Ökat informationsutbyte mellan myndigheter

– några anslutande frågor

Slutbetänkande av Utredningen om förbättrade möjligheter till informationsutbyte mellan myndigheter

Stockholm 2025

STATENS OFFENTLIGA UTREDNINGAR

SOU 2025:45

SOU och Ds finns på regeringen.se under Rättsliga dokument.

Svara på remiss – hur och varför
Statsrådsberedningen, SB PM 2021:1.
Information för dem som ska svara på remiss finns tillgänglig på regeringen.se/remisser.

Layout: Kommittéservice, Regeringskansliet
Omslag: Elanders Sverige AB
Tryck och remisshantering: Elanders Sverige AB, Stockholm 2025

ISBN 978-91-525-1227-2 (tryck)
ISBN 978-91-525-1228-9 (pdf)
ISSN 0375-250X

Till statsrådet och chefen för Justitiedepartementet Gunnar Strömmer

Regeringen beslutade den 19 oktober 2023 att ge en särskild utredare i uppdrag att överväga och föreslå förbättrade möjligheter att utbyta information om enskilda inom och mellan myndigheter och andra organ som enligt offentlighets- och sekretesslagen (2009:400) jämställs med myndigheter (dir. 2023:146). Tiden för uppdraget förlängdes genom tilläggsdirektiv den 19 september 2024 till den 28 april 2025 (dir. 2024:87).

Uppdraget avsåg att kartlägga behovet av att myndigheter får förbättrade möjligheter att utbyta information med varandra i syfte att särskilt förhindra, förebygga, upptäcka, utreda och ingripa mot fusk, felaktiga utbetalningar, regelöverträdelser och brottslighet, att analysera och ta ställning till hur behovet av att utbyta sekretessbelagd information kan tillgodoses, att särskilt överväga och lämna förslag på en generell bestämmelse som gör det möjligt att på ett effektivt sätt lämna uppgifter som omfattas av sekretess till skydd för enskilda till en annan myndighet, såväl på begäran som på eget initiativ, att analysera och ta ställning till hur behovet av att utbyta offentlig information kan tillgodoses, att särskilt överväga och lämna förslag på en bestämmelse som i större utsträckning gör det möjligt att på eget initiativ lämna ut offentliga uppgifter till en annan myndighet samt att göra en översyn, i den utsträckning det behövs, av myndigheternas registerförfattningar.

Som särskild utredare förordnades den 19 oktober 2023 lagmannen Göran Lundahl.

Till sakkunniga att biträda utredningen förordnades den 1 december 2023 rättssakkunniga Erika Löwhagen (Justitiedepartementet) och den 13 november 2024 rättssakkunniga Sofia Grönesjö (Justitie-

departementet). Till experter förordnades den 1 december 2023 kammarrättslagmannen Peder Liljeqvist och numera rättsliga experten Liselotte Westerlind. Den 5 mars 2024 förordnades följande ytterligare experter: Rättssakkunniga Sofie Abdsaleh (Finansdepartementet), kanslirådet Alexander Bornevall (Justitiedepartementet), numera ämnesrådet Sophia Busk (Justitiedepartementet), kanslirådet Johanna Edner (Finansdepartementet), departementsrådet Karin Hermanrud (Arbetsmarknadsdepartementet), numera kanslirådet Jonatan Lundqvist (Justitiedepartementet), departementssekreteraren Sandra Rosenälv (Socialdepartementet), ämnessakkunniga Hélène Runsten (Socialdepartementet) och den seniore rådgivaren Torben Vincentsen (Arbetsmarknadsdepartementet).

Torben Vincentsen entledigades från sitt uppdrag den 22 januari 2025.

Som sekreterare i utredningen anställdes rådmannen Nils Sjöblom från och med den 1 december 2023 och kammarrättsassessorn Ulrika Matsson från och med den 1 januari 2024.

Utredningen är formellt ett uppdrag för Göran Lundahl som särskild utredare. Arbetet har emellertid bedrivits i nära samråd med experter och sakkunniga och är därför avfattat i vi-form, även om det kan förekomma skilda uppfattningar i vissa delar.

Utredningen har antagit namnet Utredningen om förbättrade möjligheter till informationsutbyte mellan myndigheter (Ju 2023:22). Den 2 september 2024 överlämnade utredningen delbetänkandet *Ökat informationsutbyte mellan myndigheter. Behov och föreslagna förändringar* (SOU 2024:63). Utredningen överlämnar härmed slutbetänkandet *Ökat informationsutbyte mellan myndigheter – några anslutande frågor* (SOU 2025:45).

Uppdraget är med detta slutfört.

Stockholm i april 2025

Göran Lundahl

Nils Sjöblom
Ulrika Matsson

Innehåll

Bilagor

Sammanfattning

Vårt uppdrag

Vi har i denna del haft i uppdrag att analysera och ta ställning till hur behovet av att utbyta offentlig information kan tillgodoses, särskilt överväga och lämna förslag på en bestämmelse som i större utsträckning gör det möjligt att på eget initiativ lämna ut offentliga uppgifter till en annan myndighet, göra en översyn, i den utsträckning det behövs, av myndigheternas registerförfattningar, för att möjliggöra att de förslag som lämnas tjänar sitt syfte och kan tillämpas på ett ändamålsenligt sätt, och lämna nödvändiga författningsförslag. I vårt övergripande uppdrag har det även ingått att väga behovet av ett förbättrat informationsutbyte mot den enskildes rätt till skydd för sin personliga integritet.

Förbättrade möjligheter till utbyte av uppgifter som inte är sekretessbelagda

Bakgrund

Vad gäller s.k. offentliga uppgifter har vi i stället använt begreppet uppgifter som inte är sekretessbelagda.

Uppgifter som inte är sekretessbelagda får lämnas till en annan myndighet utan hinder av sekretess. När en annan myndighet begär att få del av uppgifter som inte är sekretessbelagda har den myndighet som förfogar över sådana uppgifter en långtgående skyldighet att lämna ut dem enligt 6 kap. 5 § offentlighets- och sekretesslagen (2009:400), OSL. Bestämmelsen är ett uttryck för myndigheters samverkansskyldighet som bl.a. framgår av 8 § förvaltningslagen (2017:900). Det finns dock ingen generell reglering som uttryck-

ligen tillåter att den utlämnande myndigheten lämnar uppgifter som inte är sekretessbelagda till en annan myndighet på eget initiativ.

Enligt dataskyddsförordningen[1] måste all vidarebehandling av personuppgifter som sker för ett annat ändamål än insamlingsmålet ha stöd i den nationella rätten eller unionsrätten, om det nya ändamålet inte är förenligt med insamlingsändamålet. Eftersom det inte finns någon generell bestämmelse om att myndigheter på eget initiativ får lämna uppgifter som inte är sekretessbelagda till en annan myndighet så föreligger i praktiken ett hinder mot sådant utlämnande, trots att det inte finns några sekretesshinder mot det.

Behovet av ett utlämnande kan dock uppstå av den anledningen att den mottagande myndigheten saknar kännedom om uppgifter som är relevanta för verksamheten, och därför inte heller kan begära ut dem. Vi har kunnat kartlägga ett stort behov av att kunna lämna ut uppgifter på eget initiativ i högre utsträckning än i dag. Behoven som vi har kunnat kartlägga avser även uppgifter som inte är sekretessbelagda.

Vi har bedömt att den befintliga tillåtligheten av egeninitierat utlämnande i vissa fall behöver förtydligas, och att det mot bakgrund av regleringen i 6 kap. 5 § OSL inte finns bärande skäl för att begränsa myndigheters möjlighet att på eget initiativ lämna relevanta uppgifter som inte är sekretessbelagda till en annan myndighet.

Vårt förslag: En ny generell bestämmelse om utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ

Vi har föreslagit att det ska införas av en ny bestämmelse i offentlighets- och sekretesslagen som ska komplettera 6 kap. 5 § i den lagen. Enligt bestämmelsen får en myndighet utan begäran lämna en uppgift till en annan myndighet, om uppgiften inte är sekretessbelagd och utlämnandet kan antas vara av betydelse för att den utlämnande eller den mottagande myndigheten ska kunna fullgöra sin författningsreglerade verksamhet. Syftet med bestämmelsen är att skapa ett tydligt rättsligt stöd för myndigheterna att, när det finns skäl för det, lämna uppgifter som inte är sekretessbelagda till andra myndigheter.

[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).

Tröskeln för sådant utlämnande som är tillåtet enligt bestämmelsen är lågt satt, det räcker med att det *kan antas* att ett utlämnande är av betydelse för att den utlämnande eller den mottagande myndigheten ska kunna fullgöra sin författningsreglerade verksamhet. Vi har dock utgått från att i många fall kommer den faktiska tillämpningen av bestämmelsen sannolikt att föregås av någon slags samverkan mellan de inblandade myndigheterna, i vart fall inför mer rutinmässiga utlämnanden.

Bestämmelsen kommer att träffa vissa uppgifter som inte är sekretessbelagda men som redan träffas av en särskilt reglerad skyldighet att lämna ut på eget initiativ. Myndigheterna får dock iaktta tillämpliga bestämmelser om uppgiftsskyldighet på eget initiativ oberoende av den nya bestämmelsen. Det krävs vidare inte att en uppgift är dokumenterad hos den utlämnande myndigheten för att bestämmelsen ska kunna tillämpas. Till skillnad från 6 kap. 5 § OSL är bestämmelsen alltså inte förenad med ett krav på att den utlämnande myndigheten förfogar över uppgiften i den meningen som avses i den bestämmelsen.

En upplysningsbestämmelse i kompletterande dataskyddsreglering om utlämnande i överensstämmelse med lag eller förordning

Bakgrund

Vad gäller s.k. registerförfattningar har vi i stället använt begreppet kompletterande dataskyddsreglering.

Inom den kompletterande dataskyddsregleringen finns det ett generellt reformbehov. Vår översyn har dock varit begränsad till bestämmelser som uttryckligen reglerar vidarebehandling av personuppgifter, bestämmelser som kan uppfattas begränsa möjligheterna till utlämnande av uppgifter (ändamålsbestämmelser) och bestämmelser som reglerar om ett utlämnande får ske elektroniskt. Vi har också kartlagt att myndigheter generellt har behov av förbättrade möjligheter till informationsutbyte som inbegriper den kompletterande dataskyddsregleringen. Totalt omfattar vår översyn ett 50-tal författningar.

I nästan alla fall där det förekommer s.k. uttömmande ändamålsbestämmelser, dvs. att personuppgifter *endast* eller *bara* får behandlas

för särskilt angivna ändamål, eller ändamålsbestämmelser som på annat sätt kan uppfattas hindra ett utlämnande, speglas dessa inte av den materiella sekretessregleringen på området. Det kan alltså uppfattas föreligga ett dataskyddsrättsligt hinder mot att behandla personuppgifter för andra ändamål än att utföra viss verksamhet, samtidigt som uppgifterna får, eller till och med ska, lämnas ut till en annan myndighet enligt bestämmelserna i offentlighets- och sekretesslagen.

I offentlighetens- och sekretesslagen anvisas på vilket sätt begränsningar av lagens bestämmelser kan göras; antingen genom undantag direkt i offentlighets- och sekretesslagen och/eller hänvisning till annan författning där vad som ska gälla i stället framgår. Vi har bedömt att samtliga förbud mot att röja en uppgift som ska gälla i det allmännas verksamhet ska framgå av offentlighets- och sekretesslagen på det sätt som anvisas.

Vi har vidare noterat att i likhet med övriga bestämmelser i kompletterande dataskyddsreglering kan ändamålsbestämmelser ha fått en förändrad tillämplighet genom digitaliseringen av den offentliga förvaltningen och den rättsliga utvecklingen. Vi har därför bedömt att ändamålsbestämmelser i kompletterande dataskyddsreglering inte vare sig syftar till att hindra, eller rent faktiskt kan hindra, tillämpligheten av bestämmelserna i offentlighets- och sekretesslagen.

Vårt förslag: I kompletterande dataskyddsreglering som omfattas av vår översyn ska det införas upplysningsbestämmelser om tillåtligheten av uppgiftslämnande i överensstämmelse med lag eller förordning

För att åstadkomma en enklare, mer enhetlig och mer lättillämpad reglering av myndigheters informationsutbyte har vi föreslagit att det införs en upplysningsbestämmelse om att personuppgifter får behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning, i de författningar som omfattas av vår översyn. Även om bestämmelsen inte har någon sekretessbrytande verkan, eller någon självständig rättslig betydelse för tillåtligheten av behandlingen, så kan den bidra till ökad förutsebarhet i frågan om hur uppgifter om enskilda registrerade får behandlas.

På vissa områden kan det finnas skäl att överväga om bestämmelser i offentlighets- och sekretesslagen bör anpassas efter de föreslagna förändringarna av den kompletterande dataskyddsregleringen. Vi har

dock bedömt att det inte faller inom ramen för vårt uppdrag att överväga de förändringar av offentlighets- och sekretesslagens bestämmelser som kan vara påkallade.

Förändringar av brottsdatalagen

Bakgrund

I all dataskyddsreglering som kompletterar brottsdatalagen (2018:1177) hänvisas till brottsdatalagens bestämmelser vad gäller frågan om vidarebehandling eller ny behandling av personuppgifter. Regleringen i brottsdatalagen innebär att det görs en dataskyddsrättslig åtskillnad mellan bestämmelser om myndigheters informationsutbyte som innebär en skyldighet att lämna uppgifter och bestämmelser som innebär en möjlighet att lämna uppgifter. När det rör sig om en möjlighet att lämna uppgifter måste den personuppgiftsansvariga myndigheten pröva om den tillkommande behandlingen är nödvändig och proportionerlig, något som inte krävs om det föreligger en skyldighet att lämna uppgifter.

Vårt förslag: I brottsdatalagen ska allt uppgiftsutlämnande som sker i överenstämmelse med lag eller förordning regleras på samma sätt

Eftersom samtliga förbud mot att röja en uppgift som ska gälla i det allmännas verksamhet framgår av offentlighets- och sekretesslagen finns det inte skäl att göra någon annan bedömning för den brottsbekämpande verksamheten än för andra verksamheter. Vi har därför föreslagit att bestämmelserna om vidarebehandling och ny behandling i brottsdatalagen ska ändras på så sätt att någon nödvändighets- och proportionalitetsprövning inte ska göras när vidarebehandling eller ny behandling sker för utlämnande i överensstämmelse med lag eller förordning. Ändringen innebär att en behörig myndighet inte behöver utföra några andra prövningar än om utlämnandet är tillåtet enligt offentlighets- och sekretesslagen, med iakttagande av vad som följer av allmänna dataskyddsrättsliga principer.

Elektroniskt utlämnande

Bakgrund

I den kompletterande dataskyddsregleringen förekommer bestämmelser som reglerar om och hur personuppgifter får lämnas ut elektroniskt. Vid *direktåtkomst* hämtar den mottagande myndigheten information direkt från den utlämnande myndighetens it-system. Utlämnande genom direktåtkomst har tidigare ansetts förknippat med högre integritetsrisker än andra former av elektroniskt utlämnande, och det är fortfarande vanligt att sådant utlämnande är förbjudet om det inte uttryckligen är tillåtet. *Annat elektroniskt utlämnande än direktåtkomst* avser inte någon särskild form av elektronisk informationsöverföring och det är vanligt att sådant utlämnande inte regleras över huvud taget, eller är tillåtet om det inte är olämpligt.

Vårt förslag: Elektroniskt utlämnande ska vara tillåtet om det inte är olämpligt

Vad gäller annat elektroniskt utlämnande än direktåtkomst har vi bedömt att det inte längre finns några sakliga skäl att begränsa myndigheters möjligheter till informationsutbyte med andra myndigheter i sådan form. Vi har därför bedömt att det bör införas tydligt tillåtande bestämmelser om elektroniskt utlämnande på annat sätt än genom direktåtkomst. Frågan om det finns sakliga skäl för en fortsatt särreglering av direktåtkomst faller dock utanför ramen för vårt uppdrag. I syfte att dels uppmärksamma behovet av nödvändiga överväganden innan ett elektroniskt utlämnande, dels utforma regleringen så enhetligt som möjligt, har vi föreslagit att bestämmelser om elektroniskt utlämnande på annat sätt än genom direktåtkomst ska förenas med ett krav på att utlämnande på detta sätt inte ska vara olämpligt. Den föreslagna bestämmelsen ska alltså inte tolkas som att den medför en rätt för mottagaren att få ut uppgifter genom någon form av elektronisk informationsöverföring. Bestämmelsen innebär därmed inte heller någon generell eller specifik skyldighet att lämna ut uppgifter på ett visst sätt eller i ett visst format. Bestämmelsen innebär endast att den myndighet som har uppgifter som den får eller måste lämna ut också har en rättslig möjlighet att göra det elektroniskt,

om det framstår som lämpligt i förhållande till de omständigheter som är aktuella, och inte utgör ett utlämnande genom direktåtkomst.

Skyddet för den personliga integriteten

Förslaget om utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ

Vi har bedömt att förslaget om att uppgifter som inte är sekretessbelagda i vissa fall ska få lämnas till en annan myndighet utan en begäran innebär flera integritetsrisker och en inskränkning i rätten till skydd för personuppgifter. Vår bedömning är att förslaget totalt sett kan medföra en personuppgiftsbehandling som kan komma att omfatta uppgifter om hela Sveriges befolkning.

Vi har dock även bedömt att det finns viktiga mål av generellt allmänt intresse som kräver att den nuvarande regleringssituationen åtgärdas för att kunna uppfyllas, bl.a. myndigheternas skyldighet att samverka med andra myndigheter och att utbyta information och de intressen som låg till grund för förslaget om en generell sekretessbrytande bestämmelse. Vi har även bedömt att bestämmelsen är nödvändig utifrån det kartlagda behovet och att det inte finns några andra sätt att åtgärda problemet på. Sammantaget har vi också bedömt att bestämmelsen, tillsammans med övrig reglering som begränsar svenska myndigheters utrymme att behandla personuppgifter, omfattar tillräckliga och adekvata skyddsåtgärder. Vi har slutligen bedömt att den föreslagna bestämmelsen är både lämplig och berättigad i förhållande till den nackdel den innebär för enskilda, dvs. proportionerlig. Vi har i det sammanhanget även bedömt att bestämmelsen bidrar till att tillförsäkra barn det skydd som krävs enligt barnkonventionen och att den därmed är förenlig med barnkonventionen.

Förslaget om att införa upplysningsbestämmelser om utlämnande i överensstämmelse med lag eller förordning

Vi har bedömt att förslaget om att det ska införas upplysningsbestämmelser om utlämnande i överensstämmelse med lag eller förordning i kompletterande dataskyddsreglering inte utgör en

sådan förändring av gällande rätt som påverkar enskildas rätt till skydd för personuppgifter.

Förslaget om utlämnande i överensstämmelse med lag eller förordning i brottsdatalagen

Vi har bedömt att förslaget om att allt uppgiftslämnande som sker i överenstämmelse med lag eller förordning ska regleras på samma sätt i brottsdatalagen inte utgör en sådan förändring av gällande rätt som påverkar enskildas rätt till skydd för personuppgifter.

Förslaget om att elektroniskt utlämnande ska vara tillåtet om det inte är olämpligt

Vi har bedömt att förslaget om att elektroniskt utlämnande på annat sätt än genom direktåtkomst ska vara tillåtet om det inte är olämpligt inte medför väsentligt förhöjda integritetsrisker eller en inskränkning av enskildas rätt till skydd för personuppgifter. Vi har även bedömt att förslaget är motiverat och proportionerligt.

Ikraftträdande- och övergångsbestämmelser

Vi har föreslagit att författningsändringarna ska träda i kraft den 1 oktober 2026. Vi har bedömt att det inte finns något behov av särskilda övergångsbestämmelser.

Konsekvenser

Allmänna konsekvenser

En ökad tydlighet, mer enhetlighet och färre motstridigheter i den sammantagna regleringen av myndigheters informationsutbyte kommer att underlätta myndigheternas samverkan med varandra och andra aktörer. Förslagen innebär att statens resurser kommer att kunna användas mer effektivt genom att omotiverade hinder för myndigheterna att utnyttja den moderna teknikens fördelar tas bort.

En konsekvens av detta blir att ärendehantering, service till enskilda och informationsutbyte mellan myndigheter kan ske på ett mer ändamålsenligt, säkert och effektivt sätt än i dag. Det kommer även innebära att enskilda ges större möjligheter att förstå lagstiftningen och därmed enklare kan tillvarata sina rättigheter enligt det allmänna dataskyddsrättsliga regelverket.

Ekonomiska konsekvenser för det allmänna och för enskilda

Vi har bedömt att våra förslag inte bör leda till något ökat resursbehov för de statliga myndigheterna. Inte heller bör våra förslag, som inte innebär några nya åligganden, leda till kostnadsökningar för kommuner och regioner. Våra förslag bör inte heller föranleda några påtagligt ökade kostnader för företag och andra enskilda.

Förslagens betydelse för brottsligheten och det brottsförebyggande arbetet

Vi har bedömt att våra förslag kommer att ge bättre förutsättningar för myndigheter att förebygga brottslig verksamhet.

Sveriges internationella åtaganden

Vi har bedömt att våra förslag är förenliga med de krav som följer av EU-rätten, Barnkonventionen och Sveriges övriga internationella åtaganden.

Övriga konsekvenser

Vi har bedömt att våra förslag inte innebär någon inskränkning i det kommunala självstyret. Vi har även bedömt att våra förslag inte heller i övrigt innebär några påtagliga konsekvenser för sysselsättning och offentlig service i olika delar av landet, för små företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt i förhållande till större företag, för jämställdheten mellan kvinnor och män eller för möjligheterna att nå de integrationspolitiska målen.

1 Författningsförslag

1.1 Förslag till lag om ändring i rennäringslagen (1971:437)

Härigenom föreskrivs i fråga om rennäringslagen (1971:437) att det ska införas en ny paragraf, 74 a §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	74 a §
	Personuppgifter som behandlas i renmärkesregistret får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.

Denna lag träder i kraft den 1 oktober 2026.

1.2 Förslag till lag om ändring i lagen (1994:448) om pantbrevsregister

Härigenom föreskrivs i fråga om lagen (1994:448) om pantbrevsregister att det ska införas en ny paragraf, 3 a §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	3 a §
	Personuppgifter som behandlas i pantbrevsregistret får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.

Denna lag träder i kraft den 1 oktober 2026.

1.3 Förslag till lag om ändring i vapenlagen (1996:67)

Härigenom föreskrivs i fråga om vapenlagen (1996:67) att det ska införas en ny paragraf, 1 a kap. 8 a §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	1 a kap.
	8 a §
	Personuppgifter som behandlas i vapenregistret får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.

Denna lag träder i kraft den 1 oktober 2026.

1.4 Förslag till lag om ändring i lagen (2001:183) om behandling av personuppgifter i verksamhet med val och folkomröstningar

Härigenom föreskrivs i fråga om lagen (2001:183) om behandling av personuppgifter i verksamhet med val och folkomröstningar

dels att nuvarande 1 kap. 5 a § ska betecknas 1 kap. 5 b §,

dels att det ska införas en ny paragraf, 1 kap. 5 a §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	1 a kap.
	5 a §
	Personuppgifter som behandlas enligt 4 och 5 §§ får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.

Denna lag träder i kraft den 1 oktober 2026.

1.5 Förslag till lag om ändring i lagen (2001:454) om behandling av personuppgifter inom socialtjänsten

Härigenom föreskrivs i fråga lagen (2001:454) om behandling av personuppgifter inom socialtjänsten att 6 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
6 §	
Personuppgifter får behandlas bara om behandlingen är nödvändig för att arbetsuppgifter inom socialtjänsten *skall* kunna utföras.	Personuppgifter får behandlas bara om behandlingen är nödvändig för att arbetsuppgifter inom socialtjänsten *ska* kunna utföras.
Personuppgifter får även behandlas för *uppgiftsutlämnande som föreskrivs* i lag eller förordning.	Personuppgifter *som behandlas enligt första stycket* får även behandlas för *uppgiftslämnande i överensstämmelse med* lag eller förordning.

En registrerad person har inte rätt att motsätta sig sådan behandling av uppgifter som är tillåten enligt denna lag.

Denna lag träder i kraft den 1 oktober 2026.

1.6 Förslag till lag om ändring i lagen om (2006:378) om lägenhetsregister

Härigenom föreskrivs i fråga om lagen (2006:378) om lägenhetsregister
dels att 20 § och rubriken närmast 20 § ska ha följande lydelse,
dels att det ska införas en ny paragraf, 5 a §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	5 a § *Personuppgifter som behandlas i lägenhetsregistret får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.*
Utlämnande på medium för automatiserad behandling	***Elektroniskt utlämnande***
20 §[1]	
Uppgifter i lägenhetsregistret får lämnas ut *på medium för automatiserad behandling endast om regeringen meddelar föreskrifter om det.*	Uppgifter i lägenhetsregistret får lämnas ut *elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt*.

Denna lag träder i kraft den 1 oktober 2026.

[1] Senaste lydelse 2016:397.

1.7 Förslag till lag om ändring i lagen (2006:444) om passagerarregister

Härigenom föreskrivs i fråga om lagen (2006:444) om passagerarregister att det ska införas en ny paragraf, 4 a §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	4 a § *Personuppgifter som behandlas i passagerarregistret får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.*

Denna lag träder i kraft den 1 oktober 2026.

1.8 Förslag till lag om ändring i lagen (2006:496) om blodsäkerhet

Härigenom föreskrivs i fråga om lagen (2006:496) om blodsäkerhet
dels att nuvarande 16 a § ska betecknas 16 b §,
dels att det ska införas en ny paragraf, 16 a §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	16 a § *Personuppgifter som behandlas enligt 16 § får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.*

Denna lag träder i kraft den 1 oktober 2026.

1.9 Förslag till lag om ändring i lagen (2007:1150) om tillsyn över hundar och katter

Härigenom föreskrivs i fråga om lagen (2007:1150) om tillsyn över hundar och katter att 5 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*

5 §[1]

Register över hund- och kattägare enligt 3 § får användas för att fastställa vem som äger en hund eller en katt.

Tullverket, Jordbruksverket, länsstyrelserna, Polismyndigheten och de kommunala nämnder som fullgör uppgifter inom miljö- och hälsoskyddsområdet får medges direktåtkomst till register över hund- och kattägare.

Personuppgifter som behandlas i registret får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.

Denna lag träder i kraft den 1 oktober 2026.

[1] Senaste lydelse 2022:186.

1.10 Förslag till lag om ändring i lagen (2008:286) om kvalitets- och säkerhetsnormer vid hantering av mänskliga vävnader och celler

Härigenom föreskrivs i fråga om lagen (2008:286) om kvalitets- och säkerhetsnormer vid hantering av mänskliga vävnader och celler

dels att nuvarande 21 a § ska betecknas 21 b §,

dels att det ska införas en ny paragraf, 21 a §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	21 a §
	Personuppgifter i det register som anges i 21 § får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.

Denna lag träder i kraft den 1 oktober 2026.

1.11 Förslag till lag om ändring i patientdatalagen (2008:355)

Härigenom föreskrivs i fråga om patientdatalagen (2008:355) att 5 kap. 6 § och rubriken närmast före 5 kap. 6 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	5 kap.
Utlämnande på medium för automatiserad behandling	***Elektroniskt utlämnande av personuppgifter***
	6 §
Får en personuppgift lämnas ut, *kan det ske på medium för automatiserad behandling*.	*Personuppgifter får* lämnas ut *elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt*.

Denna lag träder i kraft den 1 oktober 2026.

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

Härigenom föreskrivs i fråga om offentlighets- och sekretesslagen (2009:400) att det ska införas en ny paragraf, 6 kap. 5 a §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	6 kap.
	5 a §
	En myndighet får utan begäran lämna en uppgift till en annan myndighet, om
	1. uppgiften inte är sekretessbelagd, och
	2. utlämnandet kan antas vara av betydelse för att den utlämnande eller den mottagande myndigheten ska kunna fullgöra sin författningsreglerade verksamhet.

Denna lag träder i kraft den 1 oktober 2026.

1.13 Förslag till lagen om ändring i patientsäkerhetslagen (2010:659)

Härigenom föreskrivs i fråga om patientsäkerhetslagen (2010:659) att det ska införas en ny paragraf, 2 kap. 4 a §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	2 kap.
	4 a §
	Personuppgifter som behandlas i registren får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.

Denna lag träder i kraft den 1 oktober 2026.

1.14 Förslag till lag om ändring i lagen (2010:1011) om brandfarliga och explosiva varor

Härigenom föreskrivs i fråga om lagen (2010:1011) om brandfarliga och explosiva varor att det ska införas en ny paragraf, 21 e §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	21 e § *Personuppgifter som behandlas i det nationella tillståndsregistret för explosiva varor får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.*

Denna lag träder i kraft den 1 oktober 2026.

1.15 Förslag till lag om ändring i lagen (2011:725) om behörighet för lokförare

Härigenom föreskrivs i fråga om lagen (2011:725) om behörighet för lokförare

dels att 4 kap. 11 och 18 §§ ska ha följande lydelse,

dels att det ska införas två nya paragrafer, 4 kap. 11 a och 18 a §§, och närmast före 4 kap. 11 a och 18 a §§ rubriker av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
4 kap.	
11 §[1]	
Direktåtkomst till förarbevisregistret *och utlämnande av personuppgifter på medium för automatiserad behandling ur det registret* får endast medges	Direktåtkomst till förarbevisregistret får endast medges
1. den som är registrerad i förarbevisregistret när det gäller uppgifter om den registrerade själv,	
2. olycksutredande myndighet i Sverige,	
3. behörig järnvägssäkerhetsmyndighet och behörigt olycksutredande organ i annat land inom EES eller i Schweiz,	
4. Europeiska unionens järnvägsbyrå, och	
5. det järnvägsföretag eller den infrastrukturförvaltare i vars verksamhet föraren är anställd eller anlitad.	
Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om villkoren för direktåtkomst *och utlämnande av personuppgifter för automatiserad behandling*.	Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om villkoren för direktåtkomst.

[1] Senaste lydelse 2022:379.

Elektroniskt utlämnande av personuppgifter

11 a §

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

18 §

Direktåtkomst till intygsregister och utlämnande av personuppgifter *på medium för automatiserad behandling* ur sådana register får endast medges

Direktåtkomst till intygsregister och *elektroniskt* utlämnande av personuppgifter på *annat sätt än genom direktåtkomst* ur sådana register *som inte förs av det allmänna* får endast medges

1. den som är registrerad i ett intygsregister, när det gäller uppgifter om den registrerade själv i samma register,

2. tillsynsmyndigheten och olycksutredande myndighet i Sverige, samt

3. behörig järnvägssäkerhetsmyndighet och behörigt olycksutredande organ i annat land inom EES eller i Schweiz.

Regeringen meddelar föreskrifter om villkoren för direktåtkomst *och utlämnande av personuppgifter för automatiserad behandling* för sådana intygsregister som förs av det allmänna.

Regeringen meddelar föreskrifter om villkoren för direktåtkomst för sådana intygsregister som förs av det allmänna.

Elektroniskt utlämnande av personuppgifter

18 a §

Personuppgifter ur intygsregister som förs av det allmänna får lämnas ut elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt.

Denna lag träder i kraft den 1 oktober 2026.

1.16 Förslag till lagen om ändring i lagen (2012:453) om register över nationella vaccinationsprogram m.m.

Härigenom föreskrivs i fråga om lagen (2012:453) om register över nationella vaccinationsprogram m.m. att 10 § och rubriken närmast före 10 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
Utlämnande på medium för automatiserad databehandling	***Elektroniskt utlämnande av personuppgifter***
10 §	
Personuppgifter i vaccinationsregistret får lämnas ut *på medium för automatiserad databehandling endast om uppgifterna ska användas för något av de ändamål som anges i 6 §.*	Personuppgifter i vaccinationsregistret får lämnas ut *elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt.*

Denna lag träder i kraft den 1 oktober 2026.

1.17 Förslag till lag om ändring i lagen (2013:1164) om elektroniska vägtullssystem

Härigenom föreskrivs i fråga om lagen (2013:1164) om elektroniska vägtullssystem att 32 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
32 §[1]	
Personuppgifter som har erhållits enligt 28 § får endast behandlas för att identifiera ett fordon eller en ägare eller innehavare av ett fordon i syfte att ta upp eller driva in vägtullar.	
	Att personuppgifter som har erhållits enligt 28 § får lämnas ut i vissa fall framgår av offentlighets- och sekretesslagen (2009:400).

Denna lag träder i kraft den 1 oktober 2026.

[1] Senaste lydelse 2024:304.

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

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

dels att 1 § ska ha följande lydelse,

dels att det ska införas en ny paragraf, 1 a §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
1 §[1]	
Polismyndigheten får föra ett register över dna-profiler i syfte att stärka kvaliteten i den forensiska verksamheten med dna-analyser (elimineringsdatabasen) i enlighet med denna lag.	
Uppgifter i elimineringsdatabasen får endast behandlas för att upptäcka och utreda kontamineringar vid dna-analyser och hanteringen av dna-spår.	Uppgifter i elimineringsdatabasen får, *utöver vad som anges i tredje stycket*, endast behandlas för att upptäcka och utreda kontamineringar vid dna-analyser och hanteringen av dna-spår.
Begreppen dna-profil och dna-analys som används i lagen har samma betydelse som i lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område.	*Uppgifter som behandlas enligt andra stycket får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.*
	Innebörden av vissa begrepp
	1 a §
	Begreppen dna-profil och dna-analys som används i lagen har samma betydelse som i lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område.

Denna lag träder i kraft den 1 oktober 2026.

[1] Senaste lydelse 2018:1709.

1.19 Förslag till lag om ändring i lagen (2016:526) om behandling av personuppgifter i ärenden om licens för läkemedel

Härigenom föreskrivs i fråga om lagen (2016:526) om behandling av personuppgifter i ärenden om licens för läkemedel

dels att 11 § och rubriken närmast 11 § ska ha följande lydelse,

dels att det ska införas en ny paragraf, 8 a §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	8 a § *Personuppgifter som behandlas enligt 8 § får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.*
Utlämnande på medium för automatiserad behandling	***Elektroniskt utlämnande av personuppgifter***
	11 §
Får en personuppgift lämnas ut, *får det ske på medium för automatiserad behandling.*	*Personuppgifter får* lämnas ut *elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt*.

Denna lag träder i kraft den 1 oktober 2026.

1.20 Förslag till lag om ändring i spellagen (2018:1138)

Härigenom föreskrivs i fråga om spellagen (2018:1138) att det ska införas en ny paragraf, 17 kap. 4 a §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	17 kap.
	4 a §
	Personuppgifter som behandlas enligt 4 § får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.

Denna lag träder i kraft den 1 oktober 2026.

1.21 Förslag till lag om ändring i brottsdatalagen (2018:1177)

Härigenom föreskrivs i fråga om brottsdatalagen (2018:1177) att 2 kap. 4 och 22 §§ ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
2 kap.	
4 §	
Innan personuppgifter får behandlas för ett nytt ändamål ska det säkerställas att	
1. det finns en rättslig grund enligt 1 § för den nya behandlingen, och	
2. det är nödvändigt och proportionerligt att personuppgifterna behandlas för det nya ändamålet.	
I den utsträckning skyldighet att lämna uppgifter följer av lag eller förordning ska någon prövning enligt första stycket inte göras.	*Vid uppgiftslämnande som sker i överensstämmelse med* lag eller förordning ska någon prövning enligt första stycket inte göras.
22 §	
Innan personuppgifter som behandlas med stöd av denna lag behandlas för ett ändamål utanför lagens tillämpningsområde ska det säkerställas att det är nödvändigt och proportionerligt att personuppgifterna behandlas för det ändamålet.	
I den utsträckning skyldighet att lämna uppgifter följer av lag eller förordning ska någon prövning enligt första stycket inte göras.	*Vid uppgiftslämnande som sker i överensstämmelse med* lag eller förordning ska någon prövning enligt första stycket inte göras.

Denna lag träder i kraft den 1 oktober 2026.

1.22 Förslag till lag om ändring i lagen (2018:1180) om flygpassageraruppgifter i brottsbekämpningen

Härigenom föreskrivs i fråga om lagen (2018:1180) om flygpassageraruppgifter i brottsbekämpningen att 1 kap. 5 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	1 kap.
	5 §
PNR-information får endast behandlas i syfte att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller annan allvarlig brottslighet, om inte annat anges i 6 § eller 5 kap. 3 §.	
	Att PNR-information får lämnas ut i vissa fall framgår av offentlighets- och sekretesslagen (2009:400).

Denna lag träder i kraft den 1 oktober 2026.

1.23 Förslag till lag om ändring i lagen (2018:1212) om nationell läkemedelslista

Härigenom föreskrivs i fråga om lagen (2018:1212) om nationell läkemedelslista

dels att nuvarande 3 kap. 7 § ska betecknas 3 kap. 7 a §,

dels att det ska införas ny paragraf, 3 kap. 7 §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	3 kap.
	7 §
	Personuppgifter som behandlas enligt 2–5 §§ får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.

Denna lag träder i kraft den 1 oktober 2026.

1.24 Förslag till lag om ändring i vägtrafikdatalagen (2019:369)

Härigenom föreskrivs i fråga om vägtrafikdatalagen att 2 kap. 17 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	2 kap.
	17 §
Personuppgifter som behandlas enligt 3, 7, 11, 14 eller 16 § får även behandlas *när det är nödvändigt för att tillhandahålla information till*	Personuppgifter som behandlas enligt 3, 7, 11, 14 eller 16 §§ får även behandlas *för uppgiftslämnande i överensstämmelse med lag eller förordning.*
1. riksdagen eller regeringen,	
2. en annan myndighet eller en enskild, om uppgifterna lämnas med stöd av lag eller förordning, eller	
3. en utländsk myndighet, ett EU-organ eller en mellanfolklig organisation, om utlämnandet av uppgifterna sker med anledning av Sveriges medlemskap i Europeiska unionen eller i enlighet med en internationell konvention som Sverige har tillträtt eller ett av riksdagen godkänt avtal med en främmande stat eller en mellanfolklig organisation.	

Denna lag träder i kraft den 1 oktober 2026.

1.25 Förslag till lag om ändring i kustbevakningsdatalagen (2019:429)

Härigenom föreskrivs i fråga om kustbevakningsdatalagen (2019:429) att 10 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
10 §	
Personuppgifter som behandlas enligt 7 § får även behandlas *om det är nödvändigt* för *att tillhandahålla information till riksdagen och regeringen samt*, i *den utsträckning skyldigheten att lämna uppgifter följer av* lag eller förordning, *till någon annan*.	Personuppgifter som behandlas enligt 7 § får även behandlas *för uppgiftslämnande* i *överensstämmelse med* lag eller förordning.

Denna lag träder i kraft den 1 oktober 2026.

1.26 Förslag till lag om ändring i lagen (2019:508) om behandling av personuppgifter i det fördelningsanalytiska statistiksystemet för inkomster och transfereringar

Härigenom föreskrivs i fråga om lagen (2019:508) om behandling av personuppgifter i det fördelningsanalytiska statistiksystemet för inkomster och transfereringar att 5 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
5 §	
Utöver vad som anges i 4 § får Statistiska centralbyrån behandla personuppgifter om det är nödvändigt för att myndigheten ska kunna förvalta och utveckla Fasit.	
	Personuppgifter som behandlas enligt 4 § får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.

Denna lag träder i kraft den 1 oktober 2026.

1.27 Förslag till lag om ändring i lagen (2020:422) om Rättsmedicinalverkets elimineringsdatabas

Härigenom föreskrivs i fråga om lagen (2020:422) om Rättsmedicinalverkets elimineringsdatabas att 1 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
1 §	
Rättsmedicinalverket får föra ett register över dna- profiler i syfte att stärka kvaliteten i den rättsgenetiska verksamheten med dna-analyser (elimineringsdatabasen) i enlighet med denna lag.	
Uppgifter i elimineringsdatabasen får endast behandlas för att upptäcka och utreda kontamineringar av det som är föremål för dna-analys.	Uppgifter i elimineringsdatabasen får, *utöver vad som anges i tredje stycket*, endast behandlas för att upptäcka och utreda kontamineringar av det som är föremål för dna-analys. *Uppgifter som behandlas enligt andra stycket får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.*

Denna lag träder i kraft den 1 oktober 2026.

1.28 Förslag till lag om ändring i lagen (2021:319) om Transportstyrelsens olycksdatabas

Härigenom föreskrivs i fråga om lagen (2021:319) om Transportstyrelsens olycksdatabas

dels att 7 § ska ha följande lydelse,

dels att det ska införas två nya paragrafer, 7 a och 7 b §§, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
7 §	
Personuppgifter får behandlas i databasen om det är nödvändigt för 1. framställning av statistik inom trafiksäkerhetsområdet, 2. forskning som avser trafiksäkerhet, eller 3. planering, uppföljning, utvärdering eller kvalitetssäkring av trafiksäkerhetsarbete.	
Personuppgifter som behandlas enligt första stycket får behandlas även för andra ändamål, under förutsättning att behandlingen inte är oförenlig med det ändamål för vilket uppgifterna samlades in.	
	7 a § *Personuppgifter som behandlas i databasen får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.*
	7 b § *Personuppgifter som behandlas i databasen får behandlas även för andra ändamål, under förutsättning att behandlingen inte är oförenlig med det ändamål för vilket uppgifterna samlades in.*

Denna lag träder i kraft den 1 oktober 2026.

1.29 Förslag till lag om ändring i lagen (2021:626) om förarbevis för vattenskoter

Härigenom föreskrivs i fråga om lagen (2021:626) om förarbevis för vattenskoter att det ska införas en ny paragraf, 25 a §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	25 a § *Personuppgifter som behandlas enligt 25 § första stycket får även behandlas för uppgiftslämnande i överenstämmelse med lag eller förordning.*

Denna lag träder i kraft den 1 oktober 2026.

1.30 Förslag till lag om ändring i lagen (2021:1171) om behandling av personuppgifter vid Försvarsmakten

Härigenom föreskrivs i fråga om lagen (2021:1171) om behandling av personuppgifter vid Försvarsmakten att 2 kap. 9 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
2 kap.	
9 §	
Försvarsmakten får behandla personuppgifter om det är nödvändigt för diarieföring, arkivering, handläggning av ett ärende eller för att utföra annan liknande uppgift som myndigheten har.	
	Personuppgifter som behandlas enligt 2, 3 eller 5 §§ får även behandlas för uppgiftslämnande i överenstämmelse med lag eller förordning.

Denna lag träder i kraft den 1 oktober 2026.

1.31 Förslag till lag om ändring i lagen (2021:1172) om behandling av personuppgifter vid Försvarets radioanstalt

Härigenom föreskrivs i fråga om lagen (2021:1172) om behandling av personuppgifter vid Försvarets radioanstalt att det ska införas en ny paragraf, 2 kap. 8 a §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	2 kap.
	8 a §
	Personuppgifter som behandlas enligt 2, 5 eller 7 §§ får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.

Denna lag träder i kraft den 1 oktober 2026.

1.32 Förslag till lag om ändring i biobankslagen (2023:38)

Härigenom föreskrivs i fråga om biobankslagen (2023:38)
dels att 7 kap. 5 § ska ha följande lydelse,
dels att det ska införas en ny paragraf, 3 kap. 1 a § av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	3 kap.
	1 a §
	Personuppgifter som behandlas i registret får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.
	7 kap.
	5 §
PKU-registret får användas endast för de ändamål som anges i 2 § och för framställning av statistik.	PKU-registret får, *utöver vad som anges i andra stycket*, användas endast för de ändamål som anges i 2 § och för framställning av statistik.
	Personuppgifter som behandlas enligt 2 § får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.

Denna lag träder i kraft den 1 oktober 2026.

1.33 Förslag till lag om ändring i lagen (2024:488) om personuppgiftsbehandling i vissa ärenden om stöd till civilsamhället

Härigenom föreskrivs i fråga om lagen (2024:488) om personuppgiftsbehandling i vissa ärenden om stöd till civilsamhället att det ska införas en ny paragraf, 7 a §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	7 a §
	Personuppgifter som behandlas enligt 6 § får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.

Denna lag träder i kraft den 1 oktober 2026.

1.34 Förslag till lag om ändring i lagen (2024:1146) om vissa forskningsdatabaser

Härigenom föreskrivs i fråga om lagen (2024:1146) om vissa forskningsdatabaser att 3 kap. 3 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	3 kap.
	3 §
Personuppgifter och uppgifter om avlidna får, utöver vad som följer av 2 och 5 §§ samt 2 kap. 2 § första stycket 2 eller 3, *bara* lämnas ut *om det finns en skyldighet att göra det enligt* lag eller förordning.	Personuppgifter och uppgifter om avlidna får, utöver vad som följer av 2 och 5 §§ samt 2 kap. 2 § första stycket 2 eller 3, lämnas ut *i överensstämmelse med* lag eller förordning.

Denna lag träder i kraft den 1 oktober 2026.

1.35 Förslag till förordning om ändring i förordningen (1977:945) om trädgårdsväxters sundhet, sortäkthet och kvalitet

Härigenom föreskrivs i fråga om förordningen (1977:945) om trädgårdsväxters sundhet, sortäkthet och kvalitet att 3 b § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*

3 b §[1]

Personuppgifter i registret får behandlas för att göra det möjligt att spåra material som släpps ut på marknaden av leverantörer som yrkesmässigt utövar minst en av följande aktiviteter med avseende på fruktplantor och material för förökning av fruktplantor:

1. reproduktion,
2. produktion,
3. bevarande eller behandling,
4. import,
5. saluföring.

Personuppgifter i registret får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.

Denna förordning träder i kraft den 1 oktober 2026.

[1] Senaste lydelse 2016:1182.

1.36 Förslag till förordning om ändring i jaktförordningen (1987:905)

Härigenom föreskrivs i fråga om jaktförordningen (1987:905)

dels att 52 f § ska ha följande lydelse,

dels det ska införas två nya paragrafer, 52 h och 52 j §§, och närmast före 52 j § en rubrik av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
52 f §[1]	
Naturvårdsverket ska med hjälp av automatiserad behandling föra register över vilka personer som	
1. betalat viltvårdsavgift, och	
2. avlagt prov som ingår i jägarexamen.	
I ärenden om tillstånd att inneha jaktvapen ska Naturvårdsverket på begäran av Polismyndigheten lämna uppgifter om avlagt prov som ingår i jägarexamen. *Uppgifterna får lämnas ut på medium för automatiserad behandling.*	I ärenden om tillstånd att inneha jaktvapen ska Naturvårdsverket på begäran av Polismyndigheten lämna uppgifter om avlagt prov som ingår i jägarexamen.
	52 h §[2]
	Personuppgifter som behandlas i jaktkorts- och jägarexamensregistren får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.

[1] Senaste lydelse 2016:1004.
[2] Tidigare 52 h § upphävd genom 2018:380.

Elektroniskt utlämnande av personuppgifter

52 § j

Personuppgifter som behandlas i jaktkorts- och jägarexamensregistren får lämnas ut elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt.

Denna förordning träder i kraft 1 oktober 2026.

1.37 Förslag till förordning om ändring i rennäringsförordningen (1993:384)

Härigenom föreskrivs i fråga om rennäringsförordningen (1993:384) att det ska införas en ny paragraf, 13 a §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	13 a § *Personuppgifter som behandlas i företagsregistret för rennäringen får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.*

Denna förordning träder i kraft den 1 oktober 2026.

1.38 Förslag till förordning om ändring i förordningen (1993:1153) om redovisning av studier m.m. vid universitet och högskolor

Härigenom föreskrivs i fråga om förordningen (1993:1153) om redovisning av studier m.m. vid universitet och högskolor

dels att 2 kap. 6 och 6 a §§ och 4 kap. 4 § ska ha följande lydelse,

dels att rubrikerna närmast före 2 kap. 6 § och 4 kap. 4 § ska ha följande lydelse,

dels att det ska införas en ny rubrik närmast 2 kap. 6 a §, av följande lydelse,

dels att det ska införas en ny paragraf, 1 kap. 1 c §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	1 kap.
	1 c §
	Uppgifter som behandlas i studieregistret, Statistiska centralbyråns högskole- och universitetsregister och antagningsregistret enligt denna förordning får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.
	2 kap.
Utlämnande av uppgifter	***Elektroniskt utlämnande av uppgifter***
	6 §[1]
Uppgifter *på medium för automatiserad behandling får lämnas ut från en högskolas studieregister till*	Uppgifter *från högskolans studieregister får lämnas ut elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt.*
1. en annan högskola, om uppgifterna rör behörighet och underlag för urval eller studiemeriter som en student vill tillgodoräkna sig eller	

[1] Senaste lydelse 2015:133.

åberopa i samband med antagning till en utbildning eller utfärdande av examen, eller om uppgifterna behövs för utbildningssamarbete eller annan överenskommen samverkan mellan högskolorna,

2. ett lärosäte i en annan stat inom Europeiska ekonomiska samarbetsområdet eller i Schweiz under samma förutsättningar som uppgifter får lämnas ut till en högskola enligt 1,

3. Centrala studiestödsnämnden, om uppgifterna behövs för beviljande och utbetalning av studiestöd,

4. Universitets- och högskolerådet eller något annat organ som biträder högskolan med automatiserad behandling av ansökningar till en utbildning, om uppgifterna behövs för att genomföra arbetet,

5. SCB, enligt bestämmelserna i denna förordning,

6. en annan myndighet, om uppgifterna behövs för att handlägga ärenden om utfärdande av yrkeslegitimation eller meddelande av annan behörighet för ett yrke,

7. en myndighet i en annan stat inom Europeiska ekonomiska samarbetsområdet eller i Schweiz under samma förutsättningar som uppgifter får lämnas ut till svenska myndigheter enligt denna paragraf,

8. en studentkår som har sådan ställning enligt beslut av högskolan enligt 4 kap. 8 § högskolelagen (1992:1434) eller en nation som har sådan ställning enligt 4 kap. 15 § högskolelagen, om uppgifterna rör en stu-

dents registrering på kurser och behövs för att studentkåren eller nationen ska kunna bestämma om han eller hon har rätt att vara medlem i studentkåren eller nationen,

9. en student, om uppgifterna rör honom eller henne själv,

10. Vetenskapsrådet, Verket för innovationssystem, Forskningsrådet för miljö, areella näringar och samhällsbyggande samt Forskningsrådet för hälsa, arbetsliv och välfärd, om uppgifterna behövs för beviljande av medel för forskning,

11. Svenska institutet, om uppgifterna behövs för beviljande och utbetalning av stipendier, och

12. Universitetskanslersämbetet, om uppgifterna behövs för uppföljning eller för att granska hur effektivt verksamheten bedrivs vid universitet och högskolor.

Uppgiftsskyldighet

6 a §[2]

Högskolan ska utan dröjsmål till Migrationsverket lämna ut uppgift om att

1. en studieavgiftsskyldig student har antagits till en utbildning, och

2. en student som avses i 1 inte har registrerat sig på utbildningen.

Om det, utifrån de uppgifter som finns registrerade om en studieavgiftsskyldig student, finns anledning att anta att studenten har avbrutit sina studier, ska högskolan meddela Migrationsverket detta.

De uppgifter som avses i första och andra styckena får lämnas ut på medium för automatiserad behandling.

[2] Senaste lydelse 2010:595.

	4 kap.
Utlämnande av uppgifter	***Elektroniskt utlämnande av uppgifter***
	4 §[3]
Uppgifter *på medium för automatiserad behandling får lämnas ut från antagningsregistret till*	Uppgifter *från antagningsregistret får lämnas ut elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt.*
1. en högskola, om uppgifterna rör	
a) behörighet och underlag för urval eller studiemeriter som en student vill tillgodoräkna sig eller åberopa i samband med antagning till en utbildning eller utfärdande av examen,	
b) skyldighet att betala anmälningsavgift och studieavgift, och	
c) uppgift om betald anmälningsavgift och studieavgift,	
2. Centrala studiestödsnämnden, om uppgifterna behövs för beviljande och utbetalning av studiestöd,	
3. SCB, enligt bestämmelserna i denna förordning,	
4. en student, om uppgifterna rör honom eller henne själv,	
5. Svenska institutet, om uppgifterna behövs för beviljande och utbetalning av stipendier, och	
6. Säkerhetspolisen, om uppgifterna behövs för att myndigheten ska kunna fullgöra verksamhet som anges i 3 § polislagen (1984:387).	

Denna förordning träder i kraft den 1 oktober 2026.

[3] Senaste lydelse 2017:260.

1.39 Förslag till förordning om ändring i förordningen (1994:1543) om personregister över främmande staters beskickningspersonal m.m.

Härigenom föreskrivs i fråga om förordningen (1994:1543) om personregister över främmande staters beskickningspersonal m.m. att det ska införas en ny paragraf, 2 a §, och närmast före 2 a § en ny rubrik av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	Utlämnande av uppgift
	2 a §
	Uppgifterna i registret får behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.

Denna förordning träder i kraft den 1 oktober 2026.

1.40 Förslag till förordning om ändring i inskrivningsförordningen (2000:309)

Härigenom föreskrivs i fråga om inskrivningsförordningen (2000:309) att 20 c och 20 h §§ ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
20 c §[1]	
Personuppgifter som ingår i ärenderegistret får lämnas ut *på ett medium för automatiserad behandling till andra myndigheter och till en part i egna ärenden samt, om det är uppenbart att det kan ske utan risk för att enskildas personliga integritet kränks, till enskilda i andra fall.*	Personuppgifter som ingår i ärenderegistret får lämnas ut *elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt*.
20 h §[2]	
Avgifter får tas ut för utlämnande av uppgifter ur ärenderegistret som sker *på medium för automatiserad behandling.*	Avgifter får tas ut för utlämnande av uppgifter ur ärenderegistret som sker *elektroniskt på annat sätt än genom direktåtkomst*.

Lantmäteriet får meddela närmare föreskrifter om avgifter.

Denna förordning träder i kraft den 1 oktober 2026.

[1] Senaste lydelse 2011:61.
[2] Senaste lydelse 2011:61.

1.41 Förslag till förordning om ändring i utsädesförordningen (2000:1330)

Härigenom föreskrivs i fråga om utsädesförordningen (2000:1330) att 20 b § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*

20 b §[1]

Personuppgifter i registret får behandlas för att göra det möjligt att spåra material som släpps ut på marknaden av leverantörer som yrkesmässigt utövar minst en av följande aktiviteter, med avseende på utsäde av släkten och arter i bilaga 2:

1. reproduktion,
2. produktion,
3. bevarande eller behandling,
4. import,
5. saluföring.

Personuppgifter som behandlas med stöd av första stycket får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.

Denna förordning träder i kraft den 1 oktober 2026.

[1] Senaste lydelse 2020:280.

1.42 Förslag till förordning om ändring i förordningen (2006:196) om register över legitimerad hälso- och sjukvårdspersonal och personal med bevis om rätt att använda yrkestiteln undersköterska

Härigenom föreskrivs i fråga om förordning om ändring i förordningen (2006:196) om register över legitimerad hälso- och sjukvårdspersonal och personal med bevis om rätt att använda yrkestiteln undersköterska att 5 och 7 §§ och att rubriken närmast 7 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	5 §[1]
Personuppgifterna i registret får, utöver det som anges i 4 §, behandlas endast för att	
1. utöva tillsyn över hälso- och sjukvården och dess personal samt verksamhet enligt socialtjänstlagen (2001:453) och lagen (1993:387) om stöd och service till vissa funktionshindrade,	
2. lämna uppgifter till den nationella läkemedelslistan enligt lagen (2018:1212) om nationell läkemedelslista,	
3. lämna uppgifter till myndigheter och enskilda i *enlighet med det som föreskrivs i annan författning eller* avtal,	3. lämna uppgifter till myndigheter och enskilda i *överensstämmelse med lag eller förordning eller i enlighet med* avtal,
4. i samband med E-hälsomyndighetens behandling av personuppgifter enligt lagen om nationell läkemedelslista lämna uppgifter till den myndigheten för kontroll av identitet och behörighet i fråga om förskrivare, legitimerade sjuksköterskor utan behörighet att förskriva läkemedel, apotekare, receptarier och dietister,	
5. lämna uppgifter till E-hälsomyndigheten för kontroll av förskrivares identitet och behörighet vid expediering på öppenvårdsapotek av läkemedel och andra varor som förskrivits,	
6. kontrollera legitimerad hälso- och sjukvårdspersonals identitet och behörighet i samband med tjänstetillsättning och under anställning eller uppdrag,	
7. kontrollera legitimerad hälso- och sjukvårdspersonals identitet och behörighet att utfärda intyg,	

[1] Senaste lydelse 2024:283.

8. kontrollera identiteten och behörigheten för personal med bevis om rätt att använda yrkestiteln undersköterska i samband med tjänstetillsättning och under anställning eller uppdrag, och

9. framställa statistik om hälso- och sjukvård enligt lagen (2001:99) om den officiella statistiken.

Utlämnande	*Elektroniskt utlämnande av personuppgifter*
7 §	
Personuppgifterna i registret får lämnas ut *på medium för automatiserad behandling om uppgifterna skall behandlas för de ändamål som anges i 4 och 5 §§.*	Personuppgifterna i registret får lämnas ut *elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt.*

Denna förordning träder i kraft den 1 oktober 2026.

1.43 Förslag till förordning om ändring i förordningen (2007:108) om lägenhetsregister

Härigenom föreskrivs i fråga om förordningen (2007:108) om lägenhetsregister

dels att 7 § ska upphöra att gälla vid utgången av september 2026,

dels att rubriken närmast före 7 § ska utgå vid utgången av september 2026.

1.44 Förslag till förordning om ändring i förordningen (2010:1075) om brandfarliga och explosiva varor

Härigenom föreskrivs i fråga om förordningen (2010:1075) om brandfarliga och explosiva varor att 24 h § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
24 h §[1]	
Utlämnande av uppgifter från det nationella tillståndsregistret för explosiva varor får *göras på medium för automatiserad behandling.*	*Uppgifter* från det nationella tillståndsregistret för explosiva varor får *lämnas ut elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt.*

Denna förordning träder i kraft den 1 oktober 2026.

[1] Senaste lydelse 2024:479.

1.45 Förslag till förordning om ändring i förordningen (2011:58) om behandling av personuppgifter i Lantmäteriets databas för arkiverade handlingar

Härigenom föreskrivs i fråga om förordningen (2011:58) om behandling av personuppgifter i Lantmäteriets databas för arkiverade handlingar

dels att det ska införas en ny paragraf, 10 a §, av följande lydelse,

dels att 10 § och rubriken närmast 10 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
Direktåtkomst och *utlämnande på medium för automatiserad behandling*	**Direktåtkomst och *annat elektroniskt utlämnande***
10 §	
Direktåtkomst till personuppgifter i databasen får medges endast för sådana ändamål som anges i 4 §. *Detsamma gäller utlämnande av personuppgifter på medium för automatiserad behandling.*	Direktåtkomst till personuppgifter i databasen får medges endast för sådana ändamål som anges i 4 §.
	10 a §
	Personuppgifter i databasen får lämnas ut elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt.

Denna förordning träder i kraft den 1 oktober 2026.

1.46 Förslag till förordning om ändring i förordningen (2011:116) om register hos Socialstyrelsen över läkemedel som lämnats ut från apotek i Jämtlands län

Härigenom föreskrivs i fråga om förordningen (2011:116) om register hos Socialstyrelsen över läkemedel som lämnats ut från apotek i Jämtlands län att 3 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
3 §	
Personuppgifter i registret får behandlas för epidemiologiska undersökningar, forskning och framställning av statistik inom hälso- och sjukvårdsområdet.	
	Personuppgifter som behandlas enligt första stycket får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.

Denna förordning träder i kraft den 1 oktober 2026.

1.47 Förslag till förordning om ändring i förordning (2011:268) om lärar- och förskollärarregister

Härigenom föreskrivs i fråga om förordningen (2011:268) om lärar- och förskollärarregister att 9 § och rubriken närmast före 9 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
Utlämnande på medium för automatiserad databehandling	***Elektroniskt utlämnande av personuppgifter***
10 §	
Personuppgifterna i registret får lämnas ut *på medium för automatiserad behandling om uppgifterna ska behandlas för de ändamål som anges i 5 och 6 §§.*	Personuppgifterna i registret får lämnas ut *elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt.*

Denna förordning träder i kraft den 1 oktober 2026.

1.48 Förslag till förordning om ändring i förordning (2011:728) om behörighet för lokförare

Härigenom föreskrivs i fråga om förordningen (2011:728) om behörighet för lokförare att 7 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	7 §
Direktåtkomst till förarbevisregistret och intygsregister samt utlämnande av personuppgifter ur sådana register *på medium för automatiserad behandling* får endast medges om direktåtkomst eller utlämnande i varje enskilt fall föregås av en motiverad begäran.	Direktåtkomst till förarbevisregistret och intygsregister samt *elektroniskt* utlämnande av personuppgifter *på annat sätt än genom direktåtkomst* ur *intygsregister som inte förs av det allmänna* får endast medges om direktåtkomst eller utlämnande i varje enskilt fall föregås av en motiverad begäran.

Denna förordning träder i kraft den 1 oktober 2026.

1.49 Förslag till förordning om ändring i förordningen (2013:413) om kosmetiska produkter

Härigenom föreskrivs i fråga om förordningen (2013:413) om kosmetiska produkter att det ska införas en ny paragraf, 5 a §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	5 a §
	Personuppgifter som behandlas enligt 5 § får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.

Denna förordning träder i kraft den 1 oktober 2026.

1.50 Förslag till förordning om ändring i förordningen (2016:1316) med kompletterande bestämmelser till EU:s marknadsmissbruksförordning och EU:s förordning om referensvärden

Härigenom föreskrivs i fråga om förordningen (2016:1316) med kompletterande bestämmelser till EU:s marknadsmissbruksförordning och EU:s förordning om referensvärden att det ska införas en ny paragraf, 4 a §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	4 a § *Personuppgifter som behandlas i utredningsregistret får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.*

Denna förordning träder i kraft den 1 oktober 2026.

1.51 Förslag till förordning om ändring i förordning (2018:307) om donationsregister hos Socialstyrelsen

Härigenom föreskrivs i fråga om förordning (2018:307) om donationsregister hos Socialstyrelsen att 4 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*

4 §

Uppgifter i donationsregistret får behandlas för att förse sådana sjukhus och andra enheter där ingrepp enligt lagen (1995:831) om transplantation m.m. får utföras med information om vilken inställning en person har till donation av organ eller vävnader efter döden.

Uppgifter som behandlas enligt första stycket får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.

Denna förordning träder i kraft den 1 oktober 2026.

1.52 Förslag till förordning om ändring i avfallsförordningen (2020:614)

Härigenom föreskrivs i fråga om avfallsförordningen (2020:614) att det ska införas en ny paragraf, 6 kap. 10 a §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	6 kap.
	10 a §
	Uppgifter som behandlas i avfallsregistret får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.

Denna förordning träder i kraft den 1 oktober 2026.

1.53 Förslag till förordning om ändring i förordning (2020:833) om skolenhetsregister

Härigenom föreskrivs i fråga om förordningen (2020:833) om skolenhetsregister 15 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	15 §
Bestämmelserna i denna förordning inskränker inte myndigheters skyldigheter enligt vad som föreskrivs om allmänna handlingars offentlighet i tryckfrihetsförordningen eller i offentlighets- och sekretesslagen (2009:400).	*Personuppgifter som behandlas i skolenhetsregistret får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.*

Denna förordning träder i kraft den 1 oktober 2026.

1.54 Förslag till förordning om ändring i förordningen (2021:1129) om register över förordnade läkemedel för behandling av djur

Härigenom föreskrivs beträffande förordningen (2021:1129) om register över förordnade läkemedel för behandling av djur att det ska införas en ny paragraf, 6 a §, av följande lydelse

Nuvarande lydelse	*Föreslagen lydelse*
	6 a §
	Personuppgifter som behandlas i registret får behandlas även för uppgiftslämnande i överenstämmelse med lag eller förordning.

Denna förordning träder i kraft den 1 oktober 2026.

2 Utredningens uppdrag och arbete

2.1 Uppdraget

Regeringen beslutade den 19 oktober 2023 att ge en särskild utredare i uppdrag att överväga och föreslå förbättrade möjligheter att utbyta information om enskilda inom och mellan myndigheter och andra organ som enligt offentlighets- och sekretesslagen (2009:400), OSL, jämställs med myndigheter (bilaga 1).

Uppdraget avsåg att kartlägga behovet av att myndigheter får förbättrade möjligheter att utbyta information med varandra i syfte att särskilt förhindra, förebygga, upptäcka, utreda och ingripa mot fusk, felaktiga utbetalningar, regelöverträdelser och brottslighet, att analysera och ta ställning till hur behovet av att utbyta sekretessbelagd information kan tillgodoses, att särskilt överväga och lämna förslag på en generell bestämmelse som gör det möjligt att på ett effektivt sätt lämna uppgifter som omfattas av sekretess till skydd för enskilda till en annan myndighet, såväl på begäran som på eget initiativ, att analysera och ta ställning till hur behovet av att utbyta offentlig information kan tillgodoses, att särskilt överväga och lämna förslag på en bestämmelse som i större utsträckning gör det möjligt att på eget initiativ lämna ut offentliga uppgifter till en annan myndighet samt att göra en översyn, i den utsträckning det behövs, av myndigheternas registerförfattningar för att möjliggöra att de förslag som lämnas tjänar sitt syfte och kan tillämpas på ett ändamålsenligt sätt.

Genom tilläggsdirektiv den 19 september 2024 (bilaga 2) förlängdes utredningstiden till den 28 april 2025.

2.2 Delbetänkandet

I september 2024 redovisade vi vårt delbetänkande *Ökat informationsutbyte mellan myndigheter. Behov och föreslagna förändringar* (SOU 2024:63).

I delbetänkandet förslås att det ska införas en generell sekretessbrytande bestämmelse i offentlighets- och sekretesslagen. Delbetänkandet innehåller också bl.a. en redovisning av genomförd kartläggning av behovet av att myndigheter får förbättrade möjligheter att utbyta information med varandra i syfte att särskilt förhindra, förebygga, upptäcka, utreda och ingripa mot fusk, felaktiga utbetalningar, regelöverträdelser och brottslighet.

2.3 Utredningens arbete med slutbetänkandet

Utredningens arbete har bedrivits på sedvanligt sätt tillsammans med sakkunniga och experter. Vi har haft tre protokollförda sammanträden och därutöver löpande kontakt med enskilda sakkunniga och experter i vissa frågor.

Vi har haft särskild kontakt med Skolsäkerhetsutredningen (U 2022:04), 2024 års studiestödsdatautredning (U 2024:02), Utredningen om förbättrat informationsutbyte och en mer ändamålsenlig lagreglering för den arbetsmarknadspolitiska verksamheten (A 2023:01), Utredningen om Säkerhetspolisens informationshantering (Ju 2023:02) och Utredningen om skärpta krav på hederligt levnadssätt och ökade möjligheter till återkallelse av uppehållstillstånd (Ju 2023:25). Härutöver har vi samrått med Integritetsskyddsmyndigheten, IMY.

Som nämns ovan har vi haft i uppdrag att analysera myndigheternas behov av att lämna ut offentliga uppgifter på eget initiativ. Vid utförandet av detta uppdrag har vi huvudsakligen använt oss av den tidigare genomförda kartläggningen.

I våra texter hänvisar vi på många ställen till delbetänkandet (SOU 2024:63).

2.4 Avgränsningar

I enlighet med det uppdrag vi har haft har vi analyserat myndigheternas behov av att lämna ut offentliga uppgifter på eget initiativ. I kapitel 4 föreslår vi att det i offentlighets- och sekretesslagen ska införas en bestämmelse som innebär att myndigheterna får lämna ut uppgifter som inte är sekretessbelagda till andra myndigheter på eget initiativ under vissa förutsättningar. Som föreskrivs i direktiven har vi även analyserat behovet av att se över myndigheternas registerförfattningar för att de bestämmelser om utökat informationsutbyte som vi föreslår ska kunna tillämpas på ett ändamålsenligt sätt. I kapitel 5 föreslår vi ändringar i myndigheternas registerförfattningar.

Det har inte legat inom uppdraget för den här utredningen att överväga hur ett ökat informationsutbyte praktiskt bör hanteras, dvs. frågor om utvecklingen av interoperabla lösningar för den offentliga förvaltningens datadelning, samverkan, digital infrastruktur etc.

2.5 Utredningens begreppsanvändning

2.5.1 Sekretessbelagd uppgift och annars sekretessbelagd uppgift

I 3 kap. 1 § OSL, definieras begreppet ”sekretessbelagd uppgift” som en sekretessreglerad uppgift för vilken sekretess gäller i ett enskilt fall.

Begreppet förekommer i ett stort antal bestämmelser i OSL. I 6 kap. 5 § OSL t.ex. sägs att en myndighet ska på begäran av en annan myndighet lämna uppgift som den förfogar över, om inte uppgiften är sekretessbelagd eller det skulle hindra arbetets behöriga gång. Enligt lagkommentaren till 6 kap. 5 § OSL innebär bestämmelsen att om en sekretessbrytande bestämmelse är tillämplig på en uppgift är en myndighet skyldig att lämna uppgiften till en myndighet som begär det. Den sekretessbrytande bestämmelsen innebär ju – enligt lagkommentaren – att uppgiften i just den situationen inte är sekretessbelagd.[1]

[1] Lenberg m.fl., *Offentlighets- och sekretesslagen (2009:400)*, 22 november 2023, JUNO, kommentaren till 6 kap. 5 §. Se även t.ex. prop. 2020/21:163, *Förebyggande av våld i nära relationer*, s. 44, 64 och 65.

Innebörden av det som sägs i lagkommentaren är alltså att en uppgift som får lämnas ut med stöd av en sekretessbrytande bestämmelse inte är en ”sekretessbelagd uppgift”. Att det förhåller sig på det sättet följer av definitionen av begreppet sekretessbelagd uppgift. Uppgiften får lämnas ut och det gäller därmed inte sekretess för den i det enskilda fallet.

I våra direktiv sägs att det för att en uppgift ska kunna lämnas ut enligt 6 kap. 5 § OSL krävs att uppgiften inte är sekretessreglerad, att det finns ett undantag från sekretess, att uppgiften kan lämnas ut efter en sekretessprövning eller att det finns en sekretessbrytande bestämmelse som är tillämplig. Inte i något av dessa fall gäller sekretess för uppgiften och följaktligen är uppgiften inte sekretessbelagd. Det som sägs i direktiven står alltså i överensstämmelse med hur definitionen av begreppet sekretessbelagd uppgift har utformats.

Utgår man ifrån det ovan sagda är alltså en uppgift sekretessbelagd om det råder sekretess för den i det enskilda fallet. Motsatsvis borde därmed gälla att en uppgift inte ska betraktas som sekretessbelagd om det inte råder sekretess för den i det enskilda fallet, oavsett om detta beror på att den inte är sekretessreglerad, att det finns ett undantag från sekretess, att uppgiften kan lämnas ut efter en sekretessprövning eller att det finns en sekretessbrytande bestämmelse som är tillämplig.[2]

I våra direktiv finns emellertid flera uttalanden av innebörden att myndigheter får utbyta sekretessbelagda uppgifter med varandra med stöd av en sekretessbrytande bestämmelse. Liknande skrivningar förekommer även i många andra sammanhang, t.ex. i utredningar och i propositioner där sekretessfrågor behandlas.[3]

Som nämns ovan definieras begreppet sekretessbelagd uppgift som en uppgift för vilken sekretess gäller i ett enskilt fall. Om myndigheter får utbyta uppgifter med varandra med stöd av en sekretessbrytande bestämmelse gäller inte sekretess för uppgifterna just i de fallen och de kan därmed inte vara sekretessbelagda. Att hävda t.ex. att myndigheter får utbyta sekretessbelagda uppgifter med varandra med stöd av en sekretessbrytande bestämmelse framstår därför som

[2] Inte heller uppgifter som lämnas ut med förbehåll t.ex. med stöd av 10 kap. 14 § OSL eller efter av dispens av regeringen enligt exempelvis 28 kap. 16 § ska såvitt vi kan bedöma betraktas som sekretessbelagda, eftersom sekretess inte gäller för uppgifterna just i de fallen.
[3] Se bl.a. prop. 2004/05:83, *Sekretess hos den kommission och det råd som har inrättats med anledning av naturkatastrofen i Asien*, s. 15 och betänkandet *Ett förstärkt lagstöd för utlämnande av sekretesskyddade uppgifter till utlandet* (SOU 2022:16) s. 30.

inkonsekvent om man ser till hur begreppet sekretessbelagda uppgifter har definierats.

Det är troligt att detta sätt att uttrycka saken hänger ihop med att begreppet ”sekretessbrytande bestämmelse” definieras i 3 kap. 1 § OSL som en bestämmelse som innebär att en sekretessbelagd uppgift får lämnas ut under vissa förutsättningar. I lagtexten sägs alltså att ”sekretessbelagda uppgifter får lämnas ut”.[4]

Oaktat lagtextens utformning bör emellertid inte detta föranleda den slutsatsen att begreppet ”sekretessbrytande bestämmelse” ska förstås på något annat sätt än vad som följer av definitionen av detta begrepp. Det är också med den innebörden vi kommer att använda oss av begreppet *sekretessbelagda uppgifter* i betänkandet.

Av det som sagts ovan följer att en sekretessbrytande bestämmelse inte medger att sekretessbelagda uppgifter lämnas ut. Det är mera korrekt att beskriva en sekretessbrytande bestämmelse som en bestämmelse som medger att *annars sekretessbelagda* uppgifter lämnas ut. För att inte skapa oklarheter kommer vi i betänkandet formulera oss i enlighet med detta.

2.5.2 Offentliga uppgifter och uppgifter som inte är sekretessbelagda

I vårt uppdrag i denna del ingår att mot bakgrund av genomförd kartläggning att analysera och ta ställning till hur behovet av att utbyta offentliga uppgifter kan tillgodoses, särskilt överväga och lämna förslag på en bestämmelse som i större utsträckning gör det möjligt att på eget initiativ lämna ut offentliga uppgifter till en annan myndighet, och lämna nödvändiga författningsförslag.

Begreppet ”offentliga uppgifter” definieras inte i offentlighets- och sekretesslagen. Enligt våra direktiv ska emellertid med ”offentliga uppgifter” förstås sådana uppgifter som träffas av 6 kap. 5 § OSL, dvs. uppgifter som inte är sekretessbelagda. Det innebär att med offentliga uppgifter enligt våra direktiv avses uppgifter som inte är sekretessreglerade, uppgifter som omfattas av ett undantag från sekretess, uppgifter som får lämnas ut efter en sekretessprövning och uppgifter som får lämnas ut med stöd av en sekretessbrytande bestämmelse.

[4] Det finns även andra bestämmelser i OSL där likande uttryckssätt används. I 10 kap. 27 § OSL sägs t.ex. att sekretessbelagd uppgift får lämnas till en myndighet under vissa förutsättningar.

Offentliga uppgifter är alltså enligt direktiven samma sak som uppgifter som inte är sekretessbelagda.

Eftersom uttrycket offentliga uppgifter har en särskild allmänspråklig betydelse kommer vi i detta betänkande huvudsakligen använda oss av begreppen *uppgifter som inte är sekretessbelagda* eller *uppgifter som får lämnas ut*. (Se avsnitt 4.3.1.)

2.5.3 Undantag från sekretess

Någon definition av begreppet ”undantag från sekretess” finns inte i offentlighets- och sekretesslagen. Som just konstaterats avses i våra direktiv med begreppet ”offentliga uppgifter” bl.a. uppgifter som omfattas av undantag från sekretess.

I offentlighets- och sekretesslagen finns i de kapitel som innehåller materiella sekretessbestämmelser i regel också bestämmelser under rubrikerna ”sekretessbrytande bestämmelser” respektive ”undantag från sekretess”. Det görs alltså i offentlighets- och sekretesslagen en åtskillnad mellan sekretessbrytande bestämmelser och undantag från sekretess. Bestämmelserna i 25 kap. OSL kan tjäna som exempel.

I 25 kap. 1 § första stycket första meningen anges att sekretess gäller inom hälso- och sjukvården för uppgift om en enskilds hälsotillstånd eller andra personliga förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till denne lider men. I 25 kap. 10 §, som har rubriken ”undantag från sekretess”, sägs att sekretessen enligt bl.a. 1 § inte gäller i vissa sammanhang bl.a. i beslut i ärende enligt lagstiftningen om psykiatrisk tvångsvård eller rättspsykiatrisk vård, om beslutet avser frihetsberövande åtgärd (p. 1). I 25 kap. 11 §, som har rubriken ”sekretessbrytande bestämmelse”, föreskrivs att sekretessen enligt 1 § inte hindrar att uppgift lämnas från en myndighet som bedriver verksamhet som avses i 1 § i en kommun till en annan sådan myndighet i samma kommun (p. 1).

Sekretessgenombrottet enligt bestämmelsen om undantag från sekretess är brett och gäller i förhållande till alla myndigheter och enskilda. Vad avser den sekretessbrytande bestämmelsen är sekretessgenombrottet mer begränsat. Man skulle mot denna bakgrund kunna

anta att detta är skillnaden mellan sekretessbrytande bestämmelser och undantag från sekretess.

Lagstiftaren har emellertid inte varit helt konsekvent i detta avseende. I 110 kap. socialförsäkringsbalken t.ex. finns flera bestämmelser under rubriken ”undantag från sekretess” (39–42 a §§) som i princip är utformade som sekretessbrytande bestämmelser. I 40 § t.ex. föreskrivs att sekretess inte hindrar att allmän förvaltningsdomstol på begäran får lämna ut uppgifter som avses i 39 § till en arbetslöshetskassa, om uppgiften behövs för samordning med ersättning därifrån.

En sekretessbrytande bestämmelse utgör naturligtvis också ett undantag från sekretess. Och ett undantag från sekretess utgör en sekretessbrytande bestämmelse i den meningen att den innebär att annars sekretessbelagda uppgifter får lämnas ut i vissa situationer. Det förefaller alltså inte vara möjligt att på ett konsekvent sätt upprätthålla någon åtskillnad mellan sekretessbrytande bestämmelser och undantag från sekretess.

Som nämns ovan kommer vi i detta betänkande huvudsakligen använda oss av begreppen *uppgifter som inte är sekretessbelagda* eller *uppgifter som får lämnas ut* när vi avser uppgifter som är offentliga i den mening som avses i direktiven. Det saknar betydelse varför uppgifterna inte är sekretessbelagda eller får lämnas ut. Det finns därmed ingen mening med att försöka göra någon åtskillnad mellan sekretessbrytande bestämmelser och undantag från sekretess i detta sammanhang. För enkelhetens skulle kommer vi emellertid i det följande att använda oss av båda dessa begrepp.

2.5.4 Myndighet

Om inte annat uttryckligen anges eller framgår av sammanhanget avses med begreppet myndighet när det används i betänkandet alla myndigheter och övriga organ som vid tillämpningen av offentlighets- och sekretesslagen ska jämställas med myndigheter enligt 2 kap. OSL. Det innebär att med myndighet avses i betänkandet statliga myndigheter, kommuner, regioner och vissa andra aktörer som ska tillämpa offentlighets- och sekretesslagen. Vidare avses med begreppet även sådana verksamhetsgrenar inom en myndighet när de är att betrakta som självständiga i förhållande till varandra enligt 8 kap. 2 § OSL.

Det innebär t.ex. att det inom en kommun kan finnas flera myndigheter, så som begreppet används här.

2.5.5 Kompletterande dataskyddsreglering

I vårt uppdrag i denna del ingår att göra en översyn, i den utsträckning det behövs, av myndigheternas registerförfattningar för att möjliggöra att de förslag som lämnas tjänar sitt syfte och kan tillämpas på ett ändamålsenligt sätt.

Med registerförfattningar avses enligt direktiven författningar som innehåller mer sektorsspecifika bestämmelser om personuppgiftsbehandlingen vid myndigheter och som kompletterar den allmänna dataskyddsregleringen. I direktiven konstateras också att registerförfattningarnas karaktär varierar.

Kompletterande dataskyddsreglering, det som i direktiven benämns registerförfattningar, har till skillnad från generella bestämmelser om dataskydd, ett begränsat tillämpningsområde och avser normalt personuppgiftsbehandling inom en viss verksamhet, vid en viss myndighet eller inom en viss sektor. De sektorsspecifika bestämmelserna förhåller sig alltid till den allmänna regleringen och kan sägas fylla ut denna. Kompletterande reglering kan även innehålla undantag från de allmänna bestämmelserna, i den mån sådana undantag är tillåtna enligt överordnad reglering.

Sektorsspecifika dataskyddsbestämmelser behöver dock inte finnas i en egen författning, utan kan utgöra en mindre del av lagstiftning som i huvudsak omfattar materiell och/eller processuell reglering av en viss verksamhet.

Vi har därför valt att använda oss av det mer rättvisande begreppet kompletterande dataskyddsreglering, i stället för begreppet registerförfattning.

3 Den allmänna dataskyddsregleringen och uppgiftsutbyte mellan myndigheter

3.1 Inledning

För att säkerställa att EU-lagstiftningen ger samma skydd för alla medborgare inom hela EU har bestämmelser som finns i en EU-förordning företräde framför nationella lagar.[1] Det innebär att den primära regleringen av svenska myndigheters personuppgiftsbehandling i dag finns i dataskyddsförordningen[2]. Bestämmelserna i dataskyddsförordningen är alltså direkt tillämpliga och ska tillämpas av nästan alla svenska myndigheter precis som det vore en svensk författning. De situationer där personuppgiftsbehandling faller utanför dataskyddsförordningens tillämpningsområde är få; viss behandling av personuppgifter inom bl.a. Försvarsmakten och vid brottsbekämpande myndigheter regleras inte av dataskyddsförordningen, men av regelverk som i stora drag motsvarar den.

Informationshantering i form av utlämnande, överföring och mottagande av personuppgifter utgör personuppgiftsbehandling enligt dataskyddsförordningen (artikel 4.2). Dataskyddsförordningen ska tillämpas på sådan behandling av personuppgifter som helt eller delvis företas på automatisk väg samt på annan behandling än automatisk av personuppgifter som ingår i eller kommer att ingå i ett register (artikel 2.1). Det innebär att dataskyddsförordningens bestämmelser inte enbart är tillämpliga när myndigheter utbyter uppgifter digitalt,

[1] Se bl.a. EU-domstolens dom den 15 juli 1964, Flaminio Costa mot E.N.E.L., mål 6/64.
[2] 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).

dvs med dator, utan även vid viss analog hantering (se även avsnitt 5.4.5).

Eftersom nästan all informationshantering i dag är digitaliserad kan man utgå från att dataskyddsförordningen i regel är tillämplig vid sådant informationsutbyte mellan myndigheter som omfattar personuppgifter. Det innebär bl.a. att det måste finnas en rättslig grund för den behandling som informationsutbytet innebär, att utbytet inte får avse fler uppgifter än vad som är nödvändigt med hänsyn till ändamålet med utbytet och att tekniska och organisatoriska åtgärder måste vidtas av de inblandade myndigheterna i syfte att minska de risker för den personliga integriteten som behandlingen innebär. Detta framgår bl.a. av artikel 5.1 i dataskyddförordningen där de grundläggande principerna för all personuppgiftsbehandling ställs upp.

Dataskyddsförordningen omfattar inga krav på att myndigheters informationsutbyte ska regleras på något särskilt sätt i den nationella rätten. Däremot finns det en mängd olika bestämmelser både i förordningen och i annan lagstiftning som aktualiseras vid sådant informationsutbyte. I kapitel 3 i vårt delbetänkande SOU 2024:63, *Ökat informationsutbyte mellan myndigheter. Behov och föreslagna förändringar* behandlade vi vissa generella normer om myndigheters informationshantering, personlig integritet, dataskydd och sekretess. I detta kapitel lämnas i stället en samlad redogörelse över bestämmelser i den allmänna dataskyddsregleringen, dvs. främst dataskyddsförordningen, som särskilt aktualiseras vid informationsutbyte mellan myndigheter. En viss upprepning av delbetänkandet är nödvändig för fullständigheten i detta sammanhang. I vissa fall kommer redogörelsen dessutom kompletteras med exempel på regeringens bedömning av hur svensk rätt förhåller sig till dataskyddsförordningens bestämmelser, för att sätta dessa i sitt sammanhang.

3.2 Principen om ändamålsbegränsning (finalitetsprincipen)

3.2.1 Kravet på en rättslig grund

För att behandling av personuppgifter över huvud taget ska vara laglig enligt dataskyddsförordningen krävs att något av de villkor som anges i artikel 6.1 i förordningen är uppfyllda. Det innebär att en behandling är otillåten och olaglig om den inte har en rättslig

grund enligt dataskyddsförordningen. De rättsliga grunder som i huvudsak aktualiseras för myndigheter finns i artikel 6.1 c och e och är rättslig förpliktelse, uppgift av allmänt intresse och myndighetsutövning. De rättsliga grunderna som anges i artikel 6.1 c och e måste vara fastställda i den nationella rätten eller unionsrätten, vilket framgår av artikel 6.3. Det är alltså primärt lagstiftaren som genom lagstiftning beslutar om de rättsliga grunderna för myndigheternas personuppgiftsbehandling (jfr skäl 47 till dataskyddsförordningen). I svensk rätt framgår detta förhållande av 2 kap. 1 och 2 §§ lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning, dataskyddslagen, vari det görs hänvisningar till lag, författning och beslut som meddelats med stöd av lag eller författning som rättsliga grunder för personuppgiftsbehandling.

Personuppgiftsbehandling måste inte enbart ha en rättslig grund utan den måste även vara nödvändig, t.ex. för att en myndighet ska kunna utföra myndighetsutövning eller utföra en uppgift av allmänt intresse. Det unionsrättsliga begreppet nödvändigt har dock inte samma strikta innebörd som det svenska ordet nödvändigt, dvs. att någonting absolut fordras eller inte kan underlåtas. Trots att en arbetsuppgift skulle kunna utföras utan att personuppgifter behandlas på ett visst sätt så kan behandlingen anses nödvändig redan om den innebär effektivitetsvinster.[3] Regeringen har dessutom uttalat att i dagsläget bör det mer eller mindre regelmässigt anses vara nödvändigt att använda tekniska hjälpmedel och därmed behandla personuppgifter på automatisk väg, eftersom en manuell informationshantering inte utgör ett realistiskt alternativ för vare sig myndigheter eller företag.[4]

För att uppgifter ska få utbytas mellan myndigheter krävs dock inte bara att utbytet sker i enlighet de dataskyddsrättsliga bestämmelserna. Svenska myndigheters utbyte av uppgifter måste även vara förenligt med tillämpliga bestämmelser om sekretess.

Sekretessbrytande bestämmelser som anger att uppgifter får eller ska lämnas ut utgör även den rättsliga grunden för behandling av personuppgifter genom utlämnande. De dataskyddsrättsliga och sekretessrättsliga regelverken samspelar alltså på så sätt att om sekretess hindrar att en uppgift lämnas till en annan myndighet så finns

[3] EU-domstolens avgörande den 16 december 2008 i mål C-524/06, Heinz Huber mot Bundesrepublik Deutschland och prop. 2017/18:105, *Ny dataskyddslag*, s. 46 och 47.
[4] Prop. 2017/18:105, *Ny dataskyddslag*, s. 47.

det normalt inte heller någon rättslig grund för utlämnandet. När det däremot finns en sekretessbrytande bestämmelse som medför att uppgiften inte är sekretessbelagd i förhållande till den mottagande myndigheten utgör denna bestämmelse en rättslig grund för den personuppgiftsbehandling som utlämnandet omfattar (se vidare avsnitten 4.6 och 5.4).

3.2.2 Finalitetsprincipen

Allmänt

Ett uppgiftslämnande från en myndighet till en annan utgör ofta en vidarebehandling av uppgifter som den utlämnande myndigheten tidigare har samlat in för helt andra syften än att lämna ut till en annan myndighet. Typisk sett rör det sig om att uppgifter, som den utlämnande myndigheten ursprungligen har samlat in och behandlar i syfte att utföra sin verksamhet, lämnas till en annan myndighet för att den mottagande myndigheten ska kunna utföra en helt annan verksamhet. Ett utlämnande av personuppgifter mellan myndigheter aktualiserar därför den s.k. finalitetsprincipen, i dataskyddsförordningen benämnd principen om ändamålsbegränsning. Finalitetsprincipen kommer till uttryck i dataskyddsförordningen genom att det i artikel 5.1 b bl.a. anges att personuppgifter ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål.

Om en vidarebehandling av redan insamlade personuppgifter inte omfattas av de ursprungliga ändamålen måste alltså den personuppgiftsansvariga myndigheten göra en bedömning av om det nya ändamålet, dvs. vidarebehandlingen, är förenligt med de ursprungliga ändamålen. I dataskyddsförordningen föreskrivs det i artikel 6.4 hur prövningen av om en vidarebehandling är förenlig med insamlingsändamålet som utgångspunkt ska gå till. Vid prövningen ska bl.a. kopplingar mellan de ändamål för vilka personuppgifterna har samlats in och ändamålen med den avsedda ytterligare behandlingen beaktas. Det sammanhang inom vilket personuppgifterna har samlats in, särskilt förhållandet mellan de registrerade och den personuppgiftsansvarige, samt personuppgifternas art, är också förhållanden som ska beaktas. I enlighet med den s.k. ansvarsprincipen, som framgår av artikel 5.2 i dataskyddsförordningen, är det den personuppgifts-

ansvariga som ska göra den prövningen. Som en generell utgångspunkt bör dock ett utlämnande av en uppgift till en annan myndighet, i syfte att uppgiften ska användas i en helt annan verksamhet än den som den samlades in till, utgöra en behandling som inte är förenlig med insamlingsändamålet.

Myndigheters vidarebehandling för oförenliga ändamål

Som vi nämnt ovan är det lagstiftarens sak att genom lagstiftning tillhandahålla den rättsliga grunden för myndigheters behandling av personuppgifter. Myndigheter är därmed inte på samma sätt som enskilda aktörer fria att behandla personuppgifter på flera olika rättsliga grunder. För viss personuppgiftsbehandling som i huvudsak myndigheter utför finns det emellertid även särskilda bestämmelser som tillåter vidarebehandling för nya ändamål som inte är förenliga med insamlingsändamålet. Trots att myndigheters rättsliga möjligheter till personuppgiftsbehandling är mer begränsad än andra aktörers, så finns det alltså även undantag som gör att myndigheter i vissa avseenden har större möjligheter än t.ex. enskilda att vidarebehandla uppgifter.

Om en vidarebehandling är nödvändig för att fullgöra en uppgift av allmänt intresse, eller som ett led i myndighetsutövning som den personuppgiftsansvarige har fått i uppgift att utföra, kan medlemsstaternas nationella rätt fastställa för vilka uppgifter och syften ytterligare behandling bör betraktas som förenlig och laglig. Om vidarebehandlingen grundar sig på unionsrätten eller på medlemsstaternas nationella rätt som utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle i syfte att säkerställa i synnerhet viktiga mål av allmänt intresse, bör den personuppgiftsansvarige dessutom tillåtas att behandla personuppgifterna ytterligare, oavsett om detta är förenligt med ändamålen eller inte. Detta framgår av skäl 50 till dataskyddsförordningen.

Dataskyddsförordningen ger därmed utrymme för att i nationell rätt föreskriva att ytterligare behandling av personuppgifter får ske, även om vidarebehandlingen inte är förenlig med de eller det ändamål för vilket uppgifterna samlades in. Här kan även nämnas att regeringen har uttalat att det utgör ett viktigt allmänt intresse att svenska myndigheter kan utöva myndighetsutövning och annan verksamhet som

faller inom ramen för deras befogenheter på ett korrekt, effektivt och rättssäkert sätt.[5] Det innebär att vidarebehandling av personuppgifter genom informationsutbyte mellan myndigheter, som syftar till att en eller flera myndigheters verksamhet ska kunna utövas på ett korrekt, effektivt och rättssäkert sätt, uppfyller förutsättningarna i skäl 50.

I svensk rätt regleras myndigheters informationsutbyte huvudsakligen genom bestämmelserna i offentlighets- och sekretesslagen (se avsnitt 5.4). Bestämmelser som innebär att uppgifter som har samlats in för ett ändamål i en verksamhet får eller ska behandlas för ett annat ändamål i en annan verksamhet kan vara uppgiftsskyldigheter som regleras utanför offentlighets- och sekretesslagen (dvs. att uppgifter *ska* vidarebehandlas genom utlämnande till en annan myndighet) eller sekretessbrytande bestämmelser i offentlighets- och sekretesslagen (dvs. att uppgifter *får* vidarebehandlas genom utlämnande till en annan myndighet). Sådana bestämmelser kan i vissa fall utgöra en tillämpning av finalitetsprincipen, dvs. lagstiftaren har gjort bedömningen att den tillkommande behandlingen är förenlig med insamlingsändamålet. I de flesta fall bör dock bestämmelser om myndigheters informationsutbyte utgöra undantag från principen om att uppgifter inte får vidarebehandlas för något ändamål som är oförenligt med insamlingsändamålet.[6] Genom att införa en sekretessbrytande bestämmelse eller en uppgiftsskyldighet får lagstiftaren alltså uppfattas ha tagit ställning till att vidarebehandling genom utlämnande är nödvändigt och proportionerligt för att säkerställa ett viktigt mål av allmänt intresse.

Sekretessbrytande bestämmelser och uppgiftsskyldigheter i en dataskyddsrättslig kontext

Regeringen har vid flera tillfällen uttalat sig om sekretessbrytande bestämmelser och uppgiftsskyldigheter i förarbetena till sektorsspecifik kompletterande dataskyddsreglering. Dessa uttalanden har främst avsett utformningen av s.k. sekundära ändamålsbestämmelser, dvs. bestämmelser vars föremål är vidarebehandling för ändamål som inte regleras i den aktuella författningen (se vidare avsnitt 5.4.1).

[5] Prop. 2017/18:105, *Ny dataskyddslag*, s. 83.
[6] Jfr prop. 2017/18:95, *Anpassningar av vissa författningar inom skatt, tull och exekution till EU:s dataskyddsförordning*, s. 48.

Av regeringens uttalanden i dessa sammanhang framgår den bedömning som nyss redogjorts för, dvs. att lagstiftaren genom bestämmelser om att uppgifter får eller ska lämnas ut har tagit ställning till att vidarebehandling genom utlämnande är nödvändigt och proportionerligt för att säkerställa ett viktigt mål av allmänt intresse. Nedan ges några exempel på detta.

I förarbetena till lagen (2001:454) om behandling av personuppgifter inom socialtjänsten uttalade regeringen att för att tillgodose den enskildes integritet bör denne ges en så klar uppfattning som möjligt om i vilka sammanhang insamlade personuppgifter rörande honom/henne kan användas. Vad gäller uppgiftslämnande bl.a. till andra myndigheter konstaterade regeringen att det finns en rad författningar som innebär att myndigheter får eller ska lämna ut uppgifter. När bestämmelser om sådant uppgiftslämnande hade införts fick det enligt regeringen förutsättas att det hade gjorts en avvägning mellan intresset av att uppgiften lämnas ut och intresset av att skydda enskilda personers integritet, vid vilken man funnit att uppgiften bör lämnas ut. Enligt regeringens mening saknades det därför anledning att i en integritetsskyddslagstiftning särskilt reglera dessa fall av redan författningsreglerat uppgiftslämnande. Lagen om behandling av personuppgifter inom socialtjänsten skulle därför inte hindra att uppgifter lämnades ut om det följde av lag eller förordning.[7]

I förarbetena till patientdatalagen (2008:355) konstaterade regeringen att personuppgifter som behandlas i hälso- och sjukvården lämnas ut till andra i olika sammanhang, och att en myndighet på begäran av en annan myndighet ska lämna uppgifter den förfogar över i enlighet med 15 kap. 5 § sekretesslagen (1980:100) (dvs. nuvarande 6 kap. 5 § OSL). Regeringen konstaterade även att vissa sekretessbrytande bestämmelser i sekretesslagen (som i dag har sin motsvarighet i offentlighets- och sekretesslagen) inte hindrade att myndigheter inom hälso- och sjukvården lämnade uppgifter till andra myndigheter på eget initiativ. Gemensamt för allt detta uppgiftslämnande var enligt regeringen att det skedde med stöd av författningar som påbjuder eller tillåter utlämnande. När sådana bestämmelser hade införts fick det enligt regeringen förutsättas att det hade gjorts en avvägning mellan intresset av att uppgiften lämnas ut och intresset av att skydda enskilda personers integritet, vid vilken man funnit att uppgiften ska eller får lämnas ut. Enligt regeringen saknades det

[7] Prop. 2000/01:80, *Ny socialtjänstlag m.m.*, s. 143.

därför anledning att i en integritetsskyddslagstiftning förhindra att personuppgifter som finns i hälso- och sjukvården lämnas ut i dessa fall bara för att dessa numera hanteras med modern informationsteknik i stället för som tidigare på papper.[8]

I förarbetena till utlänningsdatalagen (2016:27) konstaterade regeringen åter att det finns en rad olika författningar som föreskriver en uppgiftsskyldighet för myndigheterna, dvs. att myndigheterna ska lämna ut uppgifter i vissa angivna situationer, och att myndigheter i vissa fall enligt lag eller förordning är skyldiga att på begäran lämna ut uppgifter till andra. Vidare konstaterade regeringen att det finns ett antal författningar med bestämmelser som medför att uppgifter får lämnas ut och som innebär att utlämnande är tillåtet, och att en myndighet även kan lämna ut uppgifter på eget initiativ, t.ex. för att kunna utföra en uppgift i den egna verksamheten. När bestämmelser om uppgiftslämnande har införts i lagstiftningen fick det enligt regeringen förutsättas att det gjorts en avvägning mellan intresset av att uppgiften lämnas ut och intresset av att skydda enskilda personers integritet, vid vilken man funnit att uppgiften ska eller får lämnas ut. I utlänningsdatalagen skulle därför införas en bestämmelse som medgav att uppgifter fick lämnas ut till andra myndigheter om uppgiften ska eller får lämnas ut med stöd av lag eller förordning.[9]

I samband med anpassning till EU:s dataskyddsreform av sektorsspecifik dataskyddsreglering gjordes motsvarande uttalanden även i flera andra sammanhang.[10] Det kan även nämnas att i rättsfallet HFD 2021 ref. 10 konstaterade Högsta förvaltningsdomstolen bl.a. att myndigheter hindras från att lämna bl.a. integritetskänsliga uppgifter till andra myndigheter genom sekretessbestämmelser. Domstolen ansåg att lagstiftaren härigenom får anses ha tagit ställning till när ett uppgiftslämnande är oförenligt med det eller de ändamål för vilka uppgifterna samlades in. Av rättsfallet framgår dessutom att den personuppgiftsansvariga myndigheten, utöver sekretessprövningen, inte ska göra någon kontroll av förenligheten med finalitetsprincipen i samband med lämnande av uppgifter enligt 6 kap. 5 § OSL.

[8] Prop. 2007/08:126, *Patientdatalag m.m.*, s. 59 och 60.
[9] Prop. 2015/16:65, *Utlänningsdatalag*, s. 68 och 69.
[10] Jfr prop. 2017/18:95, *Anpassningar av vissa författningar inom skatt, tull och exekution till EU:s dataskyddsförordning*, s. 57 och prop. 2017/18:112, *Anpassningar av registerförfattningar på arbetsmarknadsområdet till EU:s dataskyddsförordning*, s. 42 och 43.

3.3 Information till registrerade

3.3.1 Registrerades rättigheter

Allmänt

En viktig aspekt av dataskyddsförordningen är att enskildas (här kallat registrerades) rättigheter har stärkts i förhållande till tidigare gällande unionsrättslig dataskyddsreglering. Den registrerade kan t.ex. begära registerutdrag med information om bl.a. vilka kategorier av uppgifter som behandlas om honom eller henne (artikel 15). Vidare har den registrerade rätt att begära att få uppgifter rättade eller raderade eller att behandlingen ska begränsas (artiklarna 16–18). Enligt artikel 21.1 har den registrerade också rätt att göra invändningar mot personuppgiftsbehandling som grundar sig på bl.a. artikel 6.1 e. Den registrerade ska även ha rätt att inte bli föremål för ett beslut som enbart grundas på automatiserad behandling, inbegripen profilering, om beslutet har rättsliga följder eller på liknande sätt i betydande grad påverkar den registrerade (artikel 22).

Registrerades rättigheter (och personuppgiftsansvariga myndigheters korresponderande skyldigheter) får i och för sig begränsas. När och för vilka syften sådana begränsningar får göras framgår av artikel 23.1 i dataskyddsförordningen. En sådan begränsning får dock enbart göras om det sker med respekt för andemeningen i de grundläggande rättigheterna och friheterna och utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle i syfte att säkerställa viktiga allmänna intressen (se vidare avsnitt 10.3.4 i SOU 2024:63).

Principen om öppenhet

För att ge registrerade möjlighet att utöva kontroll över sina uppgifter och att utöva sina rättigheter enligt dataskyddsförordningen har personuppgiftsansvariga en skyldighet att tillhandahålla registrerade information om behandlingen. En av de grundläggande principerna för behandling av personuppgifter är dessutom att de ska behandlas på ett öppet sätt i förhållande till den registrerade (artikel 5.1 a). Enligt artikel 5.2 måste den personuppgiftsansvariga alltid kunna visa att personuppgifterna behandlas på ett öppet sätt gentemot den registrerade. Av artikel 12.1 framgår vidare att informationen eller

kommunikationen med registrerade bl.a. måste vara i en koncis, klar och tydlig, begriplig och lätt tillgänglig form och att ett klart och tydligt språk måste användas.

Öppenhet definieras inte i dataskyddsförordningen. Av skäl 39 framgår emellertid att det bör vara klart och tydligt för fysiska personer hur personuppgifter som rör dem insamlas, används, konsulteras eller på annat sätt behandlas samt i vilken utsträckning personuppgifterna behandlas eller kommer att behandlas. Öppenhetsprincipen gäller enligt skäl 39 framför allt informationen till registrerade om den personuppgiftsansvariges identitet och syftet med behandlingen samt ytterligare information för att sörja för en rättvis och öppen behandling för berörda fysiska personer och deras rätt att erhålla bekräftelse på och meddelande om vilka personuppgifter rörande dem som behandlas. Fysiska personer bör enligt skäl 39 göras medvetna om risker, regler, skyddsåtgärder och rättigheter i samband med behandlingen av personuppgifter och om hur de kan utöva sina rättigheter med avseende på behandlingen.

3.3.2 Skyldigheten att tillhandahålla information

Information som ska tillhandahållas

Vid informationsutbyte mellan myndigheter blir principen om öppenhet särskilt betydelsefull, eftersom förordningens bestämmelser avseende vilken information som ska ges de registrerade skiljer sig åt beroende på om uppgifterna hämtats från den registrerade själv eller erhållits på något annat sätt, t.ex. från en annan myndighet.

Personuppgiftsansvarigas skyldigheter och registrerades rättigheter när uppgifter samlas in från den registrerade regleras i artikel 13. Enligt artikel 13.1 ska den personuppgiftsansvarige ge viss information till den registrerade när uppgifterna erhålls. Informationen som enligt artikel 13.1 c ska tillhandahållas om personuppgifterna samlas in från den registrerade är bl.a. ändamålen med den behandling för vilken personuppgifterna är avsedda och den rättsliga grunden för behandlingen. Om den personuppgiftsansvariga myndigheten avser att ytterligare behandla uppgifterna för ett annat syfte än för vilket de samlades in, t.ex. genom utlämnande till en annan myndighet, ska den personuppgiftsansvariga myndigheten före denna ytterligare behandling ge den registrerade information om detta andra

syfte, om den registrerade inte redan förfogar över informationen (artikel 13.3 och 13.4).

I artikel 14 i dataskyddsförordningen regleras information som ska tillhandahållas om personuppgifterna *inte* har erhållits från den registrerade. Av artikel 14.1 framgår bl.a. vilken slags information som den personuppgiftsansvarige ska förse den registrerade med samt att den registrerade ska informeras om ändamålen med behandlingen, vilken rättslig grund behandlingen har och vilka mottagare som eventuellt ska ta del av uppgifterna. Av artikel 14.2 framgår bland annat vilken information, utöver den som avses i artikel 14.1, som den personuppgiftsansvarige ska lämna till den registrerade för att säkerställa en rättvis och transparent behandling. Artikel 14.3 anger vissa tidsangivelser för när informationen enligt de föregående punkterna ska lämnas och artikel 14.4 rör information vid ytterligare behandling av personuppgifterna för ett annat syfte än det för vilket uppgifterna samlades in.

Undantag från skyldigheten att tillhandahålla information

Vissa undantag från vad som anges i artikel 14.1–4 görs dock i artikel 14.5. Enligt artikel 14.5 a ska punkterna 1–4 ska inte tillämpas om den registrerade redan förfogar över informationen. Enligt artikel 14.5 b gäller detsamma bl.a. om tillhandahållandet av sådan information visar sig vara omöjligt eller skulle medföra en oproportionell ansträngning, eller i den mån den skyldighet som avses i punkt 1 sannolikt kommer att göra det omöjligt eller avsevärt försvårar uppfyllandet av målen med den behandlingen. Om personuppgifterna måste förbli konfidentiella till följd av tystnadsplikt enligt unionsrätten eller medlemsstaternas nationella rätt, inbegripet andra lagstadgade sekretessförpliktelser ska artikel 14.1–4 inte heller tillämpas, vilket framgår av artikel 14.5 d.

I artikel 14.5 c anges att undantag från skyldigheten att tillhandahålla information även görs vid erhållande eller utlämnande av uppgifter

- som uttryckligen föreskrivs genom unionsrätten eller genom en medlemsstats nationella rätt som den registrerade omfattas av, och
- som fastställer lämpliga åtgärder för att skydda den registrerades berättigade intressen.

Europeiska dataskyddsstyrelsen, EDPB,[11] har uttalat att en sådan lag som avses i artikel 14.5 c måste direkt avse den personuppgiftsansvarige som bör omfattas av ett obligatoriskt krav i fråga om erhållande eller utlämnande. Enligt EDPB måste de personuppgiftsansvariga därför kunna visa på vilket sätt lagen i fråga är tillämplig för dem och att de därmed måste antingen erhålla eller lämna ut personuppgifterna i fråga enligt denna. Vidare bör den personuppgiftsansvarige klargöra för de registrerade att personuppgifter erhålls och utlämnas i enlighet med lagen i fråga, om inget rättsligt förbud finns som hindrar den personuppgiftsansvarige från att göra detta.[12]

I sammanhanget bör noteras att i sitt förslag till avgörande i EU-domstolens mål C-169/23 har generaladvokaten bedömt att unionsrätten eller den nationella rätten förutsätts fylla samma funktion som den personuppgiftsansvariges informationsskyldighet enligt artikel 14.1–4 annars hade gjort. De registrerade anses alltså redan informerade genom den aktuella lagstiftningen. Enligt generaladvokaten är tillämpligheten av undantaget från skyldigheten att tillhandahålla information i artikel 14.5 c avhängig att det fastställts ”lämpliga åtgärder” för att skydda den registrerades berättigade intressen. Den relevanta lagstiftningen måste alltså säkerställa en rättvis och öppen behandling som är likvärdig med den som garanteras i artikel 14.1–4. För att den registrerade ska kunna bedöma eventuella risker förknippade med erhållandet av uppgifterna och behandlingen av dem måste det, enligt generaladvokaten, av ordalydelsen av den relevanta rättsliga bestämmelsen därför klart och tydligt framgå vem som behandlar uppgifterna, av vilken anledning och på vilket sätt dessa behandlas.[13] I sitt avgörande hänvisade EU-domstolen till generaladvokatens förslag och konstaterade även att unionslagstiftaren har velat att en registrerad ska ha rätt att få tillgång till de personuppgifter som har samlats in om honom eller henne för att vara medveten om att behandling sker och kunna kontrollera att den är laglig.[14]

[11] EDPB har enligt artikel 70 i dataskyddsförordningen i uppgift att se till att förordningen tillämpas enhetligt. För detta ändamål ska EDPB bl.a. enligt artikel 70.1 e utfärda riktlinjer, rekommendationer och bästa praxis i syfte att främja en enhetlig tillämpning av förordningen.
[12] Artikel 29-arbetsgruppen för uppgiftsskydd, *Riktlinjer om öppenhet enligt förordning (EU) 2016/679*, 17/SV, WP260rev.01, s. 33. Artikel 29-arbetsgruppens olika vägledningar avseende dataskyddsförordningen har godkänts av EDPB.
[13] Förslag till avgörande av generaladvokat Laila Medina, den 6 juni 2024 i C-169/23, Másdi, punkterna 31 och 69.
[14] EU-domstolens avgörande i C-169/23, Másdi, punkterna 51–54.

Regeringen har tidigare uttalat att kravet i artikel 14.5 c på uttryckliga föreskrifter om erhållande eller utlämnande av uppgifter i nationell rätt inte kan tolkas på annat sätt än som ett krav på föreskrifter om en *rätt* att få uppgifter eller föreskrifter om en uppgifts*skyldighet*. Enligt regeringens bedömning utgör bl.a. uppgiftsskyldigheten enligt 6 kap. 5 § OSL en sådan nationell föreskrift om erhållande eller utlämnande av uppgifter som uppfyller de krav som uppställs i artikel 14.5 c i dataskyddsförordningen. Enligt regeringen innebär ett utlämnande enligt 6 kap. 5 § OSL därmed att informationsskyldigheten enligt artikel 14.1–4 inte blir aktuell. Detta gäller enligt regeringen oavsett för vilket ändamål uppgifterna lämnas ut.[15]

Även regelrätta uppgiftsskyldigheter utanför offentlighets- och sekretesslagen måste i enlighet med regeringens uttalanden anses omfattas av undantaget i artikel 14.5 c. Myndigheter bör dock även i dessa situationer klargöra för de registrerade att personuppgifter erhålls och utlämnas i enlighet med 6 kap. 5 § OSL eller relevanta uppgiftsskyldigheter, om inget rättsligt förbud finns som hindrar den personuppgiftsansvariga myndigheten från att göra detta.[16]

Däremot förefaller uppgiftslämnande på eget initiativ som sker med stöd av sekretessbrytande bestämmelser som inte innebär en skyldighet, t.ex. bestämmelser i 10 kap. OSL, inte aktualisera undantaget från informationsskyldigheten enligt artikel 14.5 c. Däremot kan övriga bestämmelser i artikel 14.5 medföra att informationsskyldigheten inte gäller vid sådant författningsreglerat informationsutbyte mellan myndigheter som inte innebär att det föreligger en skyldighet att lämna ut uppgifter.

3.4 Tekniska och organisatoriska åtgärder samt konsekvensbedömning

3.4.1 Ett riskbaserat förhållningssätt

Vid alla former av utlämnande från en myndighet till en annan finns det bl.a. en risk för att personuppgifter får obefogad spridning. Det gäller oavsett om utlämnande sker med digitala hjälpmedel eller analogt. Dataskyddsförordningen reglerar dock inte hur behandling av

[15] Prop. 2017/18:298, *Behandling av personuppgifter för forskningsändamål*, s. 110–112.
[16] Jfr Artikel 29-arbetsgruppen för uppgiftsskydd, *Riktlinjer om öppenhet enligt förordning (EU) 2016/679*, 17/SV, WP260rev.01, s. 33.

personuppgifter rent tekniskt ska gå till, vare sig vid informationsutbyte mellan myndigheter eller vid behandling för andra ändamål. Utöver de grundläggande principerna för behandling i artikel 5, kravet på rättslig grund i artikel 6, särskilda begränsningar för känsliga personuppgifter m.m. i artiklarna 9 och 10, rättigheter för registrerade och motsvarande skyldigheter för personuppgiftsansvariga i artiklarna 12–22 och 34, innehåller dataskyddsförordningen även flera instruktioner, eller förfarandebestämmelser, som styr hur den personuppgiftsansvariga myndigheten är skyldig att agera för att skyddet för den personliga integriteten ska upprätthållas i det enskilda fallet.

I artikel 24 fastställs den personuppgiftsansvariga myndighetens ansvar för att genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med dataskyddsförordningen. Begreppen personuppgiftsansvarig och gemensamt personuppgiftsansvariga spelar alltså en viktig roll vid tillämpningen av dessa bestämmelser eftersom de fastställer vem som ska ansvara för efterlevnaden av olika dataskyddsbestämmelser.[17] Regleringen är ofta utformad på så sätt att den personuppgiftsansvariga åläggs en mer eller mindre specifik skyldighet att agera med utgångspunkt i de risker som en viss behandling bedöms föra med sig. Begreppet ”risk” är alltså centralt i dessa sammanhang och det som avses är risker för fysiska personers rättigheter och friheter. Främst avses integritetsrisker men det kan också vara andra grundläggande rättigheter, exempelvis yttrandefrihet, rätten att inte bli utsatt för diskriminering och rätten till religionsfrihet.[18]

Någon definition av vad begreppet risk rent konkret innebär finns dock inte i förordningen. Däremot anges exempel på när risker typiskt sett kan uppkomma. Det är bl.a. vid behandling av känsliga personuppgifter eller vid personuppgiftsbehandling som skulle kunna medföra immateriella skador, ekonomisk förlust, skadat anseende, förlust av konfidentialitet när det gäller personuppgifter som omfattas av tystnadsplikt, hinder mot registrerades möjlighet att utöva kontroll över sina personuppgifter, eller om behandlingen inbegriper ett stort antal personuppgifter och gäller ett stort antal registrerade (skäl 75). Hur sannolik och allvarlig risken är ska fastställas utifrån behandlingens art, omfattning, sammanhang och ändamål. Risken ska vidare

[17] EDPB, *Riktlinjer 07/2020 angående begreppen personuppgiftsansvarig och personuppgiftsbiträde i GDPR*, Version 2.0, s. 3.
[18] Jfr Artikel 29-arbetsgruppen för skydd av personuppgifter, *Statement on the role of a risk-based approach in data protection legal frameworks*, 14/EN WP 218 s. 4.

utvärderas genom en objektiv bedömning som fastställer om behandlingen medför en risk eller en hög risk (skäl 76).

3.4.2 Inbyggt dataskydd och dataskydd som standard

Allmänt

Inbyggt dataskydd och dataskydd som standard har en särskild betydelse vid myndigheters informationsutbyte. Genom artikel 25.1–2 ställs krav på myndigheterna att utforma systemen för informationsutbyte med andra myndigheter på ett sådant sätt att det säkerställs att utbytet sker med iakttagande bl.a. av principen om uppgiftsminimering i artikel 5.1 c i dataskyddsförordningen. Det innebär att själva systemet för informationsutbyte måste konstrueras så att enbart adekvata, relevanta och inga överflödiga personuppgifter lämnas ur. När ett utbyte sker med stöd av en sekretessbrytande bestämmelse och efter en begäran enligt 6 kap. 5 § OSL innebär det att systemet inte får möjliggöra överföring av andra personuppgifter än de som dels träffas av den sekretessbrytande bestämmelsen dels faktiskt begärts ut av den mottagande myndigheten.

Med beaktande av bl.a. den senaste utvecklingen, behandlingens omfattning och ändamål samt riskerna för fysiska personer, ska en personuppgiftsansvarig myndighet, både vid fastställandet av med vilka medel behandlingen utförs och vid själva behandlingen, genomföra lämpliga tekniska och organisatoriska åtgärder för ett effektivt genomförande av dataskyddsprinciperna och för integrering av nödvändiga skyddsåtgärder i behandlingen så att kraven i dataskyddsförordningen uppfylls och den registrerades rättigheter skyddas. Detta framgår av artikel 25.1 i dataskyddsförordningen och brukar benämnas inbyggt dataskydd.

Enligt artikel 25.2 ska den personuppgiftsansvarige genomföra lämpliga tekniska och organisatoriska åtgärder för att i standardfallet säkerställa att endast personuppgifter som är nödvändiga för varje specifikt ändamål med behandlingen behandlas. Den skyldigheten gäller mängden insamlade personuppgifter, behandlingens omfattning, tiden för deras lagring och deras tillgänglighet. Framför allt ska dessa åtgärder säkerställa att personuppgifter i standardfallet inte utan den enskildes medverkan görs tillgängliga för ett obegränsat antal fysiska personer. Detta brukar benämnas dataskydd som standard.

EDPB:s riktlinjer

En vägledning för myndigheter och andra

EDPB har antagit riktlinjer om inbyggt dataskydd och dataskydd som standard, som konkretiserar vad principerna innebär för de personuppgiftsansvariga. Riktlinjerna syftar bl.a. till att utreda och ge vägledning avseende kraven på inbyggt dataskydd i artikel 25.1 i dataskyddsförordningen, respektive dataskydd som standard i artikel 25.2.[19] Av riktlinjerna framgår bl.a. följande.

Artikel 25.1

Tekniska och organisatoriska åtgärder och nödvändiga skyddsåtgärder ska tolkas i vid mening, som samtliga metoder eller medel som en personuppgiftsansvarig kan använda vid behandlingen. En teknisk eller organisatorisk åtgärd och en skyddsåtgärd kan vara allt från användning av avancerade tekniska lösningar till grundläggande utbildning av personalen. Beroende på sammanhanget och de risker som är förbundna med den aktuella behandlingen kan exempel vara tillhandahållande av information om lagringen av personuppgifter, inrättande av system för hantering av integritet och informationssäkerhet etc.

Vid genomförandet av lämpliga tekniska och organisatoriska åtgärder bör åtgärderna och skyddsåtgärderna vara utformade så att var och en av principerna för dataskydd och det efterföljande skyddet av rättigheter kan genomföras på ett effektivt sätt. De valda åtgärderna och skyddsåtgärderna bör utformas för genomförandet av principerna för dataskydd i just den aktuella behandlingen. Frågan om åtgärder är effektiva beror därför på omständigheterna i samband med behandlingen i det enskilda fallet och på en bedömning av vissa omständigheter som bör beaktas vid fastställandet av medlen för behandlingen. Den personuppgiftsansvariga bör kunna dokumentera de tekniska och organisatoriska åtgärder som genomförts.

Hänvisningen till den senaste utvecklingen innebär en skyldighet för personuppgiftsansvariga att beakta de aktuella framsteg på teknikområdet som är tillgängliga på marknaden vid fastställandet av lämpliga

[19] EDPB, *Riktlinjer 4/2019 om artikel 25 Inbyggt dataskydd och dataskydd som standard*, Version 2.0, s. 3.

tekniska och organisatoriska åtgärder. Kravet är att personuppgiftsansvariga ska ha kunskap om och hålla sig uppdaterade om tekniska framsteg, om hur teknik kan medföra datasäkerhetsrisker eller möjligheter för behandlingen och om hur de åtgärder och skyddsåtgärder som säkerställer ett effektivt genomförande av principerna och de registrerades rättigheter ska genomföras och uppdateras.

Personuppgiftsansvariga måste ta hänsyn till behandlingens art, omfattning, sammanhang och ändamål när de fastställer nödvändiga åtgärder. Dessa faktorer bör tolkas i överensstämmelse med deras roll i andra bestämmelser i dataskyddsförordningen, i syfte att låta principerna för dataskydd bli en del av behandlingen. Begreppet art kan kortfattat uttryckt förstås som behandlingens inneboende egenskaper, exempelvis särskilda kategorier av personuppgifter, automatiskt beslutsfattande, skeva maktförhållanden, oförutsägbar behandling osv.

Omfattningen avser behandlingens storlek och räckvidd. Sammanhanget hänför sig till omständigheterna vid behandlingen, vilka kan påverka den registrerades förväntningar, medan ändamålet avser behandlingens syfte.

Vid genomförandet av den riskanalys som krävs för efterlevnad av artikel 25 måste den personuppgiftsansvarige identifiera vilka risker för de registrerades rättigheter som en överträdelse av principerna innebär, och fastställa deras sannolikhet och allvar så att åtgärder kan vidtas för att effektivt minska de identifierade riskerna. Det är under arbetet med att fatta beslut om hur behandlingen ska utföras och på vilket sätt behandlingen ska ske och vilka mekanismer som ska användas för att utföra behandlingen som den personuppgiftsansvarige är skyldig att bedöma de lämpliga åtgärderna och skyddsåtgärderna för att principerna och de registrerades rättigheter ska genomföras på ett effektivt sätt i behandlingen. Att redan i ett tidigt skede överväga inbyggt dataskydd och dataskydd som standard är avgörande för ett framgångsrikt genomförande av principerna och skyddet av de registrerades rättigheter.

När behandlingen har inletts är den personuppgiftsansvarige fortsatt skyldig att upprätthålla inbyggt dataskydd och dataskydd som standard, dvs. fortsätta att på ett effektivt sätt genomföra principerna för att skydda rättigheterna, hålla sig à jour med den senaste tekniken, ompröva risknivån osv. Behandlingarnas art, omfattning och sammanhang samt risken kan förändras under behandlingens gång, vilket innebär att den personuppgiftsansvarige kontinuerligt

måste utvärdera sin behandling genom regelbundna översyner och bedömningar av effektiviteten hos de åtgärder och skyddsåtgärder som valts.

Artikel 25.2

Den personuppgiftsansvarige bör välja och vara ansvarig för att införa standardinställningar och alternativ på ett sådant sätt att endast sådan behandling som är absolut nödvändig för att uppnå det fastställda, lagliga ändamålet utförs som standard. Här bör de personuppgiftsansvariga utgå från sin bedömning att behandlingen är nödvändig sett till de rättsliga grunderna i artikel 6.1.

Grundkravet är att dataskyddet ska vara inbyggt i den behandling som utförs som standard. Åtgärderna ska som standard vara lämpliga för att säkerställa att endast personuppgifter som är nödvändiga för varje särskilt ändamål med behandlingen behandlas. De organisatoriska åtgärder som stöder behandlingen ska, redan från början, vara utformade så att endast den minsta mängd personuppgifter som krävs för de särskilda åtgärderna behandlas. Detta ska särskilt beaktas när personal med olika arbetsuppgifter och olika behov får åtkomst till uppgifter. Den personuppgiftsansvarige bör begränsa vilka som kan få tillgång till personuppgifter (och vilken typ av tillgång) grundat på en bedömning av tillgångens nödvändighet, och även se till att personuppgifterna faktiskt är tillgängliga för dem som vid behov behöver dem, t.ex. i kritiska situationer. Åtkomstkontroller bör iakttas för hela dataflödet under behandlingen.

3.4.3 Lämplig säkerhetsnivå

Informationssäkerhet har en särskild betydelse vid överföring av uppgifter mellan myndigheter. En osäker anslutning mellan två olika informationshanteringssystem kan t.ex. vid en attack orsaka att både uppgifter som överförs och andra uppgifter som myndigheterna förfogar över kommer i orätta händer. En sådan incident kan orsaka stora integritetsförluster för de registrerade. Som redan konstaterats reglerar dock dataskyddsförordningen inte att vissa tekniska lösningar ska användas vare sig vid informationsutbyte

eller annan behandling. Däremot måste de lösningar som väljs uppfylla kraven enligt förordningen.

Av artikel 5.1 f i datsskyddsförordningen följer att personuppgifter ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder. Säker behandling av personuppgifter är alltså en av de grundläggande principer som gäller vid all form av personuppgiftsbehandling enligt dataskyddsförordningen. EU-domstolen har dessutom bedömt att informationssäkerhet är en integrerad del av rätten till skydd för personuppgifter enligt artikel 8 i Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna, EKMR.[20]

Enligt artikel 32.1 a–d ska den personuppgiftsansvarige 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.

Det kan röra sig om pseudonymisering och kryptering av uppgifter. Enligt artikel 4.5 innebär pseudonymisering behandling av personuppgifter på ett sätt som innebär att personuppgifterna inte längre kan tillskrivas en specifik registrerad utan att kompletterande uppgifter används, under förutsättning att dessa kompletterande uppgifter förvaras separat och är föremål för tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna inte tillskrivs en identifierad eller identifierbar fysisk person. Av artikel 34.3 a framgår att kryptering kan vara att göra uppgifterna oläsbara för alla personer som inte är behöriga att få tillgång till personuppgifterna.

Det kan även vara att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingsystemen och -tjänsterna, och att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet Detta kan bl.a. inbegripa regelbunden utbildning av personal i frågor om dataskydd och integritetsrisker, samt vikten av att följa det dataskyddsrättsliga regelverket. Det kan även röra som om att använda kryptering, åtkomstbegränsningar, autentisering i flera led, loggning och elektroniska signaturer.

[20] Se EU-domstolens avgörande i C-293/12 och C-594/12, Digital Rights Ireland Ltd, punkterna 25–29.

Tillgänglighet kan avse att ha ersättningssystem eller backupsystem, och att genomföra regelbundna funktionalitetstest. Motståndskraft kan slutligen avse att vidta åtgärder för att säkerställa att systemen fortsätter fungera under sämre förutsättningar eller störningar, t.ex. genom att stänga av delar av ett informationshanteringshanteringssystem som utsätts för en attack utan att systemets funktion påverkas, och att minimera möjligheterna att genomföra en attack.[21]

Av artikel 32.2 framgår att vid bedömningen av lämplig säkerhetsnivå ska särskild hänsyn tas till de risker som behandling medför, i synnerhet bl.a. obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

Enligt artikel 32.4 ska en personuppgiftsansvarig dessutom vidta åtgärder för att säkerställa att varje fysisk person som utför arbete under den personuppgiftsansvariges överinseende, och som får tillgång till personuppgifter, endast behandlar dessa på instruktion från den personuppgiftsansvarige, om inte unionsrätten eller medlemsstaternas nationella rätt ålägger honom eller henne att göra det. Detta kräver bl.a. att det internt vid myndigheterna finns rutiner och någon form av kontrollsystem av att bestämmelsen följs.

3.4.4 Konsekvensbedömning

När ett nytt informationsutbyte mellan myndigheter initieras, t.ex. på grund av att det införts en ny sekretessbrytande bestämmelse eller en ny uppgiftsskyldighet, bör konsekvenserna av behandlingen analyseras av de inblandade myndigheterna.

Om en typ av behandling, särskilt med användning av ny teknik och med beaktande av dess art, omfattning, sammanhang och ändamål, sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige, enligt artikel 35.1, före behandlingen utföra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter. Bedömningen ska enligt artikel 35.7 åtminstone innehålla bl.a. en systematisk beskrivning av den planerade behandlingen och behandlingens syften, en bedömning av behovet av och proportionaliteten hos behandlingen i förhåll-

[21] Jfr hänvisningarna till olika europeiska rättsfall på websidan GDPRhub, Article 32 GDPR, tillgänglig: https://gdprhub.eu/Article_32_GDPR#cite_ref-17 (hämtad 2024-10-30).

ande till syftena, en bedömning av risker och de åtgärder som planeras för att hantera riskerna, inbegripet skyddsåtgärder, säkerhetsåtgärder och rutiner för att säkerställa skyddet av personuppgifterna och för att visa att dataskyddsförordningen efterlevs.

Av skäl 69 till dataskyddsförordningen framgår vidare att det ibland kan vara förnuftigt och ekonomiskt att en konsekvensbedömning avseende dataskydd inriktar sig på ett vidare område än ett enda projekt, exempelvis när myndigheter eller organ avser att skapa en gemensam tillämpnings- eller behandlingsplattform.

Den nationella tillsynsmyndigheten, som i Sverige är Integritetsskyddsmyndigheten, IMY, ska enligt artikel 35.4 upprätta och offentliggöra en förteckning över det slags behandlingsverksamheter som omfattas av kravet på en konsekvensbedömning avseende dataskydd. Av den förteckning IMY upprättat framgår att en konsekvensbedömning avseende dataskydd ska göras om den planerade behandlingen uppfyller minst två av bl.a. följande kriterier:[22]

- Behandlar personuppgifter i syfte att fatta automatiserade beslut som har rättsliga följder eller liknande betydande följder för den registrerade.
- Behandlar känsliga personuppgifter enligt artikel 9 eller uppgifter som är av mycket personlig karaktär.
- Behandlar personuppgifter i stor omfattning.
- Kombinerar personuppgifter från två eller flera behandlingar på ett sätt som avviker från vad de registrerade rimligen kunnat förvänta sig, till exempel när man samkör register.
- Använder ny teknik eller nya organisatoriska lösningar.

Beroende på de rättsliga förutsättningarna för ett planerat uppgiftsutbyte, t.ex. avseende sekretessbestämmelser, regler för personuppgiftsbehandling vid den utlämnande och/eller mottagande myndigheten, uppgifternas karaktär, syftet med och omfattningen av utlämnandet kan personuppgiftsansvariga myndigheter som överväger att upprätta ett system för utbytet enligt dataskyddsförordningen vara skyldiga att upprätta en konsekvensbedömning. I situationer där det är osäkert om en konsekvensbedömning är nödvändig bör en sådan ändå utföras,

[22] IMY, *Förteckning enligt artikel 35.4 i Dataskyddsförordningen*, DI-2018-13200, s. 3.

eftersom det är ett användbart verktyg för att hjälpa personuppgiftsansvariga att iaktta dataskyddslagstiftningen.[23] Här kan också nämnas att personuppgiftsansvariga myndigheter även på ett generellt plan är skyldiga att ha dokumentation som visar att behandling utförs i enlighet med dataskyddsförordningen, vilket framgår av artikel 5.2 och artikel 24.1.

Om det av en konsekvensbedömning framgår att behandlingen utan skyddsåtgärder, säkerhetsåtgärder och säkerhetsmekanismer kommer att innebära en hög risk, och den personuppgiftsansvariga myndigheten anser att risken inte kan begränsas genom rimliga åtgärder, så bör samråd hållas med IMY innan behandlingen inleds. Om IMY efter ett sådant förhandssamråd anser att den planerade behandlingen skulle strida mot dataskyddsförordningen, särskilt om den personuppgiftsansvariga myndigheten inte i tillräcklig utsträckning har fastställt eller reducerat risken, har IMY möjlighet att införa en tillfällig begränsning av eller ett förbud mot behandlingen. Det nyss sagda framgår av skäl 94 samt artiklarna 36.2 och 58.2 i dataskyddsförordningen.

[23] Artikel 29-arbetsgruppen för skydd av personuppgifter, *Riktlinjer om konsekvensbedömning avseende dataskydd och fastställande av huruvida behandlingen ”sannolikt leder till en hög risk” i den mening som avses i förordning 2016/679*, 17/SV WP 248 rev. 01, s. 9.

4 Förbättrade möjligheter att utbyta uppgifter som inte är sekretessbelagda

4.1 Inledning

4.1.1 Uppdraget

I vårt delbetänkande SOU 2024:63, *Ökat informationsutbyte mellan myndigheter. Behov och föreslagna förändringar*, har vi föreslagit att det ska införas en generell sekretessbrytande bestämmelse i 10 kap. 15 a § offentlighets- och sekretesslagen (2009:400), OSL. Bestämmelsen innebär att myndigheter får lämna ut annars sekretessbelagda uppgifter till andra myndigheter i vissa situationer. Ett utlämnande ska föregås av en intresseavvägning och får ske på initiativ av den utlämnande myndigheten. Någon begäran behöver alltså inte framställas för att uppgifter ska kunna lämnas ut med stöd av den föreslagna sekretessbrytande bestämmelsen.

Vårt återstående uppdrag omfattar bl.a. att mot bakgrund av vår kartläggning av behovet av förbättrade möjligheter till informationsutbyte mellan myndigheter analysera och ta ställning till hur behovet av att utbyta s.k. offentliga uppgifter (dvs. uppgifter som inte är sekretessbelagda) kan tillgodoses. Vi ska särskilt överväga och lämna förslag på en bestämmelse som i större utsträckning gör det möjligt att på eget initiativ lämna ut sådana uppgifter till en annan myndighet.

4.1.2 Kapitlets disposition

För att sätta frågan om det bör införas utökade möjligheter att på eget initiativ lämna ut offentliga uppgifter i sitt sammanhang lämnas inledningsvis i detta kapitel en översiktlig redogörelse för relevanta rättsregler (avsnitt 4.2).

Därefter övergår vi i avsnitt 4.3 till frågan om vilka uppgifter som ska betraktas som offentliga och som därmed får lämnas ut med en tillämpning av sekretessregleringen. Vi utgår här från att uppgifter som inte är sekretessbelagda ska betraktas som offentliga uppgifter (jfr 6 kap. 5 § OSL). Uppgifter som inte är *sekretessreglerade*, uppgifter som omfattas av *undantag* från sekretess samt uppgifter som kan lämnas ut efter en *sekretessprövning* eller enligt en *sekretessbrytande* bestämmelse är inte sekretessbelagda. Det innebär att uttrycken ”offentliga uppgifter” och ”uppgifter som inte är sekretessbelagda” i betänkandet betraktas som synonyma. I kapitlet använder vi begreppet uppgifter som inte är sekretessbelagda. För att åskådliggöra skillnaden mellan att lämna uppgifter efter en begäran från en annan myndighet och att lämna uppgifter till en annan myndighet på eget initiativ redovisar vi i avsnitt 4.4 den befintliga reglering där denna skillnad tydliggörs, dvs. i utformningen av olika former av uppgiftsskyldigheter. I avsnitt 4.5 ger vi sedan några exempel på när myndigheter har en skyldighet att på eget initiativ lämna uppgifter till andra myndigheter, samt motiven bakom detta.

I avsnitt 4.6 redogör vi för det befintliga rättsliga stödet för myndigheterna att på eget initiativ lämna ut uppgifter som inte är sekretessbelagda till andra myndigheter.

I avsnitt 4.7 redogör vi därefter för vilket generellt behov det finns av att i högre utsträckning än i dag kunna lämna ut uppgifter på initiativ av den utlämnande myndigheten, samt vilka uppgifter behovet avser. Frågan om en uppgift är sekretessbelagd eller inte är dock svår att besvara annat än i en konkret utlämnandesituation. I det avsnittet utgår vi därför från behovet av att lämna ut uppgifter på eget initiativ, snarare än uppgifternas rättsliga status.

I avsnitt 4.8 redovisar vi våra överväganden och förslag. I avsnitt 4.8.1 redovisar vi vår bedömning av om de kartlagda generella behoven av ett förbättrat informationsutbyte mellan myndigheter även avser möjligheten att på eget initiativ utbyta uppgifter som inte är sekretessbelagda. I avsnitt 4.8.2 redogör vi för vår bedömning av

behoven av förtydligande av gällande rätt. Därefter redogör vi för vår bedömning av betydelsen av utlämnande på eget initiativ i avsnitt 4.8.3. I avsnitt 4.8.4 gör vi en bedömning av om den befintliga regleringen av möjligheterna till egeninitierat utlämnande är motiverad. Slutligen lämnar vi i avsnitt 4.8.5 förslag till en ny bestämmelse i offentlighets- och sekretesslagen som i likhet med 6 kap. 5 § OSL avser uppgifter som inte är sekretessbelagda.

4.2 Rättslig reglering vid informationsutbyte av uppgifter som inte är sekretessbelagda

4.2.1 Allmänna handlingars offentlighet

Offentlighetsprincipen regleras i 2 kap. tryckfrihetsförordningen, TF. Enligt 2 kap. 1 § TF ska var och en ha rätt att ta del av allmänna handlingar.

Av 2 kap. 3 § TF framgår att med handling avses en framställning i skrift eller bild samt en upptagning som endast med tekniska hjälpmedel kan läsas eller avlyssnas eller uppfattas på annat sätt. Uttrycket *handling* i tryckfrihetsförordningen tar alltså sikte på såväl traditionella pappershandlingar som exempelvis texter eller annan information lagrad på annat sätt, t.ex. i en dator.

Enligt 2 kap. 4 § TF är en handling allmän om den förvaras hos en myndighet och enligt särskilda bestämmelser är att anse som inkommen till eller upprättad där. I 2 kap. 6 § TF sägs att en sådan upptagning som avses i 2 kap. 3 § TF 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.

Rätten att ta del av allmänna handlingar får bara begränsas om det krävs med hänsyn till vissa i 2 kap. 2 § TF angivna grunder, s.k. sekretessgrunder. En sådan begränsning ska anges noga i en bestämmelse i en särskild lag eller, om det anses lämpligare i ett visst fall, i en annan lag som den särskilda lagen hänvisar till. Den särskilda lag som avses är offentlighets- och sekretesslagen.

4.2.2 Skyldigheten att lämna ut uppgifter ur allmänna handlingar till enskilda

I vårt delbetänkande lämnas en översiktlig redogörelse över offentlighets- och sekretesslagens bestämmelser (se SOU 2024:63 avsnitt 3.4). I detta sammanhang kan särskilt nämnas att det i 6 kap. 4 § OSL föreskrivs att en myndighet ska på begäran av en enskild lämna uppgift ur en allmän handling som förvaras hos myndigheten, om inte uppgiften är sekretessbelagd eller det skulle hindra arbetets behöriga gång. Bestämmelsen kan sägas komplettera de ovan nämnda bestämmelserna om rätten till utlämnande av allmän handling i tryckfrihetsförordningen (jfr även 6 kap. 1–3 och 6 §§ OSL).

4.2.3 Offentlighetsprincipen och myndigheternas utbyte av uppgifter som inte är sekretessbelagda

I lagmotiven till 1948 års tryckfrihetsförordning uttalades att bestämmelserna i 2 kap. TF reglerar den enskildes rätt att från en myndighet få ut allmänna handlingar, och att bestämmelserna inte avser tillhandahållande av allmänna handlingar myndigheter emellan. Det uttalades vidare att det alltså inte finns någon rätt för en myndighet att få ut en handling, men att myndigheterna åtminstone i viss utsträckning har en skyldighet att bistå varandra med tillhandahållande av handlingar. I lagmotiven uttalades också att bestämmelserna i 2 kap. TF visserligen inte har omedelbar betydelse för frågan om tillhandahållande av handlingar mellan myndigheter, men uppenbart har de betydelse även i detta avseende. Om handlingen är offentlig finns det inte – enligt motiven – någon anledning för en myndighet att vägra lämna ut den till en annan myndighet.[1]

Lagstiftaren intog alltså den inställningen att om handlingarna kunde lämnas ut till enskilda enligt tryckfrihetsförordningen, fanns det inget som hindrade att en myndighet lämnade ut dem till en annan myndighet på begäran. Detta låg också i linje med principen om att myndigheter skulle ”räcka varandra handen” som kom till uttryck i 47 § 1809 års regeringsform som ännu gällde när 1948 års tryckfrihetsförordning trädde i kraft.

[1] Prop. 1948:230, *med förslag till tryckfrihetsförordning m.m.,* s. 122 och 123.

När 1948 års tryckfrihetsförordning trädde i kraft begränsades allmänhetens rätt att ta del av allmänna handlingar genom bestämmelser i lagen (1937:249) om inskränkningar i rätten att utbekomma allmänna handlingar. Som nämns i vårt delbetänkande (se SOU 2024:63 avsnitt 5.1.2) var de sekretessbestämmelser som fanns i 1937 års sekretesslag med något undantag inte direkt tillämpliga på utlämnanden av handlingar mellan myndigheter. I de fall handlingarna var hemliga förutsattes i stället att det skulle prövas från fall till fall om ett utlämnande var förenligt med sekretessintresset. Varken tryckfrihetsförordningen eller dåtidens sekretessreglering hade alltså någon omedelbar betydelse för uppgiftsflödet myndigheter emellan, utan snarare en indirekt betydelse.

Som vi också redogör för i vårt delbetänkande (se SOU 2024:63 avsnitt 5.1.2) var det först genom införandet av sekretesslagen (1980:100) som sekretessbestämmelserna gjordes direkt tillämpliga på uppgiftslämnande mellan myndigheter. Den nuvarande regleringssituationen – som gällt sedan införandet 1980 års sekretesslag – innebär alltså att sekretessregleringen är tillämplig på uppgiftslämnande mellan myndigheter samtidigt som myndigheterna inte har någon rätt att utfå allmänna handlingar från varandra med stöd av 2 kap. TF.

4.2.4 Myndigheter ska samarbeta och bistå varandra

Som just konstaterats har bestämmelserna i 2 kap. TF inte någon omedelbar betydelse för frågan om tillhandahållande av handlingar mellan myndigheter. Sedan mycket länge har det emellertid ansetts vara en självklar princip att alla myndigheter är skyldiga att samarbeta och bistå varandra i den utsträckning som det kan ske. Som vi nämnt innehöll redan 1809 års regeringsform en föreskrift om att myndigheterna skulle räcka varandra handen. När 1974 års regeringsform ersatte 1809 års regeringsform ansågs det dock inte nödvändigt att i grundlag fastställa att förvaltningsmyndigheterna skulle biträda och hjälpa varandra.[2] Sedan 1809 års regeringsform upphört att gälla fanns det alltså inte någon allmän regel om samverkan mellan myndigheterna. I 15 kap. 5 § i 1980 års sekretesslag fanns dock en bestämmelse om myndigheternas skyldighet att på begäran lämna varandra upp-

[2] Prop. 1973:90, *med förslag till ny regeringsform och ny riksdagsordning m. m.*, s. 396.

gifter som de förfogade över. Denna bestämmelse motsvarar den nuvarande bestämmelsen i 6 kap. 5 § OSL (se nedan).

Allmänna bestämmelser om samverkan mellan myndigheterna återinfördes i svensk rätt först när förvaltningslagen (1986:223) trädde i kraft och ersatte 1971 års förvaltningslag (1971:290). När 1986 års förvaltningslag ersattes av den nu gällande förvaltningslagen (2017:900), FL, överfördes samarbetsbestämmelserna dit med vissa justeringar.[3]

Principen om myndigheternas skyldighet att samarbeta och bistå varandra kommer numera till uttryck i 8 § första stycket FL där det anges att en myndighet inom sitt verksamhetsområde ska samverka med andra myndigheter. I lagmotiven framhålls att syftet med bestämmelsen är att samverkan mellan myndigheter ska leda till att förvaltningen generellt ska bli så enhetlig och effektiv som möjligt. Vidare sägs att bestämmelsen också utgör ett led i regleringen av myndigheternas serviceskyldighet gentemot allmänheten och ger i det avseendet författningsstöd för sådan samverkan mellan myndigheter som underlättar enskildas kontakter med dem. Avsikten är att en handläggande myndighet – i den utsträckning som det är möjligt och lämpligt – själv ska ta den kontakt med andra myndigheter som behövs för att utredningen i ärendet ska bli tillräcklig. Som exempel på en sådan situation som bestämmelsen tar sikte på nämns i lagmotiven att myndigheter samråder och lämnar varandra upplysningar eller bistår med särskild sakkunskap genom informella kontakter per telefon eller vid möten.[4]

Bestämmelsen i 8 § första stycket FL begränsas på det sättet att samverkan ska ske inom myndighetens verksamhetsområde. Detta ligger i linje med det förhållandet att myndigheternas verksamhet styrs enlig legalitetsprincipen. Det innebär bl.a. att det inte får förekomma några nyskapelser i form av särskilda samarbetsorgan, som oberoende av tillämpliga föreskrifter fattar beslut som inte kan härledas till någon av de samverkande myndigheterna.[5]

Skyldigheten att samverka med andra myndigheter i 8 § första stycket FL gäller inte bara vid ärendehandläggning utan även vid annan förvaltningsverksamhet, dvs. sådan verksamhet som utgör

[3] Se prop. 1985/86:80, *om ny förvaltningslag*, s. 23 och 61 och prop. 2016/17:180, *En modern och rättssäker förvaltning – ny förvaltningslag*, s. 70–73.
[4] Prop. 2016/17:180, *En modern och rättssäker förvaltning – ny förvaltningslag*, s. 70 och 71.
[5] Jfr prop. 2016/17:180, *En modern och rättssäker förvaltning – ny förvaltningslag*, s. 71 och JO 1993/94 s. 458.

förvaltningsmyndighetens eller domstolens faktiska handlande (se 1 § andra stycket FL). Bestämmelsen innebär dock inte någon uppgiftsskyldighet i offentlighets- och sekretesslagens mening och bryter inte heller sekretess mellan myndigheter. Förvaltningslagens tillämpningsområde är också smalare än offentlighets- och sekretesslagens tillämpningsområde och omfattar t.ex. inte riksdagen eller de kommunala beslutande församlingarna vilket däremot offentlighets- och sekretesslagen gör.

I detta sammanhang bör också nämnas att det i 6 § andra stycket myndighetsförordningen (2007:515) föreskrivs att en myndighet ska verka för att genom samarbete med myndigheter och andra ta till vara de fördelar som kan vinnas för enskilda samt för staten som helhet. Myndighetsförordningen gäller enligt 1 § första stycket för förvaltningsmyndigheter under regeringen.

I 6 kap. 5 § OSL finns en bestämmelse om myndigheters informationsskyldighet gentemot varandra. Av den framgår att en myndighet på begäran av en annan myndighet ska lämna en uppgift som den förfogar över, om inte uppgiften är sekretessbelagd eller det skulle hindra arbetets behöriga gång. Något krav på att uppgiften ska finnas i en allmän handling uppställs alltså inte. Det är tillräckligt att myndigheten i fråga förfogar över uppgiften. Bestämmelsen anses vara en precisering av samverkansskyldigheten i 8 § första stycket FL.

4.2.5 Legalitetsprincipen m.m.

Legalitetsprincipen är grundlagsfäst genom 1 kap. 1 § regeringsformen, RF, som bl.a. anger att den offentliga makten utövas under lagarna. Bestämmelsen innebär att alla statsorgan vid all maktutövning är skyldiga att följa gällande bestämmelser i grundlagarna och i andra lagar och förordningar. Legalitetsprincipen innebär alltså att myndigheternas maktutövning i vidsträckt mening måste ha stöd i någon av de källor som tillsammans bildar rättsordningen.

Enligt 1 kap. 9 § RF ska domstolar samt förvaltningsmyndigheter och andra som fullgör offentliga förvaltningsuppgifter i sin verksamhet beakta allas likhet inför lagen samt iaktta saklighet och opartiskhet.

I 5 § första stycket FL sägs att en myndighet endast får vidta åtgärder som har stöd i rättsordningen. Bestämmelsen är tillämplig vid all förvaltningsverksamhet. I lagmotiven sägs att avsikten med be-

stämmelsen är att hindra myndigheterna från att agera helt vid sidan av sina i författning givna åligganden. Vidare uttalas att bestämmelsen tar sikte på de källor som tillsammans bildar rättsordningen i vidsträckt mening. För all typ av verksamhet som en myndighet bedriver krävs alltså någon form av normmässig förankring.[6]

Av 5 § andra stycket FL framgår att myndigheten i sin verksamhet ska vara saklig och opartisk. Vidare får myndigheten enligt 5 § tredje stycket FL ingripa i ett enskilt intresse endast om åtgärden kan antas leda till det avsedda resultatet. Åtgärden får aldrig vara mer långtgående än vad som behövs och får vidtas endast om det avsedda resultatet står i rimligt förhållande till de olägenheter som kan antas uppstå för den som åtgärden riktas mot. Det nyss sagda gäller generellt, dvs. även t.ex. för myndigheters informationshantering i den utsträckning den omfattar personuppgifter.

I dag är i princip all informationshantering som myndigheterna ägnar sig åt digitaliserad. Det innebär att dataskyddsregleringen, i första hand dataskyddsförordningen[7] och brottsdatalagen (2017:1177), BDL, i regel är tillämplig vid sådant informationsutbyte mellan myndigheter som omfattar personuppgifter.

4.2.6 Vidarebehandling av personuppgifter genom utlämnande till en annan myndighet

Finalitetsprincipen

Som utvecklas i avsnitt 3.2 utgör ett uppgiftslämnande från en myndighet till en annan ofta en vidarebehandling av uppgifter som den utlämnande myndigheten tidigare har samlat in för helt andra syften än att lämna ut uppgifterna. Ett utlämnande aktualiserar därför den s.k. finalitetsprincipen, som kommer till uttryck i artikel 5.1 b i dataskyddsförordningen och som innebär att personuppgifter ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål.

Dataskyddsförordningen ger dock utrymme för att i nationell rätt föreskriva att ytterligare behandling av personuppgifter får ske, även om vidarebehandlingen inte är förenlig med de eller det ända-

[6] Prop. 2016/17:180, *En modern och rättssäker förvaltning – Ny förvaltningslag*, s. 57–59.
[7] 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).

mål för vilket uppgifterna samlades in. Detta gäller särskilt om vidarebehandlingen sker i syfte att säkerställa viktiga allmänna intressen som anges i artikel 23.1 i dataskyddsförordningen. Sådana intressen är bl.a. förebyggande, förhindrande, utredning, avslöjande eller lagföring av brott eller verkställande av straffrättsliga sanktioner och andra viktiga mål av generellt allmänt intresse, särskilt viktiga ekonomiska eller finansiella intressen, däribland penning-, budget- eller skattefrågor, folkhälsa och social trygghet.

I svensk rätt föreskrivs tillåtligheten av vidarebehandling genom utlämnande i regel genom införandet av sekretessbrytande bestämmelser i offentlighets- och sekretesslagen eller uppgiftsskyldigheter i annan författning. Lagstiftaren har alltså genom bestämmelser om att uppgifter får eller ska lämnas ut tagit ställning till frågan om behandlingens förenlighet med finalitetsprincipen. I vissa fall är sådana bestämmelser ett uttryck för att ett utlämnande är förenligt med insamlingsändamålet. Sådana bestämmelser är dock regelmässigt ett uttryck för att en vidarebehandling genom utlämnande är tillåten *trots* att den inte är förenlig med insamlingsändamålet (jfr avsnitt 3.2.2).

Vidarebehandling (och ny behandling) enligt brottsdatalagen

Som nämns i avsnitt 5.5.1 finns särskilda bestämmelser i 2 kap. 4 § första stycket och 22 § första stycket BDL som innebär att personuppgifter får behandlas för nya ändamål såväl inom brottsdatalagens tillämpningsområde som utanför brottsdatalagens tillämpningsområde förutsatt att behandlingen föregås av att den behöriga myndigheten vid en särskild prövning finner att den är nödvändig och proportionerlig.[8] I den utsträckning skyldighet att lämna uppgifter följer av lag eller förordning ska dock någon sådan prövning inte göras enligt 2 kap. 4 § andra stycket och 22 § andra stycket BDL. Det innebär att om ett uppgiftslämnande sker enligt en bestämmelse som endast innebär en möjlighet att lämna ut uppgifter, ska det föregås av att den behöriga myndigheten prövar om utlämnandet är nödvändigt och proportionerligt. Detta bygger på den uppfattningen att lagstiftaren – om det endast finns en möjlighet att lämna ut uppgifter

[8] När behandling sker för ändamål utanför brottsdatalagens tillämpningsområde anses det inte utgöra en vidarebehandling utan en ”ny” behandling av personuppgifter, se prop. 2017/18:232, *Brottsdatalag*, s. 452.

– inte har tagit ställning till om uppgiftslämnandet är nödvändigt och proportionerligt (jfr dock vårt förslag i avsnitt 5.5.2).

Lagstiftarens sak att reglera vidarebehandling genom utlämnande

Som framgår av avsnitt 3.2 är en grundläggande förutsättning för att personuppgiftsbehandling över huvud taget ska vara laglig att den vilar på en rättslig grund. Kravet på en rättslig grund för personuppgiftsbehandling kan sägas vara en dimension av legalitetsprincipen som också framgår av annan lagstiftning.

När det gäller den behandling av personuppgifter som myndigheterna ägnar sig åt är det lagstiftarens sak att genom lagstiftning tillhandahålla den rättsliga grunden för behandlingen, oavsett om behandlingen omfattas av dataskyddsförordningen eller brottsdatalagen (jfr skäl 47 till dataskyddsförordningen). Detta gäller även för utlämnande av uppgifter till andra myndigheter. Exempelvis innebär bestämmelsen i 6 kap. 5 § OSL att lagstiftaren har tillhandahållit en rättslig grund för den personuppgiftsbehandling som en tillämpning av bestämmelsen föranleder, dvs. utlämnande av uppgifter som inte är sekretessbelagda till en annan myndighet som har begärt att få del av dem.

4.3 Uppgifter som enligt sekretessregleringen får lämnas ut

4.3.1 Uppgifter som inte är sekretessbelagda är offentliga uppgifter

Mot bakgrund av vårt uppdrag i denna del, dvs. att föreslå en bestämmelse som i större utsträckning gör det möjligt att på eget initiativ lämna ut *offentliga uppgifter* till en annan myndighet, finns det skäl att inledningsvis klargöra vad som i detta sammanhang bör omfattas av uttrycket offentliga uppgifter. Någon definition av uttrycket finns inte i offentlighets- och sekretesslagen. Rent allmänspråkligt borde uttrycket i första hand ta sikte på sådana uppgifter som får lämnas ut till var och en.

Enligt våra direktiv menas med ”offentliga uppgifter” sådana uppgifter som träffas av 6 kap. 5 § OSL, dvs. uppgifter som inte är sekretessbelagda (se även avsnitt 2.5.2). Offentliga uppgifter är därmed samma sak som uppgifter som inte är sekretessbelagda. Med offentliga uppgifter menas alltså uppgifter som inte är sekretessreglerade, uppgifter som omfattas av undantag från sekretess samt uppgifter som får lämnas ut efter en sekretessprövning eller enligt en sekretessbrytande bestämmelse. Det innebär att uppgifter som enligt sekretessregleringen får lämnas ut omfattas av begreppet. Eftersom uttrycket offentliga uppgifter har en särskild allmänspråklig betydelse kommer vi i detta sammanhang huvudsakligen använda oss av uttrycken *uppgifter som inte är sekretessbelagda* eller *uppgifter som får lämnas ut*.

4.3.2 Olika kategorier av uppgifter som inte är sekretessbelagda

Inledande anmärkning

Det finns flera olika förhållanden som kan leda till att en uppgift inte är sekretessbelagd. Enligt sekretessregleringen föreligger inte något hinder mot att lämna ut uppgifter som inte är sekretessbelagda. Annorlunda uttryckt råder det inte något förbud mot att röja en uppgift som inte är sekretessbelagd (jfr definitionen av sekretess i 3 kap. 1 § OSL).

Som vi redan påpekat är i princip all informationshantering som myndigheterna ägnar sig åt i dag digitaliserad. Det innebär att en uppgift som enligt sekretessregleringen inte är sekretessbelagd och därför får lämnas ut enligt den regleringen, bara kan lämnas ut under förutsättning att utlämnandet även sker i enlighet med dataskyddsregleringen. De två regelverken ska alltså tillämpas parallellt. Nedan redogörs enbart för vad som gäller enligt sekretessregleringen.

Uppgifterna är inte sekretessreglerade

I 3 kap. 1 § OSL definieras begreppet ”sekretess*reglerad* uppgift” som en uppgift för vilken det finns en bestämmelse om sekretess. Det finns uppgifter för vilka det inte finns någon bestämmelse om sekretess. Vissa uppgifter är alltså inte sekretessbelagda av den an-

ledningen att det inte finns någon sekretessbestämmelse som träffar uppgifterna. Det kan i sammanhanget nämnas att i 21 kap. 7 § OSL föreskrivs absolut sekretess för personuppgift om det kan antas att uppgiften efter ett utlämnande kommer att behandlas i strid med dataskyddsregleringen. Det innebär att det finns en sekretessbestämmelse som träffar alla personuppgifter, oavsett var de förekommer. Personuppgifter är därmed alltid sekretess*reglerade*, oavsett i vilket sammanhang de förekommer. Det är dock inte samma sak som att de alltid är sekretess*belagda*.

Uppgifterna omfattas av ett undantag från sekretess

Vissa uppgifter är inte sekretessbelagda av den anledningen att de är *undantagna* en materiell sekretessbestämmelse som annars hade träffat uppgifterna. Någon definition av vad som avses med begreppet ”undantag från sekretess” finns inte i offentlighets- och sekretesslagen. Vad som avses är dock bestämmelser som innebär att sekretess inte gäller i vissa sammanhang. Sådana bestämmelser om undantag från vad som annars föreskrivs finns i regel i anslutning till de materiella sekretessbestämmelserna.

Undantag från sekretess i offentlighets- och sekretesslagen gäller i flera fall för myndigheters beslut i olika frågor. När ett sådant undantag gäller är uppgifterna i beslutet (eller i de delar av beslutet som undantas från sekretess) inte sekretessbelagda. Som exempel kan nämnas bestämmelsen i 25 kap. 10 § OSL som har rubriken ”Undantag från sekretess” där det bl.a. anges att sekretessen enligt 1 § (hälso- och sjukvårdssekretessen) inte gäller i beslut i ärende enligt lagstiftningen om psykiatrisk tvångsvård eller rättspsykiatrisk vård, om beslutet avser frihetsberövande åtgärd. Undantag från sekretess kan också göras avseende vissa särskilt angivna myndigheters behov av uppgifter som annars är sekretessbelagda, eller behov som uppstår i särskilt angivna situationer.

Uppgifter som får lämnas ut efter en sekretessprövning

Uppgifter som får lämnas ut efter en *sekretessprövning* (även kallat menprövning eller skadeprövning) är inte heller sekretessbelagda. Om det t.ex. föreskrivs att sekretess gäller för en uppgift endast om

det av särskilda skäl finns anledning att anta att det uppkommer en skada av något slag om den lämnas ut, och några sådana särskilda skäl inte föreligger, är alltså uppgiften inte sekretessbelagd, utan får lämnas ut enligt sekretessregleringen.

Uppgifter som får lämnas ut med stöd av en sekretessbrytande bestämmelse

Uppgifter som får lämnas ut med stöd av en *sekretessbrytande bestämmelse* i offentlighets- och sekretesslagen är inte heller sekretessbelagda. Uppgifter som träffas av en sekretessbrytande bestämmelse (dvs. att rekvisiten i bestämmelsen är uppfyllda) är nämligen inte belagda med röjandeförbud och får därför lämnas ut.

Myndigheters uppgiftsutbyte regleras i många fall utanför offentlighets- och sekretesslagen, genom särskilda bestämmelser om uppgiftsskyldighet. Genom bestämmelsen i 10 kap. 28 § första stycket OSL, som anger att sekretess inte hindrar att en uppgift lämnas till en annan myndighet, om uppgiftsskyldighet följer av lag eller förordning, är uppgifter som träffas av en bestämmelse om uppgiftsskyldighet inte heller sekretessbelagda i förhållande till mottagaren om rekvisiten i bestämmelsen om uppgiftsskyldighet är uppfyllda.

Det kan nämnas att för utlämnande till enskilda finns ingen motsvarighet till 10 kap. 28 § OSL. För att en uppgiftsskyldighet eller en bestämmelse om att uppgifter får lämnas ut, som gäller i förhållande till enskilda och som regleras utanför offentlighets- och sekretesslagen, ska kunna bryta sekretess krävs därför att det hänvisas till den aktuella författningen i offentlighets- och sekretesslagen. Av 8 kap. 1 § OSL framgår nämligen att en uppgift för vilken sekretess gäller inte får röjas för enskilda eller för andra myndigheter, om inte annat anges i lagen eller i lag eller förordning som lagen hänvisar till. I anslutning till de materiella sekretessbestämmelserna är det därför vanligt förekommande med hänvisningar till författningar där uppgiftslämnande till enskilda regleras. Uppgifter som träffas av sådan hänvisad reglering är inte heller sekretessbelagda om förutsättningarna som anges där är uppfyllda.

4.3.3 Uppgifternas status i förhållande till mottagaren

Av det som sägs ovan följer att uppgifter kan få lämnas ut till en eller flera mottagare trots att de inte kan lämnas ut till var och en. Som exempel kan nämnas en annars sekretessbelagd uppgift som får lämnas ut från en myndighet till en annan med stöd av en sekretessbrytande bestämmelse. Om den sekretessbrytande bestämmelsen endast medger uppgiftslämnande två myndigheter emellan kan uppgifterna fortsatt vara sekretessbelagda i förhållande till enskilda och andra myndigheter än den mottagande myndighet som pekas ut i bestämmelsen. Uppgifterna är dock i så fall inte sekretessbelagda i förhållande till den utpekade, mottagande myndigheten.

Det innebär att frågan om en uppgift är sekretessbelagd eller inte alltid måste besvaras utifrån en konkret utlämnandesituation, och besvaras i förhållande till mottagaren. Uppgiftens rättsliga status som sekretessbelagd eller inte beror på alltså vilken myndighet som har uppgiften, vem mottagaren är, i vilket syfte utlämnandet sker och vad uppgiften rör.

4.4 Utformningen av uppgiftsskyldigheter

4.4.1 Allmänt

Uppgiftsskyldigheter skiljer sig från andra sekretessbrytande bestämmelser genom att de inte finns i offentlighets- och sekretesslagen, utan i annan författning. En uppgiftsskyldighet som regleras i lag eller förordning har en sekretessbrytande verkan enligt 10 kap. 28 § första stycket OSL. Bestämmelser om uppgiftsskyldighet mellan myndigheter brukar sägas vara ett sätt för lagstiftaren att reglera ett ofta förekommande informationsutbyte och att säkerställa att den mottagande myndigheten ges tillgång till de uppgifter som behövs i dennas verksamhet. En uppgift som träffas av en bestämmelse om uppgiftsskyldighet är alltså inte sekretessbelagd i förhållande till den mottagare som anges i bestämmelsen, under förutsättning att samtliga rekvisit som anges i bestämmelsen är uppfyllda.

Uppgiftsskyldigheter kan dock även avse uppgifter som annars inte är sekretessbelagda. Det är alltså inte nödvändigt att en bestämmelse om uppgiftsskyldighet ursprungligen har utformats med tanke på att uppgifterna är sekretessbelagda. Däremot krävs att

bestämmelsen uppfyller vissa krav på konkretion för att kunna bryta sekretess. Den kan ta sikte på utlämnande av uppgifter av ett speciellt slag, gälla en viss myndighets rätt att ta del av uppgifter i allmänhet, eller avse en skyldighet för en viss myndighet att lämna andra myndigheter information.[9]

Bestämmelsen i 6 kap. 5 § OSL medför en skyldighet att lämna ut uppgifter som inte är sekretessbelagda om en annan myndighet begär att få del av uppgifterna, så länge det inte hindrar arbetets behöriga gång. Skyldigheten som uppstår genom bestämmelsen är dock av en annan karaktär än de ”vanliga” uppgiftsskyldigheter som ofta tar sikte på mer avgränsade kategorier av uppgifter och som ofta utformats i syfte att bryta sekretess.

Bestämmelsen i 6 kap. 5 § OSL anses snarare utgöra en precisering av den allmänna samverkansskyldighet som gäller för myndigheter enligt 8 § FL och kan primärt sägas reglera ett generellt rättsligt förhållande mellan myndigheter, dvs. principen att alla myndigheter är skyldiga att samarbeta med och bistå varandra i den utsträckning som är möjlig, där utbyte av information är ett viktigt led. Den generella skyldigheten begränsas som utgångspunkt av sekretessregleringen, vilket framgår av att 6 kap. 5 § OSL enbart avser uppgifter som *inte är sekretessbelagda*. En mer långtgående skyldighet kan alltså följa av särskilda uppgiftsskyldigheter i lag eller förordning.[10] Det är sådana särskilda uppgiftsskyldigheter som avses i avsnitten nedan (se även exempel i SOU 2024:63, avsnitten 3.4.4, 5.1.6, 8.4.2 och 8.5.2).

4.4.2 Uppgiftsskyldigheter på begäran

Många bestämmelser om uppgiftsskyldighet är utformade på så sätt att den utlämnande myndigheten ska lämna vissa uppgifter till mottagaren på den mottagande myndighetens begäran. I likhet med 6 kap. 5 § OSL kräver sådana bestämmelser att det är den mottagande myndigheten som på så sätt initierar utlämnandet.

När uppgifterna som träffas av bestämmelsen om uppgiftsskyldighet är sekretessbelagda innebär det att ett sekretessgenombrott sker först i samband med att en mottagande myndighet har framställt en begäran om att få del av uppgifterna. Utan en sådan begäran är upp-

[9] Prop. 1979/80:2, *med förslag till sekretesslag m.m.*, Del A, s. 322.
[10] Prop. 1979/80:2, *med förslag till sekretesslag m.m.*, Del A, s. 89 och 361.

gifterna fortsatt sekretessbelagda, oavsett om övriga rekvisit för utlämnandet är uppfyllda.

Uppgiftsskyldigheter som är utformade på ett sådant sätt att det kvävs en begäran för utlämnandet kan alltså inte tillämpas om den mottagande myndigheten inte har begärt att få del av de uppgifter som avses, oavsett om uppgifterna annars varit sekretessbelagda eller inte.

Som vi redan nämnt är bestämmelser om uppgiftsskyldighet normalt ett sätt för lagstiftaren att se till att den mottagande myndigheten ges del av uppgifter som behövs i dennas verksamhet. Ordalydelsen i bestämmelser om uppgiftsskyldighet på begäran omfattar därför många gånger också ett behovsrekvisit, dvs. uppgifterna ska *behövas* hos mottagaren i ett visst sammanhang, och normalt anges även vilka uppgifter som avses. Vid prövningen av om en uppgift behövs eller inte bör emellertid den utlämnande myndigheten kunna utgå ifrån att den begärande myndigheten behöver uppgifterna om den gör gällande att så är fallet.[11]

Variationen i hur bestämmelser om uppgiftsskyldighet är utformade är dock mycket stor. I vissa bestämmelser som gäller uppgiftslämnande mellan två utpekade myndigheter anges inte över huvud taget vilka kategorier av uppgifter som avses, utan endast vilket behov hos mottagaren som ska föreligga för att utlämnande ska få ske. I andra bestämmelser anges inte vilket behov som ska föreligga hos mottagaren utan enbart att vissa kategorier av uppgifter ska lämnas ut om mottagaren begär det. I dessa fall förefaller behovsrekvisitet har ersatts av kravet på en begäran. En sådan reglering bör normalt ha utformats utifrån antagandet att en mottagande myndighet inte begär ut uppgifter som den inte har en legitim grund för att ta del av. Motsatsvis förekommer det också bestämmelser som är mycket detaljerade både vad avser vilka behov som ska föreligga hos mottagaren och vilka uppgifter som avses.[12]

Gemensamt för samtliga bestämmelser om uppgiftsskyldighet på begäran är dock kravet på en begäran från mottagaren. Det motiveras normalt av integritets- och dataskyddsrättsliga skäl. Det kan t.ex. handla om att säkerställa att samtliga uppgifter som avses i bestämmelsen inte alltid lämnas till mottagaren, eftersom denna kan ha

[11] Se bl.a. prop. 1979/80:2, *med förslag till sekretesslag m.m.*, Del A s. 323 f. och SOU 2024:53, *Stöd till invandrares utvandring*, s. 514.
[12] Jfr SOU 2023:100, *Framtiden dataskydd – Vid Skatteverket, Tullverket och Kronofogden*, s. 942–946.

varierande behov över tid i fråga om vilka slags uppgifter som behöver hämtas in, beroende på verksamhetens inriktning för tillfället. Genom att föreskriva att sekretess bryts först efter en begäran begränsas mängden uppgifter till att endast avse de uppgifter som den mottagande myndigheten vet är relevanta för verksamheten vid den aktuella tidpunkten.[13]

Att ett uppgiftslämnande ska ske på begäran innebär dock i regel inget hinder mot att en mottagande myndighet framställer en ”stående begäran” om viss information som omfattas av en bestämmelse om uppgiftsskyldighet, eller att den utlämnande och den mottagande myndigheten avtalar om aviseringar av ändrade uppgifter, löpande utlämnande med olika intervall, utlämnande genom automatiserade händelsebaserade tjänster eller genom prenumerationer.[14] Om en uppgiftsskyldighet är utformad med ett krav på en begäran föreligger dock ett hinder mot utlämnande helt på den utlämnande myndighetens egna initiativ, t.ex. redan när det finns *ett antagande* om att uppgifterna behövs hos mottagaren. Någon form av ursprunglig begäran måste alltså föregå utlämnandet, även om denna inte framställts i direkt anslutning till utlämnande i det enskilda fallet.

4.4.3 En anmärkning om uppgiftsskyldigheter på begäran

Även om den generella sekretessbrytande bestämmelsen som vi föreslog i SOU 2024:63 införs, och det därmed kommer finnas ett stöd för utlämnande på eget initiativ av annars sekretessbelagda uppgifter genom den bestämmelsen, så kommer visst informationsutbyte av annars sekretessbelagda uppgifter inte träffas av den. Så är bl.a. fallet för sekretess som är undantagen bestämmelsens tillämpningsområde, vid informationsutbyte för andra syften än de som anges i bestämmelsen och i sådan verksamhet eller sådana situationer där övervägande skäl talar för att upprätthålla sekretessen och bestämmelsen av den anledningen inte blir tillämplig.

Det innebär att oavsett vilka förslag vi lämnar i den här delen av vårt uppdrag så kommer det finnas sammanhang där det även i fortsättningen finns ett förbud mot att lämna ut relevanta uppgifter på eget initiativ och där sekretessgenombrott sker först i enlighet med

[13] Jfr t.ex. prop. 2022/23:34, *Utbetalningsmyndigheten*, s. 94.
[14] Jfr SOU 2023:100, *Framtiden dataskydd – Vid Skatteverket, Tullverket och Kronofogden*, s. 940.

en bestämmelse om uppgiftsskyldighet på begäran. Det kan alltså vara så att en myndighet som förfogar över vissa sekretessbelagda uppgifter i princip *vet* att uppgifterna är av betydelse för en annan myndighets verksamhet. Man kan samtidigt ha en *skyldighet* att lämna ut uppgifterna på begäran, dvs. med stöd av en uppgiftsskyldighet som kräver en begäran från mottagaren. Den potentiella mottagaren har dock *ingen kännedom* om att uppgifterna finns, och framställer därför ingen begäran. Den utlämnande myndigheten är dock *förhindrad* att lämna ut uppgifterna på eget initiativ, eftersom sekretessgenombrottet förutsätter en begäran.[15] I dag förefaller den beskrivna situationen vara ganska vanligt förekommande, vilket framgår av den kartläggning vi genomfört och som redovisas i avsnitt 4.7 nedan.

Någon möjlighet att i den situationen lämna ut uppgifter på eget initiativ med stöd av generalklausulen i 10 kap. 27 § OSL finns rimligen inte heller. Generalklausulen är nämligen subsidiär i förhållande till andra sekretessbrytande bestämmelser. Har det föreskrivits att en viss myndighet bara får ta del av annars sekretessbelagda uppgifter hos en annan myndighet om särskilda villkor är uppfyllda är det alltså inte tillåtet att lämna ut uppgifterna med stöd av generalklausulen om villkoren *inte* är uppfyllda.[16]

4.4.4 Uppgiftsskyldigheter på eget initiativ

Det förekommer också att myndigheter har en skyldighet att *utan* en begäran från mottagaren lämna uppgifter till en annan myndighet. Även sådana bestämmelser bryter eventuell förekommande sekretess. Precis som i bestämmelser om uppgiftsskyldighet på begäran pekas den mottagande myndighetens antagna behov av uppgifterna normalt ut i bestämmelser om uppgiftsskyldighet utan föregående begäran. Vilket behov mottagaren ska ha av uppgifterna kan dock vara mer eller mindre detaljerat angivet. I dessa fall blir dock annars sekretessbelagda uppgifter inte sekretessbelagda i förhållande till mottagaren redan när de (behovs)rekvisit som anges i bestämmelsen föreligger. Uppgiftsskyldigheter som inte kräver en begäran från mottagaren kan självfallet även avse uppgifter som annars inte är sekretessbelagda.

[15] Jfr Justitieombudsmannens kritik mot en socialsekreterare som på eget initiativ lämnat ut sekretesskyddad uppgift till Försäkringskassan i 1999/2000:JO1 s. 374.
[16] Se prop. 1979/80:2, *med förslag till sekretesslag m.m.*, Del A, s. 328.

Eftersom någon begäran inte krävs för ett utlämnande i dessa fall är det i stället vanligt förekommande att ett rekvisit för utlämnande är att uppgifterna *kan antas* behövas för viss verksamhet hos mottagaren. När en uppgift får lämnas ut redan när det kan antas att den har betydelse för mottagaren innebär det att tröskeln för utlämnandet är lågt satt.[17]

Även om en bestämmelse om uppgiftsskyldighet inte innehåller något krav på en begäran kan den trots det vara utformad på ett sätt som medför att uppgifter inte kan lämnas ut utan någon form av föregående samverkan mellan utlämnande och mottagande myndigheter. Det är t.ex. fallet när en uppgiftsskyldighet avser uppgifter som *behövs* i en särskilt angiven situation hos mottagaren. För att utlämnandet ska vara tillåtet i sådana fall krävs att den utlämnande myndigheten försäkrat sig om att de uppgifter som kan bli aktuella att lämna ut verkligen är av vikt för mottagaren, och behövs i den situation som avses i bestämmelsen. Beroende på utformningen av en uppgiftsskyldighet som inte uttryckligen kräver en begäran från den mottagande myndigheten kan ett utlämnande därmed ändå kräva att den mottagande myndigheter framställt motsvarande en begäran om att få del av vissa uppgifter.[18]

En bestämmelse om uppgiftsskyldighet som inte innehåller något krav på en begäran kan också avse en skyldighet att på eget initiativ uppmärksamma en mottagande myndighet om vissa förhållanden, eller anmäla misstanke om ett missförhållande. I sådana fall kan det röra sig om direkta underrättelseskyldigheter, där det klart framgår att det är den utlämnande myndigheten som ska ta initiativ till utlämnandet så snart förutsättningarna för utlämnandet i övrigt är uppfyllda.

[17] Jfr t.ex. prop. 2020/21:160, *Säkrare samordningsnummer och bättre förutsättningar för korrekta uppgifter i folkbokföringen*, s. 34 och 35.
[18] Jfr bl.a. prop. 2000/01:129, *Ökat informationsutbyte mellan arbetslöshetsförsäkringen, socialförsäkringen och studiestödet*, s. 60 och prop. 2007/08:160, *Utökat elektroniskt informationsutbyte*, s. 55, 56 och 80, samt bilaga 2 författningsförslag 17.

4.5 Varför har myndigheter ibland en skyldighet att lämna ut uppgifter på eget initiativ?

4.5.1 Ett urval av uppgiftsskyldigheter ur befintlig regering

Bestämmelser om uppgiftsskyldighet på begäran, liksom bestämmelsen i 6 kap. 5 § OSL, förutsätter att mottagaren har framställt en begäran om att få del av uppgifterna. På så sätt säkerställs bl.a. att enbart de uppgifter som den mottagande myndigheten vet är relevanta lämnas ut till denna. Frågan är då varför lagstiftaren i vissa fall valt att frångå detta synsätt till förmån för ett utlämnande på initiativ av den utlämnande myndigheten.

Syftet med att införa bestämmelser om uppgiftsskyldighet utan föregående begäran varierar självfallet beroende på sammanhanget. Om sådana bestämmelser ska kunna bryta eventuell sekretess måste de emellertid utformas som en *skyldighet*, eftersom enbart en möjlighet att lämna information inte bryter sekretess enligt 10 kap. 28 § första stycket OSL.

Nedan ges några exempel på motiven bakom sådan lagstiftning som möjliggör uppgiftslämnande på initiativ av den utlämnande myndigheten. Exemplen utgör enbart ett begränsat urval och det finns långt fler exempel än nedanstående på lagstiftning som innebär att en myndighet har en skyldighet att på eget initiativ upplysa en annan myndighet om ett visst förhållande. Urvalet nedan ger dock en bild av i vilka situationer, och varför, uppgiftslämnande på eget initiativ kan vara påkallat.

4.5.2 Folkbokföringen

När den reglering som i dag finns i 32 c § folkbokföringslagen (1991:481) gavs sin nuvarande utformning fick i princip samtliga myndigheter en skyldighet att underrätta Skatteverket *om det kan antas* att en uppgift i folkbokföringen är felaktig eller ofullständig, om inte särskilda skäl talar emot en sådan underrättelse. I det sammanhanget noterade regeringen att den ökade förekomsten av identitetsmissbruk har inneburit att Skatteverkets folkbokföringsverksamhet på kort tid ändrat karaktär från en registrerande myndighet, till grindvakt för välfärdssystemen. Även om Skatteverket hade identifierat indikatorer för olika typer av identitetsmissbruk bedömde

regeringen att det var svårt för Skatteverket att avgöra om en identitet var en missbrukad identitet eller inte, enbart med information från folkbokföringsverksamheten. Enligt regeringen behövs det ofta uppgifter även från andra myndigheter och verksamheter. Även för de uppgifter om identitet, familj och andra förhållanden som registreras i folkbokföringsdatabasen kunde det enligt regeringen finnas andra aktörer som har information av betydelse för att de uppgifter som registreras är korrekta.[19]

4.5.3 Skatteverkets brottsbekämpande verksamhet

Enligt den nyligen upphävda 7 § lagen (1997:1024) om Skatteverkets brottsbekämpande verksamhet hade Skatteverkets beskattningsverksamhet, folkbokföringsverksamhet och id-kortsverksamhet en skyldighet att lämna uppgifter till myndighetens brottsbekämpande verksamhet om uppgifterna *kan antas* ha samband med viss misstänkt brottslig verksamhet.[20] Skatteverkets brottsbekämpande verksamhet har enligt 8 § samma lag fortfarande en skyldighet att lämna sådana uppgifter som *kan antas* ha särskild betydelse för ett ärende i de ovan angivna verksamheterna. I förarbetena uttalade regeringen att det interna informationsutbytet inom en myndighet är särskilt viktigt för en myndighet som Skatteverket som bedriver både brottsbekämpande verksamhet och annan verksamhet såsom beskattning och folkbokföring. Inom Skatteverkets brottsbekämpande verksamhet kunde det enligt regeringen komma fram information som är till nytta i ärenden i annan verksamhet inom myndigheten, t.ex. i form av uppgifter som tyder på att en verksamhet inte har beskattats trots att detta borde ha skett eller att registrerade folkbokföringsuppgifter är felaktiga. Ett väl fungerande utbyte av information inom myndigheten uttalades därmed vara viktigt för att Skatteverket ska kunna fatta korrekta beslut i fråga om bl.a. skatt, folkbokföring och id-kort. Enligt regeringen upptäckte folkbokföringsverksamheten dessutom inte sällan uppgifter om misstänkt brottslig verksamhet som den brottsbekämpande verksamheten skulle ha nytta av. Ett

[19] Prop. 2020/21:160, *Säkrare samordningsnummer och bättre förutsättningar för korrekta uppgifter i folkbokföringen*, s. 32 och 33.
[20] Regleringen av informationsutbytet mellan Skatteverkets olika verksamhetsgrenar har mycket nyligen ändrats i enlighet med förslagen i prop. 2024/25:65, *Ökat informationsflöde till brottsbekämpningen*. Bl.a. har 7 § upphävts eftersom utlämnandet numera regleras i annan ordning, se Justitieutskottets betänkande 2024/25:JuU9, *Ökat informationsflöde till brottsbekämpningen*.

väl fungerande informationsutbyte mellan olika verksamheter inom Skatteverket var därför enligt regeringen också av stor betydelse för myndighetens möjligheter att bekämpa brott.[21]

4.5.4 Socialtjänstlagen

Enligt 11 kap. 11–11 b §§ socialtjänstlagen (2001:453) har flera myndigheter en skyldighet att lämna vissa uppgifter till socialtjänsten på eget initiativ *om det finns skäl för det*. I förarbetena till bestämmelserna konstaterade regeringen bl.a. att regleringen av när ekonomiskt bistånd kan utgå innebär att socialnämnden måste kartlägga att den biståndssökande har utnyttjat alla möjligheter som normalt stå till buds att försörja sig själv. Det var enligt regeringens mening självklart att kontroller måste kunna utföras och genom ett utökat informationsutbyte skulle de nödvändiga kontrollerna kunna ske mycket effektivare, vilket enligt regeringen var angeläget mot bakgrund av redovisade felaktiga utbetalningar. Ett informationsutbyte som grundade sig på en uppgiftsskyldighet skulle dessutom i praktiken inte innebära någon större skillnad jämfört med den befintliga systematiken där samtycke till kontrollerna inhämtades från de sökande. Det kunde nämligen enligt regeringen ifrågasättas om den enskildes samtycke till att socialnämnden hämtade in uppgifter från andra myndigheter i egentlig mening var frivilligt. Om samtycke inte lämnades var nämligen risken uppenbar att biståndsansökan inte beviljades eftersom socialnämnden då inte kunde utreda den enskildes behov av bistånd.[22]

Enligt 14 kap. 1 § socialtjänstlagen är vissa myndigheter och yrkesverksamma skyldiga att genast till socialnämnden anmäla om de i sin verksamhet *får kännedom om* eller *misstänker* att ett barn far illa. Regeringen har uttalat att syftet med bestämmelsen är att säkerställa att socialnämnden så snart som möjligt får kännedom om när en underårig far illa i hemmet. En av socialtjänstens viktigaste uppgifter är att se till att barn och ungdomar, som befinner sig i en utsatt situation, får den vård och det skydd som de behöver. För att kunna fylla denna funktion behövde socialnämnden, enligt regeringen, ha möjlighet att få uppgifter om och utreda den unges situation och

[21] Prop. 2019/20:166, *Extra ändringsbudget för 2020 – Fler kraftfulla åtgärder med anledning av coronaviruset*, s. 73.
[22] Prop. 2007/08:160, *Utökat elektroniskt informationsutbyte*, s. 140–143.

behov av hjälp. Regeringen uttalade även att socialnämnden i dessa sammanhang ofta är beroende av i vilken utsträckning man kan få uppgifter från andra myndigheter och befattningshavare som kommit i kontakt med den unge och dennas familj.[23]

4.5.5 Felaktiga utbetalningar från välfärdssystemen

Kommuner, flera statliga myndigheter och arbetslöshetskassorna har en underrättelseskyldighet enligt lagen (2008:206) om underrättelseskyldighet vid felaktiga utbetalningar från välfärdssystemen. Skyldigheten gäller när det *finns anledning att anta* att en felaktighet uppstått och det är den organisation som fattat besluten som ska motta underrättelsen.[24] I lagens förarbeten uttalade regeringen att det kan uppfattas som mycket stötande, såväl av den myndighetstjänsteman som upptäcker en felutbetalning hos en annan myndighet som av medborgare i allmänhet att underrättelse om detta inte får lämnas till den myndighet som kan åtgärda felaktigheten. Till följd av detta kan en enskild fortsätta att begå omfattande bidragsbrottslighet riktad mot en myndighet trots att en annan myndighet känner till att detta pågår. Det var enligt regeringen angeläget för medborgarnas tilltro till välfärdssystemen att sådana situationer förhindras. Att felaktiga utbetalningar förhindrades kunde också vara till gagn för den enskilde mottagaren av en utbetalning. Genom en underrättelseskyldighet kunde det undvikas att en stor skuld, och ett stort återkrav, ackumulerades.[25]

4.5.6 Utbetalningsmyndigheten

Utbetalningsmyndigheten har en underrättelseskyldighet till flera myndigheter enligt bestämmelserna 3 kap. lagen (2023:455) om Utbetalningsmyndighetens granskning av utbetalningar. I de flesta fall rör bestämmelserna felaktiga uppgifter eller andra förhållanden och underrättelse ska lämnas så snart det finns *anledning att anta*

[23] Prop. 1989/90:28, *om vård i vissa fall av barn och ungdomar*, s. 101 och 102.
[24] I SOU 2024:24, *Ett effektivt straffrättsligt skydd för statliga stöd till företag,* har föreslagits att underrättelseskyldigheten ska utvidgas till att omfatta även regionerna av samma skäl, dvs. att regionerna har tillgång till uppgifter som kan indikera att välfärdsförmåner betalas ut felaktigt.
[25] Prop. 2007/08:48, *Underrättelseskyldighet vid felaktiga utbetalningar från välfärdssystemen*, s. 18 och 19.

att ett visst förhållande föreligger som har betydelse för en särskild myndighets verksamhet. I förarbetena uttalade regeringen bl.a. att uppgifter i Bolagsverkets register som inte speglar verkliga förhållanden kan, om de inte rättas, leda till att efterföljande beslut om ekonomiskt stöd blir felaktiga. Ett exempel på detta var om det fanns anledning att anta att ett aktiebolags registrerade företrädare i själva verket är en s.k. målvakt. Om Utbetalningsmyndigheten upptäcker sådana misstänkt felaktiga uppgifter skulle det därför vara värdefullt för Bolagsverket att bli underrättade om detta. Vidare bedömde regeringen att om det t.ex. fanns anledning att anta att ett assistansbolag använder sig av målvakter eller har fiktiva anställningar är det av stor vikt att sådan information även kan nå tillsynsmyndigheten, dvs. Inspektionen för vård och omsorg, IVO. För att IVO ska kunna bedriva sitt tillsynsarbete över tillståndshavare effektivt krävdes enligt regeringen att myndigheten får kännedom om omständigheter som gör att tillståndet skulle kunna ifrågasättas. Regeringen ansåg att det var motiverat att Utbetalningsmyndigheten hade möjlighet att underrätta IVO om misstänkta felaktigheter. Om det framkommer uppgifter som ger anledning för Utbetalningsmyndigheten att anta att t.ex. ett arbetstillstånd är felaktigt var det enligt regeringen också viktigt att den informationen når Migrationsverket, så att den senare myndigheten kan förhindra att utbetalningar av välfärdsmedel går till en person som egentligen inte har rätt till sådana utbetalningar. Sådan information kunde enligt regeringen även förhindra att personer utnyttjas av oseriösa arbetsgivare. Utbetalningsmyndigheten skulle därför vara skyldig att underrätta Migrationsverket om det finns anledning att anta att ett beviljat tillstånd enligt utlänningslagen (2005:716) är felaktigt.[26]

4.5.7 LUFFA-lagen

Genom bestämmelserna i lagen (2024:307) om uppgiftsskyldighet för att motverka felaktiga utbetalningar från välfärdssystemen samt fusk, regelöverträdelser och brottslighet i arbetslivet, LUFFA-lagen, har vissa statliga myndigheter samt kommuner och arbetslöshetskassor som utgångspunkt en skyldighet att på eget initiativ lämna en uppgift som den förfogar över till en annan av dessa aktörer *om*

[26] Prop. 2022/23:34, *Utbetalningsmyndigheten*, s. 63 och 64.

uppgiften behövs i den mottagande aktörens författningsreglerade verksamhet för att säkerställa korrekta beslutsunderlag för att förebygga, förhindra, upptäcka eller utreda felaktiga utbetalningar från välfärdssystemen. I förarbetena noterade regeringen bl.a. att det i många fall saknas en rättslig grund enligt dataskyddsförordningen som tillåter att uppgifter som inte är sekretessbelagda lämnas på eget initiativ och att ett vanligt problem i samband med uppgiftsutbyte är att en myndighet inte alltid har kännedom om att en annan myndighet har uppgifter som skulle kunna vara av betydelse för den förstnämnda myndigheten. Enligt regeringen kan det i och för sig ofta vara motiverat att utforma en uppgiftsskyldighet som att ett uppgiftslämnande får ske först efter begäran. Behovet av en viss uppgift kan t.ex. variera hos en aktör och sekretessbelagda uppgifter ska inte spridas mer än vad som är motiverat. Enligt regeringen är dock vissa uppgifter av sådan art att de behövs för att säkerställa att ett beslutsunderlag bygger på tillräckliga och korrekta uppgifter. Om en aktör inte får del av sådana uppgifter finns det enligt regeringen risk att beslut fattas på felaktiga grunder eller att ändrade förhållanden inte uppmärksammas. Regeringen uttalade även att goda förutsättningar för myndigheter, kommuner och arbetslöshetskassor att fatta korrekta beslut och genomföra effektiva kontroller är avgörande för att långsiktigt kunna upprätthålla tilltron till den offentliga förvaltningen i allmänhet och välfärdssystemen i synnerhet. Det är även av central betydelse för att motverka fusk, regelöverträdelser och brottslighet i arbetslivet. Enligt regeringen fanns det därför ett stort behov av att aktörer som förfogar över sådana uppgifter lämnar ut dessa på eget initiativ.[27]

4.6 Det generella rättsliga stödet för att lämna ut uppgifter på eget initiativ

4.6.1 Sekretessbelagda uppgifter som får lämnas ut med stöd av en sekretessbrytande bestämmelse i OSL

De sekretessbrytande bestämmelserna i offentlighets- och sekretesslagen är utformade på det sättet att sekretess *inte hindrar* ett visst uppgiftslämnande, om rekvisiten i bestämmelsen är uppfyllda.

[27] Prop. 2023/24:85, *En ny lag om uppgiftsskyldighet för att motverka felaktiga utbetalningar från välfärdssystemen samt fusk, regelöverträdelser och brottslighet i arbetslivet*, s. 27, 28 och 32.

Bestämmelserna innebär alltså en möjlighet men inte någon *skyldighet* att lämna ut uppgifter på eget initiativ. Bestämmelserna innebär – vilket vi har redogjort för i vårt delbetänkande – att myndigheter har ett rättsligt stöd för att lämna ut annars sekretessbelagda uppgifter som träffas av bestämmelserna på eget initiativ (se SOU 2024:63, avsnitt 6.4). För uppgifter som träffas av en sekretessbrytande bestämmelse i offentlighets- och sekretesslagen krävs det alltså inte något ytterligare rättsligt stöd för att ett utlämnande på eget initiativ ska vara tillåtet.

4.6.2 Sekretessbelagda och inte sekretessbelagda uppgifter som får lämnas ut med stöd av en uppgiftsskyldighet

Som vi redan nämnt är det inte nödvändigt att en bestämmelse om uppgiftsskyldighet ursprungligen har utformats med tanke på att uppgifterna är sekretessbelagda. Det innebär att uppgiftsskyldigheter även kan avse uppgifter som annars inte är sekretessbelagda.

Att uppgiftsskyldigheter är utformade på olika sätt, och ibland även tillåter uppgiftslämnande på eget initiativ framgår av avsnitten 4.4 och 4.5 ovan. Det förhållandet att ett utlämnande på eget initiativ har stöd i en bestämmelse om uppgiftsskyldighet innebär, på samma sätt som om en uppgift lämnas ut med stöd av en sekretessbrytande bestämmelse i offentlighet och sekretesslagen, att det finns rättsligt stöd för sådana utlämnanden och att det finns en rättslig grund i dataskyddsrättslig mening för den personuppgiftsbehandling som föranleds av dessa utlämnanden.

4.6.3 Uppgifter som inte är sekretessbelagda och inte träffas av någon sekretessbrytande bestämmelse

Utöver de uppgifter som nämns ovan finns uppgifter som det enligt sekretessregleringen inte finns något förbud mot att röja, och som därför får lämnas ut, t.ex. uppgifter som inte är sekretessreglerade, uppgifter som redan är undantagna från sekretess eller uppgifter som inte är sekretessbelagda på grund av att en materiell sekretessbestämmelsen efter en prövning tillåter ett utlämnande (se avsnitt 4.3). Sådana uppgifter träffas av naturliga skäl inte av någon sekretessbrytande bestämmelse.

Om dessa uppgifter inte heller träffas av en bestämmelse om uppgiftsskyldighet som medger ett utlämnande till en annan myndighet på eget initiativ, så är de enda befintliga bestämmelserna som kan uppfattas ge stöd för utlämnandet de generella bestämmelserna om myndigheters samverkan. Som nämns i avsnitt 4.2.4 gäller t.ex. enligt 8 § första stycket FL att en myndighet inom sitt verksamhetsområde ska samverka med andra myndigheter. I lagmotiven nämns som exempel på en situation som bestämmelsen tar sikte på att myndigheter samråder och lämnar varandra upplysningar eller bistår med särskild sakkunskap genom informella kontakter per telefon eller vid möten.[28] Den regleringen ger dock inget uttryckligt stöd för utlämnande av uppgifter till en annan myndighet.

När det inte finns något rättsligt stöd för ett utlämnande av uppgifter till en annan myndighet finns det inte heller någon rättslig grund i dataskyddsrättslig mening för den personuppgiftsbehandling som ett sådant utlämnande skulle innebära. Det innebär att en myndighet ofta saknar möjlighet att på eget initiativ lämna uppgifter som annars inte är sekretessbelagda till en annan myndighet.

4.7 Myndigheters behov av att lämna ut uppgifter på eget initiativ

4.7.1 Ett rörligt och svårfångat förhållande

Ett situationsbundet rättsligt tillstånd

Under de senaste åren har det tillsats ett stort antal statliga utredningar som har haft till uppgift att utreda och kartlägga behovet av uppgiftsutbyte mellan olika offentliga aktörer. Till detta kommer att myndigheter också i viss utsträckning själva har uppmärksammat regeringen på behovet av förbättrade möjligheter att utbyta uppgifter. I vårt delbetänkande görs en genomgång av ett urval av kartläggningar m.m. som pågår eller har genomförts (se SOU 2024:63, avsnitt 4.2).

I dessa sammanhang är föremålet för undersökningarna ofta om det behöver genomföras förändringar i sekretessregleringen för att tillgodose framförda behov. Det är alltså, såvitt vi kunnat se, inte särskilt vanligt att behoven av att utbyta uppgifter som inte är sekretess-

[28] Prop. 2016/17:180, *En modern och rättssäker förvaltning – ny förvaltningslag*, s. 71.

belagda undersöks. Frågan om en uppgift är sekretessbelagd eller inte är också något som avgörs i en konkret utlämnandesituation och svaret påverkas bl.a. av förekomsten av sekretessbrytande bestämmelser och bestämmelser om undantag från sekretess. Det rättsliga tillståndet att en uppgift inte är sekretessbelagd i förhållande till mottagaren är alltså *situationsbundet*. I många fall borde det alltså inte vara möjligt att på förhand klassificera uppgifter som antingen sekretessbelagda eller inte sekretessbelagda. Snarare är det så att vissa uppgifter ofta inte är sekretessbelagda och att andra uppgifter ofta är sekretessbelagda, beroende på omständigheterna i det enskilda fallet vad gäller t.ex. om en begäran har framställts eller inte, och i sådant fall av vem. Detta har förmodligen bidragit till att det inte alltid är helt tydligt om de behov av förbättrade möjligheter till informationsutbyte som framkommit i olika sammanhang avser uppgifter som oftast är sekretessbelagda eller uppgifter som oftast inte är sekretessbelagda.

Vår utgångspunkt – behovet av att lämna ut uppgifter på eget initiativ

Bestämmelsen i 6 kap. 5 § OSL innebär att uppgifter som inte är sekretessbelagda ska lämnas ut *på begäran* av en annan myndighet. Någon motsvarande och generellt tillämplig bestämmelse som ger ett tydligt stöd för utlämnande av uppgifter som inte är sekretessbelagda till en annan myndighet *på eget initiativ* finns inte i offentlighets- och sekretesslagen. En central fråga är därför om det finns ett faktiskt behov av utökade möjligheter att på den utlämnande myndighetens initiativ lämna ut uppgifter som inte är sekretessbelagda till andra myndigheter.

Frågan om det på ett generellt plan finns ett behov av utökade möjligheter att lämna ut uppgifter som inte är sekretessbelagda på eget initiativ är dock komplex. Å ena sidan har vi lämnat förslag på en ny bestämmelse i offentlighets- och sekretesslagen som, om den införs, innebär att det kommer finnas ett rättsligt stöd för att lämna ut en stor mängd annars sekretessbelagda uppgifter på eget initiativ till andra myndigheter. Å andra sidan är många befintliga bestämmelser om uppgiftsskyldighet utformade på ett sådant så sätt att en begäran måste framställas för att ett sekretessgenombrott alls ska ske. Därtill kommer att flera myndigheter hanterar stora mängder

uppgifter om enskilda som enbart i undantagsfall är sekretessbelagda, och där möjligheten att lämna ut uppgifter på eget initiativ därför inte påverkas i särskilt hög utsträckning av några sekretessbrytande bestämmelser, oavsett hur dessa är utformade.

Försök att kartlägga förekomsten av ett generellt behov av utökade möjligheter att på eget initiativ lämna uppgifter som inte är sekretessbelagda till andra myndigheter kräver alltså en kartläggning av både ett rörligt och svårfångat rättsligt förhållande. Det mest ändamålsenliga förhållningssättet bör därför vara att fokusera på det senare ledet i frågeställningen, dvs. ”på eget initiativ”.

4.7.2 Departementspromemorian *Utökat informationsutbyte*, Ds 2022:13

Utredningen

I juni 2021 beslutade regeringen att tillsätta en s.k. bokstavsutredning som fick i uppdrag att utvärdera möjligheterna till informationsutbyte mellan statliga myndigheter, kommuner och arbetslöshetskassor för att fatta korrekta beslut i fråga om ersättningar från välfärdssystemen, och för att motverka arbetslivskriminalitet. I utredningens uppdrag ingick bl.a. att kartlägga vilka uppgifter berörda myndigheter, kommuner och arbetslöshetskassor behöver för att säkerställa korrekta beslutsunderlag för utbetalningar från välfärdssystemen. Utredningen hade även i uppdrag att analysera vilket behov av informationsutbyte som berörda myndigheter har för att kunna samverka och kontrollera arbetsplatser mer effektivt i syfte att motverka fusk, regelöverträdelser och brottslighet i arbetslivet och hur ett sådant informationsutbyte skulle kunna regleras. Resultatet av utredningen redovisades i departementspromemorian *Utökat informationsutbyte* (Ds 2022:13).

Behovet

Utifrån den kartläggning som genomfördes bedömde utredningen att myndigheterna har ett behov av att utbyta uppgifter på eget initiativ och att detta även omfattade uppgifter som inte är sekretessbelagda. Det konstaterades emellertid att dessa uppgifter i regel inte

kunde lämnas ut på eget initiativ i den uträckning som det fanns behov av, eftersom det i vissa fall saknades rättsligt stöd enligt dataskyddsregleringen för ett utlämnande.

I utredningens kartläggning framkom bl.a. att det fanns ett behov av att i större utsträckning på eget initiativ få lämna ut uppgifter som förekommer i Skatteverkets folkbokföringsverksamhet. De flesta uppgifter som förekommer i verksamheten är normalt sett inte sekretessbelagda. Endast om det av särskild anledning kan antas att ett utlämnande av uppgifter om enskildas personliga förhållanden från en sådan verksamhet skulle kunna leda till skada eller men kan sådana uppgifter hemlighållas (22 kap. 1 § första stycket OSL). Det rörde bl.a. uppgifter som folkbokföringsverksamheten hanterar inom ramen för sin verksamhet och som kan antas ha betydelse t.ex. för beskattningsverksamheten.[29]

Det framfördes även att andra myndigheter hade behov av att Skatteverkets beskattningsverksamhet gavs möjlighet att i större utsträckning få lämna ut uppgifter på eget initiativ. För Skatteverkets beskattningsverksamhet finns olika sekretessregler som gäller till skydd för en enskilds personliga eller ekonomiska förhållanden (27 kap. 1 och 2 §§ OSL). Beslut, varigenom skatt eller pensionsgrundande inkomst bestäms eller underlag för bestämmande av skatt fastställs, är emellertid som huvudregel undantagna från sekretess (27 kap. 6 § OSL). Även beslut i vissa ärendetyper som regleras i 27 kap. 2 § första och andra styckena OSL undantas från sekretess (27 kap. 2 § tredje stycket OSL). Det innebär att det inom Skatteverkets beskattningsverksamhet finns en stor mängd uppgifter som är undantagna från sekretess. Några exempel på uppgifter som andra myndigheter ansåg sig ha behov av rörde bland annat beslut om skatteregistreringar.[30]Andra exempel på uppgifter som Skatteverket förfogar över och som utredningen lyfte fram att andra myndigheter kunde ha behov av var vissa uppgifter på skattekonton som t.ex. beslut om slutlig skatt, debiterad preliminärskatt, moms att betala eller att få tillbaka, beslutade arbetsgivaravgifter och avdragen skatt, anstånd med betalning av skatt och omprövningsbeslut på ovanstående grundbeslut. Även beslut om godkännande eller avslag på en ansökan att få bli godkänd för F-skatt, beslut om återkallelse av F-skatt och beslut om debitering av preliminärskatt för den som är godkänd

[29] Ds 2022:13, *Utökat informationsutbyte*, s. 92–95.
[30] Ds 2022:13, *Utökat informationsutbyte*, s. 120 och 121.

för F-skatt är undantagna från sekretess (dvs. uppgifter som inte är sekretessbelagda), och ansågs kunna vara av betydelse för andra myndigheter.[31]

När det gäller uppgifter som inte är sekretessbelagda lyftes det även fram att inom Kronofogdemyndigheten gäller sekretess enligt 34 kap. 1 § OSL inte uppgift om förpliktelse som avses med den sökta verkställigheten i pågående mål eller beslut. Det innebär att uppgifter om t.ex. en avhysning eller annan handräckning, en fordrings storlek eller det belopp som ska drivas in härigenom aldrig är sekretessbelagda. Uppgifter om skatteskulder och socialförsäkringsavgifter på ett skattekonto omfattas t.ex. av sekretess enligt 27 kap. 1 § OSL (se HFD 2020 ref. 36). När beloppen förfaller till betalning och förblir obetalda överförs de per automatik (maskinellt) från Skatteverket till Kronofogdemyndigheten för indrivning. Uppgifter om förfallna samt obetalda skatteskulder och socialförsäkringsavgifter är därigenom inte sekretessbelagda hos Kronofogdemyndigheten enligt 34 kap. 1 § OSL.

Andra inte sekretessbelagda uppgifter avsåg uppgifter hos Arbetsmiljöverket. Arbetsmiljöverket ansvarar för att förvalta ett nationellt register över utstationering. En utstationerad arbetstagare är en person som skickas till ett annat land av sin arbetsgivare för att arbeta där under en begränsad tid. Utländska arbetsgivare som utstationerar arbetstagare till Sverige är bl.a. skyldiga att anmäla när utstationeringen sker. Uppgifter i utstationeringsregistret är inte sekretessreglerade och därför inte heller sekretessbelagda. Arbetsmiljöverket framförde att de hade ett behov av att få lämna ut uppgifter på eget initiativ och inte först efter en begäran.[32]

För Migrationsverkets del gäller sekretess för uppgifter om en enskilds personliga förhållanden i verksamhet för kontroll över utlänningar och i ärende om svenskt medborgarskap, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till denne lider men. För beslut i ärenden gäller sekretessen enligt första och andra styckena endast för uppgifter i skälen (37 kap. 1 § första och tredje stycket OSL). Det innebär att beslut, med undantag för skälen, om uppehålls- och arbetstillstånd, återkallelsebeslut eller förlängning av uppehålls- och arbetstillstånd i normalfallet inte är sekretessbelagda. Motsvarande gäller beslut om att utfärda uppe-

[31] Ds 2022:13, *Utökat informationsutbyte*, s. 137.
[32] Ds 2022:13, *Utökat informationsutbyte*, s. 155.

hållskort och EU-blåkort. Sekretess enligt 21 kap. 5 § OSL, som reglerar sekretess för utlänningars säkerhet, kan dock i vissa fall gälla även för uppgifter i beslutet. Behovet att få del av uppgifter som inte är sekretessbelagda framfördes bl.a. av Arbetsförmedlingen som behöver uppgifter om uppehålls- och arbetstillstånd, uppgifter om återkallelsebeslut och avslagsbeslut i ärenden som rör uppehålls- och arbetstillstånd för att säkerställa att arbetssökande har rätt att arbeta och vistas i Sverige.[33]

Promemorians förslag

I syfte att tillgodose de behov av utökade möjligheter till att utbyta uppgifter som inte är sekretessbelagda på eget initiativ som utredningen hade identifierat föreslogs att en ny bestämmelse skulle införas i 6 kap. 5 a § OSL med följande lydelse.

> En myndighet får till en annan myndighet lämna uppgift som den förfogar över, om inte uppgiften är sekretessbelagd och uppgiften kan antas vara av betydelse för att den mottagande myndigheten ska kunna fullgöra sin verksamhet.

Bestämmelsen skulle tillgodose de kartlagda behoven och innebära en möjlighet och inte en skyldighet att lämna ut uppgifter. Uppgifterna skulle då också få lämnas ut på eget initiativ. Bestämmelsen skulle då utgöra en rättslig grund i dataskyddsrättslig mening för att behandla personuppgifter i enlighet med dataskyddsförordningen när uppgifter lämnas ut på initiativ av den utlämnande myndigheten i de fall det annars saknades en rättslig grund för ett sådant utlämnande. Vidare skulle bestämmelsen komplettera bestämmelsen i 6 kap. 5 § OSL som utgör en rättslig grund för att lämna ut uppgifter som inte är sekretessbelagda efter en begäran från en annan myndighet.[34]

[33] Ds 2022:13, *Utökat informationsutbyte*, s. 102.
[34] Ds 2022:13, *Utökat informationsutbyte*, s. 260 och 261.

4.7.3 Vår kartläggning

Allmänt

I delbänkandet SOU 2024:63 har vi redogjort för vår kartläggning av behoven av förbättrade möjligheter till informationsutbyte mellan myndigheter. Kartläggningen består av två delar, en bred och en fördjupad kartläggning.

Den breda kartläggningen genomfördes i form av en digital enkät som ställdes till i princip alla myndigheter och övriga organ som har att tillämpa offentlighets- och sekretesslagen (se SOU 2024:63, avsnitt 4.4 och bilaga 2–5). Sammantaget kom det in 952 svar på enkäten, som både omfattar frågor om behovet av att lämna ut information och om behovet av att få del av information. Av naturliga skäl är det den del som avser möjligheten att *lämna ut* uppgifter till andra myndigheter som blir mest relevant att titta på när behovet av utökade möjligheter att lämna ut uppgifter på eget initiativ undersöks.

Den fördjupade kartläggningen genomfördes genom samråd och workshop m.m. med fyra olika myndighetssammansatta grupperingar, verksamma inom olika områden:

- SEFI-rådet

  Rådet för skydd av EU:s finansiella intressen, SEFI-rådet, ansvarar för att samordna åtgärder i Sverige mot bedrägerier och andra missbruk av EU-relaterade medel.

- MUR-initiativet

  Ett nätverk som består av 25 statliga myndigheter vars syfte främst är att arbeta förebyggande genom att samverka för att förhindra felaktiga utbetalningar och bidragsbrott.

- Bob-samverkan

  En struktur för ett sammanhållet arbete med barn och unga som riskerar att begå eller begår grova brott, i miljöer kopplade till organiserad brottslighet.

- Sveriges Kommuner och Regioner, SKR

  SKR är en medlems- och arbetsgivarorganisation där alla Sveriges kommuner och regioner är medlemmar.

Samråden med grupperingarna utformades efter den verksamhet som var aktuell i respektive sammanhang. I den fördjupade kartläggningen ingick även kontakt med två olika tillsynsmyndigheter, IVO och Finansinspektionen (se SOU 2024:63, avsnitt 4.5).

Vår breda kartläggning

Enkätens logik m.m.

Enkätens logik var uppbyggd på så sätt att de inledande frågorna hade funktionen av utslagsfrågor. De 142 respondenter som inledningsvis uppgav att de inte förfogade över uppgifter om enskilda som kan ha betydelse för andra myndigheter behövde inte svara på ytterligare frågor om utlämnande av uppgifter. De sammanlagt 352 respondenter som därefter uppgav att de antingen inte efterfrågade utökade möjligheter att lämna relevant information till andra myndigheter, eller inte hade någon ståndpunkt att redovisa i denna fråga, behövde sedan inte heller svara på ytterligare frågor om utlämnande, osv. Flera senare frågor gav dock möjligheten att fylla i flera alternativ, t.ex. frågor om vilka olika hinder som ansågs föreligga mot ett efterfrågat informationsutbyte.

Samtliga frågor om utlämnande avsåg sådan information om enskilda som kan ha betydelse för att andra myndigheter ska kunna fatta riktiga beslut eller på annat sätt utföra sin verksamhet. En fråga var dock mer specifik och avsåg sådan information om enskilda till andra myndigheter som kan ha betydelse för att andra myndigheter ska kunna förhindra, förebygga, upptäcka, utreda eller ingripa mot fusk, felaktiga utbetalningar, regelöverträdelser eller brottslighet. Den frågan hade dock inte karaktären av utslagsfråga.

Sekretesshinder – generellt

Hos de sammanlagt 424 respondenter som fick svara på frågan[35] om vilka sekretesshinder som föreligger mot att kunna lämna ut relevant information till andra myndigheter var det mest framträdande problemet att informationen omfattas av sekretess och att tillämpliga

[35] Flera alternativ kunde anges.

sekretessbrytande bestämmelser inte medger att information lämnas ut i tillräcklig omfattning (57,8 procent eller 245 respondenter).

Att annars sekretessbelagd information inte kan lämnas ut i tillräcklig omfattning kan avse olika förhållanden, t.ex. att rekvisiten som ställs upp för ett sekretessgenombrott är begränsande på olika sätt, eller att snävt avgränsade uppgiftskategorier anges. Med hänsyn till att de många sekretessbrytande uppgiftsskyldigheter som förekommer utanför offentlighets- och sekretesslagen innebär att ett sekretessgenombrott endast sker i samband med *en begäran* från den mottagande myndigheten, och inte när *ett behov* av att lämna ut uppgifterna uppstår, bör dock även sådan reglering kunna avses här.

Det tredje mest framträdande hindret (46,9 procent eller 199 respondenter) var att informationen omfattas av sekretess och det råder osäkerhet om det finns tillämpliga sekretessbrytande bestämmelser eller inte. Här bör osäkerhet i fråga om en sekretessbrytande bestämmelse även medger utlämnande på eget initiativ rymmas. I anslutning till detta kan också nämnas att 41 procent eller 174 respondenter uppgav att ett hinder mot utlämnande är att informationen omfattas av sekretess och befintlig sekretessbrytande reglering uppfattas som svårtolkad.

Utlämnande på eget initiativ

195 respondenter uppgav att det finns hinder mot att lämna ut relevanta uppgifter till en annan myndighet *på eget initiativ*. Bland dessa finns flera av Sveriges största myndigheter, bl.a. Centrala studiestödsnämnden, CSN, Försäkringskassan, Kriminalvården, Migrationsverket, Polismyndigheten, Skatteverkets beskattningsverksamhet, Skatteverkets folkbokföringsverksamhet, Statens institutionsstyrelse (SiS), Trafikverket, Transportstyrelsen och Tullverket. Bland övriga myndigheter kan nämnas flera ambassader, Inspektionen för arbetslöshetsförsäkringen, IVO och Tandvårds-och läkemedelsförmånsverket.

Även 135 respondenter från kommuner – såväl i storstadsområden som i glesbygd – och 18 respondenter från 11 olika regioner har uppgett att ett hinder mot att lämna relevanta uppgifter till andra myndigheter är att utlämnandet inte kan ske på eget initiativ. Respondenter i kommunerna uppgav sig till största delen vara verksamma inom

social omsorg, dvs. äldre- och handikappomsorg samt individ- och familjeomsorg (66,1 procent eller 82 kommunala respondenter).

Bland övriga aktörer, som inte är myndigheter men som ska tillämpa offentlighets- och sekretessregleringen i delar av sin verksamhet, är det enbart två respondenter som angett hinder mot att lämna ut uppgifter på eget initiativ som ett hinder för utlämnande. En av dessa var dock Sveriges a-kassor, som svarade för samtliga medlemsorganisationers räkning.

Svarsalternativet som avser hinder mot att lämna ut uppgifter på eget initiativ kan ses som ett komplement till de föregående redovisade alternativen, dvs. om begränsningar i sekretessbrytande bestämmelser, och osäkerhet om innebörden av sekretessbrytande bestämmelser, eftersom det inte förutsätter att uppgifterna träffas av en sekretessbrytande bestämmelse. Uppgifterna som avses bör alltså typiskt sett vara inte sekretessbelagda i det enskilda fallet.

Andra rättsliga hinder än sekretessregleringen

I enkäten efterfrågades inte bara om sekretessregleringen uppfattas utgöra ett hinder mot att lämna ut sådana uppgifter som kan ha betydelse för att andra myndigheter ska kunna fatta riktiga beslut eller på annat sätt utföra sin verksamhet, utan även om det fanns andra hinder mot ett sådant utlämnande.

Totalt 242 respondenter uppgav att det även fanns andra rättsliga hinder än sekretessregleringen mot relevant uppgiftslämnande till andra myndigheter. Den mest framträdande problematiken i detta sammanhang[36] var att den sammantagna regleringen av myndigheters informationsutbyte, dvs. sekretess- och dataskyddsfrågor, uppfattas som komplex och svårtillämpad (171 respondenter).

Det näst mest framträdande hindret mot att lämna ut relevanta uppgifter till andra myndigheter var att det inte finns någon rättslig grund i dataskyddsrättslig mening för den personuppgiftsbehandling som utlämnandet skulle innebära (98 respondenter). Bland de respondenter som redogjorde för detta problem finns 29 statliga myndigheter, bl.a. Bolagsverket, Domstolsverket, Inspektionen för arbetslöshetsförsäkringen, IVO, Naturvårdsverket, Patent- och registreringsverket, Polismyndigheten, Skatteverkets folkbokföringsverksamhet, Skatteverkets

[36] Flera alternativ kunde anges.

beskattningsverksamhet, Tullverket och Upphandlingsmyndigheten. Även 64 respondenter från kommuner uppgav att bristen på en rättslig grund i dataskyddsrättslig mening utgör ett hinder mot att lämna relevant information till andra myndigheter. Bland dessa finns såväl kommuner i storstadsområden som i glesbygd, och majoriteten av dessa (47 respondenter) uppgav att organisationen var verksam inom social omsorg, dvs. äldre- och handikappomsorg samt individ- och familjeomsorg.

Vilka uppgifter avses?

I enkäten ställdes även frågor om vilka uppgifter som bör kunna lämnas ut. Svarsalternativen bestod här i ett stort antal uppgiftskategorier som, beroende på i vilket sammanhang uppgifterna förekommer kan omfattas av en sekretess med ett rakt, kvalificerat skaderekvisit, dvs. en presumtion för att uppgifterna inte är sekretessbelagda, eller uppgifter som omfattas av undantag från sekretess eftersom de är intagna i ett beslut. Totalt 294 respondenter angav t.ex. att de efterfrågade möjlighet att lämna ut uppgifter om identitet, medborgarskap, bosättning, civilstånd, familjeförhållanden, vårdnadsförhållanden m.m. och 247 respondenter angav att de efterfrågade möjlighet att lämna ut uppgifter om boende, boendeform, adress, samboende, m.m. Ett flertal av dessa uppgifter är sådana som typiskt sett inte är sekretessbelagda och tillgängliga för samtliga myndigheter genom Skatteverkets system för distribution av grunduppgifter från folkbokföringen, Navet.[37] Det rör dessutom flera uppgiftskategorier som typiskt sett inte anses särskilt känsliga, och därför inte är sekretessbelagda annars än i sällsynta undantagsfall.

Bland de respondenter som efterfrågat utökade möjligheter att lämna ut uppgifter om identitet, medborgarskap, bosättning, civilstånd, familjeförhållanden, vårdnadsförhållanden m.m. finns ett stort antal ambassader. Även några av Sveriges stora statliga myndigheter, t.ex. Arbetsförmedlingen, Bolagsverket, CSN, Försäkringskassan, Skatteverkets folkbokföringsverksamhet, Polismyndigheten och Transportstyrelsen efterfrågar en sådan möjlighet, liksom 223 respondenter i kommuner över hela landet. Bland de kommunala

[37] Jfr 2 kap. 8 § lagen (2001:182) om behandling av personuppgifter i Skatteverkets folkbokföringsverksamhet.

aktörerna har 71,8 procent, eller 148 respondenter, uppgett att de är verksamma inom social omsorg, dvs. äldre- och handikappomsorg samt individ- och familjeomsorg.

Vidare kan nämnas att 141 respondenter efterfrågade möjligheter att lämna ut information om juridiska personers identitet, säte, ägarförhållanden samt firmatecknare och andra företrädare m.m. Detta är också uppgifter som i många sammanhang inte är sekretessbelagda.

Som vi nämnt inledningsvis är dock bedömningen av om en uppgift är sekretessbelagd eller inte något som ofta avgörs i en konkret utlämnandesituation. Detta gäller emellertid inte uppgifter som förekommer i sammanhang som genom bestämmelser om undantag från sekretess inte är sekretessbelagda. Här kan särskilt nämnas att totalt 268 respondenter efterfrågar möjlighet att lämna ut information om pågående ärenden och beslut. Beslut är ofta undantagna från de materiella sekretessbestämmelserna och därför inte sekretessbelagda, i vart fall inte i sin helhet. Även i denna grupp finns det flera ambassader bland respondenterna, liksom flera stora statliga myndigheter. Bland respondenterna finns även 211 respondenter från kommuner och 10 respondenter från 7 olika regioner.

Ytterligare ett exempel är att uppgifter om registrering för skatter och avgifter, underlag för fastställande av skatter och avgifter, bestämmande av skatter och avgifter och andra beskattningsuppgifter inklusive om fastighetstaxering också i många fall inte är sekretessbelagda genom Skatteverkets beslut om dessa förhållanden.[38] 81 respondenter efterfrågar möjlighet att lämna ut denna typ av uppgifter.

Något om att behovet av att få del av uppgifter

Som vi nämnt inledningsvis är det av naturliga skäl mest relevant att undersöka behoven hos en utlämnande myndighet när frågan om utlämnande på eget initiativ undersöks. I sammanhanget bör dock något också sägas om myndigheternas behov av att få del av uppgifter från andra.

464 respondenter uppgav att sekretessregleringen utgör ett hinder mot att få del av för den egna verksamheten relevanta uppgifter om enskilda som andra myndigheter förfogar över. De primära hindren uppgavs vara dels att informationen omfattas av sekretess och det

[38] Se 27 kap. 6 § OSL om undantag från den absoluta skattesekretessen.

saknas tillämpliga sekretessbrytande bestämmelser (286 respondenter eller 61,6 procent), dels att informationen omfattas av sekretess och tillämpliga sekretessbrytande bestämmelser medger inte att information lämnas ut i tillräcklig omfattning (262 respondenter eller 56,5 procent).

224 respondenter eller 48,3 procent uppgav att ett hinder mot att få del av för verksamheten relevant information som andra myndigheter förfogar över är att den utlämnande myndigheten saknar möjlighet att lämna ut uppgifterna på eget initiativ. 49 statliga myndigheter finns i denna grupp, bl.a. CSN, Försäkringskassan, Kronofogdemyndigheten, Migrationsverket, Pensionsmyndigheten, Polismyndigheten, Skatteverkets beskattningsverksamhet, Skatteverkets folkbokföringsverksamhet, Trafikverket och Transportstyrelsen. Även Inspektionen för arbetslöshetsförsäkringen, IVO, Tandvårds- och läkemedelsförmånsverket, Rättsmedicinalverket och flera ambassader finns bland de statliga myndigheterna som uppgett detta som ett hinder.

Också 161 respondenter från kommuner har uppgett att ett hinder mot att få del av för verksamheten relevant information som andra myndigheter förfogar över är att den utlämnande myndigheten saknar möjlighet att lämna ut uppgifterna på eget initiativ. Bland dessa har en majoritet, 96 respondenter eller 59,6 procent, uppgett sig vara verksamma inom social omsorg, dvs. äldre- och handikappomsorg samt individ- och familjeomsorg.

10 respondenter i 7 olika regioner har också uppgett att ett hinder mot att få del av relevant information är att den utlämnande myndigheten saknar möjlighet att lämna ut uppgifterna på eget initiativ.

Vår fördjupade kartläggning

Ett urval

I den fördjupade kartläggningen undersökte vi inte behovet av att i högre utsträckning lämna ut uppgifter till en annan myndighet på eget initiativ särskilt. Det framkom dock flera exempel på situationer där möjligheten till utlämnande av uppgifter till en annan myndighet på eget initiativ aktualiserades, varav några redogörs för nedan. Exemplen är alltså enbart ett urval av de behov vi kartlagt i detta

avseende. För en fullständig redogörelse och mer information om de samråd som hållits hänvisas till delbetänkandet.

Tillsynsmyndigheter

Med större möjlighet att få tillgång till uppgifter och förfinade utredningsmetoder blir *IVO* också allt bättre på att upptäcka förhållanden som IVO kan konstatera skulle vara av värde för andra myndigheter att få kännedom om. Utöver uppgifter som kan få direkt betydelse hos en myndighet för att säkerställa korrekta utbetalningar eller motverka brott kan det vara fråga om uppgifter som behöver anmälas till en annan myndighet för att dess data eller register ska bli korrekta. I nästa led kan uppgifterna behövas hos en utbetalande myndighet eller i en brottsutredning. IVO efterfrågar möjligheter att kunna lämna ut sådan information till berörda myndigheter.

Finansinspektionen ser hinder mot informationsutbyte t.ex. vid undandragande av skatt. På detta område ser myndigheten ett eventuellt behov av förbättringar och förenklingar vad gäller samarbete med Skatteverket. Finansinspektionen kan t.ex. i ett tillståndsärende se att ett företag förefaller ha ett s.k. upplägg som kan vara problematiskt ur ett skatterättsligt perspektiv, men som inte kan läggas till grund för ett avslag i tillståndsärendet. Motsvarande information kan Finansinspektionen även få i sin löpande tillsyn eller i en undersökning. I sådana situationer efterfrågas en möjlighet att enkelt och rutinmässigt kunna informera Skatteverket, som då ges möjlighet att utreda företaget.

SEFI-rådet

Svenska myndigheter är enligt EU-rätten skyldiga att motverka och upptäcka otillåten dubbelfinansiering och andra typer av bedrägerier om det påverkar EU:s budget. Enligt SEFI-rådet saknar de berörda myndigheterna i dagsläget möjligheter att strukturerat och regelmässigt utbyta information om utbetalda medel och stödmottagare, vilket gör det svårt att systematiskt kontrollera riktigheten i t.ex. ingivna ansökningsunderlag som läggs till grund för beslut om stöd. Enligt SEFI-rådet förekommer i enstaka ärenden och på förekommen anledning att vissa myndigheter hittar former för utbyte av

information. Enligt SEFI-rådet behöver dock myndigheterna, i syfte att fullgöra sina skyldigheter enligt EU-rätten, en möjlighet att göra det systematiskt. Utökade möjligheter att regelmässigt och systematiskt utbyta information mellan myndigheter som hanterar EU-stöd skulle bidra till att motverka och upptäcka otillåten dubbelfinansiering och andra typer av bedrägerier.

MUR-initiativet

Enligt *Skolverket* behövs det mer lättillgänglig kunskap om vilka bidrag skolhuvudmän och organisationer får. Olika myndigheter skulle på så sätt få en tydlig bild av vilka bidrag mottagarna tar emot från andra myndigheter (och kommuner), vilket skulle kunna förhindra dubbelfinansiering.

Inom *avfallsområdet* har fyra aktörer olika ansvar och utövar olika tillsyn och gör kontroller inom området; Naturvårdsverket, kommunerna, länsstyrelserna och Skatteverket. Problemet här är att de olika inblandade parterna inte vet vilken information som finns hos de andra aktörerna och som kan begäras ut. Här behövs enligt Skatteverket regelförändringar för att möjliggöra ett frivilligt informationsöverlämnande till den aktör man vet är i behov av uppgiften, t.ex. angående omständigheter som påverkar tillstånd utfärdade av länsstyrelsen eller omständigheter som bryter mot Naturvårdverkets utfärdade föreskrifter. Ingen möjlighet finns i dag att skicka denna information vidare.

Det är ett återkommande problem i lagstiftning som rör uppgiftsskyldighet att *Skatteverkets beskattningsverksamhet* ofta enbart är utpekat som en uppgiftslämnande, men inte mottagande, myndighet. Skatteverket är dock ofta i behov av extern information för att kunna agera mot oseriösa företag, exempelvis genom återkallande av F-skatt eller avregistrering som arbetsgivare eller för mervärdesskatt. Vid en utebliven avregistrering kan företag fortsätta att användas som brottsverktyg. Det kan också röra sig om information om felaktig beskattning, exempelvis svartarbete, som en annan myndighet har kännedom om men inte kan dela med Skatteverket på eget initiativ. Denna brist tas också upp av övriga myndigheter som ett återkommande problem och i dessa situationer tappar Skatteverket möjligheten till utredning och korrekta beslut om beskattning. Ett

närliggande exempel är att det inte är ovanligt att Skatteverket i samband med beskattningsutredningar får information om att personer som beskattas saknar arbetstillstånd, eller att de har fått ett sådant tillstånd på felaktiga grunder. Skatteverket kan dock inte dela med sig av den informationen på eget initiativ, och Migrationsverket å sin sida har inga möjligheter att begära ut informationen.

Skatteverkets skattebrottsenhet efterfrågar en möjlighet att kunna dela mer information med myndigheter som inte har ett brottsbekämpande uppdrag. Det kan t.ex. röra sig om att ha möjlighet att skicka signaler i syfte att förhindra brottslighet. De särskilda sekretessbrytande bestämmelserna och generalklausulen i offentlighets- och sekretesslagen bedöms inte vara tillräckliga verktyg för att åstadkomma det efterfrågade informationsutbytet.

Skatteverkets folkbokföringsverksamhet har uppgett att uppgifter inom folkbokföringsverksamheten oftast inte är sekretessbelagda. För folkbokföringsverksamheten är det därför sällan ett problem att lämna ut information efter begäran (jfr 6 kap. 5 § OSL). I Skatteverkets folkbokföringsutredningar förekommer det dock att handläggare uppmärksammar saker som andra myndigheter bedöms behöva utifrån sina respektive uppdrag. Exempel på sådan information som Skatteverket inte kan lämna ut på eget initiativ är bl.a. identitetshandlingar som inte har visats upp för Migrationsverket, madrassboenden vid kontrollbesök, utnyttjade identiteter i bolagsstyrelser och personer som saknar rätt att vistas i landet men som bor här och är folkbokförda. Det är inte heller ovanligt att folkbokföringsverksamheten utreder identitetsrelaterade fel och ändrar någons medborgarskap från ett ”EU-medborgarskap” till ett medborgarskap från tredje land, dvs. utanför EU, vilket innebär att han eller hon behöver uppehållstillstånd för att vistas i Sverige.

CSN uppger att det t.ex. finns ett behov av att på eget initiativ kunna lämna uppgifter till Skatteverket för att den myndigheten ska kunna fatta korrekta beslut om beskattning. CSN kan nämligen få in uppgifter om förekomst av svartarbete, och lämnar merkostnadslån för extra boendekostnader i samband med dubbel bosättning. Det kan i sin tur påverka den enskildes rätt till reseavdrag och skatteavdrag för dubbel bosättning. Det finns också konkreta exempel på att Polismyndigheten har haft för CSN betydelsefulla uppgifter om en person som har studiestöd för att studera på plats utomlands men som har anhållits vid återkomst till Arlanda efter en längre tids vistelse

i ett helt annat land än det tänkta studielandet. Polismyndigheten och många andra myndigheter kan i dag välja att lämna ut uppgifter till CSN om de bedömer att ett sådan utlämnande har stöd i generalklausulen i 10 kap. 27 § OSL. Utlämnande med stöd av den paragrafen fordrar dock en bedömning i det enskilda fallet och sker oftast inte på initiativ av utlämnande myndighet. Det förekommer även att en myndighet eller annan organisation upptäcker misstänkta felaktiga utbetalningar eller bidragsbrott i sin egen verksamhet. Uppgifter om stödtagare, kontaktuppgifter som telefonnummer, mailadresser, postadresser, IP-adresser etc. som förekommer i ett sådant ärende bör i sådana fall kunna delas med andra myndigheter på eget initiativ, som en input till extra kontrollåtgärder hos mottagande myndigheter och organisationer där samma stödtagare eller kontaktuppgifter förekommer.

Ett typfall som förekommer inom *Pensionsmyndigheten* är när oredovisade inkomster misstänks utifrån uppgifter i kontoutdrag som hämtats in i en kontrollutredning. I ett sådant fall hindrar sekretessregleringen Pensionsmyndigheten från att underrätta Skatteverkets beskattningsverksamhet om de misstänka oredovisade uppgifterna. Det hade inte varit något problem om Skatteverket hade skickat en begäran till om att få ta del av uppgifterna. I en sådan situation hade Pensionsmyndigheten i stället varit skyldig att lämna ut uppgifterna enligt 42 a kap. 1 § skatteförfarandelagen (2011:1244). Som en konsekvens får Skatteverket inte alltid kännedom om oredovisade inkomster, vilket i sin tur kan leda till en felaktig beskattning och i förlängningen även till en felaktig pensionsgrundande inkomst.

Kronofogdemyndigheten uppger att det behövs större möjligheter att utbyta information som rör lönegarantibedrägerier. Inom den kontexten finns det i dag en sårbarhet för felaktiga utbetalningar. För att reducera sårbarheterna krävs att de myndigheter som är delaktiga i lönegarantiärenden har en möjlighet att samverka i enskilda ärenden. Det ställer krav på att Skatteverket, Kronofogdemyndigheten, Arbetsförmedlingen och de utbetalande länsstyrelserna kan utbyta information i de ärenden där man tror att fusk eller missbruk kommer att uppstå, eller redan har uppstått.

Bob-samverkan

Vid samrådet med Bob-samverkan deltog representanter från Kriminalvården, länsstyrelserna, Polismyndigheten, SiS, Socialstyrelsen och Åklagarmyndigheten. Samrådet utgick från en handfull konkreta situationer kopplade till barn och unga som riskerar att begå eller begår grova brott i miljöer kopplade till organiserad brottslighet, där behovet av förbättrade möjligheter till informationsutbyte mellan myndigheter typiskt sett gör sig gällande. De situationer som redogjordes för och diskuterades var hämtade primärt från lokalpolisområdets vardag, där erfarenheten är att samverkansparten (t.ex. skolan, socialtjänsten eller SiS) frekvent hänvisar till sekretess och därför inte lämnar ut relevant och behövlig information till Polismyndigheten.

Vid samrådet underströks att deltagande myndigheter satsar på att hitta potentiella unga förövare tidigt, och att det arbetet i stora delar går ut på att dämpa sårbarheten hos barn och unga som riskerar att begå grova våldsbrott. En viktig komponent är att det finns ett välfungerande informationsutbyte mellan olika aktörer som kommer i kontakt med de unga och att deltagande myndigheter behöver kunna föra öppna samtal för att komma vidare med ett renodlat förebyggande arbete. Ett exempel som fördes fram var att SiS behöver få del av mer information från socialtjänsterna när det gäller var en ungdom ska placeras. Om SiS planeringsenhet inte vet vad de ska tänka på vid placeringen, t.ex. om det finns en nätverkskoppling som gör att vissa barn och unga inte bör placeras tillsammans med vissa andra, behöver socialtjänsterna få dela information om detta. Ett annat exempel som fördes fram var avseende barn och familjer som flyttar mellan olika kommuner för att undkomma samröre med bl.a. socialtjänsten. I de fallen lyftes särskilt socialtjänsternas och skolornas behov av enklare informationsutbyte fram. Under och efter diskussionerna vid samrådet med utredningen gjorde några myndigheter reflektionen att det i flera situationer som diskuterades faktiskt fanns en befintlig sekretessbrytande bestämmelse som av olika orsaker inte används. En synpunkt som framfördes var att dataskyddsfrågorna eventuellt kunde spela en viss roll i detta, och att kopplingen mellan sekretess och dataskydd har bidragit till mer restriktivitet i utlämnandesituationer.

Sveriges Kommuner och Regioner – SKR

Enligt SKR:s erfarenhet är en förutsättning för att ”lyckas” med välfärdsbrottslighet många gånger att uppgifter om enskilda skyddas av sekretess, och att myndigheter är förhindrade att utbyta information med varandra. Inom den kommunala sektorn råder ofta en presumtion för att uppgifter om enskilda är sekretessbelagda. Det innebär att olika kommunala aktörer, även t.ex. olika socialförvaltningar inom en och samma kommun, som utgångspunkt inte spontant får dela information med varandra, t.ex. om vem som beviljats en viss insats och på vilka grunder. Mot bakgrund av det starka sekretesskyddet är välfärdsbrottslighet inom den kommunala sektorn – särskilt vad gäller kommunernas verksamhet enligt socialtjänstlagen och enligt lagen (1993:387) om stöd och service till vissa funktionshindrade – också mycket svår att upptäcka.

De små möjligheterna att dela information mellan olika socialförvaltningar inom en kommun eller med socialtjänsten i en annan kommun, eller med Polismyndigheten, är också ett stort problem i relation till barn som riskerar att fara illa, exempelvis genom att rekryteras in i kriminalitet. Det är särskilt påtagligt när barn rör sig mellan olika stadsdelar eller mellan olika kommuner. Kommunernas socialtjänster har enligt socialtjänstlagen ett särskilt ansvar för dessa barn men får i dag enbart utbyta information med varandra eller med Polismyndigheten i ett fåtal, avgränsade situationer. För en effektiv förebyggande verksamhet skulle det behöva införas en utökad, och framför allt tydligt tillåtande, reglering som ger möjlighet för socialtjänsten att utbyta information om barn som riskerar att fara illa, och andra personer när det är relevant, långt tidigare och i långt fler situationer än i dag.

4.7.4 Sammanfattning

Genom kartläggningar i andra sammanhang, och den kartläggning vi genomfört framgår att myndigheter ofta uppfattar att de saknar möjligheter att på eget initiativ lämna relevanta uppgifter till andra myndigheter. Detta gäller även i situationer där den myndighet som har uppgifterna hade haft en långtgående skyldighet att lämna ut samma uppgifter om mottagaren hade begärt det. En del i problematiken är därmed att det ofta finns ett informationsunderskott hos

mottagaren. De uppgiftskategorier som efterfrågas rör vidare både uppgifter som annars är sekretessbelagda och uppgifter som annars inte är det.

4.8 Överväganden och förslag

4.8.1 Det kartlagda behovet av att på eget initiativ kunna lämna uppgifter till en annan myndighet

Vår bedömning: De kartlagda generella behoven av ett förbättrat informationsutbyte mellan myndigheter omfattar möjligheten att på eget initiativ utbyta uppgifter som inte är sekretessbelagda. Detta behov är inte på ett generellt plan tillgodosett genom annan lagstiftning vad gäller uppgifter som inte är sekretessreglerade, uppgifter som omfattas av ett undantag från sekretess och uppgifter som kan lämnas ut efter en prövning av den materiella sekretessbestämmelsen.

Skälen för vår bedömning

Kartlagda behov är till viss del tillgodosedda

I avsnitt 4.7 har vi redogjort för att det finns ett kartlagt och generellt behov av att på eget initiativ kunna lämna uppgifter till andra myndigheter. En stor del av behovet som rör bristen på rättsligt stöd för att lämna uppgifter på eget initiativ kan antas hänga samman med att många sekretessbrytande uppgiftsskyldigheter kräver en begäran, dvs. att uppgifter är sekretessbelagda i förhållande till mottagaren fram till dess en begäran om att få del av dem har framställts (jfr avsnitt 4.4.3). Om den generella sekretessbrytande bestämmelse som vi föreslagit i SOU 2024:63 införs så kommer den problematiken att minska. Som vi nämnt flera gånger tidigare utgör nämligen en sekretessbrytande bestämmelse i offentlighets- och sekretesslagen ett rättsligt stöd för att lämna ut uppgifter som träffas av bestämmelsen på eget initiativ, även om detta inte framgår uttryckligen av bestämmelsen.

De behov som redogjordes för i departementspromemorian *Utökat informationsutbyte* borde vidare i viss mån ha blivit tillgodosedda genom införandet av LUFFA-lagen. Genom bestämmelserna i LUFFA-lagen kan uppgiftsutlämnandet ske på initiativ av den utlämnande myndigheten. Vissa behov som kartlagts i andra sammanhang kan vidare förväntas ha blivit eller komma att bli tillgodosedda genom införandet av annan lagstiftning, t.ex. den nyligen införda lagen (2025:170) om skyldighet att lämna uppgifter till de brottsbekämpande myndigheterna och de förändringar av offentlighets- och sekretesslagen som infördes i samband med detta.[39] I den nya lagen är uppgiftsskyldigheten i vissa fall inte förenad med ett krav på en föregående begäran.

Det kartlagda behovet omfattar även uppgifter som annars inte är sekretessbelagda

Som vi nämnt tidigare finns det i regel inte någon på förhand avgränsad och definierad kategori av uppgifter som inte är sekretessbelagda i förhållande till en eller flera andra myndigheter. Det kartlagda generella behovet avser därför även uppgifter som annars inte är sekretessbelagda på grund av att de omfattas av ett undantag från sekretess och uppgifter som kan lämnas ut efter en prövning av den materiella sekretessbestämmelsen (jfr avsnitt 4.3.2). Baserat på resultatet av vår enkät vad gäller frågan om vilka uppgiftskategorier som avses, samt den kartläggning som redogjordes för i departementspromemorian *Utökat informationsutbyte*, bedömer vi att behovet även avser uppgifter som annars inte är sekretessbelagda på grund av att de inte är sekretessreglerade.

Behovet kvarstår vad gäller uppgifter som annars inte är sekretessbelagda

En följd av att myndigheternas handlingsutrymme vad gäller personuppgiftsbehandling är begränsat till vad som följer av lagstiftning är att myndigheters handlande som saknar stöd i rättsordningen inte är tillåtet.

[39] Se prop. 2024/25:65, *Ökat informationsflöde till brottsbekämpningen*.

Utlämnande av uppgifter som inte är sekretessbelagda i förhållande till mottagaren, på initiativ av en utlämnande myndighet, är ett sådant handlande som i dag inte är generellt fastställt i den nationella rätten eller unionsrätten. Någon generell bestämmelse som motsvarar den i 6 kap. 5 § OSL, men som i stället reglerar handlingsutrymmet att på eget initiativ lämna uppgifter som inte är sekretessbelagda till en annan myndighet, finns alltså inte.

Oavsett hur generell en sekretessbrytande bestämmelse i offentlighets- och sekretesslagen än är utformad så träffar den dessutom inte uppgifter som ”från början” inte är sekretessbelagda i det sammanhang de förekommer. En sekretessbrytande bestämmelse kan alltså rent lagtekniskt inte ligga till grund för att lämna ut sådana uppgifter på eget initiativ. Det innebär att utrymmet för att lämna ut uppgifter som inte annars är sekretessbelagda ofta är mindre än utrymmet för att lämna ut uppgifter som annars är sekretessbelagda.

Som vi redogjort för i avsnitt 4.6 är det enbart när det föreligger en *skyldighet* att på eget initiativ upplysa en annan myndighet om något förhållande som utlämnande på eget initiativ av uppgifter som annars inte är sekretessbelagda uttryckligen är tillåtet. En bestämmelse om uppgiftsskyldighet på initiativ av den utlämnande myndigheten har dock i regel ett mycket avgränsat tillämpningsområde. LUFFA-lagen gäller t.ex. enbart för uppgiftslämnande som sker för att säkerställa korrekta beslutsunderlag för att förebygga, förhindra, upptäcka eller utreda felaktiga utbetalningar från välfärdssystemen. För informationsutbyte som inte uppfyller de förutsättningar som ställs upp i en bestämmelse om uppgiftsskyldighet finns det fortsatt hinder mot att lämna ut uppgifter som annars inte är sekretessbelagda på eget initiativ.

Vad gäller sådana uppgifter som det inte råder något förbud mot att röja enligt sekretessregleringen (dvs. som annars inte är sekretessbelagda, jfr definitionen av sekretess i 3 kap. 1 § OSL) föreligger därmed *i praktiken* närmast vad som är att likställa med ett generellt förbud mot att på eget initiativ lämna dessa till en annan myndighet, trots att den utlämnande myndigheten enligt 6 kap. 5 § OSL hade varit skyldig att lämna samma uppgifter till mottagaren om en begäran hade framställts. Det generella behovet av att på eget initiativ kunna lämna sådana uppgifter till en annan myndighet kvarstår därmed, trots införandet av en generell sekretessbrytande bestämmelse och avgränsade uppgiftsskyldigheter som inte kräver en begäran.

Behovet av en enklare reglering

Vår kartläggning har visat att det finns ett mycket omfattande behov av förbättrade möjligheter till informationsutbyte mellan myndigheter som inte enbart har att göra med att uppgifter är sekretessbelagda i förhållande till andra myndigheter. Det mest framträdande problemet är den sammantagna regleringens komplexitet. Vi har därför bedömt att behovet av en tydligare, mer enhetlig och mer förutsebar sekretessreglering bör tillskrivas en stor vikt (se avsnitt 4.6.1 i SOU 2024:63).

Vi har nyss konstaterat att det lagtekniska utrymmet för att på eget initiativ lämna uppgifter som annars *inte* är sekretessbelagda i förhållande till mottagaren (dvs. där det inte föreligger något förbud mot att röja uppgifterna) kan vara mindre än utrymmet att på eget initiativ lämna uppgifter som annars *är* sekretessbelagda. Regleringens komplexitet i detta avseende kan *i sig* ge upphov till en osäkerhet om innebörd och tillämpning även av andra bestämmelser. I vår kartläggning har vi t.ex. kunnat se att det råder en generell osäkerhet om tillämpningen av befintlig reglering som bl.a. avser i vilken utsträckning det faktiskt är tillåtet att på eget initiativ lämna uppgifter till en annan myndighet, trots att utlämnandet är tillåtet enligt en sekretessbrytande bestämmelse i offentlighets- och sekretesslagen. Det kan i vart fall delvis antas bero på att det inte uttryckligen är tillåtet att på eget initiativ lämna ut uppgifter som annars inte är sekretessbelagda. Behovet av tydlighet, enhetlighet och förutsebarhet gör sig därför även gällande i frågan om möjligheterna att på eget initiativ lämna uppgifter som, oavsett skäl, inte är sekretessbelagda.

Sammanfattning

En central del i de kartlagda behoven av ett förbättrat informationsutbyte mellan myndigheter är möjligheten att lämna ut uppgifter på eget initiativ. Detta behov tillgodoses i viss utsträckning bl.a. av den generella sekretessbrytande bestämmelse vi föreslagit i SOU 2024:63. Vår bedömning är dock att de kartlagda behoven av ett förbättrat informationsutbyte mellan myndigheter även omfattar en generell möjlighet att på eget initiativ utbyta uppgifter som annars inte är sekretessbelagda. Det behovet är inte på ett generellt plan tillgodosett genom annan lagstiftning vad gäller uppgifter som inte är sekretess-

reglerade, uppgifter som omfattas av ett undantag från sekretess och uppgifter som kan lämnas ut efter en prövning av den materiella sekretessbestämmelsen. Behoven avser främst att det saknas en tydligt tillåtande reglering, men även att den befintliga regleringen är komplex.

4.8.2 Befintlig reglering behöver förtydligas

Vår bedömning: Det behöver förtydligas att det är tillåtet att på eget initiativ lämna ut uppgifter som träffas av en sekretessbrytande bestämmelse i offentlighets- och sekretesslagen.

Skälen för vår bedömning

Uppgifter som träffas av en sekretessbrytande bestämmelse[40] i offentlighets- och sekretesslagen, och som därför inte är sekretessbelagda i förhållande till mottagaren, kan redan i dag lämnas till mottagaren på initiativ av den utlämnande myndigheten. Rent rättsligt är det alltså inte behövligt med någon förändring av befintlig reglering för att möjliggöra utlämnande på eget initiativ i dessa situationer. Att de sekretessbrytande bestämmelserna i offentlighets- och sekretesslagen kan ligga till grund för ett utlämnande på eget initiativ framgår dock inte uttryckligen av bestämmelserna. I stället anges att sekretess *inte hindrar* att vissa uppgifter lämnas ut, om vissa villkor är uppfyllda. Regleringen är alltså inte särskilt tydlig i detta avseende.

Det sammantagna resultatet av vår kartläggning har lett oss till bedömningen att bl.a. behovet av en tydligare sekretessreglering bör tillskrivas en stor vikt, vilket vi nämnt ovan och redogjort för i avsnitt 4.6.1 i SOU 2024:63. I det sammanhanget uppmärksammade vi särskilt att det inte enbart är sekretessregleringen som påverkar myndigheternas handlingsutrymme. Parallellt med sekretessregleringen måste även det dataskyddsrättsliga regelverket tillämpas, vilket i många fall också inkluderar kompletterande, sektorsspecifik dataskyddsreglering. Ett av de mer framträdande praktiska problem som vi kartlagt är dessutom att regleringen uppfattas vara komplex och svårtillämpad, särskilt sammantagen med den dataskyddsrättsliga regleringen. Ur det perspektivet finns det alltså ett behov av att för-

[40] 10 kap. 28 § OSL räknas här inte till de sekretessbrytande bestämmelserna.

tydliga myndigheternas möjligheter att på eget initiativ lämna uppgifter som inte är sekretessbelagda till andra myndigheter. Ett förtydligande skulle även medföra att det finns en tydligare rättslig grund i dataskyddsrättslig mening för utlämnande på eget initiativ än det gör i dag.

Ökad tydlighet i regelverket skulle också bidra till ökad transparens för de enskilda registrerade vars uppgifter behandlas vid informationsutbyte mellan myndigheter. En sådan förändring kan därmed ses som en integritetshöjande åtgärd i förhållande till dataskyddsförordningen genom att bidra till förutsebarhet i frågan om hur uppgifter om enskilda registrerade får behandlas (jfr kraven i skäl 41 i dataskyddsförordningen). För en enskild registrerad kan utformningen av de sekretessbrytande bestämmelserna i offentlighets- och sekretesslagen till och med uppfattas som vilseledande vad gäller möjligheten att med stöd av en sådan bestämmelse lämna ut uppgifter på eget initiativ.

Det finns följaktligen ett behov av att skapa en större tydlighet gällande innebörden av bestämmelser som redan i dag tillåter utlämnande på eget initiativ från en myndighet till en annan. Behovet kan tillgodoses genom en generell reglering av utlämnande på eget initiativ av uppgifter som inte är sekretessbelagda.

4.8.3 Uppgiftslämnande på eget initiativ är ibland nödvändigt

Vår bedömning: För att ett berättigat och relevant informationsutbyte mellan myndigheter ska kunna genomföras är det i vissa fall nödvändigt att uppgifter lämnas på initiativ av den utlämnande myndigheten.

Skälen för vår bedömning

Frågan om ”på eget initiativ” satt i sitt sammanhang

En väsentlig del av det kartlagda behovet av förbättrade möjligheter till informationsutbyte mellan myndigheter utgörs som vi redan påpekat av behovet av att kunna lämna ut uppgifter på eget initiativ. Som vi konstaterat i avsnitt 4.8.1 är dock utrymmet för att på eget

initiativ lämna ut uppgifter som annars inte är sekretessbelagda dock ofta mindre än om uppgifterna i stället annars hade varit sekretessbelagda och därför träffats av en sekretessbrytande bestämmelse i offentlighets- och sekretesslagen.

Mot detta kan ställas det starka rättsliga stödet för att lämna ut samma slags uppgifter, dvs. uppgifter som inte är sekretessbelagda, på begäran av den mottagande myndigheten. Genom bestämmelsen i 6 kap. 5 § OSL finns det till och med ett krav på myndigheter att lämna uppgifter som inte är sekretessbelagda till en annan myndighet som har begärt att få del av uppgifterna, om inte utlämnandet är så resurskrävande att det skulle hindra arbetets behöriga gång.

Samtliga uppgifter som skulle träffas av en bestämmelse som gav ett generellt rättsligt stöd för att på eget initiativ lämna en uppgift som inte är sekretessbelagd till en annan myndighet skulle alltså *även* träffas av regleringen i 6 kap. 5 § OSL om en annan myndighet har begärt att få del av uppgiften. Eftersom myndigheter har en skyldighet att på begäran lämna ut uppgifter som inte är sekretessbelagda till en annan myndighet på begäran kan man fråga sig om, och i så fall varför, det är av vikt att samma uppgifter bör få lämnas ut trots att mottagaren inte har begärt att få del av uppgifterna.

Syftet med utlämnande på eget initiativ

I vår kartläggning har det sammanfattningsvis framkommit att myndigheters medarbetare ibland får del av uppgifter eller gör iakttagelser som tyder på att det förekommer felaktigheter i en annan myndighets verksamhet, men som saknar betydelse i den egna verksamheten. Myndigheten som känner till dessa uppgifter saknar dock ofta möjlighet att underrätta den myndighet som ansvarar för den verksamhet där felaktigheten kan antas förekomma men har samtidigt en skyldighet enligt 6 kap. 5 § OSL att lämna ut uppgifterna om detta skulle begäras av den andra myndigheten. Vissa aktörer har också särskilt lyft att den tänkta mottagande myndigheten i många fall saknar kännedom om att uppgifterna över huvud taget finns och därför inte heller kan framställa någon begäran om att få del av dem, trots att det inte skulle föreligga sekretesshinder mot ett utlämnande efter begäran.

De förhållanden som vi har kartlagt motsvarar alltså i stora drag den situation som kan uppstå när en uppgiftsskyldighet på begäran träffar uppgifter som är sekretessbelagda (jfr avsnitt 4.4.3). Samma slags behov som vi har kartlagt har dessutom motiverat införandet av mer avgränsade rättsliga möjligheter att lämna uppgifter till en annan myndighet på eget initiativ (jfr avsnitt 4.5).

Ett utlämnande på eget initiativ kan vara nödvändigt

Alla myndigheter är beroende av att ha tillgång till den information som är av betydelse för riktigheten i de beslut som fattas eller för att olika författningsreglerade uppgifter ska kunna utföras. Av naturliga skäl finns sällan all relevant information hos beslutsmyndigheten. Uppgifter som är av betydelse för myndigheters beslutsfattande m.m. finns i stället ofta hos fysiska eller juridiska personer. I många situationer har enskilda därför en långtgående uppgiftsskyldighet till myndigheterna och i vissa fall även en skyldighet att bevara visst underlag för att möjliggöra efterhandskontroller. Exempel på detta är bl.a. 110 kap. socialförsäkringsbalken som innehåller krav på att enskilda på heder och samvete lämnar uppgifter som är av betydelse för bedömningar i fråga om ersättning och tillämpning av bestämmelserna i balken i övrigt, och avdelning VI i skatteförfarandelagen som behandlar kontrolluppgifter, deklarationer och övriga uppgifter.

Den information som behövs för att en myndighet ska kunna utföra sina uppgifter finns dock ofta hos en annan myndighet, ibland genom att en enskild lämnat information till den andra myndigheten. Det kan också röra sig om att en annan myndighet har fattat ett beslut som har betydelse för en annan myndighets beslut eller gjort iakttagelser om förhållanden som är av betydelse för en annan myndighets verksamhet. Utlämnande av uppgifter från en myndighet till en annan kan alltså vara en förutsättning för att den mottagande myndigheten ska kunna få det underlag som behövs för att kunna fatta korrekta beslut eller på andra sätt utföra författningsreglerad verksamhet.

Informationsutbyte mellan myndigheter kan också bidra till att förenkla för enskilda, genom att de inte behöver förse en myndighet med uppgifter som redan lämnats till en annan myndighet, eller visa upp beslut som en annan myndighet redan har fattat. Möjligheten att

utbyta uppgifter utgör därför en viktig förutsättning för att myndigheter ska kunna fullgöra sina uppgifter, erbjuda medborgarnytta och för en fungerande samverkan mellan myndigheter i övrigt.[41]

I de allra flesta situationer saknar dock en myndighet närmare kännedom om vilka beslut som fattas och iakttagelser som gjorts av andra myndigheter. Utan sådan kännedom finns det inte heller skäl för att begära ut några uppgifter från den myndighet som fattat ett beslut eller gjort en relevant iakttagelse. Utlämnande av uppgifter från en myndighet till en annan, på initiativ av den utlämnande myndigheten, kan alltså vara nödvändigt för att den mottagande myndigheten ska kunna få det underlag som behövs för att kunna fatta korrekta beslut eller på andra sätt utföra författningsreglerad verksamhet. Annorlunda uttryckt är det just *informationsunderskottet* hos mottagaren som motiverar behovet av att lämna ut information från en myndighet till en annan. Hade mottagaren redan haft kännedom om de relevanta uppgifterna hade något behov av att lämna ut uppgifter inte heller funnits.

Sammanfattning

När en myndighet förfogar över uppgifter eller har kännedom om förhållanden som har betydelse för eller behövs inom en annan myndighets verksamhet bör det på ett generellt plan, vad gäller uppgifter som inte är sekretessbelagda i förhållande till mottagaren, vara både berättigat och relevant att uppgifterna kommer den berörda myndigheten till handa. Något förbud mot att röja uppgifterna finns ju inte enligt sekretesslagstiftningen. Myndigheter har också en långtgående skyldighet att lämna ut sådana uppgifter om detta begärs av den mottagande myndigheten.

I vissa situationer kräver dock ett berättigat informationsutbyte att den utlämnande myndigheten på eget initiativ har möjlighet att lämna ut uppgifterna, eftersom den mottagande myndigheten saknar kännedom om att uppgifterna över huvud taget existerar hos den utlämnande myndigheten. För att ett berättigat och relevant infor-

[41] Jfr t.ex. prop. 2023/24:85, *En ny lag om uppgiftsskyldighet för att motverka felaktiga utbetalningar från välfärdssystemen samt fusk, regelöverträdelser och brottslighet i arbetslivet*, s. 1, prop. 2022/23:34, *Utbetalningsmyndigheten*, s. 27, prop. 2020/21:160, *Säkrare samordningsnummer och bättre förutsättningar för korrekta uppgifter i folkbokföringen*, s. 18 och prop. 2019/20:123, *Ett effektivare informationsutbyte mellan polis och socialtjänst vid samverkan mot terrorism*, s. 18 och 19.

mationsutbyte mellan myndigheter ska kunna genomföras är det alltså i vissa fall nödvändigt att uppgifter lämnas på initiativ av den mottagande myndigheten.

4.8.4 Nuvarande begränsningar av möjligheten att på eget initiativ lämna uppgifter är inte motiverade

Vår bedömning: Mot bakgrund av den befintliga regleringen i 6 kap. 5 § offentlighets- och sekretesslagen saknas det bärande skäl att begränsa myndigheters möjlighet att på eget initiativ lämna uppgifter som inte är sekretessbelagda till en annan myndighet.

Skälen för vår bedömning

Uppgifter som inte är sekretessbelagda och finalitetsprincipen

Som vi redan konstaterat finns det i dag ingen generell reglering i svensk rätt som uttryckligen ger stöd åt utlämnande på eget initiativ av uppgifter som inte är sekretessbelagda till en annan myndighet. Vi har inte funnit några tydliga uttalanden om myndigheters handlingsutrymme vad gäller att utan en föregående begäran lämna ut uppgifter som inte är sekretessbelagda till en annan myndighet, vare sig i förarbetena till 1980 års sekretesslag eller förarbetena till offentlighets- och sekretesslagen.[42] Såvitt vi kunnat se har lagstiftaren alltså inte redovisat några tydliga överväganden om de mer övergripande konsekvenserna av att en uppgift *inte* är sekretessbelagd. Myndigheters handlingsutrymme vad gäller uppgifter som inte är sekretessbelagda, utöver det som framgår av 6 kap. 5 § OSL (som tidigare framgick av 15 kap. 5 § sekretesslagen) är alltså inte närmare behandlat i förarbeten. Det går följaktligen inte heller att förarbetesvägen hitta fram till vad som ursprungligen var tänkt att gälla i en situation när en myndighet på eget initiativ överväger att lämna uppgifter som inte är sekretessbelagda till en annan myndighet.

[42] Jfr dock vad som sägs om utlämnande på begäran eller på eget initiativ i SOU 2003:99, *Ny sekretesslag*, s. 115–117. Här förefaller utgångspunkten eventuellt vara att uppgifter som inte är sekretessbelagda får lämnas ut på eget initiativ till andra myndigheter utan ytterligare stöd för detta.

I dag måste dock all behandling av personuppgifter som inte är sekretessbelagda – precis som i princip all annan personuppgiftsbehandling – uppfylla kraven i dataskyddsförordningen eller brottsdatalagen. Det innebär bl.a. att det måste finnas en rättslig grund för behandlingen, dvs. ett rättsligt stöd för myndighetens handlande, som möjliggör den. Någon *uttrycklig* sådan rättslig grund för utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ finns inte i svensk rätt i dag, och som vi nyss konstaterat finns det inte heller några uttalanden i relevanta förarbeten som kan tydliggöra innebörden av frånvaron av reglering.

Det finns därför skäl för oss att söka svar på vad det egentligen innebär ur ett dataskyddsperspektiv att en uppgift *inte* är sekretessbelagd. Detta gäller särskilt i förhållande till finalitetsprincipen, dvs. principen om ändamålsbegränsning, som framgår av artikel 5.1 b i dataskyddsförordningen. Finalitetsprincipen har en avgörande betydelse när vidarebehandling av personuppgifter diskuteras, och utlämnande av uppgifter utgör normalt en vidarebehandling av uppgifter för andra ändamål än de som de samlades in för (se vidare avsnitt 3.2).

Offentlighets- och sekretesslagen ska tillämpas parallellt med dataskyddsregleringen och det finns vissa likheter mellan regelverken

När en sekretessbestämmelse utformas är syftet att den inte ska innebära en större begränsning av allmänna handlingars offentlighet än vad som är nödvändigt för att skydda det intresse som bedöms vara skyddsvärt (jfr 2 kap. 2 § TF). Som en följd av det har de materiella sekretessbestämmelserna i offentlighets- och sekretesslagen olika styrka, föremål och räckvidd beroende på var inom den offentliga förvaltningen de ska tillämpas. Det som sekretessen skyddar är emellertid *uppgifter*, oavsett om dessa förkommer i allmänna handlingar eller inte (1 kap. 1 § andra stycket OSL).

När det gäller uppgifter om levande fysiska personer så träffar sekretessregleringen undantagslöst uppgifter som också är personuppgifter enligt den allmänna dataskyddsregleringen (jfr artikel 4.1 i dataskyddsförordningen och 21 kap. 7 § OSL). Begreppet personuppgifter omfattar dessutom även information som endast indirekt är kopplad till en fysisk person. Det kan vara uppgifter som snarare är kopplade till juridiska personer, t.ex. om ett aktiebolag har sin

grundares namn som firmabeteckning. Också t.ex. IP-adresser anses vara personuppgifter så länge det går att hänföra uppgifterna till en fysisk person genom en krypteringsnyckel.[43]

När personuppgifter, dvs. uppgifter om levande fysiska personer i vid mening, behandlas så ska alltså dataskyddsbestämmelserna tillämpas parallellt med sekretessregleringen. Det är följaktligen inte fråga om att det ena eller det andra regelverket ska tillämpas när en myndighet t.ex. överväger att lämna ut en uppgift till en annan myndighet. Båda regelverket måste i stället beaktas och tillämpas inför och vid ett utlämnande.

Sekretessbestämmelser som rör uppgifter om fysiska personer syftar i första hand till att värna den enskildes personliga integritet. Som utgångspunkt ska uppgifter som är sekretessbelagda därför inte vidarebefordras utanför den verksamhet i vilken de hämtats in (jfr 7 kap. 1 § OSL). Genom att sekretessregleringen även gäller mellan myndigheter hindras myndigheter från att lämna integritetskänsliga uppgifter vidare också till andra myndigheter.

I detta avseende har sekretessregleringen likheter med den dataskyddsrättliga finalitetsprincipen som innebär att det är förbjudet att vidarebehandla uppgifter för ändamål som är oförenliga med insamlingsändamålet. Precis som sekretessregleringen är syftet med dataskyddsbestämmelserna också i först hand att skydda enskildas personliga integritet (jfr artikel 1 i dataskyddsförordningen). Både sekretessregleringen och dataskyddsregleringen (finalitetsprincipen) utgår alltså från att uppgifter om enskilda inte får lämnas vidare till andra myndigheter, utan ska ”stanna” i det sammanhang där de först samlats in.

En annan likhet mellan sekretessbestämmelser och finalitetsprincipen är att det finns ett stort utrymme för att göra undantag från grundregeln i båda fallen. För sekretessbestämmelser gäller t.ex. 10 kap. 28 § OSL, dvs. att all sekretess oavsett styrka bryts av en författningsreglerad skyldighet att lämna ut uppgifter till en annan myndighet. När finalitetsprincipen tillämpas gäller (något förenklat) att vidarebehandling för oförenliga ändamål är tillåten om det finns stöd i lagstiftningen för sådan behandling (se avsnitt 3.2.2.).

[43] Jfr EU-domstolens avgörande i mål C-582/14, Patrick Breyer vs Bundesrepublik Deutschland, där dynamiska IP-adresser bedömdes vara personuppgifter när det, med hjälp av ytterligare information, fanns möjlighet till identifiering av fysiska personer utifrån sagda IP-adresser.

Det kan upprepas att dataskyddsregleringen, inklusive finalitetsprincipen, och sekretessregleringen ska tillämpas parallellt. Det innebär bl.a. att om det finns en sekretessbrytande bestämmelse som medger undantag från huvudregeln att uppgifter inte får vidarebefordras utanför den verksamhet i vilken de hämtats in, så finns det också stöd för vidarebehandlingen genom utlämnande, trots att denna behandling är oförenligt med insamlingsändamålet. En annan konsekvens av att regelverken ska tillämpas parallellt är att enbart det förhållande att det inte finns några sekretesshinder mot ett utlämnande inte medför att det utan undantag är tillåtet. Det kan t.ex. vara så att en uppgift är överflödig i förhållande till syftet med utlämnandet, och därför inte får lämnas ut, trots att den inte är sekretessbelagd i förhållande till mottagaren. Detta följer av principen om uppgiftsminimering (artikel 5.1 c i dataskyddsförordningen).

En och samma prövning?

Som framgår ovan finns det möjligheter att göra undantag både från tillämpliga bestämmelser om sekretess och från principen om att uppgifter inte får vidarebehandlas för något ändamål som strider mot insamlingsändamålet. I båda fallen krävs dock att undantagen framgår av lagstiftningen, och när ett sådant undantag har gjorts genom sekretessbrytande bestämmelser och uppgiftsskyldigheter så utgör undantaget ett rättsligt stöd för vidarebehandling av uppgifterna under de villkor som anges i bestämmelsen.

En viktig skillnad mellan regelverken är dock att dataskyddsförordningen utgår från att det är förbjudet att vidarebehandla uppgifter för oförenliga ändamål, och kräver att lagstiftaren aktivt tar ställning till när detta ska vara *tillåtet*. Motsatsvis utgår offentlighets- och sekretesslagens bestämmelser från offentlighetsprincipen, dvs. att uppgifter ska få lämnas ut för att tillgodose insynsintresset, och här krävs i stället att lagstiftaren aktivt tar ställning till när utlämnandet *inte* är tillåtet. De två regelverken kan alltså sägas närma sig frågan om integritetsskydd från motsatta håll; i ena fallet är vidarebehandlingen förbjuden om den inte är tillåten enligt lagstiftningen, i andra fallet är utlämnandet tillåtet om det inte är förbjudet enligt sekretessregleringen. Att de två regelverken ska tillämpas parallellt kompliceras av detta förhållande.

I olika sammanhang har det tidigare gjorts gällande att syftet med finalitetsprincipen blir uppfyllt genom bestämmelser om sekretess och undantag från sekretess. I betänkandet *Ny sekretesslag* (SOU 2003:99) som låg till grund för offentlighets- och sekretesslagen uttalades t.ex. följande.[44]

> Finalitetsprincipen är ett integritetsskydd. Den har utformats i en politisk miljö där majoriteten av medlemsstaterna saknar en offentlighetsprincip och därmed inte heller har samma sekretessreglering som vi har. Vi har på grund av offentlighetsprincipen en detaljerad sekretessreglering där integritetskänsliga uppgifter har givits ett sekretesskydd. Sekretessen gäller inte bara gentemot enskilda, utan även mellan myndigheter och mellan olika självständiga verksamhetsgrenar inom samma myndighet. I vissa fall har lagstiftaren infört sekretessbrytande regler som innebär att sekretesskyddade uppgifter under vissa förutsättningar får lämnas till en eller flera andra myndigheter.
>
> Genom denna ordning uppnås samma syfte som man vill åstadkomma genom finalitetsprincipen. Myndigheterna hindras att lämna ut integritetskänsliga uppgifter till andra myndigheter, för ändamål som av lagstiftaren bedömts vara oförenliga med de ändamål för vilka uppgifterna samlats in. De uppgifter som inte försetts med något sekretesskydd eller som omfattas av sekretessbrytande regler har av lagstiftaren ansetts vara av sådan karaktär att utlämnanden till andra myndigheter, eller, när det gäller sekretessbrytande regler, vissa myndigheter, inte kan anses vara oförenliga med det ändamål för vilket uppgifterna samlats in. Detta ställningstagande kommer till uttryck i 15 kap. 5 § sekretesslagen.

I betänkandet *Myndighetsdatalag* (SOU 2015:39), som i och för sig inte lett till lagstiftning, gjordes en något mindre tillåtande bedömning än den som redogjorts för ovan. Här uttalas nämligen inget om vad som ska gälla för uppgifter som inte har försetts med något sekretesskydd. Däremot tydliggjordes utredningens ställningstagande i frågan om förhållandet mellan sekretess och finalitetsprincipen i följande uttalanden.[45]

> När det gäller frågan om utlämnande av personuppgifter till andra myndigheter eller till enskilda är det alltså vår uppfattning att behandling i form av utlämnanden är förenliga med finalitetsprincipen så länge som utlämnandena som sådana sker i överensstämmelse med lag eller förordning enligt vilken uppgifterna får eller ska lämnas ut. Härmed avses i första hand utlämnanden till annan myndighet enligt 6 kap. 5 § OSL och utlämnanden av sekretessreglerade uppgifter till en annan myndighet eller enskild, på begäran eller på eget initiativ, som sker med stöd

[44] SOU 2003:99, *Ny sekretesslag*, s. 232. I den efterföljande propositionen kom dock inte detta till uttryck.
[45] SOU 2015:39, *Myndighetsdatalag*, s. 284.

> av någon sekretessbrytande bestämmelse. Vi menar alltså att lagstiftaren genom att reglera ett uppgiftslämnande får anses ha tagit ställning till att sådana utlämnanden som ska eller får ske inte är oförenliga med ursprungliga ändamål. Myndigheterna är alltså bundna av den prövning enligt finalitetsprincipen som lagstiftaren gjort genom exempelvis en sekretessbrytande bestämmelse.

Högsta förvaltningsdomstolens uttalanden i rättsfallet HFD 2021 ref. 10 tyder på att domstolen ansluter sig till den bedömning som redogörs för i betänkandet *Ny sekretesslag*. I avgörandet uttalade domstolen nämligen följande.

> Genom sekretessbestämmelser hindras myndigheterna från att lämna bl.a. integritetskänsliga uppgifter till andra myndigheter. *Härigenom får lagstiftaren anses ha tagit ställning till när ett uppgiftslämnande är oförenligt med det eller de ändamål för vilka uppgifterna samlades in.* [Vår kursivering.] Utöver sekretessprövningen ska den personuppgiftsansvariga myndigheten således inte göra någon kontroll av förenligheten med finalitetsprincipen i samband med lämnande av uppgifter enligt 6 kap. 5 § offentlighets- och sekretesslagen.

Detta förhållningssätt, dvs. att prövningen av om en vidarebehandling genom utlämnande till en annan myndighet är förenligt med finalitetsprincipen i svensk rätt görs av lagstiftaren genom bestämmelserna i offentlighets- och sekretesslagen, är dock inte tydligt fastslaget i någon författning (se även avsnitt 5.2.4).

Vad bör då gälla för utlämnande på eget initiativ av uppgifter som inte är sekretessbelagda?

Som vi nämnt flera gånger tidigare finns det sedan länge en generell och långtgående skyldighet för myndigheter att lämna uppgifter som inte är sekretessbelagda till en annan myndighet som begär det, men ingen generell reglering som uttryckligen tillåter att samma uppgifter lämnas till samma myndighet utan en föregående begäran. Skyldigheten att på begäran lämna ut uppgifter som inte är sekretessbelagda är ett uttryck för myndigheters samverkansskyldighet som bl.a. framgår av förvaltningslagen och som begränsas av sekretessregleringen. Vi bedömer att frågan om vad som bör gälla för utlämnande på eget initiativ av uppgifter som det med stöd av 6 kap. 5 § OSL hade funnits en skyldighet att lämna ut bör besvaras med utgångspunkt i den bestämmelsen.

Först bör det åter poängteras att *samtliga* uppgifter som inte är sekretessbelagda och som kan komma att lämnas ut på eget initiativ träffas av bestämmelsen i 6 kap. 5 § OSL. Ett utlämnande på eget initiativ av uppgifter som inte är sekretessbelagda medför alltså inte att fler uppgifter än i dag skiftar rättslig karaktär från att vara sekretessbelagda till att inte vara det. Alla uppgifter som skulle kunna lämnas ut på initiativ av den utlämnande myndigheten är alltså sådana som den utlämnande myndigheten inte skulle kunna neka mottagaren att ta del av om en begäran hade framställts, om inte utlämnande varit så resurskrävande att det hindrat arbetets behöriga gång.

En av principerna bakom offentlighets- och sekretesslagen är dessutom att alla tystnadsplikter i det allmännas verksamhet ska framgå av den lagen, både i förhållande till enskilda och myndigheter.[46] Sekretessen enligt 1980 års sekretesslag, som också motsvarar dagens reglering, skulle därför i princip ha direkt giltighet också i myndigheternas verksamhet och en sekretessbelagd uppgift skulle inte få lämnas vare sig till annan myndighet eller till annan verksamhetsgren inom den egna myndigheten, eller fritt kunna utnyttjas av myndigheten eller dess personal.[47] Uppgifter som inte är sekretessbelagda är motsatsvis uppgifter som med en tillämpning av offentlighets- och sekretesslagen är av sådant slag att det *inte* ska råda något förbud mot att lämna ut dem (jfr definitionen av sekretess i 3 kap. 1 § OSL). Trots att vi inte funnit förarbetsuttalanden som ger tydlig vägledning i frågan förefaller lagstiftaren alltså ursprungligen ha utgått från att uppgifter som inte är sekretessbelagda ska kunna lämnas till en annan myndighet på eget initiativ när det finns skäl för det, särskilt mot bakgrund av principen om myndigheters skyldighet att samverka.

Att utlämnande efter en begäran uttryckligen reglerats i motsats till utlämnande på eget initiativ skulle kunna förklaras av att det har funnits ett behov av att klargöra och fastställa myndigheters *skyldighet* gentemot varandra. Myndigheter har ju, till skillnad från enskilda, ingen grundlagsskyddad rätt att ta del av allmänna handlingar hos en annan myndighet.[48] Motsatsvis kan man tänka sig att det inte har uppfattats finnas något behov av att lagstifta om en rättslig möjlighet

[46] Se t.ex. uttalandena i prop. 1979/80:2, *med förslag till sekretesslag m.m.* Del A, s. 68 och 91 m.fl. sidor, prop. 1990/91:131, *om vissa frågor om internationellt samarbete i brottmål m.m.*, s. 26, och Justitiedepartementets broschyr, *Offentlighetsprincipen och sekretess – Kortfattat om lagstiftningen*, s. 23 och 24.
[47] Prop. 1979/80:2, *med förslag till sekretesslag m.m.* Del A, s. 120.
[48] Jfr prop. 1948:230, *med förslag till tryckfrihetsförordning m.m.*, s. 122 och 123.

som inte kräver något av myndigheterna, och som mot bakgrund av principen bakom sekretessregleringen, sammantaget med myndigheters skyldighet att samverka, kan ha uppfattats som självklar. Lagstiftaren bör dessutom inte ha haft någon möjlighet att förutse att EU-rättsliga krav på den nationella lagstiftningen med tiden skulle medföra att ett sådant uppgiftsutbyte trots allt skulle komma att sakna rättsligt stöd. Att svensk rätt inte anpassats till överordnade normer (dvs. dataskyddsförordningen) i detta avseende kan vara ett förbiseende från lagstiftarens sida i samband med att dataskyddsförordningen började tillämpas i maj 2018. Det befintliga hindret mot att på eget initiativ lämna uppgifter som inte är sekretessbelagda till en annan myndighet kan då inte sägas vara ett resultat av medvetna överväganden från lagstiftaren sida, utan snarast oavsiktligt.

Skyldigheten att på begäran lämna uppgifter som inte är sekretessbelagda till en annan myndighet är dessutom inte förenad med ett krav på att den mottagande myndigheten ska ha ett behov av uppgifterna för att skyldigheten ska inträda. Det behovsrekvisit som är vanligt förekommande i särskilt reglerade uppgiftsskyldigheter förefaller alltså ha ersatts av kravet på en begäran i 6 kap. 5 § OSL. En utgångspunkt måste här ha varit att myndigheter inte samlar in eller begär att få ta del av information som saknar betydelse för verksamheten, inte minst med beaktande av legalitetsprincipen. Utifrån det synsättet uppnås, genom kravet på att en begäran ska föregå utlämnandet, ett grundläggande skydd även för uppgifter om enskilda som annars inte är sekretessbelagda, eftersom uppgifterna därigenom inte kan spridas godtyckligt mellan myndigheter eller för illegitima syften.

En begäran är dock inte avgörande för om ett legitimt behov av att utbyta information föreligger eller inte. Tvärtom kan ett sådant behov av ett utlämnande i många situationer uppstå just av den anledningen att den mottagande myndigheten *saknar kännedom* om den aktuella uppgiften eller förhållandet som avses. Som vi redogjort för i avsnitt 4.5 kommer detta synsätt bl.a. till uttryck genom de många bestämmelser om uppgiftsskyldighet utan föregående begäran som förekommer i befintlig lagstiftning. Den omständigheten att den mottagande myndigheten redan känner till uppgiften kan i stället medföra att något behov av utlämnande inte finns.[49]

[49] Jfr t.ex. prop. 2020/21:160, *Säkrare samordningsnummer och bättre förutsättningar för korrekta uppgifter i folkbokföringen*, s. 101.

Bestämmelser om uppgiftsskyldighet som inte kräver en begäran är många gånger utformade i syfte att bryta förekommande sekretess och för detta krävs enligt 10 kap. 28 § första stycket OSL en skyldighet att lämna ut uppgifter. Sådana bestämmelser innehåller ofta rekvisitet att ett utlämnande får ske om det kan antas ha betydelse för mottagaren.

I den här aktuella situationen, när uppgifterna som avses per definition inte är sekretessbelagda, ”räcker det” med en uttalad rättslig möjlighet att lämna uppgifterna om det finns skäl för det. Ett rekvisit som föreskriver att uppgifter som inte är sekretessbelagda får lämnas om det finns anledning att anta att uppgifterna behövs hos mottagaren borde dessutom fylla samma syfte som kravet att en begäran ska föregå utlämnandet enligt 6 kap. 5 § OSL. På så sätt tillåter inte regleringen att uppgifter som inte är sekretessbelagda sprids godtyckligt mellan myndigheter eller för illegitima syften.

Som vi nämnt ovan har Högsta förvaltningsdomstolen i avgörandet HFD 2021 ref. 10 uttalat 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. Det uttalandet skulle kunna leda till slutsatsen att lagstiftaren också har tagit ställning till att vidarebehandling genom utlämnande till en annan myndighet alltid är förenlig med insamlingsändamålet vad avser uppgifter som inte är sekretessbelagda. Om detta förhållningssätt skulle vara vägledande framstår det som tveksamt om lagstiftarens tänkta dataskyddsrättsliga ställningstagande endast skulle vara avhängigt den mottagande myndighetens begäran och inte den omständigheten att uppgifterna faktiskt inte är sekretessbelagda. Detta gäller särskilt mot bakgrund av syftet med sekretessregleringen, dvs. att ställa upp samtliga förbud mot att lämna ut uppgifter av hänsyn till bl.a. enskildas personliga integritet som ska gälla (jfr avsnitt 5.4.4). Att sekretessregleringen därmed även begränsar myndigheters samverkansskyldighet talar för den slutsatsen.

Under alla förhållanden finns det i dag, genom HFD 2021 ref. 10, ett vägledande avgörande som slår fast att ett utlämnande med stöd av 6 kap. 5 § OSL är förenligt med finalitetsprincipen. Mot den bakgrunden bör det i vart fall inte direkt strida mot finalitetsprincipen att *samma uppgifter* lämnas ut för i princip *samma syften* till samma *potentiella mottagare,* men på eget initiativ.

Sammanfattning

Vår sammantagna bedömning är att det saknas bärande skäl att begränsa myndigheters möjlighet att på eget initiativ lämna uppgifter som inte är sekretessbelagda till en annan myndighet på det sätt som sker i dag. Skillnaden mellan att en myndighet begär att få del av uppgifter som inte är sekretessbelagda och att en utlämnande myndighet lämnar *samma uppgifter* på eget initiativ kan rimligen inte vara avgörande för om behandlingen bör tillåtas eller inte, under förutsättning att det finns anledning att anta att uppgiften behövs i den mottagande myndighetens verksamhet.

Mot bakgrund av de kartlagda behoven och den i vissa fall avgörande betydelsen av att myndigheter kan lämna uppgifter till en annan myndighet när det finns skäl för det, finns det dessutom starka skäl för en förändring av den befintliga regleringen. Att nuvarande reglering dessutom kan vara ett resultat av lagstiftarens förbiseende i samband med att dataskyddsförordningen började tillämpas talar ytterligare för detta. I fortsättningen bör därför myndigheternas möjligheter att på eget initiativ lämna uppgifter som inte är sekretessbelagda till andra myndigheter inte begränsas på det sätt som sker i dag. Genom en tydligt tillåtande reglering av att uppgifter som inte är sekretessbelagda får lämnas ut på initiativ av den utlämnande myndigheten, när det finns skäl för det, läks också den otydlighet som finns när den rättsliga grunden finns i de befintliga sekretessbrytande bestämmelserna i offentlighets- och sekretesslagen (jfr avsnitt 4.8.2).

4.8.5 En ny generell bestämmelse om utlämnande av uppgifter som inte är sekretessbelagda

Vårt förslag: En myndighet ska få lämna en uppgift till en annan myndighet utan en begäran, om uppgiften inte är sekretessbelagd och utlämnandet kan antas vara av betydelse för att den utlämnande eller den mottagande myndigheten ska kunna fullgöra sin författningsreglerade verksamhet

Skälen för vårt förslag

Uppgifter som inte är sekretessbelagda och myndigheters samverkan

Vår bedömning i de föregående avsnitten är sammanfattningsvis att det finns ett behov av att införa ett rättsligt stöd för myndigheter att på eget initiativ lämna uppgifter som inte är sekretessbelagda till en annan myndighet. Det finns inte några sakliga skäl som kan motivera dagens regleringssituation, dvs. å ena sidan en långtgående skyldighet att på begäran lämna uppgifter som inte är sekretessbelagda till en annan myndighet, samtidigt som ett utlämnande å andra sidan av samma uppgifter på eget initiativ många gånger i praktiken är förbjudet, oavsett behovet eller nyttan av utlämnandet i övrigt.

Vi har även bedömt att det finns ett behov av att förtydliga regleringen avseende utlämnande på eget initiativ av uppgifter som inte är sekretessbelagda av den anledningen att de träffas av en sekretessbrytande bestämmelse i offentlighets- och sekretesslagen. I dag framgår endast att sekretess inte hindrar att en sådan uppgift lämnas till en annan myndighet, om förutsättningarna i bestämmelsen är uppfyllda.

I departementspromemorian *Utökat informationsutbyte* föreslogs att det skulle införas en bestämmelse i offentlighets- och sekretesslagen som skulle komplettera regleringen i 6 kap. 5 § OSL om utlämnande av uppgifter som inte är sekretessbelagda till andra myndigheter på begäran av mottagaren. Om en bestämmelse utformas på ett sådant sätt, dvs. att den i likhet med regleringen i 6 kap. 5 § OSL tar sikte på uppgifter som inte är sekretessbelagda – oavsett varför uppgifterna inte är sekretessbelagda – skulle båda de övergripande behov som vi har identifierat tillgodoses. En sådan bestämmelse skulle alltså ge ett rättsligt stöd för att på eget initiativ lämna ut uppgifter som inte är sekretessreglerade, uppgifter som omfattas av ett undantag från sekretess och uppgifter som efter en sekretessprövning inte är sekretessbelagda till en annan myndighet. Den skulle dessutom ge ett tydligare rättsligt stöd för att på eget initiativ lämna ut uppgifter som inte är sekretessbelagda av den anledningen att uppgifterna träffas av en sekretessbrytande bestämmelse i offentlighets- och sekretesslagen.

Vi förslår därför att det införs en ny bestämmelse som ger myndigheterna ett tydligt rättsligt stöd för att på eget initiativ lämna en uppgift som inte är sekretessbelagd till andra myndigheter. Bestämmelsen kommer i likhet med 6 kap. 5 § OSL att träffa alla uppgifter

som inte är sekretessbelagda, oavsett om detta beror på att de t.ex. är undantagna från sekretess eller träffas av en sekretessbrytande bestämmelse i offentlighets- och sekretesslagen. Bestämmelsen bör därför ses som ett komplement till den befintliga regleringen i 6 kap. 5 § OSL, som anses utgöra en precisering av den allmänna samverkansskyldighet som gäller för myndigheter enligt 8 § FL. Även den bestämmelse som vi föreslår kan därmed sägas reglera ett generellt rättsligt förhållande mellan myndigheter, dvs. principen att alla myndigheter ska samarbeta med och bistå varandra i den utsträckning som är möjlig, där utbyte av information är ett viktigt led. Det är en princip som det svenska förvaltningsrättsliga systemet bygger på.[50]

Samverkan mellan myndigheter begränsas dock av sekretessregleringen.[51] Både 6 kap. 5 § OSL och den bestämmelse vi föreslår avser enbart uppgifter som inte är sekretessbelagda.

Den bestämmelse som vi föreslår kommer i likhet med bestämmelserna i 6 kap. 4 och 5 §§ OSL att ta sikte på myndigheternas utlämnande av uppgifter. Det framstår som naturligt att placera bestämmelsen i anslutning till dessa bestämmelser. Den nya bestämmelsen bör därför lämpligen placeras i en ny paragraf i 6 kap. 5 a § OSL.

Utlämnandet ska antas vara av betydelse för att den utlämnande eller den mottagande myndigheten ska kunna fullgöra sin författningsreglerade verksamhet

En första förutsättning för att utlämnande med stöd av den förslagna bestämmelsen ska kunna komma i fråga är alltså att uppgifterna inte är sekretessbelagda. Frågan är vad som i ska krävas i övrigt.

Enligt den generella sekretessbrytande bestämmelsen som vi föreslagit i vårt delbetänkande är det inte den mottagande myndighetens behov av uppgiften som är avgörande för om utlämnande ska kunna ske. Det avgörande är i stället att utlämnandet behövs för något av de syften som anges i bestämmelsen. Detta innebär t.ex. att även sådant uppgiftsutlämnande som sker från en myndighet för att den mottagande myndigheten ska kunna kontrollera om den har en uppgift som den utlämnande myndigheten har för avsikt att efterfråga i ett senare skede ska vara tillåtet enligt bestämmelsen (se SOU 2024:63, avsnitt 6.5).

[50] SOU 2015:39, *Myndighetsdatalag*, s. 167.
[51] Jfr prop. 1979/80:2, *med förslag till sekretesslag m.m.*, Del A, s. 89 och 361.

En begränsning av den föreslagna bestämmelsen som innebär att ett utlämnande ska kunna komma i fråga endast om den mottagande myndigheten behöver uppgiften riskerar enligt vår mening att bli alltför snäv. Ett uppgiftsutlämnande enligt bestämmelsen bör också kunna ske för den utlämnande myndighetens skull. En myndighet kan exempelvis behöva lämna ut uppgifter som inte är sekretessbelagda för att den mottagande myndigheten ska kunna kontrollera om den har en uppgift som den utlämnande myndigheten i ett senare skede har för avsikt att efterfråga, precis som vi föreslagit avseende den generella sekretessbrytande bestämmelsen. Enligt vår bedömning bör det avgörande i stället vara om *själva utlämnandet* har betydelse för att antingen den mottagande myndigheten eller den utlämnande myndigheten ska kunna fullgöra sin författningsreglerade verksamhet.

En annan fråga är vilken grad av utredning som ska krävas när det gäller frågan om utlämnandets betydelse. I många fall kommer det inte att vara möjligt för den utlämnande myndighet att med någon högre grad av säkerhet slå fast att ett utlämnande faktiskt kommer att ha en sådan betydelse som sägs ovan. Detta borde särskilt gälla i de fall utlämnandet sker därför att det har betydelse för den mottagande myndigheten ska kunna fullgöra sin författningsreglerade verksamhet. Vår slutsats blir därmed att det för att utlämnande enligt bestämmelsen ska kunna ske inte bör krävas att det är klarlagt att det kommer att ha betydelse för den utlämnande eller den mottagande myndighetens författningsreglerade verksamhet.

Rekvisitet *kan antas* eller andra uttryck med liknande betydelse är gängse när det gäller befintliga skyldigheter att lämna uppgifter på eget initiativ (jfr avsnitt 4.5). Det innebär att tröskeln för i vilka situationer uppgifter får lämnas på initiativ av den utlämnande myndigheten är lågt satt. De kan t.ex. vara i sådana situationer som framgår av vår fördjupade kartläggning, dvs. när en myndighet fattar ett beslut eller får information om ett förhållande och där beslutet eller förhållandet typiskt sett har en betydelse för riktigheten i beslut eller verksamheten i övrigt hos en annan myndighet.

Som framgår av redogörelsen i avsnitt 4.5 har skyldigheter att lämna uppgifter på eget initiativ i regel införts för att den myndighet som uppgiftsskyldigheten gäller i förhållande till ska kunna fatta riktiga beslut och i övrigt kunna bedriva sin verksamhet. Dessa bestämmelser är i många fall avgränsade på olika sätt. Den bestämmelse vi nu föreslår är generellt utformad och träffar alltså fler situationer

än särskilda uppgiftsskyldigheter. Särskilt reglerade uppgiftsskyldigheter och sekretessbrytande bestämmelser bör dock kunna tjäna till vägledning vid tillämpningen av den bestämmelse vi föreslår. Man bör exempelvis kunna utgå ifrån att ett utlämnande av en viss *typ* av uppgifter som i en viss situation träffas av en skyldighet att lämna ut dem också kan antas vara av betydelse för att den mottagande myndigheten ska kunna fullgöra sin författningsreglerade verksamhet och därmed vara möjlig att lämna ut enligt den bestämmelse som vi föreslår. Detta förutsätter att övriga förutsättningar för utlämnande enligt bestämmelsen är uppfyllda, dvs. främst att uppgifterna inte är sekretessbelagda i det enskilda fallet.

Mot denna bakgrund föreslår vi att ett utlämnande av uppgifter som inte är sekretessbelagda på initiativ av den utlämnande myndigheten bör vara tillåtet redan när det kan antas att det har betydelse för att den utlämnande eller den mottagande myndigheten ska kunna fullgöra sin författningsreglerade verksamhet.

Föregående samråd och rutinmässiga utlämnanden

Syftet med den föreslagna bestämmelsen är att den ska utgöra ett tydligt rättsligt stöd för att på den utlämnande myndighetens initiativ lämna ut uppgifter som inte är sekretessbelagda till en annan myndighet. Detta gäller oavsett om utlämnandet sker därför att det kan antas vara av betydelse för att den utlämnande eller den mottagande myndigheten ska kunna fullgöra sin författningsreglerade verksamhet.

I sakens natur ligger att det är myndigheten själv som i regel bäst kan avgöra vilka uppgifter den behöver för att kunna fatta korrekta beslut och i övrigt bedriva sin verksamhet. Även om bestämmelsen kommer att medge utlämnande av uppgifter på eget initiativ bör man därför kunna utgå ifrån att utlämnande som sker för att det kan antas vara av betydelse för att en annan myndighet ska kunna fullgöra sin författningsreglerade verksamhet ofta kommer att föregås någon form av dialog mellan utlämnande och mottagande myndighet. Vid tveksamhet om rekvisitet *kan antas* är uppfyllt kan den myndighet som bedömer att den har uppgifter som kan antas vara av betydelse för en annan myndighets verksamhet självfallet kontakta den andra myndighet för att kontrollera om uppgifterna efterfrågas eller inte. En sådan kontakt kan resultera i

att den mottagande myndigheten begär ut uppgifterna och att det första utlämnandet därmed sker på begäran, och att efterföljande utlämnandena sker rutinmässigt och på den utlämnande myndighetens egna initiativ.[52]

Nödvändigt utlämnande?

Bestämmelsen om nödvändigt utlämnande i 10 kap. 2 § OSL innebär att sekretess inte hindrar att en uppgift lämnas till en enskild eller till en annan myndighet, om det är nödvändigt för att den utlämnande myndigheten ska kunna fullgöra sin verksamhet.

Den bestämmelse som vi föreslår innebär som nyss sagts att en myndighet får lämna ut uppgifter som inte är sekretessbelagda till en annan myndighet bl.a. om det kan antas vara av betydelse för att den utlämnande myndigheten ska kunna fullgöra sin författningsreglerade verksamhet. Såväl den bestämmelse vi nu föreslår som bestämmelsen om nödvändigt utlämnande möjliggör alltså uppgiftslämnande i den utlämnande myndighetens intresse. Något bör därför sägas om hur dessa bestämmelser förhåller sig till varandra.

Bestämmelsen om nödvändigt utlämnande i 10 kap. 2 § OSL är en sekretessbrytande bestämmelse. Om en tillämpning av 10 kap. 2 § OSL mynnar ut i att sekretess inte hindrar att annars sekretessbelagda uppgifter lämnas ut så är uppgifterna inte sekretessbelagda i förhållande till mottagaren. Vidare får sådana uppgifter som träffas av 10 kap. 2 § OSL, i likhet med vad som gäller för alla uppgifter som träffas av sekretessbrytande bestämmelser i offentlighets- och sekretesslagen, lämnas ut på eget initiativ.

Den bestämmelse vi nu föreslår bryter ingen sekretess i sig eftersom den tar sikte på uppgifter som av olika skäl bedömts inte vara sekretessbelagda. Bestämmelsen ger ett rättsligt stöd för att på eget initiativ lämna ut uppgifter som inte är sekretessreglerade, uppgifter som omfattas av ett undantag från sekretess och uppgifter som efter en sekretessprövning inte är sekretessbelagda till en annan myndighet. När det gäller sådana annars sekretessbelagda uppgifter som träffas av sekretessbrytande bestämmelser i offentlighets- och sekretesslagen, exempelvis bestämmelsen i 10 kap. 2 § OSL, kommer

[52] Jfr prop. 2000/01:129, *Ökat informationsutbyte mellan arbetslöshetsförsäkringen, socialförsäkringen och studiestödet*, s. 60 och prop. 2007/08:160, *Utökat elektroniskt informationsutbyte*, s. 56.

bestämmelsen endast utgöra ett förtydligande av vad som redan gäller, dvs. att uppgifterna får lämnas ut på eget initiativ.

Något om bestämmelsens förhållande till uppgiftsskyldigheter

Även om den generella sekretessbrytande bestämmelsen som vi föreslagit i SOU 2024:63 införs så kommer det också i fortsättningen finnas uppgifter som är sekretessbelagda i förhållande till andra myndigheter och som enbart kommer att kunna lämnas ut om det finns en skyldighet att göra det. I avsnitt 4.4.3 har vi redogjort för att uppgifter som är sekretessbelagda i förhållande till mottagaren fram till dess en begäran har framställts inte heller kommer att träffas av reglering som avser utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ. Det är en naturlig följd av att uppgifterna fortsatt är sekretessbelagda så länge ingen begäran har framställts. Införandet av en generell bestämmelse om utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ kommer alltså inte påverka informationsutbyten som enbart är tillåtna på grund av bestämmelser om uppgiftsskyldighet på begäran.

Det förekommer dock att en skyldighet att på begäran lämna uppgifter till en annan myndighet träffar uppgifter som annars *inte* är sekretessbelagda i förhållande till mottagaren. Det kan t.ex. avse beslut som är undantagna från sekretess eller uppgifter som efter en prövning enligt en tillämplig materiell sekretessbestämmelse inte är sekretessbelagda. I dessa fall kommer den föreslagna bestämmelsen att ge stöd åt ett utlämnande, oavsett om en begäran har framställts eller inte. Förutsättningen för utlämnandet på eget initiativ är ju att uppgifterna inte är sekretessbelagda i förhållande till mottagaren, vilket de inte kommer vara i dessa fall.

Införandet av en generell bestämmelse om utlämnande på eget initiativ av uppgifter som inte är sekretessbelagda kommer dock träffa samma uppgifter som omfattas av en skyldighet att på eget initiativ lämna uppgifter till en annan myndighet, oavsett om dessa annars är sekretessbelagda eller inte. I dessa fall kan det alltså uppfattas uppstå en dubbelreglering. En bestämmelse om uppgiftsskyldighet på eget initiativ utgör dock en specialreglering av utlämnandet i fråga som till skillnad från den här föreslagna bestämmelsen innebär en skyldighet att lämna ut uppgifterna. En uppgiftsskyldighet är

alltså något annat än den bestämmelse vi föreslår, som enbart ger ett rättsligt stöd åt utlämnandet men inte kräver något av den utlämnande myndigheten. Någon egentlig konkurrens mellan bestämmelser om uppgiftsskyldighet på eget initiativ och den nya bestämmelsen bör därför inte uppkomma. Myndigheterna får med andra ord iaktta tillämpliga bestämmelser om uppgiftsskyldighet på eget initiativ oberoende av den nya bestämmelsen.

Uppgifter som kan antas vara av betydelse för andra myndigheter som inte dokumenteras

Det förekommer att myndigheter uppmärksammar förhållanden som kan antas vara av betydelse för andra myndigheters verksamhet, men som inte är relevanta inom den egna verksamheten (se avsnitt 4.7.3). Någon generell skyldighet att dokumentera uppgifter som inte har någon direkt koppling till den egna myndighetens verksamhet föreligger inte. I många fall borde det i själva verket vara så att myndigheterna anser sig vara förhindrade att dokumentera sådana uppgifter, t.ex. av det skälet att det saknas en rättslig grund enligt dataskyddsregleringen att behandla uppgifterna. Om en medarbetare hos en myndighet uppmärksammar förhållanden som inte dokumenteras finns uppgifterna om dessa förhållanden endast som en minnesbild hos medarbetaren. En särskild fråga är om sådana uppgifter ska kunna lämnas ut enligt den bestämmelse vi föreslår.

I 1 kap. 1 § andra stycket OSL anges att lagen innehåller bestämmelser om tystnadsplikt i det allmännas verksamhet och om förbud att lämna ut allmänna handlingar. Vidare sägs att dessa bestämmelser avser förbud att röja uppgift, vare sig detta sker muntligen, genom utlämnande av allmän handling eller på något annat sätt (jfr även definitionen av sekretess i 3 kap. 1 § OSL). Sekretessbestämmelserna innebär alltså såväl tystnadsplikt som handlingssekretess. Om en uppgift är sekretessbelagd råder det med andra ord ett förbud att röja den oavsett om den finns i en handling hos myndigheten eller endast som en minnesbild hos en enskild medarbetare vid myndigheten.[53]

Av 6 kap. 5 § OSL framgår att en myndighet ska på begäran av en annan myndighet lämna uppgift som den förfogar över, om inte uppgiften är sekretessbelagd eller det skulle hindra arbetets behöriga

[53] Jfr prop. 1979/80:2, *med förslag till sekretesslag m.m.*, Del B s. 91 och 92.

gång. Den bestämmelsen är alltså begränsad till att avse uppgifter som myndigheten *förfogar över* och som inte är sekretessbelagda.

I lagmotiven till 15 kap. 5 § i 1980 års sekretesslag, som motsvarar bestämmelsen i 6 kap. 5 § OSL, klargörs inte vad som närmare krävs för att en myndighet ska anses förfoga över en uppgift.[54] Kammarrätten har emellertid i ett fall funnit att en myndighet inte kan anses förfoga över en uppgift som endast finns som en minnesbild hos en anställd vid en myndighet. För att en myndighet ska anses förfoga över en uppgift krävs att den finns dokumenterad i en handling eller på annat sätt.[55]

Som vi framhåller i delbetänkandet finns enligt vår bedömning anledning att ta fasta på nämnda kammarrättsavgörande (se SOU 2024:63, avsnitt 6.4). I det följande utgår vi därför ifrån att en myndighet endast kan anses förfoga över en uppgift som finns dokumenterad i en handling eller på annat sätt. Det innebär att *skyldigheten* enligt 6 kap. 5 § OSL endast träffar uppgifter som är dokumenterade. Den bestämmelse som vi föreslår kommer inte att innebära annat än en *möjlighet* för myndigheterna att på eget initiativ lämna ut en uppgift som inte är sekretessbelagd till en annan myndighet. I alla händelser kan det alltså inte uppstå någon skyldighet för myndigheten att lämna ut uppgifter som endast finns som en minnesbild hos en enskild medarbetare. I det avseendet finns det alltså en avgörande skillnad mellan 6 kap. 5 § OSL och den bestämmelse vi föreslår.

De sekretessbrytande bestämmelserna i offentlighets- och sekretesslagen är vidare inte begränsade till att endast avse uppgifter som myndigheterna förfogar över, dvs. uppgifter som har dokumenterats (se SOU 2024:63, avsnitt 6.4). En uppgift som träffas av en sekretessbrytande bestämmelse får därmed lämnas ut med stöd av bestämmelsen även om den endast finns som en minnesbild hos en enskild medarbetare hos myndigheteten.

Ett av syftena med den bestämmelse vi föreslår är att det ska förtydligas att uppgifter som träffas av de sekretessbrytande bestämmelserna i offentlighets- och sekretesslagen får lämnas ut på eget initiativ. På samma sätt som det är möjligt att lämna ut annars sekretessbelagda uppgifter som endast finns som en minnesbild hos en medarbetare hos en myndighet med stöd av de sekretessbrytande bestämmelserna i offentlighets- och sekretesslagen bör det följaktligen

[54] Prop. 1979/80:2, *med förslag till sekretesslag m.m.*, Del A, s. 361.
[55] Kammarrätten i Stockholm, dom i mål nr 2354-11, 2011-11-25.

vara möjligt att lämna ut dessa uppgifter med stöd av den bestämmelse vi föreslår. I bestämmelsen bör det därför inte uppställas något hinder mot att lämna ut uppgifter som endast finns som en minnesbild hos en enskild medarbetare hos en myndighet. Det ska alltså inte krävas att myndigheten förfogar över uppgiften, i den mening begreppet getts i ovan relaterade kammarrättsavgörande.

En sådan reglering innebär inte att varjehanda tanke hos en medarbetare vid en myndighet kan bli föremål för utlämnande enligt bestämmelsen eller att utlämnande av uppgifter som inte är dokumenterade annars kan ske godtyckligt. Ett utlämnande av en uppgift som inte har dokumenterats måste – på samma sätt som när det är fråga om uppgifter som har dokumenterats – uppfylla villkoren i bestämmelsen. För att utlämnande ska kunna ske måste det alltså vara fråga om en uppgift som inte är sekretessbelagd och det måste kunna antas att utlämnandet är av betydelse för att den utlämnande eller den mottagande myndigheten ska kunna fullgöra sin författningsreglerade verksamhet.

Att muntligen lämna ut information till en annan myndighet som inte är dokumenterad men som innehåller personuppgifter utgör inte i sig någon automatiserad behandling av personuppgifter. Dataskyddsregleringen är dock tillämplig på behandling av personuppgifter som inte är automatiserad om personuppgifterna är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.[56] Av 27 § FL framgår t.ex. att det finns en grundläggande skyldighet för en myndighet som får uppgifter på något annat sätt än genom en handling att snarast dokumentera dem, om de kan ha betydelse för ett beslut i ärendet. En skyldighet att dokumentera vissa uppgifter finns också på andra håll i lagstiftningen, tex. i 5 kap. OSL. Enligt vår bedömning innebär detta att dataskyddsregleringen i många situationer kommer att vara tillämplig vid muntligt uppgiftslämnande till andra myndigheter av uppgifter som inte har dokumenterats vid den utlämnande myndigheten. Detta medför att de grundläggande principerna i artikel 5 i dataskyddsförordningen måste iakttas, vilket bl.a. innebär att uppgifterna som lämnas ut ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas, enligt principen om uppgiftsminimering, som framgår av artikel 5.1 c.

[56] Se artikel 2.1 och 4.6 i dataskyddsförordningen och 1 kap. 3 § BDL.

5 Den kompletterande dataskyddsregleringen – en översyn

5.1 Inledning

5.1.1 Uppdraget

I vårt delbetänkande *Ökat informationsutbyte mellan myndigheter. Behov och föreslagna förändringar* (SOU 2024:63) föreslog vi att en generell sekretessbrytande bestämmelse införs i offentlighets- och sekretesslagen (2009:400), OSL. Den föreslagna bestämmelsen tar bort vissa sekretesshinder mellan myndigheter vad gäller uppgifter om enskildas personliga eller ekonomiska förhållanden. Bestämmelsen utgör också en rättslig grund för den behandling av personuppgifter som informationsutbyte med stöd av bestämmelsen innebär.

I avsnitt 4.8.5 har vi föreslagit att ytterligare en generell bestämmelse ska införas i offentlighets- och sekretesslagen. Den bestämmelsen ger ett tydligt rättsligt stöd åt att på den utlämnande myndighetens initiativ lämna ut uppgifter som inte är sekretessbelagda, när det kan antas att utlämnandet är av betydelse för att den utlämnande eller den mottagande myndigheten ska kunna fullgöra sin författningsreglerade verksamhet.

De två förslag som vi hittills har lämnat utgör tillsammans en generell, förenklad och mer tillåtande reglering av myndigheters informationsutbyte än den befintliga. Förslagen är avsedda att tillgodose de behov av förbättrade möjligheter till informationsutbyte mellan myndigheter som vi kartlagt och redovisat i vårt delbetänkande.

Sektors- eller myndighetsspecifika bestämmelser om personuppgiftsbehandling i kompletterande dataskyddslagstiftning, ofta kallat registerförfattningar, ska tillämpas parallellt med offentlighets- och

sekretesslagen. I våra direktiv nämns att det i sådana författningar kan finnas begränsningar av möjligheten att dels behandla personuppgifter för att kunna lämna ut och ta emot dem, dels lämna ut dem elektroniskt. Sådana bestämmelser kan alltså utgöra ett hinder mot att utbyta uppgifter med stöd av bestämmelserna i offentlighets- och sekretesslagen. För att syftet med våra förslag ska kunna uppnås kan alltså den kompletterande dataskyddsregleringen i vissa fall behöva ändras.

Vårt uppdrag i denna del är därför att göra en översyn av den kompletterande dataskyddsregleringen för att möjliggöra att de förslag som lämnats tjänar sitt syfte och kan tillämpas på ett ändamålsenligt sätt, och att lämna nödvändiga författningsförslag.

5.1.2 Kapitlets disposition

Sedan början av 1970-talet har den kompletterande dataskyddsregleringen utvecklats på ett i det närmaste organiskt sätt. Med det menas att lagstiftningen har växt fram till synes utan riktning eller samordning från lagstiftarens sida. Lagstiftaren har t.ex. inte haft någon konsekvent hållning i centrala frågor. I stället har det på olika områden gjorts olika rättsliga bedömningar av likadana grundförhållanden, vilket avspeglat sig i lagstiftningens varierande utformning. Lagstiftaren har inte heller använt eller utvecklat någon enhetlig begreppsapparat, trots att föremålet för regleringen (myndigheters automatiserade personuppgiftsbehandling) varit detsamma sedan flera decennier. Lagstiftaren har inte heller, trots upprepade påpekanden om behovet,[1] genomfört någon samlad analys och översyn av området. Den kompletterande dataskyddsregleringen utgör därför ett förhållandevis komplext rättsområde. För att sätta våra senare överväganden i sitt rätta sammanhang bedömer vi att det är nödvändigt att inledningsvis redogöra för några generella aspekter av den kompletterande dataskyddsregleringen. I avsnitt 5.2. beskriver vi därför översiktligt rättsområdets bakgrund och utveckling utifrån hur den allmänna regleringen har förändrats. Där redogör vi även översiktligt för den rättsliga och tekniska utvecklingen, samt hur grunddragen i den kompletterande dataskyddsregleringen inte förändrats i takt med dessa.

[1] Jfr t.ex. uppräkningen i SOU 2015:39, *Myndighetsdatalag*, s. 106–110.

I avsnitt 5.3 redogörs sedan för vad, och vilka författningar, som omfattas av vår översyn av den kompletterande dataskyddsregleringen, samt de behov som vi kartlagt på området.

Ändamålsbestämmelser i kompletterande dataskyddsreglering är en av de kategorier av bestämmelser som omfattas av översynen. Ändamålsbestämmelser, en problematisering av deras förhållande till offentlighets- och sekretesslagen och några exempel på uttömmande ändamålsbestämmelser behandlas i avsnitten 5.4.1–5.4.3.

I avsnitt 5.4.4 redogör vi för vår bedömning av hur begränsningar av utbytet av uppgifter mellan myndigheter ska regleras i svensk rätt. Vår bedömning av ändamålsbestämmelsernas faktiska förhållande till offentlighets- och sekretesslagens bestämmelser ges i avsnitt 5.4.5, och i avsnitt 5.4.6 föreslår vi sedan att det ska införas en upplysningsbestämmelse som tydliggör förhållandet mellan de olika regelverken i kompletterande dataskyddsreglering som omfattas av vår översyn. Eventuella behov av följdändringar behandlas i avsnitt 5.4.7.

Regleringen av vidarebehandling och utlämnande i dataskyddsreglering inom brottsbekämpningen behandlas i avsnitt 5.5.1. I avsnitt 5.5.2 lämnas sedan förslag på hur denna ska förändras.

I avsnitten 5.6.1–5.6.2 behandlas sedan elektroniskt utlämnande och regleringen av sådant utlämnande mellan myndigheter. I avsnitt 5.6.3 lämnar vi slutligen förslag på ny reglering av elektroniskt utlämnande i kompletterande dataskyddsreglering som omfattas av vår översyn.

5.2 Kompletterande dataskyddsreglering – då och nu

5.2.1 Allmänt om sektors- eller myndighetsspecifika bestämmelser om dataskydd

Kompletterande bestämmelser

I kapitel 3 i vårt delbetänkande (SOU 2024:63) har vi beskrivit generella normer kring myndigheters informationshantering, personlig integritet, dataskydd och sekretess. Där lämnas en samlad redogörelse över bestämmelser i den allmänna dataskyddsregleringen,

dvs. dataskyddsförordningen[2] och lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning, dataskyddslagen, och brottsdatalagen (2018:1177), BDL. Det som sägs där upprepas inte i detta sammanhang.

Kompletterande dataskyddsreglering, det som ofta kallas registerförfattningar, har till skillnad från generella bestämmelser om dataskydd ett begränsat tillämpningsområde och avser normalt personuppgiftsbehandling inom en viss verksamhet, vid en viss myndighet eller inom en viss sektor. De sektorsspecifika bestämmelserna förhåller sig alltid till den allmänna regleringen och kan sägas fylla ut denna. Kompletterande reglering kan även innehålla undantag från de allmänna bestämmelserna, i den mån sådana undantag är tillåtna enligt överordnad reglering.

Det bör påpekas att ett flertal myndigheter och sektorer inte har någon kompletterande dataskyddsreglering att förhålla sig till. I dessa fall tillämpas bara den allmänna dataskyddsregleringen. Eftersom behovet av och syftet med kompletterande reglering varierar utgör den kompletterande dataskyddsregleringen i många fall en mindre beståndsdel i lagstiftning som i övrigt innehåller bestämmelser av materiell eller processuell art, se t.ex. 114 kap. socialförsäkringsbalken, SFB, och 1 a kap. vapenlagen (1996:67). Både socialförsäkringsbalken och vapenlagen innehåller huvudsakligen bestämmelser som *inte* utgör kompletterande dataskyddsreglering.

I andra fall finns den kompletterande regleringen i en särskild lag och/eller förordning, se t.ex. lagen (2001:181) om behandling av uppgifter i Skatteverkets beskattningsverksamhet och lagen (2001:454) om behandling av personuppgifter inom socialtjänsten, med respektive tillhörande förordningar. Exemplen utgör s.k. informationshanteringsförfattningar, som är tillämpliga inom hela eller en stor del av en myndighets kärnverksamhet.

Det krävs dock inte att behandlingen är särskilt omfattande för att kompletterande reglering ska motivera en separat författning. Även mycket integritetskänslig behandling kan regleras särskilt i en egen författning (jfr avsnitt 5.4.7).

[2] 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).

Faktiska registerförfattningar

Viss registerföring som i dag är reglerad i kompletterande dataskyddsreglering har en lång historik. Lantmäteriets fastighetsregister och Skatteverkets folkbokföring är ett par exempel med månghundraåriga anor, som tidigare haft delvis andra syften och reglerats på annat sätt än i dag. Det har även förekommit författningsreglering av registerföring under lång tid i den meningen att det i författning föreskrivits att vissa register med visst innehåll ska föras och med en närmare reglering av registerverksamheten. Exempelvis har den nuvarande lagen (1998:620) om belastningsregister föregångare i lagen om allmänt kriminalregister från år 1963 som i sin tur föregicks av lagen om straffregister från år 1900.[3]

När föremålet för regleringen är ett register som *ska föras* rör det sig om bestämmelser som inte enbart reglerar personuppgiftsbehandling inom en viss verksamhet. Sådana faktiska registerförfattningar (eller registerbestämmelser, om regleringen finns insprängd i annan lagstiftning) medför i stället att en eller flera myndigheter ges ett materiellt uppdrag att föra registret i enlighet med bestämmelserna i författningen. Faktiska registerförfattningar skiljer sig alltså från annan kompletterande dataskyddsreglering, som inte ålägger en myndighet en skyldighet att bedriva ytterligare verksamhet än den som framgår av annan reglering.

Det är dock svårt att alltid dra en skarp gräns mellan faktiska registerförfattningar (eller -bestämmelser) och annan kompletterande dataskyddsreglering. Det finns t.ex. flera författningar som både innehåller bestämmelser av kompletterande dataskyddskaraktär och bestämmelser som föreskriver att ett register ska föras.

5.2.2 Den kompletterande dataskyddsregleringens bakgrund

Allmänt

Dagens kompletterande dataskyddsreglering har sin bakgrund i samhällets ökande användning av digital teknik under slutet av 1900-talet och den integritetsdebatt som följde i spåren på denna utveckling. Den debatten var i och för sig inte begränsad till Sverige utan fördes i flera länder. År 1970 utlöste dock den svenska folk- och bostads-

[3] SOU 2015:39, *Myndighetsdatalag*, s. 83 och 84.

räkningen som genomfördes med hjälp av ADB (dvs. automatisk databehandling) en särskilt intensiv debatt om den nya tekniken och dess användning i landet. I debatten kritiserades den digitala insamlingen av uppgifter om människor, deras attityder och levnadsförhållanden bl.a. för att öka myndigheternas makt och möjligheter att styra enskildas handlingar. En faktor som också ansågs vara betydelsefull var den psykologiska effekt som vetskapen om ADB-teknikens möjligheter medförde. Det ansågs därför behöva finnas insyns- och kontrollmöjligheter gentemot dem som hade tillgång till den nya tekniken, i syfte att enskilda skulle kunna lita på att deras integritet respekterades både av andra enskilda och av myndigheter.[4]

Någon generell regel om fredande av privatlivet gentemot myndighet fanns dessutom inte i svensk rätt vid tidpunkten. Det efterlystes därför en datalagstiftning med regler om vad som skulle vara tillåtet för myndigheter och enskilda i fråga om att använda digital teknik.[5] År 1973 infördes så en särskild lag, datalagen (1973:289) som skulle tillgodose behovet av en datalagstiftning. Datalagen var den första i sitt slag i världen.[6]

1973 års datalag

I datalagen användes begreppet personregister som utgångspunkt för regleringen. Med personregister avsågs enligt 1 § datalagen register, förteckning eller andra anteckningar som fördes med hjälp av automatisk databehandling, ADB, och som innehöll personuppgift som kunde hänföras till den som avsågs med uppgiften. Varje sammanställning av personuppgifter med hjälp av ADB ansågs under datalagen innebära att ett personregister hade inrättats.[7]

Utgångspunkten i datalagen var ursprungligen att bara den som anmält sig till Datainspektionen (numera Integritetsskyddsmyndigheten, IMY) och fått licens för det skulle få inrätta och föra personregister. I samband med att ett sådant tillstånd lämnades skulle Datainspektionen också meddela föreskrift om ändamålet med registret,

[4] Prop. 1973:33, *med förslag till ändringar i tryckfrihetsförordningen m.m.*, s. 44.
[5] SOU 2007:22, *Skyddet för den personliga integriteten – kartläggning och analys*, s. 498 och 499 samt prop. 1973:33, *med förslag till ändringar i tryckfrihetsförordningen m.m.*, s. 40–42.
[6] SOU 1993:10, *En ny datalag*, s. 16.
[7] Jfr Ds 2001:67, *Behandling av personuppgifter i den arbetsmarknadspolitiska verksamheten*, s. 17.

och om särskilda skäl förelåg fick tillståndet begränsas till viss tid. För att få inrätta och föra känsliga register krävdes dessutom ett särskilt tillstånd från Datainspektionen. Ett sådant tillstånd behövdes i regel för att inrätta och föra register med uppgifter om brott och brottsmisstankar, uppgifter om hälsotillstånd eller sexualliv, omdömen om den registrerade eller personuppgifter som hämtats från något annat register. Om ett personregister beslutats av riksdagen eller regeringen krävdes dock inget tillstånd.[8]

Datainspektionen skulle enligt datalagen, i den mån det behövdes för att förebygga risk för otillbörligt intrång i personlig integritet, meddela föreskrifter för tillståndsgivna register. Föreskrifterna skulle i dessa fall avse bl.a. inhämtande av uppgifter för personregistret, vilka personuppgifter som fick ingå i personregistret, utförandet av den automatiska databehandlingen, den tekniska utrustningen, de bearbetningar av personuppgifterna i registret som fick göras med automatisk databehandling och de personuppgifter som fick göras tillgängliga.[9]

Under datalagens giltighetstid reglerades dock myndigheters personregister ofta i särskilda lagar och dessa personregister krävde som nämnts inte särskilt tillstånd från Datainspektionen. Registerförfattningarna byggde dock på att den generellt tillämpliga datalagen ”fyllde ut” där det inte fanns särregler.[10] Även för särskilt reglerade register kunde Datainspektionen dessutom bemyndigas att meddela särskilda föreskrifter om ändamål m.m.

Regeringens uttalade målsättning har under en lång tid varit att register med ett stort antal registrerade och ett särskilt känsligt innehåll skulle meddelas i form av lag. Enligt Konstitutionsutskottet har det varit av stor betydelse att en författningsreglering av ADB-register (dvs. automatiserad personuppgiftsbehandling) kommit till stånd i syfte att stärka skyddet för de registrerades integritet i samband med nödvändig registrering av känsliga uppgifter i myndighetsregister.[11] Dessa uttalanden har därefter påverkat lagstiftningsmodellen vad gäller den kompletterande dataskyddsregleringen under en lång tid.[12]

[8] 2, 2 a, 5 och 4 §§ datalagen.
[9] 6 § datalagen.
[10] SOU 1997:39, *Integritet – Offentlighet – Informationsteknik*, s. 209.
[11] Prop. 1990/91:60, *om offentlighet, integritet och ADB*, s. 58 och bet. 1990/91:KU11 s. 11.
[12] Se t.ex. uppräkningen i SOU 1997: 39, *Integritet – Offentlighet – Informationsteknik*, s. 204–206.

Personuppgiftslagen

Genom personuppgiftslagen (1998:204), PUL, som genomförde 1995 års dataskyddsdirektiv[13], upphävdes datalagen. Utgångspunkten i personuppgiftslagen, som kompletterades av personuppgiftsförordningen (1998:1191), var att behandling av personuppgifter skulle vara tillåten i de fall och på de villkor lagen angav.[14] Det tidigare licens- och tillståndsförfarandet avseende personregister avskaffades därmed också slutligt och myndigheter kunde därför behandla personuppgifter direkt med stöd av personuppgiftslagen. Datainspektionen hade dock fortsatt befogenhet att bl.a. meddela vissa föreskrifter enligt bestämmelserna i personuppgiftsförordningen. Dessa föreskrifter kunde t.ex. avse i vilka fall behandling av personuppgifter var tillåten och vilka krav som skulle ställas på den personuppgiftsansvarige.[15]

I personuppgiftslagen användes inte begreppet register över huvud taget för olika samlingar av uppgifter. Däremot uttalade regeringen i lagens förarbeten att det inom den offentliga sektorn ofta förekom stora mängder känsliga uppgifter och uppgifter som hade hämtats in med stöd av straffsanktionerad uppgiftsplikt. Därför var det särskilt viktigt med ett starkt integritetsskydd när det gällde uppgifter inom all offentlig verksamhet. Myndighetsregister med ett stort antal registrerade och ett särskilt känsligt innehåll skulle därför som utgångspunkt regleras särskilt i lag, liksom tidigare.[16]

När datalagen ersattes av personuppgiftslagen kom också vissa äldre sektorsspecifika registerlagar, som hade införts när datalagen gällde, att ersättas av en modernare variant av registerlag. Trots att det inte längre fanns ett krav på tillstånd och licens från Datainspektionen, eller beslut av riksdag eller regering, för att en myndighet skulle få behandla personuppgifter automatiserat ansågs det som redan nämnts i flera fall ändå finnas ett behov av att särskilt reglera myndigheters digitala hantering av uppgifter. Begreppet databas började då användas i flera, men inte alla, sammanhang.

[13] Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.
[14] Prop. 1997/98:44, *Personuppgiftslag*, s. 64.
[15] 16 § personuppgiftsförordningen.
[16] Prop. 1997/98:44, *Personuppgiftslag*, s. 41.

Att en myndighets databas eller motsvarande skulle eller fick finnas reglerades därför ofta i lag, tillsammans med bestämmelser om bl.a. ändamålen med behandlingen, sökbegränsningar, elektroniskt utlämnande och gallringsfrister. Vilka uppgifter som fick ingå i databaser, uppgiftssamlingar eller register reglerades dock normalt i förordning och inte i lag.[17]

Även om många äldre lagar ersattes av ny reglering i samband med att personuppgiftslagen infördes så bibehölls alltså den grundläggande regleringsmodellen från datalagens tid.

Dataskyddsförordningen och dataskyddslagen

Dataskyddsförordningen, som ersatte 1995 års dataskyddsdirektiv, började tillämpas i maj 2018 och utgör sedan dess en generell reglering för behandling av personuppgifter inom EU. I Sverige kompletteras dataskyddsförordningen på ett generellt plan av dataskyddslagen. När dataskyddslagen infördes upphävdes personuppgiftslagen.

I dataskyddslagens förarbeten gjordes flera överväganden om tolkningen av centrala delar i dataskyddsförordningen, bl.a. avseende de krav som ställs i relation till den rättsliga grund för behandling som i huvudsak är aktuell för myndigheter (artikel 6.1 c och 6.1 e).

Regeringens bedömning var sammanfattningsvis att dataskyddsförordningens krav på att den grund för behandling som vanligtvis aktualiseras för myndigheter ska vara fastställd i enlighet med unionsrätten eller den nationella rätten inte innebär ett krav på att själva behandlingen av personuppgifter måste regleras. Regeringen uttalade att det i stället är den rättsliga förpliktelsen, uppgiften av allmänt intresse respektive myndighetsutövningen som ska ha stöd i rättsordningen. Den rättsliga förpliktelsen, uppgiften av allmänt intresse respektive myndighetsutövningen var enligt regeringen fastställd i enlighet med svensk rätt, om den följer av författning eller beslut som har meddelats i enlighet med regeringsformens bestämmelser.[18]

[17] Jfr t.ex. 4 § i den numera upphävda förordningen (2001:720) om behandling av personuppgifter i verksamhet enligt utlännings- och medborgarskapslagstiftningen, 2 § i den numera upphävda förordningen (2003:766) om behandling av personuppgifter inom socialförsäkringens administration och 3–5 §§ förordningen (2002:623) om behandling av personuppgifter i den arbetsmarknadspolitiska verksamheten.
[18] Prop. 2017/18:105, *Ny dataskyddslag*, s. 48.

Enligt regeringen krävdes alltså inte en reglering i nationell rätt av den personuppgiftsbehandling som ska ske med stöd av dessa rättsliga grunder. Regeringen bedömde dock att det även fortsättningsvis fanns ett utrymme för sådan sektorsspecifik särreglering om behandling av personuppgifter som finns i de svenska registerförfattningarna (dvs. kompletterande dataskyddsreglering).[19] Dataskyddslagen är därför subsidiär i förhållande till sådan reglering.

Anpassningen av de sektorsspecifika författningarna behandlades inte i lagstiftningsärendet om dataskyddslagen. Däremot gjordes en generell översyn av sektorsspecifika kompletterande dataskyddsbestämmelser i flera olika sammanhang. Den översyn, eller snarare de översyner, som då gjordes var huvudsakligen inriktade på att anpassa den sektorsspecifika regleringen till dataskyddsförordningen, bl.a. genom att upphäva hänvisningar till personuppgiftslagen och införa hänvisningar till dataskyddsförordningen och dataskyddslagen. Någon djupare analys av de sektorsspecifika bestämmelserna skedde inte i dessa sammanhang. Däremot har några sådana lagstiftningsinitiativ initierats under de senaste åren.[20]

Brottsdatalagen

2016 års datasskyddsrättsliga reform inom EU medförde även ett nytt regelverk för personuppgiftsbehandling som utförs av brottsbekämpande myndigheter, 2016 års dataskyddsdirektiv[21]. Brottsdatalagen genomför 2016 års dataskyddsdirektiv i nationell rätt och är liksom dataskyddslagen subsidiär i förhållande till sektorsspecifik reglering.

Vid tidpunkten för brottsdatalagens införande fanns det redan sektorsspecifik reglering för de brottsbekämpande myndigheterna, som kompletterade personuppgiftslagen. Regeringen konstaterade dock att anpassningen av vissa myndigheters registerförfattningar till brottsdatalagen skulle innebära omfattande strukturella och redak-

[19] Prop. 2017/18:105, *Ny dataskyddslag*, s. 22.
[20] Se t.ex. SOU 2024:57, *Ett nytt regelverk för hälsodataregister*, SOU 2024:7, *Ett säkrare och mer tillgängligt fastighetsregister* och SOU 2023:100, *Framtiden dataskydd – Vid Skatteverket, Tullverket och Kronofogden*.
[21] Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF.

tionella ändringar. Nackdelarna med att låta anpassningen till brottsdatalagen ske genom ändringslagar var enligt regeringen så stora att aktuella myndigheters registerförfattningar i stället borde upphävas och ersättas med nya lagar. De nya lagarna var dock i allt väsentligt baserade på de tidigare gällande författningarna och någon fullständig översyn av bestämmelserna genomfördes inte.[22]

5.2.3 Rättslig och teknisk utveckling

Allmänt

Då den sektorsspecifika regleringen kompletterar de allmänna bestämmelserna påverkar förändringar av det allmänna regelverket behovet och utformningen av kompletterande reglering. Om det t.ex. i den allmänna regleringen krävs särreglering på sektors- eller myndighetsnivå så har den kompletterande regleringen en annan betydelse än om det inte finns något sådant krav. Om den allmänna regleringen i stället förbjuder särreglering av vissa förhållanden så påverkar även detta utformningen av den kompletterande regleringen. Den rättsliga utvecklingen påverkar alltså både behovet av och syftet med den kompletterande dataskyddsregleringen.

Även den tekniska utvecklingen påverkar rättsområdet. 1973 års datalag kom till i det inledande skedet av digitaliseringen av den offentliga förvaltningen och samhället i stort. Vid den här tiden utgjorde informationshantering med digital teknik ett undantag från det normala, som då var manuell och analog handläggning, och det fanns endast cirka 340 ”datorsystem” som innehöll personuppgifter inom den offentliga sektorn.[23] Som vi redogjort för ovan fanns det samtidigt en utbredd rädsla för de möjligheter som den nya tekniken medförde. Sedan datorer och annan digital teknik började användas inom den offentliga sektorn har det därför i lagstiftningsarbetet genomgående lagts stor vikt vid att i integritetsskyddande syfte begränsa myndigheters möjlighet att använda digital teknik.

I förarbetena till datalagen uttalades dock att varje reglering som infördes på datahanteringsområdet behövde ses som ett provisorium. Det uttalades vidare vara fråga om lagstiftning på ett helt nytt område och om erfarenheten visade att regleringen i något avseende blev

[22] Prop. 2017/18:269, *Brottdatalag – kompletterande lagstiftning*, s. 97 och 98.
[23] SOU 1993:10, *En ny datalag*, s. 27.

onödigt betungande eller hämmande för utvecklingen behövde ändringar och kompletteringar kunna genomföras.[24] Även den tekniska utvecklingen påverkar alltså både behovet av och syftet med den kompletterande dataskyddsregleringen.

Tidigare påpekanden om anpassningen till den tekniska och rättsliga utvecklingen

Den kompletterande dataskyddsregleringen har under en lång tid och i olika sammanhang varit föremål för kritik, generellt eller avseende särskilda författningar. En stor del av kritiken går ut på att rättsområdet inte i tillräcklig utsträckning uppdaterats i takt med den rättsliga och tekniska utvecklingen.

Integritetsskyddskommittén[25] (Ju 2004:05) noterade att den reformering av registerförfattningarna som hade skett efter personuppgiftslagens ikraftträdande hade genomförts utan någon egentlig samordning vilket bl.a. lett till oklarheter i tillämpningen och svårigheter att överblicka regelverket.[26] Sammantaget var kommitténs analys att skyddet för den personliga integriteten väsentligt skulle förbättras om regelverket utformades enhetligare, tydligare och mer i överensstämmelse med bestämmelserna i framför allt (dåvarande) sekretesslagen.[27]

2005 års informationsutbytesutredning[28] (Fi 2005:08) konstaterade att registerförfattningarna saknade en enhetlig struktur och att begreppsbildningen på området var oklar och framtagen under en tid av helt andra och mer begränsade möjligheter till elektroniskt informationsutbyte. Dessa förhållanden skapade enligt utredningen onödiga hinder för utvecklingen. Den bristande strukturen i författningarna och den oklara begreppsbildningen orsakade dessutom tillämpningssvårigheter som enligt utredningen innebar ökade risker för oacceptabla intrång i den personliga integriteten.[29]

---

[24] Prop. 1973:33, *med förslag till ändringar i tryckfrihetsförordningen, m.m.*, s. 89 och 92.
[25] Integritetsskyddskommittén hade bl.a. i uppdrag att kartlägga och analysera skyddet för den personliga integriteten, samt överväga om skyddet i lagstiftningen behöver kompletteras, se dir. 2004:51.
[26] SOU 2007:22, *Skyddet för den personliga integriteten – Kartläggning och analys*, Del 1, s. 462.
[27] SOU 2007:22, *Skyddet för den personliga integriteten – Kartläggning och analys*, Del 1, s. 466.
[28] 2005 års informationsutbytesutredning hade bl.a. i uppdrag att pröva om det var lämpligt att vissa utökade möjligheter till elektroniska informationsutbyten mellan myndigheter infördes, se dir. 2005:91.
[29] SOU 2007:45, *Utökat elektroniskt informationsutbyte mellan myndigheter*, s. 393–395.

Informationshanteringsutredningen[30] (Ju 2011:11) redogjorde för bilden av registerlagstiftningen som ett svåröverblickbart och fragmenterat rättsområde. Den höga komplexiteten i regleringen förklarades bl.a. med att registerförfattningsregleringen bara är en del av det regelverk som styr en myndighets informationshantering, men anpassning till andra parallella regelverk hade inte alltid getts tillräcklig uppmärksamhet i lagstiftningsarbetet. Resultatet var bl.a. verkliga eller uppfattade motstridigheter vilket enligt utredningen medförde risk för tillämpningsproblem.[31] Utredningen ifrågasatte även i vilken mån det egentligen var till gagn för registrerades personliga integritet med den ”dubbelreglering” som ges genom att först föreskriva att myndigheten *ska* göra något i den materiella och processuella regleringen av verksamheten och sedan att den också *får* göra det i den dataskyddsrättsliga regleringen.[32]

Försäkringskassan och Pensionsmyndigheten konstaterade år 2020 att den digitala utvecklingen helt hade förändrat verksamheterna. Vid tillkomsten av den kompletterande dataskyddsregleringen var användningen av elektroniska, gemensamma system ett undantag snarare än huvudregel, och elektroniskt utlämnande ansågs då som särskilt integritetskänsligt. Den kompletterande dataskyddsregleringen försvårade därför den digitala utvecklingen. Myndigheterna, som både genomgått stora organisatoriska förändringar och fått nya uppdrag sedan den kompletterande dataskyddsregleringen utformades, saknade dessutom rättsliga förutsättningar för att i tillräcklig utsträckning dela uppgifter mellan varandra.[33]

Utredningen om dataskydd vid Skatteverket, Tullverket och Kronofogden[34] (Fi 2021:11) konstaterade att den inventering som utredningen genomfört visade att de berörda myndigheterna samstämmigt uppfattade den befintliga kompletterande dataskyddsregleringen som omodern och dåligt anpassad till digitaliseringen av myndigheternas

[30] Informationshanteringsutredningen hade bl.a. i uppdrag att utreda förutsättningarna för att skapa en generell, enhetlig och – helt eller i vart fall delvis – samlad reglering för myndigheternas personuppgiftsbehandling som kunde fungera som komplement till, eller genomföra delar av, den unionsrättsliga regleringen på området, se dir. 2011:86.
[31] SOU 2015:39, *Myndighetsdatalag*, s. 110–112.
[32] SOU 2015:39, *Myndighetsdatalag*, s. 280 och 281.
[33] Försäkringskassan och Pensionsmyndigheten, *Hemställan om ändringar i 114 kap. SFB och förordningen (2003:766) om behandling av personuppgifter inom socialförsäkringens administration*, (Försäkringskassans dnr FK 2020/001747, Pensionsmyndighetens dnr VER 2020-180), s. 43.
[34] Utredningen om dataskydd vid Skatteverket, Tullverket och Kronofogden hade bl.a. i uppdrag att göra en översyn av Skatteverkets, Tullverkets och Kronofogdemyndighetens registerförfattningar i syfte att skapa ändamålsenliga regler som är anpassade efter dagens behov, se dir. 2021:104.

verksamhet. Regleringen uppfattades även i flera fall som omotiverat hindrande för myndigheterna, utan att några uppenbara fördelar för skyddet av enskildas personliga integritet uppnåddes.[35] Det nyss sagda rörde bl.a. att ändamålsbestämmelserna kräver komplicerade analyser som saknar betydelse för den enskildes integritet och att regleringen avseende känsliga personuppgifter i vissa fall innebär direkta hinder mot att utföra författningsreglerad verksamhet. Regleringen ansågs dessutom inte anpassad till moderna ärendehanteringssystem där all handläggning sker digitalt.[36]

2024 års studiestödsdatautredning[37] (U 2024:02) konstaterade att Centrala studiestödsnämnden, CSN, hade redogjort för att den kompletterande dataskyddsregleringen bl.a. inte ger ett tydligt stöd för vilken personuppgiftsbehandling som myndigheten får utföra, vilket skapar osäkerhet kring tillåtligheten av personuppgiftsbehandling som är nödvändig för att myndigheten ska kunna utföra sitt uppdrag. Den kompletterande dataskyddsreglernigen innebär också enligt CSN att myndigheten i vissa fall är förhindrad att kontakta enskilda via e-post eller telefon och i stället måste skicka vanliga pappersbrev, att arbetet med nödvändiga kontroller vid misstanke om felaktiga utbetalningar hindras och att i andra sammanhang föreskrivet informationsutbyte med andra myndigheter inte är tillåtet.[38]

Den rättsliga utvecklingen – dataskyddsförordningen

Som vi nämnt tidigare gäller dataskyddsförordningens och dataskyddslagens bestämmelser i dag inom nästan hela den offentliga förvaltningen. EU:s dataskyddsreglering anses generellt sett vara den strängaste i världen.[39] Något krav på sådan nationell, sektorsspecifik reglering som funnits i svenska registerförfattningar och/eller dåvarande Datainspektionens föreskrifter sedan 1973 års datalag infördes finns dock inte i dataskyddsförordningen. För att säkerställa att EU-lagstiftningen ger samma skydd för alla medborgare

[35] SOU 2023:100, *Framtidens dataskydd – Vid Skatteverket, Tullverket och Kronofogden*, s. 320.
[36] SOU 2023:100, *Framtiden dataskydd – Vid Skatteverket, Tullverket och Kronofogden*, s. 502, 664 och 665.
[37] 2024 års studiestödsdatautredning hade bl.a. i uppdrag att göra en allmän översyn av CSN:s kompletterande dataskyddsreglering i syfte att skapa ändamålsenliga regler som är anpassade efter dagens behov, se dir. 2024:36.
[38] SOU 2024:95, *Modernt dataskydd vid CSN*, s. 136 och 137.
[39] Jfr Europiska rådet och Europeiska unionens råd, *Dataskydd inom EU*, tillgänglig: https://www.consilium.europa.eu/sv/policies/data-protection/ (hämtad 25-01-22).

inom hela EU har bestämmelser som finns i en EU-förordning dock företräde framför nationella lagar.[40] Dataskyddsförordningen ska alltså tillämpas av enskilda och myndigheter precis som om bestämmelserna i förordningen hade funnits i en svensk lag. Det innebär att den primära regleringen avseende personuppgiftsbehandling inom svenska myndigheter i dag finns i dataskyddsförordningen.

Dataskyddsförordningen baseras till stor del på 1995 års dataskyddsdirektivs struktur och innehåll men innebär även en rad förändringar. Förordningen ställer framför allt högre krav på personuppgiftsansvariga myndigheter än tidigare. I artikel 5.1 anges de grundläggande principerna för behandling, vilka även angavs i 1995 års dataskyddsdirektiv och personuppgiftslagen.[41] De grundläggande principerna innebär bl.a. att personuppgifter enbart får behandlas för särskilda och berättigade ändamål, att uppgifterna senare inte får behandlas på ett sätt om är oförenligt med insamlingsändamålen, att behandlingen inte får omfatta fler uppgifter än nödvändigt och att den inte får pågå längre än nödvändigt. Av artikel 5.2 i dataskyddsförordningen framgår att det är den personuppgiftsansvarige som ska ansvara för och kunna visa att de grundläggande principerna efterlevs.

För att behandling av personuppgifter över huvud taget ska vara laglig enligt dataskyddsförordningen krävs att något av de villkor som anges i artikel 6.1 i dataskyddsförordningen är uppfyllda. Av 10 § f PUL, liksom av artikel 7 i 1995 års dataskyddsdirektiv, framgick att även offentliga aktörer kunde behandla personuppgifter på grund av sitt s.k. *berättigade intresse*. Enligt dataskyddsförordningen kan en myndighet inte behandla personuppgifter på den grunden. Myndigheter kan i stället som utgångspunkt bara behandla personuppgifter om det är nödvändigt för att uppfylla en rättslig förpliktelse eller för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning (artikel 6.1 c och e).

Enligt dataskyddsförordningen ska dessutom den grund för behandling som avses i artikel 6.1 c och e fastställas i enlighet med unionsrätten eller den medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av (artikel 6.3). Något motsvarande krav på att grunden för en myndighets personuppgiftsbehandling skulle vara fastställd i unionsrätten eller den nationella rätten fanns

[40] Se bl.a. EU-domstolens dom den 15 juli 1964, Flaminio Costa mot E.N.E.L., mål 6/64.
[41] Artikel 6 i 1995 års dataskyddsdirektiv och 9 § PUL.

inte i 1995 års dataskyddsdirektiv eller i personuppgiftslagen. Det har därför ansetts möjligt att med stöd av 10 § d PUL utföra behandling av personuppgifter som var nödvändig för att utföra en arbetsuppgift av allmänt intresse, även om den rättsliga grunden inte var fastställd i författning eller liknande.[42] Dataskyddsförordningens bestämmelser om rättslig grund innebär däremot att bl.a. förpliktelser och uppgifter av allmänt intresse inte kan åberopas som rättsliga grunder för behandling av personuppgifter om den rättsliga grunden inte är fastställd i unionsrätten eller medlemsstatens nationella rätt.[43]

Vid behandling som omfattas av artikel 6.1 c och e i dataskyddsförordningen ska enligt artikel 6.3 också syftet med behandlingen fastställas i den rättsliga grunden eller, i fråga om behandling enligt punkten 6.1 e, vara nödvändigt för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning. Till skillnad från 1995 års dataskyddsdirektiv ställer artikel 6.3 dessutom upp ett uttryckligt krav på att unionsrätten eller medlemsstaternas nationella rätt ska uppfylla ett mål av allmänt intresse och vara proportionell mot det legitima mål som eftersträvas, för att kunna utgöra en rättslig grund för personuppgiftsbehandling.[44]

Dataskyddsförordningen innehåller dessutom ett stort antal bestämmelser om olika förhållanden kopplade till dataskydd. Bestämmelserna i förordningen rör alltså inte enbart grundläggande principer för behandling och vilken rättslig grund för behandling som måste föreligga. I förordningen finns även utförliga bestämmelser avseende den personuppgiftsansvariges ansvar för att genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att personuppgiftsbehandling utförs i enlighet med förordningens bestämmelser (artikel 24), bygga in dataskydd i de tekniska systemen för att rent teknisk säkerställa att de grundläggande principerna följs (artikel 25), och att vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en lämplig säkerhetsnivå (artikel 32).

Det finns även förfaranderegler om konsekvensbedömningar och samråd med de nationella tillsynsmyndigheterna vid behandling som kan innebära särskilt hög risk för de registrerade (artiklarna 35 och 36),

[42] SOU 2017:39, *Ny dataskyddslag – Kompletterande bestämmelser till EU:s dataskyddsförordning*, s. 111.
[43] Prop. 2017/18:95, *Anpassningar av vissa författningar inom skatt, tull och exekution till EU:s dataskyddsförordning*, s. 42.
[44] Jfr prop. 2017/18:105, *Ny dataskyddslag*, s. 50.

förfaranderegler vid gemensamt personuppgiftsansvar (artikel 26) och om personuppgiftsbiträden (artikel 28).

Dataskyddsförordningen innehåller dessutom flera utförliga bestämmelser om enskilda rättigheter, bl.a. avseende rätt till information om ändamålen med den behandling som utförs (kapitel III), samt bestämmelser om gränsöverskridande behandling av personuppgifter till tredjeland (kapitel V).

Ytterligare en skillnad mellan dataskyddsförordningen och 1995 års dataskyddsdirektiv är att tillsynsmyndigheternas befogenheter har stärkts, jfr artikel 58 i dataskyddsförordningen och artikel 28.3 i direktivet. I Sverige är det IMY som är tillsynsmyndighet. Genom dataskyddsförordningens bestämmelser om administrativa rättsmedel, ansvar och sanktioner (kapitel VIII) har IMY möjlighet att bl.a. påföra en myndighet administrativa sanktionsavgifter på upp till motsvarande 10 000 000 kronor om behandlingen strider mot de grundläggande principerna i dataskyddsförordningen, som kravet på att personuppgifter bara får samlas in för berättigade ändamål eller om den registrerade inte får sina rättigheter tillgodosedda (artikel 83.5 i dataskyddsförordningen och 6 kap. 2 § andra stycket dataskyddslagen).

Något om den tekniska utvecklingen

I Sverige har regeringen sedan länge haft det uttalade målet att landet ska vara bäst i världen på att använda digitaliseringens möjligheter.[45] Arbetet med att öka effektiviteten i myndigheternas verksamhet, med samverkan mellan myndigheter och med att ge medborgarna en förbättrad service är därför i dag i princip helt inriktat på att det ska ske på elektronisk väg.[46] Regeringen har också uppmärksammat att det i dagsläget mer eller mindre regelmässigt bör anses vara nödvändigt att använda tekniska hjälpmedel och därmed behandla personuppgifter på automatisk väg, eftersom en manuell informationshantering inte utgör ett realistiskt alternativ för vare sig myndigheter eller företag.[47]

[45] Budgetpropositionen för 2012, prop. 2011/12:1 utg. omr. 22, s. 84.
[46] SOU 2015:39, *Myndighetsdatalag,* s. 175.
[47] Prop. 2017/18:1055, *Ny dataskyddslag*, s. 47.

De senaste decennierna och i synnerhet de senaste åren har den tekniska utvecklingen dessutom varit oerhört snabb. Redan 1993 konstaterade Datalagsutredningen[48] (Ju 1989:02) att sedan 1973 års datalags tillkomst hade informationsteknologin genomgått en explosionsartad utveckling och hade kommit att användas inom de flesta områden och fått en allt större betydelse för samhällsutvecklingen.[49] År 2016 beskrev sedan Digitaliseringskommissionen[50] (N 2012:04) det som att vi då befann oss mitt i utvecklingen från ett industrisamhälle till ett digitalt samhälle, och att digitaliseringen innebär att saker som vi redan gör kan göras på helt nya sätt och framför allt att helt nya saker är möjliga att göra.[51]

Under de knappt 10 år som gått sedan Digitaliseringskommissionens uttalande har utvecklingen fortsatt i allt högre takt. Digitaliseringen innebär bl.a. att nya former av information uppstår och flera nya typer av handlingar hanteras, vilket t.ex. i arkivrättsliga sammanhang har bedömts ställa andra slags krav på myndigheterna än tidigare.[52] Utvecklingen av nya digitala verktyg innebär också att myndigheter har helt andra möjligheter att behandla information och kommunicera digitalt än tidigare.

Dagens it-miljöer *inom myndigheterna* består t.ex. ofta av komplexa verksamhetsstöd där informationen behandlas i olika it-komponenter och tekniska databaser. It-lösningarna och dess komponenter har komplexa samband med varandra och kan vara verksamhetsöverskridande inom en myndighet. Inom it-miljöerna används vidare s.k. logisk separation vilket innebär att de olika verksamheterna har egna digitala sfärer. Tekniska åtgärder kan t.ex. medföra att åtkomst och sammanblandning av uppgifter mellan de olika sfärerna inte är möjlig och en verksamhet kan då bara få tillgång till uppgifter i sin egen sfär. Logisk separation fungerar därmed som ett slags digitalt inre skalskydd och kan på så sätt säkerställa regelefterlevnad. Verksamhetssystemen inom en sfär kan dessutom utformas till att bara ha tillgång till de uppgifter som behövs för respektive system och

[48] Datalagsutredningen hade i uppdrag att göra en såväl saklig som lagteknisk översyn av datalagen, se SOU 1993:10, *En ny datalag*, s. 21.
[49] SOU 1993:10, *En ny datalag*, s. 27.
[50] Digitaliseringskommissionen hade bl.a. i uppdrag att redovisa kunskapssammanställningar om digitaliseringens effekter på samhället och individen, se dir. 2015:123.
[51] SOU 2016:85, *Digitaliseringens effekter på individ och samhälle – fyra temarapporter*, s. 5.
[52] Jfr SOU 2019:58, *Härifrån till evigheten – en långsiktig arkivpolitik för förvaltning och kulturarv*, s. 268.

en handläggare får genom behörighetsstyrd åtkomst bara tillgång till de uppgifter som han eller hon behöver utifrån sina arbetsuppgifter.[53]

När det kommer till att kommunicera digitalt *utanför myndigheterna* kan utlämnande av uppgifter exempelvis ske genom säker e-post eller kräva identifiering av mottagaren via en av myndigheten godkänd e-legitimation. Användande av säker e-post kan exempelvis innebära olika former av kryptering, eller att informationen inte skickas direkt till mottagaren utan i stället lagras på en säker server och enbart läsas från den säkra servern, vilket innebär att utomstående inte kan få tillgång till informationen på väg till mottagaren. Användningen av digitala kommunikationssätt har dessutom ökat markant bland enskilda under de senaste decennierna, vilket framgår av Statistiska centralbyråns, SCB, statistik över befolkningens internetanvändning. Under 2024 hade t.ex. över 80 procent av befolkningen över 16 år använt internet flera gånger om dagen och cirka 70 procent fått myndighetspost via ett digitalt konto.[54] Att digital informationshantering ökar på bekostnad av den analoga motsvarigheten illustreras också av att antalet skickade brev sedan millennieskiftet har minskat med ungefär hälften, vilket fått till följd att vanlig post numera delas ut varannan dag.[55]

Elektroniskt utlämnande kan i dag ske på flera andra sätt än genom e-post, exempelvis genom att lämna ut information på ett usb-minne eller genom direkt överföring mellan olika it-system. Ett exempel på elektroniskt utlämnande är s.k. API (Application Program Interface). Ett API fungerar som en bro mellan exempelvis två informationshanteringssystem och är ett kontrollerat sätt att överföra information på. API utgör en funktion som en programmerare kan anropa för att ”beställa hem” information från någon annans databas eller program. Informationen kan skickas exempelvis via en app, databas eller Excelfil som tar emot och sparar en kopia av informationen.[56]

[53] SOU 2023:100, *Framtiden dataskydd – Vid Skatteverket, Tullverket och Kronofogden*, s. 595.
[54] SCB, *Befolkningens it-användning*, tillgänglig: https://www.scb.se/hitta-statistik/statistik-efter-amne/forskning-och-det-digitala-samhallet/det-digitala-samhallet/befolkningens-it-anvandning/#_Nyckeltal (hämtad 2025-01-23).
[55] Postnords pressmeddelande *Så fungerar varannandagsutdelning*, tillgängligt: https://www.postnord.se/om-oss/pressmeddelanden/framtidens-post/safungerar-varannandagsutdelning (hämtad 2025-01-23).
[56] Jfr Skatteverket, *Vad är ett API?* tillgänglig: https://skatteverket.se/omoss/digitalasamarbeten/omvaraapier/vadarettapi.4.96cca41179bad4b1aaa4b8.html (hämtad 25-01-26).

Den tekniska utvecklingen har också medfört möjligheter att helt automatiserat och momentant utföra olika kontroller av informationsmottagares behörighet och om ett utlämnande är förenligt med bl.a. sekretess- och dataskyddsbestämmelser, vilket tidigare krävt manuell hantering. I dessa sammanhang kan sekretess- och andra prövningar numera göras i förväg, i samband med att de tekniska systemen för informationsutbyte mellan myndigheter utformas. Detta har bl.a. medfört nya möjligheter till rutinmässigt utlämnande mellan myndighet och vissa förändringar av hur rent juridiska begrepp som rör formerna för digital kommunikation definieras och tolkas (se vidare avsnitt 5.6.2 nedan).

Digitaliseringens snabba utveckling gör också att strukturomvandlingen går fortare än vid tidigare teknikskiften och att konsekvenserna inte alltid är möjliga att förutse och beräkna. Utvecklingstakten inom det som kallas AI (artificiell intelligens) har t.ex. överträffat alla tidigare förväntningar, även inom forskarvärlden.[57] På ett generellt plan har det dessutom skett en exponentiell tillväxt av utbyte och insamling av data, som ibland sker globalt, och enskilda personer gör i allt högre utsträckning personlig information allmänt tillgänglig.[58] Många fysiska personer delar t.ex. frivilligt uppgifter om bl.a. förflyttningar, hälsa, konsumtionsmönster, intressen, relationer, ekonomi och politiska och religiösa åsikter på sociala medier och genom att acceptera s.k. cookies[59], eller kakor, på ett sätt som måste ha framstått i det närmaste otänkbart i början av 1970-talet.

I dag är det vidare inte statsmakterna som primärt förfogar över den personliga information som enskilda gör tillgänglig på internet, utan de aktörer som äger olika digitala plattformar och sociala medier. Dessa aktörer analyserar och vidarebehandlar ofta informationen i vinstsyfte, t.ex. genom att utveckla algoritmstyrda användarupplevelser med bl.a. skräddarsydd reklam. Samma information kan dock även användas för politiska syften och fysiska personer riskerar därigenom att exponeras för algoritmstyrda budskap och selektiv nyhetsförmedling som inte enbart syftar till att påverka deras konsumtionsmönster. Även budskap som, genom att utnyttja målgrup-

[57] Se t.ex. *1 000 experter i upprop: Pausa AI-utvecklingen – går för fort* tillgängligt: https://www.sverigesradio.se/artikel/ai-utvecklingen-gar-for-fort-experter-vill-pausa-utvecklingen (hämtad 2025-01-23).
[58] Jfr Europiska rådet och Europeiska unionens råd, *Dataskydd inom EU*, tillgänglig: https://www.consilium.europa.eu/sv/policies/data-protection/ (hämtad 25-01-22).
[59] Se t.ex. Europeiska kommissionens beskrivning av kakor: https://commission.europa.eu/cookies-policy_sv (hämtad 25-02-09).

pens förutfattade meningar, syftar till att påverka enskildas politiska attityder förkommer i dessa sammanhang.[60] Det kan t.ex. röra sig om att genom s.k. trollfabriker och falska nyhetssidor sprida desinformation och polariserande budskap på bl.a. sociala medier. Spridningen av både desinformation och felaktig information kan enligt bl.a. EU-kommissionen få en rad skadliga konsekvenser, såsom att hota det demokratiska statsskicket, polarisera debatter och äventyra medborgarnas hälsa, säkerhet och miljö.[61]

I detta avseende har den digitala utvecklingen alltså lett till att vissa av de farhågor som fanns i den svenska debatten vid 1970-talets början har besannats (jfr avsnitt 5.2.2). I en svensk kontext är det dock inte i första hand statsmakterna som försöker påverka enskilda på detta sätt. Det förefaller dock troligt att svenska myndigheter i allt högre utsträckning kommer att behöva förhålla sig till detta, t.ex. i syfte att motverka desinformationskampanjer om myndigheternas verksamhet eller andra påverkansoperationer. Verksamhet med att motverka bl.a. desinformation kan i sin tur medföra att myndigheterna får utökade behov av att behandla personuppgifter.

5.2.4 Ett generellt reformbehov?

Den kompletterande dataskyddsregleringen har haft som huvudsakligt syfte att i integritetsskyddande syfte ställa upp begränsningar av myndigheters rättsliga möjligheter att använda datorer i sin verksamhet. I efterhand har dock regleringen ofta framstått som omotiverat restriktiv, trots att den tekniska utvecklingen hela tiden medfört utökade möjligheter att behandla information digitalt. Att uppgifter från självdeklarationer skulle få behandlas med dator kunde t.ex. uppfattas som mycket kontroversiellt i skiftet mellan 1970-talet och 1980-talet.[62] I dag bör det i stället vara både helt självklart och helt okontroversiellt att Skatteverket använder digital teknik för att utföra sin verksamhet. Det är alltså inte längre det faktum att

[60] Jfr Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies, *Law and ICT*, s. 83 och 84, tillgänglig: https://www.europarl.europa.eu/RegData/etudes/STUD/2024/762738/IPOL_STU(2024)762738_EN.pdf (hämtad 25-01-23).
[61] Jfr Europeiska kommissionen, *Tackling online desinformation*, tillgänglig: https://digital-strategy.ec.europa.eu/sv/policies/online-disinformation (hämtad 25-04-02).
[62] Prop. 1979/80:146, *med förslag till skatteregisterlag*, s. 19.

datorer och digital teknik används av myndigheterna som *i sig* uppfattas problematiskt ut integritetssynpunkt.[63]

Bestämmelserna i sak har visserligen kontinuerligt förändrats under årens lopp. Fler och fler myndigheter har t.ex. tillåtits att utbyta information med hjälp av datorer och att kommunicera med enskilda via t.ex. e-post. Trots det nyss sagda har grunddragen i den kompletterande regleringsmodellen inte genomgått någon genomgripande förändring under de senaste 50 åren. Grunddragen i den kompletterande regleringen har alltså utformats i en tid då:

- Digital informationshantering utgjorde ett *undantag* från det normala.
- Myndigheters datoranvändning *i sig* ansågs utgöra en integritetsrisk.
- Datoranvändning behövde *regleras särskilt* för att vara tillåten.
- Datorer enbart fick användas *i vissa sammanhang*.

Även om dagens lagstiftning i sak skiljer sig från äldre reglering så förekommer alltså bestämmelser om *samma slags förhållanden* som var föremål för reglering under 1973 års datalag, när det var den faktiska användningen av datorer som skulle begränsas. Dagens kompletterande dataskyddsreglering innehåller t.ex. ofta detaljerade ändamålsbestämmelser och andra bestämmelser som anger hur uppgifter får behandlas digitalt i viss verksamhet. Det kan t.ex. röra sig om databasreglering som begränsar vilka uppgifter som får göras gemensamt tillgängliga i verksamheten, begränsningar av att lämna ut uppgifter elektroniskt, begränsningar av möjligheten att söka efter personuppgifter, eller generella begränsningar av vilka uppgifter som får behandlas digitalt i ett visst sammanhang.

Sådana bestämmelser, som ursprungligen avsett en avgränsad form av informationshantering, är i dag tillämpliga på all informationshantering inom myndigheterna, eftersom den numera är helt digital. I en helt digitaliserad verksamhet innebär alltså begränsningar av hur och vilka uppgifter en myndighet får behandla med dator i praktiken en begränsning av den materiella verksamhetsregleringen i sig.

[63] Jfr IMY, *Integritet och ny teknik 2020–2024 – Redovisning av Integritetsskyddsmyndighetens uppdrag att följa, analysera och beskriva utvecklingen*, dnr IMY-2024-2570, s. 6.

Den kompletterande dataskyddsregleringen kan därför i många fall uppfattas utgöra ett hinder mot att myndigheterna ska kunna utföra sin verksamhet på ett korrekt, rättssäkert och effektivt sätt, utan några uppenbara integritetsvinster för enskilda. Den kan också vara svår att tillämpa samtidigt som den materiella verksamhetsregleringen, t.ex. om uppgifter som är nödvändiga för en viss verksamhet inte får hanteras digitalt. Ett regelverk med bestämmelser som inte följs eller är svåra att följa skadar respekten för regelverket, både hos dem som ska tillämpa bestämmelserna och de som ska skyddas av dem.[64] Att utformningen av de sektorsspecifika författningarna skiljer sig åt, bl.a. i fråga om detaljeringsgrad och begreppsanvändning, kan dessutom antas utgöra ett hinder för bl.a. samverkan mellan olika myndigheter och en enhetlig praxisbildning.

Grunddragen i den kompletterande regleringen har av naturliga skäl inte heller utformats med hänsyn tagen till dataskyddsförordningens syfte, funktion och innehåll. Att dataskyddsförordningen sedan maj 2018 är den primära rättskällan i dataskyddsfrågor innebär att det redan finns en omfattande reglering av dataskyddsrättsliga frågor som i princip alla som behandlar personuppgifter, såväl myndigheter som privata ekonomiska aktörer och organisationer, måste iaktta. Mot den bakgrunden bör det inte längre finns samma generella behov som tidigare av att i sektorsspecifik dataskyddsreglering begränsa eller tydliggöra vilken personuppgiftsbehandling som får förekomma inom en myndighet, i syfte att upprätthålla ett adekvat integritetsskydd.

Regeringen har på senare år vidtagit vissa åtgärder för att reformera den kompletterande dataskyddsregleringen genom att tillsätta utredningar som haft i uppdrag att analysera regleringen på sektors- eller myndighetsnivå och att förslå nödvändiga förändringar. Sådana lagstiftningsinitiativ tenderar att resultera i förslag om att den befintliga regleringen ska upphävas och ersättas av reglering som i allt väsentligt är mer tillåtande, mer flexibel och mindre begränsande än den tidigare. Det finns i dag förslag på sådan ny reglering av personuppgiftsbehandling inom bl.a. hälsodataområdet, viss verksamhet vid Lantmäteriet, flera olika verksamheter vid Skatteverket, viss verksamhet vid Tullverket, vid Kronofogdemyndigheten och vid

[64] Jfr SOU 2017:52, *Så stärker vi den personliga integriteten*, s. 56.

CSN.[65] För nuvarande utreds även förändringar av regleringen av personuppgiftsbehandling vid bl.a. Arbetsförmedlingen och Säkerhetspolisen.[66] Regeringen har dock inte vidtagit sådana lagstiftningsinitiativ vad gäller all kompletterande dataskyddsreglering. Regeringen har inte heller tagit ett samlat grepp om rättsområdet, vilket borde innebära att det finns ett generellt reformbehov som ännu inte tillgodosetts. En sådan översyn ryms dock inte inom den här utredningens uppdrag.

5.3 Omfattningen av vår översyn och vår kartläggning av behoven

5.3.1 Vilka bestämmelser omfattas av vår översyn?

I kompletterande dataskyddsreglering förekommer inte enbart bestämmelser som rör den personuppgiftsansvariga myndighetens personuppgiftsbehandling inom det aktuella tillämpningsområdet. Även bestämmelser som uttryckligen reglerar vidarebehandling för andra ändamål än insamlingsändamålen, t.ex. genom utlämnande av uppgifter till myndigheter och enskilda förekommer. Formen för utlämnandet, dvs. om ett utlämnande får ske elektroniskt, och i sådana fall vilken typ av teknisk lösning som får användas, regleras också särskilt i den kompletterande regleringen.

Till skillnad från bestämmelser som begränsar myndigheters utrymme att för egen del behandla personuppgifter har bestämmelser om vidarebehandling av uppgifter en direkt betydelse för att våra förslag om förbättrade möjligheter till informationsutbyte ska tjäna sitt syfte och kunna tillämpas på ett ändamålsenligt sätt. Om vidarebehandling genom utlämnande till andra myndigheter till synes är förbjudet eller tillåtligheten till synes begränsad i den kompletterande regleringen kan detta uppfattas som att bestämmelserna i offentlighets- och sekretesslagen inte kan tillämpas på ett ändamålsenligt sätt. Mot bakgrund av att i princip all informationshantering i dag sker elektroniskt kan även bestämmelser som begränsar möjligheterna att

[65] Se SOU 2023:100, *Framtiden dataskydd – Vid Skatteverket, Tullverket och Kronofogden*, SOU 2024:7, *Ett säkrare och mer tillgängligt fastighetsregister*, SOU 2024:57, *Ett nytt regelverk för hälsodataregister*, och SOU 2024:95, *Modernt dataskydd vid CSN*.
[66] Se dir. 2023:65, *Förbättrat informationsutbyte och en mer ändamålsenlig lagreglering för den arbetsmarknadspolitiska verksamheten* och dir. 2023:64, *Säkerhetspolisens informationshantering*.

utbyta uppgifter elektroniskt utgöra ett hinder mot de föreslagna bestämmelsernas tillämpning.

Vår översyn omfattar alltså bestämmelser i kompletterande dataskyddsreglering som kan utgöra hinder mot elektroniskt informationsutbyte mellan myndigheter, både i sak och form.

5.3.2 Vilka författningar omfattas av vår översyn?

En första grovsortering

Inom den kompletterande dataskyddsregleringen finns en stor variation i hur bestämmelser har utformats i olika sammanhang. En gemensam faktor är dock att bestämmelserna dels reglerar personuppgiftsbehandling, dels kompletterar mer allmänna bestämmelser. I syfte att söka fram de författningar som bör ingå i översynen har vi därför sökt i olika rättsdatabaser bl.a. efter följande begrepp.

- EU 2016/679
- *datalag
- Behandling av personuppgifter.

Denna sökning har resulterat i knappt 320 författningar. Vi har rensat bort författningar som uppenbart inte innehåller bestämmelser som utgör ett hinder mot informationsutbyte mellan myndigheter, t.ex. olika myndigheters instruktioner. Ett annat exempel på författningar som rensats bort är sådana som enbart hänvisar till kompletterande dataskyddsreglering, t.ex. de många författningar som innehåller en hänvisning till uppgifter som registrerats i Skatteverkets folkbokföringsdatabas enligt lagen (2001:182) om behandling av personuppgifter i Skatteverkets folkbokföringsverksamhet. Vi har även rensat bort kompletterande dataskyddsreglering som enbart är tillämplig inom den privata sektorn där bestämmelserna i offentlighets- och sekretesslagen inte tillämpas.

De författningar som kvarstått efter dessa avgränsningar utgör sådan kompletterande dataskyddsreglering som omfattats av vår inledande översyn. Det är fråga om faktiska registerförfattningar och informationshanteringsförfattningar och bestämmelser av dataskyddskaraktär i lagstiftning som i huvudsak reglerar andra frågor.

Alla författningar omfattar dock inte bestämmelser som hindrar elektroniskt informationsutbyte mellan myndigheter, eller så omhändertas de i annan ordning.

Omhändertas i annat sammanhang

Som vi nämnt tidigare pågår ett antal lagstiftningsinitiativ som syftar till att se över kompletterande reglering av personuppgiftsbehandling inom olika delar av den offentliga sektorn. Vi har både granskat de liggande förslagen och haft kontakt med de utredningar som ännu pågår. Utifrån detta har vi bedömt att det saknas skäl för oss att vidta något ytterligare åtgärd i dessa fall. Författningar som särskilt omhändertas i andra sammanhang omfattas därför inte av vår översyn.

Det gäller följande:

- Författningar om personuppgiftsbehandling och registerföring som i SOU 2023:100, *Framtidens dataskydd – För Skatteverket, Tullverket och Kronofogden*, föreslås upphävas och ersättas av nya författningar.
- Författningar som i SOU 2024:7, *Ett säkrare och mer tillgängligt fastighetsregister*, föreslås upphävas och ersättas av nya författningar.
- Författningar om olika hälsodataregister som i SOU 2024:57, *Ett nytt regelverk för hälsodataregister*, föreslås upphävas och ersättas av nya författningar.
- Författningar som i SOU 2024:95, *Modernt dataskydd vid CSN*, föreslås upphävas och ersättas av nya författningar.
- Författningar som ses över av Utredningen om ett förbättrat informationsutbyte och en mer ändamålsenlig lagreglering för den arbetsmarknadspolitiska verksamheten (A 2023:01).
- Författningar som ses över av Utredningen om Säkerhetspolisens informationshantering (Ju 2023:02).

Inga ändamålsbestämmelser

Kompletterande dataskyddsreglering utgörs ibland av ett fåtal bestämmelser som i sak t.ex. enbart föreskriver undantag från vad som annars hade gällt enligt dataskyddsförordningen. Det kan t.ex. avse bestämmelser om att rätten att invända mot behandlingen inte ska gälla, avvikande bestämmelser om rättelse av personuppgifter eller om hur lång tid vissa uppgiftskategorier får behandlas i en verksamhet. Sådan kompletterande reglering är förhållandevis vanlig och vi har identifierat ett drygt 30-tal författningar av denna karaktär, t.ex. lagen (2001:99) om den officiella statistiken och lagen (2019:504) om ansvar för god forskningssed och prövning av oredlighet i forskning.

I andra fall kan det röra sig om omfattande lagar med tillhörande förordningar som reglerar användandet av ett visst digitalt system för informationshantering som flera aktörer är anslutna till, utan att ändamålen för behandlingen regleras särskilt. Sådan reglering finns bl.a. i lagen (2021:1187) med kompletterande bestämmelser till EU:s förordningar om Schengens informationssystem och lagen (2022:913) om sammanhållen vård- och omsorgsdokumentation.

När det saknas ändamålsbestämmelser gäller antingen annan sektorsspecifik reglering eller den allmänna dataskyddsregleringen eller brottsdatalagen vad gäller frågan om tillåtna ändamål för behandling. Författningar som inte innehåller ändamålsbestämmelser omfattas därför inte av vår översyn, om de inte samtidigt innehåller bestämmelser om elektroniskt utlämnande.

Offentliga register

Faktiska registerförfattningar, dvs. sådana författningar som reglerar att ett visst register *ska* föras, syftar ofta uttryckligen till att ge offentlighet åt uppgifterna som får finnas i registret. Verksamheten med att föra ett sådant register karaktäriseras alltså av det stora inslaget av informationsförsörjning till andra aktörer.

I de ändamålsbestämmelser som förekommer i sådana faktiska registerförfattningar anges i regel att syftet med registret är att ge offentlighet till vissa uppgifter, t.ex. som i 1 kap. 4 § lagen (2008:990) om företagshypotek. I den bestämmelsen anges följande.

> För inskrivning enligt denna lag ska det föras ett register med hjälp av automatiserad behandling, benämnt företagsinteckningsregistret. *Detta ska ge offentlighet åt den information som ingår i registret* [vår kursivering].

Lagens bestämmelser kompletteras i 3 § förordningen (2003:552) om företagshypotek med ändamålsbestämmelser enligt följande.

> I fråga om personuppgifter skall registret ha till ändamål att tillhandahålla uppgifter för
> 1. verksamhet som staten ansvarar för enligt lag eller annan författning och
> a) som avser sådan egendom för vilken företagsinteckning eller annan införing sker i företagsinteckningsregistret, eller
> b) som för att kunna utföras förutsätter tillgång till den information som finns i registret,
> 2. förvärv och avyttring av egendom i vilken inteckning har skett och
> 3. kreditgivning, försäkringsgivning eller annan allmän eller enskild verksamhet där den information som ingår i företagsinteckningsregistret utgör underlag för prövningar eller beslut.

Liknande bestämmelser förekommer i flera faktiska registerförfattningar. Verksamhet med sådan registerföring bedrivs i allt väsentligt i syfte att tillhandahålla viss information till myndigheter och enskilda. I regel finns det dock ingen upplysningsbestämmelse om att bestämmelserna i registret även i andra fall kan komma att lämnas ut i överensstämmelse med lag eller förordning, som är vanligt förekommande i annan reglering (jfr avsnitt 3.2.2). Att uppgifterna i registret inte bara får utan till och med *ska* göras tillgängliga för andra aktörer är dock tydligt redan genom befintlig reglering. Dataskyddsbestämmelser som avser offentligt register bör därför inte kunna utgöra något hinder mot tillämpningen av offentlighets- och sekretesslagen. Faktiska registerförfattningar som reglerar offentliga register omfattas därför inte av vår översyn.

Vid ”avvikande” sekretessreglering m.m.

Utbytet av uppgifter mellan myndigheter regleras i stor utsträckning av bestämmelserna i 10 kap. OSL. Det är t.ex. där det närmast helt generella sekretessgenombrottet vid misstanke om begångna brott

regleras (23 och 24 §§), liksom generalklausulen[67] (27 §) och att sekretess inte hindrar att en uppgift lämnas till en annan myndighet, om uppgiftsskyldighet följer av lag eller förordning (28 §). Även den generella sekretessbrytande bestämmelsen som vi föreslagit i SOU 2024:63 kan komma att införas som en ny 15 a § i det kapitlet.

Det förekommer att det helt eller delvis görs undantag från bestämmelserna i 10 kap. OSL i anslutning till en materiell sekretessbestämmelse. Vad som i praktiken kan sägas motsvara undantag från den generella tillämpligheten av bestämmelserna i 10 kap. OSL kan även aktualiseras av att det finns s.k. användningsbegränsningar, som kan följa av EU-rätten, som svenska myndigheter är skyldiga att iaktta. Hänvisningar till sådana finns ofta i 9 kap. OSL (jfr avsnitten 5.4.1, 5.4.4 och 5.4.7 nedan).

När det i offentlighets- och sekretesslagen gjorts sådana undantag från vad som annars gäller enligt den lagen innebär det också att den generella sekretessbrytande bestämmelse som vi föreslagit antingen inte kommer att vara tillämplig i dessa sammanhang, eller att den bara får tillämpas i vissa avgränsade situationer. Det innebär att lagstiftaren redan tagit ställning till att generella bestämmelser om informationsutbyte mellan myndigheter inte ska gälla på dessa områden, och att detta redan framgår av offentlighets- och sekretesslagen (jfr avsnitt 5.4.4). Mot den bakgrunden bör kompletterande dataskyddsreglering inom dessa områden inte omfattas av vår faktiska översyn.

Inga hinder i befintlig reglering

De författningar som träffas av någon av ”uteslutningsgrunderna” ovan har avförts från vår översyn. I listan över författningar som kvarstår finns bl.a. ett 20-tal författningar som innehåller bestämmelser med innebörden att personuppgifter får behandlas för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning (jfr avsnitt 3.2.2) och som saknar faktiska begränsningar av annat elektroniskt utlämnande än direktåtkomst. Eftersom dessa författningar inte innehåller reglering som kan uppfattas stå i konflikt med offentlighets- och sekretesslagens bestämmelser, och inte heller bestämmelser som utgör faktiska hinder mot att

[67] Enligt generalklausulen i 10 kap. 27 § OSL får en sekretessbelagd uppgift, med vissa undantag, lämnas till en myndighet om det är uppenbart att intresset av att uppgiften lämnas har företräde framför det intresse som sekretessen ska skydda.

utbyta information digitalt, har vi uteslutit dem från vår översyn. Här ingår bl.a. 114 kap. socialförsäkringsbalken, domstolsdatalagen (2015:728) och utlänningsdatalagen (2016:27).

Författningar som i sak inte innehåller några hinder mot informationsutbyte men däremot en föråldrad terminologi eller markant avvikande begreppsanvändning har vi dock låtit omfattas av vår översyn.

Vår faktiska översyn

De författningar som återstår är författningar där det finns skäl att överväga en förändring av regleringen och som därmed omfattas av vår faktiska översyn. I översynen ryms därmed ett 50-tal författningar som tillämpas inom vitt skilda verksamheter och som är utformade på olika sätt. I vissa fall rör förändringsbehoven enbart terminologi och struktur, i andra fall rör behoven normkonflikter och oklarheter, eller omotiverade hinder mot att lämna ut uppgifter elektroniskt. Det som sägs i avsnitten 5.4 och 5.6 är alltså tillämpligt på samtliga författningar som omfattas, även om allt som sägs inte är aktuellt för samtliga.

5.3.3 Behoven i sak utifrån vår kartläggning

Allmänt om kartläggningen

Den första delen av vårt uppdrag omfattade bl.a. att kartlägga behovet av förbättrade möjligheter till informationsutbyte mellan myndigheter. I vårt delbetänkande har vi redogjort för hur kartläggningen genomfördes och resultatet av den, se kapitel 4 i SOU 2024:63. Till delbetänkandet är även resultatet av den digitala enkät vi genomfört bifogat, såväl sammantaget som på gruppnivå, se bilaga 2–5 till SOU 2024:63.

I enkäten, som gick ut till statliga myndigheter, kommuner, regioner och aktörer som i vissa fall likställs med myndigheter, undersöktes primärt myndigheters behov kopplade till sekretesslagstiftningen, och i vilken utsträckning sekretesslagstiftningen utgjorde ett hinder mot efterfrågat informationsutbyte. Vi frågade även om det finns andra hinder än sekretessregleringen mot sådant informationsutbyte som kan ha betydelse för att myndigheter ska kunna

fatta riktiga beslut eller på annat sätt utföra sin verksamhet, där bl.a. den kompletterande dataskyddsregleringen berördes.

Samtliga frågor i enkäten avsåg behovet av att lämna ut eller få del av sådan information om enskilda som kan ha betydelse för att andra myndigheter eller den egna myndigheten ska kunna fatta riktiga beslut eller på annat sätt utföra sin verksamhet.

Totalt 952 respondenter svarade på enkäten. Enkätens logik var uppbyggd på så sätt att de inledande frågorna i båda avsnitten (lämna ut/få del av) hade funktionen av utslagsfrågor. De 142 respondenter som inledningsvis uppgav att de *inte* förfogade över uppgifter om enskilda som kan ha betydelse för andra myndigheter behövde alltså inte svara på ytterligare frågor om utlämnande av uppgifter. De sammanlagt 352 respondenter som därefter uppgav att de antingen inte efterfrågade utökade möjligheter att lämna relevant information till andra myndigheter, eller inte hade någon ståndpunkt att redovisa i denna fråga, behövde sedan inte heller svara på ytterligare frågor om utlämnande, osv. Motsvarande systematik tillämpades i den del som avsåg att få del av information som andra myndigheter förfogade över.

Att lämna ut uppgifter

Knappt hälften av respondenterna (48,1 procent, eller 458 av totalt 952 respondenter) besvarade frågan om det finns andra hinder än sekretessregleringen mot att lämna ut relevanta uppgifter till andra myndigheter. 242 av dessa, eller 25,4 procent av samtliga respondenter, uppgav att det finns andra hinder än sekretessregleringen mot att lämna ut relevanta uppgifter till andra myndigheter.

Av dessa uppgav 172 respondenter att ett hinder var att den sammantagna regleringen av myndigheters informationsutbyte (sekretess- och dataskyddsfrågor) uppfattas som komplex och svårtillämpad. Bland de som uppgett den sammantagna regleringens komplexitet som ett hinder mot att lämna ut uppgifter finns respondenter från några av Sveriges största statliga myndigheter, bl.a. Arbetsförmedlingen, Försäkringskassan, Kriminalvården, Migrationsverket, Polismyndigheten, Regeringskansliet, Skatteverket, Transportstyrelsen och Tullverket. Även 108 respondenter från kommuner uppgav att den sammantagna regleringens komplexitet utgjorde ett hinder mot

utlämnande till andra myndigheter, liksom 14 respondenter från regionerna.

Totalt 56 respondenter uppgav att organisationen har en kompletterande dataskyddsreglering med ändamålsbegränsningar som utgör ett hinder mot att lämna ut information om enskilda till andra myndigheter. Bland dessa finns 20 statliga myndigheter, bl.a. Arbetsförmedlingen, CSN, Inspektionen för vård och omsorg (IVO), Kustbevakningen, Lantmäteriet, Polismyndigheten, Skatteverket och Transportstyrelsen. Totalt 32 respondenter i kommunerna uppgav att ändamålsbegränsningar i kompletterande dataskyddsreglering utgör ett hinder mot att lämna ut relevant information till andra myndigheter, liksom 5 respondenter från lika många regioner.

Totalt 50 respondenter uppgav att ett hinder mot att lämna ut relevanta uppgifter till andra myndigheter är att organisationen har en kompletterande dataskyddsreglering med begränsningar av möjligheten att lämna ut uppgifter elektroniskt. Bland dessa finns 18 statliga myndigheter bl.a. Arbetsförmedlingen, CSN, Kriminalvården, Kronofogdemyndigheten, Polismyndigheten, Skatteverket och Transportstyrelsen. Även 27 respondenter i kommunerna har uppgett detta hinder, liksom 5 respondenter i regionerna.

Övriga undersökta hinder som eventuellt kan kopplas till den kompletterande dataskyddsregleringen är bl.a. att organisationen inte har någon rättslig grund i dataskyddsrättslig mening för den personuppgiftsbehandling som utlämnande skulle innebära (72 respondenter angav detta som ett hinder) och att finalitetsprincipen (dvs. att personuppgifter inte får behandlas för ett ändamål som är oförenligt med insamlingsändamålet) hindrar organisationen från att lämna ut viss information om enskilda till en eller flera andra myndigheter (68 respondenter angav detta som ett hinder).

Att få del av uppgifter

Totalt 532 respondenter besvarade frågan om det finns andra hinder än sekretessregleringen mot att få del av relevant information om enskilda som andra myndigheter förfogar över. Ungefär hälften av dessa (256 respondenter) uppgav att det fanns andra hinder än sekretessregleringen mot att få del av information från andra myndigheter.

Av dessa uppgav 157 respondenter att ett hinder var att den sammantagna regleringen av myndigheters informationsutbyte (sekretess- och dataskyddsfrågor) uppfattas som komplex och svårtillämpad. Bland de respondenter som uppgett den sammantagna regleringens komplexitet som ett hinder mot att få del av uppgifter finns 42 statliga myndigheter, bl.a. Arbetsförmedlingen, CSN, Försäkringskassan, Kriminalvården, Migrationsverket, Pensionsmyndigheten, Polismyndigheten, Skatteverket och Tullverket. Bland de statliga myndigheterna finns även ambassader, Bolagsverket, Statens institutionsstyrelse (SiS), Diskrimineringsombudsmannen och flera tingsrätter. Även 109 respondenter från kommuner uppgav att den sammantagna regleringens komplexitet utgjorde ett hinder mot att få del av information från andra myndigheter, liksom 9 respondenter från regionerna.

Totalt 71 respondenter uppgav att ett hinder mot att få del av relevant information är att den myndighet som förfogar över uppgifterna inte har möjlighet att lämna ut uppgifterna elektroniskt. Bland dessa finns 31 statliga myndigheter, bl.a. Arbetsförmedlingen, Domstolsverket, Försäkringskassan, Jordbruksverket, Kriminalvården, Migrationsverket, Polismyndigheten, Skatteverket, Tullverket och Utbetalningsmyndigheten. Även en handfull ambassader uppgav detta hinder mot att få del av relevant information. Totalt 38 respondenter i kommunerna uppgav som ett hinder att den utlämnande myndigheten inte har möjlighet att lämna ut uppgifter elektroniskt, liksom 4 respondenter från lika många regioner.

Totalt 55 respondenter uppgav att ett hinder mot att få del av relevant information från andra myndigheter är att organisationen har en kompletterande dataskyddsreglering med begränsningar av vilka uppgifter som får behandlas i syfte att utföra verksamheten. Bland dessa finns 16 statliga myndigheter bl.a. Arbetsförmedlingen, CSN, Kriminalvården, Kronofogdemyndigheten, Polismyndigheten, Skatteverket, Säkerhetspolisen (SÄPO) och Transportstyrelsen. Även 35 respondenter i kommunerna har uppgett detta hinder, liksom 4 respondenter i regionerna.

Övriga undersökta hinder mot att få del av information som eventuellt kan kopplas till den kompletterande dataskyddsregleringen är att organisationen inte har någon rättslig grund i dataskyddsrättslig mening för den personuppgiftsbehandling som inhämtandet eller mottagandet skulle innebära (102 respondenter).

Sammanfattning

Det huvudsakliga syftet med enkäten var inte att undersöka myndigheternas uppfattningar om och behov av förändringar av den kompletterande dataskyddsregleringen. Enkätens resultat i de ovan relaterade delarna bekräftar dock det som sägs i våra direktiv om att den kompletterande dataskyddsregleringen kan innehålla hinder mot att lämna ut eller få del av uppgifter.

Resultatet av vår enkät visar alltså att det finns vissa behov av förändringar av den kompletterande dataskyddsregleringen i syfte att åstadkomma förbättrade möjligheter till informationsutbyte mellan myndigheter. Det rör bl.a. regleringens komplexitet, särskilt i förhållande till sekretessregleringen, och olika dataskyddsrättsliga hinder mot att behandla personuppgifter och att utbyta information med andra myndigheter. Resultatet bekräftar även att det finns ändamålsbegränsningar i den kompletterande dataskyddsregleringen som uppfattas utgöra ett hinder mot att utbyta uppgifter med andra myndigheter med stöd av bestämmelserna i offentlighets- och sekretesslagen.

5.4 Ändamålsbestämmelser – ett hinder mot utlämnande?

5.4.1 Ändamålsbestämmelser

Allmänt

Ändamålsbestämmelser i kompletterande dataskyddsreglering

Det måste alltid finnas minst ett ändamål med all personuppgiftsbehandling. Detta uttrycks i artikel 5.1 b i dataskyddsförordningen som att personuppgifter bara får samlas in för särskilda, uttryckligt angivna och berättigade ändamål. Ändamålet med behandlingen är sedan avgörande för tillämpningen av flera av de grundläggande principer för personuppgiftsbehandling som uttrycks i artikel 5 i dataskyddsförordningen. Uppgifter ska t.ex. inte vara för omfattande i förhållande till *ändamålet* med behandlingen (principen om uppgiftsminimering, artikel 5.1 c).

Av artikel 5.1 b i dataskyddsförordningen framgår även att personuppgifter inte får vidarebehandlas på ett sätt som är oförenligt med de ändamål för vilka de samlats in (finalitetsprincipen). Det innebär att vidarebehandling för ändamål som är *förenliga* med insamlingsändamålet som utgångspunkt är tillåten. Vidarebehandling för *oförenliga* ändamål är dock enbart tillåtet om det finns en bestämmelse i nationell rätt eller unionsrätten som tillåter behandlingen (jfr avsnitten 3.2.2 och 4.8.4).

Utlämnande till en annan myndighet utgör i regel vidarebehandling för oförenliga ändamål. Då sekretess enligt offentlighets- och sekretesslagen även gäller mellan myndigheter regleras uppgiftslämnande mellan svenska myndigheter huvudsakligen av bestämmelserna i den lagen. I sak regleras dock informationsutbyte oftast genom särskilda bestämmelser om uppgifts- anmälnings- eller underrättelseskyldigheter, som enligt 10 kap. 28 § första stycket OSL också bryter eventuell sekretess. Bestämmelser om skyldighet att lämna uppgifter kan också finnas i EU-rätten. När myndigheter utbyter personuppgifter ska det dataskyddsrättliga regelverket alltså tillämpas parallellt med bestämmelserna i offentlighets- och sekretesslagen.

Dataskyddsförordningen ger ett visst utrymme för att i den nationella rätten införa särskilda bestämmelser för att anpassa tillämpningen av bestämmelserna i förordningen, bl.a. avseende de enheter till vilka personuppgifterna får lämnas ut och för vilka ändamål samt ändamålsbegränsningar. Detta framgår av artikel 6.3 i dataskyddsförordningen. Kompletterande dataskyddsreglering innehåller ofta sådana bestämmelser som reglerar till vilka aktörer personuppgifter får lämnas ut och för vilka ändamål, samt ändamålsbegränsningar som på ett mer generellt plan avgränsar för vilka ändamål personuppgifter får behandlas. Sådana bestämmelser kallas fortsättningsvis ändamålsbestämmelser, men kan ha en annan benämning i författning.

Ändamålsbestämmelser i kompletterande dataskyddsreglering syftade ursprungligen till att reglera för vilka ändamål en myndighet fick använda dator i en viss verksamhet (jfr avsnitt 5.2.2). Regeringen har i senare lagstiftningsarbete uttalat att ändamålsbestämmelser kan sägas anpassa tillämpningen av dataskyddsförordningen och säkerställa en laglig och rättvis behandling av personuppgifter. Bestämmelser om tillåtna ändamål har också karaktäriserats av regeringen som en yttersta ram inom vilken personuppgiftsbehandling är tillåten, och både som del i, och ett fastställande av, den rättsliga

grunden för behandlingen.[68] Vad ändamålsbestämmelsernas nuvarande funktion är, i förhållande till dataskyddsförordningen och dataskyddslagen, är alltså inte helt tydligt.

I lagstiftningsärendet gällande dataskyddslagen tog regeringen ställning till den svenska kompletterande dataskyddsregleringens förenlighet med dataskyddsförordningens bestämmelser. Regeringen uttalade då i fråga om ändamålsbestämmelser att dataskyddsförordningen inte ställer något krav på att ändamål ska vara fastställda i författning men att det heller inte finns något som hindrar att detta görs, under förutsättning att bestämmelserna uppfyller ett mål av allmänt intresse och är proportionella mot det legitima mål som eftersträvas.[69]

Något om användningsbegränsningar

Internationella avtal och sektorsspecifika rättsakter innehåller ibland artiklar om att en myndighet bara får använda uppgifter som erhålls enligt avtalet respektive rättsakten för vissa angivna ändamål eller i viss verksamhet.[70] Som vi redan nämnt i avsnitt 5.3.2 förekommer sådana s.k. användningsbegränsningar bl.a. i EU-rätten, som i vissa fall har införts i svensk rätt t.ex. vid genomförandet av EU-direktiv. Användningsbegränsningar kan avse personuppgifter, men behöver inte göra det. Sådana bestämmelser utgör inte ändamålsbestämmelser i den mening som avses här, utan har i regel en generell tillämplighet och måste iakttas av alla svenska myndigheter.[71] De förbud mot att utnyttja uppgifter som följer av sådana begränsningar får alltså till följd att inga myndigheter kan utnyttja uppgifterna i verksamhet som faller utanför det tillåtna användningsområdet, oavsett om det föreligger sekretesshinder mot att ta del av dem eller inte. Frågan om att i strid med sådana användningsbegränsningar lämna ut uppgifter till en annan myndighet med stöd av offentlighets- och sekre-

[68] Jfr prop. 2022/23:34, *Utbetalningsmyndigheten*, s. 124, prop. 2018/19:65, *Personuppgiftsbehandling i viss verksamhet som rör allmän ordning och säkerhet – anpassningar till EU:s dataskyddsreform*, s. 43 och prop. 2017/18:171, *Dataskydd inom Socialdepartementets verksamhetsområde – en anpassning till EU:s dataskyddsförordning*, s. 83.
[69] Prop. 2017/18:105, *Ny dataskyddslag*, s. 22.
[70] SOU 2015:39, *Myndighetsdatalag*, s. 153.
[71] Jfr prop. 2021/22:127, *Bättre tillgång till finansiell information i brottsbekämpningen*, s. 44.

tesslagen bör därför aldrig bli aktuell.[72] Däremot bör sådana användningsbegränsningar inte hindra ett uppgiftsutlämnande som är tillåtet enligt offentlighets- och sekretesslagen när det utgör ett led i ett tillåtet användningsområde.

Primära och sekundära ändamål

Vad gäller s.k. informationshanteringsförfattningar, dvs. kompletterande dataskyddsreglering som typiskt sett är tillämplig inom hela eller delar av en myndighets kärnverksamhet, eller inom en specifik sektor där flera myndigheter utför samma slags verksamhet, görs det normalt en skillnad mellan s.k. primära och sekundära ändamålsbestämmelser Denna skillnad finns även i annan kompletterande dataskyddsreglering, men är särskilt framträdande i informationshanteringsförfattningar.

Primära ändamålsbestämmelser reglerar för vilka ändamål den eller de personuppgiftsansvariga myndigheterna får samla in och i övrigt behandla personuppgifter i den verksamhet där den kompletterande regleringen ska tillämpas. Primära ändamål kan vara mer eller mindre detaljerade men syftar ofta till att omfatta samtliga berättigade ändamål som kan komma att aktualiseras inom den aktuella verksamheten. Det innebär att primära ändamål i regel speglar regleringen av myndighetens verksamhet inom tillämpningsområdet.[73]

Uppgiftslämnande till andra myndigheter kan utgöra en integrerad del av ett primärt ändamål eller regleras särskilt som ett av flera primära ändamål, beroende på vilken verksamhet som är aktuell. Uppgiftslämnande som inte omfattas av ett primärt ändamål är i många fall inte särskilt reglerat i kompletterande dataskyddsreglering. När det förekommer regleras dock sådant uppgiftslämnande i bestäm-

[72] Se Lenberg m.fl., *Offentlighets- och sekretesslagen* (2009:400), 11 dec. 2024, JUNO, kommentaren till 9 kap. 2 § och prop. 1990/91:131, *om vissa frågor om internationellt samarbete i brottmål m.m.* s. 24 och 25, prop. 2011/12:15, *Genomförande av det nya EU-direktivet om bistånd med indrivning*, s. 54, prop. 2011/12:163, *Utbyte av uppgifter ur kriminalregister mellan EU:s medlemsstater*, s. 50 och 51, prop. 2012/13:4, *Genomförande av det nya EU-direktivet om administrativt samarbete i fråga om beskattning*, s. 61, 90 och 91, prop. 2014/15:41, *Genomförande av avtal mellan Sveriges regering och Amerikas förenta staters regering för att förbättra internationell efterlevnad av skatteregler och för att genomföra FATCA*, s. 196 och 197, prop. 2015/16:29, *En global standard för automatiskt utbyte av upplysningar om finansiella konton*, s. 210 och prop. 2016/17:47, *Dokumentation vid internprissättning och land-för-land-rapportering på skatteområdet*, s. 84.

[73] Jfr t.ex. SOU 2015:39, *Myndighetsdatalag*, s. 269 och 270 samt prop. 2022/23:34, *Utbetalningsmyndigheten*, s. 124.

melser om *sekundära* ändamål. Det rör sig alltså om behandling för andra behov (ändamål) än de som ligger till grund för insamlingen. Sekundära ändamål kan även röra den personuppgiftsansvariga myndighetens behandling i sammanhang utanför tillämpningsområdet för den aktuella författningen.

Bestämmelser om sekundära ändamål är inte sällan utformade på följande sätt.

- Personuppgifter som behandlas enligt X § (där de primära ändamålen anges) får även behandlas för …

På så sätt tydliggörs att det inte är fråga om att uppgifter ska kunna samlas in enbart för de sekundära ändamålen. Det rör sig alltså om reglering som avser en vidarebehandling av uppgifter som den personuppgiftsansvariga myndigheten redan har samlat in och behandlar i syfte att utföra den verksamhet som träffas av den kompletterande dataskyddsregleringen, men för andra syften än att utföra just den verksamheten.

När det däremot är fråga om faktiska registerförfattningar anges normalt för vilka ändamål registret ska föras, t.ex. att ge offentlighet till uppgifterna som ska finnas i registret eller tillhandahålla information till viss forskning. Det förekommer att sådana bestämmelser kompletteras av bestämmelser som avser ändamålen med behandling av personuppgifter i registret (jfr avsnitt 5.3.2 om offentliga register). I de flesta fall kan dock ändamålen med personuppgiftsbehandlingen sägas sammanfalla med ändamålen för registret. Även om det inte är lika vanligt som i informationshanteringsförfattningar förekommer det att sekundära ändamål regleras särskilt också i faktiska registerförfattningar.

Ett hinder mot vidarebehandling?

I vissa fall är ändamålsbestämmelserna uttömmande. Med det avses i regel att finalitetsprincipen i artikel 5. 1 b i dataskyddsförordningen inte ska tillämpas i den del som avser vidarebehandling för ändamål som är *förenliga* med insamlingsändamålet. Det bör även innebära att vidarebehandling för *oförenliga* ändamål inte heller är tillåten, även om det finns författningsstöd för sådan behandling. Annorlunda uttryckt får personuppgifter i dessa fall inte behandlas för andra

ändamål än de som uttryckligen anges i den kompletterande dataskyddsregleringen.[74]

När ändamålsbestämmelser syftar till att vara uttömmande uttrycks detta genom att orden *endast* eller *bara* finns i bestämmelsen. Sådan reglering kan både avse primära och sekundära ändamål, t.ex. att uppgifter endast får behandlas för ett primärt ändamål och ett sekundärt ändamål. I faktiska registerförfattningar reglerar uttömmande ändamålsbestämmelser normalt för vilka ändamål själva registret får *användas*, vilket ibland även avser informationsförsörjning till andra offentliga aktörer. Trots att ändamålen är uttömmande angivna kan alltså uppgiftslämnande i överensstämmelse med lag eller förordning uttryckligen vara tillåten.[75]

Det förekommer dock att uttömmande ändamålsbestämmelser är utformade på så sätt att de inte uttryckligen tillåter författningsreglerat utlämnande vare sig till enskilda eller till andra myndigheter.

Även ändamålsbestämmelser som inte är uttömmande formulerade, dvs. där orden bara eller endast inte förkommer, kan uppfattas hindra tillämpningen av offentlighets- och sekretesslagen. Det är när de primära ändamålen inte är förenade med några sekundära ändamål, eller när det förekommer sekundära ändamål, men dessa avser annan behandling än utlämnande i överensstämmelse med lag eller förordning. Eftersom inget annat sägs kan det alltså motsatsvis uppfattas föreligga ett hinder mot att lämna ut uppgifter också i dessa fall.

Oavsett hur de är formulerade kan ändamålsbestämmelser aldrig hindra utlämnande av personuppgifter som finns i allmänna handlingar till enskilda. Rätten att ta del av allmänna handlingar som framgår av 2 kap. 1 § tryckfrihetsförordningen, TF, får nämligen bara begränsas med hänvisning till de intressen som anges i 2 kap. 2 § TF, vilka utgör de s.k. sekretessgrunderna. Utlämnande av allmänna handlingar kan alltså *enbart* hindras av bestämmelser om sekretess.

Myndigheters informationsutbyte grundar sig dock inte på bestämmelserna i 2 kap. TF (jfr avsnitt 4.2). När ändamålen i kompletterande dataskyddsreglering inte omfattar utlämnande till andra

[74] Jfr prop. 2017/18:171, *Dataskydd inom Socialdepartementets verksamhetsområde – en anpassning till EU:s dataskyddsförordning*, s. 90 och prop. 2019/20:113, *En mer ändamålsenlig dataskyddsreglering för studiestödsverksamheten*, s. 21–23.

[75] Jfr den reglering som finns i 4 och 5 §§ förordningen (2006:196) om register över hälso- och sjukvårdspersonal som var föremål för prövning i rättsfallet HFD 2021 ref. 10, se avsnitt 5.4.2.

myndigheter, kan de alltså uppfattas utgöra ett hinder mot vidarebehandling av personuppgifter genom utlämnande till andra myndigheter med stöd av offentlighets- och sekretesslagens bestämmelser.

5.4.2 Ändamålsbestämmelsernas förhållande till offentlighets- och sekretesslagen

Sekretessbestämmelsernas funktion

När en sekretessbestämmelse är tillämplig, och förutsättningarna för att sekretess ska gälla är uppfyllda, hindrar bestämmelsen utlämnandet av allmänna handlingar och uppgifter ur allmänna handlingar till enskilda. För en uppgift som *inte* är sekretessbelagd finns det däremot inget förbud mot utlämnande enligt offentlighets- och sekretesslagen (jfr 3 kap. 1 § OSL). Som vi konstaterat i avsnittet ovan begränsar alltså en sekretessbestämmelse enskildas rätt att med stöd av offentlighetsprincipen ta del av handlingar och uppgifter som finns hos myndigheterna.

När det däremot är fråga om informationsutbyte mellan myndigheter hindrar tillämpligheten av en sekretessbestämmelse utlämnande av uppgifter, oavsett om uppgifterna finns i allmänna handlingar eller inte. För en uppgift som *inte* är sekretessbelagd finns det däremot inget förbud mot utlämnande enligt offentlighets- och sekretesslagen (jfr 3 kap. 1 § OSL).

En central bestämmelse i sammanhanget är 6 kap. 5 § OSL där det framgår att myndigheter har långtgående skyldigheter att lämna uppgifter som inte är sekretessbelagda till en myndighet som begär att få del av uppgifterna. Tillämpligheten av en sekretessbestämmelse mellan myndigheter begränsar alltså myndigheternas skyldighet att samverka som bl.a. framgår av 8 § förvaltningslagen (2017:900), jfr avsnitt 4.2).[76]

Sekretess och tystnadsplikt regleras i en lag

Sekretess enligt 1937 års sekretesslag, lagen (1937:249) om inskränkningar i rätten att utbekomma allmänna handlingar, gällde enbart i förhållande till enskilda. I författning särskilt föreskriven tystnads-

[76] Jfr uttalanden i JO 2006/07, s. 270 och avsnitt 4.2.4.

plikt kunde dock gälla mellan myndigheter. Tystnadsplikter reglerades dock utanför sekretesslagen och i flera olika författningar.

När sekretessbestämmelser blev tillämpliga mellan myndigheter genom införandet av 1980 års sekretesslag (1980:100) kom de många utspridda reglerna om tystnadsplikt för medarbetare i offentlig verksamhet att ersättas med en enda lag som både reglerade handlingssekretess och tystnadsplikt. En grundläggande tanke bakom förslaget var att sekretessbehovet i princip var detsamma vare sig en uppgift var dokumenterad i en allmän handling eller inte. Sekretessbestämmelserna skulle därför i princip ha direkt giltighet också i myndigheternas verksamhet och en sekretessbelagd uppgift skulle inte få lämnas vare sig till annan myndighet eller till annan verksamhetsgren inom den egna myndigheten, eller fritt kunna utnyttjas av myndigheten eller dess personal.[77]

Eftersom sekretessbestämmelserna skulle ha direkt giltighet även för informationsutbytet mellan myndigheter krävdes undantag från sekretessen. Ett flertal av dessa framgick av sekretesslagens kapitel 14, som i stora drag motsvarar kapitel 10 i offentlighets- och sekretesslagen.

Det skulle dock även vara möjligt att reglera både sekretess och undantag från sekretess i annan lag. En förutsättning för det var dock att sekretesslagen innehöll en hänvisning till den författning som reglerade vad som skulle gälla i stället för bestämmelserna i lagen. Detta villkor uttalades i propositionen till 1980 års sekretesslag hänga samman med 2 kap. 2 § andra stycket TF enligt vilken begränsning av rätten att ta del av allmänna handlingar ska anges noga i bestämmelse i en särskild lag eller i annan lag vartill den särskilda lagen hänvisar. Avsikten var att sekretesslagen skulle lämna upplysning om *samtliga* [vår kursivering] sekretessfall.[78]

I dag framgår detta i två olika bestämmelser i offentlighets- och sekretesslagen. I 2 kap. 1 § OSL anges att förbud att röja eller utnyttja en uppgift enligt lagen eller enligt lag eller förordning som lagen *hänvisar till* gäller för myndigheter. Enligt 8 kap. 1 § OSL får en uppgift för vilken sekretess gäller enligt lagen inte röjas för enskilda eller för andra myndigheter, om inte annat anges i lagen eller i lag eller förordning som lagen *hänvisar till*.

[77] Prop. 1979/80:2, *med förslag till sekretesslag m.m.* Del A, s. 120.
[78] Prop. 1979/80:2, *med förslag till sekretesslag m.m.* Del A, s. 120.

Det är alltså möjligt att göra undantag från de generella bestämmelserna i offentlighets- och sekretesslagen, både vad gäller förbud att röja en uppgift och undantag från sådana förbud, men det förutsätter att undantaget antingen anges direkt i lagen, eller i författning som det hänvisas till i lagen. En av principerna bakom offentlighets- och sekretesslagen är alltså att sekretess och tystnadsplikt, dvs. förbud att röja en uppgift oavsett på vilket sätt detta sker, inom det allmännas verksamhet alltid ska framgå av offentlighets- och sekretesslagen, antingen direkt eller genom hänvisning till en annan lag. Sekretessbestämmelser som de framgår av offentlighets- och sekretesslagen gäller alltså på samma principiella sätt både i förhållande till andra myndigheter och i förhållande till enskilda.[79]

Problemformuleringen

En normkonflikt?

I 10 kap. 15–28 §§ och 6 kap. 5 § OSL finns de generella bestämmelser som kan sägas utgöra grunden för hur myndigheter får och i vissa fall ska utbyta information utan hinder av sekretess. En central bestämmelse är som vi redan nämnt 6 kap. 5 § OSL enligt vilken en myndighet på begäran av en annan myndighet ska lämna uppgift som den förfogar över, om inte uppgiften är sekretessbelagd eller det skulle hindra arbetets behöriga gång. En annan central bestämmelse är 10 kap. 28 § första stycket OSL som innebär att sekretess inte hindrar att en uppgift lämnas till en annan myndighet, om uppgiftsskyldighet följer av lag eller förordning. Övriga bestämmelser i 10 kap. OSL avser bl.a. uppgiftslämnande till andra myndigheter vid tillsyn eller revision, vid misstanke om vissa begångna brott och i syfte att förebygga vissa brott.

Som vi nämnt ovan är röjandeförbudet i 2 kap. 1 § OSL knutet till *sekretess som framgår av offentlighets- och sekretesslagen*. Om lagstiftaren vill förhindra att vissa uppgifter lämnas ut från en myndighet till andra myndigheter med stöd av generellt tillämpliga bestäm-

[79] Se t.ex. uttalandena i prop. 1979/80:2, *med förslag till sekretesslag m.m.* Del A, s. 68 och 91, prop. 1990/91:131, *om vissa frågor om internationellt samarbete i brottmål m.m.*, s. 26, och Justitiedepartementets broschyr, *Offentlighetsprincipen och sekretess – Kortfattat om lagstiftningen*, s. 23 och 24, tillgänglig: https://www.regeringen.se/contentassets/243fe724fd9a4121 8886261ff999fc2a/offentlighetsprincipen-och-sekretess--kortfattat-om-lagstiftningen/ (hämtad 25-01-25).

melser i 10 kap. OSL kan det alltså göras undantag från de generella bestämmelserna i anslutning till den materiella sekretessregleringen. Det kan ske genom att sekretess enligt vissa bestämmelser uttryckligen undantas från tillämpningsområdet för bestämmelserna i 10 kap. OSL eller genom en hänvisning till annan författning.

Regleringen i sak, dvs. vad som ska gälla i stället för de generellt tillämpliga bestämmelserna, behöver alltså inte framgå direkt av offentlighets- och sekretesslagen. Om något annat än vad som framgår av offentlighets- och sekretesslagen ska gälla i sak förutsätts emellertid att det hänvisas till den andra författningen i offentlighets- och sekretesslagen. På så sätt utgör offentlighets- och sekretesslagen redan i dag en nästintill allomfattande reglering av hur myndigheter får, och i vissa fall ska, utbyta information med varandra. Om den i avsnitt 4.8.5 föreslagna bestämmelsen om utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ införs, borde regleringen bli heltäckande.

Ändamålsbestämmelser i kompletterande dataskyddsreglering kan dock, som vi redogjort för ovan i avsnitt 5.4.1, leda till att ett utlämnande av uppgifter mellan myndigheter i enlighet med bestämmelserna i offentlighets- och sekretesslagen uppfattas vara dataskyddsrättsligt förbjudet. Sekretessregleringen ”matchar” dock sällan ändamålsbestämmelserna, inte ens om ändamålen är uttömmande formulerade. Det innebär att det kan uppfattas som att ett informationsutbyte mellan myndigheter, som är tillåtet eller till och med krävs enligt offentlighets- och sekretesslagen, hindras av ändamålsbestämmelserna i den kompletterande dataskyddsregleringen, trots att utlämnandet är författningsreglerat genom offentlighets- och sekretesslagens bestämmelser och därmed har en rättslig grund i dataskyddsförordningens mening.

En extra sekretessreglering?

Syftet med ändamålsbestämmelser kan alltså uppfattas vara att inskränka möjligheten att lämna uppgifter till andra myndigheter mer än vad som följer av offentlighets- och sekretesslagen. Genom att införa ändamålsbestämmelser, som inte omfattar utlämnande till andra myndigheter, skulle lagstiftaren enligt det synsättet i praktiken ha infört en *helt absolut* sekretess i förhållande till andra myndigheter,

som inte framgår av offentlighets- och sekretesslagen och inte heller bryts av de generella bestämmelserna i 10 kap. OSL eller av övriga tillämpliga sekretessbrytande bestämmelser.[80]

Det nyss sagda skulle då kunna uppfattas gälla oavsett att den faktiska sekretessen på området (enligt offentlighets- och sekretesslagen) t.ex. gäller med ett omvänt skaderekvisit. Principen om att alla tystnadsplikter i det allmännas verksamhet ska framgå av offentlighets- och sekretesslagen har då frångåtts.

Frågan om förhållandet mellan dataskydd och sekretess i relevanta förarbeten

Varför är det relevant att titta bakåt?

Som vi nyss konstaterat kan ändamålsbestämmelser i kompletterande dataskyddsreglering i praktiken uppfattas utgöra en absolut sekretessreglering, som inte motsvaras av bestämmelser i offentlighets- och sekretesslagen. Frågan om förhållandet mellan dataskydd och sekretess har berörts i förarbetena till tidigare lagstiftning, bl.a. sådan som vi redan berört i avsnitt 5.2.2. Genom att undersöka hur man resonerat särskilt om förhållandet mellan de olika regelverken, och sätta resonemangen i sitt sammanhang, bör ursprunget till den regleringssituation som föreligger i dag kunna tydliggöras. Det bör därför vara relevant att i detta sammanhang översiktliga redovisa lagstiftarens överväganden över tid.

1973 års datalag

Sekretess mellan myndigheter infördes först genom 1980 års sekretesslag. I datalagens förarbeten, dvs. innan sekretessbestämmelserna började gälla mellan myndigheter, konstaterades följaktligen att integritetsproblemen som den nya tekniken medförde inte kunde lösas enbart genom en utbyggd sekretesslagstiftning. Även om man skulle införa sådana begränsningar skulle man nämligen inte därigenom hindra att (digitalt hanterade) uppgifter cirkulerade mellan olika myndigheter. För att undvika otillbörligt intrång i den personliga integriteten skulle Datainspektionen i stället meddela föreskrifter

[80] Jfr SOU 2007:22, *Skyddet för den personliga integriteten – Kartläggning och analys*, s. 465.

avseende bl.a. tillåtna ändamål med behandlingen och utlämnande av uppgifter till andra.[81]

I det här sammanhanget bör alltså frågan om hur dataskydds- och sekretessbestämmelser förhåller sig till varandra vad gäller informationsutbyte mellan myndigheter inte ha varit särskilt relevant. Till skillnad från i dag hade de olika regelverken inte samma tillämpningsområde, och det enda sättet att hindra utlämnandet av digitalt hanterade uppgifter till andra myndigheter var i stället att föreskriva begränsningar av tillåtna ändamål. Grunddragen i hur ändamålsbestämmelser utformas (med primära och sekundära ändamål) kom alltså i ett rättsligt sammanhang som också i detta avgörande avseende skiljer sig från vad som gäller i dag (jfr avsnitt 5.2.4).

Förarbetena till 1980 års sekretesslag

När sekretess mellan myndigheter infördes upphörde samtidigt en av de omständigheter som motiverat behovet av särskilda dataskyddsföreskrifter vad gällde utlämnande till andra myndigheter. I förarbetena 1980 års sekretesslag berördes frågan om sekretesslagens förhållande till begränsningar i möjligheten att lämna ut uppgifter som behandlades med stöd av digital teknik i flera olika sammanhang. Det konstaterades bl.a. att statsmakterna främst hade försökt komma till rätta med de integritetsrisker som var förknippade med den ökande användningen av digital teknik på annat sätt än genom sekretessregler. I stället hade det genom datalagen införts ett system med tillståndstvång som i princip avsåg både allmän och enskild verksamhet.[82]

I förarbetena till sekretesslagen konstaterades även att en föreskrift som enbart innebar en begränsning av möjligheten att lämna ut ADB-upptagning på maskinläsbart medium eller genom linjeanslutning till dator eller terminal, dvs. en begränsning av möjligheten att lämna ut uppgifter elektroniskt, inte utgjorde någon begränsning av rätten att få ut allmänna handlingar. Enligt förarbetena var en sådan bestämmelse inte heller i övrigt att se som ett beslut om sekretess.[83]

[81] Jfr prop. 1973:33, *med förslag till ändringar i tryckfrihetsförordningen, m. m.*, s. 90, 97 och 98.
[82] Prop. 1979/80:2, *med förslag till sekretesslag m.m.* Del A, s. 269.
[83] Prop. 1979/80:2, *med förslag till sekretesslag m.m.* Del A, s. 213.

Vad gällde informationsutbytet mellan myndigheter konstaterades att enligt 6 § datalagen kunde Datainspektionen meddela föreskrifter om bl.a. utlämnande av uppgift från ett visst register. Att Datainspektionen inte kunde meddela förbud mot utlämnande av offentliga uppgifter mellan myndigheter, om inte förbudet var begränsat till utlämnande på datormedium eller via terminalanslutning eller liknande, fick anses stå klart. Däremot var det enligt förarbetena oklart om inspektionen hade befogenhet att allmänt reglera flödet av hemliga uppgifter från en myndighets personregister till en annan myndighet. Det kunde dock inte råda något tvivel om att en sådan föreskrift inte fick komma i konflikt med specialreglering i lag eller förordning av uppgiftslämnande mellan myndigheter.[84] Någon författningsreglering av detta förhållande infördes dock inte, och inte heller någon annan formell samordning mellan de olika regelverken.

Förarbetena till personuppgiftslagen

Betänkandet *Integritet Offentlighet Informationsteknik* (SOU 1997:39) utgjorde underlaget till propositionen om personuppgiftslagen. I betänkandet anfördes att 1995 års dataskyddsdirektiv och den föreslagna nya lagen, som båda innebar att utlämnande av personuppgifter bara fick ske om utlämnandet inte var oförenligt med de ändamål för vilka uppgifterna samlats in (finalitetsprincipen), medförde att bestämmelserna om uppgiftsskyldighet behövde ses över.[85]

Regeringen diskuterade dock inte frågan om finalitetsprincipens förhållande till särskilt reglerat informationsutbyte mellan myndigheter i propositionen. I författningskommentaren till 2 § personuppgiftslagen (där lagens subsidiaritet i förhållande till andra bestämmelser reglerades) angavs dock bl.a. att bestämmelser som föreskrev att myndigheter får eller ska lämna ut uppgifter avsågs i paragrafen och att sådana bestämmelser om s.k. uppgiftsskyldighet gick före bestämmelserna i personuppgiftslagen.[86] Regeringens uttalanden rörde dock enbart de generella bestämmelserna i person-

[84] Prop. 1979/80:2, *med förslag till sekretesslag m.m.* Del A, s. 328. Jfr även prop. 2017/18:105, *Ny dataskyddslag*, s. 137 och SOU 2017:39, *Ny dataskyddslag Kompletterande bestämmelser till EU:s dataskyddsförordning*, s. 267–269.
[85] SOU 1997:39, *Integritet Offentlighet Informationsteknik*, s. 211.
[86] Prop. 1997/98:44, *Personuppgiftslag*, s. 114 och 115.

uppgiftslagen. En översyn av registerförfattningarna och av vilka särregler som borde gälla i förhållande till den nya lagen skulle omhändertas i andra sammanhang.[87]

Inte heller här infördes dock någon formell samordning eller författningsreglering av förhållandet mellan dataskyddsregleringen och dåvarande sekretesslagen.

Förarbetena till offentlighets- och sekretesslagen

År 2003 överlämnades ett av de betänkanden från Offentlighets- och sekretesskommittén (Ju 1999:06) som kom att ligga till grund för offentlighets- och sekretesslagen, *En ny sekretesslag* (SOU 2003:99).

I betänkandet konstaterades att det i flera sammanhang gjorts gällande ett behov av att klargöra förhållandet mellan dataskydds- och sekretessbestämmelser, särskilt i frågan om finalitetsprincipen utgjorde ett hinder mot informationsutbyte mellan myndigheter med stöd av sekretesslagen. För att undanröja oklarheterna föreslogs därför att ett förtydligande om tillåtligheten av uppgiftslämnande med stöd av sekretesslagen skulle införas i personuppgiftslagen.[88] Förslaget genomfördes dock inte.

Enligt kommittén kunde dock den kompletterande regleringen ses som lex specialis även i förhållande till dåvarande sekretesslagen, i vart fall om ändamålsbestämmelserna var uttömmande. Utlämnande i enlighet med sekretesslagen, som inte hade stöd i uttömmande ändamålsbestämmelser, skulle därmed utgöra en otillåten behandling. Offentlighets- och sekretesskommitténs uppfattning var dock att rättsläget mellan registerförfattningarna och sekretesslagens bestämmelser borde klargöras i ett annat sammanhang.[89]

Inte heller i samband med att offentlighets- och sekretesslagen infördes genomfördes dock någon formell samordning eller författningsreglering av förhållandet mellan dataskydd- och sekretessbestämmelser.

[87] Prop. 1997/98:44, *Personuppgiftslag*, s. 41.
[88] SOU 2003:99, *Ny sekretesslag*, s. 230, 231 och 235.
[89] SOU 2003:99, *Ny sekretesslag*, s. 237.

Relevant praxis

Inledande anmärkning

Ändamålsbestämmelser i kompletterande dataskyddsreglering saknar som vi redan konstaterat betydelse för om uppgifter får lämnas ut till enskilda med stöd av bestämmelserna om allmänna handlingars offentlighet. När frågan om ett visst utlämnande till en enskild prövas rättslig aktualiseras därför enbart offentlighets- och sekretesslagens bestämmelser. Det finns också en mängd avgöranden från domstolarna som avser utlämnande av allmänna handlingar.

Såvitt vi kunnat se finns det dock inte praxis som *uttryckligen* berör förhållandet mellan sådana ändamålsbestämmelser i kompletterande dataskyddsreglering som kan uppfattas hindra utlämnande till andra myndigheter och bestämmelserna i offentlighets- och sekretesslagen. Nedan redogörs emellertid för ett avgörande från Högsta förvaltningsdomstolen som berör ändamålsbestämmelsernas betydelse på ett mer generellt plan.

HFD 2021 ref. 10

I rättsfallet HFD 2021 ref. 10 var frågan i målet vilken prövning som skulle göras innan personuppgifter i Socialstyrelsens register över hälso- och sjukvårdspersonal kunde lämnas till en annan myndighet med stöd av bestämmelsen om uppgiftsskyldighet mellan myndigheter i offentlighets- och sekretesslagen.

Registret i fråga regleras i förordningen (2006:196) om register över hälso- och sjukvårdspersonal, som omfattar en uttömmande ändamålsreglering. Ett av ändamålen (5 § 3 förordningen) avser att lämna uppgifter till myndigheter och enskilda i enlighet med det som föreskrivs i annan författning eller avtal. Trots att ändamålen är uttömmande angivna utesluter de alltså inte uppgiftslämnande till andra myndigheter i enlighet med offentlighets- och sekretesslagen. Kammarrätten hade emellertid ansett att ett utlämnande enligt 6 kap. 5 § OSL framstod som oförenligt med finalitetsprincipen.

I sina domskäl berörde Högsta förvaltningsdomstolen inte det förhållandet att de uttömmande ändamålen uttryckligen omfattar uppgiftslämnande till andra myndigheter. I domskälen slås det däremot fast att *bestämmelser om ändamål endast gäller för dem som om-*

fattas av regleringen i fråga (vår kursivering). Den aktuella registerförordningen uttalades alltså endast gälla för Socialstyrelsens behandling av personuppgifter. Den behandling av personuppgifter som kunde komma att utföras av en mottagande myndighet om uppgifter ur registret lämnades dit reglerades därmed inte av registerförordningen utan av de dataskyddsregler som gällde för mottagaren.

Högsta förvaltningsdomstolen konstaterade därefter att när en myndighet lämnar personuppgifter till en annan myndighet enligt 6 kap. 5 § OSL så gäller de grundläggande principerna i dataskyddsförordningen för den behandlingen. Uppgiftslämnandet som sådant måste därmed följa de principer som anges i artikel 5, bl.a. finalitetsprincipen och principen om uppgiftsminimering, dvs. att inte fler uppgifter än vad som behövs lämnas ut.

Beträffande förhållandet mellan 6 kap. 5 § OSL och finalitetsprincipen var det domstolens mening att syftet med finalitetsprincipen uppnås genom bestämmelser om uppgiftsskyldighet och sekretess dvs. att uppgiftslämnandet anses vara nödvändigt och proportionerligt i de fall uppgifterna inte omfattas av sekretess. Domstolen uttalade också att genom sekretessbestämmelser hindras myndigheterna från att lämna bl.a. integritetskänsliga uppgifter till andra myndigheter. Härigenom fick lagstiftaren anses ha tagit ställning till när ett uppgiftslämnande är oförenligt med det eller de ändamål för vilka uppgifterna samlades in. Utöver sekretessprövningen skulle den personuppgiftsansvariga myndigheten därmed inte göra någon kontroll av förenligheten med finalitetsprincipen i samband med lämnande av uppgifter enligt 6 kap. 5 § OSL.

5.4.3 Exempel på utformningen av uttömmande ändamålsbestämmelser

Offentlighets- och sekretesslagen tillskrivs olika betydelse?

Som vi redogjort för i avsnitt 3.2.2 har regeringen i en lång rad lagstiftningsärenden bedömt att det saknats anledning att i kompletterande dataskyddsreglering särskilt reglera sådant uppgiftslämnande som redan är författningsreglerat (dvs. sådant som sker i enlighet med bestämmelserna i offentlighets- och sekretesslagen). Utgångspunkten har då varit att när bestämmelser som innebär att myndigheter får eller ska lämna ut uppgifter har införts får det förutsättas

att det har gjorts en avvägning mellan intresset av att uppgiften lämnas ut och intresset av att skydda enskilda personers integritet, vid vilken man funnit att uppgiften bör lämnas ut. Ett sådant förhållningssätt till hur ändamålsbestämmelser i kompletterande dataskyddsreglering ska utformas innebär att principen som offentlighets- och sekretesslagen bygger på upprätthålls, dvs. att alla tystnadsplikter i det allmännas verksamhet, även i förhållande till andra myndigheter, ska framgå av den lagen. Det innebär också att upplevda normkonflikter mellan de olika regelverken undviks.

I de fall där det förkommer uttömmande ändamålsreglering har vi granskat förarbetena för att undersöka hur regeringen motiverat utformningen av lagstiftningen i dessa fall. Det har dock sällan varit möjligt att av lagmotiven dra någon slutsats om hur de två regelverken är tänkta att samspela. Detta gäller trots att de materiella sekretessbestämmelserna i många fall införts *samtidigt* som den kompletterande dataskyddsregleringen.

Här är det alltså ofta oklart om lagstiftaren tillskrivit offentlighets- och sekretesslagen någon särskild betydelse vad gäller informationsutbytet mellan myndigheter. Det är dock lika oklart om syftet har varit att dataskyddsvägen begränsa uppgiftslämnande mellan myndigheter med stöd av offentlighets- och sekretesslagen, utan att samtidigt införa undantag eller en hänvisning i den lagen.[90] Vi har dock hittat en handfull sammanhang där syftet med den uttömmande ändamålsregleringen förefaller ha varit att göra undantag från offentlighets- och sekretesslagens bestämmelser, utan att det samtidigt införts undantag eller en hänvisning till den aktuella författningen i offentlighets- och sekretesslagen. Ett av dessa exempel redogörs för nedan, övriga behandlar vi i avsnitt 5.4.7.

Nedan ges två exempel från senare tid som tydliggör hur lagstiftarens skiftande inställning till vad offentlighets- och sekretessregleringen innebär avspeglar sig i lagstiftningen och vilka problem detta kan ge upphov till.

[90] Jfr t.ex. prop. 1998/99:72, *Rättspsykiatriskt forskningsregister*, s. 22, 33, 36–38 och 54, och prop. 2017/18:298, *Behandling av personuppgifter för forskningsändamål*, s. 152 och 153. Jfr även prop. 2005/06:141, *Genomförande av EG-direktivet om kvalitet och säkerhet hos blod och blodkomponenter*, s. 50 och 62–64.

Två exempel i närtid

Ett allt mindre problem i ny lagstiftning …

Uttömmande ändamålsbestämmelser kan användas för att begränsa integritetsintrånget i den verksamhet där bestämmelserna ska tillämpas, utan att detta påverkar uppgiftsutbyte med andra myndigheter i enlighet med offentlighets- och sekretesslagen. Ett exempel på reglering med den innebörden finns i den relativt nyligen införda uttömmande ändamålsregleringen för uppgifter som Skatteverket samlar in från vissa betaltjänstleverantörer i 1 kap. 4 a och 5 a §§ lagen om behandling av personuppgifter i Skatteverkets beskattningsverksamhet, SdbL. Själva insamlandet av uppgifter från betaltjänstleverantörer vilar på EU-rättslig grund, som huvudsakligen innebär att Skatteverket ska samla in uppgifterna för att vidarebefordra dem till en unionsgemensam funktion för kontroll av vissa skattebedrägerier.

Regleringen i 1 kap. 4 a och 5 a §§ SdbL innebär sammanfattningsvis att uttömmande ändamål gäller för Skatteverkets *egen* behandling av uppgifterna, men att uppgifterna även får vidarebehandlas för att fullgöra uppgiftslämnande i överensstämmelse med lag eller förordning, utan några begränsningar i detta avseende.

Enligt regeringen fanns det starka integritetsskäl som talade för att begränsa för vilka ändamål Skatteverket för egen del skulle få använda uppgifter från betaltjänstleverantörer. Det konstaterades bl.a. röra integritetskänsliga uppgifter om främst enskildas ekonomiska förhållanden som hämtas in från tredje man. De uppgifter som skulle samlas in hade dessutom inte något direkt samband med beskattningen. Skatteverket skulle därför för egen del enbart få behandla uppgifterna för att vidarebefordra dem till den unionsgemensamma funktionen och att kontrollera att betaltjänstleverantörerna gjorde vad som ankom på dem.[91]

Däremot bedömde regeringen att bestämmelser om utlämnande av uppgifter till andra myndigheter rörde särskilt angelägna verksamheter där det i samband med regleringens tillkomst hade gjorts bedömningen att behovet för en myndighet att få ta del av uppgifterna övervägde integritetsintresset. Skatteverket skulle därför även få behandla uppgifterna för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning. Annars kunde det enligt

[91] Prop. 2022/23:121, *Nya krav på betaltjänstleverantörer att lämna uppgifter*, s. 93 och 94.

regeringen uppstå situationer där sekretessregleringen innebar att uppgifter får, eller till och med ska, lämnas ut, men ett utlämnande hindras för att uppgiften hanteras med modern informationsteknik.[92]

Regleringen i 1 kap. 4 a och 5 a §§ SdbL utgör alltså inget hinder mot att Skatteverkets vidarebehandlar uppgifterna för utlämnande till andra myndigheter i överensstämmelse med offentlighets- och sekretesslagens bestämmelser. Däremot innebär den ett hinder mot Skatteverkets vidarebehandling i den egna verksamheten.

… men det förekommer fortfarande

Trots att det förekommer alltmer sällan finns det också exempel på nyare lagstiftningsinitiativ där lagstiftaren har infört uttömmande ändamålsbestämmelser som hindrar utbyte av uppgifter mellan myndigheter som annars är tillåtet enligt offentlighets- och sekretesslagen, utan att samtidigt anpassa den materiella sekretessregleringen till detta.

Ett aktuellt exempel finns i lagen (2024:1146) om vissa forskningsdatabaser. Det övergripande syftet med lagen är att göra det möjligt för universitet och högskolor att föra forskningsdatabaser som har ett särskilt vetenskapligt värde. Insamlingen och behandlingen av personuppgifter i en sådan forskningsdatabas ska ske med de registrerades frivilliga medverkan.[93]

I förarbetena uttalade regeringen att uppgifterna i databaserna kan vara av mycket integritetskänslig natur och att det finns ett starkt intresse av att kunna skydda dem genom bestämmelser om sekretess. Regeringen bedömde att vetskapen om att det finns ett sekretesskydd för uppgifterna i en forskningsdatabas var mycket betydelsefull för det frivilliga deltagandet och villigheten att lämna personuppgifter till en forskningsdatabas. Av integritetsskäl var det enligt regeringens mening även angeläget att upprätthålla sekretessen i förhållande till andra myndigheter.[94]

Den materiella sekretessregleringen på området avseende personuppgifter, dvs. 24 kap. 2 a § OSL, är absolut och omfattas inte av tillämpningsområdet för generalklausulen, dvs. 10 kap. 27 § OSL. Ändamålsbestämmelserna i lagen om vissa forskningsdatabaser är därtill uttömmande angivna. 3 kap. 5 § i den lagen motsvarar en

[92] Prop. 2022/23:121, *Nya krav på betaltjänstleverantörer att lämna uppgifter*, s. 111.
[93] Prop. 2024/25:19, *Långsiktig reglering av vissa forskningsdatabaser*, s. 1.
[94] Prop. 2024/25:19, *Långsiktig reglering av vissa forskningsdatabaser*, s. 190 och 193.

sekundär ändamålsbestämmelse och innebär att personuppgifter och uppgifter om avlidna, utöver vad som särskilt anges i lagen, enbart får lämnas ut om det finns en *skyldighet* att göra det enligt lag eller förordning. Syftet bakom regleringen i denna del är enligt förarbetena att undvika konflikter med annan lagstiftning.[95]

I 24 kap. 2 a § OSL, dvs. i den materiella sekretessbestämmelsen på området, finns dock inte några undantag från tillämpligheten av de generella sekretessbrytande bestämmelserna i 10 kap. OSL. Det innebär att den absoluta sekretessen bryts i förhållande till myndigheter i en mängd fall, t.ex. av 10 kap. 23 § OSL som avser misstanke om ett begånget brott av allvarligare art.

Om uppgiftslämnande med stöd av 10 kap. 23 § OSL aktualiseras efter en begäran har den utlämnande myndigheten en långgående skyldighet att lämna ut uppgifterna enligt 6 kap. 5 § OSL. Bestämmelsen i 10 kap. 23 § OSL kan emellertid ligga till grund för uppgiftslämnande både på eget initiativ och på begäran, precis som andra sekretessbrytande bestämmelser i offentlighets- och sekretesslagen.[96] Utformningen av den sekundära ändamålsbestämmelsen i 3 kap. 5 § lagen om vissa forskningsdatabaser, dvs. att uppgifter enbart får vidarebehandlas genom utlämnande när det föreligger en *skyldighet* att lämna uppgifter bör dock kunna uppfattas innebära att det inte är möjligt att tillämpa 10 kap. 23 § OSL utan en föregående begäran.[97]

Att det i anslutning till 24 kap. 2 a § OSL inte heller föreskrivits några undantag från tillämpningsområdet för 10 kap. 28 § OSL innebär vidare att de många uppgifts- anmälnings- och underrättelseskyldigheterna som finns utanför offentlighets- och sekretesslagen också bryter sekretessen enligt 24 kap. 2 a § OSL. Bestämmelser om uppgiftsskyldighet kan avse en skyldighet att *på eget initiativ* lämna upplysningar t.ex. redan vid ett antagande om att vissa missförhållanden föreligger, vilket vi redogör för i avsnitt 4.5.

Regleringen borde sammantaget kunna uppfattas innebära följande. Den sekundära ändamålsbestämmelsen i 3 kap. 5 § lagen om vissa forskningsdatabaser medger en underrättelse på eget initiativ med stöd av t.ex. 32 c § folkbokföringslagen (1991:481) dvs. om det kan antas att en uppgift i folkbokföringen är oriktig eller ofull-

[95] Prop. 2024/25:19, *Långsiktig reglering av vissa forskningsdatabaser*, s. 165.
[96] Jfr prop. 1979/80:2, *Ny sekretesslag* Del A, s. 327, prop. 1983/84:142, *om ändring i sekretesslagen (1980:100) m.m.*, s. 27 och prop. 2019/20:123, *Ett effektivare informationsutbyte mellan polis och socialtjänst vid samverkan mot terrorism*, s. 49 och 50.
[97] Jfr prop. 2024/25:19, *Långsiktig reglering av vissa forskningsdatabaser*, s. 194 och 195.

ständig. Så är fallet eftersom den bestämmelsen innehåller ett *ska*-krav och därför utgör en skyldighet att på eget initiativ underrätta Skatteverket om en misstänkt felaktighet i folkbokföringen. Däremot är ett uppgiftslämnande på eget initiativ vid misstanke om att ett allvarligt brott är begånget, med stöd av 10 kap. 23 § OSL, inte tillåtet enligt den sekundära ändamålsbestämmelsen – trots att det *dels* inte finns några sekretesshinder i något av fallen, *dels* i dataskyddsrättslig mening finns en rättslig grund för utlämnandet i båda situationerna.

Sekretess enligt 24 kap. 2 a § OSL överförs dessutom till en mottagare av uppgifterna enligt 24 kap. 2 b § OSL. I de fall mottagaren också ska tillämpa lagen om vissa forskningsdatabaser vid sin personuppgiftsbehandling kommer uppgifterna träffas av samma regelverk hos mottagaren som hos den utlämnande myndigheten. Om mottagaren däremot *inte* ska tillämpa samma kompletterande dataskyddsreglering som den utlämnande myndigheten kommer den mottagande aktören inte vara förhindrad att lämna ut uppgifterna på eget initiativ med stöd av 10 kap. 23 § OSL eller för den delen andra tillämpliga sekretessbrytande bestämmelser i offentlighets- och sekretesslagen.

Situationen kompliceras ytterligare av att det i 3 kap. 7 § första stycket lagen om vissa forskningsdatabaser föreskrivs en tystnadsplikt för mottagare av uppgifter från en forskningsdatas som inte ska tillämpa bestämmelserna i offentlighets- och sekretesslagen (dvs. hos enskilda forskningshuvudmän). Tystnadsplikten hindrar dock enbart *obehörigt röjande* av uppgifter. I lagkommentaren till den bestämmelsen anges att som obehörigt röjande anses inte att någon fullgör sådan uppgiftsskyldighet som följer av lag eller förordning. Det är enligt lagkommentaren inte heller fråga om obehörigt röjande om utlämnande sker i en situation när motsvarande uppgifter *skulle ha fått lämnas ut enligt offentlighets- och sekretesslagen*.[98] Någon hänvisning till att röjandet även ska vara förenligt med bestämmelserna i lagen om vissa forskningsdatabaser finns dock inte. Det borde innebära att tystnadsplikten för mottagare som inte ska tillämpa vare sig bestämmelserna i offentlighets- och sekretesslagen eller bestämmelserna i lagen om vissa forskningsdatabaser inte motsvarar den som utlämnande aktörer måste iaktta, vilket inte förefaller vara syftet med regleringen.

[98] Prop. 2024/25:19, *Långsiktig reglering av vissa forskningsdatabaser*, s. 255.

Av 3 kap. 7 § andra stycket lagen om vissa forskningsdatabaser framgår dessutom att för myndigheter gäller inte den tystnadsplikt som föreskrivs i paragrafens första stycke, utan bestämmelserna i offentlighets- och sekretesslagen. Regleringen av sekretess i offentlighets- och sekretesslagen går dock inte att skilja från tystnadsplikten enligt samma lag (jfr avsnitt 5.4.2). Här uppstår alltså frågan om hänvisningen till offentlighets- och sekretesslagen i fråga om tystnadsplikt för myndigheter har den innebörden att tystnadsplikten inte ska motsvara det som annars gäller enligt den sekundära ändamålsbestämmelsen i 3 kap. 5 § lagen om vissa forskningsdatabaser. Bestämmelserna i offentlighets- och sekretesslagen innebär ju som vi redan konstaterat större möjligheter att lämna ut uppgifter än vad som är tillåtet enligt den sekundära ändamålsbestämmelsen.

Sammanfattningsvis verkar lagstiftaren i detta fall inte ha tillskrivit offentlighets- och sekretesslagen den funktion som ursprungligen avsetts, dvs. att alla förbud att röja en uppgift som ska gälla i det allmännas verksamhet ska framgå av den lagen. Som framgår av redogörelsen ovan ger detta upphov både till en generell komplexitet och att det i flera avseenden uppstår konflikter och oklarheter mellan bestämmelserna i offentlighets- och sekretesslagen och den kompletterande dataskyddsregleringen.

5.4.4 Begränsningar av utbytet av uppgifter mellan myndigheter regleras i offentlighets- och sekretesslagen

Vår bedömning: Begränsningar av de möjligheter och skyldigheter i fråga om utbyte av uppgifter mellan myndigheter som följer av generella bestämmelser i offentlighets- och sekretesslagen ska ske genom hänvisning till annan författning eller undantag i den lagen.

Skälen för vår bedömning

Tillämpligheten av generella bestämmelser i offentlighets- och sekretesslagen kan behöva begränsas

Möjligheten att med stöd av generellt tillämpliga bestämmelser i offentlighets- och sekretesslagen lämna uppgifter till andra myndigheter kan i vissa fall behöva begränsas för att uppnå ett adekvat integritetsskydd, oberoende av om det finns en kompletterande dataskyddsreglering för verksamheten eller inte. En begränsning av möjligheterna till utlämnande till andra myndigheter kan till och med krävas för att lagstiftningen på ett visst område ska framstå som proportionerlig och därmed uppfylla de krav som bl.a. framgår av regeringsformen och dataskyddsförordningen. Sådana begränsningar kan även vara motiverade av att verksamheten i fråga är beroende av att enskilda frivilligt och utan någon uppenbar fördel för dem själva lämnar uppgifter till en myndighet om mer eller mindre privata förhållanden. Ett starkt sekretesskydd för uppgifterna, även i förhållande till andra myndigheter, kan i sådana situationer vara en förutsättning för enskildas vilja att bidra till verksamheten (jfr t.ex. avsnitt 8.3 i SOU 2024:63).

Skälen bakom reglering som inte medger uppgiftslämnande till andra myndigheter i enlighet med offentlighets- och sekretesslagens generella bestämmelser kan alltså väga mycket tungt. Frågan är då vilka möjligheter att förhindra informationsutbyte mellan myndigheter som lagstiftaren har.

Undantag och hänvisningar i offentlighets- och sekretesslagen

Lagrådet har uttalat att ett undantag från en bestämmelse i en lag, föranlett av att specialbestämmelser finns i en annan lag, bör tas in i den lag från vilken undantag görs.[99] Detta uttalande tydliggör hur undantag från offentlighets- och sekretesslagens generella bestämmelser är möjligt att göra.

[99] Lagrådets yttrande över förslag till lag om behandling av personuppgifter inom socialförsäkringens administration, 2003-05-15, s. 2, tillgängligt: https://www.lagradet.se/wp-content/uploads/lagradet-attachments/Personuppgifter%20inom%20socialforsakringen.pdf (hämtad 25-02-13).

Sekretess enligt offentlighets- och sekretesslagen gäller både mellan myndigheter och mellan myndigheter och enskilda (8 kap. OSL). Enligt 2 kap. 1 § OSL gäller förbud att röja eller utnyttja en uppgift enligt offentlighets- och sekretesslagen *eller enligt lag eller förordning som offentlighets- och sekretesslagen hänvisar till* för myndigheter. Om syftet är att förhindra uppgiftsutbyte med andra myndigheter kan alltså lagstiftaren införa undantag direkt i offentlighets- och sekretesslagen, eller införa en hänvisning till den författning som innehåller de begränsningar som lagstiftaren anser bör gälla på området. Begränsningar av tillämpligheten av generella bestämmelser kan alltså ske på olika sätt.

Ett exempel är utformningen av 10 kap. 23 och 24 §§ OSL som båda avser sekretessgenombrott vid misstanke om vissa begångna brott. I dessa fall är 23 § tillämplig för sekretess enligt särskilt angivna bestämmelser, och 24 § tillämplig för annan sekretess än den som anges i 23 §. Ett annat exempel är den sekretess som helt är undantagen generalklausulens tillämpningsområde (10 kap. 27 § andra stycket OSL). I de allra flesta fall bör dock en sådan regleringsmodell vara alltför trubbig. De generella bestämmelserna i 10 kap. OSL kan nämligen behöva vara tillämpliga i vissa situationer, men inte i andra.

Rubriken till 9 kap. OSL lyder Förbud i annan lagstiftning mot att röja eller utnyttja uppgift. De tre paragraferna i kapitlet innehåller hänvisningar till bestämmelser som reglerar inskränkningar i möjligheten att utnyttja eller röja vissa uppgifter i andra lagar än offentlighets- och sekretesslagen[100]. Bestämmelserna har bl.a. införts med hänvisning till principen om att alla tystnadsplikter inom det allmännas verksamhet ska framgå av nuvarande offentlighets- och sekretesslagen, antingen direkt eller genom en hänvisning till en annan lag.[101] I 9 kap. 1 § OSL finns hänvisningar till lagstiftning som innehåller bestämmelser om förbud att röja eller utnyttja vissa uppgifter som sannolikt har en väsentlig inverkan på priset på finansiella instrument. I 9 kap. 2 § OSL hänvisas till flera lagar som innehåller bestämmelser om begränsningar i möjligheten att utnyttja information som erhållits enligt internationella avtal eller EU-rättsakter. I 9 kap. 3 § OSL finns slutligen en upplysning om att utöver bestämmelserna om

[100] Prop. 2008/09:150, *Offentlighets- och sekretesslag*, s. 368.
[101] Jfr t.ex. prop. 1990/91:42, *Insiderhandel*, s. 110 och prop. 1990/91:131, *om vissa frågor om internationellt samarbete i brottmål m.m.* s. 26.

sekretess i offentlighets- och sekretesslagen finns det föreskrifter som är tillämpliga när det gäller tystnadsplikt beträffande företagshemligheter och tystnadsplikt för revisorer.

Sådana användningsbegränsningar som hänvisas till i 9 kap. 2 § OSL har ofta likheter med uttömmande ändamålsbestämmelser och anger att uppgifter endast får behandlas för vissa ändamål (jfr avsnitt 5.4.1). De utgör inte bestämmelser om sekretess och hindrar inte enskildas rätt att ta del av allmänna handlingar. Uppräkningen i 9 kap. 2 § OSL är dessutom inte heltäckande.[102] I flera relevanta förarbeten har det dock uttalats att det följer av de hänvisade användningsbegränsningarna att en annan myndighet än den som förfogar över uppgifterna inte kan utnyttja de uppgifter som avses i bestämmelserna i sin verksamhet i andra fall än som är tillåtet enligt de aktuella bestämmelserna, samt att detta innebär att det i praktiken bara borde bli aktuellt att åberopa sekretessbrytande regler i offentlighets- och sekretesslagen mellan myndigheter när en myndighet har rätt att ta del av uppgifterna enligt nämnda bestämmelserna om användningsbegränsningar.[103] Det innebär att de hänvisade användningsbegränsningarna och offentlighets- och sekretesslagens bestämmelser kan tillämpas parallellt men utan att någon normkonflikt uppstår.

Det går också att göra undantag från tillämpligheten av bestämmelserna i 10 kap. OSL i direkt anslutning till den materiella sekretessregleringen i fråga. En sådan reglering kan föreskriva att vissa av eller alla sekretessbrytande bestämmelser, t.ex. i 10 kap. OSL, inte ska gälla, och samtidigt hänvisa till den författning som anger vad som ska gälla i stället i fråga om utlämnande av uppgifter till andra myndigheter. Sådana bestämmelser finns t.ex. för sekretessen i det internationella samarbetet. Av 15 kap. 1 a § tredje stycket OSL framgår att om sekretess gäller enligt paragrafens första eller andra stycke,

[102] SOU 2015:39, *Myndighetsdatalag*, s. 153.
[103] Se Lenberg m.fl., *Offentlighets- och sekretesslagen* (2009:400), 11 dec. 2024, JUNO, kommentaren till 9 kap. 2 §. De förarbeten som avses är prop. 1990/91:131, *om vissa frågor om internationellt samarbete i brottmål m.m.* s. 24 och 25, prop. 2011/12:15, *Genomförande av det nya EU-direktivet om bistånd med indrivning*, s. 54, prop. 2011/12:163, *Utbyte av uppgifter ur kriminalregister mellan EU:s medlemsstater*, s. 50 och 51, prop. 2012/13:4, *Genomförande av det nya EU-direktivet om administrativt samarbete i fråga om beskattning*, s. 61, 90 och 91, prop. 2014/15:41, *Genomförande av avtal mellan Sveriges regering och Amerikas förenta staters regering för att förbättra internationell efterlevnad av skatteregler och för att genomföra FATCA*, s. 196 och 197, prop. 2015/16:29, *En global standard för automatiskt utbyte av upplysningar om finansiella konton*, s. 210 och prop. 2016/17:47, *Dokumentation vid internprissättning och land-för-land-rapportering på skatteområdet*, s. 84.

får de sekretessbrytande bestämmelserna i 10 kap. 5 c §, 15–27 §§ och 28 § första stycket OSL inte tillämpas.

Motsvarande reglering finns även för verksamhet som avser förande av eller uttag ur register enligt lagen (1998:620) om belastningsregister. Av 35 kap. 3 § första stycket OSL framgår att det råder absolut sekretess för uppgift i registret, och att i fråga om utlämnande av uppgifter gäller vad som är föreskrivet i lagen om belastningsregister och i säkerhetsskyddslagen (2018:585) samt i förordningar som har meddelats med stöd av dessa lagar. Av paragrafens tredje stycke framgår även att bestämmelserna i 10 kap. OSL inte gäller för sekretess enligt första stycket.

Inte heller här uppstår någon konflikt mellan dataskyddsregleringen och sekretessregleringen eftersom begränsningar av offentlighets- och sekretesslagens generella bestämmelser, liksom hänvisning till vad som ska gälla i stället, sker direkt i offentlighets- och sekretesslagen.

Undantag och begränsningar regleras i offentlighets- och sekretesslagen

Möjligheten att genom undantag direkt i offentlighets- och sekretesslagen och/eller hänvisning till annan författning ställa upp rättsliga hinder för uppgiftsutbyte mellan myndigheter med stöd av annars tillämpliga bestämmelser har använts i olika sammanhang sedan 1980 års sekretesslag infördes.[104] Det är alltså inte någon ny eller förändrad regleringsmodell som vi redogjort för ovan, utan något som i dag anvisas direkt genom bestämmelserna i offentlighets- och sekretesslagen och tidigare framgick av sekretesslagen. Den ger framför allt uttryck för principen om att alla tystnadsplikter i det allmännas verksamhet ska framgå av en lag (jfr avsnitt 5.4.2).

Någon möjlighet att avvika från denna regleringsmodell vad gäller vilken sekretess och tystnadsplikt som ska gälla inom det allmännas verksamhet finns inte i offentlighets- och sekretesslagen och fanns inte heller i 1980 års sekretesslag. Såvitt vi kunnat se finns det heller inget uttalande, beslut, annan författningsreglering eller motsvarande som tyder på att lagstiftaren ändrat inställning avseende att sekretess ska framgå av en särskild lag, dvs. offentlighets- och sekretesslagen, som ska gälla på samma sätt för myndig-

[104] Jfr prop. 1979/80:2, *med förslag till sekretesslag m.m.* Del A, s. 214.

heter som för enskilda. Vår bedömning är därför att gällande rätt är att begränsningar av de möjligheter och skyldigheter i fråga om att lämna uppgifter mellan myndigheter som följer av generella bestämmelser i offentlighets- och sekretesslagen enbart kan ske genom undantag som görs direkt i den lagen eller att i den lagen införa en hänvisning till annan författning.

5.4.5 Ändamålsbestämmelser hindrar inte uppgiftslämnande med stöd av offentlighets- och sekretesslagen

Vår bedömning: Ändamålsbestämmelser i kompletterande dataskyddsreglering hindrar inte tillämpligheten av bestämmelserna i offentlighets- och sekretesslagen.

Skälen för vår bedömning

Syftet med ändamålsbestämmelser

Ändamålsbestämmelser i kompletterande dataskyddsreglering kan aldrig påverka enskildas grundlagsskyddade rätt att få del av allmänna handlingar, utan den rätten kan enbart begränsas av faktiska bestämmelser om sekretess. I avsnitt 5.4.2 har vi däremot konstaterat att ändamålsbestämmelser riskerar att uppfattas som en slags extra sekretessreglering som enbart gäller mellan myndigheter, trots att de inte ”matchas” av faktisk sekretessreglering i offentlighets- och sekretesslagen, t.ex. genom undantag från de generellt tillämpliga bestämmelserna i 10 kap. OSL för sådan sekretess som gäller på området. Frågan är då i vilken utsträckning befintliga ändamålsbestämmelser i den kompletterande dataskyddsregleringen faktiskt syftar till att begränsa eller hindra sådant informationsutbyte mellan myndigheter som är tillåtet enligt offentlighets- och sekretesslagen.

Som vi påpekat i avsnitt 5.4.3 har lagstiftaren i regel inte fört tydliga resonemang i förarbeten om förhållandet mellan ändamålsbestämmelser i kompletterande dataskyddsreglering och den reglering av informationsutbyte mellan myndigheter som framgår av offentlighets- och sekretesslagen. Det nyss sagda gäller med några få undantag, se avsnitt 5.4.7 nedan. Om ändamålsbestämmelserna faktiskt är avsedda att begränsa de generella möjligheterna till informationsutbyte

som följer av offentlighets- och sekretesslagen är alltså i de allra flesta fall oklart, trots att den materiella sekretessregleringen inte sällan har införts samtidigt som dataskyddsregleringen. Syftet med ändamålsbestämmelserna behöver därför analyseras utifrån något annat än vad som framgår av förarbetena.

Sekretessbestämmelser gäller mellan myndigheter

Inledningsvis bör nämnas att situationen med upplevda normkonflikter mellan dataskyddsreglering och sekretessbestämmelser bör ha uppstått i samband med införandet av 1980 års sekretesslag. Det var först i detta sammanhang som sekretess och tystnadsplikt gjordes synonyma och regleringen blev samtidigt tillämplig mellan myndigheter. Innan 1980 års sekretesslag infördes hade det inte funnits några andra sätt att reglera myndigheters utbyte av uppgifter som hanterades elektroniskt än att i dataskyddsregleringen, dvs. i registerförfattning eller genom tillstånd och föreskrift från Datainspektionen, begränsa sådant uppgiftslämnande (jfr avsnitt 5.4.2).

När sekretess mellan myndigheter infördes genom 1980 års sekretesslag upphörde alltså det förhållande som motiverat behovet av att ha särskilda dataskyddsföreskrifter för när utlämnande av uppgifter till andra myndigheter fick ske. Som vi redogjort för i avsnitt 5.4.2 noterade regeringen i och för sig redan då att det fanns en osäkerhet om Datainspektionens befogenheter att begränsa informationsutbytet mellan myndigheter. Att inspektionen inte hade befogenhet att meddela föreskrifter i konflikt med specialreglering av uppgiftslämnande mellan myndigheter i lag eller förordning var dock enligt regeringen klart.[105] Det uttalandet bör kunna innebära att det ursprungliga förhållandet mellan dataskydd och sekretess var att dataskyddsregleringen inte skulle kunna innehålla särreglering i förhållande till sekretesslagen.

Någon lagstiftningsåtgärd i syfte att rent formellt samordna de olika regelverken vidtogs inte då och har inte heller vidtagits senare. I stället har den regleringsmodell som följde av 1973 års datalag, i den meningen att utlämnande till andra myndigheter har varit föremål för särskilda dataskyddsbestämmelser, fortsatt att användas ända fram till i dag.

[105] Prop. 1979/80:2, *med förslag till sekretesslag m.m.* Del A, s. 328.

Utökad tillämplighet genom teknisk utveckling

I avsnitt 5.2.4 har vi uppmärksammat att det föreligger ett generellt reformbehov vad gäller den kompletterande dataskyddsregleringen. Vi påpekar där att bestämmelser som ursprungligen avsett en avgränsad form av informationshantering numera är tillämpliga på all informationshantering vid myndigheterna. Som vi konstaterat i det avsnittet innebär begränsningar av hur och vilka uppgifter en myndighet får behandla med digitala verktyg i dag också en begränsning av den materiella verksamhetsregleringen i sig.

Samma synsätt bör kunna bringa viss klarhet i frågan om i vilken utsträckning ändamålsbestämmelser har införts i syfte att begränsa de möjligheter och skyldigheter avseende informationsutbyte som framgår av offentlighets- och sekretesslagen. Begränsningar av möjligheten att använda datorer kunde tidigare innebära att ett uppgiftslämnande till en annan myndighet fick utföras analogt, men inte att utlämnandet *i sig* var förbjudet. I t.ex. början av 2000-talet bör alltså en ändamålsreglering som var uttömmande, eller på annat sätt syntes hindra utlämnande av uppgifter, inte ha orsakat samma problem i förhållande till sekretessregleringen som i dag, eftersom uppgifter fortfarande hanterades på papper. Utlämnande kunde då i stället ske i enlighet med bestämmelserna i dåvarande sekretesslagen och på samma sätt som annan ”normal” informationshantering, dvs. på papper, via fax eller via telefon. Det nyss sagda framgår t.ex. av regeringens uttalanden i samband införandet av patientdatalagen (2008:355). Där uttalade regeringen att det saknades anledning att förhindra att personuppgifter som finns i hälso- och sjukvården lämnas ut med stöd av dåvarande sekretesslagen bara för att dessa numera hanteras med modern informationsteknik i stället för som tidigare på papper.[106] Samma resonemang om modern informationsteknik motiverade också den särskilda ändamålsregleringen för Skatteverkets behandling av uppgifter från betaltjänstleverantörer som nämns i avsnitt 5.4.3.

Med det nyss sagda i åtanke framstår också bristen på förarbetsuttalanden om ändamålsbestämmelsernas förhållande till sekretessregleringen i ett annat ljus. Frågan kan helt enkelt ha varit irrelevant eftersom den problematiken inte förväntades bli aktuell i tillämpningen. Ändamålsbestämmelser kan alltså ha fått en oavsiktligt

[106] Prop. 2007/08:126, *Patientdatalag m.m.*, s. 59 och 60.

förändrad och utökad tillämplighet genom digitaliseringen av den offentliga förvaltningen.

Utökad tillämplighet genom rättslig utveckling

I avsnitt 5.2.4 har vi också uppmärksammat att det finns ett generellt reformbehov avseende den kompletterande dataskyddsregleringen utifrån den rättsliga utvecklingen. Även om det i t.ex. början av 2000-talet bör ha varit så att informationsutbyte mellan myndigheter i många fall skedde analogt, och att dataskyddsregleringen därför inte blev tillämplig, bör detta inte ha varit lika självklart efter att dataskyddsförordningen började tillämpas 2018.

Enligt artikel 2.1 i dataskyddsförordningen är förordningens tillämpningsområde mycket brett. Förordningen ska tillämpas på sådan behandling av personuppgifter som *helt eller delvis* företas på automatisk väg, samt på *annan behandling än automatisk* av personuppgifter som ingår i eller kommer att ingå i ett register.

Även förordningens definition av behandling i artikel 4.2 är mycket bred; en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, *oberoende av om de utförs automatiserat eller ej*, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

Eftersom den kompletterande dataskyddsregleringen är just kompletterande så bör dataskyddsförordningens breda tillämpningsområde avsevärt ha minskat möjligheterna att göra en rättslig åtskillnad mellan bestämmelser som enbart träffar automatiserad behandling och bestämmelser som inte gör det. Även om det faktiska utlämnandet i dag fortfarande kan ske på papper eller muntligt så kommer också detta handlande träffas av den särskilda dataskyddsregleringen. Förordningens bestämmelser gäller nämligen ofta oberoende av om åtgärderna utförs automatiserat eller ej. Om uppgifterna dessutom behandlas digitalt hos den utlämnande myndigheten, och därför måste tas fram digitalt för att kunna läsas eller skrivas ut, så utgör detta förfarande uttryckligen en automatiserad behandling som träffas av förordningens bestämmelser. Ändamåls-

bestämmelser kan därmed ha fått en förändrad tillämplighet också genom den rättsliga utvecklingen.

Sammanfattning

Sammanfattningsvis kan alltså ändamålsbestämmelser, i takt med en tilltagande digitalisering och förändringar av den allmänna dataskyddsregleringen ha fått ”eget liv” genom att de tillskrivits en betydelse som de ursprungligen inte haft och som går utöver syftet med dem. Någon samlad och genomgripande analys av detta förhållande har dock inte gjorts, och de olika regelverken har inte heller formellt samordnats genom lagstiftning eller motsvarande.

Om ändamålsbestämmelser skulle anses utgöra ett hinder mot uppgiftslämnande i överensstämmelse offentlighets- och sekretesslagens bestämmelser så skulle det dessutom innebära att sekretess mellan myndigheter regleras i annan ordning än den som anvisas i offentlighets- och sekretesslagen. Som vi noterat i avsnitt 5.4.4 finns det dock såvitt vi kunnat se inte något uttalande, beslut eller motsvarande som tyder på att lagstiftaren ändrat inställning avseende att sekretess ska framgå av en särskild lag, dvs. offentlighets- och sekretesslagen, som ska gälla på samma sätt för myndigheter som för enskilda. I sammanhanget kan även rättsfallet HFD 2021 ref. 10 åter nämnas, där Högsta förvaltningsdomstolen konstaterade att när det fanns tillämpliga kompletterande ändamålsbestämmelser så var den enda prövning som skulle ske, innan ett utlämnande med stöd av en bestämmelse i offentlighets- och sekretesslagen, om utlämnandet var förenligt med den bestämmelsen, och inte ändamålsbestämmelserna.

Vi bedömer därför att ändamålsbestämmelser i kompletterande dataskyddsreglering, både uttömmande och andra, inte vare sig syftar till att hindra, eller rent faktiskt kan hindra, tillämpligheten av bestämmelserna i offentlighets- och sekretesslagen (jfr dock avsnitt 5.4.7 nedan).

5.4.6 En upplysningsbestämmelse om uppgiftslämnande i överensstämmelse med lag eller förordning

Vårt förslag: Det ska införas upplysningsbestämmelser om tillåtligheten av uppgiftslämnande i överensstämmelse med lag eller förordning i kompletterande dataskyddsreglering som omfattas av vår översyn.

Skälen för vårt förslag

Behovet av en tydligare och mer samordnad reglering

Vår kartläggning av behoven av förbättrade möjligheter till informationsutbyte mellan myndigheter, som redovisas delvis i avsnitt 5.3.3 och i sin helhet i kapitel 4 i vårt delbetänkande, visar att sekretessregleringen genomgående uppfattas vara komplex och svårtillämpad.

Även dataskyddsregleringen uppfattas generellt vara en komplex och svårtillämpad lagstiftning, särskilt sedan 2016 års EU-rättsliga dataskyddsreform började tillämpas i maj 2018.[107] Som ett resultat av den dataskyddsrättsliga reformen har flera myndigheter t.ex. i dag en trippel dataskyddsreglering att förhålla sig till; dataskyddsförordningen, dataskyddslagen och kompletterande dataskyddsreglering (registerförfattning).

Sekretessbestämmelserna och dataskyddsbestämmelserna överlappar dessutom varandra och ska tillämpas parallellt, inte sällan av offentliganställda utan specialkunskaper i något av rättsområdena. De var för sig komplexa, och dessutom parallellt tillämpliga, regelverken som rör informationsutbytet mellan myndigheter bör enligt vår mening i så hög utsträckning som möjligt vara fria från upplevda normkonflikter och otydligheter som ytterligare komplicerar både tillämpningen och enskildas möjlighet att förstå hur uppgifter om dem behandlas. Att en behandling av uppgifter genom utlämnande till andra myndigheter är tillåten enligt ett av regelverken, samtidigt som den till synes är förbjuden enligt det andra, är alltså något som enligt vår bedömning inte bör förekomma.[108]

[107] Jfr IMY, *Integritet och ny teknik 2020–2024 – Redovisning av Integritetsskyddsmyndighetens uppdrag att följa, analysera och beskriva utvecklingen*, dnr IMY-2024-2570, s. 11 och prop. 2017/18:105, *Ny dataskyddslag*, s. 23.
[108] Jfr dir. 2011:86, *Integritet, effektivitet och öppenhet i en modern e-förvaltning*, s. 3 och 22.

Eftersom undantag från de generella bestämmelserna i offentlighets- och sekretesslagen enbart kan göras i den lagen, direkt eller genom hänvisning till annan författning, ger uttömmande ändamålsbestämmelser och ändamålsbestämmelser som på annat sätt kan uppfattas hindra utlämnande dessutom en felaktig eller i vart fall vilseledande, bild av den personuppgiftsbehandling genom utlämnande till myndigheter som är tillåten i svensk rätt. Ändamålsbestämmelser som till synes utesluter utlämnande av uppgifter med stöd av offentlighets- och sekretesslagen kan alltså medföra en generell risk för att inget av regelverken tillämpas på så sätt som avsetts. En sådan regleringsmodell medför dessutom oklarheter och därmed även tillämpningssvårigheter. I fortsättningen bör den kompletterande dataskyddsregleringen därför inte innehålla bestämmelser som kan uppfattas begränsa myndigheters möjlighet att utbyta uppgifter i enlighet med bestämmelserna i offentlighets- och sekretesslagen.

Det finns inte skäl att göra en dataskyddsrättslig åtskillnad mellan ska och får

I kompletterande dataskyddsreglering förekommer ändamålsbestämmelser som medger utlämnande av uppgifter enbart om det i lag eller förordning finns *en skyldighet* att göra det (jfr exemplet i avsnitt 5.4.3). En sådan lagstiftning innebär inte lika stora konflikter mellan dataskyddsreglering och offentlighets- och sekretesslagen som när helt uttömmande ändamål till synes inte tillåter någon vidarebehandling genom utlämnande. Regleringen kan dock uppfattas som ett förbud mot att på *eget initiativ* lämna ut uppgifter som träffas av en sekretessbrytande bestämmelse i offentlighets- och sekretesslagen.

I avsnitt 4.7 har vi redogjort för det stora kartlagda behovet av att kunna lämna ut uppgifter på eget initiativ. I avsnitt 4.8.4 har vi redogjort för vår uppfattning om skillnaderna mellan att lämna ut uppgifter på eget initiativ och skyldigheten enligt 6 kap. 5 § OSL att efter en begäran från mottagaren lämna ut uppgifter. I det sammanhanget har vi även konstaterat att det rent lagtekniskt i många fall är nödvändigt att utforma en bestämmelse om informationsutbyte som en skyldighet att lämna ut uppgifter, antingen efter begäran eller på eget initiativ, eftersom det enligt 10 kap. 28 § första stycket OSL endast är uppgifts*skyldigheter* i annan författning som bryter sekretess. Det gäller dock inte för sekretessbrytande bestämmelser

som tas in direkt i offentlighets- och sekretesslagen, där det ”räcker” med att sekretess inte hindrar utlämnandet. Bestämmelser om uppgiftsskyldighet mellan myndigheter är dessutom ett sätt för lagstiftaren att lagtekniskt reglera ett ofta förekommande informationsutbyte och att tillförsäkra en verksamhet de uppgifter som behövs i den mottagande myndighetens verksamhet. Det bör i många fall vara dessa förhållanden, snarare än integritetsintresset, som har varit avgörande för om ett informationsutbyte reglerats som en skyldighet eller som en möjlighet för den utlämnande myndigheten.

Vad gäller vissa sekretessbrytande bestämmelser i 10 kap. OSL som rör uppgiftslämnande vid misstanke om begånget brott förefaller det dock vara så att uppgifterna placerats i just offentlighets- och sekretesslagen för att undvika att myndigheter ålades en skyldighet att lämna ut uppgifter om brott. Syftet var dock inte att myndigheterna skulle förhålla sig passiva när det uppkom misstankar om brott. Tvärtom uttalades det i förarbetena vara önskvärt att myndigheterna utnyttjade möjligheterna att lämna ut uppgifter om brott.[109]

Om en sekretessbrytande bestämmelse har utformats som en *möjlighet* eller en *skyldighet* att lämna ut uppgifter bör under alla förhållanden inte alltid ses som ett resultat av och uttryck för lagstiftarens avvägning mellan intresset av att upprätthålla skyddet för enskildas personliga integritet och andra intressen, utan snarare en lagteknisk konsekvens av bestämmelsens placering och syfte. Lagstiftarens avvägning mellan integritetsintresset och andra intressen bör i stället anses komma till uttryck huvudsakligen genom de rekvisit som anger under vilka omständigheter det ska råda ett förbud mot att röja en uppgift (sekretess) och under vilka omständigheter det får göras undantag från ett sådant förbud (sekretessgenombrott eller undantag från sekretess).

Vår bedömning är därför att det inte finns skäl för att göra någon dataskyddsrättslig åtskillnad mellan bestämmelser som innebär att uppgifter *får* lämnas ut utan hinder av sekretess och bestämmelser som innebär att uppgifter *ska* lämnas ut, dvs. mellan olika situationer där bestämmelserna i offentlighets- och sekretesslagen medför att ett utlämnande är tillåtet. Det är också en konsekvens av att förbud att röja en uppgift enbart regleras i offentlighets- och sekretesslagen.

[109] Jfr prop. 1983/84:142, *om ändringar i sekretesslagen (1980:100), m.m.*, s. 23–28 och 34–40.

Tillåtligheten av personuppgiftsbehandling i enlighet med offentlighets- och sekretesslagens bestämmelser ska tydliggöras genom en upplysningsbestämmelse

Vi har nyss bedömt att reglering som medför att en behandling av uppgifter genom utlämnande till andra myndigheter är tillåten enligt ett tillämpligt regelverk, samtidigt som den till synes är förbjuden enligt ett annat tillämpligt regelverk inte bör förekomma. Eftersom offentlighets- och sekretesslagen är den författning som anger både när det råder förbud mot att röja en uppgift och när det inte gör det, bör den kompletterande dataskyddsregleringen ändras i de fall avvikande bestämmelser förekommer där. Frågan är då hur denna ändring ska genomföras för att vara ändamålsenlig.

Som vi nämnt i avsnitt 5.4.1 är ändamålsbestämmelser uttömmande om orden *endast* eller *bara* förekommer i den aktuella paragrafen. En möjlig lösning i dessa fall skulle därför vara att helt enkelt föreslå att de orden utgår där de förekommer i kompletterande dataskyddsreglering. Risken är dock att osäkerheten om förhållandet mellan dataskyddsbestämmelser och offentlighets- och sekretesslagen kvarstår med en sådan förändring. Det går inte heller att bortse från risken att ändamålsbestämmelserna även i fortsättningen kan uppfattas vara uttömmande, eftersom inget annat sägs uttryckligen. Att även ändamålsbestämmelser som inte är uttömmande formulerade också kan uppfattas hindra uppgiftslämnande talar för det. Det förekommer också att de uttömmande ändamålsbestämmelserna har betydelse för tillåtligheten av vidarebehandling *inom* en myndighet, som vi gett ett exempel på i avsnitt 5.4.3.

I sammanhanget kan också nämnas att IMY har uttalat att även om utgångspunkten är att utlämnande av uppgifter mellan myndigheter regleras i sekretesslagstiftningen, kan det behövas reglering i registerförfattningar som *tydliggör* [vår kursivering] vilket uppgiftslämnande som är tillåtet för att den rättsliga grunden ska bli förutsebar. En sådan reglering bör dock enligt IMY inte innebära att det uppkommer konflikter med sekretessregleringen, t.ex. genom att utlämnanden som är tillåtna enligt sekretessregleringen inte är tillåtna enligt registerförfattningen.[110]

[110] IMY:s yttrande, *eSam:s promemoria En modern registerförfattning (ES 2022:6)*, dnr IMY-2022-1665, s. 7.

Vi bedömer sammantaget att tillåtligheten av uppgiftslämnande med stöd av offentlighets- och sekretesslagens bestämmelser bör komma till uttryck i en faktisk bestämmelse.

I avsnitt 3.2.2 har vi redogjort för vanligt förekommande bestämmelser i kompletterande dataskyddsreglering som anger att uppgiftslämnande i överensstämmelse med lag eller förordning är tillåten. I motiven till bestämmelserna har regeringen i dessa fall hänvisat till ett och samma förhållande, dvs. att när bestämmelser som reglerar informationsutbyte mellan myndigheter har införts får det förutsättas att det gjorts en avvägning mellan intresset av att uppgiften lämnas ut och intresset av att skydda enskilda personers integritet, vid vilken man funnit att uppgiften ska eller får lämnas ut. Motsvarande reglering, med liknande motivering, förekommer i ett flertal andra kompletterande dataskyddsförfattningar än de som exemplifieras i avsnitt 3.2.2. Det är också den form av reglering som förkommer i förslag om ny kompletterande dataskyddsreglering och i författningar som vi uteslutit från vår översyn eftersom de inte innehåller några hinder mot utlämnande, vilket vi redogjort för i avsnitt 5.3.2.

För att åstadkomma en enklare, mer enhetlig och mer lättillämpad reglering av myndigheters informationsutbyte föreslår vi att det även i de författningar som omfattas av vår översyn införs en upplysningsbestämmelse med innebörden att personuppgifter får behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning. En sådan bestämmelse betecknas i regel som en sekundär ändamålsbestämmelse.

I vissa fall finns det skäl för att anpassa bestämmelsens lydelse till den aktuella författningen, utan någon förändring i sak. I faktiska registerförfattningar framstår det t.ex. som lämpligast att ange att uppgifter som behandlas i ett särskilt register även får behandlas för uppgiftslämnande. I informationshanteringsförfattningar är det i stället lämpligast att hänvisa till uppgifter som behandlas enligt de primära ändamålen. I något fall kan det vidare vara lämpligast att upplysa om att uppgifter kan lämnas ut med stöd av offentlighets- och sekretesslagen (jfr avsnitt 5.4.7).

Genom införandet av dessa upplysningsbestämmelser, som alla har samma innebörd, uppnås en formell överensstämmelse mellan bestämmelser i den kompletterande dataskyddsregleringen och offentlighets- och sekretesslagen. Det bör i sin tur innebära att de förslag vi lämnat kan tjäna sitt syfte och tillämpas på ett ändamålsenligt sätt.

En bestämmelse som tydliggör att personuppgifter får behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning bidrar dessutom till ökad transparens för de registrerade vars uppgifter behandlas. Bestämmelse kan därmed ses som en integritetshöjande åtgärd i förhållande till dataskyddsförordningen. Även om bestämmelsen inte har någon sekretessbrytande verkan så kan den alltså bidra till ökad förutsebarhet i frågan om hur uppgifter om enskilda registrerade får behandlas.

Är det verkligen bara en upplysningsbestämmelse?

Som vi påpekat tidigare kan särskilt uttömmande ändamålsbestämmelser ha uppfattats utgöra ett hinder mot sådant uppgiftsutbyte mellan myndigheter som är föreskrivet i offentlighets- och sekretesslagen. Vi har även påpekat att om ändamålsbestämmelser skulle tillskrivas den betydelsen så skulle de utgöra de facto sekretessbestämmelser, som enbart är giltiga mellan myndigheter. Det skulle omkullkasta den ordning som offentlighets- och sekretesslagen bygger på, vilket vi inte funnit något stöd för att lagstiftaren avsett att göra. I svensk rätt regleras alltså förbud att röja en uppgift (sekretess) inte genom någon annan författning än offentlighets- och sekretesslagen, antingen direkt eller genom hänvisning till annan författning. Det förhållandet ändras inte av att den kompletterande dataskyddsregleringen inte har setts över, utvärderats och uppdaterats i takt med den tekniska och rättsliga utvecklingen. Det förhållandet ändras inte heller av att den kompletterande dataskyddsregleringen har fått en utökad tillämplighet genom den tekniska och rättsliga utvecklingen eller någon annan omständighet (jfr avsnitt 5.2.4).

Som vi nämnt tidigare har regeringen i dataskyddslagens förarbeten uttalat att dataskyddsförordningens krav på att den rättsliga grunden för myndigheters personuppgiftsbehandling ska vara fastställd (artikel 6.3) inte innebär ett krav på att själva behandlingen av personuppgifter måste regleras. Det är i stället den rättsliga förpliktelsen, uppgiften av allmänt intresse respektive myndighetsutövningen som ska ha stöd i rättsordningen. Den rättsliga förpliktelsen, uppgiften av allmänt intresse respektive myndighetsutövningen är enligt regeringen fastställd i enlighet med svensk rätt, om den följer av författning eller

beslut som har meddelats i enlighet med regeringsformens bestämmelser.[111] Detta framgår även av kapitel 2 i dataskyddslagen.

I regel utgör alltså inte ändamålsbestämmelser i den kompletterande dataskyddsregleringen *i sig* den rättsliga grunden för den personuppgiftsbehandling som kan aktualiseras inom tillämpningsområdet, förutom i vissa faktiska registerförfattningar (se avsnitt 5.2.1). Det är i stället bestämmelserna i den materiella och processuella regleringen av verksamheten som utgör rättsliga grunder för personuppgiftsbehandling.

Även författningsreglerade uppgiftsskyldigheter och sekretessbrytande bestämmelser i offentlighets- och sekretesslagen utgör rättsliga grunder för personuppgiftsbehandling. De kan utgöra en rättslig förpliktelse i enlighet med artikel 6.1 c i dataskyddsförordningen (när uppgifter ska lämnas ut) eller en uppgift av allmänt intresse i enlighet med artikel 6.1 e (när uppgifter får lämnas ut).

En bestämmelse i kompletterande dataskyddsreglering som anger att uppgifter får behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning kommer följaktligen inte *i sig* utgöra den rättsliga grunden i dataskyddsförordningens mening för uppgiftsutbytet. Den rättsliga grunden för behandling genom utlämnande utgörs i stället av de bestämmelser som tillåter eller kräver att uppgifter lämnas ut, t.ex. 6 kap. 5 §, 10 kap. 27 § eller den i SOU 2024:63 föreslagna 10 kap. 15 a § OSL. Även sådant utlämnande till enskilda som följer av offentlighetsprincipen omfattas av bestämmelsen.

De föreslagna bestämmelserna har därför ingen självständig rättslig betydelse, utan upplyser om att uppgifter även kan komma att behandlas vid utlämnande i överensstämmelse med lag eller förordning. Bestämmelserna tydliggör också att uppgifter kan komma att behandlas för ändamål som ligger utanför den verksamhet som omfattas av respektive kompletterande dataskyddsreglerings tillämpningsområde. De föreslagna bestämmelserna är dock inte avgörande för behandlingens laglighet. Prövningen av behandlingens laglighet görs i stället genom en prövning enligt offentlighets- och sekretesslagens bestämmelser, och med tillämpning av de grundläggande dataskyddsrättsliga principerna för behandling, som bl.a. principen om uppgiftsminimering som framgår av artikel 5.1 c i dataskyddsförordningen (jfr HFD 2021 ref. 10).

[111] Prop. 2017/18:105, *Ny dataskyddslag*, s. 48.

5.4.7 Ramen för vårt uppdrag – följdändringar

Vår bedömning: Det faller utanför ramen för vårt uppdrag att överväga eventuella behov av förändringar av offentlighets- och sekretesslagen som kan vara påkallade av våra förslag om förändringar av den kompletterande dataskyddsregleringen.

Skälen för vår bedömning

Följdändringar?

Trots det som sagts i avsnitt 5.4.5 verkar lagstiftarens syfte med att införa ändamålsbestämmelser i den kompletterande dataskyddsregleringen i vissa fall ha varit att hindra informationsutbyte med andra myndigheter med stöd av generellt tillämpliga bestämmelser, utan att det reglerats genom undantag i offentlighets- och sekretesslagen. De sakliga skälen bakom att införa sådan reglering kan väga mycket tungt och begränsningarna kan vara avgörande för att lagstiftningen på området har bedömts vara proportionerlig. Det kan därför finnas skäl för att överväga om sekretessregleringen (och eventuellt även den kompletterande dataskyddsregleringen) på dessa områden ska förändras, för att tillgodose de intressen som legat till grund för ändamålsbestämmelserna i den kompletterande dataskyddsregleringen. Det kan också finnas skäl att överväga om det bör införas hänvisningar till lagstiftning som innehåller generellt tillämpliga användningsbegränsningar, som alla svenska myndigheter har att iaktta, i kapitel 9 i offentlighets- och sekretesslagen.

I detta avsnitt redogör vi för några sammanhang där det som sagts ovan aktualiseras. Det är dock viktigt att understryka att det som sägs i detta avsnitt inte gör anspråk på att vara heltäckande. Vid en närmare analys kan det alltså i fler sammanhang än de som anges nedan finnas skäl att överväga om den befintliga sekretessregleringen bör förenas med undantag från generellt tillämpliga bestämmelser i offentlighets- och sekretesslagen, eller hänvisningar till annan författning.

Frågan är då om det ingår i vårt uppdrag att överväga de förändringar av sekretessregleringen och/eller hänvisningar till annan författning som eventuellt kan vara påkallade med anledning av att den kompletterande dataskyddsregleringen ändras i enlighet med vårt förslag.

Lagen (2014:400) om Polismyndighetens elimineringsdatabas

Personer vilkas dna riskerar att kontaminera material eller prover som ska bli föremål för dna-analys är skyldiga att lämna prov för dna enligt 8–9 §§ lagen om Polismyndighetens elimineringsdatabas. I förarbetena till lagen konstateras att enligt 2 kap. 6 § första stycket regeringsformen, RF, är varje medborgare gentemot det allmänna skyddad mot påtvingat kroppsligt ingrepp. Detta skydd får endast begränsas i lag. En skyldighet att lämna dna-prov har ansetts som ett sådant påtvingat kroppsligt ingrepp som omfattas av skyddet enligt 2 kap. 6 § första stycket RF. Även om ett kroppsligt ingrepp som tagande av ett dna-prov sker utan fysiskt tvång är det att betrakta som påtvingat, om det finns ett krav på att den enskilde ska lämna provet och kravet är förenat med ett hot om sanktioner. Offentligt anställda omfattas av skyddet mot påtvingat kroppsligt ingrepp i förhållande till sin arbetsgivare.[112]

Uppgifter i elimineringsdatabasen får enligt 1 § andra stycket lagen om Polismyndighetens elimineringsdatabas *endast* behandlas för att upptäcka och utreda kontamineringar vid dna-analyser och hanteringen av dna-spår. I lagkommentaren anges att detta innebär att uppgifter i databasen aldrig får användas för att utreda brott.[113] Det finns även en mycket begränsande reglering av vem som får ha tillgång till elimineringsdatabasen i 5 § förordningen (2014:405) om Polismyndighetens elimineringsdatabas.

För uppgifterna i databasen gäller sekretess med ett omvänt skaderekvisit, dvs. med en presumtion för sekretess, enligt 35 kap. 19 a § OSL. Uppgifter som efter en skadeprövning inte träffas av sekretessen är dock inte sekretessbelagda och måste därför som utgångspunkt lämnas ut till den myndighet som begär det, oavsett vilken myndighet det rör sig om och oavsett i vilket syfte uppgifterna begärs ut (6 kap. 5 § OSL, jfr avsnitt 4.8.4).

Sekretess enligt 35 kap. 19 a § OSL är vidare inte undantagen tillämpningsområdet för bestämmelserna i 10 kap. OSL, dvs. inte heller generalklausulens tillämpningsområde. Det innebär att sekretessen för uppgifter i elimineringsdatabasen bryts i förhållande till myndigheter i flera olika sammanhang, och även kommer att brytas av den generella sekretessbrytande bestämmelse som vi före-

[112] Prop. 2013/14:110, *En ny organisation för polisen*, s. 456.
[113] Prop. 2013/14:110, *En ny organisation för polisen*, s. 539.

slagit ska införas som en ny 10 kap. 15 a § OSL. Bestämmelserna i offentlighets- och sekretesslagen medför alltså att uppgifter i elimineringsdatabasen får lämnas ut bl.a. för att utreda brott.

I nuläget kan den uttömmande ändamålsregleringen uppfattas uppställa ett hinder mot utlämnande till andra myndigheter med stöd av bestämmelser i offentlighets- och sekretesslagen. Mot bakgrund av förarbetsuttalandena förefaller det också vara ett av syftena med bestämmelsen. Om det däremot införs en bestämmelse i lagen om Polismyndighetens elimineringsdatabas, som anger att uppgifter som behandlas med stöd av lagen även får behandlas för att fullgöra uppgiftslämnande i överensstämmelse med lag eller förordning, bör det inte kunna uppfattas föreligga ett hinder mot utlämnande i överensstämmelse med offentlighets- och sekretesslagens bestämmelser.

Det kan dock finnas starka skäl att i sak behålla de begränsningar av möjligheterna till utlämnande till andra myndigheter som i dag enbart följer av lagen om Polismyndighetens elimineringsdatabas, men inte av offentlighets- och sekretesslagen. En sådan begränsning kan framstå som befogad bl.a. mot bakgrund av skyldigheten att lämna prov, den inneboende integritetskänsligheten i dna-material och riskerna med spridning av sådant material. Grundlagskravet på att inskränkningar av grundläggande rättigheter aldrig får gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den talar också för detta (jfr 2 kap. 20 och 21 §§ RF). Samma skäl som motiverat den uttömmande ändamålsregleringen kan alltså motivera en förändring av sekretessbestämmelserna för Polismyndighetens elimineringsdatabas. Detta kan t.ex. ske genom att i anslutning till 35 kap. 19 a § OSL införa ett undantag från tillämpligheten av bestämmelserna i 10 kap. OSL för uppgifter som är sekretessbelagda med stöd av bestämmelsen. Det kan även behöva övervägas om sekretessen i verksamheten bör vara absolut.

Lagen (2020:422) om Rättsmedicinalverkets elimineringsdatabas

Regleringen i lagen om Rättsmedicinalverkets elimineringsdatabas motsvarar i allt väsentligt den reglering som finns i lagen om Polismyndighetens elimineringsdatabas. Samma överväganden som motiverat den uttömmande ändamålsbestämmelsen vid Polismyndigheten har även motiverat en sådan bestämmelse vid Rättsmedicinalverket

(jfr 1 kap. 1 § andra stycket lagen om Rättsmedicinalverkets elimineringsdatabas).[114]

För uppgifterna i Rättsmedicinalverkets databas gäller dock sekretess enligt 25 kap. 1 § OSL (hälso- och sjukvårdssekretessen) som både är undantagen generalklausulens tillämpningsområde och tilllämpningsområdet för den generella sekretessbrytande bestämmelse som vi föreslagit (10 kap. 15 a § OSL). Övriga generella bestämmelser i 10 kap. OSL bryter dock sekretess enligt 25 kap. 1 § OSL. Det innebär att sekretessen bryts i förhållande till myndigheter i flera olika sammanhang, bl.a. med stöd av 10 kap. 23 § OSL som gäller vid misstanke om vissa begångna brott. I dag kan dock den uttömmande ändamålsregeringen uppfattas uppställa ett hinder mot utlämnande till andra myndigheter med stöd av (vissa) generella bestämmelser i offentlighets- och sekretesslagen.

Om det införs en bestämmelse i lagen om Rättsmedicinalverkets elimineringsdatabas, som anger att uppgifter som behandlas med stöd av lagen även får behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning, skulle det inte finnas några sådana uppfattade hinder. Samma skäl att behålla begränsningar av möjligheten till vidarebehandling genom utlämnande till myndigheter som redovisas i stycket ovan, om Polismyndighetens elimineringsdatabas, är därför giltiga även här och samma lösning som anges ovan skulle kunna användas i detta sammanhang.

Lag (2018:1180) om flygpassageraruppgifter i brottsbekämpningen

Lagen om flygpassageraruppgifter i brottsbekämpningen genomför direktiv EU 2016/68 om användning av passageraruppgiftssamlingar (PNR-uppgifter) för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och annan allvarlig brottslighet.

Lagen utgör i och för sig inte någon renodlad dataskyddsreglering och kompletterar inte heller uttryckligen bestämmelserna i brottsdatalagen. Däremot har lagen samma syfte som kompletterande dataskyddsreglering generellt sett har, dvs. att tillgodose behovet av vissa uppgifter i viss verksamhet och att skydda människor mot att deras personliga integritet kränks vid behandling av uppgifter om dem (jfr 1 kap. 2 § lagen om flygpassageraruppgifter i brottsbekämp-

[114] Prop. 2019/20:106, *Stärkt integritet i Rättsmedicinalverkets verksamhet*, s. 68–70.

ningen). Lagen innehåller dessutom vissa ändamålsbestämmelser. Vi har därför inkluderat lagen i vår översyn.

I 1 kap. 5 § lagen om flygpassageraruppgifter i brottsbekämpningen finns portalparagrafen om behandling av s.k. PNR-information. Genom bestämmelsen genomförs artiklarna 1.2 och 7.4 samt delvis artiklarna 9.2 och 10.2 i PNR-direktivet.[115] Bestämmelsen är inte en ändamålsbestämmelse utan av samma karaktär som andra användningsbegränsningar som följer av internationell rätt (jfr avsnitten 5.4.1 och 5.4.4). I paragrafen anges att PNR-information *endast* får behandlas i syfte att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller annan allvarlig brottslighet (med vissa undantag). PNR-uppgifterna får enligt lagen också behandlas när det är nödvändigt för att tillhandahålla uppgifter som behövs för verksamhet som rör nationell säkerhet enligt 1 kap. 6 § och för behandling för annan brottslighet hos behöriga myndigheter enligt 5 kap. 3 §. Därutöver finns uttömmande ändamålsbestämmelser i 3 kap. 4 § samma lag, som avser behandling av uppgifter vid den s.k. enheten för passagerarinformation.

För PNR-uppgifter gäller sekretess enligt 18 kap. 1–2 §§ OSL (allmänna intressen) och enligt 35 kap. 1 § 4 OSL (enskilda) med ett omvänt skaderekvisit. I förarbetena uttalas att enligt regeringens mening gav det omvända skaderekvisitet i 35 kap. 1 § OSL, med en presumtion för sekretess, ett tillräckligt starkt skydd för uppgifterna. Någon ny eller förändrad sekretessreglering behövdes därför inte.[116] I förarbetena uttalades vidare att de begränsningar som skulle gälla för behandling av PNR-information får till följd att en myndighet inte kan utnyttja uppgifterna i sin verksamhet i andra fall än vad som anges i lagens bestämmelser. Det innebar enligt regeringen att sekretessbrytande regler i praktiken enbart borde bli aktuella att åberopa när en myndighet har rätt att ta del av uppgifterna för sådana ändamål som anges i lagen.[117] I förarbetena uttalades även att de uttömmande ändamålsbestämmelserna som skulle gälla för enheten för passagerarinformation skulle utesluta en tillämpning av 2 kap. 4 § BDL om nya ändamål (se avsnitt 5.5 om brottsdatalagen).[118]

[115] Prop. 2017/18:234, *Lag om flygpassageraruppgifter i brottsbekämpningen*, s. 140.
[116] Prop. 2017/18:234, *Lag om flygpassageraruppgifter i brottsbekämpningen*, s. 128 och 129.
[117] Prop. 2017/18:234, *Lag om flygpassageraruppgifter i brottsbekämpningen*, s. 129.
[118] Prop. 2017/18:234, *Lag om flygpassageraruppgifter i brottsbekämpningen*, s. 66 och 67.

Regeringens ovan relaterade uttalanden motsvarar de uttalanden som gjorts i förarbetena till 9 kap. 2 § OSL och som återges i avsnitt 5.4.4. Det görs dock ingen hänvisning till de användningsbegränsningar som följer av lagen om flygpassageraruppgifter i brottsbekämpningen i kapitel 9 i offentlighets- och sekretesslagen. Det görs heller inga undantag från tillämpligheten av bestämmelserna i t.ex. 10 kap. OSL för uppgifter som skyddas av sekretess enligt 35 kap. 1 § 4 OSL. Det innebär att det enligt offentlighets- och sekretesslagens bestämmelser är tillåtet att utbyta PNR-uppgifter i andra syften än de som framgår av lagen om flygpassageraruppgifter i brottsbekämpningen, och att lagens användningsbegränsningar inte framgår av offentlighets- och sekretesslagen.

Användningsbegränsningarna i lagen om flygpassageraruppgifter i brottsbekämpningen är emellertid en följd av ett EU-direktiv och har en generell tillämplighet.[119] Som regeringen konstaterade i förarbetena innebär det att sekretessbrytande regler i praktiken enbart bör bli aktuella att åberopa när en myndighet har rätt att ta del av uppgifterna för sådana ändamål som anges i lagen. Detta bör även gälla vid en begäran om att få del av uppgifter som inte är sekretessbelagda med stöd av 6 kap. 5 § OSL.[120]

Användningsbegränsningar av den karaktär som finns i lagen om flygpassageraruppgifter i brottsbekämpningen gäller alltså alldeles oavsett vad som framgår av offentlighets- och sekretesslagen om svenska myndigheters möjlighet att utbyta uppgifter. Det är därmed inte nödvändigt att det görs en hänvisning i offentlighets- och sekretesslagen för att en sådan användningsbegränsning ska gälla. För att regleringen ska vara så enhetlig som möjligt, och för att principen om att alla tystnadsplikter i det allmännas verksamhet ska upprätthållas, bör det dock vara lämpligt att införa sådana hänvisningar när det är aktuellt. Det är också ett av skälen bakom den befintliga regleringen i 9 kap. 2 § OSL (jfr avsnitt 5.4.4).

Vårt uppdrag i den här delen är emellertid inte att lämna förslag om förändringar av offentlighets- och sekretesslagen. Som vi noterat i avsnitt 5.4.1 bör dessutom användningsbegränsningar som följer av t.ex. ett EU-direktiv inte utgöra något hinder mot tillämpningen av bestämmelserna i offentlighets- och sekretesslagen vid utlämnande

[119] Se om PNR-direktivet i EDPB, *Statement 2/2025 on the implementation of the PNR Directive in light of CJEU Judgment C-817/19 Adopted on 13 March 2025*.
[120] Jfr SOU 2015:39, *Myndighetsdatalag*, s. 154–157.

som sker som ett led i ett tillåtet användningsområde. Vi har därför föreslagit att det ska införas en upplysingsbestämmelse även i lagen om flygpassageraruppgifter i brottsbekämpningen. Upplysningsbestämmelsen har dock anpassats efter den befintliga regleringen på så sätt att det inte anges att uppgifter får behandlas för utlämnande i överensstämmelse med lag eller förordning, som i övriga författningar. I stället har vi föreslagit att bestämmelsen ska lyda *att PNR-information får lämnas ut i vissa fall framgår av offentlighets- och sekretesslagen*.

Av samma skäl som motiverat den befintliga regleringen i 9 kap. 2 § OSL borde det dock även finnas skäl för att i det kapitlet även införa en hänvisning till användningsbegränsningarna i lagen om flygpassageraruppgifter i brottsbekämpningen. PNR-uppgifter erhålls dock inte från utländska myndigheter, utan från s.k. lufttrafikföretag. Hänvisningen till lagen om flygpassageraruppgifter i brottsbekämpningen kan därför inte införas i den befintliga 9 kap. 2 § OSL, som enbart avser uppgifter som en svensk myndighet har fått från en myndighet i en annan stat. Hänvisningen till användningsbegränsningarna i lagen om flygpassageraruppgifter i brottsbekämpningen borde dock kunna införas som en ny 9 kap. 4 § OSL. På så sätt upprätthålls systematiken i offentlighets- och sekretesslagen.

Lagen (2013:1164) om elektroniska vägtullssystem

I likhet med lagen om flygpassageraruppgifter i brottsbekämpningen genomför lagen om elektroniska vägtullssystem ett EU-direktiv i svensk rätt, EU 2019/520 av den 19 mars 2019 om driftskompatibilitet mellan elektroniska vägtullssystem och underlättande av gränsöverskridande informationsutbyte om underlåtenhet att betala vägavgifter i unionen.

Lagen om elektroniska vägtullssystem utgör inte någon renodlad dataskyddsreglering men innehåller vissa bestämmelser om behandling av personuppgifter (31–32 a §§).

Av 27–28 §§ lagen om elektroniska vägtullssystem följer att den svenska myndighet som är s.k. kontaktpunkt får utbyta vissa uppgifter med utländska kontaktpunkter.

I 32 § samma lag anges att personuppgifter som har erhållits enligt 28 § endast får behandlas för att identifiera ett fordon eller en ägare eller innehavare av ett fordon i syfte att ta upp eller driva in vägtullar. Paragrafen reglerar alltså hur uppgifter som den svenska myndigheten har erhållit från ett annat land får användas.[121] Den genomför direktivets bestämmelser om att personuppgifter som har erhållits genom förfarandet för informationsutbyte med ett annat land bara får behandlas i syfte att ta ut eller driva in vägtullar.[122]

I lagens förarbeten konstaterade regeringen att 27 kap. 1 § OSL och 29 kap. 5 a § OSL, som innebär absolut sekretess, gäller för verksamheten.[123] Även absolut sekretess bryts dock i förhållande till andra myndigheter av bestämmelserna i offentlighets- och sekretesslagen och av särskilt reglerade uppgiftsskyldigheter. Precis som anges i föregående stycke innebär det att offentlighets- och sekretesslagens bestämmelser medger informationsutbyte för andra ändamål än för att identifiera ett fordon eller en ägare eller innehavare av ett fordon i syfte att ta upp eller driva in vägtullar.

Såvitt vi kunnat se har regeringen inte i förarbetena till lagen om elektroniska vägtullssystem gjort några överväganden om att användningsbegränsningarna som följer av direktivet, och som framgår av 32 § den lagen, har sådana konsekvenser för tillämpningen av bestämmelserna i offentlighets- och sekretesslagen som ofta uppmärksammas i andra förarbeten där användningsbegränsningar förekommer (se avsnitt 5.4.4). Mot bakgrund av bestämmelserna i direktivet som anger för vilka syften uppgifter får behandlas (jfr t.ex. artikel 27 i direktivet) bör dock användningsbegränsningarna som framgår av lagen om elektroniska vägtullssystem ha samma innebörd som övriga användningsbegränsningar som kan aktualiseras inom EU-rätten när information utbyts mellan medlemsstaterna. Det som sägs ovan i stycket om lagen om flygpassageraruppgifter i brottsbekämpningen är därför giltigt även här. Den upplysningsbestämmelse som vi föreslår ska införas i lagen om elektroniska vägtullssystem är därför utformad på samma sätt som den bestämmelse som vi föreslår ska införas i lagen om flygpassageraruppgifter i brottsbekämpningen.

[121] Prop. 2023/24:113, *Rätt till uppgifter om en EETS-betalningsförmedlares kunder och deras fordon*, s. 19.
[122] Prop. 2021/22:118, *Genomförande av direktivet om elektroniska vägtullssystem*, s. 58.
[123] Prop. 2021/22:118, *Genomförande av direktivet om elektroniska vägtullssystem*, s. 53.

På samma sätt som för lagen om flygpassageraruppgifter i brottsbekämpningen kan det alltså finnas ett behov av att införa en hänvisning i offentlighets- och sekretesslagen för att upprätthålla lagens systematik. Eftersom de uppgifter som avses i lagen om elektroniska vägtullssystem erhålls från en utländsk myndighet bör en eventuell hänvisning kunna införas i 9 kap. 2 § OSL.

Några övriga sammanhang där behovet av följdändringar kan behöva övervägas

Utöver de tydliga exempel som vi redogjort för ovan har vi även funnit vissa andra sammanhang där det kan finnas skäl att överväga behovet av ändringar i offentlighets- och sekretesslagen. I de författningar som anges nedan är dock inte vare sig regleringen som sådan eller de förarbetsuttalanden som vi funnit lika tydliga. I många fall omfattar regleringen dessutom otydligheter. Det kan t.ex. vara att det görs en omotiverad dataskyddsrättlig åtskillnad mellan sekretessbrytande bestämmelser utifrån hur de lagtekniskt är utformade eller att tystnadsplikten på området anges motsvara vad som följer av offentlighets- och sekretesslagen (jfr avsnitt 5.4.3).

Det kan dock finnas andra omständigheter som medför att det kan behöva övervägas om sekretesskyddet i förhållande till andra myndigheter ska stärkas, eller om det bör införas hänvisningar till annan lagstiftning i offentlighets- och sekretesslagen. Det kan t.ex. röra sig om att de uppgifter som behandlas är särskilt känsliga, inte får behandlas för vissa ändamål enligt EU-rätten, eller rör uppgifter om barn.

- Lagen (2006:444) om passagerarregister
- Lagen (2006:496) om blodsäkerhet
- Lagen (2008:286) om kvalitets- och säkerhetsnormer vid hantering av mänskliga vävnader och celler
- Lagen (2011:725) om behörighet för lokförare
- Lagen (2016:1306) med kompletterande bestämmelser till EU:s marknadsmissbruksförordning

- Lagen (2019:508) om behandling av personuppgifter i det fördelningsanalytiska statistiksystemet för inkomster och transfereringar
- Biobankslagen (2023:38)

Att överväga följdändringar faller inte inom ramen för vårt uppdrag

Vårt uppdrag i denna del är begränsat till att göra en översyn av den kompletterande dataskyddsregleringen och att föreslå de ändringar som krävs för att våra förslag om förbättrade möjligheter till informationsutbyte mellan myndigheter kan tjäna sitt syfte och tillämpas på ett ändamålsenligt sätt. I allt lagstiftningsarbete som berör frågor om dataskydd och sekretess måste det emellertid tas hänsyn till hur förslagen påverkar enskildas integritet, oavsett om det tydligt framgår av direktiven eller inte. Vi har också nyss konstaterat att det finns sammanhang där det mot bakgrund av våra förslag om ändringar av den kompletterande dataskyddsregleringen kan vara påkallat att helt eller delvis undanta viss sekretess från tillämpningsområdet för t.ex. bestämmelserna i 10 kap. OSL, eller att införa bestämmelser i offentlighets- och sekretesslagen som hänvisar till användningsbegränsningar eller motsvarande i annan författning.

Utan en närmare analys går det dock inte att slå fast att det i samtliga fall som anges ovan faktiskt förhåller sig så att regleringen på området måste ändras för att tillgodose integritetsintresset, EU-rättsliga krav eller för att upprätthålla principen som offentlighets- och sekretesslagen bygger på. Vi har t.ex. kunnat se att den svenska lagstiftaren i vissa fall infört strängare dataskyddsbestämmelser än vad som krävs enligt EU-rätten (jfr avsnitt 5.5 om brottsdatalagen). I andra fall kan övrig tillämplig dataskyddsreglering, som t.ex. krav på samtycke från enskilda innan en vidarebehandling, bedömas medföra att det finns ett fullgott integritetsskydd trots införandet av ett tydligt rättsligt stöd för utlämnande i överensstämmelse med lag eller förordning. Under alla förhållanden kräver överväganden om förändringar av sekretessregleringen analyser av övrig relevant lagstiftning som inte kan anses falla inom ramen för vårt uppdrag.

Här bör också nämnas att i de fall det görs faktiska undantag från de generella bestämmelserna i offentlighets- och sekretesslagen i anslutning till materiella sekretessbestämmelser krävs det reglering

i annan ordning avseende vilket uppgiftslämnande som trots allt ska få förekomma. Som vi påpekat i avsnitt 5.4.4 finns sådan reglering i dag bl.a. för uppgifter i belastningsregistret (35 kap. 3 § OSL). I förordningen (1999:1134) om belastningsregister finns därför ett stort antal, ofta mycket detaljerade, bestämmelser med innebörden att uppgifter från belastningsregistret ska lämnas till olika aktörer för vissa syften. Vid införandet av nya undantag från 10 kap. OSL kan det därför förväntas krävas en kartläggning – i varje enskilt fall – av vilket befintligt uppgiftsutbyte som behöver regleras i särskild ordning för att fortsatt vara tillåtet. Det kan inte anses falla inom ramen för vårt uppdrag i denna del att genomföra sådana kartläggningar av flera olika myndigheters befintliga informationsutbyte.

Om sekretessen på vissa områden dessutom skulle bedömas behöva vara absolut, för att hindra ett utlämnande av uppgifter som efter en sekretessprövning bedöms inte vara sekretessbelagda och därför kan komma att behöva lämnas ut med stöd av 6 kap. 5 § OSL, krävs dessutom överväganden om enskildas intresse av insyn i verksamheten.

Sammanfattningsvis bedömer vi att det inte faller inom ramen för vårt uppdrag att överväga de förändringar av offentlighets- och sekretesslagens bestämmelser som eventuellt kan vara påkallade av våra förslag i denna del.

5.5 Regleringen av vidarebehandling och utlämnande i brottsdatalagen

5.5.1 Dataskyddsreglering som kompletterar brottsdatalagen

Allmänt

En ramlag

Brottsdatalagen är en ramlag som kompletteras av sektorsspecifik reglering för var och en av de brottsbekämpande myndigheterna. Det finns alltså sektorsspecifik kompletterande dataskyddsreglering för Polismyndigheten, Tullverket, Kustbevakningen, Skatteverket, Åklagarmyndigheten, Kriminalvården och domstolarna. I de författningar som gäller utöver brottsdatalagen finns dock inga särskilda bestämmelser om behandling av personuppgifter för nya ända-

mål. I lagarna hänvisas i stället till 2 kap. 4 och 22 §§ BDL när det gäller frågan om behandling av personuppgifter för nya ändamål.[124]

Bestämmelserna i 2 kap. 4 och 22 §§ BDL tar sikte på all form av personuppgiftsbehandling. Det väsentliga är att behandlingen sker för ett nytt ändamål, oavsett om det sker för ett ändamål som ligger inom eller utanför brottsdatalagens tillämpningsområde. Det innebär att alla ovan nämnda myndigheter ska tillämpa samma bestämmelser vid utlämnande av uppgifter till andra myndigheter och att dessa bestämmelser *i sak* finns i brottsdatalagen och inte i den kompletterande regleringen.

Inom tillämpningsområdet

I 2 kap. 4 § BDL finns bestämmelser som tar sikte på vidarebehandling av personuppgifter för nya ändamål inom brottsdatalagens tillämpningsområde.

Av 2 kap. 4 § första stycket BDL framgår att innan personuppgifter får behandlas för ett nytt ändamål ska det säkerställas att det finns en rättslig grund för den nya behandlingen, och att det är nödvändigt och proportionerligt att personuppgifterna behandlas för det nya ändamålet.

I paragrafens andra stycket anges att i den utsträckning skyldighet att lämna uppgifter följer av lag eller förordning ska någon prövning enligt första stycket inte göras.

Utanför tillämpningsområdet

I 2 kap. 22 § BDL finns bestämmelser som reglerar förutsättningarna för behandling av personuppgifter som behandlas enligt brottsdatalagen utanför brottsdatalagens tillämpningsområde.

[124] Se 2 kap. 2 § lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område, 2 kap. 2 § lagen (2018:1694) om Tullverkets behandling av personuppgifter inom brottsdatalagens område, 2 kap. 2 § lagen (2018:1695) om Kustbevakningens behandling av personuppgifter inom brottsdatalagens område, 2 kap. 2 § lagen (2018:1696) om Skatteverkets behandling av personuppgifter inom brottsdatalagens område, 2 kap. 2 § lagen (2018:1697) om åklagarväsendets behandling av personuppgifter inom brottsdatalagens område, 2 kap. 2 § lagen (2018:1698) om kriminalvårdens behandling av personuppgifter inom brottsdatalagens område och 2 kap. 2 § lagen (2018:1699) om domstolarnas behandling av personuppgifter inom brottsdatalagens område.

Av 2 kap. 22 § första stycket BDL framgår att innan personuppgifter som behandlas med stöd av lagen får behandlas för ett ändamål utanför lagens tillämpningsområde, ska det säkerställas att det är nödvändigt och proportionerligt att personuppgifterna behandlas för det ändamålet.

I paragrafens andra stycket anges att i den utsträckning skyldighet att lämna uppgifter följer av lag eller förordning ska någon prövning enligt första stycket inte göras.

Undantag för uppgiftslämnande som sker med stöd av uppgiftsskyldigheter

Som framgår ovan görs det i brottsdatalagen en rättslig åtskillnad mellan sådan behandling av personuppgifter som föranleds av en *skyldighet* att lämna ut uppgifter och all annan behandling som innebär att uppgifter behandlas för ett nytt ändamål. Kraven på att den tillkommande behandlingens nödvändighet och proportionalitet ska prövas särskilt för att vara tillåten gäller inte när det rör sig om en skyldighet att lämna uppgifter. Däremot måste en sådan prövning göras när det enbart rör sig om en *möjlighet* att lämna uppgifter.

Skälen bakom denna åtskillnad uttalas i förarbetena vara att när det i lag eller förordning föreskrivs att uppgifter ska lämnas ut så har lagstiftaren tagit ställning till att det dels är så viktigt att det ska införas en skyldighet att lämna information, dels att eventuell sekretess ska brytas. Enligt regeringen fick lagstiftaren då också anses ha tagit ställning till att uppgiftslämnandet är nödvändigt och proportionerligt. En uppgiftsskyldighet skulle därför ersätta prövningen av om det är nödvändigt och proportionerligt att personuppgifter behandlas för nya ändamål, oavsett om det gäller ändamål inom eller utanför brottsdatalagens tillämpningsområde. Regeringen ansåg också att en myndighets skyldighet enligt 6 kap. 5 § OSL att på begäran av en annan myndighet lämna ut uppgift som den förfogar över bör omfattas av undantaget för när en prövning av om det är nödvändigt och proportionerligt att personuppgifter behandlas för nya ändamål inte ska göras. I annat fall fanns det enligt regeringen en risk att det uppstår en normkollision mellan 6 kap. 5 § OSL och bestämmelserna i 2 kap. 4 och 22 §§ BDL.[125]

[125] Prop. 2017/18:232, *Brottsdatalag*, s. 138.

Om det i lag eller förordning bara hade föreskrivits en möjlighet, men ingen skyldighet, att lämna uppgifter skulle myndigheten däremot behöva pröva om det är nödvändigt och proportionerligt att lämna ut uppgifter, eftersom lagstiftaren då inte hade gjort den prövningen.[126] I lagkommentaren anges dock att den prövning som ska ske när det bara finns en möjlighet att lämna uppgifter i regel bör mynna ut i att det är nödvändigt och proportionerligt att lämna ut uppgifter.[127]

Även om gränsen inte är lika skarpt dragen i brottsdatalagen som i viss dataskyddsreglering som kompletterar dataskyddsförordningen har alltså lagstiftaren även i detta sammanhang gjort en rättslig åtskillnad mellan olika bestämmelser i offentlighets- och sekretesslagen (jfr avsnitt 5.4.6 om skillnaden mellan *får* och *ska*).

5.5.2 Förändringar av brottsdatalagen

Vårt förslag: I brottsdatalagen ska allt uppgiftsutlämnande som sker i överenstämmelse med lag eller förordning regleras på samma sätt vad gäller vilka prövningar som ska göras inför ett utlämnande.

Skälen för vårt förlag

Skillnaden mellan brottsdatalagen och dataskyddsreglering som kompletterar dataskyddsförordningen

Den befintliga regleringen i 2 kap. 4 och 22 §§ BDL innebär att lagstiftaren gjort en rättslig åtskillnad mellan bestämmelser i offentlighets- och sekretesslagen som innebär att uppgifter *får* lämnas ut till andra myndigheter och bestämmelser som innebär att uppgifter *ska* lämnas ut. Innan uppgifter lämnas ut med stöd av en bestämmelse som innebär att uppgifter *får* lämnas ut måste tillämparen pröva om utlämnandet är nödvändigt och proportionerligt.

Utöver utlämnandets förenlighet med övrig dataskyddsreglering och sekretesslagstiftningen måste den utlämnande myndigheten alltså göra ytterligare en prövning inför utlämnande på eget initiativ med stöd av de sekretessbrytande bestämmelserna i offentlighets- och

[126] Prop. 2017/18:232, *Brottsdatalag*, s. 138.
[127] Prop. 2017/18:232, *Brottsdatalag*, s. 443 och 452.

sekretesslagen. Om den i avsnitt 4.8.5 föreslagna bestämmelsen om utlämnande på eget initiativ av uppgifter som inte är sekretessbelagda införs så kommer det nyss sagda även gälla vid tillämpningen av den bestämmelsen.

Någon sådan prövning krävs dock inte när det föreligger en skyldighet att lämna ut uppgifter (jfr avsnitt 4.8.4 om skillnaderna mellan utlämnande efter en begäran och på eget initiativ). Regleringen utgår från uppfattningen att lagstiftaren inte har prövat om ett uppgiftsutlämnande är nödvändigt och proportionerligt när det inte föreligger någon skyldighet att lämna ut uppgifter, och att denna prövning i stället ankommer på den som ska tillämpa bestämmelserna.[128]

I avsnitt 5.4.6 har vi gjort bedömningen att det inte är motiverat att i dataskyddsreglering som (i huvudsak) kompletterar dataskyddsförordningen göra någon rättslig åtskillnad mellan olika bestämmelser i offentlighets- och sekretesslagen. I dataskyddsreglering som kompletterar dataskyddsförordningen är det dock vanligt att ändamålsbestämmelser synbart motsvarar ett förbud mot utlämnande i andra fall än när en skyldighet föreligger. Regleringen i brottsdatalagen innebär motsatsvis inte att den utlämnande myndigheten alltid är dataskyddsrättsligt förhindrad att lämna uppgifter med stöd av bestämmelser som innebär en möjlighet men ingen skyldighet. Tvärtom anges i lagkommentarerna att den prövning som ska ske när det bara finns en möjlighet att lämna uppgifter i regel bör mynna ut i att det är nödvändigt och proportionerligt att lämna ut uppgifter.[129] Utfallet av prövningen är alltså redan anvisad, i tillåtande riktning.

Det är vidare bara vissa av de brottsbekämpande myndigheterna som i enkätsvar uppgett att den kompletterande datasskyddsregleringen innehåller ändamålsbegränsningar som utgör ett hinder mot att lämna ut information om enskilda till andra myndigheter (jfr avsnitt 5.3.3). Det kan därför ifrågasättas om det faktiskt finns ett behov av att förändra den befintliga regleringen i brottsdatalagen.

[128] Jfr prop. 2017/18:232, *Brottsdatalag*, s. 138.
[129] Prop. 2017/18:232, *Brottsdatalag*, s. 443 och 452.

Det finns ett generellt behov av en konsekvent och tydlig lagstiftning

I avsnitt 5.4.6 har vi konstaterat att när den kompletterande dataskyddsregleringen ställer upp vad som kan uppfattas som hinder mot tillämpningen av bestämmelserna i offentlighets- och sekretesslagen så bidrar det till en generell risk för att inget av regelverken tillämpas på så sätt som avsetts. En sådan regleringsmodell medför dessutom oklarheter och därmed även tillämpningssvårigheter. I samma avsnitt har vi även redogjort för vår bedömning att lagstiftarens avvägning mellan skyddet för enskildas personliga integritet och andra intressen kommer till uttryck genom de rekvisit som ställs upp i offentlighets- och sekretesslagens bestämmelser och i bestämmelser om uppgiftsskyldighet enligt 10 kap. 28 § första stycket OSL. Detta gäller både för bestämmelser som förbjuder och som tillåter informationsutbyte mellan myndigheter och oavsett i vilket sammanhang bestämmelserna tillämpas. Att vi nu diskuterar brottsbekämpande myndigheters personuppgiftsbehandling påverkar alltså inte den bedömningen. Med den utgångspunkten bör den extra prövning som föreskrivs i 2 kap. 4 och 22 §§ BDL vara överflödig ur integritetssynpunkt.

Kravet på ytterligare en prövning, utöver bl.a. sekretessprövningen, medför dessutom att tillämparen tvingas ompröva lagstiftarens ställningstaganden i fråga om avvägningen mellan integritet och andra intressen, så som de kommer till uttryck i offentlighets- och sekretesslagen. Den befintliga regleringen är därmed både inkonsekvent och otydlig i fråga om vad som ska gälla och kan, beroende på hur tillämparens prövning faller ut, medföra att det uppstår en normkonflikt mellan regelverken. Det generella behovet av en konsekvent och tydlig lagstiftning gör sig alltså även gällande på brottsdatalagens område.

Direktivet då?

Brottsdatalagen genomför som vi redan påpekat 2016 års dataskyddsdirektiv i svensk rätt. Det innebär bl.a. att den svenska lagstiftaren inte fritt kan utforma eller ändra den nationella lagstiftningen. När förändringar av brottsdatalagen övervägs måste därför hänsyn tas till vad som framgår av den EU-rättsliga regleringen.

Artikel 4.2 i dataskyddsdirektivet ligger till grund för bestämmelsen i 2 kap. 4 § BDL. Av den artikeln framgår att behandling som utförs av samma eller en annan personuppgiftsansvarig för något annat ändamål inom direktivets tillämpningsområde än det för vilket personuppgifterna samlas in ska tillåtas om

a) den personuppgiftsansvarige i enlighet med unionsrätten eller medlemsstaternas nationella rätt är bemyndigad att behandla sådana personuppgifter för ett sådant ändamål, och

b) behandlingen är nödvändig och står i proportion till detta andra ändamål i enlighet med unionsrätten eller medlemsstaternas nationella rätt.

I förarbetena till bestämmelsen bedömde regeringen att det inte var klart om kravet på nödvändighet i artikel 4.2 i direktivet avser något annat än det krav som ingår i bedömningen av om det finns rättslig grund för behandlingen. Enligt regeringen borde dock utgångspunkten vara att om det finns en rättslig grund för att behandla personuppgifter för ett nytt ändamål, så är personuppgiftsbehandlingen också nödvändig för det nya ändamålet. Enligt regeringen var det med andra ord bara i rena undantagsfall som kravet på nödvändighet enligt artikel 4.2 i direktivet, utöver kravet på rättslig grund, begränsar möjligheten att vidarebehandla personuppgifter för nya ändamål.[130] Vad gäller proportionalitetsbedömningen uttalade regeringen att den innebär att skälen för att personuppgifterna behandlas för det nya ändamålet ska väga tyngre än det intrång som behandlingen innebär för den enskilde. Vad som står att vinna med vidarebehandlingen ska alltså vägas mot intrånget i enskildas integritet.[131]

Av artikel 9.1 i dataskyddsdirektivet följer att personuppgifter som samlas in av behöriga myndigheter för ändamål inom tillämpningsområdet inte behandlas för ändamål utanför tillämpningsområdet om inte sådan behandling är tillåten enligt unionsrätten eller medlemsstaternas nationella rätt. När personuppgifter behandlas för andra ändamål ska dataskyddsförordningen tillämpas, om inte behandlingen utförs som ett led i en verksamhet som inte omfattas av unionsrätten. Innebörden är alltså att det krävs författningsstöd för att personuppgifter som behandlas för ett ändamål inom data-

[130] Prop. 2017/18:232, *Brottsdatalag*, s. 128.
[131] Prop. 2017/18:232, *Brottsdatalag*, s. 128.

skyddsdirektivets område ska få behandlas för ändamål utanför direktivets tillämpningsområde. Något krav på att behandlingen ska vara nödvändig och proportionerlig som i artikel 4.2 finns dock inte.

Regleringen i 2 kap. 22 § BDL, som anger under vilka förutsättningar vidarebehandling av personuppgifter för nya ändamål utanför brottsdatalagens tillämpningsområde får ske, motsvarar dock den som framgår av 2 kap. 4 § BDL. Även här åläggs alltså den behöriga myndigheten att innan en behandling för ändamål utanför lagens tillämpningsområde påbörjas göra en nödvändighets- och proportionalitetsbedömning. Bestämmelsen i brottsdatalagen går alltså utöver vad som krävs enligt artikel 9.1 i dataskyddsdirektivet.[132] Regeringens motiv till att ändå införa bestämmelsen var att det inte framstod som rimligt att kräva en noggrannare prövning för behandling för nya ändamål inom ramlagens tillämpningsområde än utanför det.[133]

Som vi nämnt ovan och utvecklat närmare i avsnitt 5.4.6 bedömer vi att lagstiftaren måste anses ha gjort de bedömningar och avvägningar som är påkallade ur ett integritetsperspektiv vid utformningen av bestämmelserna i offentlighets- och sekretesslagen. Lagstiftaren har alltså redan tagit ställning till frågan om nödvändighet och proportionalitet, bl.a. genom utformningen av de sekretessbrytande bestämmelsernas rekvisit och tillämpningsområde. Att vidarebehandling genom utlämnande till en annan myndighet i överensstämmelse med lag eller förordning är tillåtet enligt brottsdatalagen, utan någon ytterligare prövning än de som följer av de allmänna dataskyddsrättsliga principerna bör därför inte strida mot kraven i artikel 4.2 och artikel 9.1 i dataskyddsdirektivet.

Uppgiftslämnande i överenstämmelse med lag eller förordning bör dataskyddsrättsligt regleras enhetligt

Eftersom samtliga förbud mot att röja en uppgift som ska gälla i det allmännas verksamhet framgår av offentlighets- och sekretesslagen finns det inte skäl att göra någon annan bedömning för den

[132] Jfr Lagrådets yttrande över förslag till brottsdatalag, 2018-03-23, s. 8, tillgängligt: https://www.lagradet.se/wp-content/uploads/lagradet-attachments/Brottsdatalag.pdf (hämtad 2025-02-21).
[133] Prop. 2017/18:232, *Brottsdatalag*, s. 134.

brottsbekämpande verksamheten än den som framgår av avsnitten 5.4.4 och 5.4.5.

Vi föreslår därför att bestämmelserna i 2 kap. 4 och 22 §§ BDL ska ändras på så sätt att någon nödvändighets- och proportionalitetsprövning inte ska göras när vidarebehandling sker för utlämnande i överensstämmelse med lag eller förordning. Den generella regleringen inom det brottsbekämpande området får därmed samma förhållande till offentlighets- och sekretesslagens bestämmelser som dataskyddsreglering som kompletterar dataskyddsförordningen.

Ändringen innebär att en behörig myndighet inte behöver utföra några andra prövningar inför ett utlämnande än om det är tillåtet enligt offentlighets- och sekretesslagen, dock självfallet med iakttagande av vad som följer av allmänna dataskyddsrättsliga principer, t.ex. principen om uppgiftsminimering. Detta ska gälla oavsett om uppgiftsutlämnandet sker till en annan behörig myndighet som ska behandla uppgifterna för ett ändamål inom brottsdatalagens tillämpningsområde (2 kap. 4 § BDL) eller om uppgifterna lämnas ut till en myndighet som ska behandla dem för ändamål utanför brottsdatalagens tillämpningsområde (2 kap. 22 § BDL).

Genom den föreslagna ändringen bör det bli tydligare för enskilda hur personuppgifter kan komma att behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning, oavsett om behandlingen utgör en skyldighet eller möjlighet för den utlämnande myndigheten. Förändringen bör därmed bidra till ökad transparens för de registrerade vars uppgifter behandlas och kan därför, i likhet med förslaget i avsnitt 5.4.6, ses som en integritetshöjande åtgärd.

5.6 Elektroniskt utlämnande

5.6.1 Allmänt om elektroniskt utlämnande

Begreppet elektroniskt utlämnande

I kompletterande dataskyddsreglering används normalt begreppet elektroniskt utlämnande för sådant utlämnande av uppgifter som sker med digitala hjälpmedel, dvs. utlämnande som sker i någon form som inte är analog. Analogt utlämnande kan t.ex. vara muntligen eller på papper. I det följande använder vi begreppet elektro-

niskt utlämnande (eller varianter på detta) när vi syftar på utlämnande av uppgifter som inte sker analogt utan med digital teknik.

Utlämnande till enskilda

När det gäller utlämnande av allmänna handlingar från myndigheter till enskilda finns det en generell reglering av formen för utlämnande i tryckfrihetsförordningen. Enskilda har genom 2 kap. 15 § TF rätt att ta del av allmänna handlingar hos den myndighet som förvarar dem, på ett sådant sätt att den kan läsas eller avlyssnas eller uppfattas på annat sätt. Den som önskar det har även rätt att mot en fastställd avgift få en avskrift eller kopia av en allmän handling, till den del handlingen får lämnas ut, vilket framgår av 2 kap. 16 § första stycket TF. En myndighet är dock enligt samma bestämmelse inte i större utsträckning än vad som följer av lag skyldig att lämna ut en *upptagning för automatiserad behandling* i annan form än genom utskrift. Bestämmelsen benämns ofta ”utskriftsundantaget”.[134]

Av förarbetena till tryckfrihetsförordningen framgår att det framför allt var register- och databashantering som avsågs med uttrycket upptagning för automatiserad behandling. Ett utlämnande av sådana handlingar i form av kopia ansågs kunna riskera att uppgifter behandlades automatiserat på ett sätt som kunde medföra otillbörliga integritetsintrång. Det var mot den bakgrunden som utskriftsundantaget infördes. Med ”utskrift” avses att en teknisk upptagning överförs till skrift. Bestämmelsen innebär dock inte något förbud mot att handlingar lämnas ut i elektronisk form.[135] Enskilda har alltså sammanfattningsvis en grundlagsskyddad rätt att få en kopia av en allmän handling, men den rätten omfattar inte att få kopian digitalt.

I sammanhanget bör nämnas att det finns ett förslag om att reglera myndigheters digitala kommunikation med enskilda på ett generellt plan, som ännu inte lett till lagstiftning. I juni 2024 föreslog Utredningen om digital post (I 2020:03) att det skulle införas en ny lag om användning av myndighetsgemensam infrastruktur för digital post. Enligt den föreslagna lagen ska myndigheterna skicka myndighetspost genom den myndighetsgemensamma infrastrukturen för digital

[134] Jfr Högsta förvaltningsdomstolens avgörande HFD 2021 ref. 25.
[135] Prop. 1973:33, *med förslag till ändringar i tryckfrihetsförordningen, m.m.*, s. 80–82, 86 och 113, och prop. 1975/76:160, *om nya grundlagsbestämmelser angående allmänna handlingars offentlighet*, s. 82, 83 och 189.

post, om det inte finns säkerhetsskäl eller andra skäl som talar emot det. Det föreslås även att myndigheterna ska få skicka annat än myndighetspost genom infrastrukturen om det är lämpligt.[136]

I nuläget är det dock fortfarande bestämmelserna i den kompletterande dataskyddsregleringen som kan sägas komplettera utskriftsundantaget, i den meningen att de anger när och under vilka förutsättningar uppgifter får lämnas ut elektroniskt till enskilda och när det inte får ske på detta sätt. Det är emellertid först om det i en kompletterande dataskyddslag (eller i annan lag) föreskrivs *en rätt* för enskilda att få del av uppgifter elektroniskt som enskilda har en sådan rätt (jfr 2 kap. 16 § första stycket TF om att enskilda *inte i större utsträckning än vad som följer av lag* […]). Om någon sådan rätt inte har föreskrivits gäller utskriftundantaget.

Om en myndighet enligt tillämplig kompletterande dataskyddsreglering under vissa förhållanden *får* lämna ut uppgifter elektroniskt till enskilda så finns det alltså som utgångspunkt inget hinder mot att myndigheten nekar ett sådant utlämnande och i stället lämnar ut uppgifter i analog form. Det kan t.ex. bli aktuellt om lämplig säkerhet för personuppgifter inte kan säkerställas vid ett elektroniskt utlämnande (jfr artikel 5. 1 f i dataskyddsförordningen). I en sådan situation finns det som utgångspunkt ingen rätt för enskilda att överklaga myndighetens beslut att neka ett elektroniskt utlämnande, under förutsättning att uppgifterna tillhandahålls på annat sätt.[137]

Utlämnande till myndigheter

Myndigheters informationsutbyte grundar sig inte på bestämmelserna i tryckfrihetsförordningen. I svensk rätt är det som vi redan påpekat främst offentlighets- och sekretesslagens bestämmelser som avgör när informationsutbyte mellan myndigheter får ske, samt vad som framgår av särskilt reglerade uppgiftsskyldigheter. Regleringen är som utgångspunkt teknikneutral. Med det menas att i regel berör varken offentlighets- och sekretesslagens bestämmelser eller särskilda uppgiftsskyldigheter frågan om hur ett utlämnande rent praktiskt får eller ska genomföras, t.ex. om det ska ske muntligt, på papper, via fax, eller genom e-post. Bestämmelser som innebär att myndig-

[136] SOU 2024:47, *Digital myndighetspost*, s. 29.
[137] Jfr Kammarrätten i Jönköpings dom den 9 augusti 2012 i mål 2491–12 och Kammarrätten i Stockholms dom den 1 april 2015 i mål 2230–15.

heter får eller ska utbyta viss information besvarar alltså i regel inte frågan om hur detta får eller ska gå till rent praktiskt.

Enligt 2 § förordningen (2003:770) om statliga myndigheters elektroniska informationsutbyte ska en myndighet i sin verksamhet främja utvecklingen av ett säkert och effektivt elektroniskt informationsutbyte inom den offentliga förvaltningen. Hur detta ska gå till anvisas dock inte. Under 2023 föreslog Utredningen om interoperabilitet vid datadelning (I 2022:03) att en skyldighet för den offentliga förvaltningen att använda nationella interoperabilitetslösningar ska införas i en särskild lag. Lösningarna kan avse exempelvis standarder, specifikationer och andra liknande lösningar eller krav som ska tillämpas vid datadelning.[138] Utredningens förslag har dock inte lett till lagstiftning. I dag finns det alltså inte någon generell reglering av vilka särskilda former myndigheters elektroniska informationsutbyte ska ha, eller vilka tekniska lösningar som får användas.

5.6.2 Reglering av elektroniskt utlämnande mellan myndigheter

Allmänt

Bestämmelser som avser elektroniskt utlämnande till andra myndigheter förekommer huvudsakligen i den kompletterande dataskyddsregleringen. Sedan myndigheters personuppgiftsbehandling med stöd av ADB, dvs. digitala informationshantering, började regleras genom 1973 års datalag har formerna för och tillåtligheten av elektroniskt uppgiftslämnande av uppgifter reglerats, antingen i särskild författning eller genom Datainspektionens föreskrifter. Som vi konstaterat i avsnitt 5.4.2 gällde inte sekretess enligt 1937 års sekretesslag mellan myndigheter. Begränsningar av myndigheters möjlighet att utbyta uppgifter elektroniskt kunde följaktligen ha en annan funktion och betydelse innan 1980 års sekretesslag medförde att sekretessreglerna också skulle tillämpas mellan myndigheter.

Regleringen av elektroniskt utlämnande i den kompletterande dataskyddsregleringen utgår sällan från dagens olika tekniska möjligheter att utbyta information (jfr avsnitt 5.2.3). I stället används i regel två olika juridiska begrepp för att reglera formen för utlämnande; *direktåtkomst* och *elektroniskt utlämnande på annat sätt än genom direkt-*

[138] SOU 2023:96, *En reform för datadelning*, s. 199.

åtkomst. Dessa begrepp har sitt ursprung i den digitala informationshantering som förekom under 1970- och 1980-talen och benämndes tidigare terminalåtkomst och utlämnande på medium för automatiserad behandling. Den äldre termen utlämnande på medium för automatiserad behandling förekommer fortfarande i viss kompletterande dataskyddsreglering.

Direktåtkomst

Allmänt

Direktåtkomst är en form av elektronisk informationsöverföring som sammanfattningsvis innebär att den mottagande myndigheten kan hämta information direkt från den utlämnande myndighetens it-system. Det skiljer sig alltså från sådant utlämnande som föregås av en manuell eller automatiserad kontroll eller annan prövning i det enskilda fallet av om utlämnandet ska ske.

Utlämnande genom det som i dag benämns som direktåtkomst kännetecknades ursprungligen av en tillgång via terminal eller liknande till en ”dataanläggning” och kallades då terminalåtkomst.[139] I de tidiga systemen för terminalåtkomst ansågs det saknas teknisk möjlighet att begränsa den enskilde medarbetarens åtkomst till enbart sådana uppgifter som han eller hon behövde för sitt arbete. Att en uppgift var tillgänglig ”via terminal” ansågs därför öka risken för att någon obehörigen tog del av den, vilket i sin tur försvagade sekretesskyddet.[140] Ett vanligt sätt att beskriva direktåtkomst har varit att ett sådant utlämnande innebär att mottagaren på egen hand kan söka i den utlämnande myndighetens digitala informationssamling, men utan att kunna påverka innehållet. Direktåtkomst kan dock även ge användaren möjlighet att hämta in information till sitt eget system och bearbeta den där.[141]

I begreppet direktåtkomst ligger också att den utlämnande myndigheten saknar kontroll över vilka faktiska uppgifter, av de som åtkomst har medgetts till, som den mottagande parten vid ett visst

[139] Jfr beskrivningen i prop. 1973:33, *med förslag till ändringar i tryckfrihetsförordningen m.m.*, s. 77.
[140] Jfr prop. 1979/80:146, *med förslag till skatteregisterlag*, s. 21 och 31.
[141] Se t.ex. prop. 2016/17:58, *Uppgifter på individnivå i arbetsgivardeklarationen*, s. 112.

tillfälle tar del av.[142] Den myndighet som lämnar ut uppgifter genom direktåtkomst fattar därmed inte något beslut om utlämnande av uppgifter i varje enskilt fall som den mottagande myndigheten tar del av uppgifterna. I stället måste den utlämnande myndigheten göra en förhandsprövning av förutsättningarna för utlämnande i samband med att åtkomsten rent tekniskt upprättas. En sådan prövning innefattar alla uppgifter som mottagaren har möjlighet att ta del av genom direktåtkomsten.

Lagstiftaren har under en lång tid bedömt att direktåtkomst är en så integritetskänslig form av personuppgiftsbehandling att den i princip endast är tillåten om det finns ett uttryckligt stöd för den i lag.[143] Myndigheters möjlighet att utbyta uppgifter elektroniskt genom direktåtkomst är följaktligen ofta starkt begränsad. Bestämmelser som förbjuder direktåtkomst, eller som anger i vilka fall direktåtkomst får förekomma, finns i regel i den kompletterande dataskyddsregleringen. Det bör dock nämnas att det även har förekommit oreglerat uppgiftslämnande genom direktåtkomst.[144]

Överskottsinformation

Vid direktåtkomst uppkommer vissa rättsliga förhållanden som utgör en väsentlig skillnad mellan direktåtkomst och andra former av elektroniskt utlämnande. Ett utlämnande genom direktåtkomst omfattar som vi nyss påpekat *samtliga* uppgifter som den mottagande myndigheten har rätt att ta del av på detta sätt. Som en generell utgångspunkt kan det emellertid förutsättas att en mottagande myndighet inte faktiskt kommer att ta del av samtliga uppgifter som lämnas ut genom direktåtkomst. Det är först när det uppkommer ett sakligt behov av uppgifterna som den mottagande myndigheten har en rättslig grund att ta del av dem. Exempelvis måste den mottagande myndigheten normalt anses sakna rättslig grund för behandling av uppgifter om en person som inte förkommer i den egna verksamheten, men som är aktuell hos den utlämnande myndigheten i

[142] Jfr tex. prop. 2004/05:164, *Tullverkets brottsbekämpning – Effektivare uppgiftsbehandling*, s. 83, prop. 2005/06:52, *Elektronisk informationsöverföring hos arbetslöshetskassorna och inom Arbetsmarknadsverket*, s. 8 och prop. 2016/17:58, *Uppgifter på individnivå i arbetsgivardeklarationen*, s. 127.
[143] Jfr redogörelsen i SOU 2010:4, *Allmänna handlingar i elektronisk-form – offentlighet och integritet*, s. 133, 134 och 365 och prop. 2022/23:34, *Utbetalningsmyndigheten*, s. 140–142.
[144] SOU 2012:90, *Överskottsinformation vid direktåtkomst*, s. 121.

ett sådant sammanhang att vissa uppgifter om personen omfattas av direktåtkomsten. Den information som den mottagande myndigheten har teknisk tillgång till genom direktåtkomsten, men som myndigheten inte har skäl att faktiskt ta del av utgör s.k. överskottsinformation.

Regleringen av allmänna handlingar i 2 kap. TF innebär sammanfattningsvis att *samtliga* handlingar som görs tillgängliga genom direktåtkomst anses som *inkomna* hos den mottagande myndigheten. Det gäller oavsett om den mottagande myndigheten faktiskt har tagit del av dem eller inte. För frågan om vad som utgör en inkommen allmän handling hos den mottagande myndigheten spelar det alltså ingen roll om mottagarmyndigheten i ett enskilt fall faktiskt använder sig av möjligheten att söka fram en uppgift som den utlämnande myndigheten lämnat ut genom direktåtkomst. Det räcker att denna möjlighet finns tillgänglig för mottagaren. Förekomsten av överskottsinformation innebär alltså att det finns handlingar hos den mottagande myndigheten som är allmänna där, men som den mottagande myndigheten inte för egen del har rätt att ta del av.[145]

Direktåtkomst i dag

Redan för drygt 15 år sedan konstaterade regeringen att teknikutvecklingen hade lett till att skillnaden mellan direktåtkomst och annat elektroniskt utlämnande blivit så liten att det ibland kunde vara svårt att dra en gräns mellan de olika formerna för elektronisk informationsöverföring.[146] Liknande bedömningar har gjorts i flera andra sammanhang sedan dess. Användarupplevelsen blir exempelvis densamma i en digital s.k. fråga-svar-tjänst som vid direktåtkomst. I båda fallen lämnas uppgifter ut momentant, utan någon mänsklig inblandning.[147]

Genom Högsta förvaltningsdomstolens avgörande HFD 2015 ref. 61 (det s.k. LEFI Online-avgörandet, som gjorts generellt tillämpligt genom HFD 2020 not. 16) har ett visst klargörande beträffande gränsdragningen mellan direktåtkomst och annat elektroniskt

[145] Se vidare SOU 2012:90, *Överskottsinformation vid direktåtkomst*.
[146] Prop. 2007/08:160, *Utökat elektroniskt informationsutbyte*, s. 58.
[147] Jfr prop. 2021/22:177, *Sammanhållen vård och omsorgsdokumentation*, s. 79, SOU 2021:46, *Snabbare lagföring – ett snabbförfarande i brottmål*, s. 416 och Skatteverkets remissvar 2020-04-20, Promemorian *De brottsbekämpande myndigheternas direktåtkomst till beskattningsdatabasen*, Ju2020/00320/L4, s. 4.

utlämnande skett. Av det rättsfallet följer att om ett automatiserat system för informationsöverföring inte kräver en reaktion av den utlämnande myndigheten föreligger direktåtkomst. Om systemet däremot kräver en (helt automatiserad) reaktion från den utlämnande myndigheten föreligger dock inte direktåtkomst, trots att systemet ger användaren samma momentana svar som vid direktåtkomst.[148]

Direktåtkomst till annars sekretessbelagda uppgifter utformas i dag ofta på så sätt att den information som omfattas av de sekretessbrytande bestämmelserna läggs över på en särskild digital yta i den utlämnande myndighetens system. En mottagande myndighet har då enbart tillgång till denna avgränsade yta. Överskottsinformationen utgörs därmed inte av den totala uppgiftsmängden hos den utlämnande myndigheten. I dag finns det följaktligen inte någon faktisk möjlighet för den mottagande myndigheten att fritt söka i den utlämnande myndighetens totala uppgiftsmängd vid direktåtkomst. Med dagens teknik kan åtkomsten även begränsas hos den mottagande myndigheten till att endast avse uppgifter som behövs för de arbetsuppgifter den enskilda medarbetaren har.[149]

I flera olika sammanhang har det under de senare decennierna påpekats att det går att ifrågasätta om den rättsliga uppdelningen mellan direktåtkomst och annat elektroniskt utlämnande är berättigad, såväl ur integritetssynpunkt som rent tekniskt.[150] Regeringen har dessutom i ett lagstiftningsärende avseende i vilken form uppgifter ska lämnas mellan olika aktörer inom vården, uttalat att det inte [längre] är en stor skillnad mellan direktåtkomst och en elektronisk fråga-svar-funktion vad gäller risken för integritetsintrång.[151] Det finns även förslag om att inte längre särreglera utlämnande genom direktåtkomst vid vissa myndigheter, som ännu inte genomförts. I dessa sammanhang har särskilt lyfts att genom den tekniska utvecklingen har skillnaden i integritetshänseende mellan direktåtkomst och andra former av utlämnande blivit väsentligt mindre, att direktåtkomst kan medföra vissa fördelar ur integritetssynpunkt och att de överväganden som är förknippade med upprättandet av

[148] Jfr SOU 2023:100, *Framtiden dataskydd – Vid Skatteverket, Tullverket och Kronofogden*, s. 804.
[149] SOU 2023:100, *Framtiden dataskydd – Vid Skatteverket, Tullverket och Kronofogden*, s. 754.
[150] Se bl.a. eSam, *En modern registerförfattning*, dnr ES2022-06, s. 41, SOU 2015:39, *Myndighetsdatalag*, s. 151 och prop. 2000/01:33, *Behandling av personuppgifter inom skatt, tull och exekution*, s. 110 och 111.
[151] Prop. 2021/22:177, *Sammanhållen vård och omsorgsdokumentation*, s. 79.

en direktåtkomst får en adekvat reglering genom dataskyddsförordningens bestämmelser.[152]

Annat elektroniskt utlämnande än direktåtkomst

För annat elektroniskt utlämnande än direktåtkomst brukade begreppet ”utlämnande på medium för automatiserad behandling” tidigare användas i dataskyddssammanhang. Som vi nämnt inledningsvis finns begreppet kvar i viss kompletterande dataskyddsreglering men har under senare tid i flera fall ersatts av begreppet ”annat elektroniskt utlämnande än direktåtkomst”. Någon skillnad i innebörd mellan de två begreppen finns dock inte och det finns inte heller någon legaldefinition av något av dem.[153] Utmärkande är i stället att utlämnandeformen *inte* utgör direktåtkomst.

Till skillnad från direktåtkomst avses här inte någon särskild form av elektronisk informationsöverföring. Vad som avses rent konkret har dessutom varierat beroende på vilken informationshanteringsteknik som varit tillgänglig för tillfället. Ursprungligen avsågs en fysisk bärare av information som krävde någon form av automatiserad teknik för att avläsas eller avlyssnas. Vid millennieskiftet angavs utlämnande på magnetband eller diskett som exempel, tekniker som är helt utdaterade i dag.[154] Ännu tidigare exempel är s.k. hålkort och hålremsor.[155]

Sådant utlämnande som avses kan, som vi redogjort för i avsnitt 5.2.3, i dag exempelvis innebära att elektronisk information överförs via e-post, genom utlämnande av uppgifter på ett flyttbart lagringsmedium, t.ex. usb-minne, eller genom ett system för direkt överföring från ett datorsystem till ett annat, t.ex. ett API eller en fråga-svartjänst.[156] Ett annat exempel är s.k. batch-körningar. Stora informationsmängder, batcher, lämnas då över digitalt till den mottagande myndigheten med vissa intervaller. Ett sätt att beskriva förfarandet är att de uppgifter som ett reglerat uppgiftslämnande omfattar lämnas över i bulk, utan en prövning av behovet *i det enskilda*

[152] SOU 2023:100, *Framtiden dataskydd – Vid Skatteverket, Tullverket och Kronofogden*, s. 825 och 826 och SOU 2024:95, *Modernt dataskydd vid CSN*, s. 343 och 344.
[153] Jfr t.ex. prop. 2019/20:106, *Stärkt integritet i Rättsmedicinalverkets verksamhet*, s. 56 och prop. 2022/23:34, *Utbetalningsmyndigheten*, s. 140.
[154] Jfr prop. 2000/01:33, *Behandling av personuppgifter inom skatt, tull och exekution*, s. 234.
[155] Prop. 1973:33, *med förslag till ändringar i tryckfrihetsförordningen m.m.*, s. 75.
[156] Jfr HFD 2015 ref. 61, LEFI Online-avgörandet.

fallet hos den mottagande myndigheten. Den fördröjning som är inbyggd i systemet, jämfört med om utlämnandet hade skett genom direktåtkomst, anses innebära en möjlighet för utlämnaren att kontrollera vilken information som ska lämnas ut. Den faktiska sekretessprövningen sker dock i praktiken i samband med att den tekniska förbindelsen som möjliggör körningen upprättas mellan myndigheterna.[157] I likhet med direktåtkomst bygger alltså även sådana moderna former av informationsutbyte som inte utgör direktåtkomst på en i förväg genomförd sekretessprövning och automatiserade kontroller.[158]

Sedan personuppgiftslagen infördes, och särskilt på senare tid, har utlämnande på medium för automatiserad behandling, dvs. annat elektroniskt utlämnande än direktåtkomst, i många fall inte bedömts behöva regleras särskilt när det gäller informationsutbyte mellan myndigheter. Om reglering av formerna för utlämnande över huvud taget förekommer är det vanligt att regleringen anger att elektroniskt utlämnande på annat sätt än direktåtkomst är tillåtet, eller att sådant utlämnande är tillåtet om det inte är olämpligt.[159]

Även om det är sällsynt förekommer det dock fortfarande begränsningar av myndigheters möjlighet att utbyta uppgifter med andra myndigheter elektroniskt på annat sätt än genom direktåtkomst. I dessa fall kan det t.ex. röra sig om att en bestämmelse i den kompletterande dataskyddsreglernigen anger att utlämnande på medium på automatiserad behandling bara får ske till särskilt angivna mottagare och för vissa syften.

5.6.3 Elektroniskt utlämnande på annat sätt än genom direktåtkomst ska vara tillåtet om det inte är olämpligt

Vårt förslag: Elektroniskt utlämnande på annat sätt än genom direktåtkomst ska vara tillåtet om det inte är olämpligt.

[157] Jfr SOU 2015:39, *Myndighetsdatalag*, s. 128.
[158] SOU 2023:100, *Framtiden dataskydd – Vid Skatteverket, Tullverket och Kronofogden*, s. 805 och 806.
[159] Jfr t.ex. 1 kap. 12 § lagen (2023:457) om behandling av personuppgifter vid Utbetalningsmyndigheten och 2 kap. 12 § lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område.

Skälen för vårt förslag

Uppgiftsutbyte mellan myndigheter sker i dag digitalt

Som vi nyss konstaterat förekommer det, även om det är sällsynt, att det finns begränsningar av myndigheters möjlighet att utbyta uppgifter med andra myndigheter elektroniskt på annat sätt än genom direktåtkomst. I princip samtliga fall där det förekommer är regleringen av äldre datum. Att det finns begränsningar av myndigheters möjligheter att lämna ut uppgifter elektroniskt, som uppfattas hindra ett efterfrågat informationsutbyte, syns även i resultaten av vår kartläggning (se avsnitt 5.3.3).

Samhällets generella övergång till digital informationshantering har medfört att informationsflödet, såväl mellan myndigheter som i övrigt, numera främst är digitalt. I tidigare lagstiftningsärenden där formerna för utlämnande varit i fråga har regeringen konstaterat att både i Sverige och inom EU uppmuntras myndigheter att i så stor utsträckning som möjligt dra nytta av de effektivitetsvinster som modern teknik kan ge.[160] Regeringen har även uttalat att en manuell informationshantering i dag inte kan sägas vara ett realistiskt alternativ för vare sig myndigheter eller företag.[161] Informationsutbyte i elektronisk form är alltså en integrerad del i myndigheternas verksamhet i dag.

Målet för digitaliseringspolitiken är dessutom sedan flera år att Sverige ska vara bäst i världen på att använda digitaliseringens möjligheter.[162] Regeringen har 2018 uttalat att målet för digitaliseringen av den offentliga förvaltningen bl.a. är en enklare vardag för medborgare och högre kvalitet och effektivitet i verksamheten. Vidare har regeringen gjort bedömningen att digitalt ska vara förstahandsval i den offentliga förvaltningens verksamhet.[163]

Inom den offentliga sektorn finns det sammanfattningsvis ett stort och legitimt behov av att kunna lämna ut och ta emot personuppgifter och andra uppgifter elektroniskt. På senare tid har det därför i olika sammanhang införts bestämmelser i kompletterande dataskyddsreglering med innebörden att annat elektroniskt utlämnande än direktåtkomst är tillåtet, eller att sådant utlämnande är tillåtet om

[160] Jfr prop. 2020/21:224, *Behandling av personuppgifter vid Försvarsmakten och Försvarets Radioanstalt*, s. 104.
[161] Prop. 2017/18:105, *Ny dataskyddslag*, s. 47.
[162] Budgetpropositionen för 2012, prop. 2011/12:1 utg. omr. 22, s. 84.
[163] Budgetpropositionen för 2019, prop. 2018/19:1 utg. omr. 2, s. 53.

det inte är olämpligt. Det finns dessutom ett antal sådana förslag som ännu inte lett till lagstiftning.

Det går i och för sig inte att ifrågasätta att automatiserad behandling av stora mängder personuppgifter, som särskilt kan bli aktuellt vid informationsutbyte mellan myndigheter, kan medföra förhöjda risker ur integritetssynpunkt. Som vi har redogjort för i avsnitten 3.4 och 5.2.3 aktualiserar dock ett informationsutbyte mellan myndigheter inte enbart sekretessfrågor utan även en mängd bestämmelser i den allmänna dataskyddsregleringen som också ska tillämpas. I de allra flesta fall, dvs. när dataskyddsförordningen är tillämplig, finns det därför redan en omfattande reglering som bl.a. kräver att tekniska system för digitalt informationsutbyte utformas eller anpassas på så sätt att de grundläggande principerna för personuppgiftsbehandling iakttas. Vi anser därför att det inte går att utgå från att integritetsriskerna är lägre vid ett analogt utlämnande än vid ett elektroniskt utlämnande. Användandet av olika tekniska funktioner kan i stället innebära en högre grad av skydd för personuppgifter än om ett pappersbrev eller en fax hade skickats. Under förutsättning att utlämnandet sker med tillämpning av tillgängliga tekniker för säker informationsöverföring kan elektroniskt utlämnande alltså innebära ett starkare integritetsskydd än vid analog hantering.

Vad gäller annat elektroniskt utlämnande än direktåtkomst utgår vi därför från att det i dag inte längre finns några sakliga skäl att begränsa myndigheters möjligheter till informationsutbyte med andra myndigheter i sådan form. Vi föreslår därför att det ska införas generella bestämmelser som på ett tydligt sätt tillåter elektroniskt utlämnande i kompletterande dataskyddsreglering som omfattas av vår översyn.

Frågan om direktåtkomst

Som vi redogjort för i avsnitt 5.6.2 har skillnaderna mellan direktåtkomst och annat elektroniskt utlämnande kontinuerligt minskat, såväl vad gäller de generella integritetsriskerna som vilka prövningar som görs innan ett utlämnande. I dag finns det förslag på kompletterande dataskyddsreglering där myndigheten ges en rättslig möjlighet att utforma system för informationsutbytet med andra myndigheter på det sätt som framstår som mest lämpligt, dvs. även om det innebär att uppgifter kommer att lämnas ut genom direktåtkomst. Inom

tillämpningsområdet för sådana författningar kommer det alltså inte finnas några absoluta hinder mot att lämna ut uppgifter genom direktåtkomst, om förslagen genomförs.[164]

Om elektroniskt utlämnande över huvud taget är reglerat i kompletterande dataskyddsreglering är det dock fortfarande vanligast att utlämnande genom direktåtkomst antingen är uttryckligen förbjudet, eller att sådant utlämnande enbart är tillåtet i de fall det är uttryckligen reglerat. I dag framstår dock inte frågan om *vilken* teknik som används som avgörande för integritetsriskerna, utan *hur* tekniken används.[165] Att myndigheter är dataskyddsrättsligt förhindrade att utforma tekniska system för informationsutbyte med andra myndigheter utifrån vad som i det enskilda fallet framstår som mest effektivt, säkert och ändamålsenligt går därför självfallet att ifrågasätta. För att våra förslag om förbättrade möjligheter till informationsutbyte mellan myndigheter ska tjäna sitt syfte och vara möjliga att tillämpa på ett ändamålsenligt sätt skulle vår översyn därmed kunna omfatta bestämmelser om direktåtkomst.

Att utlämnande genom direktåtkomst är förbjudet innebär dock inget hinder mot andra former av elektroniskt utlämnande. I dag finns det informationsdelningssystem som uppfyller samma krav på momentan tillgång till uppdaterad information, utan tidskrävande prövningar i det enskilda fallet, som ofta legat till grund för tillåtligheten av direktåtkomst, utan att systemen rent juridiskt klassas som direktåtkomst. Regeringen har dessutom tidigare bedömt att en ändamålsenlig avvägning mellan riskerna med att överföra uppgifter elektroniskt och behovet av effektiva arbetssätt uppnås genom en reglering som tydliggör att uppgifter får lämnas ut elektroniskt, men som samtidigt uttryckligen reglerar att direktåtkomst inte är tillåtet. Enligt regeringen är en sådan regleringsmodell också att anse som en skyddsåtgärd enligt dataskyddsförordningen.[166]

Mot bakgrund av att utlämnande genom direktåtkomst tidigare har bedömts vara mycket integritetskänsligt bör frågan om det finns sakliga skäl för en fortsatt särreglering av direktåtkomst inom i princip hela den offentliga sektorn under alla förhållanden falla utanför ramen för vårt uppdrag.

---

[164] Se författningsförslagen i SOU 2023:100, *Framtiden dataskydd – Vid Skatteverket, Tullverket och Kronofogden* och i SOU 2024:95, *Modernt dataskydd vid CSN*.
[165] Jfr IMY, *Integritet och ny teknik 2020–2024 – Redovisning av Integritetsskyddsmyndighetens uppdrag att följa, analysera och beskriva utvecklingen*, dnr IMY-2024-2570, s. 6.
[166] Prop. 2022/23:34, *Utbetalningsmyndigheten*, s. 142.

Utlämnande till enskilda kommer att omfattas i vissa fall

Äldre kompletterande dataskyddsreglering innehöll ofta detaljerade bestämmelser om vilka uppgifter som fick lämnas ut elektroniskt, särskilt när det gällde utlämnande till enskilda. I de fall sådan reglering fortfarande gäller finns det ofta viss reglering för elektroniskt utlämnande till enskilda och annan reglering av elektroniskt utlämnande till myndigheter. Det förekommer att det innebär att myndigheter är förhindrade att kommunicera med enskilda digitalt, och därför är hänvisade till att skicka pappersbrev.[167] Mot bakgrund av regeringens målsättning med digitaliseringspolitiken, befolkningens ökande internetanvändning och den tekniska utvecklingen med allt säkrare digitala kommunikationssätt finns det enligt vår mening starka skäl för att upphäva reglering som i praktiken förbjuder myndigheter att t.ex. skicka säker e-post till enskilda. Frågor om myndigheters digitala kommunikation med enskilda faller dock utanför ramen för vårt uppdrag.

Det förekommer emellertid att utlämnande till enskilda inte regleras i särskild ordning, utan att allt elektroniskt utlämnande träffas av en och samma bestämmelse. Förändringar av denna bestämmelse blir alltså tillämpliga även vid utlämnande till enskilda. Trots att vårt uppdrag är begränsat till myndigheters informationsutbyte anser vi att det saknas skäl för att i dessa författningar undanta utlämnandet till enskilda från bestämmelsens tillämpningsområde. Som vi nyss konstaterat framstår det inte längre som motiverat att av integritetsskäl hindra myndigheters användning t.ex. av e-post, vilket vi även utvecklar nedan. Införandet av en bestämmelse om att elektroniskt utlämnande är tillåtet kommer alltså i vissa fall även träffa utlämnande till enskilda.

Elektroniskt utlämnande ska vara tillåtet om det inte är olämpligt

Inledningsvis bedömde vi att det i dag inte längre finns några sakliga skäl för att begränsa myndigheters möjligheter till informationsutbyte med andra myndigheter genom annat elektroniskt utlämnande än direktåtkomst. Vi bedömde också att det bör införas bestämmelser som var tydligt tillåtande i detta avseende. Frågan är då hur bestämmelser som tillåter sådant utlämnande ska utformas.

[167] Jfr SOU 2023:100, *Framtidens dataskydd – Vid Skatteverket, Tullverket och Kronofogden*, s. 798.

För det första bör sägas att begreppet utlämnande på medium för automatiserad behandling är tydligt präglat av en annan tids informationshanteringsmöjligheter och mot bakgrund av den tekniska utvecklingen framstår det som svårbegripligt. Det är sannolikt få personer som i dagligt tal skulle kalla t.ex. e-post för ett medium för automatiserad behandling. I andra sammanhang har begreppet medium för automatiserad behandling övergetts till förmån för begreppet elektroniskt utlämnande, eller närliggande uttryck. Exempelvis används begreppet ”lämna ut elektroniskt” i domstolsdatalagen. Regeringen har också uttalat att ett modernare uttryckssätt än utlämnande på medium för automatiserad behandling är att föredra och att det i samband med översynen av registerförfattningarna på brottsdatalagens område var lämpligt att göra den förändringen.[168] Vi bedömer att termen medium för automatiserad behandling bör utmönstras även ur övrig kompletterande dataskyddsreglering, till förmån för begreppet elektroniskt utlämnande. Det innebär också att nya former av elektroniskt utlämnande som vi i dag inte känner till, men som kan komma att följa av den tekniska utvecklingen, också omfattas av bestämmelsen. Författningarna kommer därför inte att behöva ändras för att följa med den tekniska utvecklingen på området.

För att upprätthålla ett adekvat skydd för den personliga integriteten vid utlämnande i elektronisk form är det viktigt att inte fler uppgifter än nödvändigt lämnas ut och att utlämnandet sker på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling, genom lämpliga tekniska eller organisatoriska åtgärder. Detta är krav som i dag följer direkt av dataskyddsförordningen (se avsnitt 3.4). Bedömningar av detta slag måste därför anses vara en naturlig del i myndigheters verksamhet där utlämnandefrågor aktualiseras.

För att uppnå en ändamålsenlig avvägning mellan myndigheternas intresse av att på ett effektivt sätt lämna ut personuppgifter i elektronisk form och risker med att överföra uppgifter elektroniskt innehåller kompletterande dataskyddsreglering ofta en bestämmelse som anger när sådant utlämnande får ske. Den formulering som ofta har valts i modernare författningar är att elektroniskt utlämnande (på annat sätt än genom direktåtkomst) får ske om det inte är olämpligt.[169]

[168] Prop. 2017/18:269, *Brottsdatalag – kompletterande lagstiftning*, s. 136.
[169] Jfr t.ex. 19 § första stycket kustbevakningsdatalagen (2019:429), 1 kap. 9 § lagen om Rättsmedicinalverkets behandling av personuppgifter och 2 kap. 9 § första stycket lagen (2018:1694) om Tullverkets behandling av personuppgifter inom brottsdatalagens område.

I den föreslagna lagen om användning av myndighetsgemensam infrastruktur för digital post finns också motsvarande reglering, dvs. att elektroniskt utlämnande bara får ske om det inte finns säkerhetsskäl eller andra skäl som talar emot det, alternativt om ett sådant utlämnande framstår som lämpligt.[170]

I syfte att dels uppmärksamma behovet av nödvändiga överväganden innan ett elektroniskt utlämnande, dels utforma regleringen så enhetligt som möjligt, föreslår vi att de tillåtande bestämmelserna om elektroniskt utlämnande på annat sätt än genom direktåtkomst ska förenas med ett krav på att utlämnande på detta sätt inte ska vara olämpligt.

Den äldre regleringsmodellen har i vissa fall fått till följd att det förekommer långa uppräkningar av till vilka aktörer uppgifter får lämnas ut elektroniskt på annat sätt än genom direktåtkomst. Bestämmelsen som vi föreslår är i stället generellt tillämplig inom ramen för respektive författnings tillämpningsområde. I kompletterande dataskyddsreglering där tillåtligheten av elektroniskt utlämnande på annat sätt än genom direktåtkomst regleras särskilt för varje mottagare kommer ett sådana bestämmelser behöva upphävas, för att undvika dubbelreglering och åstadkomma en tydlig och ändamålsenlig reglering.

Den föreslagna bestämmelsen ska inte tolkas som att den medför en rätt för vare sig mottagande myndigheter eller enskilda att få ut uppgifter genom någon form av elektronisk informationsöverföring. Bestämmelsen innebär därmed inte heller någon generell eller specifik skyldighet att lämna ut uppgifter på ett visst sätt eller i ett visst format (jfr avsnitt 5.6.1 om det s.k. utskriftsundantaget i 2 kap. 16 § TF vad gäller utlämnande till enskilda). Det är t.ex. inte säkert att en avvägning mellan behovet och riskerna i *alla tänkbara fall* medger att uppgifter över huvud taget lämnas ut elektroniskt. Den föreslagna bestämmelsen är följaktligen inte tvingande för myndigheterna avseende att lämna ut personuppgifter elektroniskt. Det som bestämmelsen innebär är dock att myndigheterna inte är rättsligt förhindrade att använda sig av olika elektroniska former för informationsöverföring, så länge dessa inte utgör direktåtkomst.

Bestämmelsen innebär alltså att den myndighet som innehar uppgifter som den får eller måste lämna ut också har en rättslig möjlighet att göra det elektroniskt, om det framstår som lämpligt i för-

[170] SOU 2024:47, *Digital myndighetspost*, s. 29.

hållande till de omständigheter som är aktuella, och inte utgör ett utlämnande genom direktåtkomst.

Bestämmelsen kommer att vara tillämplig oavsett omfattningen av utlämnandet. Den kan alltså komma att ligga till grund för regelmässiga och stora informationsflöden mellan myndigheter i ett särskilt system. När det övervägs på vilket sätt information ska överföras elektroniskt måste det, som vid all annan behandling, enligt dataskyddsförordningen göras ett flertal avvägningar mellan de intressen som talar för en viss teknisk lösning, och de integritetsskäl som talar emot (se avsnitt 3.4). När ett nytt system för regelbundet eller omfattande informationsutbyte utarbetas bör i normalfallet både den utlämnande och den mottagande myndigheten vara delaktiga i arbetet, oavsett hur systemet klassificeras rättsligt. Det bör exempelvis krävas gemensamma överväganden i fråga om vilka faktiska uppgifter mottagaren har ett behov av, hur dessa lämpligen ska avgränsas, hur kommunikationen mellan de olika it-systemen ska fungera och vilka övriga villkor som ska gälla för utlämnandet, innan ett uppgiftslämnande påbörjas. Den tekniska lösning som myndigheterna utarbetar ska bl.a. utformas så att principerna för dataskydd iakttas vid behandlingen. I den mån principerna för dataskydd inte bedöms kunna iakttas vid en särskild form av informationsöverföring måste en annan form väljas.

Med det nyss sagda avses inte att varje enskild informationsöverföring ska kräva omfattande bedömningar, utan att myndigheterna bör överväga de aspekter som är väsentliga ur integritetssynpunkt t.ex. vid inrättande av nya system för överföring, eller när nya skyldigheter eller möjligheter att lämna ut uppgifter införs. Riskerna med att överföra uppgifter elektroniskt, som bl.a. kan bestå i en ökad fara att uppgifter sprids eller att någon annan än den avsedda mottagaren får del av uppgifterna, måste då vägas mot de inblandade myndigheternas behov av effektiva arbetssätt. Myndigheterna måste också beakta principen om uppgiftminimering som framgår av artikel 5.1 c i dataskyddsförordningen och som innebär att personuppgifter inte får vara för omfattande i förhållande till de ändamål för vilka de behandlas. Vid elektroniskt utbyte av känsliga uppgifter i den mening som avses i artikel 9.1 i dataskyddsförordningen bör integritets- och informationssäkerhetsfrågor ges en särskild betydelse när formen för ett elektroniskt informationsutbyte övervägs.

Trots det som anges ovan bör påpekas att regeringen i tidigare lagstiftningsärenden har varit av uppfattningen att det normalt sett aldrig bör anses olämpligt att lämna ut personuppgifter elektroniskt till andra myndigheter.[171] I normalfallet bör det därför inte heller i fortsättningen anses olämpligt att lämna ut personuppgifter elektroniskt på annat sätt än genom direktåtkomst till andra myndigheter. Detsamma borde i de allra flesta fall gälla för enskilda. Här kan åter nämnas att det finns förslag på lagstiftning som kräver att statliga och kommunala myndigheter kommunicerar med enskilda digitalt, om det inte finns säkerhetsskäl eller andra skäl som talar emot det.[172]

När det gäller utlämnande till enskilda kan det dock krävas närmare överväganden bl.a. med hänsyn till vem mottagaren är och vilken säkerhet mottagaren har för sin personuppgiftsbehandling. Om det i ett enskilt fall skulle bedömas vara olämpligt ur integritetssynpunkt att lämna ut personuppgifter elektroniskt, dvs. att principerna för dataskydd inte kan iakttas vid ett sådant utlämnande, bör uppgifterna lämnas ut på annat sätt. Det nyss sagda gäller även för utlämnande till myndigheter. Om mottagaren av uppgifterna kan antas komma att behandla uppgifterna på ett sätt som står i strid med bl.a. dataskyddsförordningen gäller dock sekretess för uppgifterna enligt 21 kap. 7 § OSL. I sådana fall får uppgifterna inte över huvud taget lämnas ut, vare sig i analog form eller elektroniskt.

[171] Jfr t.ex. prop. 2017/18:269, *Brottsdatalag – kompletterande lagstiftning*, s. 136. Se även SOU 2015:39, *Myndighetsdatalag*, s. 447 och 448.
[172] Se förslaget till lag om användning av myndighetsgemensam infrastruktur för digital post i SOU 2024:47, *Digital myndighetspost*, s. 29.

6 Skyddet för den personliga integriteten

6.1 Inledning

6.1.1 Våra förslag

Vi har förslagit en förändring av offentlighets- och sekretesslagen (2009:400), OSL, som på ett generellt plan påverkar myndigheters möjligheter att samverka och utbyta information. Förslaget innebär att det ska införas en ny generell bestämmelse, 6 kap. 5 a § OSL, som kompletterar den befintliga regleringen i 6 kap. 5 § samma lag, men som till skillnad från den bestämmelsen inte kräver en begäran från mottagaren och som inte heller innebär att den utlämnande myndigheten åläggs en skyldighet att lämna uppgifter till andra myndigheter. Bestämmelsens syfte är att ge myndigheter ett uttryckligt rättsligt stöd för att på eget initiativ lämna uppgifter som inte är sekretessbelagda till andra myndigheter, om utlämnandet kan antas vara av betydelse för att den utlämnande eller den mottagande myndigheten ska kunna fullgöra sin författningsreglerade verksamhet, se avsnitt 4.8.5.

Vi har även föreslagit vissa förtydliganden av gällande rätt vad gäller myndigheters informationsutbyte. Förslaget innebär att det i dataskyddsreglering som, med något undantag, kompletterar dataskyddsförordningen[1] på sektors- eller myndighetsnivå ska införas upplysningsbestämmelser som tydliggör att personuppgifter får behandlas i enlighet med offentlighets- och sekretesslagens bestämmelser (avsnitt 5.4.6). Vi har också föreslagit att det inte ska göras någon dataskyddsrättlig åtskillnad mellan olika former av sekre-

[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).

tessbrytande bestämmelser i brottsdatalagen (2018:1177), BDL, se avsnitt 5.5.2.

Slutligen har vi i avsnitt 5.6.3 föreslagit att omotiverade hinder mot att myndigheter utbyter uppgifter elektroniskt på annat sätt än genom direktåtkomst ska upphävas i den mån sådan reglering förekommer i den kompletterande dataskyddsregleringen. I det sammanhanget har vi föreslagit att elektroniskt utlämnande på annat sätt än genom direktåtkomst ska vara tillåtet om det inte är olämpligt.

Det övergripande syftet med samtliga förslag är att förtydliga vad som redan gäller enligt offentlighets- och sekretesslagen avseende förbud att röja uppgifter och undantag från dessa förbud. Förslagen syftar också till att anpassa regleringen i offentlighets- och sekretesslagen till det allmänna dataskyddsrättliga regelverket. Genom en reglering som är tydlig och fri från synbara konflikter och motsägelser kan myndigheternas möjligheter att samverka och, som en del av samverkan, utbyta information med varandra förbättras. Som ett resultat av våra förslag kan särskilt utbytet av personuppgifter förväntas bli mindre komplicerat för tillämparen och därmed utökas.

6.1.2 Kapitlets disposition

I detta kapitel redogör vi för vår analys av förslagens inverkan på den personliga integriteten. Eftersom det huvudsakligen är förslaget om en ny generell bestämmelse om utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ som innebär en sådan förändring av gällande rätt som påverkar enskildas rätt till skydd för personuppgifter fokuserar vi våra överväganden på det förslaget.

I avsnitt 6.2 gör vi några inledande anmärkningar som bl.a. avser förhållandet till integritetanalysen i vårt delbetänkande.

Vi redogör därefter för de integritetsrisker som vi har identifierat och som är förknippade med föreslaget om utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ (avsnitt 6.3). Därefter redogör vi i avsnitt 6.4 för vår bedömning av förslagets sammantagna proportionalitet.

I avsnitt 6.5 görs sedan överväganden om våra förslag om förändringar i den kompletterande dataskyddsregleringen och brottsdatalagen.

6.2 Några inledande anmärkningar

6.2.1 Delbetänkandet

En viktig del i integritetsanalysen vid lagstiftningsarbete är bedömningen av om konsekvenserna för den personliga integriteten är nödvändiga och proportionerliga i förhållande till det man avser att uppnå med lagstiftningsåtgärden. Som redan nämnts avhandlar vi frågan om proportionalitet särskilt i avsnitt 6.4 nedan. En förutsättning för att vi ska kunna göra en proportionalitetsbedömning är dock att det sker en kartläggning av integritetsriskerna. I Integritetsskyddsmyndighetens, IMY, *Vägledning för integritetsanalys i lagstiftningsarbete* (dnr IMY-2022-10835) ges instruktioner om hur integritetsrisker kan identifieras. Med stöd av vägledningen redogör vi nedan för vad en bestämmelse som möjliggör utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ, till andra myndigheter, innebär i fråga om integritetsrisker för enskilda.

I kapitel 6 i vårt delbetänkande SOU 2023:63, *Ökat informationsutbyte mellan myndigheter. Behov och föreslagna förändringar* föreslog vi att det skulle införas en ny generell sekretessbrytande bestämmelse i offentlighets- och sekretesslagen. I integritetshänseende finns det både stora likheter och väsentliga skillnader mellan förslaget om en generell sekretessbrytande bestämmelse och förslaget om en bestämmelse om utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ. De mest framträdande likheterna är att båda förslagen kan förväntas medföra en utökad personuppgiftsbehandling i samband med informationsutbyte mellan myndigheter och att det inte finns någon egentlig begränsning av vilka uppgiftskategorier som kan komma att utbytas. I princip alla uppgifter som myndigheter behandlar kan nämligen vara ”inte sekretessbelagda” beroende på i vilket sammanhang de förekommer, t.ex. i ett offentliggjort beslut. Den mest framträdande skillnaden är att förslaget om utlämnande på eget initiativ inte bryter sekretess, dvs. att det inte görs några nya undantag från befintliga förbud mot att röja en uppgift genom bestämmelsen.

I kapitel 10 i delbetänkandet redogjorde vi för vår analys av de integritetsrisker som är förknippade med vårt förslag om en generell sekretessbrytande bestämmelse, och vår bedömning av det förslagets proportionalitet. För att illustrera likheterna och skillnaderna mellan förslagen har vi valt att i detta sammanhang utgå från strukturen och innehållet i kapitel 10 i vårt delbetänkande. Det innebär att detta

kapitel kommer att innehålla vissa upprepningar i förhållande till delbetänkandet. Vår bedömning är dock att fördelarna med en tydlig och enhetlig bedömning i frågor om integritetsrisker och förslagens proportionalitet överväger nackdelarna med en upprepning.

Däremot upprepas inte i detta sammanhang vad som framgår av kapitel 3 i delbetänkandet, dvs. en grundläggande beskrivning av gällande regler om personlig integritet, dataskydd och sekretess. Inte heller upprepas i detta kapitel redogörelsen för proportionalitetsprincipen och relevant reglering, de europeiska domstolarnas roll i frågor om proportionalitet och hur vår proportionalitetsbedömning ska genomföras. I detta avseende hänvisas till avsnitt 10.3.1 i SOU 2024:63.

6.2.2 ”På eget initiativ”

Uppgifter som inte är sekretessbelagda är sådana som det inte finns något förbud mot att lämna ut (röja) enligt sekretessregleringen (jfr avsnitt 4.3). Myndigheter har redan i dag en långtgående skyldighet enligt 6 kap. 5 § OSL att på begäran av en annan myndighet lämna ut sådana uppgifter. Vårt förslag om en bestämmelse som ska komplettera 6 kap. 5 § OSL innebär att myndigheter också kommer att få ett uttryckligt rättsligt stöd för att *på eget initiativ* lämna ut relevanta uppgifter som annars inte är sekretessbelagda till andra myndigheter. I dag är ett sådant utlämnande bara tillåtet om det finns en tillämplig bestämmelse om uppgiftsskyldighet som kräver att den utlämnande myndigheten på eget initiativ lämnar uppgifter till en annan myndighet (jfr avsnitt 4.6). Eftersom samtliga uppgifter som kan komma att lämnas ut med stöd av den föreslagna bestämmelsen är sådana som inte omfattas av något röjandeförbud och som den utlämnande myndigheten redan har en långtgående skyldighet att lämna ut på begäran, bör det vara omständigheten att de nu kan lämnas *på eget initiativ* som är av betydelse vid bedömningen av integritetsriskerna och bestämmelsens proportionalitet. I de kommande avsnitten är det därför den aspekten av förslaget som vi lägger vikt vid.

6.3 Integritetsrisker vid utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ

6.3.1 En generellt förhöjd integritetsrisk

Vår bedömning: En generell bestämmelse om utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ innebär en generellt förhöjd risk för intrång i den personliga integriteten (integritetsrisk).

Skälen för vår bedömning

Vad avses med integritetsrisk?

Den i avsnitt 4.8.5 föreslagna bestämmelsen möjliggör utlämnande på eget initiativ av personuppgifter, dvs. uppgifter som avser en identifierad eller identifierbar fysisk person (artikel 4.1 i dataskyddsförordningen) som inte är sekretessbelagda. Insamlande och utlämnande är exempel på åtgärder som utgör behandling av personuppgifter. Personuppgiftsbehandling är dock ett vidsträckt begrepp som även omfattar registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring av personuppgifter (artikel 4.2 i dataskyddsförordningen).

Vid personuppgiftsbehandling måste flera regelverk följas för att värna den personliga integriteten. Någon enhetlig definition av begreppet personlig integritet finns dock inte. En kränkning av den personliga integriteten har bl.a. beskrivits som ett intrång i en fredad sfär som den enskilde bör vara tillförsäkrad och där ett oönskat intrång, såväl psykiskt som fysiskt, bör kunna avvisas.[2]

Uppfattningen om vad som är en personlig sfär varierar dock mellan olika kulturer och miljöer. Inställningen till den personliga integriteten ändras dessutom över tid, vilket bl.a. den utbredda användningen av sociala medier under det senaste decenniet vittnar om (jfr avsnitt 5.2.3). En rimlig utgångspunkt för bedömningen av vad

[2] Prop. 2005/06:173, *Översyn av personuppgiftslagen*, s. 15.

som utgör en integritetsrisk borde därför kunna vara den enskildes intresse av att skydda information om sina personliga förhållanden.[3]

Det finns inte någon definition av vad begreppet integritetsrisk rent konkret innebär i dataskyddsförordningen. Däremot anges exempel på när risker typiskt sett kan uppkomma i skäl 75 till dataskyddsförordningen. Det är bl.a. vid följande situationer:

- Personuppgiftsbehandling som inbegriper ett stort antal personuppgifter och gäller ett stort antal registrerade.
- Behandling av känsliga personuppgifter.
- Behandling av personuppgifter om sårbara fysiska personer, framför allt barn.
- Behandling av uppgifter om fällande domar i brottmål samt lagöverträdelser som innefattar brott eller därmed sammanhängande säkerhetsåtgärder.
- Personuppgiftsbehandling som skulle kunna medföra
  - ekonomisk förlust, skadat anseende eller annan betydande ekonomisk eller social nackdel,
  - förlust av konfidentialitet när det gäller personuppgifter som omfattas av tystnadsplikt, eller
  - hinder mot registrerades möjlighet att utöva kontroll över sina personuppgifter. Hur sannolik och allvarlig risken är ska enligt skäl 76 till dataskyddsförordningen fastställas utifrån behandlingens art, omfattning, sammanhang och ändamål.

En generellt förhöjd risk för intrång i den personliga integriteten

Genom den allmänna dataskyddsregleringen, kompletterande dataskyddsreglering, det förvaltningsrättsliga regelverket m.m. är myndigheter sammanfattningsvis förhindrade att behandla andra eller fler personuppgifter än de som behövs för att utföra sina respektive författningsreglerade verksamheter, vilket vi bl.a. redogjort för i avsnitten 3.2 och 3.3 i vårt delbetänkande. Den begränsningen är också

[3] Jfr regeringens uttalanden i prop. 2009/10:80, *En reformerad grundlag*, s. 175.

ett utflöde av legalitetsprincipen, dvs. att myndigheters agerande, även vad gäller att behandla personuppgifter, måste ha stöd i rättsordningen.

När sekretess först infördes mellan myndigheter gjordes uttalanden i propositionen om att ett fullgott skydd för den personliga integriteten krävde att en uppgift inte spreds utanför det sammanhang där den inhämtats. Hos en annan myndighet kunde uppgiften nämligen ligga till grund för åtgärder som hade en negativ innebörd för den enskilde, och ett större antal personer skulle dessutom kunna få kunskap om ett känsligt förhållande. Att det fanns lagstöd för åtgärderna hos den andra myndigheten spelade i sig ingen roll för frågan om ett fullgott integritetsskydd.[4]

Att vi nu diskuterar utbyte av uppgifter som inte är sekretessbelagda gör inte det uttalandet mindre relevant. Som vi redogjort för i avsnitt 4.7.1 är frågan om en uppgift är sekretessbelagd eller inte något som många gånger avgörs i en konkret utlämnandesituation och svaret kan därför påverkas bl.a. av vem som är mottagare, förekomsten av sekretessbrytande bestämmelser och bestämmelser om undantag från sekretess. Det rättsliga förhållandet att en uppgift inte är sekretessbelagd i förhållande till en annan myndighet är alltså i många fall ett situationsbundet rättsligt tillstånd som enbart innebär att det inte råder något förbud mot att röja uppgiften *i den aktuella situationen*. Det går alltså inte att i alla fall rakt av likställa det faktum att uppgifter inte är sekretessbelagda med att de inte är känsliga ur integritetssynpunkt.

Samtliga omständigheter som enligt dataskyddsförordningen kan medföra en förhöjd risk för integritetsintrång kan dessutom direkt eller indirekt aktualiseras av en generell bestämmelse som ger myndigheter förbättrade möjligheter till utbyte av uppgifter som inte är sekretessbelagda. Detta kan även gälla förlust av konfidentialitet, eftersom sekretess som kan gälla i förhållande till andra än mottagaren inte alltid följer med en uppgift när den lämnats till en annan myndighet, vilket kan leda till ett svagare sekretesskydd hos mottagaren än hos den utlämnande myndigheten.

I regel innebär ett informationsutbyte mellan myndigheter dessutom att uppgifter behandlas för ett annat ändamål än det som uppgifterna samlades in för, dvs. att uppgifter sprids utanför det sammanhang där de inhämtats och för andra syften än det ursprungliga. Oavsett uppgifternas sekretessrättsliga status aktualiseras därmed

[4] Prop. 1979/80:2, *med förslag till sekretesslag m.m.*, s. 90.

en av de grundläggande principerna för behandlingen enligt dataskyddsförordningen, dvs. principen om ändamålsbegränsning som framgår av artikel 5.1 b (finalitetsprincipen) jfr avsnitt 3.2.

I många fall innebär ett utlämnande till en annan myndighet också att den uppgift som utbyts ligger till grund för kontroller av enskildas rätt till olika förmåner eller skyldighet att betala skatt, vilket kan uppfattas som negativt av enskilda. Regeringen har t.ex. bedömt att en hantering av uppgifter som syftar till att utreda brott kan normalt anses vara mer känslig än en hantering som uteslutande sker för att ge en myndighet underlag för förbättringar av kvaliteten i handläggningen. Även uppgiftssamlingar som används som underlag för att fatta beslut som direkt rör den enskilde kan enligt regeringen uppfattas som mer ingripande.[5] Visst informationsutbyte mellan myndigheter som inbegriper uppgifter som inte är sekretessbelagda kan vidare innebära att fler personer får kännedom om ett känsligt förhållande. Det kan t.ex. vara fallet om uppgifter om hälsa ingår i ett beslut.

Att ett utlämnande är påkallat för att fullgöra författningsreglerad verksamhet, och därför motiveras av ett viktigt allmänt intresse[6], är alltså inte avgörande för bedömningen av om det uppkommer ett integritetsintrång eller inte. Integritetsintrånget sker redan när uppgifter om enskilda personer behandlas. Däremot kan syftet med integritetsintrånget få betydelse för frågan om intrånget är berättigat eller inte.

I vår kartläggning har vi kunnat se att bristen på rättsligt stöd för att lämna ut uppgifter på eget initiativ är ett av de mer framträdande hindren mot efterfrågat informationsutbyte mellan myndigheter (jfr avsnitt 4.7). En stor del av dessa hinder kommer att upphävas vid införandet av den sekretessbrytande bestämmelse som vi föreslår i vårt delbetänkande. Även den nu föreslagna bestämmelsen, som träffar uppgifter som annars inte är sekretessbelagda, kan resultera i en utökad personuppgiftsbehandling. När uppgifter som i dag endast kan lämnas ut på begäran också kommer att kunna lämnas ut på den utlämnande myndighetens eget initiativ finns dessutom en risk att den utlämnande myndigheten felbedömt mottagarens behov av uppgifterna. Ett utlämnande på eget initiativ kan alltså

[5] Prop. 2020/21:124, *Transportstyrelsens olycksdatabas*, s. 16.
[6] Jfr prop. 2017/18:105, *Ny dataskyddslag*, s. 83.

medföra en ökad personuppgiftsbehandling som senare inte visar sig vara nödvändig för det tänkta syftet.

Vår bedömning är därför att en bestämmelse som ger myndigheter ett tydligt rättsligt stöd för att lämna ut uppgifter som inte är sekretessbelagda på eget initiativ innebär en generell förhöjd risk för intrång i den personliga integriteten (integritetsrisk).

6.3.2 Utökad och ny personuppgiftsbehandling

Vår bedömning: En generell bestämmelse om utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ kan komma att medföra en utökad personuppgiftsbehandling vid ett stort antal myndigheter. Det kommer även att kunna medföra viss ny personuppgiftsbehandling.

Skälen för vår bedömning

Både utökad och viss ny behandling

Förslaget om en bestämmelse om utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ innebär inte *i sig* att myndigheter kommer att vara skyldiga att utföra någon ny eller utökad personuppgiftsbehandling. I avsnitt 4.7 har vi dock redogjort för att det både efterfrågas utökade möjligheter att på eget initiativ lämna ut information om enskilda till andra myndigheter och att på den andra myndighetens eget initiativ få del av sådana uppgifter som andra myndigheter förfogar över. Det är därför rimligt att anta att den föreslagna bestämmelsen också kommer att användas för sådant informationsutbyte som efterfrågas, dvs. uppgiftslämnande på eget initiativ i syfte att myndigheter ska kunna fatta riktiga beslut eller i övrigt utföra sin verksamhet. Det motsvarar också behovsrekvisiten i den föreslagna bestämmelsen.

För samtliga uppgifter som träffas av den föreslagna bestämmelsen, dvs. uppgifter som inte är sekretessbelagda, finns det i och för sig redan en långtgående skyldighet att lämna ut dessa på begäran (6 kap. 5 § OSL). För att myndigheter ska kunna lämna ut uppgifter med stöd av bestämmelsen om utlämnande på eget initiativ behöver de dock behandla personuppgifter i större utsträckning än vad de gör

i dag. I de fall uppgifterna träffas av en sekretessbrytande bestämmelse i offentlighets- och sekretesslagen finns det förvisso redan ett rättsligt stöd för utlämnande på eget initiativ, som dock inte är särskilt tydligt (jfr avsnitt 4.8.2). Det kan därför antas att den föreslagna bestämmelsen, som i detta avseende enbart förtydligar vad som redan gäller, kommer att medföra en utökad personuppgiftsbehandling med stöd av befintliga sekretessbrytande bestämmelser i offentlighets- och sekretesslagen.

Med hänsyn till den breda definitionen av personuppgiftsbehandling är det inte bara själva utlämnandet till en annan myndighet som utgör en behandling av personuppgifter. Även en rad åtgärder som behöver vidtas inför ett utlämnande kommer att medföra personuppgiftsbehandling, t.ex. strukturering, kontroll, bearbetning och justering av uppgifter. Dessa former av behandling sker redan i dag när en begäran enligt 6 kap. 5 § OSL inkommer. Att samma uppgifter, dvs. uppgifter som inte är sekretessbelagda, nu också kommer att få lämnas ut på eget initiativ innebär dock att dessa olika former av behandling kommer att öka.

Även mottagande myndigheter kommer att behandla personuppgifter i större utsträckning än vad de gör i dag. Mottagande myndigheter kommer att ta emot och därefter bearbeta uppgifterna som de får från andra myndigheter. Det kommer dessutom krävas inledande överväganden om personuppgifter ska raderas hos den mottagande myndigheten, eller om det finns ett legitimt behov av uppgifterna i verksamheten. Därtill kommer det arkivrättsliga regelverket, som bl.a. medför att mottagande myndigheter som utgångspunkt måste behandla inkomna uppgifter i sina arkiv.

Sammanfattningsvis kommer myndigheter behandla personuppgifter i flera led när uppgifter som inte är sekretessbelagda utbyts med stöd av bestämmelsen om utlämnande på eget initiativ. Det kommer dock i regel inte vara fråga om någon ny personuppgiftsbehandling, utan en *utökad* behandling, i jämförelse med den behandling i form av utlämnande på begäran och annan behandling som är förknippad med utbytet, som sker i dag. Eftersom själva utlämnandet i dag i många fall är tillåtet först efter en begäran kommer det även kunna uppstå situationer som är att likställa med en helt ny personuppgiftsbehandling. Det är i de fall uppgifterna i och för sig inte är sekretessbelagda men inte heller tidigare har begärts ut eller lämnats ut med stöd av en sekretessbrytande bestämmelse.

När det inte längre är en *begäran* som kommer att vara avgörande för om uppgifter som inte är sekretessbelagda får lämnas till en annan myndighet, utan det antagna *behovet* av utlämnandet, kommer personuppgiftsbehandlingen inom den offentliga sektorn med stor sannolikhet att öka. En utökad, eller ny, personuppgiftsbehandling innebär i sig ökade integritetsrisker. Bestämmelsen om utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ utgör dock inte en rättslig grund för en myndighet att behandla andra eller fler personuppgifter än sådana som är motiverade av myndighetens ordinarie verksamhet.

Övervakning eller kartläggning?

Även om myndigheter i regel inte kan förväntas ha närmare kännedom om behoven hos andra myndigheter är tröskeln för utlämnande med stöd av den föreslagna bestämmelsen lågt satt. Det som krävs är att uppgifterna inte är sekretessbelagda och att utlämnandet *kan antas* vara av betydelse för att antingen den mottagande eller den utlämnande myndigheten ska kunna fullgöra sin författningsreglerade verksamhet. Den föreslagna bestämmelsen innebär att myndigheter kommer att kunna få del av uppgifter om enskilda utan att ha framställt en begäran om det. Mottagandet av uppgifter som i och för sig inte är sekretessbelagda, men som tidigare varit okända för den mottagande myndigheten och därför inte begärts ut, kommer medföra att en ökad mängd uppgifter kan komma att ansamlas hos myndigheterna.

En ökad mängd uppgifter medför en utökad möjlighet att ”lägga pussel” hos den mottagande myndigheten. Med det avses att flera olika, var för sig harmlösa, uppgifter om en människa kan ge en mer heltäckande bild av vederbörandes livssituation och förehavanden än om uppgifterna hålls åtskilda. Det skulle t.ex. kunna bli möjligt att genom ett sådant pusselläggande få en mer detaljerad bild av en persons relationer med andra människor, intressen, resor, politisk eller religiös tillhörighet och privatekonomi. Beroende på syftet med pusselläggandet kan en myndighet också få en mer heltäckande bild av personers förehavanden som indikerar involvering i t.ex. brottslig verksamhet. Att en större mängd uppgifter med stöd av bestämmelsen kan komma att lämnas till en annan myndighet utan begäran bör alltså *i sig* utgöra en integritetsrisk.

Enligt regeringsformen, RF, måste en myndighet ha stöd i lag för sådan personuppgiftsbehandling som utgör ett betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden (jfr 2 kap. 6 § andra stycket och 20 § RF). Rätten till skydd mot betydande intrång i den personliga integriteten är alltså inte absolut utan kan begränsas. Det finns dock vissa krav som måste uppfyllas för att en sådan begränsning ska vara godtagbar, vilket framgår av 2 kap. 21 § RF. En begränsning får enligt den nyss nämnda bestämmelsen göras endast för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. Begränsningen får vidare aldrig gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den, och inte heller sträcka sig så långt att den utgör ett hot mot den fria åsiktsbildningen såsom en av folkstyrelsens grundvalar. Begränsningen får vidare inte göras enbart på grund av politisk, religiös, kulturell eller annan sådan åskådning.

Enligt motiven till bestämmelsen i 2 kap. 6 § andra stycket RF är det avgörande för om en åtgärd ska anses innebära övervakning eller kartläggning inte dess huvudsakliga syfte, utan vilken effekt åtgärden har. Vad som avses med övervakning respektive kartläggning får bedömas med utgångspunkt från vad som enligt normalt språkbruk läggs i dessa begrepp.[7] Vad gäller begreppet kartläggning av den enskildes personliga förhållanden anges bl.a. följande i förarbetena.[8]

> En åtgärd från det allmännas sida som vidtas primärt i syfte att ge myndigheterna underlag för beslutsfattande i enskilda fall, exempelvis insamling av uppgifter av visst slag för beslut om t.ex. beskattning eller liknande, kan – även om avsikten inte är att kartlägga enskilda – i många fall anses innebära kartläggning av enskildas förhållanden. Så torde fallet vara i fråga om ett stort antal uppgiftssamlingar som det allmänna förfogar över. En mycket stor mängd information som rör enskildas personliga förhållanden finns t.ex. lagrad i Skatteverkets, Tullverkets, Försäkringskassans och Kronofogdemyndighetens olika databaser. […] Flera av dessa uppgiftssamlingar omfattar en stor andel av landets hela befolkning och flera av dem innehåller också till viss del mycket integritetskänsliga uppgifter. […] I flertalet fall är uppgifterna tillgängliga för myndigheterna på sådant sätt att lagringen och behandlingen av uppgifterna kan sägas innebära att enskilda kartläggs, även om det huvudsakliga ändamålet med behandlingen är ett helt annat.

[7] Prop. 2009/10:80, *En reformerad grundlag*, s. 250.
[8] Prop. 2009/10:80, *En reformerad grundlag*, s. 180.

För sådan omfattande personuppgiftsbehandling som exemplifieras i citatet ovan krävs alltså särskilt lagstöd, oavsett om myndighetens syfte med behandlingen är att övervaka och kartlägga enskilda, eller att fatta riktiga beslut eller på annat sätt utföra sin verksamhet.

I förarbetena till 2 kap. 6 § andra stycket RF noterade regeringen emellertid också att det förekommer ingrepp i enskildas integritet av varierande karaktär, intensitet och omfattning. För att grundlagsbestämmelsen inte skulle innebära ett hinder mot sådan lagstiftning som behövs till skydd för viktiga samhällsintressen eller lagstiftning som utgör ett led i anpassningen av normerna till den fortgående samhällsutvecklingen menade regeringen att det grundlagsskyddade området borde avgränsas på ett sådant sätt att det enbart omfattade de mest ingripande intrången. Det utökade rättighetsskyddet borde utformas så att det tog sikte på att skydda den personliga integriteten mot vissa intrång som kan anses vara särskilt känsliga.[9]

I vårt delbetänkande gjorde vi därför sammanfattningsvis bedömningen att en generell sekretessbrytande bestämmelse, som inte innebär en skyldighet att lämna uppgifter till en annan myndighet, inte *i sig* aktualiserar det utökade grundlagsskyddet (jfr avsnitt 10.2.4 i SOU 2024:63). Inte heller bestämmelsen om utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ utgör någon skyldighet att lämna uppgifter till en annan myndighet. Någon sekretess bryts dessutom inte av bestämmelsen. De bedömningar som redogörs för i delbetänkandet bör därför i relevanta delar vara aktuella även här.

Samtidigt går det inte att bortse från att vår tidigare föreslagna sekretessbrytande bestämmelse och den nu aktuella bestämmelsen, inte minst sammantaget och tillsammans med våra övriga förslag, kan få följder som motsvarar de omständigheter som det lagts särskild vikt vid när det utökade grundlagsskyddet aktualiserats på grund av införandet av nya uppgiftsskyldigheter.

I förarbetena till lagen (2024:307) om uppgiftsskyldighet för att motverka felaktiga utbetalningar från välfärdssystemen samt fusk, regelöverträdelser och brottslighet i arbetslivet (LUFFA-lagen) gjorde regeringen en sammantagen bedömning av följderna av uppgiftsskyldigheten enligt den lagen. Det avsåg bl.a. en ökad spridning av uppgifter, vilket gav en risk för att en större mängd information om en enskild individ samlades hos den aktör som mottagit uppgifterna.

[9] Prop. 2009/10:80, *En reformerad grundlag*, s. 177 och 182.

Uppgiftsskyldigheten kunde därmed enligt regeringen anses *bidra till* kartläggning av den enskildas personliga förhållanden. Sammantaget ansågs detta innebära ett så betydande intrång i den personliga integriteten som avses i 2 kap. 6 § andra stycket RF.[10]

I förarbetena till lagen (2025:170) om skyldighet att lämna uppgifter till de brottsbekämpande myndigheterna delade regeringen den bedömning som utredningen hade gjort i betänkandet som föregick propositionen.[11] Där hade bl.a. konstaterats att uppgiftsskyldighet enligt lagen innebar en *väsentlig förskjutning* i balansen mellan en effektiv brottsbekämpning och skyddet för den personliga integriteten. Utredningen la också vikt vid bl.a. syftet med uppgiftsskyldigheten och att den *i förlängningen* leder till ny och utökad personuppgiftsbehandling i den brottsbekämpande verksamheten. Uppgiftsskyldigheten till de brottsbekämpande myndigheterna bedömdes sammantaget medföra ett betydande intrång i den personliga integriteten, som skulle komma att ske utan samtycke och innebära kartläggning av enskildas personliga förhållande.[12]

Sammanfattningsvis framgår av förarbetena till de ovan angivna lagarna att det inte enbart är en *faktisk åtgärd* som innebär en kartläggning eller övervakning av enskilda (t.ex. förandet av en uppgiftssamling) som träffas av det utökade grundlagsskyddet. Beroende på omständigheterna kan det i stället vara tillräckligt att en lagstiftningsåtgärd om informationsutbyte mellan myndigheter kan *bidra till* att enskilda kartläggs, även om detta sker hos andra myndigheter än de som faktiskt kommer tillämpa regleringen vid ett utlämnande. I likhet med vad som anges ovan innebär också våra förslag om förändringar av offentlighets- och sekretesslagen sammantaget en väsentlig förskjutning i balansen mellan effektiviteten i den offentliga förvaltningen och integritetsintresset. Taget för sig kan förslaget om egeninitierat utlämnande av uppgifter vidare få som resultat att uppgifter sprids och samlas in på ett sätt som kan bidra till, eller i förlängningen resultera i, att enskilda kartläggs i sådan omfattning att det utgör ett betydande intrång i den personliga integriteten.

Det bör dock åter påpekas att den nu aktuella bestämmelsen enbart möjliggör utlämnande på eget initiativ av *samma* uppgifter som det i dag redan finns en skyldighet att lämna ut på begäran. Som vi

[10] Prop. 2023/24:85, *En ny lag om uppgiftsskyldighet för att motverka felaktiga utbetalningar från välfärdssystemen samt fusk, regelöverträdelser och brottslighet i arbetslivet*, s. 64 och 65.
[11] Prop. 2024/25:65, *Ökat informationsflöde till brottsbekämpningen*, s. 98.
[12] SOU 2023:69, *Ökat informationsflöde till brottsbekämpningen*, s. 367–371.

nämnt tidigare kan en myndighet vidare inte med stöd av den nu föreslagna bestämmelsen behandla andra uppgifter än sådana som den har en rättslig grund för att behandla genom annan reglering. För det fall bestämmelsen ändå anses utgöra ett sådant betydande intrång i den personliga integriteten som avses i 2 kap. 6 § andra stycket RF kan det konstateras att bestämmelsen föreslås införas i lag (jfr 2 kap. 20 § RF). Bestämmelsen tillgodoser vidare ändamål som är godtagbara i ett demokratiskt samhälle och är nödvändig med hänsyn till det ändamål som har föranlett den, vilket vi utvecklar i avsnitten 6.4.2 och 6.4.7 nedan. Förslaget, som är generellt, sträcker sig heller inte så långt att det utgör ett hot mot den fria åsiktsbildningen (jfr 2 kap. 21 § RF).

6.3.3 Samma kategorier av personuppgifter som i dag

Vår bedömning: En generell bestämmelse om utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ medför inte att andra uppgifter än i dag kommer att kunna behandlas i samband med, och som ett resultat av, informationsutbyte mellan myndigheter.

Skälen för vår bedömning

När ett lagförslag om ett utökat informationsutbyte övervägs har karaktären av de personuppgifter som myndigheterna kommer få utbyta i regel stor betydelse för vilka integritetsrisker som behandlingen av uppgifterna kan medföra för enskilda som berörs. För att bedöma integritetsriskerna måste uppgifternas karaktär som utgångspunkt bedömas tillsammans med andra faktorer, t.ex. i vilket sammanhang som uppgifterna kommer att behandlas, för vilka ändamål och vilka personer som kan komma att få åtkomst till uppgifterna. Som vi konstaterat inledningsvis har den omständigheten att uppgifter inte är sekretessbelagda ingen avgörande betydelse för bedömningen av integritetsriskerna.

Av avsnitten 4.4.3 och 4.4.4 och bilaga 2–5 i vårt delbetänkande framgår vilka uppgiftskategorier som myndigheter generellt efterfrågar möjlighet att kunna *lämna ut* till andra myndigheter, och vilka

uppgiftskategorier som myndigheter önskar *ta del av* från andra myndigheter (jfr även avsnitt 4.7). I båda fall rör det sig om informationsutbyte i syfte att en myndighet ska kunna fatta riktiga beslut eller i övrigt utföra sin verksamhet. Som vi redogjort för i avsnitt 4.7.1 kan de flesta uppgifter som behandlas vid svenska myndigheter, beroende på omständigheterna, vara inte sekretessbelagda. Det är därför rimligt att anta att de efterfrågade uppgiftskategorierna även kommer att lämnas ut med stöd av bestämmelsen om utlämnande på eget initiativ, när bestämmelsen är tillämplig.

Det är dock inte möjligt att inom ramen för vårt uppdrag bedöma de eventuella särskilda integritetsrisker som kommer med ett utlämnande på *eget initiativ*, till skillnad från det redan tillåtna utlämnandet på *begäran*, för varje specifik uppgiftstyp utifrån uppgifternas karaktär. Förslaget om utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ medför dock inte att andra uppgifter än i dag kommer att kunna behandlas i samband med, och som ett resultat av, informationsutbyte mellan myndigheter. Bestämmelsen träffar nämligen enbart uppgifter som inte är sekretessbelagda och sådana uppgifter finns det redan en långtgående skyldighet att lämna ut på begäran (6 kap. 5 § OSL).

6.3.4 Känsliga personuppgifter, uppgifter om lagöverträdelser och uppgifter som rör sårbara personer

Vår bedömning: En generell bestämmelse om utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ kan komma att leda till en ökad behandling av känsliga personuppgifter, uppgifter om lagöverträdelser m.m. och uppgifter om barn. Förslaget kan även komma att leda till en viss ökad behandling av uppgifter om särskilt skyddsvärda grupper, som personer med skyddade personuppgifter.

Skälen för vår bedömning

Särskild reglering vid behandling av känsliga personuppgifter

Särskilda kategorier av personuppgifter (känsliga personuppgifter) omgärdas av en särskild skyddsreglering. Personuppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening eller som rör hälsa, sexualliv eller sexuell läggning utgör sådana känsliga personuppgifter som inte får behandlas enligt artikel 9.1 i dataskyddsförordningen och 2 kap. 11 § första stycket BDL. Det finns dock en rad undantag från huvudregeln att känsliga personuppgifter inte får behandlas. Av artikel 9.2 g i dataskyddsförordningen framgår att förbudet inte gäller om behandlingen är nödvändig av hänsyn till ett viktigt allmänt intresse, på grundval av unionsrätten eller medlemsstaternas nationella rätt, vilken ska stå i proportion till det eftersträvade syftet, vara förenligt med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.

Enligt 3 kap. 3 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning, dataskyddslagen, får känsliga personuppgifter behandlas av en myndighet med stöd av artikel 9.2 g i dataskyddsförordningen under vissa förutsättningar. Det är om uppgifterna har lämnats till myndigheten och behandlingen krävs enligt lag, om behandlingen är nödvändig för handläggningen av ett ärende, eller i annat fall, om behandlingen är nödvändig med hänsyn till ett viktigt allmänt intresse och inte innebär ett otillbörligt intrång i den registrerades personliga integritet.

Vidare finns även undantag från huvudregeln i 2 kap. 11 § andra stycket BDL. Där framgår att uppgifter om en person som behandlas på annan grund får kompletteras med känsliga personuppgifter, om det är absolut nödvändigt för ändamålet med behandlingen. Känsliga personuppgifter får även behandlas för diarieföring, eller om uppgifterna har lämnats till en behörig myndighet i en anmälan, ansökan eller liknande och behandlingen är nödvändig för myndighetens handläggning, se 2 kap. 2 och 13 §§ BDL. I sektorspecifik kompletterande dataskyddsreglering kan det också finnas ytterligare bestämmelser som anger under vilka förhållanden känsliga personuppgifter får be-

handlas av den eller de myndigheter som ska tillämpa den kompletterande regleringen.

Känsliga personuppgifter kan komma att behandlas i utökad omfattning

Av vår kartläggning (se bilaga 2–5 i SOU 2024:63) framgår att myndigheterna efterfrågar möjligheter att både lämna ut och få del av vissa känsliga personuppgifter, i syfte att fatta riktiga beslut eller i övrigt utföra verksamhet inom en myndighet, som inte tillgodoses genom befintlig reglering. Jämfört med andra uppgiftskategorier efterfrågas dock inte möjligheten att utbyta känsliga personuppgifter i särskilt hög utsträckning. I stället är det, med undantag för uppgifter om hälsa, de minst efterfrågade uppgiftskategorierna både vad avser att lämna ut information, och framför allt vad avser att ta del av information.

Som vi redogjort för i avsnitt 4.7.1 kan de flesta uppgifter som behandlas vid svenska myndigheter i vissa fall vara inte sekretessbelagda. Det är därför rimligt att anta att fler känsliga personuppgifter kommer att utbytas med stöd av den nu föreslagna bestämmelsen. Redan uppgiften om att någon har beviljats en socialförsäkringsförmån har t.ex. ansetts kunna utgöra en känslig personuppgift om hälsa.[13]

I många situationer där ett egeninitierat utlämnande av en känslig personuppgift övervägs bör det dock vara så att uppgiften inte är sekretessbelagd av den anledningen att den träffas av en sekretessbrytande bestämmelse i offentlighets- och sekretesslagen. Det innebär att uppgiften redan får lämnas ut på eget initiativ, även utan den bestämmelse vi föreslagit ska införas som en ny 6 kap. 5 a § OSL. När uppgifter utbyts med stöd av en sekretessbrytande bestämmelse har behovet av att uppgiften utbyts redan vägts mot den enskildes integritetsintresse vid införandet av bestämmelsen.

För de myndigheter som ska tillämpa dataskyddsförordningen finns stöd för behandling av känsliga personuppgifter i både dataskyddsförordningen och kapitel 3 i dataskyddslagen, och i flera fall även i kompletterande dataskyddsreglering. I många fall är den kompletterande dataskyddsregleringen begränsande i förhållande till vad

[13] Prop. 2022/23:34, *Utbetalningsmyndigheten*, s. 134 och SOU 2020:35, *Kontroll för ökad tilltro – en ny myndighet för att förebygga, förhindra och upptäcka felaktiga utbetalningar från välfärdssystemen*, s. 363.

som annars gäller enligt dataskyddsförordningen och dataskyddslagen, och i andra fall är den kompletterande dataskyddsregleringen mer tillåtande. De allra flesta myndigheter har dock något stöd för att behandla känsliga personuppgifter inom ramen för sin verksamhet, under förutsättning att det finns en rättslig grund för behandlingen och att de grundläggande principerna för behandling iakttas vid sådan behandling. Bestämmelsen om utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ innebär inte att dessa grundförutsättningar för myndigheters behandling av känsliga personuppgifter förändras. Däremot innebär den att behandling av sådana uppgifter kan komma att ske i större utsträckning än i dag.

Det kan dock inte uteslutas att det i kompletterande dataskyddsreglering eller i annan motsvarande reglering finns ett totalt förbud mot att behandla känsliga personuppgifter inom viss verksamhet. I vissa andra fall saknas det en rättslig grund för myndigheter att över huvud taget behandla känsliga personuppgifter, dvs. verksamheten är sådan att behandling av känsliga personuppgifter aldrig kan vara legitim. I sådana fall möjliggör inte heller bestämmelsen om utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ att mottagaren behandlar dessa uppgifter, utöver eventuell behandling i form av radering.

Även de brottsbekämpande myndigheterna behandlar redan i dag känsliga personuppgifter med stöd av sina respektive registerförfattningar inom brottsdatalagens område. Dessa personuppgifter får endast behandlas som ett komplement till andra uppgifter som behandlas om en person och enbart när det är absolut nödvändigt för ändamålet med behandlingen. Det innebär att om andra uppgifter om en person samlas in i samband med t.ex. en förundersökning får de kompletteras med uppgifter om religiös övertygelse eller etniskt ursprung om det är av betydelse för utredningen. En sådan situation kan t.ex. råda för att utreda hets mot folkgrupp, och under en utredning av sexualbrott kan det ibland vara befogat att anteckna uppgifter om den misstänktes sexualliv. Med hänsyn till den restriktivitet som ligger i uttrycket ”absolut nödvändigt” måste dock behovet av att göra sådana kompletteringar prövas noga i det enskilda fallet. Bestämmelsen om att en utlämnande myndighet på eget initiativ får lämna ut uppgifter som inte är sekretessbelagda förändrar inte det förhållandet, i likhet med vad som anges ovan.

Däremot måste alla myndigheter som utgångspunkt följa bestämmelserna i 5 kap. OSL, som i stort innebär att handlingar som kommer in till en myndighet måste registreras. Det går inte att utesluta att känsliga personuppgifter kan komma att lämnas från en myndighet till en annan myndighet som saknar behov eller rättslig möjlighet att för egen del behandla uppgifterna, men ändå måste behandla dessa för att uppfylla sina skyldigheter att registrera, och i vissa fall bevara i enlighet med det arkivrättsliga regelverket, dessa uppgifter (se avsnitt 3.4.1 i vårt delbetänkande).

Sammanfattningsvis kommer förslaget om en bestämmelse om utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ sannolikt att innebära en utökad behandling av känsliga personuppgifter i situationer där det redan i dag finns en rättslig grund för sådan behandling. Där möjligheterna till sådan behandling i dag är begränsade kvarstår dock begränsningarna oförändrade. Även om det rättsliga utrymmet för myndigheter att över huvud taget behandla känsliga personuppgifter i den egna verksamheten inte ökar genom den föreslagna bestämmelsen kan det uppstå en mer omfattande behandling av sådana uppgifter. I vissa fall kan bestämmelsen även medföra en ny behandling av känsliga personuppgifter som inte är sekretessbelagda, dvs. om behandling i form av *egeninitierat* utlämnande av sådana uppgifter tidigare inte varit uttryckligen tillåten, eller som ett resultat av bestämmelser om hantering av allmänna handlingar. Känsliga personuppgifter som inte är sekretessbelagda kommer därmed att kunna behandlas i högre utsträckning än i dag. Som vi konstaterat i avsnitt 6.3.3 innebär den föreslagna bestämmelsen om utlämnande på eget initiativ dock inte att fler uppgifter ändrar rättslig karaktär från att vara sekretessbelagda till att vara inte sekretessbelagda.

Uppgifter om lagöverträdelser m.m.

Av vår kartläggning framgår att det finns en efterfrågan både på att kunna lämna ut och att få del av uppgifter såväl om misstänkta som om begångna brott (se bilagorna 2–5 i SOU 2024:63). Bestämmelsen om utlämnande på eget initiativ kommer att möjliggöra att myndigheter utan en föregående begäran lämnar sådana uppgifter till en annan myndighet, under förutsättning att uppgifterna inte är sekretessbelagda. Någon generellt begränsande reglering motsvarande

den som avser känsliga personuppgifter finns inte för uppgifter om brott m.m. men även dessa uppgifter är ofta mycket integritetskänsliga.

Enligt artikel 10 i dataskyddsförordningen får behandling av personuppgifter som rör fällande domar i brottmål och lagöverträdelser som innefattar brott eller därmed sammanhängande säkerhetsåtgärder endast utföras under kontroll av en myndighet eller då behandling är tillåten enligt unionsrätten eller nationell rätt, där lämpliga skyddsåtgärder för de registrerades rättigheter och friheter fastställs. Ett fullständigt register över fällande domar i brottmål får endast föras under kontroll av en myndighet. Regeringen har i propositionen som föregick dataskyddslagen uttalat att den del av artikel 10 som rör behandling av uppgifter under kontroll av en myndighet är direkt tillämplig och i vart fall bör innebära att det är tillåtet att behandla uppgifter som rör lagöverträdelser om den personuppgiftsansvarige är en myndighet.[14] Innebörden av artikel 10 har förtydligats i svensk rätt genom bestämmelsen i 3 kap. 8 § dataskyddslagen, där det anges att personuppgifter som avses i artikel 10 får behandlas av myndigheter. I vissa fall begränsas dock myndigheters rättsliga möjligheter att behandla uppgifter om lagöverträdelser m.m. av bestämmelser i kompletterande dataskyddsreglering.[15]

Att uppgifter om lagöverträdelser m.m. som inte är sekretessbelagda kan komma att lämnas ut på eget initiativ i högre utsträckning än i dag kan leda till både ny och utökad behandling av sådana uppgifter. Förutom att en enskild kan ha en önskan att hålla uppgifter om lagöverträdelser hemliga av sociala skäl, kan en ökad spridning också vara förknippat med skadat anseende eller ekonomisk förlust, t.ex. om en anställning inte blir av. En utökad behandling av uppgifter om lagöverträdelser m.m. kan också riskera att ytterligare spä på integritetsriskerna vid sådant ”pusselläggande” vi redogjort för ovan. Kombinerat med en utökad användning av AI-tekniker vid analys och urval av kontrollobjekt (se avsnitt 6.3.5) riskerar det i förlängningen att leda till att personer som tidigare t.ex. begått ett brott blir granskade mer frekvent än andra, av flera olika myndigheter.

[14] Prop. 2017/18:105, *Ny dataskyddslag*, s. 99.
[15] Jfr t.ex. 1 kap. 7 § lagen (2001:181) om behandling av uppgifter i Skatteverkets beskattningsverksamhet.

Bestämmelsen om utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ innebär dock inte i sig att myndigheter som saknar legitima skäl att behandla uppgifter om lagöverträdelser m.m. ges en rättslig möjlighet att göra det. Den rättsliga grunden för att i den aktuella verksamheten behandla sådana uppgifter måste alltså sökas i annan reglering.

Grupper med särskilt behov av skydd

Uppgifter som rör personer med skyddade personuppgifter och personer som i övrigt är utsatta för våld eller förtryck utgör inte per automatik känsliga personuppgifter enligt uppräkningen i artikel 9.1 i dataskyddsförordningen eller 2 kap. 11 § första stycket BDL. En av de risksituationer som anges i skäl 75 till dataskyddsförordningen är dock vid behandling av personuppgifter som rör särskilt sårbara personer, vilket bl.a. personer med skyddade personuppgifter bör uppfattas vara.

Uppgifter om personer med skyddade personuppgifter och om personer som är utsatta för våld eller förtryck behöver inte vara sekretessbelagda i förhållande till andra myndigheter. Med stöd av 6 kap. 5 § OSL kan myndigheter alltså redan i dag ha en långtgående skyldighet att på begäran lämna sådana uppgifter till en annan myndighet. Vad gäller uppgifter som kan vara sekretessbelagda med stöd av de generellt tillämpliga bestämmelserna i 21 kap. OSL kan det t.ex. antas att uppgifter som hålls hemliga för enskilda inte bedöms inte vara sekretessbelagda i förhållande till myndigheter efter en skadeprövning.

Fingerade folkbokföringsuppgifter, som alltså rör personer med fingerad identitet enligt lagen (1991:483) om fingerade personuppgifter, är i regel inte sekretessbelagda. Däremot föreligger det en presumtion för sekretess för uppgiften om kopplingen mellan fingerade personuppgifter och den enskildes verkliga personuppgifter, jfr 21 kap. 3 § tredje stycket OSL.

Personer som har den högsta nivån av skydd för sina verkliga uppgifter, dvs. inte fingerade personuppgifter, har *skyddad folkbokföring*. Då framgår inte den verkliga adressen av personens folkbokföringsuppgifter och den sprids inte heller till andra myndigheter via Skatteverkets system för distribution av folkbokföringsuppgifter till myn-

digheter (Navet). Vissa uppgifter gällande den som har skyddad folkbokföring är alltså oftast sekretessbelagda med stöd av 22 kap. 2 § OSL även i förhållande till andra myndigheter.[16]

En *sekretessmarkering* är en lägre nivå av skyddade personuppgifter än skyddad folkbokföring. Den som inte uppfyller kraven för skyddad folkbokföring kan i vissa fall få en sekretessmarkering i stället, om personen eller dennes närstående riskerar att lida men om uppgifter om personen lämnas ut. En sekretessmarkering registreras i folkbokföringsdatabasen och lämnas ut till andra myndigheter via Navet. När det föreligger en sekretessmarkering i folkbokföringsdatabasen överförs dock alla folkbokföringsuppgifter om personen via Navet till andra myndigheter. En sekretessmarkering är alltså enbart en varningssignal om behovet av att göra en noggrann skadeprövning när uppgifter om en person begärs ut.[17]

Sammanfattningsvis är skyddade personuppgifter och uppgifter om personer som är utsatta för våld eller förtryck ofta inte sekretessbelagda i förhållande till andra myndigheter. Det innebär att den föreslagna bestämmelsen om utlämnande på eget initiativ av uppgifter som inte är sekretessbelagda kan medföra en utökad behandling av sådana uppgifter i enlighet med vad som anges i detta kapitel.

Uppgifter om barn

Uppgifter om barn, som inte är sekretessbelagda i förhållande till mottagaren, kommer att kunna lämnas ut till en myndighet med stöd av bestämmelsen om utlämnande på eget initiativ. Personuppgifter om barn utgör inte per automatik känsliga uppgifter. Av skäl 38 till dataskyddsförordningen framgår dock att barns personuppgifter förtjänar särskilt skydd, eftersom barn kan vara mindre medvetna om berörda risker, följder och skyddsåtgärder samt om sina rättigheter när det gäller behandling av personuppgifter. Av

[16] Jfr Skatteverket, *Vägledning för offentliga aktörers hantering av skyddade personuppgifter*, tillgänglig: https://skatteverket.se/offentligaaktorer/folkbokforing/vagledningforoffentligaaktorershanteringavskyddadepersonuppgifter.4.18e1b10334ebe8bc80002541.html (hämtad 25-02-20).
[17] Jfr Skatteverket, *Vägledning för offentliga aktörers hantering av skyddade personuppgifter*, tillgänglig: https://skatteverket.se/offentligaaktorer/folkbokforing/vagledningforoffentligaaktorershanteringavskyddadepersonuppgifter.4.18e1b10334ebe8bc80002541.html (hämtad 25-02-20).

skäl 50 till dataskyddsdirektivet[18] framgår bl.a. att de åtgärder som den personuppgiftsansvarige vidtar bör omfatta utarbetande och genomförande av särskilda skyddsåtgärder för behandling av personuppgifter om barn.

Sedan den 1 januari 2020 gäller artiklarna 1–42 i FN:s konvention den 20 november 1989 om barnets rättigheter (SÖ1990:20), barnkonventionen, som svensk lag enligt lagen (2018:1197) om Förenta nationernas konvention om barnets rättigheter. När behandling av personuppgifter om barn aktualiseras måste därför framför allt barnkonventionen beaktas. Av artikel 3 framgår att vid alla åtgärder som rör barn ska i första hand beaktas vad som bedöms vara barnets bästa, vare sig de vidtas av offentliga eller privata sociala välfärdsinstitutioner, domstolar, administrativa myndigheter eller lagstiftande organ. Det innebär att när en myndighet överväger att på eget initiativ lämna ut uppgifter om barn, som inte är sekretessbelagda, till en annan myndighet med stöd av den föreslagna bestämmelsen måste även barnkonventionen beaktas inför utlämnandet.

Bestämmelsen om utlämnande på eget initiativ innebär att inte sekretessbelagda uppgifter om barn sannolikt kommer att behandlas vid och som ett resultat av myndigheters informationsutbyte i högre utsträckning än i dag, när dessa uppgifter huvudsakligen får lämnas ut efter en begäran från den mottagande myndigheten (6 kap. 5 § OSL). Även om utlämnande myndigheter måste beakta barnets bästa, och det enbart kan bli fråga om att lämna ut uppgifter om barn som inte är sekretessbelagda, bör den utökade behandlingen av uppgifter om barn anses utgöra en risk för barns personliga integritet. Det bör dock poängteras att även mottagande myndigheter måste beakta barnets bästa i den eventuella fortsatta behandlingen av uppgifterna.

[18] Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF.

6.3.5 Omfattningen av personuppgiftsbehandlingen

Vår bedömning: En generell bestämmelse om utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ kan totalt sett medföra en personuppgiftsbehandling som kan omfatta uppgifter om hela Sveriges befolkning.

Skälen för vår bedömning

En omfattande personuppgiftsbehandling

Uppgifter som inte är sekretessbelagda kan i dag ofta bara lämnas till en annan myndighet om mottagaren framställt en begäran om att få del av uppgifterna (6 kap. 5 § OSL). Som vi konstaterat i avsnitt 4.8.2 är det rättsliga stödet för att på eget initiativ lämna ut uppgifter som träffas av en sekretessbrytande bestämmelse i offentlighets- och sekretesslagen dessutom ganska otydligt.

Den föreslagna bestämmelsen om utlämnande på eget initiativ träffar såväl uppgifter som inte är sekretessreglerade och uppgifter som är undantagna från sekretess, som uppgifter som efter en skadeprövning inte bedöms vara sekretessbelagda och uppgifter som träffas av en sekretessbrytande bestämmelse. Bestämmelsen innebär en ny och förenklad reglering av när uppgifter som inte är sekretessbelagda i förhållande till mottagaren – oavsett varför uppgifterna inte är sekretessbelagda – får lämnas till andra myndigheter. Den möjliggör inte enbart ett utlämnande i syfte att tillgodose behoven hos en mottagande myndighet, utan även utlämnande för att den utlämnande myndigheten ska kunna hämta in relevant information från, eller effektivt samverka med, andra myndigheter. Att en sådan reglering kan medföra en omfattade personuppgiftsbehandling är uppenbart.

Någon närmare beskrivning av den förväntade totala omfattningen av den personuppgiftsbehandling som bestämmelsen kan ge upphov till är svår att göra. Skälet till det är att utlämnande enbart får ske om det finns anledning att anta att det behövs för fullgörande av författningsreglerad verksamhet hos den utlämnande eller mottagande myndigheten. Myndigheter kan generellt sett inte förväntas närmare känna till andra myndigheters verksamhet och därtill hörande behov av information. Utan sådan kännedom bör det inte heller finnas någon anledning att anta att en annan myndig-

het kan behöva vissa uppgifter. Det utökade informationsutbytet som den nu aktuella bestämmelsen leder till, i den mån detta sker för den mottagande myndighetens behov, borde dessutom rimligen endast omfatta uppgifter som en mottagande myndighet inte redan vet att den utlämnande myndigheten förfogar över och som därför kan begäras ut. Omfattningen av det utökade informationsutbytet ska därför inte överdrivas.

Med det sagt har vi kunnat kartlägga ett förhållandevis omfattande behov av att kunna lämna ut uppgifter på eget initiativ. Vi har även tidigare bedömt att behovet av ett utlämnande kan vara knutet till den mottagande myndighetens okunskap om att en viss uppgift över huvud taget existerar (jfr avsnitt 4.8.3). Det är därför rimligt att anta att omfattningen av behandling av uppgifter som inte är sekretessbelagda kommer att öka, jämfört med den som i dag sker med stöd av 6 kap. 5 § OSL. Det kan dock åter påpekas att inga uppgifter kommer att skifta rättslig karaktär från att vara sekretessbelagda till att inte vara det med stöd av bestämmelsen. Samtliga uppgifter som kan komma att lämnas ut på eget initiativ är alltså sådana som den utlämnande myndigheten har en långtgående skyldighet att lämna ut på begäran, enligt 6 kap. 5 § OSL.

Som nyss påpekats saknar dock myndigheter ofta närmare kännedom om i vilken utsträckning andra myndigheter faktiskt har behov av sådana uppgifter som den egna myndigheten förfogar över. I vissa fall kan det sannolikt visa sig att den information som lämnas på eget initiativ trots allt saknar betydelse hos den mottagande myndigheten. Om så sker bör de inblandade myndigheterna samverka kring vilka kategorier av uppgifter som kan vara relevanta att lämna på eget initiativ och vilka som inte är det. Motsatsvis kan det i samverkan även upptäckas att uppgifter som en utlämnande myndighet inte har bedömt vara efterfrågade av mottagaren trots allt är det. Det förefaller också sannolikt att det inte alltid är de rättsliga möjligheterna för den utlämnande myndigheten att lämna ut uppgifter på eget initiativ som är avgörande. Bristande s.k. interoperabilitet (dvs. förmågan att tillhandahålla eller ta del av data genom informationssystem som interagerar med varandra) kan också påverka omfattningen av informationsutbytet.[19]

[19] Se dock förslag till lag och förordning om den offentliga förvaltningens interoperabilitet i SOU 2023:96, *En reform för datadelning*, s. 31–33.

Det är alltså först efter att myndigheter fått förbättrade möjligheter att på eget initiativ lämna ut uppgifter som inte är sekretessbelagda som den närmare omfattningen av det informationsutbyte som en bestämmelse om utlämnande på eget initiativ möjliggör kan förväntas bli känd.

Syftet med bestämmelsen är dock att ge myndigheter rättsliga möjligheter att på eget initiativ lämna ut uppgifter som inte är sekretessbelagda i högre utsträckning än i dag. Utlämnande av uppgifter med stöd av den föreslagna bestämmelsen kommer i och för sig enbart kunna ske om de övriga rekvisit som anges i bestämmelsen är uppfyllda. Det innebär att ett utlämnande bara kommer att kunna ske om det kan antas vara av betydelse antingen för att den mottagande eller den utlämnande myndigheten ska kunna fullgöra författningsreglerad verksamhet. Hela Sveriges befolkning kan dock förutsättas ha kontakt med myndigheter på ett sådant sätt att personuppgifter om dem behandlas hos en eller flera myndigheter. Det gäller även personer som vistas i landet för att arbeta under en kortare tid, eller som på annat sätt har kontakt med eller förekommer vid svenska myndigheter utan att vara folkbokförda. Dessa uppgifter kan i många fall, och av olika skäl, vara inte sekretessbelagda i förhållande till andra myndigheter (jfr avsnitt 4.7.1). Sammanfattningsvis bör alltså omfattningen av utlämnandet på eget initiativ, och därmed den personuppgiftsbehandling som den föreslagna bestämmelsen resulterar i, kunna beröra hela Sveriges befolkning och andra personer som förekommer vid svenska myndigheter.

Något om AI

Allt fler myndigheter använder sig i dag av olika digitala modeller som kan klassas som AI (artificiell intelligens) för att bl.a. spara resurser i administrativ verksamhet, kommunicera med allmänheten, som beslutsstöd vid myndighetsutövning, eller i kärnverksamhet som inte handlar om myndighetsutövning. Allt fler myndigheter använder också AI för att bl.a. undersöka var riskerna för fel och fusk är störst.[20] I dag utgör alltså utvecklandet av digitala analys- och urvalsmodeller,

[20] Statskontoret 2024, *Myndigheterna och AI – En studie om möjligheter och risker med att använda AI i statsförvaltningen*, s. 19.

t.ex. i syfte att förebygga och förhindra fusk och regelöverträdelser, en integrerad del av många myndigheters verksamhet.

I vårt delbetänkande bedömde vi att införandet av en generell sekretessbrytande bestämmelse skulle kunna medföra att myndigheter utbyter uppgifter för att utveckla och att köra olika analysverktyg, och att vissa av dessa modeller med stor sannolikhet kommer att utvecklas med stöd av maskininlärning, dvs. AI. I det sammanhanget noterade vi även att särskilt utvecklingen av olika AI-modeller kräver tillgång till stora mängder data (jfr avsnitt 10.2.6 i SOU 2024:63). Vilken data, dvs. vilka uppgifter, som behövs för att utveckla en AI-modell varierar självfallet beroende på i vilket sammanhang modellen är tänkt att användas. Det bör dock vara vanligt att både annars sekretessbelagda och annars inte sekretessbelagda uppgifter är relevanta i utvecklingsstadiet.

Att myndigheter skulle ha så god insyn i andra myndigheters digitala utvecklingsprojekt att de på *eget initiativ* skulle lämna uppgifter som inte är sekretessbelagda till en annan myndighet i detta syfte känns i dag långsökt. Över tid bör det dock inte uteslutas. Mest troligt är emellertid att uppgifter som inte är sekretessbelagda, och som kan ha betydelse i den interna digitala utvecklingen inom en myndighet, även fortsättningsvis begärs ut av mottagaren med stöd av 6 kap. 5 § OSL.

6.4 Proportionaliteten av förslaget om utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ

6.4.1 Ett klarlagt, faktiskt och konkret problem

Vår bedömning: Vår kartläggning visar att det finns ett faktiskt och konkret problem kopplat till myndigheters bristande möjligheter att på eget initiativ lämna uppgifter som inte är sekretessbelagda till en annan myndighet.

Skälen för vår bedömning

Behovet av en tydlig problembeskrivning

En lagstiftningsåtgärd som begränsar rätten till skydd för personuppgifter behöver först och främst vila på en objektiv och faktabaserad beskrivning av den företeelse som motiverar lagstiftningsåtgärden. Det problem eller missförhållande som lagstiftningsåtgärden avser att avhjälpa måste alltså vara klarlagt.[21] I avsaknad av en tydlig beskrivning av problemet som motiverar den föreslagna bestämmelsen om utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ blir det annars svårt att bedöma t.ex. om bestämmelsen är nödvändig eller om det finns andra sätt att åtgärda problemet på.

Vi har haft i uppdrag att kartlägga de behov av förbättrade möjligheter till informationsutbyte mellan myndigheter som föreligger i dag. Hur vi utfört vår kartläggning och resultatet av densamma redogörs för i kapitel 4 i vårt delbetänkande. I avsnitt 4.7 har vi lämnat en samlad redogörelse för vår kartläggning i den del som avser behovet av att kunna lämna ut uppgifter på eget initiativ. I avsnitten 4.3 och 4.8 har vi dessutom analyserat befintlig lagstiftningen på området. Genom kartläggningen och de analyser av rättsläget som vi genomfört får de problem och de missförhållanden som motiverar den föreslagna bestämmelsen om utlämnande på eget initiativ anses vara beskrivna med tillräcklig tydlighet och konkretion. Nedan följer dock en sammanfattning av den problematik som vi kartlagt.

Problem kopplat till bristande möjligheter att lämna ut uppgifter på eget initiativ

Ett behov av att på eget initiativ lämna ut uppgifter till en annan myndighet kan i många fall uppstå i princip uteslutande av det skälet att den potentiella mottagaren saknar kännedom om uppgifterna. Om en myndighet t.ex. iakttar förhållanden som är tydliga indikatorer på regelöverträdelser i en annan myndighets verksamhet, och den myndigheten redan känner till dessa förhållanden, bör det alltså i regel inte föreligga något behov av utlämnande.

[21] Jfr EDPS, *Assessing the necessity of measures that limit the fundamental right to the protection of personal data*: A Toolkit, 2017, s. 9, tillgänglig: 1https://www.edps.europa.eu/sites/default/files/publication/17-04-11_necessity_toolkit_en_0.pdf7-04-11_necessity_toolkit_en_0.pdf (hämtad 25-03-02).

Om uppgifterna är sekretessbelagda hos den myndighet som gjort iakttagelsen och om uppgifterna träffas av en sekretessbrytande bestämmelse i offentlighets- och sekretesslagen kan den myndigheten, med stöd av den bestämmelsen, på eget initiativ lämna ut uppgifterna som den mottagande myndigheten inte känner till. Stödet för att på eget initiativ lämna uppgifter är dock i dessa fall inte särskilt tydligt, och det råder osäkerhet om tillämpningen av sådana bestämmelser.

För uppgifter som inte är sekretessreglerade, uppgifter som omfattas av ett undantag från sekretess och uppgifter som kan lämnas ut efter en prövning enligt en materiell sekretessbestämmelse föreligger det inget röjandeförbud enligt sekretessregleringen. Sådana uppgifter kan alltså lämnas ut till en annan myndighet utan hinder av sekretess. Det finns dessutom en långgående skyldighet enligt 6 kap. 5 § OSL att på begäran av en annan myndighet lämna ut sådana uppgifter. Det saknas dock ett generellt och uttryckligt rättsligt stöd i sekretessregleringen för att lämna sådana uppgifter till en annan myndighet på eget initiativ.

All personuppgiftbehandling måste dessutom vila på en rättslig grund för att vara laglig i dataskyddsrättslig mening. När det som vid uppgiftslämnande mellan myndigheter rör vidarebehandling för ändamål som är oförenligt med insamlingsändamålet måste behandlingen vara uttryckligen reglerad i den nationella rätten eller i unionsrätten. Om någon sådan reglering inte finns är vidarebehandlingen förbjuden.

Det innebär att bristen på ett uttryckligt rättsligt stöd i praktiken medför ett hinder mot att på eget initiativ lämna ut uppgifter till en annan myndighet, trots att det inte råder något röjandeförbud för uppgifterna enligt sekretessregleringen och trots den långtgående skyldigheten enligt 6 kap. 5 § OSL att lämna ut samma uppgifter, till samma mottagare, på begäran. Det innebär också att det rent lagtekniska utrymmet för att lämna ut uppgifter som *inte* är sekretessbelagda ofta är mindre än utrymmet för att lämna ut uppgifter som är det och som därför träffas av en sekretessbrytande bestämmelse i offentlighets- och sekretesslagen.

Befintlig reglering utgör alltså ett hinder mot att myndigheter på eget initiativ lämnar relevant information till andra myndigheter, som är särskilt påtagligt vad gäller uppgifter som inte är sekretessbelagda. Regleringen måste därför uppfattas som otydlig och motstridig i detta avseende, och bidrar till den höga och generella komplexiteten

på området. Nuvarande hinder mot egeninitierat utlämnande av uppgifter som inte är sekretessbelagda resulterar dessutom i att relevanta och berättigade informationsutbyten mellan myndigheter inte blir av.

6.4.2 Den generella bestämmelsen motiveras av viktiga mål av generellt allmänt intresse

Vår bedömning: Det finns viktiga mål av generellt allmänt intresse som kräver att problemet åtgärdas för att kunna uppfyllas. Den föreslagna bestämmelsen åtgärdar det kartlagda, faktiska och konkreta problemet.

Skälen för vår bedömning

Inledande anmärkningar

Vårt uppdrag är utformat på så sätt att vi inledningsvis har haft i uppdrag att kartlägga behoven av förbättrade möjligheter till informationsutbyte mellan myndigheter och i ett delbetänkande föreslå hur behovet av att utbyta sekretessbelagda uppgifter kan tillgodoses. Inom ramen för den här delen av uppdraget har vi bl.a. haft att i uppdrag att överväga förändringar av regleringen av utbyte av uppgifter som inte är sekretessbelagda. Som vi redogjort för i avsnitt 4.7.1 är det dock svårt att dra upp någon absolut rättslig gräns mellan uppgifter som skyddas av sekretess och uppgifter som inte skyddas av sekretess. Om en uppgift är sekretessbelagd eller inte är i stället många gånger ett situationsbundet och föränderligt rättsligt förhållande. Det bör också nämnas att om den generella sekretessbrytande bestämmelsen som vi föreslog i delbetänkandet införs så kommer långt fler uppgifter än i dag inte vara sekretessbelagda myndigheter emellan. Mot den bakgrunden har vi bl.a. bedömt att det mest ändamålsenliga är att fokusera på behovet av att kunna lämna ut uppgifter på eget initiativ, snarare än uppgifternas sekretessrättsliga status. Det innebär att det inte på ett tydligt och enkelt sätt går att skilja de behov som låg till grund för vårt förslag om en generell sekretessbrytande bestämmelse från de behov som ligger till grund för vårt förslag om en generell bestämmelse om utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ.

Myndigheternas möjlighet att utföra sin verksamhet och att samverka

Det svenska förvaltningsrättsliga systemet bygger på att myndigheter så långt möjligt ska samverka, även när det gäller utbyte av information.[22] Att visst informationsutbyte mellan myndigheter är tillåtet är alltså en grundläggande förutsättning för att svenska myndigheter ska kunna utföra sina uppgifter. Eftersom frågan om en uppgift är sekretessbelagd eller inte många gånger är avhängig omständigheterna i det enskilda fallet gäller det nyss sagda även uppgifter som inte är sekretessbelagda. Regeringen har tidigare uttalat att verksamhet som innefattar myndighetsutövning utgör ett viktigt allmänt intresse i den mening som avses i dataskyddsförordningen. I det sammanhanget uttalade regeringen dessutom att det också måste anses utgöra ett viktigt allmänt intresse att svenska myndigheter även utanför området för myndighetsutövning kan bedriva den verksamhet som tydligt faller inom ramen för deras befogenheter på ett korrekt, rättssäkert och effektivt sätt.[23] Myndigheter har dessutom en generell skyldighet enligt förvaltningslagen att samarbeta och bistå varandra i den utsträckning som är möjlig, där utbyte av information är ett viktigt led (jfr avsnitt 4.2.4).

I vårt delbetänkande har vi dock kunnat konstatera att dagens reglering av myndigheters informationsutbyte är så komplex att tillämpningen försvåras, ibland till den grad att regleringen inte ens tillämpas. Myndigheters samverkansskyldighet är dessutom tänkt att begränsas av sekretessregleringen.[24] Vad gäller uppgifter som annars inte är sekretessbelagda, dvs. som det inte råder något förbud mot att röja enligt sekretesslagstiftningen, innebär dock den befintliga regleringen att det i praktiken ofta föreligger hinder mot att lämna relevanta uppgifter till en annan myndighet på eget initiativ, oavsett behovet och betydelsen av ett sådant utlämnande. Den befintliga regleringen kan därmed sägas utgöra ett hinder mot det viktiga allmänna intresset av att Sveriges myndigheter kan bedriva myndighetsutövning, och övrig verksamhet som tydligt faller inom ramen för deras befogenheter, på ett korrekt, rättssäkert och effektivt sätt.

I många fall kan enskilda gynnas av att myndigheters generella funktionalitet är hög, och att relevant informationsutbyte mellan myndigheter sköts av myndigheterna själva i stället för att gå om-

[22] SOU 2015:39, *Myndighetsdatalag*, s. 167.
[23] Prop. 2017/18:105, *Ny datsskyddslag*, s. 83.
[24] Jfr prop. 1979/80:2, *med förslag till sekretesslag m.m.*, Del A, s. 89 och 361.

vägen om den enskilde. Det skapar ökad medborgarnytta och kan vara särskilt betydelsefullt när syftet med verksamheten är att hjälpa svaga grupper som saknar resurser att överblicka vilken information som är betydelsefull för att de ska få den hjälp eller det stöd de behöver. En stor andel av befolkningen upplever t.ex. att det inte är lätt att göra rätt när man ansöker om bidrag eller ersättning, vilket framgår motsatsvis av Ekonomistyrningsverkets, ESV, årliga attitydundersökning för 2024. I åldersgruppen 18–29 år är andelen 49 procent och i åldersgruppen 30–44 år är andelen 45 procent. I åldersgrupperna 45–64 år, och 65 år och uppåt, ligger andelen på 37 respektive 32 procent. Totalt för hela befolkningen ligger andelen som inte upplever att det är lätt att göra rätt när man ansöker om bidrag eller ersättning på 42 procent.[25]

Om myndigheter har möjligheter att på eget initiativ lämna information som inte är sekretessbelagd och som är relevant för en annan myndighets t.ex. prövning av en ansökan om en förmån eller för något annat beslut så slipper enskilda dessutom lämna samma information till flera olika myndigheter. Det kan även röra sig om att myndigheters service till enskilda förbättras. Utan ett ändamålsenligt informationsutbyte mellan olika myndigheter måste enskilda i större utsträckning komma in med kompletterande underlag i sin kontakt med olika myndigheter. Det innebär att respektive myndighet i hög utsträckning måste inhämta uppgifter från enskilda för sin handläggning, vilket innebär att medborgarnas kontaktytor med myndigheter är fler än nödvändigt. När uppgifter lämnas direkt av enskilda kvarstår dessutom myndighetens behov att kontrollera och verifiera lämnade uppgifter. Även enskilda som inte gjort något fel, eller som gjort ett uppenbart oavsiktligt fel, kan därför tvingas utstå vad som kan uppfattas som integritetskränkande och tidskrävande kontroller eller upprepade kompletteringar. Omfattande kontroller kan dessutom leda till en mer omfattande personuppgiftsbehandling än vad som hade varit nödvändigt om relevanta uppgifter som inte är sekretessbelagda kan lämnas ut direkt, och på eget initiativ, från andra myndigheter.

[25] ESV, *Resultat från 2024 års attitydundersökning – olika gruppers inställning till bidragsbrott*, ESV 2024:38, s. 13.

En lägesbild

I takt med att samhället förändras ställs myndigheterna sammanfattningsvis inför nya utmaningar vilket förutsätter att deras verksamhet också kan anpassas efter ändrade förhållanden. Några områden som under de senaste åren särskilt har påverkat det svenska samhället är utvecklingen inom den grova organiserade brottsligheten i Sverige och omfattningen av felaktiga utbetalningar från välfärdssystemen. Regeringen har i flera sammanhang gjort bedömningen att den grova organiserade brottsligheten i dag är systemhotande och kräver omfattande lagstiftningsreformer. Regeringen har även uttalat att den organiserade brottsligheten utgör ett hot mot det fria och öppna samhället.[26]

I avsnitt 10.3.3 i vårt delbetänkande har vi redogjort för olika aktörers analys av samhällsutvecklingen och påpekanden om behoven av förbättrade möjligheter för myndigheter att utbyta information. Den negativa samhällsutveckling som redogörs för där omfattar bl.a. ökad arbetlivskriminalitet, ökande kostnader för brottslighet, djupgående band mellan brottsligheten och legitima affärsverksamheter, samt att svenska institutioner har visat sig vara sårbara för infiltration, korruption och välfärdsbedrägerier. I flera sammanhang påpekas också att riskerna med utvecklingen är allvarliga och bl.a. kan innebära allvarliga konsekvenser för arbetstagare, konkurrenssnedvridning, ett underminerat förtroende för finansiella system och strukturer, att statens våldsmonopol och kontroll över det egna territoriet utmanas, liksom att rättsstatens principer samt medborgares demokratiska rättigheter hotas.

Viktiga mål av generellt allmänt intresse

Det viktiga allmänna intresset av att myndigheterna ska kunna utföra sin verksamhet på ett korrekt, rättssäkert och effektivt sätt måste uppfattas vara ett grundläggande mål av generellt allmänt intresse. I detta intresse ingår myndigheternas skyldighet att samverka med andra myndigheter och utbyta information. Myndigheters verksamhet

[26] Se t.ex. pressmeddelande från Finansdepartementet, *Nya åtgärder för att motverka felaktiga utbetalningar och välfärdsbrott*, 24-05-30, pressmeddelande från Justitiedepartementet, *Regeringen går vidare med förslag om en ny förverkandelagstiftning*, 24-05-24, och pressmeddelande från Utbildningsdepartementet, *Tre skolmyndigheter får i uppdrag att motverka välfärdsbrott, ekonomisk brottslighet och organiserad brottslighet*, 24-01-02.

rör i många fall statens säkerhet, den allmänna säkerheten, landets ekonomiska välstånd eller förebyggande av oordning eller brott eller skydd för hälsa eller moral eller personers fri- och rättigheter (jfr artikel 8.2 i Europakonventionen[27]). Det motsvarar även sådana mål som anges artikel 23.1 i dataskyddsförordningen (se avsnitt 6.4.3). I förlängningen innebär en generellt hög funktionalitet inom den offentliga sektorn att många andra viktiga mål av generellt allmänt intresse också blir uppfyllda.

Ett viktigt mål av generellt allmänt intresse är att de brottsbekämpande myndigheterna ska ha goda möjligheter att motverka brott. Det innebär bl.a. att barn och unga ska skyddas från att utnyttjas i kriminella sammanhang, att enskilda ska skyddas mot att utsättas för risk för våldsbrott som sprängningar och skjutningar och även mot brottslighet som drabbar enskilda ekonomiskt, t.ex. bedrägerier. Det innebär även att brottsutsatta personer ska kunna få upprättelse genom att förövare lagförs, och att de gemensamma resurserna i välfärdssystemen skyddas från att gå till organiserad brottslighet eller på annat sätt utgöra brottsvinster.

Vårt förslag om att myndigheter på eget initiativ ska få lämna ut relevanta uppgifter som inte är sekretessbelagda både möjliggör sådant uppgiftslämnande som i dag inte är tillåtet, och förtydligar tillåtligheten av sådant uppgiftslämnande som i dag är tillåtet, även till myndigheter vars verksamhet omfattar att förebygga eller bekämpa brottslig verksamhet. Förslaget syftar därmed bl.a. till att ge de brottsbekämpande myndigheterna förbättrade förutsättningar att förebygga och bekämpa brott. Att ett sådant syfte kan motivera en inskränkning av t.ex. rätten till privatliv i artikel 8 Europakonventionen är givet.

I Sverige har välfärdssystemen en viktig roll för att säkerställa människors trygghet vid exempelvis arbetslöshet och sjukdom. Förtroendet för välfärdssystemen är centralt för systemens legitimitet och folkliga stöd. Regeringen har bedömt att felaktiga utbetalningar och brottslighet riktad mot välfärdssystemen och andra offentliga stödsystem undergräver förtroendet för systemen.[28] Med ett försämrat förtroende riskerar tilltron till myndigheternas förmåga att hantera allmänna medel och utföra sina uppdrag att skadas och viljan att bidra till välfärdssystemens finansiering att urholkas. Det måste

[27] Europeiska konventionen om skydd för de mänskliga rättigheterna.
[28] Prop. 2023/24:85, *En ny lag om uppgiftsskyldighet för att motverka felaktiga utbetalningar från välfärdssystemen samt fusk, regelöverträdelser och brottslighet i arbetslivet*, s. 10.

anses vara ett viktigt mål av generellt allmänt intresse att förtroendet för de svenska välfärdssystemen bevaras, och i förlängningen att de finns kvar. Förslaget om att myndigheter ska kunna samverka genom att på eget initiativ lämna relevanta uppgifter som inte är sekretessbelagda till andra myndigheter syftar därmed även till att skapa förbättrade förutsättningar att upprätthålla de svenska välfärdssystemen, som måste anses vara del av landets ekonomiska välstånd, och att upprätthålla skydd för hälsa eller moral. Att ett sådant syfte kan motivera en inskränkning av t.ex. rätten till privatliv i artikel 8 Europakonventionen är också självklart.

Arbetslivskriminalitet och regelöverträdelser inom arbetslivet riskerar arbetstagares rättigheter och motverkar lika villkor för företag. Arbetslivskriminalitet ledet till att konkurrensen snedvrids och att seriösa företagare konkurreras ut av oseriösa företag. Den orsakar en otrygghet på arbetsmarknaden, att arbetskraft utnyttjas och att offentliga medel riskerar att gå till kriminella. Även upprätthållandet av respekten för reglerna i arbetslivet är därför ett viktigt mål av generellt allmänt intresse. Förslaget syftar därmed till att skapa förbättrade förutsättningar att upprätthålla den svenska arbetsmarknadsmodellen, som måste anses vara del av landets ekonomiska välstånd, och att upprätthålla skydd för hälsa eller moral, vilket också är en legitim grund för en inskränkande lagstiftningsåtgärd.

En bestämmelse om utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ åtgärdar det kartlagda problemet

För att åtgärda de problem vi kunnat kartlägga krävs enligt vår bedömning en tydligt tillåtande, enkel och förutsebar reglering av när myndigheter på eget initiativ får lämna uppgifter till en annan myndighet som ett led i samverkan mellan myndigheter. Som vi nämnt tidigare begränsas myndigheternas samverkan vad gäller uppgiftsutbyte av sekretessregleringen, vilket bl.a. tydliggörs av att den befintliga, generella skyldigheten att på begäran lämna uppgifter till en annan myndighet enbart träffar uppgifter som inte är sekretessbelagda (6 kap. 5 § OSL). En ny generell bestämmelse om utlämnande på eget initiativ, som i likhet med 6 kap. 5 § OSL enbart träffar uppgifter som inte är sekretessbelagda, utgör en tydligt tillåtande, enkel och förutsebar reglering av när myndigheter får samverka genom att på eget initiativ lämna uppgifter till varandra. En sådan bestämmelse

kompletterar den befintliga regleringen i 6 kap. 5 § OSL och får anses bidra till en ökad uppfyllelse av de viktiga mål av generellt allmänt intresse som vi redogjort för ovan. Sammanfattningsvis är vår bedömning att en generell bestämmelse om utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ åtgärdar de konkreta, faktiska problem vi kartlagt.

6.4.3 En inskränkning av rätten till skydd för personuppgifter men ingen begränsning av registrerades rättigheter enligt dataskyddsförordningen

Våra bedömningar: Den föreslagna bestämmelsen utgör en inskränkning av rätten till skydd för personuppgifter.

Den innebär dock inte en begränsning av tillämpningsområdet för de skyldigheter för personuppgiftsansvariga myndigheter och rättigheter för registrerade som föreskrivs i artiklarna 12–22 och 34 i dataskyddsförordningen.

Skälen för våra bedömningar

En inskränkning av rätten till skydd för personuppgifter?

Artikel 8.1 i Europakonventionen garanterar enskilda rätten till skydd bl.a. för sitt privatliv. Europadomstolen[29] har uttalat att begreppet privatliv är ett brett begrepp som inte går att definiera på ett uttömmande sätt. Det omfattar både en persons fysiska och psykiska integritet och kan omfatta en mängd olika aspekter av en persons identitet. Behandling av personuppgifter träffas alltså ofta av bestämmelser om rätten till skydd för privatlivet. Redan att en myndighet behandlar uppgifter om en persons privatliv, dvs. personuppgifter, kan i vissa fall utgöra en inskränkning av rätten till skydd för privatlivet.[30] I Europadomstolens praxis finns flera exempel på när inskränkningar av rätten till skydd för privatlivet har konstaterats föreligga, när en sådan inskränkning varit berättigad, dvs. proportionerlig,

[29] Europeiska domstolen för de mänskliga rättigheterna.
[30] Se t.ex. Europadomstolens avgörande i Leander mot Sverige, mål nr 9248/81, punkt 48, och domstolens avgörande i S. och Marper mot Förenade kungariket, mål nr 30562/04 och 30566/04, punkt 103.

och när den i flera fall inte har bedömts vara berättigat. Europadomstolen har t.ex. bedömt att brottsbekämpande myndigheters långvariga behandling av personuppgifter om sexualbrott mot minderåriga utgör ett intrång i rätten till skydd för personuppgifter, men att ett sådant intrång under vissa förhållanden kan vara berättigat.[31] Domstolen har även bedömt att om det i nationella rätten finns skyddsåtgärder som hindrar myndigheterna från skönsmässig tillämpning, kan hemlig telefonavlyssning och behandling av de uppgifter en sådan avlyssning ger upphov till vara berättigad.[32]

Artikel 7 i EU-stadgan[33] garanterar var och en rätten till respekt för sitt privatliv och familjeliv, sin bostad och sina kommunikationer. I artikel 8.1 i EU-stadgan ges var och en dessutom uttryckligen rätt till skydd av de personuppgifter som rör honom eller henne. EU-domstolen har uttalat att åtkomst till en fysisk persons personuppgifter för lagring eller användning påverkar denna persons grundläggande rätt till respekt för privatlivet. Denna rätt omfattar nämligen all information som avser en identifierad eller identifierbar fysisk person. EU-domstolen har även slagit fast att utlämnande av personuppgifter till tredjeman, såsom en myndighet, utgör ett ingrepp i de grundläggande rättigheter som slås fast i artiklarna 7 och 8 i EU-stadgan, oavsett hur de lämnade uppgifterna senare används. Det förhåller sig på samma sätt med lagringen av personuppgifter och åtkomsten till sådana uppgifter i syfte att myndigheter ska använda sig av dem.[34]

En generell bestämmelse om utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ möjliggör utökad, och i mindre utsträckning, ny personuppgiftsbehandling inom i princip hela den offentliga sektorn, även för brottsbekämpande ändamål. Utlämnande på eget initiativ som i dag är tillåtet med stöd av en sekretessbrytande bestämmelse i offentlighets- och sekretesslagen träffas av bestäm-

[31] Se Europadomstolens pressmeddelande *Inclusion in national sex offender database did not infringe the right to respect for private life – No Violation of Article 8 (right to respect for private and family life) of the European Convention on Human Rights*, angående avgörande i målen B.B. mot Frankrike, nr 5335/06, Gardel mot Frankrike, nr 16428/05 och M.B. mot Frankrike nr 22115/06, tillgänglig: https://hudoc.echr.coe.int/fre-press?i=003-4480954-5400075 (hämtad 25-03-05).
[32] Se Europadomstolens pressmeddelande *Use of personal telephone data by an investigating judge did not breach the Convention*, angående avgörande i målet Figueiredo Teixeira mot Andorra, nr 72384/14, tillgänglig: https://hudoc.echr.coe.int/eng-press?i=003-5539990-6976357 (hämtad 25-03-05).
[33] Europeiska unionens stadga om de grundläggande rättigheterna.
[34] Se EU-domstolens avgörande i Schrems II, mål nr C-311/18, punkterna 170 och 171.

melsen, och i dessa fall förtydligar bestämmelsen stödet för det egeninitierade utlämnandet. Även utlämnande av uppgifter på eget initiativ som annars inte är sekretessbelagda, men som i dag inte är uttryckligen tillåtet, träffas av bestämmelsen. Bestämmelsen möjliggör utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ, men innebär inte någon skyldighet för den utlämnande myndigheten. Samma uppgifter, dvs. uppgifter som inte är sekretessbelagda, omfattas dock redan i dag av en skyldighet att lämna ut dem, men det kräver att den mottagande myndigheten begärt att få del av uppgifterna med stöd av den befintliga regleringen i 6 kap. 5 § OSL.

Sammantaget bör den generella bestämmelsen om utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ innebära en inskränkning av enskildas rätt till skydd för personuppgifter. Det innebär dock inte i sig att bestämmelsen strider mot överordnade normer. Däremot innebär det att den måste uppfylla vissa krav, t.ex. att den ska vara nödvändig (se avsnitt 6.4.7)

En begränsning av enskildas rättigheter enligt dataskyddsförordningen?

Vi har ovan konstaterat att den föreslagna bestämmelsen innebär en inskränkning av rätten till skydd för personuppgifter. Vad gäller myndigheter kan rätten till skydd för personuppgifter något förenklat sägas kräva att myndigheter avstår från att behandla personuppgifter. Det kan därmed beskrivas som en s.k. negativ rättighet som egentligen inte kräver en aktiv handling från en myndighets sida för att kunna åtnjutas av enskilda. Enligt dataskyddsförordningen har dock enskilda registrerade också flera positiva rättigheter, dvs. rättigheter som kräver ett faktiskt agerande av myndigheterna och som ålägger dem en rad skyldigheter.

Flera av de enskildas (registrerades) rättigheter anges i kapitel III, dvs. artiklarna 12–22 i dataskyddsförordningen. Av dessa bestämmelser framgår att en personuppgiftsansvarig myndighet bl.a. måste ge de registrerade information när vederbörandes personuppgifter behandlas, rätta felaktiga personuppgifter på begäran av den registrerade och upphöra med behandling om den registrerade motsätter sig den. I artikel 34 finns även en skyldighet för personuppgiftsansvariga att underrätta registrerade om personuppgiftsincidenter.

Av artikel 23.1 i dataskyddsförordningen framgår att registrerades rättigheter (och personuppgiftsansvarigas korresponderande skyldigheter enligt artikel 5) får begränsas i vissa fall. En sådan begränsning får dock bara införas om det sker med respekt för andemeningen i de grundläggande rättigheterna och friheterna och utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle. Det kan bl.a. vara i syfte att säkerställa den nationella eller allmänna säkerheten, förebygga brott eller säkerställa andra av unionens eller en medlemsstats viktiga mål av generellt allmänt intresse, särskilt ett av unionens eller en medlemsstats viktiga ekonomiska eller finansiella intressen.[35]

Den föreslagna bestämmelsen innebär att enskildas rätt till skydd för personuppgifter inskränks och medför som vi redogjort för i avsnitt 6.3 ett flertal integritetsrisker. Bestämmelsen omfattar dock inga begränsningar av de rättigheter och skyldigheter som är möjliga att begränsa enligt artikel 23.1 i dataskyddsförordningen. Det innebär att enskilda även i fortsättningen har rätt att få klar och tydlig information från myndigheterna om den personuppgiftsbehandling som är aktuell och ändamålen med den, få tillgång till de personuppgifter som behandlas (registerutdrag) och rätt att göra invändningar mot behandling, om inte annat framgår av andra bestämmelser (se vidare avsnitt 3.3 om skyldigheten att lämna information).

6.4.4 Skyddsåtgärder

Vår bedömning: Den föreslagna bestämmelsen är förenad med adekvata och tillräckliga skyddsåtgärder.

Skälen för vår bedömning

Om en inskränkning av rätten till skydd för personuppgifter förenas med skyddsåtgärder, dvs. någon form av begränsning av inskränkningen, kan det medföra att den framstår som mer berättigad än den skulle gjort utan sådana.[36] Enligt Europadomstolens praxis läggs

[35] Jfr Europeiska dataskyddsstyrelsen, EDPB, *Riktlinjer 10/2020 om begränsningar enligt artikel 23 i den allmänna dataskyddsförordningen*, Version 2.1, s. 6, 7, 11 och 20.
[36] Jfr Europeiska dataskyddsstyrelsen, EDPS, *Necessity & Proportionality*, tillgänglig: https://www.edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en?page=1 (hämtad 25-03-06).

särskilt vikt vid att en inskränkande lagstiftningsåtgärd måste förenas med skyddsåtgärder i den nationella rätten som medför att myndigheter inte ges ett obegränsat handlingsutrymme eller en okontrollerad makt (unfettered power). När Europadomstolen överväger om det finns adekvata skyddsåtgärder är det dock inte enbart den aktuella lagstiftningsåtgärden som granskas. Skyddsåtgärder som finns – eller saknas – i den nationella rätten i övrigt tas också i beaktande.[37]

På grund av offentlighetsprincipen har vi i svensk lagstiftning en unik och detaljerad sekretessreglering där integritetskänsliga uppgifter om enskilda har getts ett skydd. Sekretesskyddet gäller inte bara gentemot enskilda, utan även mellan myndigheter och mellan olika självständiga verksamhetsgrenar inom samma myndighet. Myndigheterna hindras alltså genom sekretessregleringen från att lämna ut integritetskänsliga uppgifter till andra myndigheter. Regleringen utgör därmed även en begränsning av myndigheternas samverkansskyldighet enligt bl.a. förvaltningslagen.[38]

Utformningen av de materiella sekretessbestämmelserna, dvs. skyddet för uppgifter om enskilda, speglar hur lagstiftaren har balanserat integritetsintresset mot motstående intressen i olika sammanhang. En konsekvens av sekretesslagstiftningens systematik är att uppgifter som inte är sekretessbelagda hos en myndighet, och som därför kan lämnas till en annan myndighet på eget initiativ med stöd av den föreslagna bestämmelsen, många gånger kommer att bli sekretessbelagda hos mottagaren.

I vissa fall har lagstiftaren infört sekretessbrytande regler som innebär att sekretesskyddade uppgifter under vissa förutsättningar får lämnas till en eller flera andra myndigheter som behöver uppgifterna i sin verksamhet. I andra fall har lagstiftaren infört undantag från sekretess för att t.ex. tillgodose intresset av insyn i myndigheternas beslutsfattande och verksamhet. Det finns även sammanhang där sekretess enbart gäller om uppgifter av särskilda skäl bör hållas hemliga. Sammanfattningsvis har dock lagstiftaren bedömt att uppgifter som inte har försetts med något sekretesskydd, som omfattas av sekretessbrytande regler eller som är undantagna från sekretess

[37] Jfr t.ex. domstolens avgörande i Hasan och Chaush mot Bulgarien, mål nr 30985/96, punkt 85 och där relaterad rättspraxis. Se även Europadomstolens pressmeddelande *Use of personal telephone data by an investigating judge did not breach the Convention*, angående avgörande i Figueiredo Teixeira mot Andorra, mål nr 72384/14, tillgänglig: https://hudoc.echr.coe.int/eng-press?i=003-5539990-6976357 (hämtad 25-03-05).
[38] Jfr prop. 1979/80:2, *med förslag till sekretesslag m.m.*, Del A, s. 89 och 361.

är av sådan karaktär att utlämnanden till andra myndigheter, eller, när det gäller sekretessbrytande bestämmelser, vissa myndigheter, bör kunna ske utan hinder av sekretess.[39] En generell bestämmelse om utlämnande av uppgifter som inte är sekretessbelagda bör därför anses vara förenad med skyddsåtgärder redan av det skälet att den enbart träffar uppgifter som lagstiftaren, med beaktande av motstående intressen, redan har bedömt ska kunna lämnas ut. Bestämmelsen medför inte att fler uppgifter än i dag skiftar rättslig status från att vara sekretessbelagda till att inte vara det. De begränsningar av myndigheters handlingsutrymme som sekretessregleringen ställer upp påverkas alltså inte av bestämmelsen.

Bestämmelsen om utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ medger vidare enbart sådant utlämnande som kan antas vara av betydelse för fullgörande av den utlämnande eller mottagande myndighetens författningsreglerade verksamhet. Som vi utvecklat i avsnitt 4.8.4 bör bestämmelsen i detta avseende ses i ljuset av den befintliga regleringen i 6 kap. 5 § OSL, som den föreslagna bestämmelsen är avsedd att komplettera. Skyldigheten enligt 6 kap. 5 § OSL att på begäran lämna uppgifter som inte är sekretessbelagda till en annan myndighet är inte förenad med ett krav på att den mottagande myndigheten ska ha ett behov av uppgifterna för att skyldigheten ska inträda. En utgångspunkt måste här ha varit att myndigheter inte samlar in eller begär att få ta del av information som saknar betydelse för verksamheten, inte minst med beaktande av legalitetsprincipen. Utifrån det synsättet uppnås genom kravet på att en begäran ska föregå utlämnandet ett grundläggande skydd även för uppgifter om enskilda som annars inte är sekretessbelagda, eftersom uppgifterna därigenom inte kan spridas godtyckligt mellan myndigheter eller för illegitima syften.

Att den generella bestämmelsen om utlämnande på eget initiativ innehåller ett krav på att utlämnandet ska antas vara av betydelse för att den utlämnande eller den mottagande myndigheten ska kunna fullgöra författningsreglerad verksamhet bör ha samma funktion som kravet att en begäran ska föregå utlämnandet enligt 6 kap. 5 § OSL. På så sätt tillåter inte regleringen att uppgifter som inte är sekretessbelagda sprids godtyckligt mellan myndigheter eller för illegitima syften. Även detta måste anses utgöra en skyddsåtgärd, eftersom

[39] Jfr SOU 2003:99, *Ny sekretesslag*, s. 232.

rekvisiten för utlämnandet på eget initiativ medför att myndigheternas handlingsutrymme är begränsat.

I avsnitten 3.1–3.3 i vårt delbetänkande har vi redogjort för några generella bestämmelser som i princip samtliga svenska myndigheter måste iaktta. Vi har även redogjort för den dataskyddsrättsliga systematiken, där personuppgiftsbehandling vid svenska myndigheter ofta regleras på tre nivåer, dvs. genom dataskyddsförordningen, dataskyddslagen och i många fall även genom sektorsspecifik dataskyddsreglering. Det kan också noteras att genom lagen (1994:1219) om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna har Europakonventionen inkorporerats i svensk rätt. Vidare gäller enligt 2 kap. 19 § RF att lagar och andra föreskrifter inte får meddelas i strid med Sveriges åtaganden enligt Europakonventionen. Regeringen har uttalat att det därför bör vara mycket ovanligt att svensk rätt (dvs. den rättsliga grunden för personuppgiftsbehandling vid svenska myndigheter, vår anmärkning) inte uppfyller Europakonventionens krav.[40] Det innebär att den materiella och processuella reglering som behovet av ett utlämnande på eget initiativ ska prövas mot redan ställer upp krav på myndigheterna som motsvarar de som följer av Europakonventionen.

Sammanfattningsvis bedömer vi att utformningen av den generella bestämmelsen om utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ, tillsammans med övrig reglering som begränsar svenska myndigheters utrymme att behandla personuppgifter, utgör tillräckliga och adekvata skyddsåtgärder.

6.4.5 Den föreslagna bestämmelsen är tillräckligt tydlig och precis för att dess tillämpningen ska vara förutsebar för personer som berörs av den

Vår bedömning: Utformningen av den föreslagna bestämmelsen är tillräckligt tydlig och precis och dess tillämpning är tillräckligt förutsebar för personer som berörs av den.

[40] Prop. 2017/18:105, *Ny dataskyddslag*, s. 50.

Skälen för vår bedömning

Kravet på förutsebarhet

EU-domstolen har uttalat att de föreskrifter som ligger till grund för behandling av personuppgifter måste innehålla tydliga och precisa bestämmelser som reglerar räckvidden och tillämpningen av den aktuella åtgärden samt ange minimikrav, så att de personer vars personuppgifter lämnas ut ges tillräckliga garantier för att uppgifterna på ett effektivt sätt är skyddade mot riskerna för missbruk. Dessa föreskrifter måste även vara rättsligt bindande enligt nationell rätt och i synnerhet ange under vilka omständigheter och på vilka villkor en åtgärd för behandling av sådana uppgifter får vidtas, vilket säkerställer att ingreppet begränsas till vad som är strikt nödvändigt.[41] EU-domstolen har dock även uttalat att de grundläggande rättigheterna avseende respekt för privatlivet och skydd för personuppgifter inte utgör några absoluta rättigheter, utan ska förstås utifrån sin uppgift i samhället och vägas mot andra grundläggande rättigheter. Begränsningar får därför göras, förutsatt att de, i enlighet med vad som anges i artikel 52.1 i EU-stadgan, är föreskrivna i lag och förenliga med det väsentliga innehållet i de grundläggande rättigheterna och proportionalitetsprincipen.[42]

Uttrycket ”med stöd av lag” i artikel 52.1 i EU-stadgan kräver inledningsvis att det måste finnas stöd för en inskränkande åtgärd i den nationella rätten. Lagkravet ska dock inte förstås som ett formellt krav på lagform, utan även annan normgivningsnivå avses. Av artikel 8.2 i Europakonventionen följer att inskränkningar i rätten till skydd för personuppgifter inte får ske annat än med stöd av lag. Enligt Europadomstolen omfattar begreppet lag både ”skriven rätt” inklusive regler av lägre status än lag, liksom föreskrifter m.m. som meddelats med stöd av bemyndiganden från lagstiftaren, och oskriven lag. Begreppet lag omfattar alltså både faktisk lagstiftning (inkl. föreskrifter m.m.) och praxis.[43]

Vi föreslår att den generella bestämmelsen om utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ ska införas i offentlighets- och sekretesslagen, vilket innebär att detta grundläggande

[41] EU-domstolens avgörande i C-175/20, Valsts ieņēmumu dienests, punkt 83.
[42] EU-domstolens avgörande i C 439/19, Latvijas Republikas Saeima (Prickning), punkt 105.
[43] Se Europadomstolens avgörande i Sanoma Uitgevers B.V. mot Nederländerna, mål nr 38224/03, punkt 83.

krav kan uppfattas vara uppfyllt. Att bestämmelsen formellt sett finns i lag (i den mening begreppet har i sammanhanget) är dock inte tillräckligt för att kravet enligt artikel 8.2 i Europakonventionen ska vara uppfyllt. Bestämmelsen i fråga måste också vara tillgänglig för de personer som berörs av den och konsekvenserna av bestämmelsen måste framför allt vara förutsägbara för dessa personer. Att bestämmelsen ska vara förutsägbar innebär att personer som berörs av den måste ha en möjlighet att anpassa sitt agerande efter bestämmelsen, dvs. att de måste ges en, beroende på omständigheterna, rimlig möjlighet att – med hjälp av rådgivning om det är påkallat – förutse vilka konsekvenser ett visst agerande får. Bestämmelsen måste alltså vara tillräckligt tydligt formulerad avseende under vilka omständigheter och förutsättningar myndigheter får vidta de åtgärder som avses. Den nationella rätten måste även innehålla någon form av rättsligt skydd mot skönsmässigt intrång i enskildas rättigheter enligt Europakonventionen.[44]

Om en bestämmelse medför att det finns ett visst tolkningsutrymme måste det finnas någon indikation på omfattningen av detta för att lagkravet ska vara uppfyllt. Europadomstolen har dock vid flera tillfällen påpekat att det är omöjligt att utforma lagar på ett sådant sätt att absolut säkerhet om deras omfattning uppnås, och att strävan efter en sådan precision kan medföra en överdriven stelhet. Europadomstolen har också noterat att många lagar är vagt utformade och att tolkningen är en fråga för rättstillämparen. I dessa fall kan andra regler som myndigheter måste följa, även om de inte utgör lag, tas i beaktande vid bedömningen av om kravet på förutsebarhet är uppfyllt, så länge de som berörs görs tillräckligt medvetna om innehållet i dessa andra bestämmelser.[45]

Den föreslagna bestämmelsen är tillräckligt förutsebar för de som berörs av den

Eftersom svensk lag publiceras i Svensk författningssamling bör kravet på tillgänglighet anses vara uppfyllt. Att en bestämmelse om myndigheters utbyte av uppgifter som inte är sekretessbelagda har

[44] Se t.ex. Europadomstolens avgöranden i Malone mot Förenade Kungariket, mål nr 8691/79, punkterna 66 och 67 och i Vlasov mot Ryssland, mål nr 78146/01, punkt 125.
[45] Se Europadomstolens avgörande i Silver m.fl. mot Förenade Kungariket, mål nr 7136/75 m.fl. punkterna 88 och 89.

ett generellt tillämpningsområde är vidare inte någon nyhet i svensk rätt, eftersom bestämmelsen i 6 kap. 5 § OSL har funnits sedan 1980 års sekretesslag (1980:100) infördes. Som vi nämnt tidigare syftar den generella bestämmelsen om utlämnande på eget initiativ till att komplettera uppgiftsskyldigheten enligt 6 kap. 5 § OSL och att tydliggöra den rättsliga regleringen av myndigheters generella samverkansskyldighet, som i sin tur begränsas av sekretessregleringen.

I 6 kap. 5 § OSL ges det inga indikationer om till vilka myndigheter en uppgift kan komma att lämnas ut med stöd av bestämmelse, eller vilka konkreta uppgifter som kan komma i fråga. Det enda som föreskrivs vad gäller vilka uppgifter som kan komma att lämnas med stöd av den bestämmelsen är att de inte får vara sekretessbelagda. I det avseendet innebär den generella bestämmelsen om utlämnande på eget initiativ ingen markant skillnad från redan gällande rätt. Det är därmed svårt att hävda att enbart det förhållandet att myndigheter utbyter alla slags uppgifter som inte är sekretessbelagda, utan begränsning till särskilda syften, *i sig* medför att en bestämmelse inte är godtagbar enligt överordnade normer eller att kravet på förutsebarhet inte är uppfyllt. Om bestämmelsen innehåller en begränsning av det tolkningsutrymme (i förlängningen handlingsutrymmet) som rättstillämparen ges genom bestämmelsen, kan det som nämnts ovan bidra till att en bestämmelse framstår som godtagbar, trots ett annars mycket brett tillämpningsområde.

Att utforma en generell bestämmelse på ett sådant sätt att enskilda har möjlighet att förutse tillämpningen av den i det enskilda fallet är självfallet förenat med svårigheter. För det första bör det vara svårt för enskilda att avgöra vilka uppgifter som är sekretessbelagda och vilka som inte är det. Vilka icke-sekretessbelagda uppgifter som kan antas ha betydelse för fullgörandet av författningsreglerad verksamhet kan vidare vara mycket svårt att avgöra för en enskild, i vart fall om han eller hon inte har en god kännedom om den processuella och materiella reglering som styr myndigheternas verksamhet. Mot bakgrund av att AI-teknik sannolikt kommer att användas i allt högre utsträckning inom den offentliga förvaltningen bör dessutom svårigheterna att förutse tillämpningen av bestämmelsen bli större (se avsnitt 6.3.5 och avsnitt 10.2.6 i SOU 2024:63). Samma eller liknande påpekanden gör sig dock gällande även för 6 kap. 5 § OSL.

Den generella bestämmelsen om utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ innebär alltså att uppgifter som enskilda lämnar till en myndighet för ett syfte kan komma att lämnas till en stor mängd andra myndigheter, och behandlas för helt andra ändamål än det ursprungliga, utan att enskilda alltid har en möjlighet att närmare förutse vilka dessa andra mottagare och ändamål är. Enligt Europadomstolens praxis krävs dock inte att enskilda ska kunna förutse exakt vilka förfaranden som en inskränkande lagstiftningsåtgärd ger upphov till. Det grundläggande kravet är i stället att personer som berörs ska ha tillgång till bestämmelsen, ges en möjlighet att – med hjälp av rådgivning om det är påkallat – anpassa sitt agerande efter bestämmelsen och att det finns begränsningar av myndigheternas tolkningsutrymme och handlingsutrymme.

Vår bedömning är att den generella bestämmelsen om utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ uppfyller dessa krav. Även den reglering som styr mottagande myndigheters verksamhet, inklusive vissa myndighetsföreskrifter, är nämligen publicerad i Svensk författningssamling och därmed tillgängliga för enskilda som berörs. Med stöd av juridisk eller annan rådgivning bör enskilda därtill kunna få en tydligare bild av hur uppgiftsflödet kan komma att se ut och anpassa sitt agerande efter detta. Vad gäller begränsningar av myndigheternas handlingsutrymme hänvisas till avsnitten 6.4.4 och 6.4.6.

Redan genom bestämmelsens ordalydelse kommer det dessutom finnas en tydlighet i fråga om att en uppgift som lämnas till en myndighet kan komma att lämnas till andra myndigheter på den första myndighetens initiativ, om uppgiften inte är sekretessbelagd. Det finns också en tydlighet i att ett sådant utbyte inte är tillåtet i alla situationer, utan att utlämnandet måste kunna antas vara av betydelse för att den mottagande, eller den utlämnande myndigheten ska kunna fullgöra sin, författningsreglerade verksamhet.

Enskilda ges genom denna tydlighet en möjlighet att förutse att den information hon eller han lämnar till en myndighet kan komma att lämnas till en eller flera andra myndigheter. Denna tydlighet innebär också att enskilda har en möjlighet att anpassa sitt agerande efter bestämmelsen. Genom bestämmelsen blir det också tydligt för enskilda att de uppgifter som vederbörande lämnar till en myndighet kan komma att kontrolleras mot uppgifter som lämnats till en annan myndighet.

Som vi konstaterat i avsnitt 6.4.3 innebär den generella bestämmelsen om utlämnande på eget initiativ dessutom inte att enskildas (registrerades) rättigheter enligt dataskyddsförordningen begränsas. Personuppgiftsansvariga myndigheters skyldighet att tillgodose enskildas rättigheter är i inte heller begränsad genom bestämmelsen. Enskilda har alltså även fortsättningsvis rättigheter bl.a. vad avser att få information om behandlingen, och begära registerutdrag. I regel kommer därför myndigheterna behöva upplysa enskilda om den behandling av personuppgifter som den generella bestämmelsen om utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ kan komma att ge upphov till (jfr avsnitt 3.3). Motsvarande bestämmelser kommer fortsättningsvis även att gälla inom brottsdatalagens tillämpningsområde.

6.4.6 Införandet av den föreslagna bestämmelsen är en godtagbar åtgärd i ett demokratiskt samhälle och förenlig med det väsentliga innehållet i dataskyddsreglering

Vår bedömning: En generell bestämmelse om utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ är godtagbar i ett demokratiskt samhälle och förenlig med det väsentliga innehållet i reglering till skydd för den personliga integriteten.

Skälen för vår bedömning

Som vi konstaterat ovan är utformningen av den unika och detaljerade svenska sekretessregleringen resultatet av lagstiftarens avvägning mellan integritetsintressen och motstående intressen inom hela den offentliga förvaltningen. Sammanfattningsvis har lagstiftaren bedömt att uppgifter som inte har försetts med något sekretesskydd, som omfattas av sekretessbrytande regler eller som är undantagna från sekretess är av sådan karaktär att utlämnanden till andra myndigheter, eller, när det gäller sekretessbrytande bestämmelser, vissa myndigheter, bör kunna ske utan hinder av sekretess. Syftet med sekretessregleringen är alltså att reglera samtliga förbud mot att röja uppgifter som ska gälla i den offentliga förvaltningen (jfr avsnitt 5.4.4).

Som vi påpekat tidigare begränsar sekretessregleringen därmed också myndigheternas lagstadgade samverkansskyldighet. En sådan ordning måste på ett rent generellt plan anses vara godtagbar i ett demokratiskt samhälle.

I dag är dock utrymmet för att på eget initiativ lämna uppgifter som *inte* är sekretessbelagda ofta mindre än utrymmet att på eget initiativ lämna uppgifter som annars *är* sekretessbelagda. Som vi påpekat i avsnitt 4.8.4 förfaller det vara en konsekvens av dataskyddsförordningens krav på den nationella rätten, dvs. att vidarebehandlingen måste vara uttryckligen tillåten för att vara laglig. I det sammanhanget har vi även påpekat att lagstiftaren kan ha utgått från att det självklart varit tillåtet för en myndighet att på eget initiativ lämna uppgifter som inte är sekretessbelagda till en annan myndighet, inte minst mot bakgrund av syftet med sekretessregleringen och myndigheternas skyldighet att samverka. Lagstiftaren kan dessutom knappast ha haft möjlighet att förutse den EU-rättsliga utvecklingen på dataskyddsområdet. Både regleringen av myndigheternas möjlighet att samverka genom informationsutbyte och den svenska sekretesslagstiftningen kan därmed sägas anpassas till den allmänna dataskyddsregleringen genom den föreslagna bestämmelsen.

Bestämmelsen innebär inte att myndigheter ges rätt att behandla uppgifter om enskilda urskillningslöst eller att myndigheter kan behandla personuppgifter i strid med bestämmelser i dataskyddsförordningen, dataskyddslagen, brottsdatalagen eller kompletterande dataskyddsreglering. Bestämmelsen innebär inte heller någon begränsning av enskildas rättigheter och personuppgiftsansvarigas skyldigheter enligt främst dataskyddsförordningen (se avsnitt 6.4.3). Den innebär inte heller att mottagande myndigheter ges utrymme att behandla personuppgifter i strid med legalitetsprincipen som den bl.a. kommer till uttryck i förvaltningslagen. Tillsammans med övrig svensk rätt finns det skyddsåtgärder som medför att myndigheternas handlingsutrymme är begränsat (se avsnitt 6.4.4). Bestämmelsen möjliggör alltså inte en urskillningslös personuppgiftsbehandling hos myndigheterna.[46]

Vi har tidigare påpekat att utlämnande med stöd av bestämmelsen enbart får ske om det finns anledning att anta att det behövs för fullgörande av författningsreglerad verksamhet. Myndigheter kan dock generellt sett inte förväntas ha närmare kännedom om andra myn-

[46] Jfr EU-domstolens avgörande i C-175/20, Valsts ienemumu dienests.

digheters verksamhet och därtill hörande behov av information. Utan sådan kännedom bör det inte heller finnas någon anledning att anta att en annan myndighet kan behöva vissa uppgifter. Den generella bestämmelsen medger alltså inte heller att uppgifter får spridas urskillningslöst. Vid ett utlämnande i syfte att tillgodose någon annan myndighets behov måste den utlämnande myndigheten framför allt iaktta de krav som framgår av artikel 5.1 i dataskyddsförordningen, och därigenom bl.a. begränsa utlämnandet till de uppgifter som kan antas vara av betydelse för att den mottagande myndighetens behov ska tillgodoses.[47]

Den generella bestämmelsen om utlämnande på eget initiativ gäller vidare enbart mellan myndigheter, och inte gentemot enskilda. Bestämmelsen innebär alltså inte att myndigheter får göra personuppgifter som inte är sekretessbelagda tillgängliga för ett obegränsat antal personer.[48] Slutligen bör åter påpekas att en generell bestämmelse som *möjliggör* utlämnande av uppgifter på eget initiativ inte utgör en skyldighet för myndigheterna att sprida eller på annat sätt behandla uppgifter som inte är sekretessbelagda.

En generell bestämmelse om utlämnande av uppgifter som inte är sekretessbelagda till en annan myndighet får därför sammantaget anses vara förenlig med det väsentliga innehållet i reglering till skydd för den personliga integriteten. Att myndigheter genom bestämmelsen får möjlighet att på eget initiativ lämna uppgifter som inte är sekretessbelagda till en annan myndighet bör följaktligen inte anses vara oacceptabelt i ett demokratiskt samhälle.

6.4.7 Den föreslagna bestämmelsen är nödvändig för att åtgärda det kartlagda problemet

Vår bedömning: En generell bestämmelse om utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ är nödvändig utifrån det kartlagda problemet. Några andra sätt att åtgärda problemet på finns inte.

[47] Jfr EU-domstolens avgörande i C-268/21, Norra Stockholm Bygg.
[48] Jfr EU-domstolens avgöranden i C-184/20, Vyriausioji Tarnybinės Etikos Komisija och i C-439/19, Latvijas Republikas Saeima.

Skälen för vår bedömning

Om nödvändighet

En grundläggande aspekt när det gäller att utvärdera en inskränkning av rätten till skydd för personuppgifter är att åtgärden ska vara nödvändig. Överväganden om åtgärdens nödvändighet bör dessutom kunna föregå den mer övergripande proportionalitetsbedömningen, dvs. frågan om åtgärden är lämplig och berättigad i förhållande till den nackdel den innebär för enskilda. Först om en inskränkande åtgärd bedöms vara nödvändig bör nämligen övriga delar av proportionalitetsbedömningen vara meningsfulla att utföra. Om andra, mindre inskränkande, åtgärder hade kunnat nå samma mål bör nämligen dessa väljas i stället.[49]

Inom ramen för nödvändighetsbedömnigen måste det alltså övervägas varför inte redan existerande eller andra, mindre inskränkande, åtgärder är tillräckliga för att åtgärda problemet eller missförhållandet. Frågan om en inskränkande lagstiftningsåtgärd är nödvändig måste därför utvärderas utifrån de faktiska omständigheter som föreligger, rekvisiten eller förutsättningarna som uppställs i den inskränkande lagstiftningsåtgärden och det mål som eftersträvas med åtgärden.[50]

Även om det är upp till den nationella lagstiftaren att göra de initiala övervägandena om en åtgärd är nödvändig är det, i vart fall vad gäller skyddet för privatlivet enligt artikel 8.1 i Europakonventionen, upp till Europadomstolen att göra den slutliga bedömningen.[51] Enligt fast praxis lämnas dock ett visst handlingsutrymme till den nationella lagstiftaren. Handlingsutrymmets storlek är bl.a. beroende av vilken rättighet som aktualiseras, dess betydelse för enskilda, inskränkningens natur och syftet med den inskränkande åtgärden.

I EU-domstolens rättspraxis tillämpas en strikt behovsprövning för alla begränsningar av utövandet av rätten till skydd av personuppgifter och rätten till respekt för privatlivet med avseende på behandling av personuppgifter. Undantag från eller begränsningar i

[49] Jfr Europeiska dataskyddsstyrelsen, EDPB, *Riktlinjer 10/2020 om begränsningar enligt artikel 23 i den allmänna dataskyddsförordningen*, Version 2.1, s. 13.
[50] Jfr EDPS, *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*, 2017, s. 8, tillgänglig: https://www.edps.europa.eu/sites/default/files/publication/17-04-11_necessity_toolkit_en_0.pdf (hämtad 25-07-21).
[51] Se Europadomstolens avgörande i mål 24876/94, Coster mot Förenade kungariket, punkt 104.

förhållande till skyddet av personuppgifter får inte gå utöver gränserna för vad som är strikt nödvändigt.[52]

Den generella bestämmelsen om utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ är nödvändig

I avsnitt 4.6 i vårt delbetänkande gör vi en distinktion mellan *utökade* och *förbättrade* möjligheter att utbyta information. Syftet med det var att åskådliggöra den mest framträdande kartlagda problematiken, dvs. att det inte alltid är avsaknad av sekretessbrytande bestämmelser som förefaller vara det största hindret mot ett ändamålsenligt informationsutbyte, utan själva regleringens komplexa systematik.

De behov av förbättrade möjligheter till informationsutbyte mellan myndigheter som vi kunnat kartlägga finns inom i princip hela den offentliga sektorn. En stor del av det kartlagda behovet är bristen på rättsligt stöd för att på eget initiativ lämna relevanta uppgifter till andra myndigheter. Som vi konstaterat i avsnitt 4.8.1 avser det även uppgifter som inte är sekretessbelagda.

Distinktionen mellan utökade och förbättrade möjligheter till informationsutbyte aktualiseras även i detta sammanhang, när utlämnande av uppgifter som inte är sekretessbelagda diskuteras. Uppgifter som inte är sekretessbelagda är uppgifter som det inte råder något förbud mot att röja enligt sekretessregleringen. Sådana uppgifter har myndigheter dessutom en långtgående skyldighet att lämna till en annan myndighet på begäran, utan någon begränsning till vissa syften, ändamål eller behov hos mottagaren. Ur ett sekretessrättsligt perspektiv är det alltså inte tal om någon faktisk *utökning* av möjligheterna till informationsutbyte mellan myndigheter. Som vi redan nämnt är dock utrymmet för att på eget initiativ lämna uppgifter som det enligt sekretessregleringen inte råder något förbud mot att röja i dag ofta mer begränsat än om uppgifterna hade träffats av ett röjandeförbud och därför även träffats av ett undantag från sagda förbud (jfr avsnitt 4.8.4).

Dagens paradoxala regleringssituation bör vara ett resultat av att sekretessregleringen och dataskyddsregleringen ska tillämpas parallellt och har samma övergripande syfte, men närmar sig frågan om integritetsskydd från motsatt håll. I den svenska sekretessregleringen är

[52] Se EU-domstolens avgöranden i C-73/07, Tietosuojavaltuutettu/Satakunnan Markkinapörssi Oy och Satamedia Oy, punkt 56 och i C 623/17, Privacy International, punkt 68.

det *förbudet* mot att röja en uppgift som måste regleras genom bestämmelser om sekretess. I den dataskyddsrättsliga kontexten måste i stället *tillåtligheten* av en vidarebehandling regleras. Eftersom det i svensk rätt inte finns någon generell tillåtande reglering av vidarebehandling genom utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ så uppstår många gånger i praktiken ett dataskyddsrättsligt hinder mot sådant utlämnande.

För att offentlighets- och sekretesslagens bestämmelser ska kunna uppfylla sitt syfte, dvs. att reglera de röjandeförbud som ska gälla inom den offentliga förvaltningen, måste alltså den nationella rätten anpassas till den allmänna EU-rättsliga dataskyddsregleringen. Något annat sätt att utföra denna anpassning på än att införa en bestämmelse som kompletterar 6 kap. 5 § OSL, och som i likhet med den bestämmelsen avser utlämnande av uppgifter som inte är sekretessbelagda till andra myndigheter, men som avser utlämnande på eget initiativ, finns inte enligt vår bedömning. Det finns alltså inga mindre inskränkande åtgärder att tillgå för att uppnå det eftersträvade målet. Bestämmelsen som vi föreslagit är därför nödvändig.

6.4.8 En lämplig och berättigad bestämmelse

Vår bedömning: Den föreslagna generella bestämmelsen om utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ är både lämplig och berättigad i förhållande till den nackdel den innebär för enskilda. Bestämmelsen är därmed proportionerlig.

Skälen för vår bedömning

Bestämmelsen är generellt sett lämplig och berättigad

En förutsättning för att en inskränkande åtgärd ska framstå som berättigad är att åtgärden är lämplig för att uppnå det eftersträvande målet. Att åtgärden ska vara lämplig betyder att det ska finnas ett logiskt samband mellan åtgärden och det legitima, eftersträvade målet. Att en åtgärd är berättigad innebär att fördelarna med åtgärden väger tyngre än de nackdelar för enskilda som det innebär att rätten till skydd för personuppgifter inskränks.

I avsnitt 6.4.2 har vi konstaterat att en bestämmelse om utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ åtgärdar de faktiska och konkreta problem vi kunnat kartlägga. I avsnitt 6.4.7 har vi nyss konstaterat att bestämmelsen dessutom är nödvändig för att åtgärda de problem vi identifierat. Att det finns ett logiskt samband mellan det kartlagda behovet och den föreslagna åtgärden står därmed klart, vilket innebär att den är *lämplig* för att uppnå det eftersträvade målet.

Vad gäller frågan om bestämmelsen är *berättigad* har vi i avsnitt 6.3 redogjort för de risker för enskilda som vi bedömer att en generell bestämmelse om utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ ger upphov till. I avsnitt 6.4.3 har vi även konstaterat att bestämmelsen utgör en inskränkning i enskildas rätt till skydd för personuppgifter. De är alltså dessa risker och detta förhållande som vid prövningen av om bestämmelsen är berättigad ska vägas mot de fördelar som kan uppnås med bestämmelsen.

Som vi redan konstaterat i avsnitt 6.4.7 förefaller det underliggande behovet av den bestämmelse vi föreslår vara att det på grund av den EU-rättsliga utvecklingen uppstått ett dataskyddsrättsligt hinder mot att på eget initiativ lämna ut uppgifter som det enligt den svenska sekretessregleringen inte finns några förbud mot att lämna ut till en annan myndighet. Detta dataskyddsrättsliga hinder innebär att myndigheters samverkansskyldighet vad gäller informationsutbyte inte längre enbart begränsas av sekretessregleringen, vilket utifrån förarbetsuttalanden verkar ha varit lagstiftarens avsikt[53], utan även av en ”krock” mellan två olika lagtekniska system som båda syftar till att åstadkomma ett adekvat integritetsskydd. Det skydd för uppgifter om enskilda som uppställs genom det dataskyddsrättliga hindret mot att på eget initiativ lämna uppgifter som inte är sekretessbelagda till andra myndigheter förefaller alltså snarare vara ett resultat av ett förbiseende från lagstiftaren sida, än av medvetna överväganden. Detta har bl.a. gett upphov till en komplex och motstridig reglering. Betydelsen av att svensk rätt anpassas till överordnad reglering i detta avseende bör därför väga mycket tungt.

I avsnitt 6.3.3 har vi vidare konstaterat att det inte är andra uppgifter än i dag som kommer att kunna utbytas mellan myndigheter med stöd av bestämmelsen. Det är alltså enbart sådana uppgifter som myndigheter redan har en långtgående skyldighet att på begäran

[53] Jfr prop. 1979/80:2, *med förslag till sekretesslag m.m.*, Del A, s. 89 och 361.

lämna till andra myndigheter, utan några begränsningar vad gäller syfte, ändamål eller behov, som träffas av bestämmelsen.

I avsnitt 6.4.2 har vi redogjort för de viktiga mål av generellt allmänt intresse som på ett övergripande plan motiverar att myndigheter ges bättre möjligheter att utbyta information. Däri ingår bl.a. brottsoffers rätt till skydd genom att få den upprättelse som en lagföring av förövaren innebär, barn och ungas rätt att få skydd från ett liv i kriminalitet samt det starka intresset av att skydda de gemensamma resurserna från att gå till kriminella, och därmed i förlängningen upprätthållandet av välfärdssystemen. Ett särskilt viktigt mål är att myndigheterna kan utföra sin verksamhet på ett korrekt, rättssäkert och effektivt sätt, samt att samverka, vilket kan vara mycket positivt för enskilda som kommer i kontakt med myndigheterna.

I avsnitt 6.4.6 har vi gjort bedömningen att bestämmelsen är godtagbar i ett demokratiskt samhälle och förenlig med de grundläggande bestämmelserna om dataskydd.

I avsnitt 6.4.4 har vi vidare konstaterat att bestämmelsen bl.a. inte ger myndigheter obegränsat handlingsutrymme, vare sig taget för sig eller sedd tillsammans med övrig reglering som styr hur myndigheter får hantera information om enskilda.

Mot bakgrund av de överväganden vi redogjort för ovan är vår bedömning att den generella bestämmelsen om utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ framstår som både lämplig och berättigad (dvs. proportionerlig) på ett generellt plan, trots de integritetsrisker som bestämmelsen medför och trots att den innebär en inskränkning av enskildas rätt till skydd för personuppgifter.

Särskilt om uppgifter om barn och barnkonventionen

I avsnitt 6.3.4 har vi redogjort för att en generell bestämmelse om utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ medför integritetsrisker för barn. Uppgifter om barn är särskilt skyddsvärda enligt den allmänna dataskyddsregleringen. Av artikel 3 i barnkonventionen följer att vid alla åtgärder som rör barn ska i första hand beaktas vad som bedöms vara barnets bästa, vare sig de vidtas av offentliga eller privata sociala välfärdsinstitutioner, domstolar, administrativa myndigheter eller lagstiftande organ.

Barnkonventionen ska ses som en helhet och rättigheterna i konventionen ska tolkas i relation till varandra.[54] När det gäller att säkerställa ett barns rättigheter finns inte alltid enkla och givna lösningar. Det handlar oftast om att väga olika intressen mot varandra och i praktiken kan det innebära att nödvändiga val och prioriteringar måste göras. Även om ett utökat informationsutbyte i och för sig innebär en generell integritetsrisk för barn, så kan det samtidigt vara nödvändigt för att samhället ska kunna tillgodose barns behov och tillförsäkra barn deras rättigheter.

Som vi nämnt i avsnitt 6.4.2 gör sig i princip samma skäl gällande i det här sammanhanget som för förslaget om en generell sekretessbrytande bestämmelse. Vid bedömningen av förslagets förenlighet med barnkonventionen måste det därmed beaktas att ett tungt vägande skäl för såväl den tidigare föreslagna sekretessbrytande bestämmelsen som det nu aktuella förslaget är intresset av att skydda barn från att utnyttjas och dras in i brottslighet. Barnombudsmannen har i remissvar på delbetänkandet bl.a. välkomnat ett stärkt informationsutbyte mellan myndigheter i syfte att skydda och stödja barn i utsatta situationer/som riskerar att fara illa, och påpekat vikten av att förenkla informationsdelningen mellan myndigheter så att sekretess inte utgör ett hinder i de fall där barn och unga kan behöva stöd eller skydd.[55]

Även uppgifter som inte är sekretessbelagda av andra skäl än att de träffas av en sekretessbrytande bestämmelse, dvs. uppgifter som efter en sekretessprövning får lämnas ut eller som omfattas av ett undantag från sekretess, kan behöva lämnas ut i syfte att uppmärksamma en annan myndighet på barn och ungas behov av skydd eller stöd. Barn och ungas utsatthet inom kriminell verksamhet är alltså ett starkt skäl till att även den nu aktuella bestämmelsen framstår som motiverad, eftersom barn och unga drabbas särskilt hårt av de problem vi kartlagt och redovisat i vårt delbetänkande. Även andra barn i det utsatta barnets närhet, t.ex. i skola, fritidsverksamhet eller familj kan behöva skyddas.

Förslaget om en generell bestämmelse om utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ innebär alltså att uppgifter om barn med stor sannolikhet kommer att lämnas ut i brotts-

[54] Prop. 2017/18:186, *Inkorporering av FN:s konvention om barnets rättigheter*, s. 77.
[55] Barnombudsmannen, *Remittering av delbetänkandet Ökat informationsutbyte mellan myndigheter – Behov och föreslagna förändringar (SOU 2024:63)*, Dnr: 2024-0236.

förebyggande syfte i högre utsträckning än i dag. Som vi noterat tidigare går det dock inte fullt ut att bedöma i vilken utsträckning sådant utlämnande kommer att utökas på grund av bestämmelsen. För att stärka skyddet för barn som riskerar att fara illa i kriminella sammanhang är det dock viktigt att möjligheten till uppgiftslämnande på eget initiativ finns och utnyttjas när det uppstår ett behov av det, även vad gäller uppgifter som annars inte är sekretessbelagda.

Det faktum att barn begår och utsätts för brott visar enligt vår mening *i sig* att det krävs fler och kraftfulla åtgärder för att motverka denna utveckling. Tillgång till information är många gånger en grundläggande förutsättning för att myndigheter, särskilt socialtjänsten, ska kunna vidta lämpliga åtgärder. En generell bestämmelse om utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ, som kompletterar 6 kap. 5 § OSL och därigenom tydliggör myndigheternas skyldighet att samverka, kan bidra till att fler barn som riskerar att begå brott eller utsättas för brottslig verksamhet får adekvata insatser, vilket i sig innebär ett stärkt skydd för barn.

Den föreslagna bestämmelsen medför förbättrade möjligheter till utlämnande på eget initiativ både av uppgifter som annars inte är sekretessbelagda och uppgifter som annars är sekretessbelagda men som träffas av en sekretessbrytande bestämmelse. Det bör innebära förbättrade möjligheter för andra myndigheter att lämna relevanta uppgifter t.ex. till socialtjänsten i ett tidigt skede, innan någon brottslig handling har begåtts. På samma sätt möjliggör bestämmelsen också utlämnande av uppgifter som inte är sekretessbelagda som i förlängningen kan motverka att barn växer upp i våldsamma miljöer eller i utsatta förhållanden.

Genom en generell bestämmelse om utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ kan myndigheterna sammanfattningsvis få tillgång till fler uppgifter om enskilda individer, även vuxna, som kan vara av stort värde för myndigheternas möjligheter att vidta adekvata åtgärder. Intresset av att barn som lever under svåra förhållanden får adekvat stöd och hjälp väger dock enligt vår mening tyngre än vuxnas personliga integritet.

Bestämmelsen om utlämnande på eget initiativ innebär ingen skyldighet för myndigheter att lämna uppgifter som inte är sekretessbelagda till en annan myndighet. Som vi konstaterat tidigare måste dessutom barnkonventionen beaktas i situationer där det övervägs om uppgifter som rör barn och som inte är sekretessbelagda ska

lämnas ut till en annan myndighet. Barnkonventionen måste även beaktas av mottagaren av uppgifterna.

Sammantaget framstår den generella bestämmelsen om utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ som en lämplig och berättigad åtgärd även i förhållande till barns särskilda behov av skydd för personuppgifter. Förslaget bedöms i sin helhet bidra till att tillförsäkra barn det skydd som krävs enligt, och är därmed förenlig med, barnkonventionen.

6.4.9 En rättslig grund för personuppgiftsbehandling

Vår bedömning: Genom den föreslagna bestämmelsen får myndigheter en rättslig grund för att på eget initiativ lämna ut uppgifter som inte är sekretessbelagda till andra myndigheter i enlighet med bestämmelsen. Den personuppgiftsbehandling i form av utlämnande som blir en följd av förslaget kommer vara nödvändig för att utföra en uppgift av allmänt intresse.

Skälen för vår bedömning

Enligt dataskyddsförordningen är det lagstiftarens sak att genom lagstiftning tillhandahålla den rättsliga grunden för myndigheters behandling av personuppgifter. Av 2 kap. 1–2 §§ dataskyddslagen framgår att rättsliga grunder för myndigheters personuppgiftsbehandling huvudsakligen utgörs av lag eller förordning, eller beslut som har meddelats med stöd av lag eller förordning. Den generella bestämmelsen om utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ föreslås införas i lag, vilket innebär att den uppfyller formkravet på en rättslig grund för personuppgiftsbehandling.

Ett grundläggande krav på en rättslig grund för myndigheters personuppgiftsbehandling är dock att den ska uppfylla ett mål av allmänt intresse och vara proportionell mot det legitima mål som eftersträvas (artikel 6.3 i dataskyddsförordningen). Vi har i detta kapitel gjort bedömningen att den generella bestämmelsen om utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ uppfyller dessa krav. Den generella bestämmelsen utgör därmed en rättslig grund för den behandling av personuppgifter som är för-

knippad med sådant informationsutbyte mellan myndigheter som omfattas av bestämmelsen.

Bestämmelsen kompletterar 6 kap. 5 § OSL, som innebär att myndigheter har en skyldighet att på begäran av en annan myndighet lämna ut uppgifter som inte är sekretessbelagda. Den generella bestämmelsen om utlämnande av samma slags uppgifter på eget initiativ medför dock inte att det uppstår någon skyldighet, utan endast en möjlighet, att lämna ut uppgifter. Eftersom bestämmelsen inte utgör en skyldighet för myndigheter kommer behandlingen inte aktualisera artikel 6.1 c i dataskyddsförordningen, dvs. sådan behandling som är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige. Den personuppgiftsbehandling som blir en följd av förslaget kommer dock vara nödvändig för att utföra en uppgift av allmänt intresse (artikel 6.1 e och 2 kap. 2 § dataskyddslagen).

I avsnitt 5.4.1 har vi redogjort för att det i kompletterande dataskyddsreglering ofta görs en skillnad mellan primära ändamål och sekundära ändamål med personuppgiftsbehandling. Primära ändamål är sådana ändamål som går att hänföra till den processuella eller materiella regleringen av en myndighets egen verksamhet. Sekundära ändamål avser hur personuppgifter som redan har samlats in och behandlas i verksamheten för de primära ändamålen får vidarebehandlas, t.ex. genom utlämnande till andra myndigheter i överensstämmelse med lag eller förordning. Personuppgiftsbehandling med stöd av den generella bestämmelsen om utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ kommer att ske för sekundära ändamål.

6.5 Förslagen om ändringar i den kompletterande dataskyddsregleringen och brottsdatalagen

6.5.1 Förslaget om uppgiftslämnande i överensstämmelse med lag eller förordning

Vår bedömning: Förslaget om att det ska införas upplysningsbestämmelser om utlämnande i överensstämmelse med lag eller förordning i kompletterande dataskyddsreglering utgör inte en sådan förändring av gällande rätt som påverkar enskildas rätt till skydd för personuppgifter.

Skälen för vår bedömning

Förbud mot att röja en uppgift regleras i offentlighets- och sekretesslagen

Förslaget i avsnitt 5.4.6 innebär att det införs nya eller ändrade sekundära ändamål om uppgiftslämnande i överenstämmelse med lag eller förordning i den kompletterande dataskyddsreglering som omfattas av vår översyn. I det avsnittet har vi konstaterat att de nya sekundära ändamålen endast utgör upplysningsbestämmelser, eftersom den rättsliga grunden för personuppgiftsbehandling genom uppgiftsutbyte mellan myndigheter finns i offentlighets- och sekretesslagens bestämmelser, och inte i den kompletterande dataskyddsregleringen. Offentlighets- och sekretesslagen är dessutom den författning som i svensk rätt reglerar samtliga förbud mot att röja en uppgift, eller i dataskyddsrättsliga termer förbud mot vidarebehandling genom utlämnande till andra, som ska gälla. Detta sker antingen direkt i den lagen eller genom hänvisningar i lagen till annan författning.

Införandet av upplysningsbestämmelser i kompletterande dataskyddsreglering som motsvarar det nyss sagda medför alltså inte att myndigheter får vare sig utökade eller mindre rättsliga möjligheter till personuppgiftsbehandling genom uppgiftsutbyte med andra myndigheter. Enskildas rätt till skydd för personuppgifter påverkas alltså inte av de föreslagna förändringarna.

Som vi påpekat i avsnitt 5.4.6 kan införandet av upplysingsbestämmelser i stället snarare ses som en integritetshöjande åtgärd. Bestämmelser som *tydliggör* att personuppgifter får behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning bidrar nämligen till ökad transparens för de registrerade vars uppgifter behandlas. Även om bestämmelserna varken har någon sekretessbrytande verkan eller utgör självständiga rättsliga grunder för personuppgiftsbehandling, så kan de alltså bidra till ökad förutsebarhet i frågan om hur uppgifter om enskilda registrerade får behandlas.

Behov av följdändringar?

Trots det som sägs ovan går det inte att bortse från att det under en lång tid rått osäkerhet om det rättsliga förhållandet mellan sekretess- och dataskyddsbestämmelser, vilket vi översiktligt redogjort för i

avsnitt 5.4.2. Någon formell och tydlig samordning mellan regelverken har dock aldrig införts. Att så inte skett kan förklara att även lagstiftaren i några sammanhang verkar ha utgått från att ändamålsbestämmelser i kompletterande dataskyddsreglering kan begränsa tillämpligheten av bestämmelserna i offentlighets- och sekretesslagen, vilket vi redogör för i avsnitt 5.4.7. I det avsnittet har vi även uppmärksammat att det därför kan finns skäl för att överväga om den materiella sekretessregleringen på vissa områden ska ändras för att motsvara lagstiftarens förmodade syfte med att införa ändamålsbestämmelserna.

Att lagstiftaren, eventuellt av förbiseende, inte har utformat den materiella sekretessregleringen så att den motsvarar vad som sägs i förarbetena om hur vissa uppgifter inte bör få utbytas mellan myndigheter kan dock inte ändra grundförhållandet i svensk rätt, dvs. att samtliga förbud mot att röja en uppgift ska framgå av offentlighets- och sekretesslagen, antingen direkt eller genom hänvisning till en annan författning. De föreslagna bestämmelserna om uppgiftslämnande i överensstämmelse med lag eller förordning tydliggör alltså gällande rätt, men medför ingen förändring av rättsläget. Även i de sammanhang som nämns i avsnitt 5.4.7 utgör de föreslagna förändringarna i den kompletterande dataskyddsregleringen alltså enbart upplysningsbestämmelser som inte påverkar enskildas rätt till skydd för personuppgifter.

6.5.2 Förslaget om förändringar i brottsdatalagen

Vår bedömning: Förslaget om att det i brottsdatalagen inte ska göras någon dataskyddsrättlig åtskillnad mellan olika former av sekretessbrytande bestämmelser utgör inte en sådan förändring av gällande rätt som påverkar enskildas rätt till skydd för personuppgifter.

Skälen för vårt förslag

Förslaget i avsnitt 5.5.2 innebär att den dataskyddsrättsliga regleringen inom det brottsbekämpande området får samma förhållande till offentlighets- och sekretesslagens bestämmelser som dataskyddsreglering som kompletterar dataskyddsförordningen.

Ändringarna innebär att en behörig myndighet inte behöver utföra några andra prövningar inför ett utlämnande än om det är tillåtet enligt offentlighets- och sekretesslagen, dock självfallet med iakttagande av vad som följer av allmänna dataskyddsrättsliga principer, t.ex. principen om uppgiftsminimering. Detta ska gälla oavsett om uppgiftsutlämnandet sker till en annan behörig myndighet som ska behandla uppgifterna för ett ändamål inom brottsdatalagens tillämpningsområde eller om uppgifterna lämnas ut till en myndighet som ska behandla dem för ändamål utanför brottsdatalagens tillämpningsområde.

Som vi konstaterat i avsnitt 5.4.4 är offentlighets- och sekretesslagen den författning som i svensk rätt reglerar samtliga förbud mot att röja en uppgift, eller i dataskyddsrättsliga termer förbud mot vidarebehandling genom utlämnande till andra, som ska gälla. Detta sker antingen direkt i den lagen eller genom hänvisningar i lagen till annan författning. De föreslagna förändringarna i brottsdatalagen medför alltså inte att behöriga myndigheter får vare sig utökade eller mindre rättsliga möjligheter till personuppgiftsbehandling genom uppgiftsutbyte med andra myndigheter. Enskildas rätt till skydd för personuppgifter påverkas alltså inte av de föreslagna förändringarna. Som vi påpekat i avsnitt 5.5.2 kan förslaget i stället ses som en integritetshöjande åtgärd.

6.5.3 Förslaget om elektroniskt utlämnande på annat sätt än genom direktåtkomst

Våra bedömningar: Förslaget om att elektroniskt utlämnande på annat sätt än genom direktåtkomst ska vara tillåtet om det inte är olämpligt medför inte väsentligt förhöjda integritetsrisker eller en inskränkning av enskildas rätt till skydd för personuppgifter.

Förslaget är motiverat och proportionerligt.

Skälen för vår bedömning

Vid alla former av utlämnande från en myndighet till en annan finns det en risk för att uppgifterna behandlas på ett annat sätt än som ursprungligen varit avsikten, eller i ett sammanhang där de inte behövs. Det gäller dock oavsett om utlämnande sker med digitala hjälpmedel eller analogt.

I kompletterande dataskyddsreglering förekommer reglering som hindrar myndigheter från att använda sig av digitala kommunikationssätt, dvs. elektroniskt informationsutbyte. Befintliga hinder mot elektroniskt informationsutbyte utgår från antagandet att det är datoranvändandet *som sådant* som utgör en integritetsrisk (jfr avsnitt 5.2). Mot bakgrund av den tekniska utvecklingen går det dock inte längre att utgå från att integritetsriskerna är lägre vid ett analogt utlämnande än vid ett elektroniskt utlämnande. Användandet av olika digitala lösningar kan i stället innebära en högre grad av skydd för personuppgifter än om ett pappersbrev eller en fax hade skickats, eller om information hade lämnats muntligt. Under förutsättning att utlämnandet sker med tillämpning av tillgängliga tekniker för säker informationsöverföring kan elektroniskt utlämnande alltså innebära ett starkare integritetsskydd än vid analog hantering.

Dataskyddsförordningen ska dessutom tillämpas av myndigheterna som vore det en svensk författning. Dataskyddsförordningen innehåller i och för sig inte några bestämmelser som uttryckligen tar sikte på sättet att lämna ut personuppgifter. I kapitel 3 har dock vi redogjort för dataskyddsförordningens krav på myndigheter som aktualiseras vid elektroniskt utlämnande. När det övervägs på vilket sätt information ska överföras måste det, som vid all annan behandling, enligt dataskyddsförordningen göras ett flertal avvägningar mellan de intressen som talar för en viss teknisk lösning, och de integritetsskäl som talar emot. Det bör därför inte vara möjligt för en myndighet att iaktta dataskyddsförordningens direkt tillämpliga bestämmelser utan att ägna tillräcklig uppmärksamhet åt frågor om t.ex. informationssäkerhet och integritetsskydd vid elektroniskt utlämnande. Detta framgår av den föreslagna bestämmelsen genom att sådant utlämnande enbart är tillåtet om det inte är olämpligt. Bestämmelsen medför alltså inte annat än en *möjlighet* för myndigheter att lämna ut uppgifter elektroniskt, och därmed inte heller någon rätt för mottagare att få ut uppgifter i någon särskild form, vilket vi ut-

vecklar i avsnitt 5.6.3. I det avsnittet har vi också gjort ytterligare överväganden om förslagets förhållande till integritetsrisker m.m.

Sammantaget bedömer vi att förslaget om att elektroniskt utlämnande på annat sätt än genom direktåtkomst ska vara tillåtet om det inte är olämpligt inte innebär några väsentligt förhöjda integritetsrisker och att det inte heller innebär att enskildas rätt till skydd för personuppgifter inskränks.

Som vi redovisat i avsnitt 5.6.3 har samhällets generella övergång till digital informationshantering medfört att informationsflödet, såväl mellan myndigheter som i övrigt, numera främst är digitalt. Regeringen har t.ex. uttalat att en manuell informationshantering i dag kan inte sägas vara ett realistiskt alternativ för vare sig myndigheter eller företag.[56] Regeringen har även uttalat att målet för digitaliseringen av den offentliga förvaltningen bl.a. är en enklare vardag för medborgare och högre kvalitet och effektivitet i verksamheten. Vidare har regeringen gjort bedömningen att digitalt ska vara förstahandsval i den offentliga förvaltningens verksamhet.[57]

Begränsningar av myndigheters möjlighet att använda sig av digital kommunikation, som dels inte medför några tydliga vinster i integritetshänseende, dels utgår från helt andra möjligheter till informationshantering än dagens, kan därför inte längre vara anses vara motiverade. Sådana begränsningar bör alltså i dag anses utgöra omotiverade hinder mot att myndigheterna utför sin verksamhet på ett effektivt sätt. Då en manuell informationshantering inte längre kan anses vara ett realistiskt alternativ för myndigheter måste slutsatsen vara att förslaget om elektroniskt utlämnande på annat sätt än genom direktåtkomst är motiverat av viktiga allmänna intressen. Som vi nämnt tidigare har regeringen nämligen också bedömt att det är ett viktigt allmänt intresse att svenska myndigheter även utanför området för myndighetsutövning kan bedriva den verksamhet som tydligt faller inom ramen för deras befogenheter på ett korrekt, rättssäkert och effektivt sätt.[58]

Förslaget om att elektroniskt utlämnande på annat sätt än genom direktåtkomst ska vara tillåtet om det inte är olämpligt åtgärdar den nämnda problematiken och framstår både som nödvändigt, lämpligt och berättigat. Det är därmed proportionerligt.

[56] Prop. 2017/18:105, *Ny dataskyddslag*, s. 47.
[57] Budgetpropositionen för 2019, prop. 2018/19:1 utg. omr. 2, s. 53.
[58] Prop. 2017/18:105, *Ny datsskyddslag*, s. 83.

7 Ikraftträdande och övergångsbestämmelser

Vårt förslag: Författningsändringarna ska träda i kraft den 1 oktober 2026.

Vår bedömning: Det finns inget behov av särskilda övergångsbestämmelser.

Skälen för vår bedömning

Vi har i det här betänkandet föreslagit att det i offentlighets- och sekretesslagen (2009:400) ska införas en generell bestämmelse som ger myndigheterna ett tydligt rättsligt stöd för att lämna ut uppgifter som inte är sekretessbelagda till andra myndigheter på eget initiativ. Vi har även föreslagit att det ska införas upplysningsbestämmelser i kompletterande dataskyddsreglering som omfattas av vår översyn, som tydliggör att uppgiftslämnande i överensstämmelse med lag eller förordning är tillåtet, och att elektroniskt utlämnande på annat sätt än genom direktåtkomst ska vara tillåtet om det inte är olämpligt. Några särskilda anpassningar eller åtgärder som påverkar ikraftträdandet av de föreslagna bestämmelserna behöver inte göras. Med hänsyn tagen till remissförfarandet, till det sedvanliga beredningsarbetet inom Regeringskansliet och till riksdagsbehandlingen bedömer vi att tidpunkten den 1 oktober 2026 är realistisk. Mot bakgrund av förslagens karaktär, dvs. att de dels rör uppgifter som det i dag inte råder något förbud mot att lämna ut, dels utgör upplysningsbestämmelser, och dels utgör en nödvändig anpassning till digitaliseringen av den offentliga förvaltningen, bedömer vi att några övergångsbestämmelser inte behövs.

8 Konsekvenser

8.1 Inledning

Av kommittéförordningen (1998:1474) framgår att en utredning ska redovisa vilka konsekvenser de förslag som utredningen lämnar kan ha i flera olika avseenden. Utöver bestämmelserna i kommittéförordningen finns i förordningen om konsekvensutredningar (2024:183) bestämmelser om vad en utredning ska redovisa. Den förordningen trädde i kraft den 6 maj 2024 och gäller enligt övergångsbestämmelserna inte de utredningar som tillsatts före ikraftträdandet. För sådana utredningar gäller i stället kommittéförordningens bestämmelser i 14–15 a § i den äldre lydelsen samt 6 och 7 §§ i den numera upphävda förordningen (2007:1244) om konsekvensutredning vid regelgivning.

Av dessa bestämmelser framgår att om förslagen i ett betänkande påverkar kostnaderna eller intäkterna för staten, kommuner, regioner, företag eller andra enskilda, ska en beräkning av dessa konsekvenser redovisas i betänkandet. Om förslagen innebär samhällsekonomiska konsekvenser i övrigt, ska dessa redovisas När det gäller kostnadsökningar och intäktsminskningar för staten, kommuner eller regioner, ska kommittén föreslå en finansiering (14 § kommittéförordningen).

Om förslagen i ett betänkande har betydelse för den kommunala självstyrelsen, ska konsekvenserna i det avseendet anges i betänkandet. Detsamma gäller när ett förslag har betydelse för brottsligheten och det brottsförebyggande arbetet, för sysselsättning och offentlig service i olika delar av landet, för små företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt i förhållande till större företags, för jämställdheten mellan kvinnor och män eller för möjligheterna att nå de integrationspolitiska målen (15 § kommittéförordningen).

Om ett betänkande innehåller förslag till nya eller ändrade regler, ska förslagens kostnadsmässiga och andra konsekvenser anges på ett sätt som motsvarar de krav på innehållet i konsekvensutredningar

som finns i 6 och 7 §§ förordningen om konsekvensutredning vid regelgivning (15 a § kommittéförordningen).

Av dessa bestämmelser framgår att en konsekvensutredning ska innehålla följande.

- en beskrivning av problemet och vad man vill uppnå,
- en beskrivning av vilka alternativa lösningar som finns för det man vill uppnå och vilka effekterna blir om någon reglering inte kommer till stånd,
- uppgifter om vilka som berörs av regleringen,
- uppgifter om vilka kostnadsmässiga och andra konsekvenser regleringen medför och en jämförelse av konsekvenserna för de övervägda regeringsalternativen,
- en bedömning av om regleringen överensstämmer med eller går utöver de skyldigheter som följer av Sveriges anslutning till Europeiska unionen, och
- en bedömning av om särskilda hänsyn behöver tas när det gäller tidpunkten för ikraftträdande och om det finns behov av speciella informationsinsatser (6 § förordningen om konsekvensutredning vid regelgivning).

Kan regleringen få effekter av betydelse för företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt ska konsekvensutredningen, utöver vad som följer av 6 § och i den omfattning som är möjlig, innehålla en beskrivning av följande:

- antalet företag som berörs, vilka branscher företagen är verksamma i samt storleken på företagen,
- vilken tidsåtgång regleringen kan föra med sig för företagen och vad regleringen innebär för företagens administrativa kostnader,
- vilka andra kostnader den föreslagna regleringen medför för företagen och vilka förändringar i verksamheten som företagen kan behöva vidta till följd av den föreslagna regleringen,
- i vilken utsträckning regleringen kan komma att påverka konkurrensförhållandena för företagen,

- hur regleringen i andra avseenden kan komma att påverka företagen, och
- om särskilda hänsyn behöver tas till små företag vid reglernas utformning (7 § förordningen om konsekvensutredning vid regelgivning).

Enligt våra direktiv ska vi härutöver genomföra en integritetsanalys och redovisa vilka konsekvenser förslagen innebär för spridandet av personuppgifter inom och mellan myndigheter.

8.2 Våra förslag

I detta betänkande föreslår vi att det ska införas en bestämmelse i offentlighets- och sekretesslagen (2009:400), OSL, som innebär att myndigheter får lämna ut uppgifter som inte är sekretessbelagda på eget initiativ om utlämnandet kan antas ha betydelse för att den utlämnande eller den mottagande myndigheten ska kunna fullgöra sin författningsreglerade verksamhet. Vi föreslår också ändringar i den kompletterande dataskyddsregleringen som innebär att det inte kommer föreligga några upplevda dataskyddsrättsliga hinder mot tillämpningen av offentlighets- och sekretesslagens bestämmelser, och att omotiverade hinder mot elektroniskt utlämnande på annat sätt än genom direktåtkomst tas bort.

Genom den föreslagna bestämmelsen i offentlighets- och sekretesslagen införs ett generellt rättsligt stöd för att lämna ut uppgifter som inte är sekretessbelagda till andra myndigheter på eget initiativ. Det ska dock påpekas att den generella sekretessbrytande bestämmelsen som vi föreslog i delbetänkandet på samma sätt som andra sekretessbrytande bestämmelserna i offentlighets- och sekretesslagen i sig utgör ett rättsligt stöd för myndigheterna att lämna ut annars sekretessbelagda uppgifter som träffas av bestämmelserna på eget initiativ, även om det inte uttryckligen framgår av dessa bestämmelser. Det innebär att den bestämmelse vi nu föreslår endast utgör ett förtydligande av vad som redan gäller avseende sådana uppgifter.

De sekretessbrytande bestämmelserna i offentlighets- och sekretesslagen är begränsade i de avseendet att de endast träffar uppgifter som från början har bedömts vara sekretessbelagda i det sammanhang de förekommer. Bestämmelserna kan alltså rent lagtekniskt

inte åberopas som stöd för att på eget initiativ lämna ut uppgifter som är undantagna från sekretess, uppgifter som efter en prövning enligt en materiell sekretessbestämmelse inte är sekretessbelagda och uppgifter som över huvud taget inte är sekretessreglerade. När det gäller dessa uppgifter innebär den föreslagna bestämmelsen en materiell förändring av rättsläget, eftersom det i dag inte finns något generellt rättsligt stöd för myndigheterna att lämna ut sådana uppgifter på eget initiativ.

Vi föreslår dessutom att det ska införas upplysningsbestämmelser i den kompletterande dataskyddsregleringen om att personuppgifter också får behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning. Genom dessa bestämmelser tydliggörs att frågan om en uppgift är sekretessbelagd eller om den får lämnas ut från en myndighet till en annan myndighet regleras i offentlighets- och sekretesslagen, och inte i den kompletterande dataskyddsregleringen. Syftet med förslaget i denna del är att undanröja upplevda regelkonflikter mellan offentlighets- och sekretesslagen och den kompletterande dataskyddsregleringen.

Slutligen föreslår vi att omotiverade rättsliga begränsningar av myndigheternas möjligheter att lämna ut uppgifter elektroniskt på annat sätt än genom direktåtkomst ska upphävas. I stället ska elektroniskt utlämnande av personuppgifter, som inte utgör direktåtkomst, vara tillåtet om det inte är olämpligt. Vi föreslår också en språklig modernisering av de bestämmelser i den kompletterande dataskyddsregleringen som reglerar myndigheternas möjligheter att lämna ut uppgifter elektroniskt på annat sätt än genom direktåtkomst.

8.3 Några utgångspunkter

Som framgår av avsnitt 4.7 visar bl.a. den kartläggning som vi genomförde i delbetänkandet (se kapitel 4 i SOU 2024:63) att myndigheterna har ett behov av att på eget initiativ lämna ut uppgifter till andra myndigheter. Av skäl som redogörs för i avsnitt 4.8.1 menar vi att man utifrån detta förhållande kan dra slutsatsen att detta också omfattar uppgifter som inte är sekretessbelagda i förhållande till mottagaren. Mot bakgrund av kartläggningen anser vi att det finns fog för antagandet att informationsutbytet mellan myndigheter

kommer att öka om våra förslag genomförs, vilket vi utvecklat i avsnitt 8.5.

Bestämmelsen är generell och ska tillämpas av samtliga aktörer som ska jämställas med myndigheter vid tillämpningen av offentlighets- och sekretesslagen (jfr 2 kap. 3–4 §§ OSL och bilagan till den lagen). Det förhållandet att det är en så pass brokig och omfattande skara aktörer som kommer att tillämpa den föreslagna bestämmelsen gör, enligt vår mening, varje försök att uppskatta vilket genomslag den kommer att få osäkert.

I vårt delbetänkande (se avsnitt 4.2 i SOU 2024:63) redogör vi för ett urval av aktuella lagstiftningsinitiativ med syfte att utöka, eller förbättra möjligheterna till, informationsutbytet mellan myndigheter. I delbetänkandet gör vi bedömningen att det förhållandevis stora antal förslag som har lämnats och som kommer att lämnas inom en snar framtid sammantaget innebar vissa svårigheter att bedöma effekterna av det förslag vi lämnar där. Denna iakttagelse bör vara relevant också i detta sammanhang.

Även om den föreslagna bestämmelsen om utlämnande av uppgifter på eget initiativ under alla förhållanden kan förutsättas leda till ett utökat informationsutbyte mellan myndigheter är frågan om utbytets omfattning dessutom delvis beroende av faktorer som ligger utanför utredningens uppdrag att ta ställning till. En sådan faktor är utvecklingen av interoperabla lösningar för den offentliga förvaltningens datadelning. Utredningen om interoperabilitet vid datadelning (I 2022:03) har 2023 föreslagit[1] att en skyldighet för den offentliga förvaltningen att använda nationella interoperabilitetslösningar ska införas i en särskild lag. Utredningens förslag har dock inte lett till lagstiftning. Om sådana lösningar kommer att skapas och i så fall när är alltså osäkert.

Sammantaget är det svårt att med någon närmare precision förutse vilket genomslag vårt förslag om utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ kommer att få. Det gäller även för våra övriga förslag. Det är därmed även svårt att bedöma förslagens konsekvenser med någon närmare precision.

Som nämnts ovan ska vi genomföra en integritetsanalys och redovisa vilka konsekvenser förslagen innebär för spridandet av personuppgifter inom och mellan myndigheter. Uppdraget i dessa delar redovisas i kapitel 6. Som framgår av den redovisningen anser vi att

[1] SOU 2023:96, *En reform för datadelning*, s. 199.

det intrång i den personliga integriteten som vårt förslag innebär i form av större möjligheter för myndigheter att utbyta information om enskilda är motiverat och står i proportion till nyttan med förslaget.

8.4 Allmänna konsekvenser

8.4.1 Problemen

Vår kartläggning visar att myndigheterna har behov av att i större utsträckning än i dag lämna ut uppgifter som inte är sekretessbelagda på eget initiativ. Som framgår av avsnitt 4.6 finns i dagsläget inget generellt rättsligt stöd för myndigheterna att lämna ut sådana uppgifter på eget initiativ. Det gäller trots att uppgifter som inte är sekretessbelagda dels inte omfattas av ett röjandeförbud enligt sekretessregleringen, dels måste lämnas ut till en annan myndighet på begäran, om inte utlämnandet är så resurskrävande att det hindrar arbetets behöriga gång. Behovet av att lämna uppgifter till en annan myndighet uppstår dock ofta på grund av att den mottagande myndigheten inte känner till att uppgifterna existerar, vilket även innebär att mottagaren saknar möjlighet att begära ut dem. Bristen på rättsligt stöd för att lämna ut uppgifter som inte är sekretessbelagda på eget initiativ leder alltså till att myndigheter inte får del av sådan information som de behöver för att fatta riktiga beslut och utföra sin verksamhet i övrigt, trots att det inte föreligger några sekretesshinder mot ett sådant utlämnande.

Vidare kan ändamålsbestämmelser i kompletterande dataskyddsreglering uppfattas utgöra en särskild sekretessreglering som enbart gäller mellan myndigheter, trots att den materiella sekretessregleringen enligt offentlighets- och sekretesslagen medför relativt stora möjligheter att utbyta uppgifter med andra myndigheter, t.ex. med stöd av de sekretessbrytande bestämmelserna i 10 kap. OSL. När den kompletterande dataskyddsregleringen omfattar bestämmelser som till synes utesluter en tillämpning av offentlighets- och sekretesslagens bestämmelser uppstår en normkonflikt som kan leda till att inget av regelverken tillämpas på det sätt som lagstiftaren avsett. Det bidrar även till en allmän komplexitet i den sammantagna regleringen av myndigheters informationsutbyte som på ett generellt plan förvårar tillämpningen.

I den kompletterande dataskyddsregleringen förekommer det dessutom att myndigheters möjlighet att lämna ut uppgifter elektroniskt på annat sätt än genom direktåtkomst är begränsade i olika avseenden, även i förhållande till andra offentliga aktörer. Det kan t.ex. innebära att myndigheter är förhindrade att använda e-post i kontakten med andra myndigheter. Regleringen bygger på antagandet att det alltid är mer integritetskänsligt att överföra uppgifter digitalt än analogt, vilket möjligtvis ägde giltighet under en tid av helt andra och mer begränsade möjligheter till elektroniskt informationsutbyte. I dag måste det anses vara ett överspelat förhållningssätt, inte minst mot bakgrund av de direkt tillämpliga bestämmelserna i dataskyddsförordningen[2] och den tekniska utvecklingen. Regeringen har t.ex. uttalat att en manuell informationshantering i dag inte kan sägas vara ett realistiskt alternativ för vare sig myndigheter eller företag.[3] Sektorspecifika hinder mot att utbyta information elektroniskt innebär alltså att berörda myndigheter är förhindrade att lämna ut uppgifter till andra myndigheter med hjälp av moderna tekniker, utan någon uppenbar fördel för enskildas personliga integritet. Sådan reglering strider dessutom bl.a. mot regeringens uttalade målsättning[4] om digitalt som förstahandsval i den offentliga förvaltningen.

8.4.2 Vilka konsekvenser uppstår om inget görs?

Bestämmelsen om utlämnande på eget initiativ

Vårt förslag om en ny bestämmelse i offentlighets- och sekretesslagen, som ger myndigheterna ett rättsligt stöd för att på eget initiativ lämna uppgifter som inte är sekretessbelagda till en annan myndighet, syftar till att komplettera den befintliga regleringen i 6 kap. 5 § OSL och kommer i likhet med denna att träffa alla uppgifter som inte är sekretessbelagda, oavsett om detta beror på att de t.ex. är undantagna från sekretess eller träffas av en sekretessbrytande bestämmelse i offentlighets- och sekretesslagen. Bestämmelsen förtydligar på så sätt det generella rättsliga förhållandet mellan myndigheter, dvs. principen att alla myndigheter ska samarbeta med och bistå

[2] 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).
[3] Prop. 2017/18:105, *Ny dataskyddslag*, s. 47.
[4] Budgetpropositionen för 2019, prop. 2018/19:1 utg. omr. 2, s. 53.

varandra i den utsträckning som är möjlig, där utbyte av information är ett viktigt led, jfr 8 § förvaltningslagen (2017:900). Det bör på ett övergripande plan kunna leda till att regleringen av myndigheters informationsutbyte blir mindre komplex och svårtillämpad, och i förlängningen till att myndigheterna i större utsträckning får del av information som är nödvändig för att fatta korrekta beslut och bedriva en effektiv verksamhet.

Om förslaget inte genomförs kommer komplexiteten och tillämpningssvårigheterna i detta avseende i stället att bestå. Om förslaget inte genomförs kommer det vidare att innebära att utrymmet för att lämna ut uppgifter som annars inte är sekretessbelagda även i fortsättningen ofta kommer att vara mindre än utrymmet för att lämna ut uppgifter som annars är sekretessbelagda, vilket måste anses vara en paradoxal ordning som sannolikt bidrar till upplevelsen av regleringens komplexitet. Även otydligheten vad gäller möjligheten att på eget initiativ lämna ut uppgifter som träffas av en sekretessbrytande bestämmelse i offentlighets- och sekretesslagen kommer att bestå om förslaget inte införs, vilket kan förväntas leda till att uppgifter inte utbyts med stöd av befintliga sådana bestämmelser i den utsträckning som varit lagstiftarens avsikt. Det gäller även för utlämnande med stöd av den generella sekretessbrytande bestämmelse som vi föreslagit i vårt delbetänkande, om den införs. Detta kan i sin tur antas leda till att förtroendet för det allmänna skadas eftersom staten inte gör vad den kan för att bidra till ett tydligt och enkelt regelverk och för att ge myndigheterna goda förutsättningar för att utföra sitt uppdrag.

Upplysningsbestämmelser i den kompletterande dataskyddsregleringen

Förslaget om att införa upplysningsbestämmelser i den kompletterande dataskyddsregleringen syftar till att förtydliga gällande rätt avseende hur förbud att röja en uppgift regleras. Det syftar även till att tydliggöra hur myndigheters informationsutbyte regleras i den svenska rättsordningen. Genom förslaget upphävs den upplevda normkonflikten mellan ändamålsbestämmelser i den kompletterande dataskyddsregleringen och offentlighets- och sekretesslagens bestämmelser. Den konflikten är i huvudsak ett resultat av att den kompletterande dataskyddsregleringen inte utvärderats och uppdaterats i takt

med den tekniska och rättsliga utvecklingen. Förslaget bidrar därmed också till att den kompletterande dataskyddsregleringen blir mer modern och ändamålsenlig. Förslaget leder också till en ökad tydlighet i den sammantagna regleringen av myndigheters informationsutbyte.

Om upplysningsbestämmelser inte införs i den kompletterande dataskyddsregleringen i enlighet med vårt förslag så kommer de upplevda normkonflikterna i stället bestå. Den kompletterande dataskyddsregleringen riskerar också att försämra myndigheternas möjligheter att utbyta information med stöd av offentlighets- och sekretesslagens bestämmelser, och därmed att informationsutbyte inte kommer till stånd i den utsträckning lagstiftaren avsett. Även här kan det leda till att förtroendet för det allmänna skadas eftersom staten inte gör vad den kan för att upprätthålla gällande regelverk och ge myndigheterna goda förutsättningar för att utföra sitt uppdrag.

Bestämmelser om elektroniskt utlämnande

Förslaget om att elektroniskt utlämnande på annat sätt än genom direktåtkomst ska vara tillåtet om det inte är olämpligt ger myndigheterna bättre möjligheter att med ny teknik åstadkomma ett säkert, ändamålsenligt och effektivt informationsutbyte främst med andra myndigheter. Att berörda myndigheter inte längre kommer att vara hänvisade till att kommunicera analogt i vissa fall kommer medföra möjligheter till effektivisering. Om förslaget inte införs kommer berörda myndigheter i stället att fortsatt vara hänvisade till analog kommunikation i vissa fall, vilket i dag inte kan anses vara en rimlig ordning.

Sammanfattning

En ökad tydlighet, mer enhetlighet och färre motstridigheter i den sammantagna regleringen av myndigheters informationsutbyte i sak kommer att underlätta myndigheternas samverkan med varandra och andra aktörer. Förslagen innebär att statens resurser kommer att kunna användas mer effektivt genom att omotiverade hinder för myndigheterna att utnyttja den moderna teknikens fördelar tas bort.

En konsekvens av detta blir att ärendehantering, service till enskilda och informationsutbyte mellan myndigheter kan ske på ett

mer ändamålsenligt, säkert och effektivt sätt än i dag. Det kommer även innebära att enskilda ges större möjligheter att förstå lagstiftningen och därmed enklare kan tillvarata sina rättigheter enligt det allmänna dataskyddsrättsliga regelverket.

Om förslagen inte genomförs kommer de problem som beskrivits i föregående avsnitt att kvarstå och de positiva konsekvenserna av förslagen att utebli. Myndigheterna kommer i stället fortsatt vara tvungna att följa svårtolkade och omoderna bestämmelser som inte medför något nämnvärt förhöjt integritetsskydd och som utgår från att digital informationshantering är ett komplement till pappershantering. I många fall kommer myndigheterna även fortsättningsvis att vara förhindrade att på eget initiativ lämna ut relevanta uppgifter som annars inte är sekretessbelagda till en annan myndighet.

8.5 Ekonomiska konsekvenser för det allmänna och för enskilda

Vår bedömning: Våra förslag bör inte leda till något ökat resursbehov för de statliga myndigheterna. Inte heller bör våra förslag, som inte innebär några nya åligganden, leda till kostnadsökningar för kommuner och regioner. Våra förslag bör inte heller föranleda några påtagligt ökade kostnader för företag och andra enskilda.

Skälen för vår bedömning

Några allmänna iakttagelser

I delbetänkandet gjorde vi sammanfattningsvis den bedömningen att det förslag vi där lämnar kommer att leda till påtagligt positiva samhällsekonomiska effekter, att det inte bör leda till något ökat resursbehov för de statliga myndigheterna och att det inte heller bör leda till kostnadsökningar för kommuner och regioner.

Delbetänkandet har remissbehandlats och vi kan konstatera att flera remissinstanser inte delar vår bedömning och menar att förslaget i stället kommer att leda till kostnadsökningar som inte ryms inom befintliga ramar.

Vi har nu bl.a. föreslagit att det i offentlighets- och sekretesslagen ska införas en bestämmelse som innebär att myndigheterna får lämna ut uppgifter som inte är sekretessbelagda till andra myndigheter under vissa förutsättningar. Bestämmelsen skapar alltså inte någon skyldighet för myndigheterna att lämna ut uppgifter. Inte heller tas några sekretesshinder bort genom bestämmelsen. Den föreslagna bestämmelsen innebär inte heller i övrigt att myndigheterna får några nya eller ändrade uppgifter eller uppdrag. Förslaget syftar i stället till att förenkla myndigheters parallella tillämpning av sekretessregleringen och dataskyddsregleringen genom att det kommer finnas en rättslig grund i dataskyddsrättslig mening för att på eget initiativ lämna ut uppgifter, som det enligt sekretessregleringen inte finns något förbud mot att röja, till en annan myndighet.

Bestämmelsen innebär alltså inget annat än en möjlighet för myndigheterna att under vissa förutsättningar lämna ut uppgifter som med en tillämpning av befintlig reglering i offentlighets- och sekretesslagen inte är sekretessbelagda. Som påpekats inledningsvis är det dessutom så att bestämmelsen, i förhållande till sådana annars sekretessbelagda uppgifter som träffas av de sekretessbrytande bestämmelserna i offentlighets- och sekretesslagen, endast utgör ett förtydligande av vad som redan gäller.

Vi föreslår också vissa ändringar i den kompletterande dataskyddsregleringen. Vad gäller de upplysningsbestämmelser om utlämnande i överensstämmelse med lag eller förordning som föreslås införas innebär detta inte annat än att den kompletterande dataskyddsregleringen anpassas till dagens förhållanden, där analog hantering av information i princip har upphört, och att det uppstår en formell överensstämmelse med sekretessregleringen, som i svensk rätt är den lagstiftning i vilken förbud mot att röja en uppgift ställs upp. I denna del innebär våra förslag alltså att förekommande motstridigheter mellan regelverken upphävs och att regleringen blir mer enhetlig. Även i denna del syftar förslagen till att förenkla myndigheters parallella tillämpning av sekretessregleringen och dataskyddsregleringen.

Våra förslag om förändringar av den kompletterande dataskyddsregleringen innebär också att omotiverade och omoderna hinder mot att lämna ut uppgifter elektroniskt på annat sätt än genom direktåtkomst tas bort. Det är vår bedömning att dessa ändringar kommer att bidra till att förenkla för de berörda myndigheterna och göra informationshanteringen mer effektiv.

Av olika anledningar är det som redan påpekats svårt att med någon närmare precision förutse konsekvenserna av våra förslag. Det innebär förstås att det också är svårt att med någon närmare precision förutse förslagens ekonomiska konsekvenser. Vi menar emellertid att man i vart fall bör kunna sluta sig till att de förslag vi nu lämnar inte kommer att ha lika långtgående konsekvenser för myndigheterna som det förslag vi lämnade i delbetänkandet. Vissa konsekvenser bör dock kunna förutses.

I sina remissyttranden över delbetänkandet har ett antal remissinstanser påpekat att det förslag som lämnas där kommer att kräva att de anställdas kompetens höjs i form av informationsinsatser och vidareutbildningar och liknande, vilket innebär kostnadsökningar. Det bör kunna antas att det förslag vi nu lämnar kommer att föranleda liknande synpunkter.

Vi delar bilden av att det i många fall finns ett behov av kompetenshöjande åtgärder vad gäller den sammantagna regleringen av myndigheters informationsutbyte, dvs. sekretess och dataskydd. Detta behov synes dock i första hand ha sin grund i det förhållandet att det sammantagna rättsområdet är komplext, innehåller motstridigheter och är svårtillämpat. Vår bedömning är alltså att behovet av kompetenshöjande åtgärder inte kan säga vara en konsekvens av de förslag vi nu lämnar, utan redan i dag existerar till följd av den gällande regleringens komplexitet och bristen på samordning.

Syftet med våra förslag är dock att bidra till att rättsområdet blir mindre komplext och lättare att tillämpa, vilket borde minska det generella behovet av utbildning över tid. Våra förslag bör alltså endast innebära en viss inledande ökning av behovet av utbildningsinsatser. Behovet av utbildning till följd av våra förslag över tid bör dock inte vara särskilt stort i förhållande till behovet i dag. Att t.ex. ta fram nya styrande eller stödjande dokument samt genomföra informationsinsatser som kan komma att krävas till följd av en ändrad reglering får dessutom anses ingå i myndigheternas ordinarie uppgifter. Det rör sig därmed i dessa delar om begränsade kostnader för myndigheterna som bör rymmas inom befintliga ekonomiska ramar.

I ett antal remissvar över delbetänkandet påpekas bl.a. att de förslag som där lämnas kommer att föranleda en ökad administrativ börda och att det kommer att nödvändiggöra investeringar i nya itlösningar. Även de förslag vi nu lämnar kan förväntas komma att medföra sådana konsekvenser för myndigheterna och att detta kommer

att uppfattas vara kostnadsdrivande. Det är emellertid vår sammantagna bedömning att dessa kostnader bör rymmas inom befintliga ramar. Den föreslagna bestämmelsen om utlämnande på eget initiativ innebär dessutom inte några krav på att myndigheterna ska införa eller utveckla nya it-system för kommunikation med andra myndigheter eller krav på att ändra sina arbetssätt. Detsamma gäller för övriga förslag som lämnats.

Statliga myndigheter

Våra förslag innebär inte att det införs någon skyldighet att lämna ut uppgifter. Samtidigt är det vår bedömning att regleringen kommer att leda till ett ökat informationsutbyte. Det är ofrånkomligt att ett ökat informationsutbyte kommer att leda till en ökad arbetsbörda såväl för den utlämnande som för den mottagande myndigheten. Det är också rimligt att tänka sig att våra förslag i praktiken kommer att kräva att myndigheterna i större utsträckning samverkar med varandra, kring omfattningen av utlämnandet från en myndighet till en annan. Det är ofrånkomligt att även detta kommer att ta resurser i anspråk.

Den bestämmelse som vi föreslår i offentlighets- och sekretesslagen kommer emellertid att innebära att det tydliggörs att uppgifter som inte är sekretessbelagda får lämnas ut på eget initiativ i vissa situationer. Vidare kommer de ändringar som vi föreslår i den kompletterande dataskyddsregleringen innebära att den upplevda normkonflikten mellan dataskyddsregleringen och sekretessregleringen tas bort. Rättsläget kommer att klarna vilket i sin tur kommer att innebära att myndigheterna inte behöver lägga lika stora resurser på att genomföra tidsödande och komplicerade rättsliga bedömningar av förhållandet mellan de två regelverken. Här bör också nämnas att vårt förslag om att ta bort onödiga hinder mot att lämna ut uppgifter elektroniskt på annat sätt än genom direktåtkomst kommer att innebära att berörda myndigheter kan lämna ut uppgifter till andra myndigheter exempelvis via e-post i stället för genom traditionell post, vilket får förmodas vara mindre resurskrävande.

Det förväntade ökade informationsutbytet och den ökning av arbetsbördan som kan uppstå med anledning av det kommer, enligt vår bedömning, balanseras av de positiva effekter som man kan för-

vänta sig att förslagen kommer att medföra. Den ökade effektivitet och de besparingar som den innebär bör alltså väga upp det ökade resursbehov som inledningsvis och under en övergångsperiod kan uppstå när lagstiftningen är ny.

Härtill kommer att våra förslag kan förväntas ge bättre förutsättningar för myndigheterna att få ett fullständigt och korrekt beslutsunderlag och även i övrigt förbättra förutsättningarna att utföra sina uppgifter. Sammantaget bedömer vi att de ekonomiska konsekvenserna av den föreslagna regleringen bör kunna hanteras inom befintliga ekonomiska ramar.

Kommuner och regioner

Våra förslag innebär inget annat än att det införs en möjlighet att lämna ut uppgifter som inte är sekretessbelagda i vissa situationer. Våra förslag innebär således inte några åligganden för kommuner och regioner. Den kommunala finansieringsprincipen är alltså inte aktuell.

På motsvarande sätt som gäller för statliga myndigheter kan våra förslag förväntas leda till ett utökat informationsutbyte, såväl i förhållande till statliga myndigheter som inom och mellan olika kommuner och regioner. Den hanteringen kan förväntas leda till en ökad arbetsbörda. Vi bedömer emellertid att våra förslag kommer att innebära en förenkling även för kommunernas och regionernas del. Man kan också förvänta sig att förslagen kommer att underlätta för kommunerna och regionerna genom att beslutsunderlagen blir bättre och genom att förslagen leder till allmänt förbättrade möjligheter att effektivt fullgöra sina uppgifter. Vidare bör kostnaderna för den ökade arbetsbörda som förslagen kan medföra vägas mot de utgiftsminskningar som förväntas uppstå hos kommunerna och regionerna till följd av minskade felaktiga utbetalningar och ökade skatteintäkter. Det ökade informationsutbyte som förslagen möjliggör kan bl.a. väntas leda till minskade felaktiga utbetalningar vid exempelvis kommuners och regioners köp av välfärdstjänster och därmed till direkta utgiftsminskningar för kommunerna och regionerna. Sammantaget bedömer vi därför att förslagen på sikt inte innebär någon ökad kostnad för kommunerna och regionerna.

I följande avsnitt redovisas de konsekvenser som väntas uppstå för bl.a. kommuners brottsförebyggande arbete.

Företag och andra enskilda

Enligt vår bedömning kommer förslagen inte föranleda några påtagligt ökade kostnader för företag och andra enskilda.

8.6 Förslagens betydelse för brottsligheten och det brottsförebyggande arbetet

Vår bedömning: Våra förslag kommer att ge bättre förutsättningar för myndigheter att förebygga brottslig verksamhet och utreda brott.

Skälen för vår bedömning

Den föreslagna bestämmelsen i offentlighets- och sekretesslagen om utlämnande på eget initiativ förtydligar som vi redan påpekat ett generellt rättsligt förhållande mellan myndigheter, dvs. principen att alla myndigheter ska samarbeta med och bistå varandra i den utsträckning som är möjlig, där utbyte av information är ett viktigt led. Det kartlagda behovet av att kunna lämna ut uppgifter på eget initiativ till andra myndigheter är dessutom stort och genomgående, och avser bl.a. uppgiftslämnande för brottsförebyggande och brottsbekämpande ändamål. Genom förtydligandet av att uppgifter som inte är sekretessbelagda får lämnas till en annan myndighet på eget initiativ kommer myndigheter därför sannolikt även att lämna ut uppgifter med stöd av den föreslagna bestämmelsen för att utlämnandet kan antas ha betydelse för att förebygga brottslig verksamhet och för att utreda brott. Man bör kunna utgå från att uppgiftsutbytet också kommer få betydelse för sådan verksamhet.

Om bestämmelsen om utlämnande på eget initiativ kommer att bidra till att förhindra brott, t.ex. inom den organiserade brottsligheten eller till att motverka att unga dras in i kriminalitet, eller att förhindra fortsatt kriminalitet, är samhällsvinsterna mycket stora.

Positiva effekter bör också uppstå genom att färre individer hamnar i kriminalitet och färre utsätts för brott. Förhindrande av brott leder också till positiva effekter för myndigheternas verksamheter, i synnerhet för de utbetalande myndigheterna. Om brott mot välfärden minskar leder det till betydande positiva ekonomiska konsekvenser för samhällsekonomin. Fler utredda brott kommer leda till att fler gärningsmän kommer att kunna straffas och att fler brottsoffer får upprättelse, vilket i förlängningen kommer att kunna leda till ett tryggare samhälle.

Sammantaget är det vår bedömning att den föreslagna bestämmelsen om utlämnande på eget initiativ av uppgifter som inte är sekretessbelagda kommer att ge bättre förutsättningar för myndigheter att förebygga brottslig verksamhet och utreda brott.

Övriga förslag, dvs. förslagen om att det ska införas upplysningsbestämmelser om uppgiftslämnande i överensstämmelse med lag eller förordning i den kompletterande dataskyddsregleringen och att omotiverade hinder mot elektroniskt informationsutbyte tas bort, bör i mindre utsträckning ha betydelse för brottsligheten och det brottsförebyggande arbetet. I den mån uttömmande ändamålsbestämmelser faktiskt har uppfattats utgöra ett hinder mot utlämnande i överensstämmelse med offentlighets- och sekretesslagens bestämmelser bör dock förslagen kunna ha en viss betydelse, av samma skäl som anges ovan.

8.7 Sveriges internationella åtaganden

Vår bedömning: Våra förslag är förenliga med de krav som följer av EU-rätten, barnkonventionen och Sveriges övriga internationella åtaganden

Skälen för vår bedömning

Av den integritetsanalys vi redovisar i kapitel 6 framgår att vi bedömer att det intrång i den personliga integriteten som våra förslag innebär, i form av större möjligheter för myndigheter att utbyta information, är motiverat och står i proportion till nyttan med förslagen. Vår bedömning är därför att förslagen är förenliga både med våra internatio-

nella åtaganden enligt Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna och övriga åtaganden när det gäller mänskliga rättigheter och den EU-rättsliga lagstiftningen, såväl vad gäller dataskydd som i övrigt.

Förslaget om utlämnande av uppgifter som inte är sekretessbelagda på eget initiativ berör även barn. I avsnitt 6.4.8 har vi gjort särskilda överväganden om riskerna för barn och förslagets proportionalitet. Det är vår bedömning att vårt förslag i den delen är förenligt med barnkonventionen[5]. Förslagen om förändringar av den kompletterande dataskyddsregleringen bör dock inte ha några särskilda konsekvenser för barn.

8.8 Övriga konsekvenser

Vår bedömning: Våra förslag innebär ingen inskränkning i det kommunala självstyret. Inte heller i övrigt innebär våra förslag några konsekvenser av det slag som följer av 15 § kommittéförordningen.

Skälen för vår bedömning

Som vi konstaterar i avsnitt 8.5 innebär våra förslag inte några åliggganden för kommuner och regioner. Våra förslag inskränker därmed inte det kommunala självstyret.

Våra förslag innebär inte heller några påtagliga konsekvenser för sysselsättning och offentlig service i olika delar av landet, för små företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt i förhållande till större företag.

Det övergripande målet för jämställdhetspolitiken är att kvinnor och män ska ha samma makt att forma samhället och sina egna liv. Förslaget innebär att möjligheterna för myndigheter att utbyta uppgifter förbättras. Förslaget bedöms därmed kunna öka förmågan att förebygga, upptäcka och förhindra brottslighet. Förslaget kan därmed förväntas bidra till att våldsutsatta kvinnor i högre grad skyddas från upprepat våld. Därmed kan förslaget förväntas bidra till att uppnå det jämställdhetspolitiska målet att mäns våld mot kvinnor ska upphöra.

[5] Förenta nationernas konvention den 20 november 1989 om barnets rättigheter.

9 Författningskommentar

9.1 Förslaget till lag om ändring i rennäringslagen (1971:437)

74 a §

Personuppgifter som behandlas i renmärkesregistret får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.

Paragrafen, som är ny, innehåller en s.k. sekundär ändamålsbestämmelse om möjligheten att behandla personuppgifter i renmärkesregistret för ändamål utöver de som anges i den primära ändamålsbestämmelsen i 74 § tredje stycket första meningen. Övervägandena finns i avsnitt 5.4.6.

Av bestämmelsen, som är en upplysningsbestämmelse, följer att de uppgifter som behandlas i renmärkesregistret även får behandlas för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning. Behandlingen förutsätter alltså att uppgifterna redan är föremål för behandling i registret enligt 74 § tredje stycket första meningen. Bestämmelsen omfattar sådant uppgiftslämnande som sker på grund av att myndigheten ska lämna ut uppgifter, t.ex. med stöd av 6 kap. 5 § offentlighets- och sekretesslagen (2009:400), OSL, i fall då utlämnande inte kan ske med stöd av 74 § tredje stycket första meningen. Bestämmelsen omfattar även sådant uppgiftslämnande som sker med stöd av bestämmelser som medför att uppgifter får lämnas ut, t.ex. den s.k. generalklausulen i 10 kap. 27 § OSL. Bestämmelsen omfattar uppgiftslämnande till myndigheter och enskilda. Det avgörande är att uppgiftslämnandet sker med stöd av lag eller förordning.

9.2 Förslaget till lag om ändring i lagen (1994:448) om pantbrevsregister

3 a §

Personuppgifter som behandlas i pantbrevsregistret får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.

Paragrafen, som är ny, innehåller en s.k. sekundär ändamålsbestämmelse om möjligheten att behandla personuppgifter i pantbrevsregistret för ändamål utöver de som anges i den primära ändamålsbestämmelsen i 3 §. Övervägandena finns i avsnitt 5.4.6.

Av bestämmelsen, som är en upplysningsbestämmelse, följer att de uppgifter som behandlas i pantbrevsregistret för primära ändamål enligt 3 § även får behandlas för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning. Behandlingen förutsätter alltså att uppgifterna redan är föremål för behandling enligt 3 §. Bestämmelsen omfattar sådant uppgiftslämnande som sker på grund av att myndigheten ska lämna ut uppgifter, t.ex. med stöd av 6 kap. 5 § OSL i fall då utlämnande inte kan ske med stöd av 3 §. Bestämmelsen omfattar även sådant uppgiftslämnande som sker med stöd av bestämmelser som medför att uppgifter får lämnas ut, t.ex. den s.k. generalklausulen i 10 kap. 27 § OSL. Bestämmelsen omfattar uppgiftslämnande till myndigheter och enskilda. Det avgörande är att uppgiftslämnandet sker med stöd av lag eller förordning.

9.3 Förslaget till lag om ändring i vapenlagen (1996:67)

1 a kap.

8 a §

Personuppgifter som behandlas i vapenregistret får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.

Paragrafen, som är ny, innehåller en s.k. sekundär ändamålsbestämmelse om möjligheten att behandla personuppgifter i vapenregistret för ändamål utöver de som anges i den primära ändamålsbestämmelsen i 8 §. Övervägandena finns i avsnitt 5.4.6.

Av bestämmelsen, som är en upplysningsbestämmelse, följer att de uppgifter som behandlas för primära ändamål enligt 8 § även får behandlas för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning. Behandlingen förutsätter alltså att uppgifterna redan är föremål för behandling enligt 8 §. Bestämmelsen omfattar sådant uppgiftslämnande som sker på grund av att myndigheten ska lämna ut uppgifter, t.ex. med stöd av 6 kap. 5 § OSL i fall då utlämnande inte kan ske med stöd av 8 §. Bestämmelsen omfattar även sådant uppgiftslämnande som sker med stöd av bestämmelser som medför att uppgifter får lämnas ut, t.ex. den s.k. generalklausulen i 10 kap. 27 § OSL. Bestämmelsen omfattar uppgiftslämnande till myndigheter och enskilda. Det avgörande är att uppgiftslämnandet sker med stöd av lag eller förordning.

9.4 Förslaget till lag om ändring i lagen (2001:183) om behandling av personuppgifter i verksamhet med val och folkomröstningar

1 a kap.

5 a §

Personuppgifter som behandlas enligt 4 och 5 §§ får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.

Paragrafen, som är ny, innehåller en s.k. sekundär ändamålsbestämmelse om möjligheten att behandla personuppgifter för ändamål utöver de som anges i de primära ändamålsbestämmelserna i 4 och 5 §§. Övervägandena finns i avsnitt 5.4.6.

Av bestämmelsen, som är en upplysningsbestämmelse, följer att de uppgifter som behandlas för primära ändamål enligt 4 och 5 §§ även får behandlas för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning. Behandlingen förutsätter alltså att uppgifterna redan är föremål för behandling enligt 4 och 5 §§. Bestämmelsen omfattar sådant uppgiftslämnande som sker på grund av att myndigheten ska lämna ut uppgifter, t.ex. med stöd av 6 kap. 5 § OSL i fall då utlämnande inte kan ske med stöd av 4 och 5 §§. Bestämmelsen omfattar även sådant uppgiftslämnande som sker med stöd av bestämmelser som medför att uppgifter får lämnas

ut, t.ex. den s.k. generalklausulen i 10 kap. 27 § OSL. Bestämmelsen omfattar uppgiftslämnande till myndigheter och enskilda. Det avgörande är att uppgiftslämnandet sker med stöd av lag eller förordning.

9.5 Förslaget till lag om ändring i lagen (2001:454) om behandling av personuppgifter inom socialtjänsten

6 §

Personuppgifter får behandlas bara om behandlingen är nödvändig för att arbetsuppgifter inom socialtjänsten *ska* kunna utföras.

Personuppgifter *som behandlas enligt första stycket* får även behandlas för *uppgiftslämnande i överensstämmelse med* lag eller förordning.

En registrerad person har inte rätt att motsätta sig sådan behandling av uppgifter som är tillåten enligt denna lag.

Paragrafen reglerar när behandling av personuppgifter är tillåten (jfr prop. 2000/01:80, s. 143 och 175). Övervägandena finns i avsnitt 5.4.6.

Ändringen i *första stycket* är redaktionell.

Ändringen i *andra stycket* utgör ett förtydligande av det s.k. sekundära ändamålet om möjligheten att behandla personuppgifter för ändamål utöver de som anges i den primära ändamålsbestämmelsen i paragrafens första stycke. Genom ändringen anpassas bestämmelsens utformning till övrig kompletterande dataskyddsreglering. Någon ändring i sak är inte avsedd.

Tredje stycket ändras inte.

9.6 Förslaget till lag om ändring i lagen om (2006:378) om lägenhetsregister

5 a §

Personuppgifter som behandlas i lägenhetsregistret får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.

Paragrafen, som är ny, innehåller en s.k. sekundär ändamålsbestämmelse om möjligheten att behandla personuppgifter för ändamål

utöver de som anges i den primära ändamålsbestämmelsen i 5 §. Övervägandena finns i avsnitt 5.4.6.

Av bestämmelsen, som är en upplysningsbestämmelse, följer att de personuppgifter som behandlas för primära ändamål enligt 5 § även får behandlas för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning. Behandlingen förutsätter alltså att uppgifterna redan är föremål för behandling enligt 5 §. Bestämmelsen omfattar sådant uppgiftslämnande som sker på grund av att myndigheten ska lämna ut uppgifter, t.ex. med stöd av 6 kap. 5 § OSL, i fall då utlämnande inte kan ske med stöd av 5 §. Bestämmelsen omfattar även sådant uppgiftslämnande som sker med stöd av bestämmelser som medför att uppgifter får lämnas ut, t.ex. den s.k. generalklausulen i 10 kap. 27 § OSL. Bestämmelsen omfattar uppgiftslämnande till myndigheter och enskilda. Det avgörande är att uppgiftslämnandet sker med stöd av lag eller förordning.

Elektroniskt utlämnande

20 §

Uppgifter i lägenhetsregistret får lämnas ut *elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt*.

Paragrafen utgör en upplysningsbestämmelse om att uppgifter som inte är sekretessbelagda kan lämnas ut elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt (jfr prop. 2004/05:171, s. 80 och prop. 2015/16:141 s. 11). Övervägandena finns i avsnitt 5.6.3.

Paragrafen ändras på så sätt att begränsningar som innebär att utlämnande av uppgifter ur lägenhetsregistret på medium för automatiserad behandling endast är tillåtet om regeringen meddelar föreskrifter om det och om det sker för vissa närmare angivna ändamål tas bort. En språklig anpassning till övrig kompletterande dataskyddsreglering har också gjorts.

Bestämmelsen medför inte någon rätt för vare sig mottagande myndigheter eller enskilda att få ut uppgifter elektroniskt. Inte heller medför bestämmelsen någon skyldighet att lämna ut uppgifter elektroniskt. Bestämmelsen innebär däremot att det inte finns något hinder mot att lämna ut uppgifter i lägenhetsregistret på det sättet om att det inte är olämpligt. Bedömningen av om utlämnandet är

olämpligt ska ske med beaktande av vad syftet med utlämnandet är, vem mottagaren är, vilka uppgifter det rör sig om samt om nödvändiga säkerhetsåtgärder är vidtagna. Utlämnande till andra myndigheter bör i normalfallet anses vara lämpligt. Detsamma borde i de allra flesta fall gälla för enskilda. När det gäller utlämnande till enskilda kan det dock krävas närmare överväganden bl.a. med hänsyn till vem mottagaren är och mottagarens personuppgiftsbehandling efter ett utlämnande.

9.7 Förslaget till lag om ändring i lagen (2006:444) om passagerarregister

4 a §

Personuppgifter som behandlas i passagerarregistret får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.

Paragrafen, som är ny, innehåller en s.k. sekundär ändamålsbestämmelse om möjligheten att behandla personuppgifter för ändamål utöver de som anges i den primära ändamålsbestämmelsen i 4 §. Övervägandena finns i avsnitt 5.4.6.

Av bestämmelsen, som är en upplysningsbestämmelse, följer att de personuppgifter som behandlas för primära ändamål enligt 4 § även får behandlas för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning. Behandlingen förutsätter alltså att uppgifterna redan är föremål för behandling enligt 4 §. Bestämmelsen omfattar sådant uppgiftslämnande som sker på grund av att myndigheten ska lämna ut uppgifter, t.ex. med stöd av 6 kap. 5 § OSL i fall då utlämnande inte kan ske med stöd av 4 §. Bestämmelsen omfattar även sådant uppgiftslämnande som sker med stöd av bestämmelser som medför att uppgifter får lämnas ut, t.ex. den s.k. generalklausulen i 10 kap. 27 § OSL. Bestämmelsen omfattar uppgiftslämnande till myndigheter och enskilda. Det avgörande är att uppgiftslämnandet sker med stöd av lag eller förordning.

9.8 Förslaget till lag om ändring i lagen (2006:496) om blodsäkerhet

16 a §

Personuppgifter som behandlas enligt 16 § får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.

Paragrafen, som är ny, innehåller en s.k. sekundär ändamålsbestämmelse om möjligheten att behandla personuppgifter för ändamål utöver de som anges i den primära ändamålsbestämmelsen i 16 §. Övervägandena finns i avsnitt 5.4.6.

Av bestämmelsen, som är en upplysningsbestämmelse, följer att de personuppgifter som behandlas för primära ändamål enligt 16 § även får behandlas för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning. Behandlingen förutsätter alltså att uppgifterna redan är föremål för behandling enligt 16 §. Bestämmelsen omfattar sådant uppgiftslämnande som sker på grund av att myndigheten ska lämna ut uppgifter, t.ex. med stöd av 6 kap. 5 § OSL i fall då utlämnande inte kan ske med stöd av 16 §. Bestämmelsen omfattar även sådant uppgiftslämnande som sker med stöd av bestämmelser som medför att uppgifter får lämnas ut, t.ex. vid misstanke om vissa begångna brott enligt 10 kap. 23 § OSL. Bestämmelsen omfattar uppgiftslämnande till myndigheter och enskilda. Det avgörande är att uppgiftslämnandet sker med stöd av lag eller förordning.

9.9 Förslaget till lag om ändring i lagen (2007:1150) om tillsyn över hundar och katter

5 §

Register över hund- och kattägare enligt 3 § får användas för att fastställa vem som äger en hund eller en katt.

Tullverket, Jordbruksverket, länsstyrelserna, Polismyndigheten och de kommunala nämnder som fullgör uppgifter inom miljö- och hälsoskyddsområdet får medges direktåtkomst till register över hund- och kattägare.

Personuppgifter som behandlas i registret får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.

Paragrafen reglerar ändamålen med register över hund- och kattägare och myndigheters direktåtkomst till registret (jfr prop. 2021/22:49 s. 37 och 38). Övervägandena finns i avsnitt 5.4.6.

Första och *andra styckena* ändras inte.

Tredje stycket, som är nytt, innehåller en s.k. sekundär ändamålsbestämmelse om möjligheten att behandla personuppgifter för ändamål utöver de som anges i den primära ändamålsbestämmelsen i första stycket.

Av bestämmelsen, som är en upplysningsbestämmelse, följer att de personuppgifter som behandlas för primära ändamål enligt första stycket även får behandlas för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning. Behandlingen förutsätter alltså att uppgifterna redan är föremål för behandling enligt första stycket. Bestämmelsen omfattar sådant uppgiftslämnande som sker på grund av att myndigheten ska lämna ut uppgifter, t.ex. med stöd av 6 kap. 5 § OSL i fall då utlämnande inte kan ske med stöd av första stycket. Bestämmelsen omfattar även sådant uppgiftslämnande som sker med stöd av bestämmelser som medför att uppgifter får lämnas ut, t.ex. den s.k. generalklausulen i 10 kap. 27 § OSL. Bestämmelsen omfattar uppgiftslämnande till myndigheter och enskilda. Det avgörande är att uppgiftslämnandet sker med stöd av lag eller förordning.

9.10 Förslaget till lag om ändring i lagen (2008:286) om kvalitets- och säkerhetsnormer vid hantering av mänskliga vävnader och celler

21 a §

Personuppgifter i det register som anges i 21 § får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.

Paragrafen, som är ny, innehåller en s.k. sekundär ändamålsbestämmelse om möjligheten att behandla personuppgifter för ändamål utöver de som anges i den primära ändamålsbestämmelsen i 21 § andra stycket. Övervägandena finns i avsnitt 5.4.6.

Av bestämmelsen, som är en upplysningsbestämmelse, följer att de personuppgifter som behandlas för primära ändamål enligt 21 § andra stycket även får behandlas för att fullgöra uppgiftslämnande

som sker i överensstämmelse med lag eller förordning. Behandlingen förutsätter alltså att uppgifterna redan är föremål för behandling enligt 21 § andra stycket. Bestämmelsen omfattar sådant uppgiftslämnande som sker på grund av att myndigheten ska lämna ut uppgifter, t.ex. med stöd av 6 kap. 5 § OSL i fall då utlämnande inte kan ske med stöd av 21 § andra stycket. Bestämmelsen omfattar även sådant uppgiftslämnande som sker med stöd av bestämmelser som medför att uppgifter får lämnas ut, t.ex. vid misstanke om vissa brott enligt 10 kap. 23 § OSL. Bestämmelsen omfattar uppgiftslämnande till myndigheter och enskilda. Det avgörande är att uppgiftslämnandet sker med stöd av lag eller förordning.

9.11 Förslaget till lag om ändring i patientdatalagen (2008:355)

5 kap.

Elektroniskt utlämnande av personuppgifter

6 §

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

Paragrafen utgör en upplysningsbestämmelse om att uppgifter som inte är sekretessbelagda kan lämnas ut elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt (jfr prop. 2007/08:126, s. 246 och 247). Övervägandena finns i avsnitt 5.6.3.

Ändringen utgör en modernisering och en språklig anpassning till övrig kompletterande dataskyddsreglering. Någon ändring i sak är inte avsedd.

9.12 Förslaget till lag om ändring i offentlighets- och sekretesslagen (2009:400)

6 kap.

5 a §

En myndighet får utan begäran lämna en uppgift till en annan myndighet, om
1. uppgiften inte är sekretessbelagd, och
2. utlämnandet kan antas vara av betydelse för att den utlämnande eller den mottagande myndigheten ska kunna fullgöra sin författningsreglerade verksamhet.

Paragrafen, som är ny, innehåller bestämmelser om att en myndighet utan begäran får lämna en uppgift till en annan myndighet, om uppgiften inte är sekretessbelagd, och utlämnandet kan antas vara av betydelse för att den utlämnande eller den mottagande myndigheten ska kunna fullgöra sin författningsreglerade verksamhet.

Övervägandena finns i avsnitt 4.8.1–4.8.5. Bestämmelsen innebär en möjlighet att på eget initiativ lämna ut uppgifter som inte är sekretessbelagda till mottagaren.

Bestämmelsen innebär att det finns en rättslig grund för att behandla personuppgifter i enlighet med EU:s dataskyddsförordning[1] när uppgifter som inte är sekretessbelagda i förhållande till mottagaren lämnas ut på initiativ av den utlämnande myndigheten i de situationer som anges i bestämmelsen.

Om uppgifter får lämnas ut enligt bestämmelsen behöver den utlämnande myndigheten inte göra någon prövning enligt finalitetsprincipen.

Något krav på att uppgifterna som lämnas ut ska vara dokumenterade uppställs inte. Även uppgifter som enbart finns som en minnesbild hos medarbetare vid myndigheten kan alltså lämnas ut enligt bestämmelsen. Bestämmelsen kompletterar bestämmelsen i 6 kap. 5 § OSL som innebär en skyldighet att på begäran av en annan myndighet lämna ut uppgifter som inte är sekretessbelagda och som myndigheten förfogar över, om det inte skulle hindra arbetets behöriga gång.

[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).

Enligt *första punkten* krävs att uppgiften inte är sekretessbelagd. För att en uppgift ska kunna lämnas ut förutsätts därmed antingen att uppgiften inte är sekretessreglerad, att det finns ett undantag från annars gällande sekretess, att uppgiften kan lämnas ut efter en sekretessprövning, eller att det finns en sekretessbrytande bestämmelse som är tillämplig på uppgiften. Förhållandena kan vara sådana att en uppgift inte är sekretessbelagd i förhållande till en myndighet men sekretessbelagd i förhållande till exempelvis enskilda.

Enligt *andra punkten* krävs att utlämnandet kan antas vara av betydelse för att den utlämnande eller den mottagande myndighetens ska kunna fullgöra sin författningsreglerade verksamhet. Det är alltså själva utlämnandet som ska antas vara av betydelse. Med författningsreglerad verksamhet avses verksamhet som följer av lag, förordning eller föreskrifter eller av ett beslut som har meddelats enligt lag eller annan författning. Utlämnandet ska alltså antas vara av betydelse för fullgörandet av sådan författningsreglerad verksamhet som myndigheterna ägnar sig åt. Rekvisitet ”kan antas” innebär att tröskeln för i vilka situationer uppgifter som inte är sekretessbelagda får lämnas ut på initiativ av den utlämnande myndigheten är lågt satt. För att ett utlämnande ska kunna ske krävs alltså inte att det helt säkert går att förutse vilken betydelse som utlämnandet kommer att ha. Det är tillräckligt att omständigheterna är sådana att det kan antas att utlämnandet har betydelse för att den utlämnande eller den mottagande myndighetens ska kunna fullgöra sin författningsreglerade verksamhet.

Ett utlämnande kan vara motiverat av att det kan antas vara av betydelse för att antingen den utlämnande eller den mottagande myndigheten ska kunna fullgöra sin författningsreglerade verksamhet.

I det förstnämnda fallet motiveras utlämnandet av att det kan antas vara av betydelse för myndighetens egen författningsreglerade verksamhet. En myndighet kan t.ex. lämna ut uppgifter till en annan myndighet av det skälet att den mottagande myndigheten ska kontrollera om den har uppgifter som den utlämnande myndigheten i ett senare skede har för avsikt att begära ut.

I det senare fallet är det fråga om att utlämnandet kan antas vara av betydelse för att den mottagande myndigheten ska kunna fullgöra sin författningsreglerade verksamhet. Att en myndighet fattar ett beslut eller får information om ett förhållande som har betydelse för riktigheten i beslut eller verksamheten i övrigt hos en annan myndighet utgör ett exempel på detta.

Det ankommer i dessa fall på den utlämnande myndigheten att bedöma om uppgifterna kan antas vara av betydelse för att den mottagande myndigheten ska kunna fullgöra sin författningsreglerade verksamhet. Vid denna bedömning bör särskilt reglerade uppgiftsskyldigheter och sekretessbrytande bestämmelser kunna tjäna till vägledning. Man bör exempelvis kunna utgå ifrån att ett utlämnande av en viss typ av uppgifter som i en viss situation träffas av en skyldighet att lämna ut dem också kan antas vara av betydelse för att den mottagande myndigheten ska kunna fullgöra sin författningsreglerade verksamhet och därmed vara möjliga att lämna ut enligt den bestämmelsen. Detta förutsätter förstås att övriga förutsättningar för utlämnande enligt bestämmelsen är uppfyllda, dvs. främst att uppgifterna inte är sekretessbelagda i det enskilda fallet.

9.13 Förslaget till lagen om ändring i patientsäkerhetslagen (2010:659)

2 kap.

4 a §

Personuppgifter som behandlas i registren får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.

Paragrafen, som är ny, innehåller en s.k. sekundär ändamålsbestämmelse om möjligheten att behandla personuppgifter för ändamål utöver de som anges i den primära ändamålsbestämmelsen i 4 §. Övervägandena finns i avsnitt 5.4.6.

Av bestämmelsen, som är en upplysningsbestämmelse, följer att de personuppgifter som behandlas i registret för de primära ändamål som avses i 4 § även får behandlas för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning. Behandlingen förutsätter alltså att uppgifterna redan är föremål för behandling enligt 4 §. Bestämmelsen omfattar sådant uppgiftslämnande som sker på grund av att myndigheten ska lämna ut uppgifter, t.ex. med stöd av 6 kap. 5 § OSL i fall då utlämnande inte kan ske med stöd av 4 §. Bestämmelsen omfattar även sådant uppgiftslämnande som sker med stöd av bestämmelser som medför att uppgifter får lämnas ut, t.ex. den s.k. generalklausulen i 10 kap. 27 § OSL. Bestämmelsen

omfattar uppgiftslämnande till myndigheter och enskilda. Det avgörande är att uppgiftslämnandet sker med stöd av lag eller förordning.

9.14 Förslaget till lag om ändring i lagen (2010:1011) om brandfarliga och explosiva varor

21 e §

Personuppgifter som behandlas i det nationella tillståndsregistret för explosiva varor får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.

Paragrafen, som är ny, innehåller en s.k. sekundär ändamålsbestämmelse om möjligheten att behandla personuppgifter i det nationella tillståndsregistret för explosiva varor för ändamål utöver de som anges i den primära ändamålsbestämmelsen i 21 b §. Övervägandena finns i avsnitt 5.4.6.

Av bestämmelsen, som är en upplysningsbestämmelse, följer att de personuppgifter som behandlas registret för de primära ändamål som avses i 21 b § även får behandlas för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning. Behandlingen förutsätter alltså att uppgifterna redan är föremål för behandling enligt 21 b §. Bestämmelsen omfattar sådant uppgiftslämnande som sker på grund av att myndigheten ska lämna ut uppgifter, t.ex. med stöd av 6 kap. 5 § OSL i fall då utlämnande inte kan ske med stöd av 21 b §. Bestämmelsen omfattar även sådant uppgiftslämnande som sker med stöd av bestämmelser som medför att uppgifter får lämnas ut, t.ex. den s.k. generalklausulen i 10 kap. 27 § OSL. Bestämmelsen omfattar uppgiftslämnande till myndigheter och enskilda. Det avgörande är att uppgiftslämnandet sker med stöd av lag eller förordning.

9.15 Förslaget till lag om ändring i lagen (2011:725) om behörighet för lokförare

4 kap.

11 §

Direktåtkomst till förarbevisregistret får endast medges

1. den som är registrerad i förarbevisregistret när det gäller uppgifter om den registrerade själv,
2. olycksutredande myndighet i Sverige,
3. behörig järnvägssäkerhetsmyndighet och behörigt olycksutredande organ i annat land inom EES eller i Schweiz,
4. Europeiska unionens järnvägsbyrå, och
5. det järnvägsföretag eller den infrastrukturförvaltare i vars verksamhet föraren är anställd eller anlitad.

Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om villkoren för direktåtkomst.

I paragrafen regleras frågor om direktåtkomst till förarbevisregistret (jfr prop. prop. 2010/11:122 s. 114). Övervägandena finns i avsnitt 5.6.3.

Paragrafens *första stycke* ändras på så sätt att regleringen om utlämnande av personuppgifter på medium för automatiserad behandling ur det registret tas bort. Ändringen innebär att paragrafen endast reglerar i vilka fall direktåtkomst till förarbevisregistret får medges. Elektroniskt utlämnande på annat sätt än genom direktåtkomst av personuppgifter ur förarbevisregistret regleras i stället i den nya 11 a §.

Som en följd av ändringen i första stycket har *andra stycket* ändrats till att endast avse regeringens föreskriftsrätt för direktåtkomst.

Elektroniskt utlämnande av personuppgifter

11 a §

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

I paragrafen, som är ny, regleras möjligheten att lämna ut personuppgifter ur förarbevisregistret på annat sätt än genom direktåtkomst. Övervägandena finns i avsnitt 5.6.3.

Bestämmelsen medför inte någon rätt för vare sig mottagande myndigheter eller enskilda att få ut uppgifter elektroniskt. Inte heller medför bestämmelsen någon skyldighet att lämna ut uppgifter elektroniskt. Bestämmelsen innebär däremot att det inte finns något hinder mot att lämna ut uppgifter i förarbevisregistret på det sättet om det inte är olämpligt. Bedömningen av om utlämnandet är olämpligt ska ske med beaktande av vad syftet med utlämnandet är, vem mottagaren är, vilka uppgifter det rör sig om samt om nödvändiga säkerhetsåtgärder är vidtagna. Utlämnande till andra myndighet bör i normalfallet anses vara lämpligt. Detsamma borde i de allra flesta fall gälla för enskilda. När det gäller utlämnande till enskilda kan det dock krävas närmare överväganden bl.a. med hänsyn till vem mottagaren är och mottagarens behandling efter utlämnande.

18 §

Direktåtkomst till intygsregister och *elektroniskt* utlämnande av personuppgifter på *annat sätt än genom direktåtkomst* ur sådana register *som inte förs av det allmänna* får endast medges

1. den som är registrerad i ett intygsregister, när det gäller uppgifter om den registrerade själv i samma register,
2. tillsynsmyndigheten och olycksutredande myndighet i Sverige, samt
3. behörig järnvägssäkerhetsmyndighet och behörigt olycksutredande organ i annat land inom EES eller i Schweiz.

Regeringen meddelar föreskrifter om villkoren för direktåtkomst för sådana intygsregister som förs av det allmänna.

I paragrafen regleras frågor om direktåtkomst till intygsregister (jfr prop. 2010/11:122 s. 115). Övervägandena finns i avsnitt 5.6.3.

Paragrafens *första stycke* ändras på så sätt att regleringen om utlämnande av personuppgifter på medium för automatiserad behandling ur ett sådant register som förs av det allmänna tas bort. Ändringen innebär att paragrafen endast reglerar i vilka fall direktåtkomst till intygsregister och elektroniskt utlämnande av personuppgifter på annat sätt än genom direktåtkomst ur intygsregister som inte först av det allmänna får medges. Elektroniskt utlämnande av personuppgifter på annat sätt än genom direktåtkomst ur intygsregister som förs av det allmänna regleras i den nya 18 a §.

Som en följd av ändringen i första stycket har *andra stycket* ändrats till att endast avse regeringens föreskriftsrätt för direktåtkomst.

Elektroniskt utlämnande av personuppgifter

18 a §

Personuppgifter ur intygsregister som förs av det allmänna får lämnas ut elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt.

I paragrafen som är ny regleras möjlighet att lämna ut personuppgifter ur intygsregister som förs av det allmänna på annat sätt än genom direktåtkomst. Övervägandena finns i avsnitt 5.6.3.

Bestämmelsen medför inte någon rätt för vare sig mottagande myndigheter eller enskilda att få ut uppgifter elektroniskt. Inte heller medför bestämmelsen någon skyldighet att lämna ut uppgifter elektroniskt. Bestämmelsen innebär däremot att det inte finns något hinder mot att lämna ut uppgifter i ett intygsregister på det sättet om det inte är olämpligt. Bedömningen av om utlämnandet är olämpligt ska ske med beaktande av vad syftet med utlämnandet är, vem mottagaren är, vilka uppgifter det rör sig om samt om nödvändiga säkerhetsåtgärder är vidtagna. Utlämnande till andra myndighet bör i normalfallet anses vara lämpligt. Detsamma borde i de allra flesta fall gälla för enskilda. När det gäller utlämnande till enskilda kan det dock krävas närmare överväganden bl.a. med hänsyn till vem mottagaren är och mottagarens behandling efter utlämnande.

9.16 Förslaget till lag om ändring i lagen (2012:453) om register över nationella vaccinationsprogram m.m.

Elektroniskt utlämnande av personuppgifter

10 §

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

Paragrafen utgör en upplysningsbestämmelse om att uppgifter som inte är sekretessbelagda kan lämnas ut elektroniskt på annat sätt än genom direktåtkomst (jfr prop. 2011/12:123 s. 82). Övervägandena finns i avsnitt 5.6.3.

Ändringen utgör en modernisering och en språklig anpassning till övrig kompletterande dataskyddsreglering. Någon ändring i sak är inte avsedd.

9.17 Förslaget till lag om ändring i lagen (2013:1164) om elektroniska vägtullssystem

32 §

Personuppgifter som har erhållits enligt 28 § får endast behandlas för att identifiera ett fordon eller en ägare eller innehavare av ett fordon i syfte att ta upp eller driva in vägtullar.

Att personuppgifter som har erhållits enligt 28 § får lämnas ut i vissa fall framgår av offentlighets- och sekretesslagen (2009:400).

I paragrafen regleras hur personuppgifter som den nationella kontaktpunkten har erhållit från ett annat land får användas (jfr prop. 2021/22:118 s. 95 och 96). Övervägandena finns i avsnitt 5.4.6 och 5.4.7.

Bestämmelsen innebär att personuppgifter som har erhållits enligt 28 § endast får användas för vissa syften. Detta hindrar emellertid inte att uppgifterna lämnas ut om det är tillåtet enligt offentlighets- och sekretesslagen så länge utlämnandet utgör ett led i ett tillåtet användningsområde.

I *andra stycket*, som är nytt, införs en upplysningsbestämmelse som tydliggör att personuppgifter som har erhållits enligt 28 § får lämnas ut i vissa fall enligt offentlighets- och sekretesslagen.

Bestämmelsen omfattar sådant uppgiftslämnande som sker på grund av att myndigheten ska lämna ut uppgifter, t.ex. med stöd av 6 kap. 5 § OSL. Vidare omfattar bestämmelsen även sådant uppgiftslämnande som sker med stöd av bestämmelser som medför att uppgifter får lämnas ut, t.ex. enligt generalklausulen i 10 kap. 27 § OSL.

9.18 Förslaget till lag om ändring i lagen (2014:400) om Polismyndighetens elimineringsdatabas

1 §

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

Uppgifter i elimineringsdatabasen får, *utöver vad som anges i tredje stycket*, endast behandlas för att upptäcka och utreda kontamineringar vid dna-analyser och hanteringen av dna-spår.

Uppgifter som behandlas enligt andra stycket får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.

Paragrafen reglerar Polismyndighetens rätt att föra register över dna-profiler (jfr prop. 2013/14:110 s. 538 och 539). Övervägandena finns i avsnitt 5.4.6.

Första stycket ändras inte.

Andra stycket ändrats på det sättet att det införs en hänvisning till den bestämmelse som införs i tredje stycket. Härigenom tydliggörs att sådana uppgifter som behandlas enligt andra stycket även får behandlas för uppgiftslämnande i överensstämmelse med lag och förordning.

Det nuvarande tredje stycket förs över till den nya 1 a § och ersätts med ett nytt tredje stycke.

I det nya *tredje stycket* införs en s.k. sekundär ändamålsbestämmelse. Av bestämmelsen, som är en upplysningsbestämmelse, följer att uppgifter som behandlas enligt första stycket även får behandlas för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning. Behandlingen förutsätter alltså att uppgifterna redan är föremål för behandling enligt andra stycket. Bestämmelsen omfattar sådant uppgiftslämnande som sker på grund av att myndigheten ska lämna ut uppgifter, t.ex. med stöd av 6 kap. 5 § OSL i fall då utlämnande inte kan ske med stöd av första stycket. Bestämmelsen omfattar även sådant uppgiftslämnande som sker med stöd av bestämmelser som medför att uppgifter får lämnas ut, t.ex. den s.k. generalklausulen i 10 kap. 27 § OSL. Bestämmelsen omfattar uppgiftslämnande till myndigheter och enskilda. Det avgörande är att uppgiftslämnandet sker med stöd av lag eller förordning.

Innebörden av vissa begrepp

1 a §

Begreppen dna-profil och dna-analys som används i lagen har samma betydelse som i lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område.

Bestämmelsen har utan ändringar förs över från nuvarande 1 § tredje stycket (jfr prop. 2017/18:269 s. 389).

9.19 Förslaget till lag om ändring i lagen (2016:526) om behandling av personuppgifter i ärenden om licens för läkemedel

8 a §

Personuppgifter som behandlas enligt 8 § får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.

Paragrafen, som är ny, innehåller en s.k. sekundär ändamålsbestämmelse om möjligheten att behandla personuppgifter för ändamål utöver de som anges i den primära ändamålsbestämmelsen i 8 §. Övervägandena finns i avsnitt 5.4.6.

Av bestämmelsen, som är en upplysningsbestämmelse, följer att de personuppgifter som behandlas för primära ändamål enligt 8 § även får behandlas för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning. Behandlingen förutsätter alltså att uppgifterna redan är föremål för behandling enligt 8 §. Bestämmelsen omfattar sådant uppgiftslämnande som sker på grund av att myndigheten ska lämna ut uppgifter, t.ex. med stöd av 6 kap. 5 § OSL i fall då utlämnande inte kan ske med stöd av 8 §. Bestämmelsen omfattar även sådant uppgiftslämnande som sker med stöd av bestämmelser som medför att uppgifter får lämnas ut, t.ex. den s.k. generalklausulen i 10 kap. 27 § OSL. Bestämmelsen omfattar uppgiftslämnande till myndigheter och enskilda. Det avgörande är att uppgiftslämnandet sker med stöd av lag eller förordning.

Elektroniskt utlämnande av personuppgifter

11 §

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

Paragrafen utgör en upplysningsbestämmelse om att uppgifter som inte är sekretessbelagda kan lämnas ut elektroniskt på annat sätt än genom direktåtkomst (jfr prop. 2015/16:143, s. 148). Övervägandena finns i avsnitt 5.6.3.

Ändringen utgör en modernisering och en språklig anpassning till övrig kompletterande dataskyddsreglering. Någon ändring i sak är inte avsedd.

9.20 Förslaget till lag om ändring i spellagen (2018:1138)

17 kap.

4 a §

Personuppgifter som behandlas enligt 4 § får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.

Paragrafen, som är ny, innehåller en s.k. sekundär ändamålsbestämmelse om möjligheten att behandla personuppgifter för ändamål utöver de som anges i den primära ändamålsbestämmelsen i 17 kap. 4 §. Övervägandena finns i avsnitt 5.4.6.

Av bestämmelsen, som är en upplysningsbestämmelse, följer att de uppgifter som behandlas för primära ändamål enligt 17 kap. 4 § även får behandlas för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning. Behandlingen förutsätter alltså att uppgifterna redan är föremål för behandling enligt 17 kap. 4 §. Bestämmelsen omfattar sådant uppgiftslämnande som sker på grund av att myndigheten ska lämna ut uppgifter, t.ex. med stöd av 6 kap. 5 § OSL i fall då utlämnande inte kan ske med stöd av 17 kap. 4 §. Bestämmelsen omfattar även sådant uppgiftslämnande som sker med stöd av bestämmelser som medför att uppgifter får lämnas ut, t.ex. den s.k. generalklausulen i 10 kap. 27 § OSL. Bestämmelsen

omfattar uppgiftslämnande till myndigheter och enskilda. Det avgörande är att uppgiftslämnandet sker med stöd av lag eller förordning.

9.21 Förslaget till lag om ändring i brottsdatalagen (2018:1177)

2 kap.

4 §

Innan personuppgifter får behandlas för ett nytt ändamål ska det säkerställas att

1. det finns en rättslig grund enligt 1 § för den nya behandlingen, och
2. det är nödvändigt och proportionerligt att personuppgifterna behandlas för det nya ändamålet.

Vid uppgiftslämnande som sker i överensstämmelse med lag eller förordning ska någon prövning enligt första stycket inte göras.

I paragrafen regleras förutsättningarna för att personuppgifter ska få behandlas för ett nytt ändamål inom lagens tillämpningsområde (jfr prop. 2017/18:232, s. 442 och 443). Övervägandena finns i avsnitt 5.5.2.

Första stycket ändras inte.

Ändringen i *andra stycket* innebär att en prövning enligt första stycket inte ska göras vid uppgiftslämnande som sker i överensstämmelse med lag eller förordning. Bestämmelsen omfattar sådant uppgiftslämnande som sker på grund av att myndigheten ska lämna ut uppgifter, t.ex. med stöd av 6 kap. 5 § OSL i fall då utlämnande inte kan ske med stöd av 1 eller 2 §§. Bestämmelsen omfattar även sådant uppgiftslämnande som sker med stöd av bestämmelser som medför att uppgifter får lämnas ut, t.ex. den s.k. generalklausulen i 10 kap. 27 § OSL. Bestämmelsen omfattar uppgiftslämnande till myndigheter och enskilda. Det avgörande är att uppgiftslämnandet sker med stöd av lag eller förordning.

22 §

Innan personuppgifter som behandlas med stöd av denna lag behandlas för ett ändamål utanför lagens tillämpningsområde ska det säkerställas att det är nödvändigt och proportionerligt att personuppgifterna behandlas för det ändamålet.

Vid uppgiftslämnande som sker i överensstämmelse med lag eller förordning ska någon prövning enligt första stycket inte göras.

I paragrafen anges vad som gäller när fråga uppkommer om att behandla personuppgifter, som behandlas med stöd av lagen, för nya ändamål utanför lagens tillämpningsområde (jfr prop. 2017/18:232, s. 451 och 452). Övervägandena finns i avsnitt 5.5.2.

Första stycket ändras inte.

Ändringen i *andra stycket* innebär att en prövning enligt första stycket inte ska göras vid uppgiftslämnande som sker i överensstämmelse med lag eller förordning. Bestämmelsen omfattar sådant uppgiftslämnande som sker på grund av att myndigheten ska lämna ut uppgifter, t.ex. med stöd av 6 kap. 5 § OSL. Bestämmelsen omfattar även sådant uppgiftslämnande som sker med stöd av bestämmelser som medför att uppgifter får lämnas ut, t.ex. den s.k. generalklausulen i 10 kap. 27 § OSL. Bestämmelsen omfattar uppgiftslämnande till myndigheter och enskilda. Det avgörande är att uppgiftslämnandet sker med stöd av lag eller förordning.

9.22 Förslaget till lag om ändring i lagen (2018:1180) om flygpassageraruppgifter i brottsbekämpningen

1 kap.

5 §

PNR-information får endast behandlas i syfte att förebygga, förhindra, upptäcka, utreda eller lagföra terroristbrottslighet eller annan allvarlig brottslighet, om inte annat anges i 6 § eller 5 kap. 3 §.

Att PNR-information får lämnas ut i vissa fall framgår av offentlighets- och sekretesslagen (2009:400).

I paragrafen regleras hur PNR-information får användas (jfr prop. 2017/18:234 s. 140). Övervägandena finns i avsnitt 5.4.1 och 5.4.7.

Bestämmelsen innebär att PNR-information endast får användas för vissa syften. Detta hindrar emellertid inte att uppgifterna lämnas ut om det är tillåtet enligt offentlighets- och sekretesslagen så länge utlämnandet utgör ett led i ett tillåtet användningsområde.

I *andra stycket*, som är nytt införs, en upplysningsbestämmelse som tydliggör att PNR-information får lämnas ut i vissa fall enligt offentlighets- och sekretesslagen.

9.23 Förslaget till lag om ändring i lagen (2018:1212) om nationell läkemedelslista

3 kap.

7 §

Personuppgifter som behandlas enligt 2–5 §§ får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.

Paragrafen, som är ny, innehåller en s.k. sekundär ändamålsbestämmelse om möjligheten att behandla personuppgifter för ändamål utöver de som anges i de primära ändamålsbestämmelserna i 3 kap. 2–5 §§. Övervägandena finns i avsnitt 5.4.6.

Av bestämmelsen, som är en upplysningsbestämmelse, följer att de uppgifter som behandlas för primära ändamål enligt 3 kap. 2–5 §§ även får behandlas för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning. Behandlingen förutsätter alltså att uppgifterna redan är föremål för behandling enligt 3 kap. 2–5 §§. Bestämmelsen omfattar sådant uppgiftslämnande som sker på grund av att myndigheten ska lämna ut uppgifter, t.ex. med stöd av 6 kap. 5 § OSL i fall då utlämnande inte kan ske med stöd av 3 kap. 2–5 §§. Bestämmelsen omfattar även sådant uppgiftslämnande som sker med stöd av bestämmelser som medför att uppgifter får lämnas ut, t.ex. den s.k. generalklausulen i 10 kap. 27 § OSL. Bestämmelsen omfattar uppgiftslämnande till myndigheter och enskilda. Det avgörande är att uppgiftslämnandet sker med stöd av lag eller förordning.

9.24 Förslaget till lag om ändring i vägtrafikdatalagen (2019:369)

2 kap.

17 §

Personuppgifter som behandlas enligt 3, 7, 11, 14 eller 16 §§ får även behandlas *för uppgiftslämnande i överensstämmelse med lag eller förordning.*

Paragrafen innehåller en s.k. sekundär ändamålsbestämmelse om möjligheten att behandla personuppgifter för ändamål utöver de som anges i de primära ändamålsbestämmelserna (jfr prop. 2018/19:33, s. 218). Övervägandena finns i avsnitt 5.4.6.

Av bestämmelsen, som är en upplysningsbestämmelse, följer att de personuppgifter som behandlas för primära ändamål enligt 3, 7, 11, 14 eller 16 §§ även får behandlas för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning. Behandlingen förutsätter alltså att uppgifterna redan är föremål för behandling enligt 3, 7, 11, 14 eller 16 §§. Bestämmelsen omfattar sådant uppgiftslämnande som sker på grund av att myndigheten ska lämna ut uppgifter, t.ex. med stöd av 6 kap. 5 § OSL i fall då utlämnande inte kan ske med stöd av 3, 7, 11, 14 eller 16 §§. Bestämmelsen omfattar även sådant uppgiftslämnande som sker med stöd av bestämmelser som medför att uppgifter får lämnas ut, t.ex. den s.k. generalklausulen i 10 kap. 27 § OSL. Bestämmelsen omfattar uppgiftslämnande till myndigheter och enskilda. Det avgörande är att uppgiftslämnandet sker med stöd av lag eller förordning.

Ändringen utgör en modernisering och en språklig anpassning till övrig kompletterande dataskyddsreglering. Någon ändring i sak är inte avsedd.

9.25 Förslaget till lag om ändring i kustbevakningsdatalagen (2019:429)

10 §

Personuppgifter som behandlas enligt 7 § får även behandlas *för uppgiftslämnande i överensstämmelse med* lag eller förordning.

Paragrafen reglerar ytterligare sekundära ändamål för vilka personuppgifter får behandlas, utöver vad som anges om sekundära ändamål i 9 § (jfr prop. 2018/19:65, s. 178). Övervägandena finns i avsnitt 5.4.6.

Genom ändringen tydliggörs att de uppgifter som behandlas för primära ändamål även får behandlas för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning. Behandlingen förutsätter alltså att uppgifterna redan är föremål för behandling enligt 7 §. Bestämmelsen omfattar liksom tidigare sådant uppgiftslämnande som sker på grund av att uppgifter ska lämnas ut, t.ex. med stöd av 6 kap. 5 § OSL i fall då utlämnande inte kan ske med stöd av 7 §. Bestämmelsen omfattar även sådant uppgiftslämnande som sker med stöd av bestämmelser som medför att uppgifter får lämnas ut, t.ex. den s.k. generalklausulen i 10 kap. 27 § OSL. Bestämmelsen omfattar uppgiftslämnande till myndigheter och enskilda. Det avgörande är att uppgiftslämnandet sker med stöd av lag eller förordning.

9.26 Förslaget till lag om ändring i lagen (2019:508) om behandling av personuppgifter i det fördelningsanalytiska statistiksystemet för inkomster och transfereringar

5 §

Utöver vad som anges i 4 § får Statistiska centralbyrån behandla personuppgifter om det är nödvändigt för att myndigheten ska kunna förvalta och utveckla Fasit.

Personuppgifter som behandlas enligt 4 § får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.

I paragrafen regleras förutsättningarna för att behandla sådana personuppgifter som finns i Fasit för andra ändamål än sådana som anges i 4 § (jfr prop. 2018/19:118 s. 52). Övervägandena finns i avsnitt 5.4.6.

I *andra stycket,* som är nytt, införs en s.k. sekundär ändamålsbestämmelse. Av bestämmelsen, som är en upplysningsbestämmelse, följer att de personuppgifter som behandlas för primära ändamål enligt 4 § även får behandlas för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning. Behandlingen förutsätter alltså att uppgifterna redan är föremål för behandling

enligt 4 §. Bestämmelsen omfattar sådant uppgiftslämnande som sker på grund av att myndigheten ska lämna ut uppgifter, t.ex. med stöd av 6 kap. 5 § OSL, i fall då utlämnande inte kan ske med stöd av första stycket. Bestämmelsen omfattar även sådant uppgiftslämnande som sker med stöd av bestämmelser som medför att uppgifter får lämnas ut, t.ex. den s.k. generalklausulen i 10 kap. 27 § OSL. Bestämmelsen omfattar uppgiftslämnande till myndigheter och enskilda. Det avgörande är att uppgiftslämnandet sker med stöd av lag eller förordning.

9.27 Förslaget till lag om ändring i lagen (2020:422) om Rättsmedicinalverkets elimineringsdatabas

1 §

Rättsmedicinalverket får föra ett register över dna- profiler i syfte att stärka kvaliteten i den rättsgenetiska verksamheten med dna-analyser (elimineringsdatabasen) i enlighet med denna lag.

Uppgifter i elimineringsdatabasen får, *utöver vad som anges i tredje stycket*, endast behandlas för att upptäcka och utreda kontamineringar av det som är föremål för dna-analys.

Uppgifter som behandlas enligt andra stycket får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.

I paragrafen regleras Rättsmedicinalverket rätt att föra ett register över dna-profiler som benämns elimineringsdatabasen och för vilka syften det får föras (jfr prop. 2019/20:106 s. 100). Övervägandena finns i avsnitt 5.4.6.

Första stycket ändras inte.

Andra stycket ändras på det sättet att det införs en hänvisning till den bestämmelse som införs i tredje stycket. Härigenom tydliggörs att sådana uppgifter som behandlas enligt andra stycket även får behandlas för uppgiftslämnande i överensstämmelse med lag och förordning.

I det nya *tredje stycket* införs en s.k. sekundär ändamålsbestämmelse. Av bestämmelsen, som är en upplysningsbestämmelse, framgår att uppgifter som behandlas enligt andra stycket även får behandlas för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning. Behandlingen förutsätter alltså att uppgifterna redan är föremål för behandling enligt andra stycket. Bestäm-

melsen omfattar sådant uppgiftslämnande som sker på grund av att myndigheten ska lämna ut uppgifter, t.ex. med stöd av 6 kap. 5 § OSL i fall då utlämnande inte kan ske med stöd av första stycket. Bestämmelsen omfattar även sådant uppgiftslämnande som sker med stöd av bestämmelser som medför att uppgifter får lämnas ut, t.ex. vid misstanke om vissa begångna brott enligt 10 kap. 23 § OSL. Bestämmelsen omfattar uppgiftslämnande till myndigheter och enskilda. Det avgörande är att uppgiftslämnandet sker med stöd av lag eller förordning.

9.28 Förslaget till lag om ändring i lagen (2021:319) om Transportstyrelsens olycksdatabas

7 §

Personuppgifter får behandlas i databasen om det är nödvändigt för
1. framställning av statistik inom trafiksäkerhetsområdet,
2. forskning som avser trafiksäkerhet, eller
3. planering, uppföljning, utvärdering eller kvalitetssäkring av trafiksäkerhetsarbete.

Paragrafen reglerar för vilka ändamål personuppgifter får behandlas i Transportstyrelsens olycksdatabas (jfr prop. 2020/21:124 s. 86 och 87).

Ändringen innebär att det nuvarande andra stycket flyttas till den nya 7 b §.

7 a §

Personuppgifter som behandlas enligt 7 § får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.

Paragrafen, som är ny, innehåller en s.k. sekundär ändamålsbestämmelse om möjligheten att behandla personuppgifter för ändamål utöver de som anges i den primära ändamålsbestämmelsen i 7 §. Övervägandena finns i avsnitt 5.4.6.

Av bestämmelsen, som är en upplysningsbestämmelse, följer att de personuppgifter som behandlas för primära ändamål enligt 7 § även får behandlas för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning. Behandlingen förutsätter

alltså att uppgifterna redan är föremål för behandling enligt 7 §. Bestämmelsen omfattar sådant uppgiftslämnande som sker på grund av att myndigheten ska lämna ut uppgifter, t.ex. med stöd av 6 kap. 5 § OSL i fall då utlämnande inte kan ske med stöd av 7 §. Bestämmelsen omfattar även sådant uppgiftslämnande som sker med stöd av bestämmelser som medför att uppgifter får lämnas ut, t.ex. den s.k. generalklausulen i 10 kap. 27 § OSL. Bestämmelsen omfattar uppgiftslämnande till myndigheter och enskilda. Det avgörande är att uppgiftslämnandet sker med stöd av lag eller förordning.

7 b §

Personuppgifter som behandlas i databasen får behandlas även för andra ändamål, under förutsättning att behandlingen inte är oförenlig med det ändamål för vilket uppgifterna samlades in.

Bestämmelsen förs över från nuvarande 1 § tredje stycket med endast en redaktionell ändring (jfr prop. 2020/21:124 s. 86 och 87).

9.29 Förslaget om lag om ändring i lagen (2021:626) om förarbevis för vattenskoter

25 a §

Personuppgifter som behandlas enligt 25 § första stycket får även behandlas för uppgiftslämnande i överenstämmelse med lag eller förordning.

Paragrafen, som är ny, innehåller en s.k. sekundär ändamålsbestämmelse om möjligheten att behandla personuppgifter för ändamål utöver de som anges i den primära ändamålsbestämmelsen i 25 §. Övervägandena finns i avsnitt 5.4.6.

Av bestämmelsen, som är en upplysningsbestämmelse, följer att de personuppgifter som behandlas för primära ändamål enligt 25 § även får behandlas för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning. Behandlingen förutsätter alltså att uppgifterna redan är föremål för behandling enligt 25 §. Bestämmelsen omfattar sådant uppgiftslämnande som sker på grund av att myndigheten ska lämna ut uppgifter, t.ex. med stöd av 6 kap. 5 § OSL i fall då utlämnande inte kan ske med stöd av 25 §. Bestäm-

melsen omfattar även sådant uppgiftslämnande som sker med stöd av bestämmelser som medför att uppgifter får lämnas ut, t.ex. den s.k. generalklausulen i 10 kap. 27 § OSL. Bestämmelsen omfattar uppgiftslämnande till myndigheter och enskilda. Det avgörande är att uppgiftslämnandet sker med stöd av lag eller förordning.

9.30 Förslaget till lag om ändring i lagen (2021:1171) om behandling av personuppgifter vid Försvarsmakten

2 kap.

9 §

Försvarsmakten får behandla personuppgifter om det är nödvändigt för diarieföring, arkivering, handläggning av ett ärende eller för att utföra annan liknande uppgift som myndigheten har.

Personuppgifter som behandlas enligt 2, 3 eller 5 §§ får även behandlas för uppgiftslämnande i överenstämmelse med lag eller förordning.

Paragrafen innehåller förutsättningarna för behandling av personuppgifter i Försvarsmaktens ärendehantering. Bestämmelsen avser ärenden som inleds såväl på Försvarsmaktens eget initiativ som efter framställning av annan (jfr prop. 2020/21:224, s. 180). Övervägandena finns i avsnitt 5.4.6.

Genom *andra stycket*, som är nytt, införs en s.k. sekundär ändamålsbestämmelse om möjligheten att behandla personuppgifter för ändamål utöver de som anges i de primära ändamålsbestämmelserna i 2 kap. 2, 3 och 5 §§. Genom bestämmelsen, som är en upplysningsbestämmelse, tydliggörs att de uppgifter som behandlas för primära ändamål även får behandlas för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning. Behandlingen förutsätter alltså att uppgifterna redan är föremål för behandling enligt 2, 3 eller 5 §§. Bestämmelsen omfattar sådant uppgiftslämnande som sker på grund av att uppgifter ska lämnas ut, t.ex. med stöd av 6 kap. 5 § OSL i fall då utlämnande inte kan ske med stöd av 2, 3 eller 5 §§. Bestämmelsen omfattar även sådant uppgiftslämnande som sker med stöd av bestämmelser som medför att uppgifter får lämnas ut, t.ex. den s.k. generalklausulen i 10 kap. 27 § OSL. Bestämmelsen

omfattar uppgiftslämnande till myndigheter och enskilda. Det avgörande är att uppgiftslämnandet sker med stöd av lag eller förordning.

9.31 Förslaget till lag om ändring i lagen (2021:1172) om behandling av personuppgifter vid Försvarets radioanstalt

2 kap.

8 a §

Personuppgifter som behandlas enligt 2, 5 eller 7 §§ får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.

Paragrafen, som är ny, innehåller en s.k. sekundär ändamålsbestämmelse om möjligheten att behandla personuppgifter för ändamål utöver de som anges i den primära ändamålsbestämmelsen i 2, 5 eller 7 §§. Övervägandena finns i avsnitt 5.4.6.

Av bestämmelsen, som är en upplysningsbestämmelse, följer att de personuppgifter som behandlas för primära ändamål enligt 2, 5 eller 7 §§ även får behandlas för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning. Behandlingen förutsätter alltså att uppgifterna redan är föremål för behandling enligt 2, 5 eller 7 §§. Bestämmelsen omfattar sådant uppgiftslämnande som sker på grund av att myndigheten ska lämna ut uppgifter, t.ex. med stöd av 6 kap. 5 § OSL i fall då utlämnande inte kan ske med stöd av 2, 5 eller 7 §§. Bestämmelsen omfattar även sådant uppgiftslämnande som sker med stöd av bestämmelser som medför att uppgifter får lämnas ut, t.ex. den s.k. generalklausulen i 10 kap. 27 § OSL. Bestämmelsen omfattar uppgiftslämnande till myndigheter och enskilda. Det avgörande är att uppgiftslämnandet sker med stöd av lag eller förordning.

9.32 Förslaget till lag om ändring i biobankslagen (2023:38)

3 kap.

1 a §

Personuppgifter som behandlas i registret får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.

Paragrafen, som är ny, innehåller en s.k. sekundär ändamålsbestämmelse om möjligheten att behandla personuppgifter för ändamål utöver de som anges i den primära ändamålsbestämmelsen i 3 kap. 1 §. Övervägandena finns i avsnitt 5.4.6.

Av bestämmelsen, som är en upplysningsbestämmelse, följer att de uppgifter som behandlas för primära ändamål i registret enligt 3 kap. 1 § även får behandlas för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning. Behandlingen förutsätter alltså att uppgifterna redan är föremål för behandling enligt 3 kap. 1 §. Bestämmelsen omfattar sådant uppgiftslämnande som sker på grund av att myndigheten ska lämna ut uppgifter, t.ex. med stöd av 6 kap. 5 § OSL i fall då utlämnande inte kan ske med stöd av 3 kap. 1 §. Bestämmelsen omfattar även sådant uppgiftslämnande som sker med stöd av bestämmelser som medför att uppgifter får lämnas ut, t.ex. den s.k. generalklausulen i 10 kap. 27 § OSL. Bestämmelsen omfattar uppgiftslämnande till myndigheter och enskilda. Det avgörande är att uppgiftslämnandet sker med stöd av lag eller förordning.

7 kap.

5 §

PKU-registret får, *utöver vad som anges i andra stycket*, användas endast för de ändamål som anges i 2 § och för framställning av statistik.

Personuppgifter som behandlas enligt 2 § får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.

I paragrafen regleras vad PKU-registret får användas för (jfr prop. 2021/22:257 s. 281). Övervägandena finns i avsnitt 5.4.6.

Paragrafen ändras på det sättet att det tydliggörs att sådana personuppgifter som behandlas för de primära ändamål som anges i 2 § även får behandlas för uppgiftslämnande i överensstämmelse med lag och förordning i enlighet med det nya andra stycket.

I det nya andra stycket införs ytterligare en s.k. sekundär ändamålsbestämmelse. Av bestämmelsen, som är en upplysningsbestämmelse, följer att de personuppgifter som behandlas för primära ändamål enligt 2 § även får behandlas för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning. Behandlingen förutsätter alltså att uppgifterna redan är föremål för behandling enligt 2 §. Bestämmelsen omfattar sådant uppgiftslämnande som sker på grund av att myndigheten ska lämna ut uppgifter, t.ex. med stöd av 6 kap. 5 § OSL i fall då utlämnande inte kan ske med stöd av 2 §. Bestämmelsen omfattar även sådant uppgiftslämnande som sker med stöd av bestämmelser som medför att uppgifter får lämnas ut, t.ex. den s.k. generalklausulen i 10 kap. 27 § OSL. Bestämmelsen omfattar uppgiftslämnande till myndigheter och enskilda. Det avgörande är att uppgiftslämnandet sker med stöd av lag eller förordning.

9.33 Förslaget till lag om ändring i lagen (2024:488) om personuppgiftsbehandling i vissa ärenden om stöd till civilsamhället

7 a §

Personuppgifter som behandlas enligt 6 § får även behandlas för uppgiftslämnande i överensstämmelse med lag eller förordning.

Paragrafen, som är ny, innehåller en s.k. sekundär ändamålsbestämmelse om möjligheten att behandla personuppgifter för ändamål utöver de som anges i den primära ändamålsbestämmelsen i 6 §. Övervägandena finns i avsnitt 5.4.6.

Av bestämmelsen, som är en upplysningsbestämmelse, följer att de personuppgifter som behandlas för primära ändamål enligt 6 § även får behandlas för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning. Behandlingen förutsätter alltså att uppgifterna redan är föremål för behandling enligt 6 §. Bestämmelsen omfattar sådant uppgiftslämnande som sker på grund av att myndigheten ska lämna ut uppgifter, t.ex. med stöd av 6 kap.

5 § OSL i fall då utlämnande inte kan ske med stöd av 6 §. Bestämmelsen omfattar även sådant uppgiftslämnande som sker med stöd av bestämmelser som medför att uppgifter får lämnas ut, t.ex. den s.k. generalklausulen i 10 kap. 27 § OSL. Bestämmelsen omfattar uppgiftslämnande till myndigheter och enskilda. Det avgörande är att uppgiftslämnandet sker med stöd av lag eller förordning.

9.34 Förslaget till lag om ändring i lagen (2024:1146) om vissa forskningsdatabaser

3 kap.

3 §

Personuppgifter och uppgifter om avlidna får, utöver vad som följer av 2 och 5 §§ samt 2 kap. 2 § första stycket 2 eller 3, lämnas ut *i överensstämmelse med* lag eller förordning.

Paragrafen reglerar utlämnande av personuppgifter och uppgifter om avlidna från en forskningsdatabas (jfr prop. 2024/25:19 s. 250 och 251). Övervägandena finns i avsnitt 5.4.6.

Genom ändringen tydliggörs att personuppgifter och uppgifter om avlidna, utöver vad som följer av 2 och 5 §§ samt 2 kap. 2 § första stycket 2 eller 3, får lämnas ut i överensstämmelse med lag eller förordning. Bestämmelsen omfattar liksom tidigare sådant uppgiftslämnande som sker på grund av att uppgifter ska lämnas ut, t.ex. med stöd av 6 kap. 5 § OSL i fall då utlämnande inte kan ske med stöd av 2 och 5 §§ samt 2 kap. 2 § första stycket 2 eller 3. Bestämmelsen omfattar även sådant uppgiftslämnande som sker med stöd av bestämmelser som medför att uppgifter får lämnas ut, t.ex. vid misstanke om vissa begångna brott enligt 10 kap. 23 § OSL. Bestämmelsen omfattar uppgiftslämnande till myndigheter och enskilda. Det avgörande är att uppgiftslämnandet sker med stöd av lag eller förordning.

Kommittédirektiv 2023:146

Förbättrade möjligheter till informationsutbyte mellan myndigheter

Beslut vid regeringssammanträde den 19 oktober 2023

Sammanfattning

En särskild utredare ska överväga och föreslå förbättrade möjligheter att utbyta information om enskilda inom och mellan myndigheter och andra organ som enligt offentlighets- och sekretesslagen (2009:400), förkortad OSL, jämställs med myndigheter. Syftet är att information ska kunna utbytas i den utsträckning som det behövs för att myndigheterna bl.a. ska kunna förhindra, förebygga, upptäcka, utreda och ingripa mot fusk, felaktiga utbetalningar, regelöverträdelser och brottslighet så effektivt som möjligt, utan att det medför ett oproportionerligt intrång i den personliga integriteten.

Utredaren ska bl.a.

- kartlägga behovet av att myndigheter får förbättrade möjligheter att utbyta information med varandra i syfte att särskilt förhindra, förebygga, upptäcka, utreda och ingripa mot fusk, felaktiga utbetalningar, regelöverträdelser och brottslighet,
- analysera och ta ställning till hur behovet av att utbyta sekretessbelagd information kan tillgodoses,
- särskilt överväga och lämna förslag på en generell bestämmelse som gör det möjligt att på ett effektivt sätt lämna uppgifter som omfattas av sekretess till skydd för enskilda till en annan myndighet, såväl på begäran som på eget initiativ,

- analysera och ta ställning till hur behovet av att utbyta offentlig information kan tillgodoses,
- särskilt överväga och lämna förslag på en bestämmelse som i större utsträckning gör det möjligt att på eget initiativ lämna ut offentliga uppgifter till en annan myndighet,
- göra en översyn, i den utsträckning det behövs, av myndigheternas registerförfattningar, för att möjliggöra att de förslag som lämnas tjänar sitt syfte och kan tillämpas på ett ändamålsenligt sätt, och
- lämna nödvändiga författningsförslag.

Uppdraget ska slutredovisas senast den 28 februari 2025. Senast den 30 augusti 2024 ska utredaren lämna en delredovisning av uppdraget att kartlägga myndigheternas behov av förbättrade möjligheter till informationsutbyte, att analysera och ta ställning till hur behovet av att utbyta sekretessbelagd information kan tillgodoses samt att särskilt överväga och lämna förslag på en generell möjlighet att lämna uppgifter som omfattas av sekretess till skydd för enskilda till en annan myndighet, såväl på begäran som på eget initiativ.

Uppdraget att överväga förbättrade möjligheter att utbyta uppgifter om enskilda mellan myndigheter

Vikten av ett välfungerande informationsutbyte

Tillit till det offentliga och till ett lands institutioner är en av grundstenarna för ett välfungerande samhälle. Grundläggande för medborgarnas tillit är att det allmänna sköter sina åtaganden på ett effektivt och rättssäkert sätt. För det behöver myndigheterna tillgång till uppgifter som är korrekta, aktuella och relevanta. Uppgifter som finns tillgängliga hos en myndighet kan vara avgörande för att en annan myndighet ska kunna utföra sitt uppdrag på ett effektivt sätt. Det gäller inte minst i fråga om att förebygga, förhindra och ingripa mot fusk, felaktiga utbetalningar, regelöverträdelser och brottslighet.

En viktig beståndsdel i det allmännas åtagande är välfärdssystemen. Utbetalningar av medel från det allmänna ska vara korrekta och göras på ett sådant sätt att de kommer rätt personer och företag till del. Missbruk och felaktigt nyttjande av välfärdssystemen gör inte bara att

systemen riskerar att tappa i legitimitet utan orsakar även betydande ekonomiska förluster för det allmänna. Ekonomistyrningsverket bedömer att den totala omfattningen av felaktiga utbetalningar från välfärdssystemen under 2021 uppgick till mellan 13 och 16,3 miljarder kronor (Omfattningen av felaktiga utbetalningar från välfärdssystemen, ESV 2023:22). Angrepp på utbetalande system och undandragande av skatter och avgifter bedöms fortsatt vara ett av de allvarligaste hoten mot samhället från den organiserade brottsligheten (Myndighetsgemensam lägesbild om organiserad brottslighet 2021 och 2023).

Felaktiga utbetalningar från välfärdssystemen är del av det som brukar betecknas som den kriminella ekonomin. Polismyndigheten m.fl. karakteriserar kriminell ekonomi som ett ekosystem av brottsvinster som genereras, hanteras och till delar återinvesteras i fortsatt brottslig verksamhet. Även legala medel, till exempel olika typer av bidrag eller lån, som används för investering i brottslig verksamhet omfattas. Brottsvinsterna återinvesteras i den illegala verksamheten eller förs in i det legala systemet inom eller utanför Sverige, vilket försvårar upptäckt och lagföring (Myndighetsgemensam lägesbild organiserad brottslighet 2023). Brottsvinster genereras från en rad olika källor. Det kan handla om alltifrån narkotikahandel, välfärdsbrott och arbetslivskriminalitet till undandragande av skatt, penningtvätt och illegal avfallshantering.

Under de senaste åren har våld i form av skjutningar och sprängningar ökat. På senare tid har polisen vittnat om att allt yngre personer påträffas, både som offer och som gärningsmän, i samband med grova våldsbrott och uppgörelser mellan kriminella nätverk. Genom att använda sig av yngre personer som utförare kan äldre kriminella skydda sig själva för exponering och straff. Barn som inte är straffmyndiga utför i stället de grova brotten. I en rapport om kriminella nätverk i polisregion Stockholm uppges att en majoritet av de aktiva nätverken involverar personer under 16 år i sin brottsliga verksamhet och att det sker i större utsträckning än vad som tidigare varit känt (Kriminella nätverk inom den organiserade brottsligheten i region Stockholm, Polismyndigheten 2021).

Det är angeläget att vidta åtgärder för att skydda barn och unga som riskerar att fara illa och utnyttjas i kriminella sammanhang och förhindra att de börjar att begå brott eller lockas in i en livsstil som är präglad av brottslighet. För att det ska vara möjligt kan myndig-

heter som kommer i kontakt med barn och unga behöva få bättre förutsättningar att dela och ta emot relevant information.

Enligt flera myndigheter som samverkar mot organiserad brottslighet utnyttjar kriminella aktörer de luckor som uppstår när det finns ett delat ansvar mellan myndigheter i form av kontroll och tillsyn kontra exempelvis ansvar för utbetalningar. Informationsutbyte och samverkan anses av dessa myndigheter samtidigt begränsas av sekretessregler på ett sätt som gör det svårt för vissa myndigheter att på egen hand upptäcka brottslighet (Myndighetsgemensam lägesbild organiserad brottslighet 2021).

Ett välfungerande informationsutbyte mellan myndigheter är ofta en grundläggande förutsättning för att olika former av fusk, regelöverträdelser och brottslighet ska kunna förebyggas, utredas och bekämpas. Detsamma gäller för att bl.a. förhindra och upptäcka felaktiga utbetalningar. Ett exempel är migrationsområdet där ett effektivt informationsutbyte kan bidra till att motverka att arbetskraft exploateras och att felaktiga uppgifter läggs till grund för uppehållstillstånd i Sverige. Ett annat exempel där ett välfungerande informationsutbyte kan vara en viktig komponent för att minska riskerna för oegentligheter är myndigheternas utbetalningar av EU-medel som är kopplade till olika EU-fonder och EU-program. I dagsläget saknar myndigheterna möjlighet att strukturerat och regelmässigt utbyta och samköra uppgifter om stödmottagare, däribland möjligheten att kontrollera riktigheten i vissa ingivna underlag. Ett förbättrat informationsutbyte mellan de myndigheter som administrerar EU-medel kan därför bidra till att bl.a. förebygga och motverka dubbelfinansiering och andra typer av bedrägerier.

Företeelser som exempelvis fusk, regelöverträdelser och brottslighet är samhällsövergripande. Av det skälet är behovet av informationsutbyte inte begränsat till ett visst samhällsområde eller några enstaka myndigheter. Det gäller även om behovet av information skiljer sig åt mellan olika myndigheter och verksamheter. De brottsbekämpande myndigheternas behov av information från andra myndigheter kan t.ex. vara olika stort beroende på vilken brottslighet och vilka aktörer det är frågan om. Det kan röra sig om uppgifter på individnivå, dvs. som rör enskilda, men också uppgifter av betydelse för att skapa lägesbilder av brottslighet eller förstå brottsupplägg.

Ett ineffektivt informationsutbyte är kostsamt för samhället och kan urholka förtroendet för det allmänna. Ett välfungerande informationsutbyte mellan myndigheter bidrar däremot till att reducera samhällets kostnader, och sårbarhet och stärka dess motståndskraft mot bl.a. fusk, regelöverträdelser och brottslighet.

Dagens möjligheter att utbyta uppgifter

Bestämmelser om sekretess och utlämnande av uppgifter

Vilken information myndigheter får utbyta styrs av flera olika regelverk. OSL innehåller bestämmelser om tystnadsplikt i det allmännas verksamhet och om förbud mot att lämna ut handlingar. En sekretessbelagd uppgift får som utgångspunkt inte lämnas från en myndighet till en annan, eller mellan olika verksamhetsgrenar inom samma myndighet när de är att betrakta som självständiga i förhållande till varandra (8 kap. 1 och 2 §§ OSL). Skälet till detta är intresset av att uppgifter som omfattas av sekretess inte når en större krets än vad som är absolut nödvändigt. För att myndigheter ska kunna utbyta sekretessbelagda uppgifter krävs i princip att en sekretessbrytande bestämmelse är tillämplig. Som huvudregel gäller också att ett utlämnande ska föregås av en begäran från en myndighet om att få en eller flera uppgifter från en annan myndighet.

I 10 kap. OSL finns ett antal sekretessbrytande bestämmelser och undantag från sekretess som gäller till förmån för såväl enskilda som myndigheter. Enligt 10 kap. 2 § OSL hindrar inte sekretess att en uppgift lämnas till en enskild eller en annan myndighet, om det är nödvändigt för att den utlämnande myndigheten ska kunna fullgöra sin verksamhet. Bestämmelsen ska tillämpas restriktivt och avsikten är inte att en myndighet av rena effektivitetsskäl ska kunna bryta sekretessen. Sekretessen får endast brytas i de fall då det för fullgörandet av ett visst åtagande som en myndighet har är en nödvändig förutsättning att en sekretessbelagd uppgift lämnas ut (prop. 1979/80:2 del A s. 465 och prop. 2008/09:150 s. 368).

I 10 kap. 27 § OSL finns den s.k. generalklausulen som innebär att sekretess inte hindrar att uppgifter lämnas till en myndighet om det är uppenbart att intresset av att uppgifterna lämnas har företräde framför det intresse som sekretessen ska skydda. Syftet med generalklausulen är att den ska utgöra en ventil för det fall uppgifter uppen-

bart behöver lämnas ut och situationen inte har kunnat förutses i lagstiftningen. Från bestämmelsens tillämpningsområde finns vissa undantag. Bestämmelsen bryter t.ex. inte sekretess för vissa uppgifter om enskilda inom socialtjänsten och hälso- och sjukvården.

I 10 kap. 28 § OSL anges att sekretess inte hindrar att en uppgift lämnas till en annan myndighet, om uppgiftsskyldighet följer av lag eller förordning. Bestämmelser om uppgiftsskyldighet används ofta för att reglera ett vanligen förekommande informationsutbyte mellan myndigheter. Om en bestämmelse om uppgiftsskyldighet är tillämplig, innebär det att såväl sekretessbelagda som offentliga uppgifter ska lämnas ut.

I 6 kap. 5 § OSL regleras en skyldighet för myndigheter att lämna uppgifter. Enligt bestämmelsen ska en myndighet på begäran av en annan myndighet lämna en uppgift som den förfogar över, om inte uppgiften är sekretessbelagd eller det skulle hindra arbetets behöriga gång. Bestämmelsen bryter alltså inte eventuell sekretess. För att en uppgift ska kunna lämnas ut krävs att uppgiften inte är sekretessreglerad, att det finns ett undantag från sekretess, att uppgiften kan lämnas ut efter en sekretessprövning eller att det finns en sekretessbrytande bestämmelse som är tillämplig. Skyldigheten gäller alla uppgifter som en myndighet förfogar över, alltså inte bara uppgifter ur allmänna handlingar (prop. 1979/80:2 Del A s. 361).

Bestämmelser om behandling av personuppgifter

Den information som myndigheter behöver utbyta är ofta personuppgifter. Möjligheten att utbyta personuppgifter påverkas inte bara av eventuell sekretess, utan också av bestämmelser om behandling av personuppgifter. För personuppgiftsbehandling i allmänhet gäller 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), här benämnd EU:s dataskyddsförordning. Ett av syftena med förordningen är att skydda fysiska personers grundläggande friheter och rättigheter, särskilt deras rätt till skydd för personuppgifter.

I artikel 5 i EU:s dataskyddsförordning anges de grundläggande principerna för behandling av personuppgifter, bl.a. att uppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade, att de ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas, att de ska vara korrekta och om nödvändigt uppdaterade samt att de ska behandlas på ett sätt som säkerställer lämplig säkerhet för uppgifterna. Personuppgifter ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål (den s.k. finalitetsprincipen).

I artikel 6 i EU:s dataskyddsförordning uttrycks kravet att det ska finnas en rättslig grund för varje behandling av personuppgifter. Bland de rättsliga grunder som anges i artikeln kan nämnas att behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige (artikel 6.1 c) eller för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning (artikel 6.1 e). Av artikel 6.3 framgår det att den rättsliga grunden ska fastställas i unionsrätten eller i nationell rätt vid behandling enligt artikel 6.1 c och e. En bestämmelse i nationell rätt som tillåter viss behandling av personuppgifter måste uppfylla ett mål av allmänt intresse och vara proportionell mot det legitima mål som eftersträvas. Grunden ska vara tydlig och precis, och dess tillämpning ska vara förutsebar för personer som omfattas av den (skäl 41 i EU:s dataskyddsförordning). I artikel 9 i EU:s dataskyddsförordning finns bestämmelser om behandling av särskilda kategorier av personuppgifter, s.k. känsliga personuppgifter. Till dessa särskilda kategorier hör bl.a. uppgifter som avslöjar politiska åsikter och religiös övertygelse samt uppgifter om hälsa.

EU:s dataskyddsförordning kompletteras i olika avseenden av nationella författningar som t.ex. lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning, här benämnd dataskyddslagen. Förutom dataskyddslagen finns även registerförfattningar som reglerar hur personuppgifter får behandlas i vissa offentliga verksamheter.

När vissa behöriga myndigheter behandlar personuppgifter i syfte att t.ex. förebygga, förhindra eller upptäcka brottslig verksamhet gäller i stället brottsdatalagen (2018:1177), genom vilken det s.k. dataskyddsdirektivet i huvudsak har genomförts. Brottsdatalagen är, liksom dataskyddslagen, subsidiär. Om det för en myndighet som be-

driver verksamhet inom brottsdatalagens tillämpningsområde finns en författning med bestämmelser som avviker från brottsdatalagen, ska därför den författningen tillämpas.

En effektiv och ändamålsenlig samverkan förutsätter goda möjligheter att utbyta information

Det är viktigt att allmänheten har förtroende för att myndigheterna utför sina förvaltningsuppgifter på ett ansvarsfullt och korrekt sätt. För att den statliga förvaltningen ska kunna vara effektiv och rättssäker krävs att det finns ett gott samarbete myndigheterna emellan. Skyldigheten för myndigheter att samverka och bistå varandra framgår bl.a. av 8 § förvaltningslagen (2017:900). Lagen gäller för i princip hela förvaltningen och omfattar både statliga och kommunala förvaltningsmyndigheter (prop. 2016/17:180 s. 25–27). I myndighetsförordningen (2007:515), som är tillämplig för alla förvaltningsmyndigheter under regeringen, anges vidare att myndigheter ska verka för att genom samarbete med myndigheter och andra ta till vara de fördelar som kan vinnas för enskilda samt för staten som helhet (6 §). Bestämmelsen syftar till att underlätta för myndigheter att fullgöra sin verksamhet.

Behovet av att myndigheter ges förbättrade möjligheter att utbyta information med varandra har uppmärksammats inom flera myndighetsgemensamma samverkansinsatser. Delegationen mot arbetslivskriminalitet bedömer att det myndighetsgemensamma arbetet skulle kunna bli mer effektivt och träffsäkert om möjligheten till informationsutbyte stärktes (se betänkandet Arbetslivskriminalitet En definition, en inledande bedömning av omfattningen, lärdomar från Norge [SO 2022:36]). Ett annat exempel är den myndighetsgemensamma satsningen mot organiserad brottslighet där tolv myndigheter samverkar strategiskt och operativt utifrån en gemensam inriktning, på regeringens uppdrag sedan 2009. I rapporten Myndigheter i samverkan mot organiserad brottslighet 2022 framhåller myndigheterna inom satsningen att informationsdelning mellan myndigheterna är en viktig del av den operativa verksamheten som har bidragit till att andra myndigheter har kunnat uppnå framgång i sitt arbete.

Behovet av ett utökat informationsutbyte mellan myndigheter har även uppmärksammats av en rad olika utredningar de senaste åren (se t.ex. Bidragsbrott och underrättelseskyldighet vid felaktiga utbetal-

ningar från välfärdssystemen – en utvärdering [SOU 2018:14], Samlade åtgärder för korrekta utbetalningar från välfärdssystemen [SOU 2019:59], Kontroll för ökad tilltro [SOU 2020:35], Uppdrag om förhindrande av brott kopplade till de stödåtgärder med statsfinansiella, samhällsekonomiska konsekvenser som vidtas med anledning av det nya coronaviruset [Ds 2020:28] och Myndigheter i samverkan mot arbetslivskriminalitet [Ds 2021:1]).

Även i pågående utredningar uppmärksammas behovet av ett utökat informationsutbyte mellan myndigheter. Regeringen beslutade i januari i år om tilläggsdirektiv till Utredningen om förbättrade möjligheter att utbyta information med brottsbekämpande myndigheter (Ju 2022:03). Utredaren ska även ska ta ställning till hur det kan införas en ny huvudregel i sekretesslagstiftningen som innebär att de myndigheter och andra aktörer som omfattas av uppdraget ska kunna utbyta information med brottsbekämpande myndigheter när det behövs för att förebygga och bekämpa brott (dir 2023:11). Uppdraget ska redovisas den 31 oktober 2023.

Ett antal åtgärder har redan vidtagits för att förbättra möjligheterna till informationsutbyte mellan myndigheter i syfte att bl.a. hindra felaktiga utbetalningar och motverka brottslighet, och det pågår ett antal utredningar som syftar till att på olika sätt förbättra informationsöverföringen mellan myndigheter. Den 1 januari 2024 ska den nya Utbetalningsmyndigheten inleda sin verksamhet med att förebygga, förhindra och upptäcka felaktiga utbetalningar från välfärdssystemen, och arbetet med att förbereda verksamheten pågår (dir 2022:8 och 2022:137). Samtidigt visar den kartläggning som har gjorts i promemorian Utökat informationsutbyte (Ds 2022:13) att omfattande behov av utökat informationsutbyte kvarstår. I promemorian görs bedömningen att myndigheterna behöver ges bättre förutsättningar att ta ett helhetsansvar för det offentliga åtagandet genom att bl.a. på eget initiativ kunna uppmärksamma andra myndigheter på felaktigheter eller andra omständigheter som har betydelse för den mottagande myndighetens verksamhet. Myndigheterna behöver även ges bättre förutsättningar att kunna utbyta information elektroniskt.

Undersökningarna i promemorian Utökat informationsutbyte har varit avgränsade till behovet av ytterligare informationsutbyte för att säkerställa att myndigheter, kommuner och arbetslöshetskassor har tillgång till den information om enskilda personer och företag som de behöver för att fatta korrekta beslut i fråga om ersättningar från

välfärdssystemen, och för att motverka arbetslivskriminalitet. För att det ska vara möjligt att ta ett större grepp om frågan om förbättrat informationsutbyte mellan myndigheter krävs att en mer heltäckande kartläggning av behovet görs.

Utredaren ska därför

- med utgångspunkt i den kartläggning som gjorts i promemorian Utökat informationsutbyte (Ds 2022:13) och med beaktande av det arbete som pågår i bl.a. Utredningen om förbättrade möjligheter att utbyta information med brottsbekämpande myndigheter (Ju 2022:03) kartlägga behovet av att myndigheter får förbättrade möjligheter att utbyta information i syfte att särskilt förhindra, förebygga, upptäcka, utreda och ingripa mot fusk, felaktiga utbetalningar, regelöverträdelser och brottslighet.

Begränsningar och hinder som försvårar ett effektivt och ändamålsenligt informationsutbyte

I flera utredningar och myndighetsrapporter och i den allmänna debatten har ett antal begränsningar och hinder som försvårar ett effektivt och ändamålsenligt informationsutbyte mellan myndigheter återkommande lyfts fram. Enligt den analys som har gjorts i promemorian Utökat informationsutbyte (Ds 2022:13) är bilden av vad som hindrar eller begränsar informationsutbytet mångfasetterad. De rättsliga hindren är mest framträdande, men vid sidan av dem handlar det om hinder förknippade med tekniska förutsättningar och hinder kopplade till tillämpning av regelverket. När det gäller rättsliga hinder konstaterar utredningen att befintliga sekretessbrytande bestämmelser inte medger att uppgifter av betydelse för en annan myndighet eller kommun utbyts i tillräcklig omfattning. Generalklausulens tillämpningsområde är för begränsat och befintliga bestämmelser om uppgiftsskyldighet är i vissa fall för detaljerade. Det befintliga regelverket medger inte heller att uppgifter i tillräcklig omfattning lämnas på en utlämnande myndighets eget initiativ. Enligt promemorian skulle en utökad möjlighet för myndigheter att på eget initiativ lämna ut uppgifter innebära att den mottagande myndigheten i större utsträckning får kännedom om uppgifter som har betydelse för den egna verksamheten vilket bl.a. skulle leda till bättre beslutsunderlag och effektivare kontrollverksamhet.

En annan begränsning som lyfts fram i promemorian Utökat informationsutbyte är att regelverken om hur personuppgifter får behandlas inte i tillräcklig omfattning möjliggör att uppgifter kan utbytas elektroniskt. Att uppgifter kan utbytas elektroniskt är enligt utredningen i princip en förutsättning för ett effektivt informationsutbyte. Utredningen bedömer att det finns omotiverade begränsningar eller hinder för myndigheter att utbyta personuppgifter elektroniskt.

Försäkringskassan lyfter i en hemställan till regeringen fram att det regelverk som i dag finns för hur myndigheter får dela uppgifter med varandra har kommit att bli svåröverskådligt och svårtillämpat med nya uppgiftsskyldigheter som har tillkommit vartefter (Ju2021/01700). Myndigheten anser att dagens regelverk inte är tillräckligt effektivt eller ändamålsenligt för att kunna komma till rätta med de felaktiga utbetalningarna från välfärdssystemen. Försäkringskassan efterlyser en utredning som analyserar om sekretessgränserna mellan myndigheter ska avskaffas när det gäller sekretess till skydd för enskilda.

Enligt Brottsförebyggande rådets rapport Informationsdelning mellan polis och socialtjänst (2021:2) är det oklart vad i sekretesslagstiftningen som utgör ett hinder för informationsdelning, men enligt rapporten handlar det huvudsakligen om avsaknaden av vägledning om hur lagen ska tillämpas i enskilda fall, snarare än bestämmelsernas utformning. Förutom att sekretesslagstiftningen ses som komplicerad, är många rädda för att göra fel på grund av det personliga ansvar som följer av straffbestämmelsen om brott mot tystnadsplikten. Det faktum att en tjänsteman däremot sällan riskerar något ansvar om information inte lämnas ut bidrar till att sekretessbrytande bestämmelser inte utnyttjas i den utsträckning som är möjligt.

En generell sekretessbrytande bestämmelse

Ett sätt att förbättra myndigheternas möjligheter att utbyta information kan vara att införa en generell sekretessbrytande bestämmelse som ger myndigheterna en möjlighet att utbyta sekretessbelagda uppgifter mer rutinmässigt. Ett sådant förslag har lämnats i promemorian Utökat informationsutbyte (Ds 2022:13). Förslaget innebär att sekretess inte ska hindra att en uppgift som en myndighet förfogar över lämnas till en annan myndighet, om uppgiften behövs för att den mottagande myndigheten ska kunna fullgöra sin författningsregle-

rade verksamhet. Bestämmelsen föreslås endast bryta sekretess till skydd för enskilda och omfattar ett rutinmässigt utlämnande av uppgifter. En uppgift ska dock inte lämnas ut om övervägande skäl talar mot det. Viss sekretess till skydd för enskilda föreslås undantas, däribland s.k. hälso- och sjukvårdssekretess och socialtjänstsekretess. Bestämmelsen innebär att uppgifter ska få lämnas ut såväl på begäran som på eget initiativ. Det innebär inte att den myndighet som förfogar över uppgiften har en skyldighet att lämna ut uppgifter på eget initiativ. Om en myndighet vet att en annan myndighet behöver uppgifterna, bör dock uppgifterna lämnas ut om övriga förutsättningar är uppfyllda. Informationsutbytet föreslås ske inom ramen för såväl handläggning av ärenden som myndigheters faktiska handlande.

Förslaget i promemorian har remitterats och bereds i Regeringskansliet. De flesta remissinstanser är positiva till förslaget om införandet av en generell sekretessbrytande bestämmelse, medan några instanser är kritiska, bl.a. Justitiekanslern (JK) och Integritetsskyddsmyndigheten (IMY). IMY avstyrker förslaget mot bakgrund av att det bl.a. saknas en kartläggning av förslagets konkreta konsekvenser för spridningen av personuppgifter. Enligt myndigheten behövs en sådan kartläggning för att det ska vara möjligt att bedöma om det intrång i integriteten som förslaget medför är proportionerligt. IMY anser även att bestämmelsen inte är så tydlig och precis att en enskild kan förutse att de uppgifter som finns registrerade om honom eller henne kan komma att lämnas ut. Enligt JK:s mening medför förslaget en risk att sekretessbelagda uppgifter felaktigt och i alltför stor utsträckning utbyts mellan myndigheter, vilket skulle strida mot dataskyddsförordningens krav på att behandlingen av personuppgifter ska vara nödvändig i förhållande till sina syften och krav på uppgiftsminimering.

Utredaren ska därför

- mot bakgrund av genomförd kartläggning analysera och ta ställning till hur behovet av att utbyta sekretessbelagd information kan tillgodoses,
- särskilt överväga och lämna förslag på en generell bestämmelse som gör det möjligt att lämna uppgifter som omfattas av sekretess till skydd för enskilda till en annan myndighet, såväl på begäran som på eget initiativ,

- göra en översyn av vilka befintliga sekretessbrytande bestämmelser som kan behöva upphävas eller ändras vid införandet av en generell sekretessbrytande bestämmelse,
- göra en analys av hur de förslag som lämnas förhåller sig till intresset av sekretesskydd för enskildas personliga och ekonomiska förhållanden, och
- lämna nödvändiga författningsförslag.

Utökad möjlighet att utbyta offentliga uppgifter

I dag finns en skyldighet för myndigheter att lämna ut offentliga uppgifter om en annan myndighet begär att få del av uppgifterna, så länge det inte hindrar arbetets behöriga gång (6 kap. 5 § OSL). Det är även möjligt för en myndighet att lämna ut offentliga uppgifter om dessa omfattas av bestämmelser om uppgiftsskyldighet. Många gånger kan offentliga uppgifter som en myndighet förfogar över vara av betydelse för en annan myndighet eller för en annan självständig verksamhetsgren inom samma myndighet. En myndighet kan t.ex. i samband med sin handläggning av ärenden få uppgifter som är offentliga och som kan ha direkt betydelse för en annan myndighets eller självständig verksamhetsgrens beslutsfattande. Den kartläggning som har gjorts i Utökat informationsutbyte (Ds 2022:13) visar att det utöver det behov av informationsutbyte som har förutsetts av lagstiftaren och som därför omfattas av en uppgiftsskyldighet kan uppkomma andra situationer där offentliga uppgifter som är av betydelse för en annan myndighets verksamhet kan behöva utbytas.

I promemorian lämnas ett förslag till en ny bestämmelse i OSL som gör det möjligt för en myndighet att i större utsträckning på eget initiativ lämna ut offentliga uppgifter till en annan myndighet. Enligt bestämmelsen får en myndighet till en annan myndighet lämna uppgift som den förfogar över, om inte uppgiften är sekretessbelagd och uppgiften kan antas vara av betydelse för att den mottagande myndigheten ska kunna fullgöra sin verksamhet. Förslaget har remitterats och bereds inom Regeringskansliet. De flesta remissinstanserna är positiva till införandet av bestämmelsen men några remissinstanser, bl.a. JK och IMY, är kritiska av i princip samma skäl som när det gäller den av utredaren föreslagna generella sekretessbrytande regleringen.

Utredaren ska därför

- mot bakgrund av genomförd kartläggning analysera och ta ställning till hur behovet av att utbyta offentliga uppgifter kan tillgodoses,
- särskilt överväga och lämna förslag på en bestämmelse som i större utsträckning gör det möjligt att på eget initiativ lämna ut offentliga uppgifter till en annan myndighet, och
- lämna nödvändiga författningsförslag.

Ett utökat informationsutbyte och den personliga integriteten

Ett utökat informationsutbyte kan innebära ett intrång i den enskildes personliga integritet. Regler om skydd för den personliga integriteten finns bl.a. i regeringsformen (2 kap. 6 § andra stycket), i den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna (artikel 8) och i Europeiska unionens stadga om de grundläggande rättigheterna (artiklarna 7 och 8). Ett allmänt skydd för den personliga integriteten finns även i dataskyddsförordningen.

Enligt 2 kap. 6 § andra stycket regeringsformen är var och en skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Skyddet för den personliga integriteten är inte absolut, utan kan under vissa förutsättningar begränsas med hänsyn till andra motstående intressen. Begränsningen måste dock ske genom lag (2 kap. 20 § första stycket 2 regeringsformen). Denna begränsning får vidare ske endast för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle, och får aldrig gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den, och inte heller sträcka sig så långt att den utgör ett hot mot den fria åsiktsbildningen såsom en av folkstyrelsens grundvalar. Begränsningen får inte göras enbart på grund av politisk, religiös, kulturell eller annan sådan åskådning (2 kap. 21 § regeringsformen).

När ett intrång i den personliga integriteten ska bedömas måste en analys och avvägning göras mellan olika berättigade intressen. Det intrång som sker i den enskildes personliga integritet måste vara befogat och stå i rimlig proportion till de fördelar som intrånget bidrar

med till det motstående intresset. Ett utökat informationsutbyte mellan myndigheter kan leda till ökad kartläggning av enskilda. Omfattande behandling av personuppgifter, däribland känsliga sådana, kan utgöra ett stort intrång i enskildas personliga integritet. Ett sådant intrång kan påverka allmänhetens förtroende för myndigheterna negativt, något som i sin tur kan ha en negativ påverkan på vissa myndigheters förutsättningar att utföra sitt arbete. Myndigheternas tillgång till information kan också vara beroende av att enskilda har förtroende för myndigheterna. Ett utökat informationsutbyte kan därför leda till att enskilda inte vågar lämna korrekta uppgifter till myndigheter eller inte söker stöd och hjälp. Särskilt i fall som rör barn behöver det göras noggranna avvägningar av vad som är ett agerande för barnets bästa i enlighet med FN:s konvention om barnets rättigheter, vilken gäller som svensk lag.

I detta sammanhang måste det dock beaktas att det finns ett starkt intresse på såväl samhällsnivå som individnivå av att fusk, felaktiga utbetalningar, regelöverträdelser och brottslighet förhindras och beivras. Vikten av att myndigheter utbyter information med varandra har dessutom ökat inte minst mot bakgrund av att den organiserade brottsligheten har utvecklats till att bli mer samhällshotande och verka inom allt fler delar av samhället. Ett införande av såväl en bestämmelse som möjliggör ett utökat utbyte av offentliga uppgifter, som en generell sekretessbrytande bestämmelse förutsätter noggranna avvägningar, bl.a. av hur förslaget kan utformas och avgränsas så att enskildas starka integritetsintressen kan beaktas. Vid införande av en sekretessbrytande bestämmelse bör bl.a. överväganden göras av om de aktuella uppgifterna kommer att ha ett sekretesskydd hos den mottagande myndigheten samt, om så inte är fallet, om de bör ha det (jfr prop. 1979/80:2 Del A s. 75–76). Det är viktigt att det även görs en analys av om EU:s dataskyddsförordnings krav på bl.a. rättslig grund för behandling av personuppgifter är uppfyllda. I det ligger att se till att den nationella regleringen dels är proportionerlig i förhållande till det legitima mål som eftersträvas, dels är tydlig, precis och förutsägbar för personer som kommer att omfattas av den.

Utredaren ska därför

- väga behovet av ett förbättrat informationsutbyte mot den enskildes rätt till skydd för sin personliga integritet, och
- ta ställning till hur förslag som lämnas ska utformas och avgränsas för att vara förenliga med bl.a. 2 kap. 6 § andra stycket regeringsformen och EU:s dataskyddsförordning.

Utökade möjligheter att utbyta information förutsätter att myndigheternas registerförfattningar ses över

I svensk rätt finns ett stort antal s.k. registerförfattningar som innehåller mer sektorsspecifika bestämmelser om personuppgiftsbehandlingen vid myndigheter och som kompletterar EU:s dataskyddsförordning, dataskyddslagen och brottsdatalagen. Som exempel kan nämnas studiestödsdatalagen (2009:287), 114 kap. socialförsäkringsbalken och lagen (2001:181) om behandling av uppgifter i Skatteverkets beskattningsverksamhet, med tillhörande förordningar.

Registerförfattningarnas karaktär varierar. Det är dock vanligt att de innehåller bestämmelser om för vilka ändamål personuppgifter får behandlas, personuppgiftsansvar, sökbegränsningar, elektroniskt utlämnande och direktåtkomst (se betänkandet Myndighetsdatalag [SOU 2015:39] s. 98). Ändamålsbestämmelser i registerförfattningar kan sägas anpassa tillämpningen av EU:s dataskyddsförordning och säkerställa en laglig och rättvis behandling av personuppgifter. Ändamålsbestämmelserna ger tillsammans med finalitetsprincipen en ram för vilken personuppgiftsbehandling som är tillåten.

Registerförfattningarna reglerar även formen för utlämnande av uppgifter. Bestämmelser om ett elektroniskt utlämnande av uppgifter kan se ut på olika sätt. De kan utformas som regler om direktåtkomst, vilket innebär att en mottagare har direkt tillgång till någon annans register eller databas och därigenom på egen hand kan ta del av information (se HFD 2015 ref. 61). Det finns även bestämmelser om annat elektroniskt utlämnande, ibland kallat utlämnande på medium för automatiserad behandling, som inbegriper utlämnande av uppgifter per e-post, på usb-minne eller genom elektronisk direktöverföring från ett datorsystem till ett annat. I EU:s dataskyddsförordning finns inte några särskilda bestämmelser som reglerar formerna för ett utlämnande, utan det krävs, i likhet med vad som gäller för all behandling av per-

sonuppgifter, att behandlingen uppfyller bestämmelserna i förordningen. Den personuppgiftsansvarige är dock skyldig att säkerställa en lämplig säkerhetsnivå i förhållande till de risker som en digital hantering kan medföra (jfr artikel 5.1 f och artikel 32 i EU:s dataskyddsförordning).

Den analys som har gjorts i promemorian Utökat informationsutbyte (Ds 2022:13) visar att det i myndigheternas registerförfattningar kan finnas vissa begränsningar av möjligheten att dels behandla personuppgifter för att kunna lämna ut och ta emot dem, dels lämna ut dem elektroniskt på annat sätt än genom direktåtkomst. För att syftet med förslag om förbättrat informationsutbyte ska kunna uppnås kan vissa registerförfattningar behöva ändras.

Utredaren ska därför

- göra en översyn, i den utsträckning det behövs, av myndigheternas registerförfattningar, för att möjliggöra att de förslag som lämnas tjänar sitt syfte och kan tillämpas på ett ändamålsenligt sätt, och
- lämna nödvändiga författningsförslag.

Konsekvensbeskrivningar

Förslag på författningsändringar ska föregås av en integritetsanalys. Utredaren ska redovisa vilka konsekvenser förslagen innebär för spridningen av personuppgifter inom och mellan myndigheter. Utredaren ska vidare redovisa de offentligfinansiella konsekvenserna av de förslag som läggs fram. Om förslagen kan förväntas leda till kostnadsökningar för de allmänna, ska utredaren föreslå hur dessa ska finansieras. Kostnader för specifika myndigheter ska redovisas separat.

Kontakter och redovisning av uppdraget

Utredaren ska hålla sig informerad om och beakta relevant arbete som pågår inom Regeringskansliet och utredningsväsendet. Under genomförandet av uppdraget ska utredaren, i den utsträckning som bedöms lämplig, också ha en dialog med och inhämta upplysningar från de aktörer som berörs av aktuella frågor.

Uppdraget ska redovisas senast den 28 februari 2025. Senast den 30 augusti 2024 ska utredaren lämna en delredovisning av uppdraget

att kartlägga myndigheternas behov av förbättrade möjligheter till informationsutbyte, att analysera och ta ställning till hur behovet av att utbyta sekretessbelagd information kan tillgodoses samt att särskilt överväga och lämna förslag på en generell möjlighet att lämna uppgifter som omfattas av sekretess till skydd för enskilda till en annan myndighet, såväl på begäran som på eget initiativ.

(Justitiedepartementet)

Kommittédirektiv 2024:87

Tilläggsdirektiv till Utredningen om förbättrade möjligheter till informationsutbyte mellan myndigheter (Ju 2023:22)

Beslut vid regeringssammanträde den 19 september 2024

Förlängd tid för uppdraget

Regeringen beslutade den 19 oktober 2023 kommittédirektiven Förbättrade möjligheter till informationsutbyte mellan myndigheter (dir. 2023:146). Uppdraget skulle enligt direktiven redovisas senast den 28 februari 2025.

Utredningstiden förlängs. Uppdraget ska i stället redovisas senast den 28 april 2025.

(Justitiedepartementet)

Statens offentliga utredningar 2025

Kronologisk förteckning

1. Skärpta krav för svenskt medborgarskap. Ju.
2. Några frågor om grundläggande fri- och rättigheter. Ju.
3. Skatteincitament för forskning och utveckling. En översyn av FoU-avdraget och expertskattereglerna. Fi.
4. Moderna och enklare skatteregler för arbetslivet. Fi.
5. Avgift för områdessamverkan – och andra åtgärder för trygghet i byggd miljö. LI.
6. Plikten kallar! En modern personalförsörjning av det civila försvaret. Fö.
7. Ny kärnkraft i Sverige – effektivare tillståndsprövning och ändamålsenliga avgifter. KN.
8. Bättre förutsättningar för trygghet och studiero i skolan. U.
9. På språklig grund. U.
10. En förändrad abortlag – för en god, säker och tillgänglig abortvård. S.
11. Straffbarhetsåldern. Ju.
12. AI-kommissionens Färdplan för Sverige. Fi.
13. En effektivare organisering av mindre myndigheter – analys och förslag. Fi.
14. En skärpt miljöstraffrätt och ett effektivt sanktionssystem. KN.
15. Stärkta drivkrafter och möjligheter för biståndsmottagare. Volym 1 och 2. S.
16. Ett nytt regelverk för uppsikt och förvar. Ju.
17. Anpassning av svensk rätt till EU:s avskogningsförordning. LI.
18. Ett likvärdigt betygssystem. Volym 1 och 2. U.
19. Kunskap för alla – nya läroplaner med fokus på undervisning och lärande. U.
20. Kommunal anslutning till Utbetalningsmyndighetens verksamhet. Fi.
21. Miljömålsberedningens förslag om en strategi för hur Sverige ska leva upp till EU:s åtaganden inom biologisk mångfald respektive nettoupptag av växthusgaser från markanvändningssektorn (LULUCF). KN.
22. Förbättrad konkurrens i offentlig och privat verksamhet. KN.
23. Ersättningsregler med brottsoffret i fokus. Ju.
24. Publiken i fokus – reformer för ett starkare filmland. Ku.
25. Arbetslivskriminalitet – upplägg, verktyg och åtgärder, fortsatt arbete. A.
26. Tid för undervisningsuppdraget – åtgärder för god undervisning och läraryrkenas attraktivitet. U.
27. En socionomutbildning i tiden. U.
28. Frihet från våld, förtryck och utnyttjande. En jämställdhetspolitisk strategi mot våld och en stärkt styrning av centrala myndigheter. A.
29. Ökad kvalitet hos Samhall och fler vägar till skyddat arbete. A.
30. Enklare mervärdesskatteregler vid försäljning av begagnade varor och donation av livsmedel. Fi.
31. Utmönstring av permanent uppehållstillstånd och vissa anpassningar till miniminivån enligt EU:s migrations- och asylpakt. Ju.
32. Vissa förändringar av jaktlagstiftningen. LI.
33. Skärpta och tydligare krav på vandel för uppehållstillstånd. Ju.
34. Ett modernare konsumentskydd vid distansavtal. Ju.
35. Etableringsboendelagen – ett nytt system för bosättning för vissa nyanlända. A.

36. Skydd för biologisk mångfald i havsområden utanför nationell jurisdiktion. UD.
37. Skärpta villkor för friskolesektorn. U.
38. Att omhänderta barn och unga. S.
39. Digital teknik på lika villkor. En reglering för socialtjänsten och verksamhet enligt LSS. S.
40. Säkrare tivoli. Ju.
41. Pensionsnivåer och pensionsavgiften – analyser på hundra års sikt. S.
42. Säkerhetsskyddslagen – ytterligare kompletteringar. Ju.
43. Säkerställ tillgången till läkemedel – förordnande och utlämnande i bristsituationer. S.
44. Förbättrat stöd i skolan. U.
45. Ökat informationsutbyte mellan myndigheter – några anslutande frågor. Ju.

Statens offentliga utredningar 2025

Systematisk förteckning

Anpassning av svensk rätt till EU:s avskogningsförordning. [17]

Vissa förändringar av jaktlagstiftningen. [32]

Socialdepartementet

En förändrad abortlag – för en god, säker och tillgänglig abortvård. [10]

Stärkta drivkrafter och möjligheter för biståndsmottagare Volym 1 och 2. [15]

Att omhänderta barn och unga. [38]

Digital teknik på lika villkor. En reglering för socialtjänsten och verksamhet enligt LSS. [39]

Pensionsnivåer och pensionsavgiften – analyser på hundra års sikt. [41

Säkerställ tillgången till läkemedel – förordnande och utlämnande i bristsituationer. [43]

Utbildningsdepartementet

Bättre förutsättningar för trygghet och studiero i skolan. [8]

På språklig grund. [9]

Ett likvärdigt betygssystem Volym 1 och 2. [18]

Kunskap för alla – nya läroplaner med fokus på undervisning och lärande. [19]

Tid för undervisningsuppdraget – åtgärder för god undervisning och läraryrkenas attraktivitet. [26]

En socionomutbildning i tiden [27]

Skärpta villkor för friskolesektorn. [37]

Förbättrat stöd i skolan [44]

Utrikesdepartementet

Skydd för biologisk mångfald i havsområden utanför nationell jurisdiktion. [36]