär som eget påverkar inte personuppgiftsansvaret, utan

personuppgiftsansvaret måste analyseras utifrån gällande dataskyddsbestämmelser.

Vem som är personuppgiftsansvarig beror på vem som bestämmer ändamål och medel med behandlingen. För myndigheters del är det en fråga om myndighetens uppdrag. En myndighet ska i enlighet med legalitetsprincipen inte bedriva verksamhet utan stöd i författning eller uppdrag från regeringen. Det är således ur myndighetens uppdrag som ändamål och medel ska kunna härledas, när en myndighet använder egna utrymmen.

Personuppgiftsansvaret kan vara olika i olika situationer och bero på de faktiska omständigheterna. Personuppgiftsansvaret kan vara både gemensamt och delat. En förutsättning för att myndigheter ska få behandla personuppgifter gemensamt, är att behandlingen har stöd i samtliga inblandade myndigheters uppdrag. I samband med detta är artikel 5 och 6 dataskyddsförordningen relevanta. Det krävs att de grundläggande principerna följs, såsom kravet på berättigat ändamål och uppgiftsminimering. Därutöver måste myndigheterna ha rättsligt stöd för den gemensamma behandlingen och om det är fråga om behandling med stöd av artikel 6.1 c eller e måste grunden vara fastställd i unionsrätt eller nationell rätt, på så sätt som dataskyddsförordningen kräver. Efter en analys av vilken behandling som är tillåten borde det vara möjligt att komma fram till vem eller vilka som är personuppgiftsansvariga. Undantaget i 2 kap. 10 § tryckfrihetsförordningen påverkar inte bedömningen av personuppgiftsansvaret, utan bedömningen ska ske utifrån faktiska omständigheter.

Datainspektionen kan inledningsvis konstatera en grundläggande problematik i utredningen rörande personuppgiftsansvar för egna utrymmen, då man velat undgå att handlingar ska anses vara inkomna till myndigheten, genom att utgå från 2 kap. 10 § första stycket tryckfrihetsförordningen. I denna bestämmelse anges att en handling som förvaras hos en myndighet endast som led i teknisk bearbetning eller teknisk lagring för annans räkning inte anses som allmän handling hos den myndigheten. Detta krav medför att myndigheten inte ska ta del av de uppgifter som en enskild behandlar i ett eget utrymme. Datainspektionen menar att vid bedömning av vem eller vilka som är personuppgiftsansvariga måste man utgå från dataskyddsförordningens bestämmelser då de utgör den primära rättskällan vid behandling av personuppgifter.

Eget utrymme – krav på säkerhetsåtgärder m.m.

Det faktum att en myndighet utformar ett eget utrymme så att det uppfyller kraven i 2 kap. 10 § första stycket tryckfrihetsförordningen saknar betydelse vid tillämpningen av dataskyddsförordningen. Myndigheter omfattas av dataskyddsförordningen när de behandlar personuppgifter. Begreppet *behandling* definieras i artikel 4 dataskyddsförordningen och det omfattar bland annat lagring och tillhandahållande av personuppgifter. I och med att personuppgifter lagras i egna utrymmen är dataskyddsförordningen tillämplig på dem, även om avsikten är att myndigheten inte ska ta del av de uppgifter som en enskild behandlar i ett eget utrymme.

Datainspektionen noterar att utredningen förklarar att en personuppgiftsansvarig som tillhandahåller och anvisar enskilda en särskild kommunikationskanal också ansvarar för den behandling som sker innan uppgifterna inkommit till myndigheten. I betänkandet hänvisas till Högsta förvaltningsdomstolens dom HFD 2012 ref. 21 och utredningen anger att även om den personuppgiftsansvarige inte kan uppfylla sitt ansvar fullt ut är denne skyldig att vidta nödvändiga *säkerhetsåtgärder* för att uppgifterna som behandlas i tjänsten ska ha ett tillräckligt skydd också innan de överförs till den personuppgiftsansvarige i fråga.

Datainspektionen anser att denna formulering är missvisande. Det ovan nämnda rättsfallet avser olika tjänster som Försäkringskassan anvisade, där enskilda avsågs kommunicera med myndigheten genom elektroniska kommunikationskanaler via olika operatörer, såsom Sms-meddelanden. Uppgifterna var inte tillgängliga för Försäkringskassan förrän de nådde kassans elektroniska mottagningsställen. Högsta förvaltningsdomstolen gjorde dock bedömningen att den serie av åtgärder i fråga om personuppgifter som vidtogs i de aktuella fallen kunde betraktas som led i Försäkringskassans behandling av uppgifter i enskilda ärenden och att detta gällde trots att Försäkringskassan saknade möjlighet att påverka hur uppgifterna hanterades innan de blev tillgängliga för kassan. Domstolen bedömde att även om detta innebor svårigheter vid bedömningen av de skyldigheter och sanktionsmöjligheter som föreskrevs i personuppgiftslagen och som tog sikte på personuppgiftsansvaret, så hindrade det emellertid inte att Försäkringskassan ålades att redovisa säkerheten vid behandlingen av personuppgifter enligt 43 § b personuppgiftslagen.

När en myndighet använder sig av egna utrymmen är situationen dock väsentligt annorlunda jämfört med rättsfallet ovan, i och med att de enskilda kommunicerar direkt myndighetens system och att uppgifterna därmed direkt är tillgängliga för myndigheten. Personuppgiftsansvaret när det gäller egna utrymmen begränsar sig således inte till säkerhetsåtgärder. När en

myndighet använder egna utrymmen är den skyldig att beakta även andra krav som följer av dataskyddsförordningen, såsom det grundläggande kravet på uppgiftsminimering enligt artikel 5 c, vilket kan påverka utformningen av utrymmet. Ett annat exempel på sådana krav är skyldigheten att informera de registrerade enligt artikel 13-15 dataskyddsförordningen.

Eget utrymme – allmänna handlingar

Datainspektionen anser att skyldigheten att ge registrerade rätt till information enligt artikel 13-15 innebär att myndigheter är skyldiga att ta del av uppgifter i egna utrymmen även innan avsikten varit att ge in dem till myndigheten. Detta medför att kraven enligt 2 kap. 10 § första stycket tryckfrihetsförordningen inte uppfylls och att handlingarna därmed måste vara att anse som allmänna. Datainspektionen är medveten om att utredningens uppdrag var begränsat så att författningsförslagen inte ska omfatta ändringar av grundlag eller bestämmelser på personuppgiftsområdet. Inspektionen anser dock att när det är bestämmelser rörande allmänna handlingar som utgör hinder för att kunna använda egna utrymmen på önskat vis, måste man peka på behovet av ändringar i det regelverket.

Uppdrag att ta fram allmänna råd eller annat stödmaterial

Utredningen föreslår att en myndighet ska ges i uppdrag att, i samverkan med Datainspektionen och Myndigheten för samhällsskydd och beredskap, ta fram allmänna råd eller annat stödmaterial om hur myndigheter kan utveckla digitala tjänster som innefattar eget utrymme.

Datainspektionen vill framhålla att utgångspunkten för förslag som berör Datainspektionens roll och uppdrag behöver ha sin grund i de krav som följer av dataskyddsförordningen. Inspektionens uppdrag avseende dataskyddsförordningen regleras i dataskyddsförordningen. Det följer av artikel 57 att tillsynsmyndigheten ska övervaka och verkställa tillämpningen av förordningen, men av artikeln följer även uppgifter som att öka allmänhetens medvetenhet, ge råd åt det nationella parlamentet, regeringen och andra institutioner och organ om lagstiftningsåtgärder och administrativa åtgärder rörande skyddet av fysiska personers rättigheter och friheter när det gäller behandling av personuppgifter. Vidare följer av artikel 52.4 att medlemsstaten ska säkerställa att tillsynsmyndigheten förfogar över de personella, tekniska och finansiella resurser som behövs för att myndigheten ska kunna utföra sina uppgifter och utöva sina befogenheter vilka följer av förordningen, inklusive inom ramen för det ömsesidiga biståndet inom EU, samarbetet och deltagandet i styrelsens verksamhet.

Det föreligger vissa juridiska svårigheter i samband med utveckling av digitala tjänster. Några av dessa frågor, såsom begränsning av registrerades rättigheter, kan hanteras genom nationell reglering. Dessa frågor bör dock inte hanteras genom framtagande av allmänna råd, utan lagstiftning. Datainspektionen bedömer således att det är oklart vad som skulle kunna förändras genom det föreslagna uppdraget. De rättsliga svårigheter som föreligger nu, kommer inte att kunna korrigeras eller avhjälpas genom framtagande av allmänna råd och stödmaterial. Mot bakgrund av detta avstyrker Datainspektionen förslaget i denna del.

10. Tystnadsplikt för privata leverantörer

Punkt 2 h i artikel 9 dataskyddsförordningen anger att känsliga personuppgifter får behandlas om det är nödvändigt av skäl som hör samman med bland annat hälso- och sjukvård och social omsorg under förutsättning att de villkor och skyddsåtgärder som avses i punkt 3 är uppfyllda.

I artikel 9.3 dataskyddsförordningen anges följande.

Personuppgifter som avses i punkt 1 får behandlas för de ändamål som avses i punkt 2 h, när uppgifterna behandlas av eller under ansvar av en yrkesutövare som omfattas av tystnadsplikt enligt unionsrätten eller medlemsstaternas nationella rätt eller bestämmelser som fastställs av nationella behöriga organ eller av en annan person som också omfattas av tystnadsplikt enligt unionsrätten eller medlemsstaternas nationella rätt eller bestämmelser som fastställs av nationella behöriga organ.

Kravet på lagreglerad tystnadsplikt är nytt i förhållande till personuppgiftslagen. Datainspektionen kan konstatera att informationshanteringen är central inom hälso- och sjukvård och social omsorg. Det är fråga om en omfattande behandling av känsliga personuppgifter, som är nödvändig för att dessa verksamheter ska fungera. Inspektionen tillstyrker således förslaget till lag om tystnadsplikt vid utkontraktering av teknisk bearbetning och lagring. En lagstadgad tystnadsplikt för de personuppgiftsbiträden som idag inte omfattas av en sådan behöver införas för att den personuppgiftsbehandling som sker idag inom hälso- och sjukvård och social omsorg ska vara förenlig med artikel 9.2 h och 9.3 i dataskyddsförordningen.

11. It-avtal

Utredningens föreslår att Datainspektionen, Myndigheten för digital förvaltning och Myndigheten för samhällsskydd och beredskap ska få i

särskilt uppdrag att gemensamt och i samråd med Sveriges kommuner och landsting, utforma standardavtalsklausuler för personuppgiftsbiträdesavtal som tecknas mellan en myndighet som personuppgiftsansvarig och en privat leverantör som personuppgiftsbiträde inom ramen för myndighetens köp av it-drift eller andra it-baserade funktioner.

Det är positivt med samverkan mellan myndigheter på områden där myndigheterna har angränsande uppdrag. Datainspektionens möjlighet att fastställa standardavtalsklausuler för personuppgiftsbiträdesavtal regleras i artikel 28.8 dataskyddsförordningen. Enligt artikel 64 dataskyddsförordningen krävs det att inspektionen inhämtar yttrande från Europeiska dataskyddsstyrelsen.

Datainspektionen ska i sitt uppdrag som tillsynsmyndighet enligt dataskyddsförordningen också vara oberoende. Detta innebär betydande svårigheter för ett nationellt samarbete på så sätt som föreslås. Utöver detta bör man beakta att det aktuella området är stort och komplext, då det inte enbart omfattar den offentliga sektorn utan även innebär att man måste tillgodose den privata sektorns behov. Komplexiteten belyses av att andra myndigheter synes ha betydande svårigheter att lösa dessa frågor. Mot bakgrund av dessa omständigheter avstyrker Datainspektionen förslaget i denna del.

Detta beslut har fattats av generaldirektören Lena Lindgren Schelin efter föredragning av juristen Mattias Sandström. Vid den slutliga handläggningen har även chefsjuristen Hans-Olof Lindblom deltagit.

Lena Lindgren Schelin, 2018-10-04 (Det här är en elektronisk signatur)