Promemoria

En modern registerförfattning

ES2022-06

Juni 2022

Sammanfattning

Senare års samhällsutveckling har lett till att många registerförfattningar i dag är föråldrade. Ofta är regleringen begränsande utan att medföra större skydd för enskildas integritet. Dagens registerförfattningar skapar en problematik för myndigheters verksamhet, främst inom digitaliseringsområdet. Specificerade ändamålsbestämmelser samt detaljerade uppräkningar av vilka personuppgifter som får behandlas hindrar myndigheten från att fullgöra sitt författningsenliga uppdrag. Det föreligger onödiga begränsningar för hur uppgifter kan användas i myndighetens utvecklingsverksamhet. Regleringar av formen för utlämnande av uppgifter kan t.ex. hindra möjligheten att erbjuda e-tjänster. Dagens utformning av registerförfattningarna utgör ett hinder för myndigheternas digitala transformation.

För att regeringens mål för digitalisering av den offentliga förvaltningen ska kunna uppnås måste det bli enklare för myndigheter att, i enlighet med de krav som uppställs i dataskyddsförordningen, utföra den personuppgiftsbehandling som krävs för myndighetens uppdrag.

eSam anser att registerförfattningarna bör moderniseras för att stödja digitaliseringen med bibehållet integritetsskydd. I promemorian ges förslag på hur en sådan utformning skulle kunna se ut. Arbetet har avgränsats till två huvudfrågor: en alltför detaljerad ändamålsreglering samt begränsningar av formerna för utlämnanden. Förslagen utgör en grundreglering som kan utvecklas med beaktande av varje myndighets behov och förutsättningar.

eSam förespråkar följande:

Ändamålsbestämmelse
Ändamålsbestämmelser bör formuleras så att myndigheten får behandla personuppgifter om det är nödvändigt för att myndigheten ska kunna utföra sina uppgifter enligt lag eller förordning.

Finalitetsprincipen
Registerförfattningar ska som huvudregel inte innehålla någon bestämmelse som reglerar finalitetsprincipen. I stället ska principen i dataskyddsförordningen gälla, om inte lagstiftaren uttryckligen angett att principen inte är tillämplig. Vidarebehandling av känsliga personuppgifter behöver inte regleras särskilt.

Registerinnehåll
Registerförfattningar ska som huvudregel inte innehålla bestämmelser om vilka personuppgifter som får behandlas. Om det behövs av särskilda skäl föreslår eSam en reglering av

- att vissa särskilt känsliga personuppgifter inte får behandlas eller ska behandlas på visst sätt, eller
- att registret minst ska innehålla vissa personuppgifter.

Om en uppräkning behövs bör den om möjligt avse kategorier av uppgifter och regleras på en så låg normgivningsnivå som möjligt. Det bör göras en tydlig åtskillnad mellan å ena sidan sådana uppgifter som ingår i själva registret och å andra sidan sådana uppgifter som den registerförande myndigheten får behandla för att kunna utföra sina skyldigheter kopplade till registret.

Utlämnande av information från myndigheter
Registerförfattningars reglering kring utlämnanden ska vara teknikneutrala utan att uppställa något särskilt krav på formen för utlämnande. Direktåtkomst ska endast regleras i författning om sådan åtkomst behöver begränsas. I annat fall ska det vara upp till myndigheten att avgöra formen för utlämnande.

Sekretessbrytande bestämmelser
Registerförfattningarna bör renodlas från sekretessbrytande bestämmelser. Dessa bör i stället finnas i offentlighets- och sekretesslagstiftningen eller i materiell författning.

Innehåll

1. Inledning ... 7
   1.1 Allmänt om registerförfattningar ... 8
   1.2 Registerförfattningarnas relation till dataskyddsförordningen ... 10
   1.3 Problem med registerförfattningar ... 11
2. Ändamålsbestämmelser ... 13
   2.1 Allmänt om ändamål ... 14
   2.2 Reglering av myndigheternas verksamhet ... 14
      2.2.1 Legalitetsprincipen ... 14
      2.2.2 Fastställelse av den rättsliga grunden ... 14
      2.2.3 Regeringsformen ställer krav på lagform i vissa fall ... 16
   2.3 Ändamålsbestämmelser behövs ... 16
      2.3.1 Hur ändamålsbestämmelserna bör formuleras ... 17
      2.3.2 När detaljerade ändamålsbestämmelser ändå kan behövas ... 18
   2.4 Säkerhetsåtgärder och andra obligatoriska åtgärder ... 18
   2.5 Behov av konsekvensbedömning avseende dataskydd i lagstiftningsarbetet ... 19
3. Finalitetsprincipen ... 20
   3.1 Allmänt om finalitetsprincipen ... 20
      3.1.1 Finalitetsprincipen i registerförfattning ... 21
      3.1.2 Tillämpning av finalitetsprincipen ... 22
      3.1.3 Särskilt om överföring till andra myndigheter ... 23
      3.1.4 Särskilt om testverksamhet ... 24
4. Registerinnehåll ... 26
   4.1 Allmänt om registerinnehåll ... 26
      4.1.1 Bakgrund ... 26
      4.1.2 Behovet av bestämmelser om registerinnehåll ... 27
      4.1.3 Vilka uppgifter behöver myndigheter behandla? ... 28
   4.2 Närmare om förslaget till reglering av registerinnehåll ... 29
5. Formen för utlämnande av information från myndigheter ... 31
   5.1 Allmänt om utlämnande ... 31
   5.2 Reglering gällande form för utlämnande ... 32
   5.3 Formerna för elektroniskt utlämnande ... 33
      5.3.1 Utlämnande på medium för automatiserad behandling ... 33
      5.3.2 Direktåtkomst ... 34
      5.3.3 Skillnaden mellan direktåtkomst och annat elektroniskt utlämnande ... 38
   5.4 Formen för utlämnande ska som huvudregel inte regleras ... 41

5.4.1 Teknikneutralitet som huvudregel 41
5.4.2 Ansvarsprincipen 42
5.4.3 Val av utlämnandeform 42
5.4.4 Rekvisitet "olämpligt" är obehövligt 43
6. Sekretessbrytande bestämmelser 46

1. Inledning

De flesta myndigheter har egna registerförfattningar som reglerar hur personuppgifter får behandlas inom myndigheten. Rättsområdet är svåröverblickbart och fragmentariskt och det har tidigare funnits ambitioner att samla regleringen i en enda lag om myndigheters behandling av personuppgifter. Dessa förslag har emellertid inte lett till lagstiftning. I samband med ikraftträdande av dataskyddsförordningen[1] år 2018 gjordes en översyn av samtliga registerförfattningars förenlighet med den nya förordningen. Detta ledde enbart till smärre justeringar och den myndighetsspecifika lagstiftningen behölls, som ett komplement till dataskyddsförordningen.

Senare års samhällsutveckling har lett till att många registerförfattningar i dag är föråldrade. Ofta är regleringen begränsande utan att medföra större skydd för enskildas integritet. För att regeringens mål[2] för digitalisering av den offentliga förvaltningen ska kunna uppnås måste det bli enklare för myndigheter att, i enlighet med de krav som uppställs i dataskyddsförordningen, utföra den personuppgiftsbehandling som krävs för myndighetens uppdrag.

Syftet med denna promemoria är att belysa den problematik som dagens registerförfattningar skapar för myndigheters verksamhet, främst inom digitaliseringsområdet. I promemorian ges förslag till hur registerförfattningar skulle kunna moderniseras för att stödja digitaliseringen med bibehållet integritetsskydd. Förslagen utgör en grundreglering som kan utvecklas med beaktande av varje myndighets behov och förutsättningar. I vissa fall, beroende på myndighetens uppdrag och verksamhet samt personuppgifternas känslighet, kan en större detaljeringsgrad behövas i den tillämpliga registerförfattningen. Särreglering kan behövas både vad avser hur ändamålen formuleras och vilka kategorier av personuppgifter som får behandlas. En bärande tanke i denna promemoria är att utgångspunkten för allt arbete med att ta fram eller förändra registerförfattningar alltid bör vara enkelhet och breda formuleringar i lag och förordning. En högre grad av precisering bör motiveras särskilt, i stället för tvärtom. Historiskt sett har utgångspunkten många gånger varit just den omvända, dvs. en hög detaljeringsgrad som successivt fått hanteras i takt med att problem i tillämpningen uppstår samt teknik och myndighetsuppdrag utvecklas.

Promemorian tar i första hand sikte på registerförfattningar som kompletterar dataskyddsförordningen. Arbetet är avgränsat till två huvudfrågor: en alltför detaljerad ändamålsreglering samt begränsningar av formerna för utlämnanden. Promemorian

[1] 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).
[2] Se bl.a. nationella datastrategin och digitaliseringsstrategin.

riktar sig i första hand till jurister, men bör vara av betydelse även för en vidare krets. Tanken är att innehållet ska kunna användas av myndigheter vid utformning av remiss och hemställan. Förhoppningen är också att promemorian ska beaktas av lagstiftaren i det rättsutvecklande arbetet.

Arbetet med att ta fram promemorian har genomförts av en särskild arbetsgrupp bestående av Sofie Wildiér, Jens Västberg, Gunnar Svensson, Ann Svensson, Erik Janzon, Malgorzata Drewniak, Marie-Louise Orre, Hugo Lloyd, Jenny Wentrup, Magnus Ahlgren, Tina Hård, Emma Gardfors och Linda Lindström. Kvalitetssäkring har skett i eSams rättsliga expertgrupp, expertgruppen i säkerhet samt koordineringsgruppen för arkitektur. Beredning har skett via eSams samordningsgrupp och promemorian har remitterats till Integritetsskyddsmyndigheten.

1.1 Allmänt om registerförfattningar

Registerförfattningar reglerar en myndighets personuppgiftsbehandling och syftar till att garantera enskilda registrerade ett skydd för deras personliga integritet. I svensk rätt finns en mängd olika registerförfattningar. År 2015 föreslog Informationshanterings-utredningen en ny modellreglering för registerförfattningar genom en ny generellt tillämplig lag – myndighetsdatalagen. Förslaget ledde emellertid inte till lagstiftning.

I Informationshanteringsutredningens uppdrag ingick att inventera befintliga registerförfattningar. Utifrån inventeringen sorterade utredningen författningarna i tre kategorier: renodlade registerförfattningar, informationshanteringsförfattningar och annan reglering med inslag av dataskyddsbestämmelser.[3]

De renodlade registerförfattningarna[4] utmärks av att tillämpningsområdet endast avser inrättandet, förandet och användningen av ett register eller annan bestämd informationssamling. Genom en sådan registerförfattning åläggs en myndighet att föra ett visst register och registerföringen blir genom författningsregleringen en del i myndighetens uppdrag. I de flesta fall utgörs regleringen av förordningar. Om författningarna har lagform så har i allmänhet åberopats riksdagens och regeringens ställningstagande i början av 1990-talet om att myndighetsregister med ett stort antal registrerade och ett särskilt känsligt innehåll bör regleras särskilt i lag i syfte att stärka skyddet för de registrerades integritet.[5]

[3] SOU 2015:39 s. 96 f.
[4] I de flesta fall rör det sig om förordningar, men de kan också ha lagform. Exempel på renodlade registerförfattningar är förordningen (2014:885) om register över vigselförrättare samt lagen (2012:453) om register över nationella vaccinprogram.
[5] SOU 2015:39 s. 97 ff.

Informationshanteringsförfattningarna[6] har som övergripande funktion att särreglera personuppgiftsbehandling inom vissa utpekade verksamheter eller myndigheter. Oftast omfattar regleringen såväl registerföring och ärendehanteringssystem eller andra strukturerade personuppgiftssamlingar som annan slags behandling utan koppling till ärendehanteringssystem, såsom behandling i löpande text. Utmärkande för denna kategori av registerförfattningar är att de i huvudsak reglerar vilken personuppgiftsbehandling myndigheter får utföra inom ramen för författningens tillämpningsområde. Inte sällan finns dock särbestämmelser rörande vissa register, databaser eller gemensamt tillgängliga uppgiftssamlingar som får eller ska finnas i den aktuella myndighetens verksamhet. På de områden där det finns mer eller mindre heltäckande informationshanteringsförfattningar för berörda myndigheters verksamhet brukar det indirekt av de beskrivna tillämpningsområdena och genom förarbetsuttalanden framgå att myndigheternas personal- och ekonomiadministration inte omfattas av regleringen i fråga.

Det finns många likheter mellan renodlade registerförfattningar och informationshanteringsförfattningar. Ofta reglerar båda dessa kategorier personuppgiftsansvar, tillåtna ändamål för dels insamling och myndighetens egen användning av personuppgifter (primära ändamål), dels tillhandahållande av personuppgifter till externa mottagare (sekundära ändamål), vilka personuppgifter som får behandlas, betydelsen av den registrerades inställning till behandlingen, sökbegrepp, specifika hanteringsregler för register, databaser eller andra uppgiftssamlingar, säkerhetsfrågor såsom begränsningar av tillgången till lagrade personuppgifter, direktåtkomst och annat elektroniskt utlämnande samt bevarande och gallring.[7]

Den tredje kategorin är egentligen inte registerförfattningar alls, utan *annan reglering med inslag av dataskyddsbestämmelser*. Till denna kategori hör olika slags författningar som bara till en mindre del innehåller bestämmelser som rör personuppgiftsbehandling och i den delen utgör särreglering i förhållande till den generella dataskyddsregleringen, t.ex. vissa bestämmelser om registerföring i skogsvårdslagen (1979:429) och vapenlagen (1996:67).[8] Aktuell promemoria omfattar inte denna kategori.

[6] T.ex. lagen (2001:184) om behandling av uppgifter i Kronofogdemyndighetens verksamhet med tillhörande förordning samt lagen (2002:546) om behandling av personuppgifter inom den arbetsmarknadspolitiska verksamheten med tillhörande förordning.
[7] SOU 2015:39 s. 100 ff.
[8] SOU 2015:39 s. 103.

1.2 Registerförfattningarnas relation till dataskyddsförordningen

Ytterst är det dataskyddsförordningen som reglerar personuppgiftsbehandling i svensk rätt.[9] Myndighetsspecifika registerförfattningar kompletterar dataskyddsförordningen och innehåller avvikelser som ansetts nödvändiga eller lämpliga på det aktuella området i förhållande till det generella dataskyddet.

Informationshanteringsförfattningar innehåller ofta reglering som inte rör ren personuppgiftsbehandling, såsom uppgiftsskyldighet och sekretessbrytande bestämmelser. eSam förespråkar att registerförfattningar renodlas till en dataskyddslagstiftning. Det är också så att de juridiska begreppen i registerförfattningar inte alltid överensstämmer med begreppen i dataskyddsförordningen, vilket kan försvåra tillämpningen. Enligt Informationshanteringsutredningen har det i många registerförfattningar skett en sammanblandning mellan vad som i dataskyddsrättslig mening är *särskilda bestämda ändamål* respektive tillåtna *rättsliga grunder för behandling.*[10] Vidare finns det i registerförfattningar begrepp som inte alls regleras i dataskyddsförordningen. eSam är av uppfattningen att den nomenklatur som används i dataskyddsförordningen så långt det är möjligt bör användas även i registerförfattningar.

Ändamål

Personuppgifter ska enligt artikel 5.1 b i dataskyddsförordningen samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål. Av artikel 4.7 framgår att ändamålen och medlen för behandlingen ska bestämmas av den personuppgiftsansvarige. Dataskyddsförordningen ställer inte något krav på att de särskilda ändamålen ska vara fastställda i författning, men det finns heller inget som hindrar att detta görs, förutsatt att bestämmelserna uppfyller ett mål av allmänt intresse och är proportionella mot det legitima mål som eftersträvas, enligt artikel 6.3 andra stycket.[11] Ändamålsbestämmelser i registerförfattning utgör sådan reglering. Oavsett om ändamålen fastställts i författning eller inte är det dock alltid den personuppgiftsansvarige som ansvarar för, och ska kunna visa att, principerna i artikel 5 efterlevs. Enligt skäl 39 till dataskyddsförordningen bör de specifika ändamål som personuppgifterna behandlas för vara tydliga och legitima och ha bestämts vid den tidpunkt då personuppgifterna samlades in.

[9] Dataskyddsförordningen kompletteras i svensk rätt av dataskyddslagen (2018:218) och kompletteringsförordningen (2018:219). Vid 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 samt vid behandling av personuppgifter som en behörig myndighet utför i syfte att upprätthålla allmän ordning och säkerhet gäller i stället brottsdatalagen (2018:1177) och brottsdataförordningen (2018:1202,) som i svensk rätt genomför dataskyddsdirektivet.
[10] SOU 2015:39 s. 279.
[11] Prop. 2017/18:105 s. 48.

Rättslig grund för behandling

Enligt dataskyddsförordningen får behandling av personuppgifter bara ske om det finns en *rättslig grund* för behandlingen. I artikel 6 formuleras ett antal alternativa krav på den rättsliga grunden för en behandling, varav åtminstone ett måste vara uppfyllt för att behandlingen ska vara laglig i dataskyddsförordningens mening. För myndigheter är det främst två rättsliga grunder som är aktuella. Enligt artikel 6.1 c och e finns rättslig grund om behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige eller om behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning. Av artikel 6.3 första stycket framgår att den rättsliga grund för behandlingen som avses i artikel 6.1 c och e ska fastställas i enlighet med unionsrätten eller nationell rätt.

Sambandet mellan ändamål och rättslig grund

Syftet med personuppgiftsbehandlingen ska fastställas i den rättsliga grunden eller, i fråga om behandling enligt punkt 6.1 e, vara nödvändigt för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning (artikel 6.3 andra stycket). *Ändamålet* för varje enskild behandling av personuppgifter måste således vara nödvändigt. Det måste finnas ett samband mellan behandlingen av personuppgifter och den rättsliga förpliktelsen alternativt den fastställda arbetsuppgiften eller myndighetsutövningen.

1.3 Problem med registerförfattningar

Registerförfattningarna, som reglerar hur myndigheter får behandla personuppgifter i sina verksamheter, är inte följden av ett systematiskt arbete. De framstår snarare som ett lapptäcke av föråldrade författningar inom ett svåröverblickbart och fragmenterat rättsområde med bristande enhetlighet, struktur och normtekniska lösningar. Detta medför stora svårigheter för myndigheterna att hänga med i den tekniska utvecklingen, särskilt när det gäller utveckling av en effektiv och samverkande e-förvaltning.[12]

Tydligt avgränsade och specificerade ändamålsbestämmelser samt detaljerade uppräkningar av vilka personuppgifter som får behandlas står ofta i kontrast till myndighetens uttryckliga uppdrag som är bredare formulerat i andra författningar eller regeringsbeslut. Regleringarna innebär att det uppstår hinder för myndigheten att fullgöra sitt författningsenliga uppdrag,[13] vilket egentligen inte är föranlett av några reella risker för den personliga integriteten, utan oftast uteslutande är av lagteknisk karaktär.

[12] eSams skrivelse Behov av samlad översyn av registerförfattningarna, VER 2015:190.
[13] Se Försäkringskassans och Pensionsmyndighetens hemställan om ändringar i 114 kap. SFB och förordningen (2003:766) om behandling av personuppgifter inom socialförsäkringens administration, FK 2020/001747 resp. VER 2020-180, Kriminalvårdens framställan om översyn av Kriminalvårdens registerförfattningar på dataskyddsområdet, KV 2020-16617 samt lagen (2006:378) om lägenhetsregister och förordning (2007:108) om lägenhetsregister.

Det är vanligt förekommande att myndigheter ställs inför en osäkerhet om en utvecklingsinsats ryms inom befintliga ändamål. Ofta uppstår frågor kring testverksamhet och om detta är tillåtet inom befintlig reglering i registerförfattningen. Osäkerhet föreligger kring möjligheterna att använda data inom myndighetens verksamhet för AI-utveckling.

Regeringen har i sin digitaliseringsstrategi uttryckt en vision om ett hållbart digitaliserat Sverige med det övergripande målet att Sverige ska vara bäst i världen på att använda digitaliseringens möjligheter.[14] Flera registerförfattningar innehåller begränsningar i när uppgifter får lämnas ut elektroniskt,[15] vilket försvårar att bidra till regeringens mål. Exempelvis kan regleringarna innebära hinder för myndigheterna att ge medborgarna digital service i form av e-tjänster.[16]

Bestämmelser om direktåtkomst ger upphov till olika tolkningar och missförstånd mellan parter som ska utbyta uppgifter. Diskussionen förflyttas till att handla om lagtolkning i stället för att fokusera på åtgärder som i praktiken skulle stärka skyddet för den personliga integriteten, exempelvis vilka åtgärder som behöver vidtas av vilken part avseende informationssäkerheten.

[14] För ett hållbart digitaliserat Sverige – en digitaliseringsstrategi, N2017/03643/D.
[15] Se Arbetsförmedlingens hemställan En mer träffsäker och enhetlig arbetsmarknadspolitisk bedömning och förbättrad kvalitet i uppföljningen av matchningstjänster, Af-2022/0013 1747, 2022-02-22.
[16] Se Kronofogdemyndighetens hemställan Bättre och snabbare service i Kronofogdemyndighetens verksamhet, KFM 22992-2020.

2. Ändamålsbestämmelser

eSam förespråkar att registerförfattningars ändamålsbestämmelser formuleras enligt följande.

[Myndighetens namn] får behandla personuppgifter om det är nödvändigt för att myndigheten ska kunna utföra sina uppgifter enligt lag eller förordning.

Formuleringen omfattar även uppdrag som myndigheten får i regleringsbrev eller i särskilda beslut av regeringen. Sådana uppdrag måste vara förenliga med överordnade författningar, däribland regeringsformens bestämmelser om regeringens styrning av myndigheterna.[17]

Med behandling menas såväl insamling som efterföljande behandling, som ryms inom det angivna insamlingsändamålet. Formuleringen omfattar också utlämnande av personuppgifter till annan myndighet eller organisation, när det framgår av lag eller förordning att utlämnande ska eller får ske. Den traditionella uppdelningen i primära och sekundära ändamål är därför inte nödvändig, vilket överensstämmer med dataskyddsförordningens reglering.

Föreslagen formulering bör alltid användas som utgångspunkt. Det kan förekomma situationer och verksamheter där ändamålen behöver specificeras ytterligare av lagstiftaren. Den vägledande principen bör emellertid vara att det krävs skäl av viss tyngd för att frångå denna formulering. I vissa fall kan en lösning i stället vara att i lagen reglera säkerhetsåtgärder, såsom sökbegränsningar.

När de tillåtna ändamålen för myndigheten är brett formulerade i registerförfattning ställs högre krav på myndigheten för att uppfylla de krav som finns i dataskyddsförordningen. Myndigheten måste göra en behovsanalys för att bedöma om behandling av uppgifterna ligger inom myndighetens uppdrag och även formulera ett specifikt ändamål för varje insamling av uppgifter. Varje senare behandling måste också ställas mot detta insamlingsändamål. Detta kan innebära ett större arbete initialt för myndigheten, men har den fördelen att tillåtna ändamål för behandling kan utvecklas i symbios med myndighetens uppdrag.

[17] I förarbetena till dataskyddslagen uttrycks detta på följande vis. ”Myndigheternas uppdrag och åligganden framgår av författningar, regeringsbeslut och kommunala reglementen, antagna i enlighet med regeringsformens bestämmelser om normgivningskompetens och kommunalt självstyre. De åtgärder som myndigheterna vidtar i syfte att utföra dessa uppdrag eller uppfylla dessa åligganden har därmed i sig en legal grund, som har offentliggjorts genom tydliga, precisa och förutsebara regler” (prop. 2017/18:105, sid. 57).

2.1 Allmänt om ändamål

Vid behandling av personuppgifter är ändamålet av central betydelse och ändamålsbestämningen påverkar bedömningen i flera led. Enligt artikel 5.1 b. i dataskyddsförordningen ska personuppgifter samlas in för vissa angivna ändamål och eventuell vidarebehandling av uppgifterna ska prövas gentemot dessa ändamål. Artikel 5.1 c anger att personuppgifter ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas. Ändamålet har också betydelse bl.a. för vad som är en lämplig säkerhetsnivå enligt artikel 32 i dataskyddsförordningen. Vidare ska det register som varje personuppgiftsansvarig ska föra över behandling enligt artikel 30 innehålla uppgift om ändamålet med behandlingen, liksom den information som ska lämnas till den registrerade enligt artikel 13–15. Även vid bedömning av rätt till rättelse, radering och begränsning av behandling enligt artikel 16–18 i dataskyddsförordningen görs avvägningar med beaktande av ändamålet med behandlingen. De angivna ändamålen har således stor betydelse inom dataskyddsregleringen.

När det kommer till myndigheters verksamhet har lagstiftaren genom registerförfattningar anpassat tillämpningen av dataskyddsförordningen.

2.2 Reglering av myndigheternas verksamhet

2.2.1 Legalitetsprincipen

Den offentliga makten ska utövas under lagarna. Lagstiftaren lämnar uppdrag till förvaltningen på olika sätt, exempelvis genom allmänna bestämmelser i lag eller detaljerade regler i speciallagstiftning. Regeringen formulerar också myndighetens uppdrag genom bestämmelser i myndighetens instruktion eller i annan förordning. Legalitetskravet kan också uppfyllas genom ett förvaltningsbeslut av regeringen, t.ex. när åtgärden ska utföras enligt myndighetens regleringsbrev.

2.2.2 Fastställelse av den rättsliga grunden

I propositionen Ny dataskyddslag konstaterar regeringen att en rättslig grund inte måste fastställas i en av riksdagen beslutad lag men däremot att grunden måste vara fastställd i laga ordning, dvs. på ett konstitutionellt korrekt sätt.[18]

Vad detta konkret innebär i svensk rätt har förtydligats i lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen). Enligt

[18] Prop. 2017/18:105 s. 51.

2 kap. 1 § dataskyddslagen får personuppgifter behandlas med stöd av artikel 6.1 c i dataskyddsförordningen, om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna fullgöra en rättslig förpliktelse som följer av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning. Tydliga uppdrag att behandla personuppgifter i författning, exempelvis en myndighets instruktion, kan också utgöra en rättslig förpliktelse.

Enligt 2 kap. 2 § dataskyddslagen får personuppgifter behandlas med stöd av artikel 6.1 e i dataskyddsförordningen, om behandlingen är nödvändig för att utföra en uppgift av allmänt intresse som följer av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning, eller som ett led i den personuppgiftsansvariges myndighetsutövning enligt lag eller annan författning.

I normalfallet utgör en myndighets uppdrag enligt författning, instruktion eller regleringsbrev en rättslig grund för behandling av personuppgifter enligt artikel 6.1 e. All verksamhet som myndigheter ska bedriva, inom ramen för sin befogenhet, anses vara av allmänt intresse. Vissa myndigheter har av riksdagen eller regeringen getts befogenhet att bedriva viss uppdragsverksamhet. Även denna typ av verksamhet är motiverad av ett allmänt intresse.[19]

Av skäl 41 framgår också att den rättsliga grunden bör vara tydlig och precis och dess tillämpning förutsägbar för dem som omfattas av den, i enlighet med rättspraxis vid Europeiska unionens domstol och Europeiska domstolen för de mänskliga rättigheterna. Vilken grad av tydlighet och precision som krävs i fråga om den rättsliga grunden för att en viss behandling av personuppgifter ska anses vara nödvändig måste bedömas från fall till fall, utifrån behandlingens karaktär. En behandling av personuppgifter som inte utgör någon egentlig kränkning av den personliga integriteten kan ske med stöd av en rättslig grund som är allmänt hållen medan ett mer kännbart intrång kräver att den rättsliga grunden är mer preciserad och därmed gör intrånget förutsebart.[20]

Om en myndighets verksamhet är väl reglerad finns mindre behov av en registerförfattning. Inför dataskyddsförordningens ikraftträdande aktualiserades frågan om behovet av en särskild registerförfattning för utbildningsområdet. Regeringen uttalade då att syftet med behandling av personuppgifter inom utbildningsområdet tydligt framgår av bestämmelserna i skollagen, högskolelagen, lagen om yrkeshögskolan och de andra författningar som reglerar verksamheten på området och att det är förutsägbart för personer som omfattas av dessa regler vilken behandling av personuppgifter som är nödvändig för att personuppgiftsansvariga ska kunna utföra sina

[19] Prop. 2019/20:106 s. 37 samt prop. 2017/18:105 s. 53-54 och s. 56-59.
[20] Jfr prop. 2017/18:218 s. 122.

uppdrag och åligganden.[21] Det ansågs då saknas skäl att införa ytterligare registerförfattningar om behandling av personuppgifter inom utbildningsområdet.

2.2.3 Regeringsformen ställer krav på lagform i vissa fall

Enligt 2 kap. 6 § 2 st. regeringsformen (RF) 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. Av 2 kap. 20 § 1 st. 2 p. RF framgår att skyddet mot intrång som innebär övervakning och kartläggning av den enskildes personliga förhållanden är en fri- och rättighet som bara får begränsas genom lag i den utsträckning som medges i 21–24 §§ RF.

2.3 Ändamålsbestämmelser behövs

Det skulle kunna ifrågasättas vilken funktion eller mervärde en sådan ändamålsbestämmelse som eSam föreslår egentligen har, eftersom den enbart hänvisar till annan lag eller förordning. Det kan diskuteras om ändamålsbestämmelsen helt hade kunnat tas bort.

Informationshanteringsutredningen lämnade i betänkandet Myndighetsdatalag (SOU 2015:39) förslag till en registerförfattning som helt saknade ändamålsbestämmelser och som i princip skulle reglera personuppgiftsbehandlingen vid alla statliga och kommunala myndigheter. Utredningens förslag ledde inte till lagstiftning. I remissvaren riktades kritik bl.a. mot att förslaget inte var förenligt med 2 kap. 6 § 2 st. RF.

Regeringen har i senare lagstiftningsarbete uttalat att borttagande av ändamålsbestämmelserna skulle leda till otydlighet och oförutsebarhet och inte vara till nytta för vare sig myndigheterna eller de registrerade personerna.[22] eSam instämmer i denna bedömning. Ändamålsbestämmelserna fyller en viktig funktion eftersom de sätter ramar för behandlingen av personuppgifter, vilket begränsar den personuppgiftsansvariges handlingsfrihet samtidigt som de skapar tydlighet för tillämparen. Genom föreslagen formulering framgår tydligt att det är myndighetens uppdrag som utgör ramen. Bestämmelsen blir därför av central betydelse för skyddet av den enskildes personliga integritet. Enligt artikel 23.2 a ska dessutom lagstiftning som begränsar tillämpningsområdet för förordningens rättigheter och skyldigheter innehålla specifika ändamålsbestämmelser, när så är relevant.

[21] Prop. 2017/18:218, sid. 122.
[22] Se prop. 2017/18:112 s. 53.

2.3.1 Hur ändamålsbestämmelserna bör formuleras

Med hänsyn till den snabba digitala utvecklingen och svårigheten att förutsäga myndigheternas framtida behov av personuppgiftsbehandling, förordas den bredare formen av ändamålsbestämmelse, som får kompletteras med specificerade ändamål som fastställs av myndigheterna själva inför varje enskild behandling.

Det finns både för- och nackdelar med en detaljerad respektive bredare ändamålsbestämmelse. En detaljerad uppräkning av de ändamål för vilka myndigheten får behandla personuppgifter är tydligare och mer förutsebar för såväl tillämpare som de registrerade. Vid behov kan personuppgifter behandlas för en kombination av flera olika ändamål. Vida ändamål förutsätter att myndigheten anger specifika ändamål för varje enskild behandling, vilket i sig medför en mer omständlig hantering. Å andra sidan ger en vid ändamålsbestämmelse ett större utrymme att behandla personuppgifter för de ändamål som myndighetens uppdrag förutsätter. En ökad flexibilitet i ändamålsutformningen ger verksamheten förutsättningar att hålla jämna steg med samhällsutvecklingen.

Det finns olika sätt att formulera ändamålsbestämmelser. En begränsad bestämmelse finns t.ex. i 4 § studiestödsdatalagen (2009:287) där handläggning av ärenden anges som ett ändamål, medan administration respektive förberedelse av handläggning är två andra ändamål. Centrala studiestödsnämnden (CSN) får därutöver behandla personuppgifter för vissa andra specificerade ändamål. Även Skatteverket måste förhålla sig till en detaljerad uppräkning i sin ändamålsbestämmelse i 1 kap. 4 § lagen (2001:181) om behandling av uppgifter i Skatteverkets beskattningsverksamhet.

Det finns dock registerlagstiftning även inom dataskyddsförordningens tillämpningsområde som har en bredare och mindre detaljerad ändamålsbestämmelse. Enligt 2 kap. 1 § lagen (2020:421) om Rättsmedicinalverkets behandling av personuppgifter får Rättsmedicinalverket behandla personuppgifter om det är nödvändigt för att myndigheten ska kunna utföra sina uppgifter i den rättspsykiatriska, rättskemiska, rättsmedicinska eller rättsgenetiska verksamheten. Utformningen av ändamålsbestämmelsen anges i förarbetena utgöra en lämplig avgränsning som beaktar både verksamhetens behov av att behandla personuppgifter och skyddet för enskildas personliga integritet. Regeringen konstaterar dock att för att leva upp till dataskyddsförordningens krav på särskilda, uttryckligt angivna och berättigade ändamål kommer Rättsmedicinalverket normalt också att behöva formulera mer preciserade

ändamål för de specifika behandlingar av personuppgifter som sker i myndighetens verksamhet.[23]

Brett formulerade ändamålsbestämmelser i registerförfattningar kan göra det nödvändigt att införa andra, integritetshöjande villkor i författningarna, beroende på personuppgifternas känslighet, detaljeringsgrad, antalet registrerade, den potentiella spridningen m.m. Det kan exempelvis röra sig om en uttrycklig sökbegränsning med innebörden att det är förbjudet att göra sökningar i syfte att få fram ett urval av personer grundat på personuppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening eller som rör sexualliv eller sexuell läggning.[24] Ett annat exempel på integritetshöjande villkor i lagstiftningen är s.k. integritetshöjande samtycken, som inte utgör laglig grund för behandlingen, men utan vilkas inhämtande viss behandling inte får ske.[25] Ett liknande integritetshöjande villkor är s.k. opt-out, enligt vilket personuppgifter inte får behandlas om den enskilde motsätter sig det.[26]

2.3.2 När detaljerade ändamålsbestämmelser ändå kan behövas

I vissa situationer kan det behövas snävare ändamålsbestämmelser, såsom när det rör sig om behandling av mycket integritetskänsliga uppgifter. Ett exempel på detta är lagen (2020:422) om Rättsmedicinalverkets elimineringsdatabas. I lagen, som rör register över dna-profiler, förskrivs att uppgifter i elimineringsdatabasen endast får behandlas för att upptäcka och utreda kontamineringar av det som är föremål för dna-analys. Således kan uppgifterna inte användas för andra ändamål, som att utreda brottsmisstankar mot dem som ingår i elimineringsdatabasen, bl.a. personer som är anställda vid Rättsmedicinalverket som i den egenskapen kommer i kontakt med det som är föremål för dna-analys.

2.4 Säkerhetsåtgärder och andra obligatoriska åtgärder

Av artikel 24, 25 och 32 i dataskyddsförordningen följer att en personuppgiftsansvarig myndighet vid behandling av personuppgifter är skyldig att säkerställa skyddet av dessa genom att vidta lämpliga tekniska och organisatoriska åtgärder. Däribland finns skyldighet att begränsa möjligheterna till åtkomst och kontrollera åtkomsten till personuppgifter t.ex. genom att generera, bevara och analysera åtkomstloggar. Den personuppgiftsbehandling som måste ske för att uppfylla säkerhetskraven följer således

[23] Prop. 2019/20:106 s. 39.
[24] Ett exempel på sådan sökbegränsning finns i 2 kap. 3 § lagen (2020:421) om Rättsmedicinalverkets behandling av personuppgifter.
[25] En sådan reglering finns i 4 kap. 1 § lagen (2018:1212) om nationell läkemedelslista.
[26] En sådan reglering finns i 7 kap. 2 § patientdatalagen (2008:355).

direkt av dataskyddsförordningen och behöver därför inte uttryckas i några nationella bestämmelser om sådana ändamål.

2.5 Behov av konsekvensbedömning avseende dataskydd i lagstiftningsarbetet

Mer omfattande ändringar i registerförfattningar kan medföra att lagstiftaren genomför en konsekvensbedömning avseende dataskydd enligt dataskyddsförordningens artikel 35. Om en grundlig konsekvensbedömning har genomförts inom ramen för lagstiftningsprocessen behöver de personuppgiftsansvariga myndigheter som tillämpar den nya eller ändrade registerförfattningen inte genomföra egna konsekvensbedömningar avseende dataskydd, åtminstone inte i den mån tillämpningen följer direkt av den aktuella registerförfattningen, se artikel 35 dataskyddsförordningen. Många gånger behöver myndigheterna emellertid ändå genomföra egna konsekvensbedömningar, särskilt i den mån det finns alternativa tillämpningar eller tolkningar av författningen. Det är möjligt att en vid ändamålsreglering i registerförfattning skulle medföra en större skyldighet för myndigheten att göra konsekvensbedömningar, men i praktiken torde detta inte utgöra något problem.

3. Finalitetsprincipen

eSam förespråkar att registerförfattningar som huvudregel inte ska innehålla någon bestämmelse som reglerar finalitetsprincipen. I stället ska principen i dataskyddsförordningen gälla, om inte lagstiftaren uttryckligen angett att principen inte är tillämplig.

Utlämnande av personuppgifter till andra myndigheter ska inte regleras genom ändamålsbestämmelser.

Testverksamhet behöver som utgångspunkt inte regleras som ett särskilt ändamål.

Vidarebehandling av känsliga personuppgifter behöver inte regleras särskilt.

Eftersom finalitetsprincipen finns reglerad i dataskyddsförordningen, som är direkt tillämplig i svensk rätt, saknas skäl att ange principen i registerförfattning. Utgångspunkten bör vara att finalitetsprincipen alltid kan tillämpas, om inte lagstiftaren uttryckligen i lag angett att den inte är tillämplig i visst fall.

Vad gäller frågan om vidarebehandling av känsliga personuppgifter så krävs ingen särskild reglering om det, eftersom bestämmelsen i artikel 9 i dataskyddsförordningen omfattar all slags behandling. Utgångspunkten bör således vara att det inte finns något ytterligare hinder mot vidarebehandling. Annat gäller om det uttryckligen i lag angetts begränsningar i detta avseende.[27]

3.1 Allmänt om finalitetsprincipen

Kravet att personuppgifter inte får behandlas på ett sätt som är oförenligt med insamlingsändamålen benämns i dataskyddsförordningen som principen om ändamålsbegränsning, men brukar i svensk litteratur kallas för finalitetsprincipen. Principen finns reglerad i dataskyddsförordningen, men också uttryckligen i flera olika registerförfattningar.[28] Syftet med ändamålsbestämmelser i registerförfattningar är normalt att ange en yttersta ram inom vilken uppgifterna får behandlas.[29] Vissa registerförfattningar är uttömmande reglerade, medan andra har en kompletterande finalitetsprincip. Det senare alternativet innebär att finalitetsprincipen utgör den yttersta ramen inom vilken personuppgifter får behandlas.[30]

[27] Jfr t.ex. 14 § utlänningsdatalagen (2016:27).
[28] Se t.ex. 2 kap. 3 § KFMdbL och 1 kap 5 § SdbL
[29] Se t.ex. prop. 1997/98:97 s. 121 och prop. 2000/01:33 s. 99.
[30] Jfr prop. 2019/20:113 s. 9.

3.1.1 Finalitetsprincipen i registerförfattning

Informationshanteringsförfattningar har ofta sina ändamålsbestämmelser uppdelade i primära respektive sekundära ändamål.[31] Med primära ändamål avses då myndighetens egen användning av personuppgifter. Med sekundära ändamål avses främst tillhandahållande av personuppgifter till externa mottagare. Denna uppdelning finns inte angiven i dataskyddsförordningen och bör inte heller finnas i registerförfattningar. I stället bör all behandling för ett visst ändamål omfatta även sådan vidarebehandling som följer insamlingen, så länge behandlingen omfattas av det fastställda insamlingsändamålet. Det saknas anledning att särskilja insamling och utlämnande från andra behandlingar. Exempelvis samlar vissa myndigheter in uppgifter med det primära syftet att tillhandahålla uppgifterna till annan.[32]

Bestämmelsen i art. 5.1 b i dataskyddsförordningen medför bl.a. att det är väsentligt att alla de ändamål för vilka man kan tänkas behöva använda insamlade uppgifter finns angivna redan då uppgifterna samlas in.[33] När primära ändamål finns uttryckligt angivna i en registerförfattning får insamling anses ske för samtliga dessa. Vid en mindre detaljerad ändamålsreglering ställs krav på att myndigheten vid insamling formulerar ändamålen på ett lämpligt sätt. Vid vidarebehandling är det först när man går utanför det vid insamlingen angivna ändamålet som finalitetsprincipen blir aktuell.

Finalitetsprincipen i registerförfattningar kan tillsammans med uppräkningen av tillåtna ändamål i berörda lagar utgöra en sådan ändamålsbegränsning som får införas i nationell rätt enligt artikel 6.3 i dataskyddsförordningen.[34] Bestämmelser som innebär att uppgifter som har samlats in för ett ändamål får eller ska behandlas för ett annat ändamål kan i vissa fall utgöra en tillämpning av finalitetsprincipen, dvs. lagstiftaren har gjort bedömningen att behandlingen är förenlig med insamlingsändamålen. I andra fall kan befintliga lagbestämmelser anses utgöra undantag från finalitetsprincipen.[35]

Om finalitetsprincipen finns reglerad i registerförfattning har lagstiftaren gett den personuppgiftsansvariga myndigheten utrymme att själv bestämma kompletterande ändamål. Detsamma gäller om finalitetsprincipen inte har reglerats i en registerförfattning, då följer principen av dataskyddsförordningen. Om en registerförfattning uttömmande anger i vilka fall uppgifter får lämnas ut har lagstiftaren bedömt att finalitetsprincipen inte kan användas. Detta oavsett om lagstiftaren ansett att principen inte är tillämplig eller om lagstiftaren redan har tillämpat finalitetsprincipen

[31] Se t.ex. lagen (2001:184) om behandling av uppgifter i Kronofogdemyndighetens verksamhet 2 kap. 2 och 3 §§.
[32] Jfr Bolagsverkets s.k. publicitetsregister, t.ex. ändamålsbestämmelsen i 2 kap. 1 § andra stycket aktiebolagsförordningen (2005:559).
[33] Jfr. SOU 2015:39 s. 264.
[34] Se prop. 2017/18:95 s. 56.
[35] Jfr. prop. 2017/18:95 s. 47 f.

och därvid funnit att varje nytt ändamål skulle vara oförenligt med de författningsreglerade ändamålen.[36] Vid en sådan bedömning är det således inte möjligt att med stöd av finalitetsprincipen i dataskyddsförordningen vidarebehandla uppgifterna för ändamål som inte regleras i registerförfattning. En sådan reglering innebär ofta en begränsning för myndigheten.

3.1.2 Tillämpning av finalitetsprincipen

Bestämmelser som reglerar finalitetsprincipen i registerförfattningar är utformade i nära anslutning till artikel 5.1 b i dataskyddsförordningen och bör tolkas på samma sätt.[37] Detta innebär bl.a. att behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1 i EU:s dataskyddsförordning inte ska anses vara oförenlig med insamlingsändamålen. Det innebär också att de omständigheter som anges i artikel 6.4 a–e i dataskyddsförordningen och skäl 50 ska beaktas vid bedömningen av om behandlingen är förenlig med insamlingsändamålen.[38]

I skäl 50 klargörs att det vid tillåten återanvändning av insamlade personuppgifter för andra ändamål inte krävs någon ny rättslig grund enligt artikel 6.1 för behandling av personuppgifterna för de nya ändamålen.

Det är det eller de ändamål som bestämts senast vid insamlingen av personuppgifterna som ska jämföras med det nya ändamålet, inte de icke oförenliga ändamål som redan kan ha bestämts efter insamlingen. Om flera ändamål har bestämts vid insamlingen av personuppgifterna, krävs det att det nya ändamålet inte är oförenligt med något av de ursprungligen bestämda ändamålen. Ju fler olika ursprungliga ändamål man bestämmer vid insamlingen av personuppgifterna, desto färre nya ändamål kan man således i teorin behandla personuppgifterna för. Å andra sidan får vidarebehandling ske för flera nya ändamål som är oförenliga med varandra, så länge inte något av de nya ändamålen är oförenligt med det ursprungliga insamlingsändamålet.[39]

Den personuppgiftsansvarige måste under hela behandlingstiden hålla reda på för vilka ändamål varje personuppgift har samlats in. Innan den personuppgiftsansvarige får behandla personuppgifter för annat ändamål än det för vilket de samlades in måste den personuppgiftsansvarige som huvudregel ge de registrerade information om bl.a. det nya ändamålet.[40] Regeringen har ansett att det ligger i personuppgiftsansvaret att se till att

[36] Se SOU 2015:39 s. 270 ff..
[37] Se prop. 2017/18:254 s. 61.
[38] Jfr. prop. 2019/20:106 s. 93.
[39] Öman, Dataskyddsförordningen (GDPR) m.m. En kommentar, uppl. 2:1, s. 128.
[40] Art. 13.3 och 14.4 i dataskyddsförordningen.

personuppgifter som behandlas för olika ändamål inte blandas.[41] Regleringen gör det extra viktigt att vid insamling av personuppgifter ange alla de ändamål för vilka man kan tänkas behöva använda de insamlade personuppgifterna.[42]

Socialdatautredningen resonerade kring oförenlighetsrekvisitet genom att anföra att man vid en ”oförenlighetsprövning” hypotetiskt bör utgå från hur en registrerad typiskt sett, alltså inte den registrerade i det enskilda fallet, 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 det nya ändamålet inte anses vara oförenligt med det ursprungliga ändamålet.[43]

3.1.3 Särskilt om överföring till andra myndigheter

Informationshanteringsutredningen har uttalat att i vad mån en myndighet får lämna ut personuppgifter till andra myndigheter inte bör regleras genom ändamålsbestämmelser.[44] eSam instämmer i denna bedömning. Vid utlämnande till en annan myndighet bör i stället författningsreglerad uppgiftsskyldighet och sekretesslagstiftning vara avgörande.

En skyldighet att lämna personuppgifter till en annan myndighet kan finnas reglerad i lag. En sådan författningsreglerad uppgiftsskyldighet bryter också förekommande sekretesskydd enligt 10 kap. 28 § offentlighets- och sekretesslagen (2009:400) (OSL). Registerförfattningar innehåller ofta en bestämmelse om att uppgifter får behandlas om det behövs för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning. Registerförfattningar kan också innehålla sekretessbrytande bestämmelser, vilket inte förespråkas av eSam (se avsnitt 6 nedan).

Enligt 6 kap. 5 § OSL ska en myndighet på begäran av en annan myndighet lämna uppgift som den förfogar över, om inte uppgiften är sekretessbelagd eller det skulle hindra arbetets behöriga gång. Skyldigheten anses utgöra en precisering av den allmänna samverkansskyldighet som gäller för myndigheter enligt 8 § förvaltningslagen. Enligt Högsta förvaltningsdomstolens uttalanden i rättsfallet HFD 2021 ref. 10 står ett sådant utlämnande inte heller i strid med finalitetsprincipen.[45]

[41] Se prop. 2008/09:145 s. 336.
[42] Öman, Dataskyddsförordningen (GDPR) m.m. En kommentar, uppl. 2:1, s. 127 f.
[43] SOU 1999:109 s. 160. Jfr också Datainspektionens uttalande i beslut den 15 september 2014, dnr. 1275-2013.
[44] SOU 2015:39 s. 281.
[45] I rättsfallet uttalar Högsta förvaltningsdomstolen att lagstiftaren genom bestämmelser om sekretess får anses ha tagit ställning till när ett uppgiftslämnande är oförenligt med det eller de ändamål för vilka uppgifterna samlades in. Utöver en sekretessprövning ska den personuppgiftsansvariga myndigheten således inte göra någon kontroll av förenligheten med finalitetsprincipen i samband med utlämnande av uppgifter enligt 6 kap. 5 § offentlighets- och sekretesslagen.

3.1.4 Särskilt om testverksamhet

Begreppet behandling[46] omfattar i stort sett all sorts användning av personuppgifter. Det kan t.ex. röra sig om insamling, registrering, förvaring, överföring och radering. Så snart personuppgifter på något sätt hanteras är det fråga om en behandling. Testning är en typ av behandling som, liksom andra behandlingar, kräver rättslig grund och ett ändamål. Testning kan emellertid i vissa fall även anses vara ett eget ändamål. Det senare torde främst bli aktuellt då testning inte sker inom ursprungsverksamheten. Då kan en bedömning enligt finalitetsprincipen behöva göras.

Datainspektionen (numera Integritetsskyddsmyndigheten) har gjort en skillnad på testning för att säkerställa befintliga uppgifter och testning för utveckling av nya system. I beslut den 15 september 2014, dnr 1275-2013, uttalade dåvarande Datainspektionen att det för att säkerställa att de uppgifter som finns i produktion behandlas på ett korrekt sätt och för att upptäcka och korrigera felaktiga personuppgifter i vissa fall kan vara nödvändigt att behandla personuppgifter i testmiljö. En sådan behandling har också ett naturligt samband med det ursprungliga syftet med behandlingen, att tillhandahålla den ifrågavarande tjänsten, och anses i allmänhet inte oförenligt med ändamålen för den ursprungliga behandlingen. I de fall personuppgifter behandlas för tester som görs i samband med utveckling av nya system och införande av nya funktioner i befintliga system menade Datainspektionen att sådana tester har ett svagare samband med den ursprungliga behandlingen av personuppgifterna. Att sambandet är svagare blir tydligt inte minst när behandlingen sker endast till syfte att utveckla systemen för framtida beställningar. Behandling av personuppgifter för sådant ändamål kan därför, enligt Datainspektionens mening, oftare än vad som är fallet med kontroller för att säkerställa korrekta uppgifter eller korrekt behandling vara att anse som oförenligt med det ändamål för vilket uppgifterna samlades in.

eSam menar att testning som behandlingsform som huvudregel inte behöver prövas gentemot finalitetsprincipen. Lagrådet har uttalat att planering, uppföljning och utvärdering av en verksamhet är en integrerad del av själva verksamheten och inte någon från denna fristående aktivitet samt att detta är så självklart att det inte behöver sägas uttryckligen.[47]

Vissa registerförfattningar har testverksamhet angivet som ett särskilt ändamål. I 11 § utlänningsdatalagen (2016:27) har införts en uttrycklig bestämmelse om utförande av testverksamhet. I förarbeten angavs att personuppgiftsbehandling får utföras om den behövs för att testverksamhet ska kunna bedrivas. Det kan t.ex. handla om att

[46] Se artikel 4.2 i dataskyddsförordningen.
[47] Se prop. 2004/05:164 s. 179, jfr. s. 66 f. och 116.

kontrollera att befintliga IT-system fungerar och att göra prov av ny teknik i syfte att kunna delta i det internationella samarbetet. Det anges emellertid att sådan verksamhet många gånger måste anses ha ett sådant samband med verksamheten i övrigt att den inte skulle behöva regleras i en särskild ändamålsbestämmelse, men regleringen motiveras med att det inom ramen för utlännings- och medborgarskapslagstiftningen nyligen införts en särskild ändamålsbestämmelse i förordningen om behandling av personuppgifter i verksamhet enligt utlännings- och medborgarskapslagstiftningen.[48]

I förarbeten till ändring av studiestödsdatalagen (2009:287) gjordes bedömningen att tester som avser utveckling av befintlig eller ny IT-infrastruktur är en administrativ uppgift som CSN behöver utföra för att kunna sköta studiestödsverksamheten och att uppgiften har ett sådant samband med CSN:s studiestödsverksamhet i övrigt att någon särskild ändamålsbestämmelse inte behövs för den verksamheten. Det anges vidare att det är en huvudprincip att testverksamhet inte behöver regleras som ett särskilt ändamål.[49]

Mot bakgrund av senare tids rättsutveckling konstaterar eSam att testverksamhet som utgångpunkt inte behöver regleras som ett särskilt ändamål. Testning är en typ av behandling som ska prövas mot det fastställda insamlingsändamålet. Många gånger faller denna typ av behandling inom det bestämda ändamålet. Då behöver en prövning inte göras enligt finalitetsprincipen. En bedömning av vad som faller inom ett verksamhetsändamål ska göras utifrån formuleringen av ändamålet och, i enlighet med eSams förslag till ändamålsreglering, myndighetens uppdrag. Om den avsedda testningen syftar till att utveckla kärnverksamheten måste en sådan behandling vara tillåten, även om den avser utveckling av nya modeller eller IT-system. Om en behandling i form av testning i undantagsfall skulle avse ett ändamål som faller utanför myndighetens reglering, så måste en bedömning göras utifrån finalitetsprincipen. Om insamling av personuppgifter ska ske enbart för utförande av testning måste ett specifikt ändamål för testverksamhet formuleras. Ett sådant kan vara oförenligt med ändamålsreglering i registerförfattning.

[48] Se prop. 2015/16:65 s. 64. och s. 117.
[49] Se prop. 2019/20:113 s. 18 ff.

4. Registerinnehåll

eSam förespråkar att registerförfattningar som huvudregel inte ska innehålla bestämmelser om vilka personuppgifter som får behandlas.

Om det behövs av särskilda skäl föreslår eSam en reglering av

- att vissa särskilt känsliga personuppgifter inte får behandlas eller ska behandlas på visst sätt, eller
- att registret minst ska innehålla vissa personuppgifter.

Om en uppräkning behövs bör den om möjligt avse kategorier av uppgifter och regleras på en så låg normgivningsnivå som möjligt. Det bör göras en tydlig åtskillnad mellan å ena sidan sådana uppgifter som ingår i själva registret och å andra sidan sådana uppgifter som den registerförande myndigheten får behandla för att kunna utföra sina skyldigheter kopplade till registret.

Bestämmelser om vilka personuppgifter som får behandlas bör aldrig kunna hindra en myndighet från att utföra sina uppdrag eller följa tillämpliga regelverk. Det bör därför sällan komma ifråga att räkna upp vilka personuppgifter som får behandlas i en informationshanteringsförfattning. Dataskyddsförordningens principer om bl.a. ändamålsbegränsning och uppgiftsminimering, i kombination med myndighetens uppdrag enligt författningar och regeringsbeslut, bör sätta ramarna för vilka uppgifter som vid var tid får behandlas. Detsamma borde i stor utsträckning också gälla för renodlade registerförfattningar, så länge ändamålen för registret är tydligt angivet. Det kan dock finnas vissa undantagsfall, se avsnitt 4.2.

4.1 Allmänt om registerinnehåll

4.1.1 Bakgrund

Registerförfattningar innehåller ofta en uppräkning av vilka personuppgifter som får behandlas. Sådana bestämmelser finns både i renodlade registerförfattningar och i informationshanteringsförfattningar. Uppräkningen är i många fall mycket detaljerad och räknar upp vilka specifika uppgifter som får behandlas. Det finns också exempel på registerförfattningar, främst informationshanteringsförfattningar, som inte innehåller någon sådan uppräkning, utan i stället tillåter behandling av alla de personuppgifter som behövs för ändamålen. Att registerförfattningarna ofta räknar upp exakt vilka specifika personuppgifter som får behandlas har sannolikt sin bakgrund i den numera upphävda datalagen (1973:289). För att få föra ett personregister med ADB enligt den dåvarande

lagen krävdes normalt tillstånd från (och senare anmälan till) Datainspektionen. Datainspektionen skulle dessutom meddela föreskrifter om bl.a. *vilka personuppgifter* som fick ingå i registret.[50]

Enligt principen om uppgiftsminimering i artikel 5.1 c i dataskyddsförordningen får inte fler personuppgifter behandlas än vad som är relevant för ändamålen. Förordningen tillåter under vissa omständigheter nationell reglering som kompletterar förordningen (se artikel 6.3), exempelvis får det finnas nationella bestämmelser om vilken *typ* av uppgifter som ska behandlas. Informationen till registrerade, vars uppgifter erhållits av någon annan än individerna själva, ska enligt artikel 14.1 d) innehålla information om de *kategorier* av personuppgifter som behandlingen gäller.

I dataskyddsförordningen hänvisas alltså inte till exakt vilka personuppgifter som behandlingen får avse, utan vilken *typ* eller *kategori* av uppgifter det gäller. Frågan är om dataskyddsförordningen kan sägas förutsätta någon form av indelning eller gruppering av personuppgifter. Dataskyddsförordningen skulle kanske kunna tolkas som att det som får regleras nationellt är olika grupperingar eller klassificeringar av personuppgifter.

4.1.2 Behovet av bestämmelser om registerinnehåll

Med det regelverk och de skyddsåtgärder som numera omgärdar behandling av personuppgifter till följd av dataskyddsförordningen borde behovet av nationell särreglering i form av detaljerade registerförfattningar minska kraftigt. Dataskyddsförordningen ställer krav på att bara uppgifter som är nödvändiga för ändamålen behandlas och att konsekvensbedömningar i många fall ska genomföras. Efterlevnaden säkerställs genom kraftfulla sanktionsmöjligheter. De skäl som tidigare anförts för det svenska systemet med en målsättning att ha särskild detaljreglering i lagform borde därför numera i stor utsträckning vara tillgodosedda genom det generella regelverk som dataskyddsförordningen innebär.

Vid normgivning bör därför noga övervägas om en särreglering överhuvudtaget behövs och i så fall vilken detaljeringsgrad och vilken normgivningsnivå som är nödvändig i just det aktuella sammanhanget, för att skapa ett tillräckligt integritetsskydd. En grundläggande utgångspunkt bör vara att detaljeringsgraden inte ska gå utöver vad som är nödvändigt och att normgivningsnivån bör väljas för att skapa så stor flexibilitet som är möjligt med bibehållet skydd för individers integritet.

Behovet av detaljeringsgrad avseende vilka personuppgifter som ska få behandlas kan variera mycket mellan olika myndigheter och sammanhang. En skillnad i regleringen kan

[50] SOU 2015:39 s.86.

därför vara motiverad, bland annat utifrån hur känsliga uppgifter det är fråga om, vilket syfte ett register har och om det är fråga om ett renodlat register eller en myndighets hela informationshantering. Känsliga personuppgifter och uppgifter som omfattas av sekretess ställer andra skyddskrav än uppgifter som är offentliga. Å andra sidan kan även det faktum att syftet med en uppgiftssamling är att offentliggöra informationen medföra krav på viss återhållsamhet i fråga om vilka personuppgifter som registret får innehålla.

4.1.3 Vilka uppgifter behöver myndigheter behandla?

Det är ofta svårt att på förhand förutse exakt vilka uppgifter som behöver behandlas av en myndighet över tid. Detta gäller i synnerhet informationshanteringsförfattningar, men också renodlade registerförfattningar. En detaljerad reglering av vilka uppgifter som får behandlas kan därför medföra hinder för legitim och berättigad personuppgiftsbehandling som myndigheten behöver utföra för att fullgöra sitt uppdrag och följa de krav som ställs.[51] En sådan reglering kan också innebära ett kontinuerligt behov av ändringar av registerförfattningen, i takt med att nya behov uppkommer. Sådana nya behov kan uppstå bland annat genom nya eller förändrade uppdrag, ändringar i lagstiftning eller praxis eller som en följd av den tekniska utvecklingen och digitaliseringen.

Myndigheter kan inte fullt ut styra vilka personuppgifter som kommer att behandlas. Vem som helst kan skicka in vilken information som helst till en myndighet. Informationen innehåller ofta någon typ av personuppgifter som behöver behandlas av myndigheten för att tillämpliga regler om t.ex. allmänna handlingar och ärendehantering ska kunna följas. Det finns därför ett behov för myndigheten att få behandla alla uppgifter som inkommer, oavsett vad de rör.

Myndigheter kan ha ett behov av att behandla andra uppgifter än de som räknas upp i en bestämmelse om registerinnehåll i en registerförfattning för att uppfylla de krav som uppställs i dataskyddsförordningen och andra regelverk. Personuppgifter ska enligt artikel 5.1 d) i dataskyddsförordningen vara korrekta och om nödvändigt uppdaterade. Myndigheterna kan därför behöva kvalitetssäkra, verifiera och validera de uppräknade uppgifterna med hjälp av andra uppgifter. För att skicka så kallade registerutdrag enligt artikel 15 i dataskyddsförordningen kan individens adress eller andra kontaktuppgifter behöva behandlas, oavsett om sådana uppgifter finns med i bestämmelsen om registerinnehåll eller inte.

Dataskyddsförordningen ställer krav på säkerhet och skydd mot obehörig åtkomst. För att säkerställa detta kan myndigheterna behöva verifiera identitet och i vissa fall

[51] Se t.ex. om Kriminalvårdens registerförfattning, KV 2020-16617.

behörighet för åtkomst till uppgifterna. Som exempel på en brist i det här sammanhanget kan nämnas Patent- och registreringsverkets register och diarier för patent, varumärken och mönsterskydd (design). De aktuella registerförfattningarna anger inte att personnummer eller liknande verifieringsuppgift ska utgöra en del av registret. Ett annat exempel är att sjuksköterskor utan förskrivningsrätt, dietister och farmaceuter i hälso- och sjukvården under vissa förutsättningar får ha direktåtkomst till uppgifter i den nationella läkemedelslistan,[52] men uppgifter om dem finns inte uppräknade i bestämmelsen om registerinnehåll. Uppgifter som behövs för verifiering av identitet och eventuell behörighet kan alltså behöva behandlas av myndigheter även om sådana uppgifter inte ingår i registerförfattningens uppräkning.

4.2 Närmare om förslaget till reglering av registerinnehåll

I vårt komplexa, digitaliserade och globaliserade samhälle är det numera mycket svårt att på ett entydigt sätt på förhand avgöra exakt vilka uppgifter som kommer att behöva behandlas av en myndighet över tid.

Dataskyddsförordningens principer om bl.a. ändamålsbegränsning och uppgiftsminimering, i kombination med myndighetens uppdrag enligt författningar och regeringsbeslut, sätter ramarna för vilka uppgifter som vid var tid får behandlas. Dessa principer och författningar bör sammantaget kunna utgöra en tillräckligt tydlig och begränsande reglering.

Det bör därför i normalfallet vara upp till myndigheten att avgöra vilka uppgifter som ska behandlas, mot bakgrund av ändamålen och myndighetens uppdrag. Huvudregeln bör vara att registerförfattningar, såväl informationshanteringsförfattningar som renodlade registerförfattningar, inte ska innehålla några bestämmelser om registerinnehåll eller annars vilka uppgifter som får behandlas.[53] Principen om uppgiftsminimering i dataskyddsförordningen avgör då vilka uppgifter som får behandlas.

I vissa fall kan det finnas personuppgifter som lagstiftaren bedömer vara extra integritetskänsliga eller skyddsvärda och som befinner sig i gränslandet för vad som kan tänkas behöva behandlas för ändamålet. I dessa fall skulle en omvänd reglering kunna tillämpas, där det i författningen i stället anges att sådana personuppgifter *inte* får behandlas eller ska behandlas på ett visst sätt. I andra fall kan en viss uppräkning av registerinnehållet vara motiverad. Det gäller främst renodlade registerförfattningar. Syftet med ett register i traditionell mening är ofta att vissa uppgifter ska samlas på ett ställe för att därifrån kunna tillhandahållas för andra mottagare eller för att registreringen i sig får

[52] 5 kap. 3 § 2 lagen (2018:1212) om nationell läkemedelslista.
[53] Jfr. Arbetsförmedlingens hemställan En mer träffsäker och enhetlig arbetsmarknadspolitisk bedömning och förbättrad kvalitet i uppföljningen av matchningstjänster, Af-2022/0013 1747, s. 42 ff.

vissa rättsverkningar. Om lagstiftaren behöver säkerställa att en viss uppgift faktiskt finns tillgänglig i ett register, för att det t.ex. får rättsverkan som bevis för ett visst förhållande eller för en viss mottagares behov, skulle en uppräkning kunna göras av de uppgifter som registret *minst* ska innehålla.

I de fall då det bedöms nödvändigt att reglera vilka personuppgifter som får behandlas borde det ofta räcka att olika kategorier av uppgifter anges, i stället för att specifika uppgifter pekas ut. På så sätt preciseras vilken typ av uppgifter det kan vara fråga om, samtidigt som det ger utrymme för en viss flexibilitet. I stället för att räkna upp t.ex. namn och personnummer eller samordningsnummer skulle bestämmelsen kunna avse ”uppgifter som kan identifiera en individ” eller något liknande. En sådan kategorisering skulle skapa nödvändiga förutsättningar för att behandla även sådana utländska identitetsuppgifter som krävs enligt eIDAS-förordningen. Det verkar också stå i bättre överensstämmelse med regleringen om kategorier i dataskyddsförordningen. Sådana preciseringar bör därutöver regleras på en så låg normgivningsnivå som möjligt, t.ex. i en förordning, för att skapa den flexibilitet som är nödvändig över tid.

Om en uppräkning görs i en registerförfattning bör det göras en tydlig åtskillnad mellan å ena sidan sådana uppgifter som ingår i själva registret, t.ex. för att det får viss rättsverkan eller för att ska tillhandahållas andra mottagare, och å andra sidan sådana uppgifter som den registerförande myndigheten därutöver får behandla för att kunna utföra sina skyldigheter kopplade till registret, för att möjliggöra t.ex. verifiering, spårbarhet eller löpande uppdatering av grunddata från andra myndigheter (registervård). Det bör alltså vara tydligt att myndigheten själv får behandla uppgifter för att uppfylla kraven på t.ex. säkerhet, kvalitetssäkring och registervård, även om sådana uppgifter inte ingår i själva registret.

5. Formen för utlämnande av information från myndigheter

eSam förespråkar att registerförfattningars reglering kring utlämnanden är teknikneutrala utan att uppställa något särskilt krav på formen för utlämnande.

Direktåtkomst ska endast regleras i författning om sådan åtkomst behöver begränsas. I annat fall ska det vara upp till myndigheten att avgöra formen för utlämnande.

Dataskyddsförordningen reglerar inte uttryckligen på vilket sätt uppgifter får lämnas ut och det saknas ofta skäl att begränsa frågan i registerförfattning. Utgångspunkten bör vara att myndigheten själv ska kunna bedöma på vilket sätt ett utlämnande kan ske. Vid bedömningen måste överväganden kring effektivitet, säkerhet och tillförlitlighet göras. Det är inte befogat ur ett dataskyddsperspektiv att generellt undanta möjligheten till elektroniska utlämnanden.[54]

Med stöd av reglerna i dataskyddsförordningen och med utgångspunkt i den ansvarsprincip som gäller kan en myndighet utveckla tekniker för informationsutbyte som är säkra och ändamålsenliga utan att informationsutbytet är reglerat i alla detaljer. Om det i ett enskilt fall finns anledning att begränsa användning av direktåtkomst kan lagstiftaren reglera detta i registerförfattning. Utgångspunkten bör emellertid vara ett en sådan reglering inte behövs. Om direktåtkomst inte regleras särskilt är det upp till myndigheten att avgöra formen för utlämnande, med beaktande av dataskyddsförordningens krav på säkerhet.

5.1 Allmänt om utlämnande

Utlämnande av information från en myndighet måste med hänsyn till legalitetsprincipen[55] ha stöd i rättsordningen. Det finns ett flertal författningar som ger förutsättningar för utlämnande av information från myndigheter och dessa avser såväl utlämnande till enskilda som till andra myndigheter.[56] Myndigheter kan också ha uppdrag

[54] Jfr. Kronofogdens hemställan Bättre och snabbare service i Kronofogdemyndighetens verksamhet, KFM 22992-2020.
[55] Se 1 kap. 1 § tredje stycket regeringsformen och 5 § förvaltningslagen.
[56] Se t.ex. 2 kap. 16 § TF och 6 kap. 5 § OSL.

i rättsordningen att tillgängliggöra information på eget initiativ. Det är då inte frågan om frivilliga utlämnanden, utan aktiviteter som följer av myndighetens uppdrag.[57]

En fråga om utlämnande kan delas upp i två delar. Den första delen avser frågan om informationen kan lämnas ut. Här är främst regler i tryckfrihetsförordningen samt offentlighets- och sekretesslagen relevanta. Denna promemoria syftar till att analysera den andra delen av frågan, dvs. på vilket sätt informationen kan lämnas ut.

5.2 Reglering gällande form för utlämnande

Det finns inte någon generell reglering som anger hur myndigheter ska lämna ut information. Mellan myndigheter finns allmänna regler som påverkar informationsutbytet. I till exempel 8 § förvaltningslagen (2017:900) anges att myndigheter ska hjälpa varandra inom ramen för den egna verksamheten. I 6 § myndighetsförordningen (2007:515) anges att myndigheter ska verka för att genom samarbete med andra myndigheter ta till vara de fördelar som kan vinnas för enskilda samt för staten som helhet. Varken i dessa allmänna samverkansbestämmelser eller i någon annan generellt gällande reglering finns det bestämmelser som anger hur information kan eller får tillhandahållas mellan myndigheter. Möjligen kan man uppfatta bestämmelserna så att myndigheterna ska välja handlingsmönster och metoder som är effektiva och ändamålsenliga i det enskilda fallet.[58]

När det gäller sättet för utlämnande av handlingar från myndigheter till enskilda är främst regleringen i tryckfrihetsförordningen av betydelse, liksom särskilda bestämmelser i registerförfattningar.[59] Även förordningen (2003:234) om tiden för tillhandahållande av domar och beslut, m.m. innehåller regler att beakta. I 2 kap. 15-16 §§ tryckfrihetsförordningen (TF) regleras möjligheten för enskild att ta del av en allmän handling hos den förvarande myndigheten, eller genom att ta del av en avskrift eller kopia av handlingen. I 2 kap. 16 § finns det s.k. utskriftsundantaget som innebär att en myndighet inte i större utsträckning än vad som följer av lag är skyldig att lämna ut en upptagning för automatiserad behandling i annan form än utskrift. Syftet med utskriftsundantaget är att förhindra att utlämnade uppgifter behandlas automatiserat på ett sätt som kan medföra otillbörligt intrång i enskildas personliga integritet.[60] Bestämmelsen innebär dock inte i sig något förbud mot utlämnande av handlingar i elektronisk form.[61] Ett digitalt utlämnande av en allmän handling sker inte med stöd av

[57] Se t.ex. lag (2000:224) om fastighetsregister och förordning (2016:822) med instruktion för Statistiska centralbyrån.
[58] Jfr. prop. 2016/17:180 s. 70 En modern och rättssäker förvaltning – ny förvaltningslag.
[59] Det finns också ett förslag om en ny lag om den offentliga sektorns tillgängliggörande av data. Den föreslagna lagen bedöms vara förenlig med de förslag som framställs i denna promemoria.
[60] Prop. 1972:33 s. 85.
[61] A.a. s. 85 f.

offentlighetsprincipen, utan är ett utslag av myndighetens serviceskyldighet.[62] Tryckfrihetsförordningen och offentlighetsprincipen innebär inte att sättet för tillhandahållande av information författningsmässigt är styrt till analogt eller digitalt sätt. Enligt dessa regler är det i stället myndigheten som avgör sättet för tillhandahållandet.

Många registerförfattningar innehåller bestämmelser som reglerar sättet för utlämnande av personuppgifter. Ofta handlar det om begränsningar av möjligheter till elektroniska utlämnanden.[63] I dataskyddsförordningen finns emellertid inte någon särskild bestämmelse som förbjuder eller påbjuder visst sätt för tillhandahållande av information. Emellertid kan kraven på säkerhet enligt artiklarna 5.1 f och 32 kräva särskilda överväganden och åtgärder vid ett utlämnande.

5.3 Formerna för elektroniskt utlämnande

När en myndighet ska lämna ut information elektroniskt kan det ske på flera olika sätt. Rättsligt är tillhandahållandet reglerat antingen genom att en myndighet upplåter direktåtkomst till en informationsmängd eller så sker utlämnandet på medium för automatiserad behandling.

5.3.1 Utlämnande på medium för automatiserad behandling

Med begreppet utlämnande på medium för automatiserad behandling avses andra elektroniska utlämnanden än de som sker genom direktåtkomst.[64] Många av de registerförfattningar som tillkom efter personuppgiftslagens införande innehåller regler för sådana utlämnanden.

Utlämnandet liknar i huvudsak ett traditionellt utlämnande av konventionella handlingar eller uppgifter i handlingar. Exemplen har varierat beroende på informationsteknikens utveckling. I äldre förarbeten[65] talas det om att begreppet avser ett utlämnande på magnetband, skivminnen eller en handling med visuellt läsbar text, om texten var maskinläsbar och avsikten var att avläsning skulle ske maskinellt. I senare motivuttalanden[66] anförs att utlämnande på medium för automatiserad behandling kan ske genom filöverföring, på diskett eller på annat sätt med hjälp av automatisk databehandling. Med dagens teknik kan utlämnande av information ske exempelvis genom direkt överföring från ett datorsystem till ett annat via ett elektroniskt kommunikationsnät, på ett USB-minne, genom e-post eller att uppgifter lämnas och

[62] A.a. s. 86.
[63] Se t.ex. 2 kap. 6 § lag (2001:181) om behandling av uppgifter i Skatteverkets beskattningsverksamhet och 2 kap. 25 § lag (2001:184) om behandling av uppgifter i Kronofogdemyndighetens verksamhet.
[64] SOU 2015:39 s. 443.
[65] Prop. 1979/80:146 s. 48.
[66] Prop. 1995/96:201 s. 31.

hämtas via inloggning till en e-tjänst. Tekniska lösningar som API:er[67] och SHS[68] är vanliga. Till skillnad från vid direktåtkomst så ska myndigheten reagera på och kontrollera varje sökfråga som görs i tjänsten. Denna kontroll, som vid behov ska innefatta en sekretessprövning, kan emellertid vara automatiserad.

5.3.1.1 Ändring av begrepp

I nyare registerlagar används inte längre begreppet medium för automatiserad behandling.[69] I Polismyndighetens, Tullverkets, Kustbevakningens och Skatteverkets registerlagstiftning inom det brottsbekämpande området används i stället begreppet *lämnas ut elektroniskt på annat sätt än genom direktåtkomst.*[70] Samma definition används i domstolsdatalagen (2015:728) och i lagen (2020:421) om Rättsmedicinalverkets behandling av personuppgifter. Med elektroniskt utlämnande avses således både direktåtkomst som annat utlämnande i elektronisk form.[71] Det är dessutom modernare och enklare att förstå. Eftersom eSam förespråkar en teknikneutral reglering är begreppet elektroniskt utlämnande lämpligt att använda i registerförfattningar, i den mån format alls behöver regleras.

5.3.2 Direktåtkomst

En form av elektroniskt utlämnande som ofta särregleras är direktåtkomst. I tidigare registerförfattningar användes begreppet terminalåtkomst. Genom terminalåtkomsten gavs andra myndigheter en behörighetsstyrd direkt åtkomst till hela eller delar av den upplåtande myndighetens informationssamling. En uppkopplad myndighet kunde genom terminalåtkomsten i rätt tid få tillgång till information utan tidsödande administration genom att begära ut handlingar eller uppgifter via telefon eller brevledes. Begreppet har sedermera ersatts av det mer moderna begreppet direktåtkomst.

Det finns ingen legaldefinition av begreppet direktåtkomst. Med direktåtkomst avses vanligtvis att någon har direkt tillgång till någon annans informationssamling och på egen hand kan söka efter information, utan att kunna påverka innehållet i informationssamlingen. I begreppet ligger också att den som är personuppgiftsansvarig för informationssamlingen inte har någon kontroll över vilka uppgifter som mottagaren vid ett visst söktillfälle tar del av. Den myndighet som lämnar ut uppgifter genom direktåtkomst fattar således inte något beslut om utlämnande av de uppgifter som den

[67] API är förkortningen för Application Program Interface och kan kort beskrivas som ett strukturerat sätt att överföra data från ett system till ett annat. Informationsutbytet via API:er (eller bastjänster) beskrivs närmare i eSams vägledning för verksamhetsutveckling inom e-förvaltning 3.0. Se även prop. 2019/20:83 s. 27-29.
[68] Spridnings- och hämtningssystemet (SHS) är en metod för ett säkert utbyte av information. Informationsutbytet är standardiserat, vilket innebär att samma teknik används vare sig mottagaren är ett internt verksamhetssystem eller en annan myndighet. SHS utgör idag grundbulten i många myndigheters kommunikationssystem. SHS beskrivs närmare i SOES fördjupande analys Spridnings- och hämtningssystemet (SHS), 2014-10-23.
[69] En sådan bestämmelse saknas helt i lagen (2018:1212) om nationell läkemedelslista.
[70] Se t.ex. 2 kap. 9 § lagen (2018:1694) om tullverkets behandling av personuppgifter inom brottsdatalagens område.
[71] Prop. 2019/20:106 s. 54.

som har direktåtkomst tar del av i varje enskilt fall. I stället måste en förhandsprövning göras beträffande förutsättningarna för utlämnande. En sådan prövning innefattar alla de uppgifter som mottagaren har möjlighet att ta del av genom direktåtkomsten. Vid prövningen ska givetvis säkerställas att sekretess inte hindrar ett utlämnande. Är uppgifterna som omfattas av direktåtkomsten sekretessbelagda krävs det att en tillämplig sekretessbrytande regel kan tillämpas redan vid förhandsprövningen. Direktåtkomst kan ges till både en enskild och till annan myndighet. Vid direktåtkomst mellan myndigheter finns det i 11 kap. 4 § offentlighets- och sekretesslagen en bestämmelse om överförd sekretess.

Genom att en direktåtkomst etableras mellan två myndigheter blir den informationssamling som direktåtkomsten omfattar allmän handling också hos den myndighet som utnyttjar direktåtkomsten. Av regleringen i 2 kap. 9 § TF följer att en upptagning anses inkommen till en myndighet när någon annan har gjord den tillgänglig för myndigheten så att den kan läsas, avlyssnas eller uppfattas på annat sätt med tekniskt hjälpmedel som myndigheten själv utnyttjar. Kvalificeringen som allmän handling gäller all den information som direktåtkomsten omfattar oavsett om den myndighet som utnyttjar direktåtkomsten faktiskt tar del av informationen eller ens har rättliga förutsättningar i det enskilda fallet att ta del av informationen. Det är i detta sammanhang som problemställningen runt överskottsinformation[72] i samband med direktåtkomst uppstår.

Den faktiska begränsningen av direktåtkomsten görs med hjälp av olika tekniska lösningar, beroende på hur omfattningen av direktåtkomsten har begränsats i det enskilda fallet, exempelvis genom olika behörighetsnivåer. Det är den personuppgiftsansvariga myndigheten som ska se till att åtkomst begränsas på det sätt som föreskrivs.

Den tekniska utvecklingen har orsakat tillämpningsproblem i gränsdragningen mellan utlämnande via direktåtkomst och utlämnande på medium för automatiserad behandling. Utvecklingen inom it-området har inneburit att utlämnande på medium för automatiserad behandling kan vara ett elektroniskt informationsutbyte i realtid mellan myndigheter. Det effektivitetsmått som tidigare särskilde direktåtkomst är numera lika relevant för annat elektroniskt utlämnande. Den tekniska utvecklingen har dock inneburit bitvis svårbedömda frågor kring vilken prövning som äger rum vid utlämnande, vem som ska anses utföra prövningen, vilka beslut som fattas i olika led av

[72] I SOU 2012:90 s. 12 definieras överskottsinformation som externt tillgänglig information som mottagande myndighet vid direktåtkomst eller liknande elektronisk tillgång till en annan myndighets elektroniska informationssamling tekniskt sett har tillgång till men som mottagarmyndigheten inte får använda i ett enskilt fall eller ta del av utan att t.ex. vissa förutsättningar är uppfyllda. Med överskottsinformation kan också menas information som mottagarmyndigheten visserligen får men ännu inte har använt i sin verksamhet.

hanteringen av utlämnande och under vilka förutsättningar ett s.k. överskott av allmänna handlingar uppkommer hos myndigheter. Genom rättsfallet HFD 2015 ref. 61 (LEFI Online) har viss klarhet skapats kring vilka kriterier som utmärker direktåtkomst respektive utlämnande på medium för automatiserad behandling, se avsnitt 5.3.3 nedan.

Elektroniska register och en myndighets åtkomst till en annan myndighets informationssamling ansågs redan på 1970-talet som känsligt. En viktig aspekt av direktåtkomsten och som gör att just den formen av utlämnande anses integritetskritisk är att prövningen av utlämnandet sker i förväg. Prövningen omfattar dessutom typer eller kategorier av uppgifter avseende en definierad population. Det innebär att utlämnandet, som sker när den mottagande myndigheten får tillgång till informationssamlingen, avser en större mängd information.

Eftersom direktåtkomst har ansetts innebära att den utlämnande myndigheten i det enskilda fallet inte har kontroll över vilka uppgifter som lämnas ut har det från persondataskyddssynpunkt ansetts vara av stor betydelse att särskilt reglera frågor om direktåtkomst i registerlagstiftningen.[73]

Genom direktåtkomst skapas allmänna handlingar av de uppgifter som den mottagande myndigheten får tillgång till och överskottsinformation uppstår, vilken ökar risken för intrång i den registrerades integritet och annan spridning av känsliga uppgifter. Problematiken med överskottsinformation har berörts bl.a. i betänkandet Överskottsinformation vid direktåtkomst (SOU 2012:90) s 39 ff.

Reglering av direktåtkomst

Det finns inte något direkt krav på att ett utlämnande genom direktåtkomst ska ha stöd i författning för att vara tillåten. I förarbeten till bestämmelser om direktåtkomst framgår emellertid att det ofta finns ett antagande om att direktåtkomst uttryckligen måste tillåtas genom en föreskrift i författning. eSam är av uppfattningen att så inte är fallet.

Utlämnande i form av direktåtkomst regleras i huvudsak på tre olika sätt. Ett sätt är att i författning beskriva några fall då direktåtkomst får medges. Ett exempel på detta förfaringssätt är den direktåtkomst som får medges till Skatteverkets beskattningsdatabas. I 2 kap. 7–8 d §§ lagen (2001:181) om behandling av uppgifter i Skatteverkets beskattningsverksamhet regleras vilka myndigheter, eller självständiga verksamhetsgrenar inom Skatteverket, som får ha direktåtkomst till beskattningsdatabasen. Förutom att föreskriva vilka myndigheter som får ha direktåtkomst, anges också vilka uppgifter som direktåtkomsten får omfatta. Det anges

[73] SOU 2010:4 s. 365.

också i vissa av bestämmelserna att regeringen meddelar närmare föreskrifter om vilka uppgifter och handlingar direktåtkomsten får omfatta.[74]

Ett annat sätt är att uttömmande reglera i vilka fall direktåtkomst får medges. Denna lagstiftningsteknik har använts exempelvis i fråga om socialförsäkringsdatabasen som innehåller personuppgifter i Försäkringskassans och Pensionsmyndighetens verksamhet. I 114 kap. 18–22 §§ SFB finns bestämmelser om direktåtkomst till socialförsäkringsdatabasen. Enligt 18 § är direktåtkomst till socialförsäkringsdatabasen endast tillåten i den utsträckning som anges i lag eller förordning. I 19–22 §§ finns därefter bestämmelser om vissa myndigheter eller organ med myndighetsuppgifter som, förutom Försäkringskassan och Pensionsmyndigheten, får ha sådan direktåtkomst och att det gäller i den utsträckning det behövs för särskilt nämnda ärendeslag eller ändamål.[75]

Direktåtkomst kan också regleras på det sättet att författningen ger uttryck för när direktåtkomst inte får förekomma, dvs. i form av förbud mot direktåtkomst. Så är fallet med direktåtkomst till personuppgifter inom socialtjänsten. Enligt 11 § lagen (2001:454) om behandling av personuppgifter inom socialtjänsten bemyndigas regeringen att meddela föreskrifter om bl.a. direktåtkomst. I 24 § förordningen (2001:637) om behandling av personuppgifter inom socialtjänsten föreskrivs att Socialstyrelsen får i verksamhet som avses i lagen (2007:606) om utredningar avseende vissa dödsfall inte medge andra myndigheter eller enskilda direktåtkomst till personuppgifter.[76]

I många registerförfattningar finns även regler om direktåtkomst för enskilda, såväl fysiska som juridiska personer. Vilka som får ha direktåtkomst till uppgifter i ett visst register varierar beroende på syftet med registret. Registerförfattningar innehåller ofta en bestämmelse om att den registrerade får ha direktåtkomst till uppgifter om sig själv.[77]

I många författningar preciseras på olika sätt vilken typ av mottagare som får ha direktåtkomst. Det kan t.ex. anges att sökande eller parter och deras ombud eller biträden får ha direktåtkomst till vissa uppgifter.[78] Det gäller oavsett om det är fråga om fysiska eller juridiska personer. Det finns bestämmelser i registerförfattningar som tillåter direktåtkomst för mer avgränsade kategorier av mottagare, t.ex. vårdgivare (oavsett om de är offentliga eller privata), arbetslöshetskassorna, djurägare och djurhållare, arbetsgivare och registrerade pantbrevshavare.[79] I några fall är det i stället vissa

[74] SOU 2015:39 s. 122 f.
[75] SOU 2015:39 s. 123.
[76] SOU 2015:39 s. 124.
[77] I vissa fall även ombud, se 5 kap. 6 § lagen (2018:1212) om nationell läkemedelslista.
[78] Se t.ex. 2 kap. 28 § lagen (2001:184) om behandling av uppgifter i Kronofogdemyndighetens verksamhet och 9-10 §§ förordningen (2001:590), 17 § domstolsdatalagen (2015:728) och 19 § utlänningsdatalagen (2016:27).
[79] Se t.ex. 6 kap. 1 § patientdatalagen (2008:355), 11 § studiestödsdatalagen (2009:287), 12 § lagen (2002:546) om behandling av personuppgifter i den arbetsmarknadspolitiska verksamheten, 114 kap. 21 § socialförsäkringsbalken (2010:110), 12 § lagen 2002:546 om behandling av

yrkesgrupper som får ha direktåtkomst, t.ex. expedierande personal på apotek och viss hälso- och sjukvårdspersonal (oavsett om de arbetar i offentlig eller privat vård).[80]

I andra registerförfattningar, som har som ändamål att ge offentlighet åt den information som ingår i registret, är det i stället en väldigt bred mottagarkrets som får ha direktåtkomst, t.ex. sådan ”allmän eller enskild verksamhet” där informationen i registret utgör underlag för prövningar eller beslut.[81] Ibland avgränsas sådan direktåtkomst genom att det anges att den bara får medges i den utsträckning det är förenligt med regleringen om tredjelandsöverföring i dataskyddsförordningen.[82]

5.3.3 Skillnaden mellan direktåtkomst och annat elektroniskt utlämnande

Gränsdragningen mellan utlämnande via direktåtkomst och annat elektroniskt utlämnande har orsakat tillämpningsproblem, särskilt under senare år när den tekniska utvecklingen gjort skillnaden mindre. Högsta förvaltningsdomstolen har i rättsfallet HFD 2015 ref. 61 (LEFI Online) redogjort för hur skiljelinjen ska dras.

Utifrån Högsta förvaltningsdomstolens bedömning kan två generella slutsatser identifieras. För det första ska begreppet direktåtkomst bestämmas med utgångspunkt i bestämmelserna i 2 kap. 6 § första stycket TF. För det andra ska sådan teknisk tillgång som avses i TF inte föreligga om ett utlämnande förutsätter att den utlämnande myndigheten reagerar på en begäran om att de efterfrågade uppgifterna ska lämnas ut.

Av 2 kap. 4 § TF framgår det att en handling är allmän, om den förvaras hos en myndighet och enligt 9 eller 10 § är att anse som inkommen till eller upprättad hos en myndighet. Vidare stadgas det i 2 kap. 6 § första stycket TF att en upptagning som avses i 3 § anses förvarad hos en myndighet, om upptagningen är tillgänglig för myndigheten med tekniskt hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att den kan läsas eller avlyssnas eller uppfattas på annat sätt. Till följd av Högsta förvaltningsdomstolens tolkning av 2 kap. 6 § första stycket TF är bedömningen av vad som anses förvarat (hos myndighet) inte bara samordnad med vad som anses inkommit (till myndighet), utan samma bedömning blir också avgörande för om direktåtkomst eller annat elektroniskt utlämnande ska anses föreligga. Med andra ord föreligger

personuppgifter i den arbetsmarknadspolitiska verksamheten, 8 § förordningen 2021:1129 om register över förordnade läkemedel för behandling av djur och 19 § lagen (1994:448) om pantbrevsregister.

[80] Se t.ex. 5 kap. lagen (2018:1212) om nationell läkemedelslista, 16 § lagen (2016:526) om behandling av personuppgifter i ärenden om licens för läkemedel och 8 § förordningen 2021:1129 om register över förordnade läkemedel för behandling av djur.

[81] Se t.ex. aktiebolagsförordningen (2005:559), handelsregisterförordningen (1974:188) och 7 § lagen (2000:224) om fastighetsregister.

[82] Se t.ex. 16 § förordningen (2014:936) om näringsförbud och 13 § förordningen (1985:357) om registrering av och underrättelse om domar om förbud mot juridiskt eller ekonomiskt biträde i vissa fall.

direktåtkomst om handlingen är att anse som förvarad enligt TF hos den mottagande myndigheten och tvärtom.[83]

Efter domen har eSam publicerat vägledningen Elektroniskt informationsutbyte - en vägledning för utlämnande i elektronisk form. Vägledningen innehåller bl.a. juridiska överväganden samt en redogörelse för en konkret modell för informationsutbyte. Enligt eSam är det avgörande för bedömningen om den utlämnande myndigheten måste reagera på begäran eller inte.

Om informationsöverföringssystemet är konstruerat så att utlämnande myndighet automatiserat måste reagera på en begäran om att få ut en handling, har den mottagande myndigheten inte någon sådan tillgång till handlingen som avses i 2 kap. 6 § första stycket TF. Handlingen är inte tillgänglig förrän prövningen gjorts och handlingen har lämnats ut. Därmed uppkommer inte något överskott av allmänna handlingar hos den mottagande myndigheten. Om en handling inte är tillgänglig enligt 2 kap. 6 § första stycket TF har den mottagande myndigheten inte heller direktåtkomst till den.

En myndighet reagerar på en begäran om att få ut uppgifter genom att automatiserat kontrollera vilka uppgifter som begärs ut och i varje enskilt fall pröva att begäran är förenlig med de rättsregler som gäller för att få uppgifterna utlämnade. En sådan prövning i en tjänst för fråga-svar sker genom tekniska kontroller av att alla i tjänsten inbyggda regler är uppfyllda i det enskilda fallet för att svar ska lämnas med begärda uppgifter.

En grundförutsättning är att verktyget för att lämna ut uppgifterna, i vilket också kontrollfunktionerna för den automatiserade prövningen finns inbyggda, är under den utlämnande myndighetens juridiska och faktiska kontroll. Styrningen och funktionerna för att automatiserat fatta beslut ska således vara inbyggda i den utlämnande myndighetens system. Mottagande myndighet får inte ha några sådana tekniska hjälpmedel som möjliggör för mottagaren att söka fram och ta del av uppgifter som inte först har genomgått den utlämnande myndighetens automatiserade prövning.[84]

Datainspektionen (numera IMY) har påpekat att Högsta förvaltningsdomstolen i det aktuella rättsfallet endast har tagit ställning till frågan om direktåtkomst utifrån de speciella förutsättningar som förelåg i det aktuella målet.[85] Det bör dock enligt eSams mening kunna förutsättas att den bedömning som gjordes av domstolen kommer att gälla även i andra fall där en myndighet får direktåtkomst till uppgifter hos en annan

[83] Jfr HFD 2020 not 16, punkten 12.
[84] Kirei 2021:02.
[85] Datainspektionens yttrande 2017-03-17 i dnr 253-2017. Se även Sören Ömans expertkommentar för Blendow Lexnova,december 2015.

myndighet, i vart fall om inte särskilda uttalanden i förarbetena i det enskilda fallet föranleder någon annan tolkning.

Både Högsta förvaltningsdomstolens dom i LEFI Online-målet och eSams vägledning avser förhållandet att såväl utlämnande som mottagande part är svenska myndigheter. Högsta förvaltningsdomstolen knyter frågan om direktåtkomst till tryckfrihetsförordningens begrepp förvarad allmän handling. Några förvarade allmänna handlingar i tryckfrihetsförordningens mening finns normalt inte hos enskilda. Frågan är därför vilken betydelse domstolens tolkning får om mottagaren inte är en svensk myndighet, utan en enskild för vilken tryckfrihetsförordningens bestämmelser om förvarad allmän handling inte gäller. Det är därför mer osäkert vilka slutsatser som kan dras utifrån domen vad gäller direktåtkomst till enskilda. Det kan inte heller uteslutas att det har haft betydelse för utgången i målet att mottagarna var svenska myndigheter, eftersom detta kan sägas innebära en slags inneboende säkerhet, såväl strukturellt som av sekretesskäl. Frågan blir då vilken betydelse mottagarens organisationsform har när det gäller tolkningen av begreppet direktåtkomst.

Regeringen uttalade i förarbetena till lagen (2018:1212) om nationell läkemedelslista att Högsta förvaltningsdomstolens dom kan tolkas så att den tekniska utformningen av en myndighets system för utlämnande av uppgifter kan bli avgörande för om utlämnandet ska anses som direktåtkomst eller som annat utlämnande på medium för automatiserad behandling.[86] Betydelsen av mottagarens organisationsform och därmed tillämpligheten av bestämmelserna i tryckfrihetsförordningen diskuterades inte. Även utredningen om e-recept inom EES uttalar i sitt delbetänkande att begreppet direktåtkomst bör tolkas utifrån den tekniska lösningen.[87]

Enligt eSams mening är det rimligt att begreppet direktåtkomst tolkas på samma sätt, oavsett om mottagaren är en svensk myndighet eller inte. Att samma tekniska lösning skulle tolkas på olika sätt beroende på mottagarens organisationsform vore både orimligt och rättsosäkert. En sådan ordning skulle dessutom bli mycket svår att tillämpa. I vissa fall får direktåtkomst medges till kategorier av mottagare som kan vara både privata och offentliga, t.ex. vårdgivare och arbetsgivare. Det vore mycket märkligt om en och samma tekniska lösning som tillämpas för båda dessa typer av mottagare skulle få olika juridiska konsekvenser.

Det innebär alltså att en lösning som tekniskt utformas på ett sådant sätt att utlämnande myndighet inte måste reagera på en begäran om att få ut en handling och att uppgifterna därför hade ansetts vara förvarade hos mottagaren om den var en svensk myndighet

[86] Prop. 2017/18:223 s. 143.
[87] SOU 2021:102 s 202.

också bör betraktas som direktåtkomst om mottagaren har en annan organisationsform eller är en fysisk person.

5.4 Formen för utlämnande ska som huvudregel inte regleras

5.4.1 Teknikneutralitet som huvudregel

I princip all personuppgiftsbehandling på myndigheter sker i dag digitalt och det är inte motiverat med ett analogt utlämnandesätt som norm.[88] Det finns inte skäl att påstå att ett analogt utlämnande skulle vara säkrare ur ett dataskyddsperspektiv. Med modern teknik är det enkelt för mottagaren att omvandla text på papper till ett digitalt format. Dessutom kan det i dagens samhälle inte anses säkrare att per post skicka analoga underrättelser än att skicka handlingen genom digitala kanaler. Ett elektroniskt utlämnande av uppgifter kan idag ske säkert med hjälp av tekniker såsom filöverföring och API mellan tekniska system. Autentiserings- och auktorisationsprocesser säkerställer att utlämnandet sker till en behörig part. Kryptering och andra säkerhetsmekanismer säkerställer att överföringen av uppgifter sker på ett betryggande sätt. Det finns idag en mängd olika valmöjligheter för säkert digitalt tillhandahållande av information. E-post är i det sammanhanget sällan ett förstahandsalternativ.

eSam menar att regleringen som huvudregel bör vara teknikneutral. Myndigheten har då att, i varje enskilt fall, bedöma på vilket sätt informationen ska tillhandahållas och hur tillhandahållandet ska utformas. Genom en bra design[89] kan integritetsrisker i tillhandahållandet minskas eller i bästa fall elimineras. Designen kan avse att tillgodose säkerhetsmässiga krav, övervakning av användning av en informationstjänst och begränsning av överskottsinformation. Dataskyddsförordningens krav på bl.a. uppgiftsminimering och säkerhet är givetvis viktiga mål vid utformning av tillhandahållandet. Det bör som utgångspunkt inte heller lagtekniskt göras någon skillnad mellan direktåtkomst eller annat elektroniskt utlämnande. Om det i enskilt fall finns anledning att begränsa användning av direktåtkomst kan lagstiftaren reglera detta i registerförfattning.

[88] Det finns bestämmelser om elektroniskt informationsutbyte som en huvudregel bl.a. i EU-förordningen (2018/1724) om en gemensam digital ingång för tillhandahållande av information, förfaranden samt hjälp- och problemlösningstjänster och Europaparlamentets och rådets förordning (EU) nr 952/2013 av den 9 oktober 2013 om fastställande av en tullkodex för unionen.
[89] Med syfte att uppnå inbyggt dataskydd enligt artikel 25 i dataskyddsförordningen.

5.4.2 Ansvarsprincipen

Enligt principen om ansvarsskyldighet i artikel 5.2 i dataskyddsförordningen ska den personuppgiftsansvarige myndigheten ansvara för och kunna visa att den följer förordningens principer för behandling av personuppgifter.

Med utgångspunkt i denna princip kan en myndighet eller myndigheter i samverkan utveckla tekniker för informationsutbyte som är säkra och ändamålsenliga utan att formen för informationsutbytet är lagreglerad. Då skulle också inlåsningseffekter till följd av teknikutveckling minskas. En lösare författningsreglering innebär ett större ansvar för myndigheten som vid utlämnanden måste göra en prövning av format. Många gånger kommer myndigheten emellertid kunna upprätthålla ett fullgott dataskydd genom säkerhetsåtgärder, såsom vid val av teknisk lösning.

5.4.3 Val av utlämnandeform

Enligt artikel 32 i dataskyddsförordningen ska myndigheten vid behandling av personuppgifter vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till de risker som behandlingen medför. Artikel 25 reglerar krav om inbyggt dataskydd och dataskydd som standard. Av skäl 31 i dataskyddsförordningen framgår att varje begäran från en myndighet ska vara skriftlig, motiverad, läggas fram i det enskilda fallet och inte gälla ett helt register eller leda till att register kopplas samman.

Såväl direktåtkomst som utlämnande på medium för automatiserad behandling ställer krav på autentisering och auktorisering. Båda formerna av utlämnande kräver att överenskommelser mellan myndigheter görs och även ofta att loggning av trafik sker hos den utlämnande myndigheten. Om tillgängliggörandet sker till enskild krävs att myndigheten fattar beslut om att tillgängliggörande får ske mot bakgrund av den enskildes begäran. Oavsett form behöver således samtliga av dessa krav vara uppfyllda. Redan vid konstruktion eller val av programvara ska myndigheten beakta dataskyddsregleringen och utforma systemen så att dataskyddsprinciperna följs.[90]

Vid direktåtkomst finns det efter medgivande ingen möjlighet för den utlämnande myndigheten att stoppa utlämnandet för varje söktillfälle. Det föreligger därmed en ökad risk för integritetsintrång och spridning av andra känsliga uppgifter. Av Informationshanteringsutredningens slutbetänkande[91] framgår att det är ett starkt rättssäkerhetskrav att gränserna mellan myndigheterna i rättslig mening kan upprätthållas. eSam har i sin vägledning Elektroniskt informationsutbyte - en vägledning

[90] Jfr. Skatteverkets remissvar vad gäller De brottsbekämpande myndigheternas direktåtkomst till beskattningsdatabasen, Ju2020/00320/L4.
[91] Myndighetsdatalag (SOU 2015:39).

för utlämnande i elektronisk form förordat att utlämnande av uppgifter inte bör ske genom direktåtkomst. Eftersom den tekniska utvecklingen har lett till att samma effektivitetsvinster kan uppnås med en fråga-svar-funktion, så väljer myndigheter ofta en sådan automatiserad lösning i stället.

I vissa fall kan direktåtkomst emellertid vara att föredra, oftast på grund av särskild verksamhetsreglering. T.ex. har Lantmäteriet för närvarande i sitt myndighetsuppdrag att tillhandahålla personuppgifter ur fastighetsregistret till enskilda utifrån samhällets behov,[92] vilket innebär att informationen bl.a. ska kunna laddas ner i form av en s.k. bulknedladdning och kunna vidareutnyttjas för olika ändamål. Sådan personuppgiftsbehandling, som alltså möjliggör nedladdning, urval och bearbetningar, kan medföra att det uppstår ökade integritetsrisker jämfört med om informationen görs tillgänglig via direktåtkomst.[93] Urval och bearbetningar kan leda till att uppgifter sammanställs och medför att det sker kartläggningar som är känsliga ur integritetssynpunkt. För att minska sådana risker kan direktåtkomst utformas som sök- och visningstjänster och särskiljas från tjänster som syftar till att möjliggöra nedladdning av information. Vid direktåtkomst ligger informationen kvar hos den registerhållande myndigheten och innebär på så sätt ökad kontroll över informationen även när den behandlas i olika led av vidareutnyttjande i dataplattormar och dataprodukter som tillhandahålls av privata aktörer till användare i såväl privat som offentlig sektor. Teknikutvecklingen kring realtidsdata eller så kallade dynamiska data[94] kan också kräva särskilda överväganden kring formen för utlämnande där tillhandahållande av information som huvudregel behöver baseras på ett proaktiv tillgängliggörande.

eSam menar att den personuppgiftsansvariga myndigheten själv bör ha möjlighet att bedöma vilken form för utlämnande som är lämplig, med beaktande av tekniska och organisatoriska skyddsåtgärder. Här kan flera omständigheter vara av betydelse, såsom materiell lagstiftning, vilken typ av personuppgifter det rör sig om och vilka risker som finns. Regleringen i registerförfattningar bör således som utgångspunkt vara teknikneutral. Om lagstiftaren bedömer det nödvändigt kan vissa integritetshöjande regler finnas angivna, som gäller oberoende av vald teknik för utlämnande.

5.4.4 Rekvisitet "olämpligt" är obehövligt

I Polismyndighetens, Tullverkets, Kustbevakningens och Skatteverkets registerlagstiftning inom det brottsbekämpande området i registerlag för

[92] Se 1 § lagen (2000:224) om fastighetsregister och 3 § 2 p förordningen (2009:946) med instruktion för Lantmäteriet.
[93] Se integritetsbedömning i fråga om uppgift om inteckningar i fastighetsregistret, prop. 1999/2000:39 s. 96-98.
[94] Läs mer om dynamiska data i SOU 2020:55.

Rättsmedicinalverket och i domstolsdatalagen anges att personuppgifter får lämnas ut elektroniskt om det inte är olämpligt.[95]

Fråga uppkommer vilka kriterier som kan komma att ingå i en lämplighetsbedömning då en myndighet ska lämna ut personuppgifter elektroniskt. E-offentlighetskommittén diskuterade i slutbetänkandet ”Allmänna handlingar i elektronisk form” kring begreppet olämplighet i förhållande till elektroniskt utlämnande av allmänna handlingar.[96] E-offentlighetskommittén fann att kriteriet olämplighet främst syftar på att myndigheten ska överväga effekterna av ett elektroniskt utlämnande för upprätthållandet av skyddet för enskildas personliga integritet.[97]

I förarbeten till Rättsmedicinalverkets registerförfattning anges att det vid lämplighetsbedömningen bör göras skillnad mellan utlämnande till myndigheter och utlämnande till enskilda. Det bör normalt inte anses olämpligt att lämna ut personuppgifter elektroniskt till myndigheter. Om det i ett enskilt fall skulle bedömas vara olämpligt bör emellertid personuppgifterna lämnas ut på annat sätt. När det gäller enskilda kan det krävas närmare överväganden bl.a. med hänsyn till vem mottagaren är och vilken säkerhet mottagaren har för sin personuppgiftsbehandling. Vid bedömningen av om ett utlämnande är olämpligt ska bl.a. typen av personuppgifter beaktas. Den närmare innebörden av vad som ska anses vara ett olämpligt utlämnande får dock utvecklas genom tillsynsmyndighetens arbete och i domstolspraxis.[98]

Frågan om elektroniskt utlämnande till enskilda är särskilt svårbedömd när det på grund av uppgifternas art, struktur, antal eller någon annan särskild omständighet finns anledning att befara att utlämnandet kan leda till integritetsrisker.[99] Om det kan antas att personuppgifterna kan komma att behandlas i strid med dataskyddsförordningen eller dataskyddslagen om de lämnas ut elektroniskt gäller sekretess enligt 21 kap. 7 §

---

[95] I Rättsmedicinalverkets registerlag är det uttryckligen angivet att utlämnade inte får ske genom direktåtkomst. I övriga registerlagar uttrycks att personuppgifter får lämnas ut elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt. Reglering finns också i vilka fall direktåtkomst är tillåten. Se 2 kap. 12 § lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område, 2 kap. 9 § lagen (2018:1694) om Tullverkets behandling av personuppgifter inom brottsdatalagen område, 2 kap. 8 § lagen (2018:1695) om Kustbevakningens behandling av personuppgifter inom brottsdatalagens område, 2 kap. 9 § lagen (2018:1696) om Skatteverkets behandling av personuppgifter inom brottsdatalagens område, 16 § domstolsdatalagen (2015:728) och 1 kap. 9 § lagen (2020:421) om Rättsmedicinalverkets behandling av personuppgifter.

[96] SOU 2010:4 s. 312.

[97] Andra exempel som ges är att det kan vara olämpligt att lämna ut en handling i elektronisk form om det finns regler i myndighetens registerförfattning som indikerar att den aktuella uppgiften eller handlingen bör omgärdas av en viss försiktighet. Det kan exempelvis gälla särskilda gallringsregler för vissa uppgifter som indikerar att de är i viss mening känsliga. Vidare kan det röra sig om sådana handlingar som innehåller uppgifter som omfattas av förbud mot att använda vissa sökbegrepp. Omfattningen av personuppgifter kan naturligtvis också vara utslagsgivande. Är det t.ex. fråga om massuttag kan det finnas skäl att närmare överväga lämpligheten av ett utlämnande i elektronisk form. Det kan även beroende på omständigheterna också vara olämpligt att lämna ut en handling i elektronisk form som myndigheten fått tillgång till genom direktåtkomst hos en annan myndighet. Utöver integritetsskyddsaspekter kan det finnas andra faktorer som talar mot att lämna ut den allmänna handlingen i elektronisk form. Det kan vara faktorer som säkerhetsaspekter och tekniska eller praktiska faktorer som talar mot ett elektroniskt utlämnande i det specifika fallet. Även vid omfattande uttag av t.ex. geografisk information som tar stora resurser i anspråk att hantera och som därtill kan vara svåra att ”förpacka” och leverera, kan det vara motiverat att neka en begäran om utfående i elektronisk form. Vidare kan det finnas situationer där myndigheten kommer fram till att det framstår som olämpligt att lämna ut en efterfrågad handling i elektronisk form då det i det enskilda fallet är osäkert om en rimlig säkerhetsnivå till skydd för i handlingen ingående personuppgifter kan upprätthållas vid utlämnande genom t.ex. e-post.

[98] Prop. 2019/20:106 s. 55 f. Se även prop. 2017/18:269 s.136.

[99] Jfr. prop. 2014/15:148 s. 114.

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. Vid begäran av en allmän handling med stöd av tryckfrihetsförordningen får den utlämnande myndigheten inte efterforska syftet med begäran, vilket kan ha betydelse vid prövningen av om det i ett enskilt fall är lämpligt att lämna ut en handling med personuppgifter elektroniskt.[100] Vidare undersökningar kan dock vara tillåtet om det finns konkreta omständigheter som indikerar att mottagaren kommer att behandla uppgifterna på ett sätt som strider mot dataskyddsregleringen, t.ex. massuttag eller selekterade uttag.[101]

Vid prövningen av om personuppgifter kan lämnas ut elektroniskt är informationssäkerheten av stor betydelse. Det kan finnas situationer där det framstår som olämpligt att lämna ut en efterfrågad handling i elektronisk form när det i det enskilda fallet är osäkert om en rimlig säkerhetsnivå till skydd för i handlingen ingående personuppgifter kan upprätthållas vid utlämnande genom t.ex. e-post. En sådan bedömning måste alltid göras, oaktat formulering i registerförfattning.

Samtliga de kriterier som kan ingå i en lämplighetsbedömning och som har lyfts fram i förarbeten är sådana som tillgodoses genom reglering i dataskyddsförordningen och offentlighets- och sekretesslagen. En reglering om lämplighetsbedömning i registerförfattning framstår därför som obehövlig.[102]

[100] Prop. 2017/18:269 s. 321.
[101] JO:s beslut 2013-08-28 (dnr 4171-2011)
[102] Jfr. Arbetsförmedlingens hemställan En mer träffsäker och enhetlig arbetsmarknadspolitisk bedömning och förbättrad kvalitet i uppföljningen av matchningstjänster, Af-2022/0013 1747, s. 42.

6. Sekretessbrytande bestämmelser

eSam förespråkar att registerförfattningar renodlas från sekretessbrytande bestämmelser.

För utlämnande av sekretesskyddad information krävs en sekretessbrytande bestämmelse. Sådana bestämmelser kan finnas i registerförfattningar.[103] Det förekommer också att en bestämmelse om direktåtkomst innehåller den sekretessbrytande regeln. Om särreglering beträffande direktåtkomst tas bort så måste lagstiftaren säkerställa att den sekretessbrytande bestämmelsen återfinns i annan lag eller förordning. eSam menar att sekretessbrytande bestämmelser inte hör hemma i registerförfattningar. Dessa bör i stället finnas i offentlighets- och sekretesslagstiftningen eller i materiell författning. En sådan ändring skulle även vara att föredra ur pedagogisk synvinkel, då regleringen upplevs som mer tillgänglig för en utomstående. Ur ett dataskyddsperspektiv vore det också bättre om registerförfattningarna renodlas till att enbart innehålla bestämmelser om personuppgiftsskydd.

[103] Se t.ex. 7 § 3 st. förordning (2001:588) om behandling av uppgifter i Skatteverkets beskattningsverksamhet.

eSam är ett medlemsdrivet program för samverkan mellan myndigheter för att underlätta och påskynda digitaliseringen inom det offentliga. eSam bildades 2015 som en frivillig fortsättning på E-delegationen. En viktig uppgift för eSam är att ta fram stöd och vägledningar som ger förutsättningar för att öka den digitala samverkan inom offentlig förvaltning.

Alla stöddokument finns på esamverka.se

I eSam ingår Arbetsförmedlingen, Bolagsverket, Boverket, Centrala Studiestödsnämnden, Domstolsverket, eHälso-myndigheten, Ekonomistyrningsverket, Folkhälsomyndigheten, Försäkringskassan, Havs- och vattenmyndigheten, Inspektionen för vård och omsorg, Jordbruksverket, Kriminalvården, Kronofogdemyndigheten, Lantmäteriet, Länsstyrelserna, Migrationsverket, Naturvårdsverket, Patent- och Registreringsverket, Pensionsmyndigheten, Polisen, Riksarkivet, Rättsmedicinalverket, Sida, Skatteverket, Skolverket, Statens institutionsstyrelse, Statens servicecenter, Statens tjänstepensionsverk, Statistiska centralbyrån, Tillväxtverket, Trafikverket, Transportstyrelsen, Tullverket och Universitets- och högskolerådet.