Vägledning

Utkontraktering – sekretess och dataskydd

ES2023-06

Juli 2023

Innehåll

1. Inledning

Utkontraktering (eller outsourcing), dvs. att låta externa tjänsteleverantörer utföra funktioner som annars skulle skötas i egen regi, är en viktig del i myndigheternas strategi för att utveckla den digitala förvaltningen. Utkontraktering som utförs av annan myndighet benämns ibland *samordning*. I denna vägledning används begreppet utkontraktering både för utkontraktering som utförs av enskild leverantör och utkontraktering som utförs av en annan myndighet.

Utkontraktering kan avse olika typer av it-tjänster, t.ex. infrastrukturtjänster, molntjänster,[1] systemleveranstjänster, it-konsulttjänster, it-projekt och liknande. Många myndigheter har utkontrakterat drift och förvaltning av informationssystem, tekniskt stöd såsom it-support samt teknisk bearbetning såsom skanning, tryck och postbefordran av dokument och liknande funktioner.

Komplexiteten i den kravställning som behöver göras av en upphandlande myndighet vid utkontraktering har med åren ökat markant, bl.a. genom tillkomsten av EU:s dataskyddsförordning (dataskyddsförordningen),[2] NIS2-direktivet, U.S CLOUD Act, sektion 702 av Foreign Intelligence Surveillance Act (FISA 702) och liknande regelverk i andra länders lagstiftning. Därtill har ändringar skett av säkerhetskyddslagstiftningen och lagen (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter (tystnadspliktslagen) har tillkommit.

1.1 Syfte och avgränsning

Denna vägledning[3] syftar till att ge juridiskt stöd för de överväganden rörande sekretess och dataskydd som en myndighet måste göra inför en planerad utkontraktering. I vägledningen ges också stöd avseende utkontraktering av hantering av allmänna handlingar.

Andra överväganden som behöver göras inför en utkontraktering beskrivs endast kortfattat i avsnitt 2. Det ges således inte någon fullständig genomgång av alla överväganden som ska göras och checklistan är begränsad i första hand till de rättsliga förutsättningarna för sekretess och dataskydd. Vägledningen avser främst utkontraktering av it-tjänster, men kan användas även för andra tjänster.

[1] Molntjänster kan delas upp i tre olika typer beroende på vilka externa it-resurser som tjänsten ger tillgång till; Infrastructure as a Service (IaaS), Platform as a Service (PaaS) och Software as a Service (SaaS).
[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] Vägledningen ersätter eSams tidigare vägledning Outsourcing 2.0 En vägledning om sekretess och dataskydd.

1.2 Målgrupp

Denna vägledning vänder sig i första hand till jurister och andra som i sitt arbete inom statliga myndigheter deltar i utformningen av en utkontraktering eller har att bedöma om en planerad utkontraktering är författningsenlig.

1.3 Medverkande

Arbetet med att ta fram denna vägledning har genomförts av en särskild arbetsgrupp bestående av Gunnar Svensson (Skatteverket), Jens Västberg (Riksarkivet), Tina Hård (E-hälsomyndigheten), Anna Sjögren (E-hälsomyndigheten), Elin Hallström (Skatteverket), Henrik Karlsson (Migrationsverket), Pontus Schenkel (Transportstyrelsen), Sofie Wildiér (Kronofogdemyndigheten), Maria Sertcanli (Säkerhetspolisen) och Linda Lindström. Kvalitetssäkring har skett i eSams rättsliga expertgrupp, expertgruppen i säkerhet samt koordineringsgruppen för arkitektur. Beredning har skett via eSams samordningsgrupp och rättschefsforum och därefter har beslut fattats av eSams styrgrupp.

2. Inför utkontraktering

Statliga myndigheter har relativt stort utrymme att själva avgöra på vilket sätt deras respektive uppdrag ska fullgöras,[4] dvs. hur och av vem arbetsuppgifterna ska utföras. Utkontraktering kan därför i princip aktualiseras beträffande flertalet av de uppgifter som en myndighet ansvarar för. Ett överlämnande av en arbetsuppgift som innefattar myndighetsutövning måste emellertid ha stöd i lag.[5]

Inför förändring eller utveckling av en myndighets verksamhet, där utkontraktering övervägs, behöver myndigheten normalt gå igenom ett antal steg för att genomföra förändringen genom utkontraktering. I detta avsnitt beskrivs kortfattat vilka överväganden och steg som en myndighet behöver ta. eSam har en molngrupp som kan ge stöd i medlemmarnas arbete med utkontraktering och molntjänster.

2.1 Identifiera behov och välj it-tjänster

Inför en förändring eller utveckling av verksamheten måste en analys göras av myndighetens behov och vilken information som ska hanteras. Beroende på vilka behov myndigheten har kan förändringen eller utvecklingen genomföras på olika sätt genom olika it-tjänster.

Om myndigheten överväger att införskaffa en viss programvara till ett administrativt system och konsulttjänster behövs för utveckling och anpassning, löpande support eller underhålls- och driftstjänster, kan behovet lösas genom att programvarulicenser upphandlas eller avropas tillsammans med de olika tjänsterna (konsult-, support-, underhålls- och drifttjänster). En sådan förändring kan emellertid också genomföras så att myndigheten avropar eller upphandlar en systemleverans som tjänst, där programvarulicensen paketerats tillsammans med övriga tjänster som tillhandahålls som en funktion under viss bestämd avtalstid. Många systemprogramvaror tillhandahålls numera dessutom i en mycket standardiserad form som molntjänster, där myndigheten får tillgång till tjänstens standardfunktionalitet via ett webbgränssnitt och där myndighetens data lagras i leverantörens datacenter tillsammans med andra kunders data (logiskt avskiljt).

[4] 12 kap. 2-3 §§ Regeringsformen (RF).
[5] 12 kap. 4 § RF.

Valet av it-tjänst behöver anpassas efter de identifierade behoven.

2.2 Informationsklassning

Inför utkontraktering behöver en informationsklassning göras, för att kartlägga vilka informationsmängder som kommer att hanteras. I informationsklassningen värderas bl.a. vilken betydelse och vilket värde informationen har för verksamheten (informationens skyddsvärde). I avsnitt 7 redogörs för regler om informationssäkerhet som behöver beaktas vid en utkontraktering, bl.a. bestämmelser i säkerhetsskyddslagen (2018:585). En heltäckande och väl genomarbetad informationsklassning underlättar det fortsatta arbetet med utkontraktering.

2.3 Rättsliga förutsättningar

När uppgifter ska utkontrakteras krävs att myndigheten gör olika juridiska överväganden. Den som ska göra en prövning av lagligheten och lämpligheten av utkontraktering av it-tjänster har att förhålla sig till ett omfattande regelverk då relevanta bestämmelser finns utspridda i ett flertal lagar. För att veta vilka regelverk som ska tillämpas i det specifika fallet och för att kunna göra nödvändiga bedömningar måste det klargöras vad det är för uppgifter som ska hanteras, vilka som kommer att hantera uppgifterna, hur behandling kommer ske samt var informationen kommer behandlas och lagras.

Eftersom de olika it-tjänsterna innebär olika typer av tillgång till myndighetens information, it-system och verksamhet i övrigt behöver myndigheten förstå de olika it-tjänsternas uppbyggnad och innehåll och analysera vilken tillgång som respektive it-tjänst kräver. Myndigheten måste genomföra en rättslig analys för att kontrollera att informationshanteringen följer gällande regelverk och för att identifiera vilka krav som myndigheten behöver ställa för att säkerställa att tillgången är rättsenlig. Det behöver bl.a. göras bedömningar utifrån dataskyddsreglering, sekretessreglering, regler om allmänna handlingar samt informationsäkerhetsregler. Vald it-lösning kan behöva omvärderas eller anpassas för att utformningen ska bli författningsenlig. Överväganden kring sekretess, dataskydd och allmänna handlingar utvecklas i efterföljande avsnitt 4-6. Informationsäkerhet behandlas kortfattat i avsnitt 7.

2.4 Risk- och säkerhetsbedömning

Utifrån den rättsliga bedömningen och informationsklassningen behöver myndigheten också analysera de risker som kan uppkomma i samband med tilltänkt it-tjänst och se på säkerhetsåtgärder kopplat till dessa risker. Det kan exempelvis föreligga omständigheter som försvårar myndighetens möjligheter att säkerställa ett tillfredsställande skydd, såsom

att andra länders rättsordningar kan bli tillämpliga eller att tjänsteleverantören använder sig av många olika underleverantörer.

I anknytning till it-tjänster där det kan uppkomma ansamlingar av data, bör risker med aggregering[6] beaktas, liksom risker med telemetri.[7] Risker utifrån förutsättningar att kontrollera myndighetens egna digitala data och hur den används (digital suveränitet) behöver också värderas. Förutsättningarna för kontinuitetsplanering behöver beaktas.

2.5 Bestäm hur inköp ska genomföras

Efter att det har säkerställts att rätt it-tjänster valts och att uppgifter kan tillgängliggöras för leverantören på ett rättsenligt, säkert och lämpligt sätt behöver förutsättningarna för en upphandling eller ett avrop av valda it-tjänster genomlysas. I vissa fall kan myndigheten köpa in it-tjänster genom befintliga ramavtal. I så fall måste myndigheten granska bakomliggande ramavtal för att säkerställa att den upphandlade it-tjänsten uppfyller de specifika krav som myndigheten har. När möjligheten att avropa it-tjänster inte finns får myndigheten istället överväga hur en upphandling bäst kan genomföras. Beroende på myndighetens verksamhetsområde gäller olika regelverk för hur upphandlingen av it-tjänster ska genomföras.[8] Där finns regler om när myndigheten måste genomföra en upphandling och hur en sådan ska genomföras.

Upphandlingslagstiftningen innehåller inte några särskilda regler för it-tjänster. It-tjänster omfattas istället av den allmänna definition av tjänster i 1 kap. 21 § i lagen om offentlig upphandling (LOU).[9] En it-tjänst behöver med andra ord upphandlas på samma sätt som andra typer av tjänster, så som inköp av administrativa tjänster eller städtjänster. Hur upphandlingen ska genomföras beror på värdet av det som ska upphandlas och andra bakomliggande omständigheter. Rör det sig om it-tjänster av mindre värde kan myndigheten under vissa omständigheter genomföra en s.k. direktupphandling, där myndigheten kan vända sig direkt till önskad leverantör för inköp av tjänsterna. I de flesta fall är dock inköp av it-tjänster kostsamma. Därför är myndigheten normalt skyldig att använda andra förfaranden.

Vid utformningen av ett upphandlingsunderlag, som leverantörer baserar sitt anbud på, måste myndigheten säkerställa att de krav som myndigheten har på it-tjänsten blir

[6] Med aggregering i detta sammanhang avser sammanförande av datamängder, jfr annan betydelse i statistiska sammanhang där aggregera innebär att man lägger ihop flera observationer för att man inte ska kunna identifiera enskilda svar (anonymisering).
[7] Se avsnitt 3.7 i rapporten 2022 Coordinated Enforcement Action, Use of cloud-based services by the public sector, Adopted on 17 January 2023. Telemetridata, eller diagnostisk information, definieras där som data som rör användningen av infrastrukturer eller tjänster, till exempel resursidentifierare, taggar, informations- och behörighetsroller, användarstatistik om olika typer av användare.
[8] De regelverk för upphandling som kan aktualiseras är lag (2016:1145) om offentlig upphandling (LOU), lag (2016:1146) om upphandling inom försörjningssektorerna (LUF), lag (2016:1147) om upphandling av koncessioner (LUK) och lag (2011:1029) om upphandling på försvars- och säkerhetsområdet (LUFS). En myndighet som generellt omfattas av LOU kan tillämpa LUFS om upphandlingsföremålet är av sådant slag att det omfattas av något av de tillämpningsområden som gäller för den lagen.
[9] I vissa fall kan det vara en gränsdragningsfråga om det är en tjänst eller en vara.

specificerade. Möjligheten att i efterhand ställa ytterligare krav på exempelvis säkerhet är ytterst begränsad i upphandlingslagstiftningen.

2.6 Säkerställ nödvändiga avtalsregleringar

Oberoende av om myndigheten genomför en upphandling eller avropar från ett befintligt ramavtal måste avtalsvillkoren granskas och utformas så att leverantören blir avtalsrättsligt förpliktad att tillhandahålla it-tjänsten med överenskommet innehåll.

Avtal om utkontraktering av it-tjänster är ofta omfattande avtal med en lång rad regleringar. En del av regleringarna är allmänna kontraktsrättsliga regleringar som brukar förekomma i affärsjuridiska avtal i allmänhet t.ex. avseende avtalstid, uppsägningsregler, force majeure, lagval och forum för tvist. Andra regler är mer specifika för it-avtal såsom upplåtelse av programrättigheter, intrångsbestämmelser och tillgång till data. Ett flertal specifika avtalsregleringar behöver normalt finnas med i ett it-avtal för att på ett ändamålsenligt sätt reglera parternas mellanhavanden. Avtalsregleringar som särskilt kan behöva uppmärksammas vid utkontraktering och som brukar vara relevanta för flera olika it-tjänster är bl.a. tjänstebeskrivning, avtalssekretess, personuppgiftsbiträdesavtal, säkerhetsåtgärder, ansvarsfrågor, förändring av ägarförhållanden, samverkan och revision, uppsägning av avtal samt avtalets upphörande. Det behöver undersökas hur dessa regleringar förhåller sig till varandra, särskilt i omfattande avtal.

För att ge stöd till myndigheterna i it-avtalsarbetet har eSam tagit fram en vägledning om it-tjänsternas avtal. Vägledningen innehåller en beskrivning av de vanligaste it-avtalstyperna, dess nyckelregleringar och vanliga fallgropar. eSam har även tagit fram it-avtalsvillkor anpassade att användas vid upphandling och kontraktering av olika slags it-tjänster inom offentlig sektor. Avtalsvillkoren är utformade för att användas som bilaga till ett specifikt huvudavtal men kan också användas av myndigheten som en checklista eller stöd för att säkerställa att nödvändiga avtalsregleringar finns med i avtalet.[10]

Om tjänsteleverantören är en myndighet kan myndigheterna i vissa fall ingå en överenskommelse som reglerar hur tjänsten ska genomföras. Överenskommelsen bör innehålla en stor del av de regleringar som normalt återfinns i it-avtal av den här typen av tjänster.[11]

[10] Vägledningen, huvudavtalsmallar och it-avtalsvillkoren finns att hitta på esamverka.se. I dagsläget finns huvudavtalsmallar och allmänna villkor för it-drift, it-konsulttjänster, it-support, agila it-projekt och it-projekt. Till respektive avtalsvillkor finns kommentarer som är tänkta att underlätta användningen av avtalsvillkoret genom att förklara vissa regleringar och tydliggöra hur avtalsvillkoret är tänkt att användas.
[11] Statliga myndigheter kan inte ingå avtal med varandra, affärsförhållanden inom staten kan endast regleras genom överenskommelser, HFD 2021 ref. 35.

3. Begreppet teknisk bearbetning eller teknisk lagring

Ett begrepp som är av betydelse för flera av de rättsliga bedömningarna vid en utkontraktering är *teknisk bearbetning eller teknisk lagring*. I detta avsnitt görs därför en genomgång av begreppets innebörd och därefter redovisas i kommande avsnitt 4-5 de rättsliga bedömningar som behöver göras utifrån begreppet vid allmänna handlingar och sekretess.

Teknisk bearbetning eller teknisk lagring finns som begrepp i tryckfrihetsförordningen (TF), i offentlighets- och sekretesslagen (2009:400) (OSL) och i tystnadspliktslagen. Begreppet är av betydelse för bedömningen av vad som är en allmän handling (TF), när sekretessen för en sekretessbelagd uppgift kan brytas (OSL) och vilket författningsreglerat skydd som uppgiften får hos en leverantör av en tjänst (OSL och tystnadspliktslagen).[12]

En utkontrakterad tjänst kan helt eller delvis bestå av moment som kan definieras såsom teknisk bearbetning eller teknisk lagring. Vid utkontraktering av tjänster som innefattar informationshantering behöver därför ofta bedömas om dessa tjänster kan inrymmas i begreppen teknisk bearbetning eller teknisk lagring. Det kan vara så att inte samtliga av de tjänster som omfattas av utkontrakteringen ryms inom teknisk bearbetning eller teknisk lagring. Det är därför viktigt att definiera var gränsen går mellan tjänster eller delar av tjänster som är teknisk bearbetning eller teknisk lagring respektive vilka tjänster eller delar av tjänster som inte är det.

I det följande görs en genomgång av de olika regleringarna och praxis, av rekvisiten ”endast” och “för uppdragsgivarens räkning” samt bedömning av begreppets innebörd i samband med myndigheters utkontraktering av olika typer av it-tjänster. Denna genomgång syftar till att ge vägledning i de bedömningar som behöver göras i följande avsnitt om allmänna handlingar och sekretess (se avsnitt 4-5).

3.1 Förarbeten och praxis

3.1.1 Bakgrund till begreppets tillkomst

Teknikutvecklingen under 1960- och 70-talen, samt den uppkomna marknaden för nya aktörer innebar att myndigheter i allt större utsträckning utkontrakterade delar av sin informationshantering till externa aktörer, såväl myndigheter som enskilda. Frågor med

[12] 2 kap. 9 § 3 st. och 13 § 1 st. TF, 10 kap. 2 a §, 11 kap. 4 a § och i 40 kap. 5 § OSL och i 4 § tystnadspliktslagen.

bäring på bl.a. inkommande-, expeditions- och förvaringsbegreppen behövde då lösas. Detta ledde fram till ett behov av att se över tryckfrihetsförordningens reglering om allmänna handlingar i relation till sådana informationsmängder som behandlades i en digital miljö.[13]

I 2 kap. 9 § 3 st. och 2 kap. 13 § 1 st. TF framgår några av resultaten av de reformer som genomfördes på mitten av 70-talet. Regleringen möjliggör att en myndighet kan låta en extern aktör, såväl annan myndighet som enskild, utföra en del av myndighetens informationshantering utan att överföringarna av information mellan uppdragsgivande myndighet och uppdragstagande aktör leder till att nya allmänna handlingar uppkommer. Den grundläggande förutsättningen för detta är att den externa aktörens uppdrag med handlingen är endast teknisk bearbetning eller teknisk lagring för den myndighets räkning som tillhandahållit handlingen. I förarbetena[14] anges att när en myndighet endast tar teknisk befattning med en upptagning så kräver inte offentlighetsprincipen att allmänheten ska ha tillgång till upptagningen hos den myndigheten. Det är fullt tillräckligt att upptagningen finns tillgänglig enligt offentlighetsregleringen hos den handläggande myndigheten.[15] Den information som kan hämtas från upptagningen kan inte sägas ingå i den behandlande myndighetens informationstillgångar.[16] Den tekniska befattning som kunde accepteras och som innebar att vissa undantag från tryckfrihetsförordningens regler om allmänna handlingar gjordes tillämpliga, fick i lagtexten benämningen teknisk bearbetning eller teknisk lagring.

I förarbetena[17] till OSL och tystnadspliktslagen[18] klargörs att innebörden av begreppet teknisk bearbetning eller teknisk lagring är densamma i TF, OSL och tystnadspliktslagen.

Regleringen i 2 kap. 9 § 3 st. och 13 § 1 st. TF är teknikneutral, vilket framgår av att regleringen innehåller uttrycket handling.[19] Teknikneutraliteten lyfts också fram i förarbetena till både 10 kap. 2 a § OSL och 4 § tystnadspliktslagen[20] och verkar då närmast avse tillhandahållande via molntjänster eller "on prem"-tjänster.

---

[13] Beskrevs då som ADB-behandlingar eller andra tekniska upptagningar, se Kungl. Maj:ts proposition med förslag till ändringar i tryckfrihetsförordningen, m. m.; given Stockholms slott den 16 februari 1973, (prop. 1973:33), s 2.
[14] Reformen genomfördes i dåvarande i 2 kap. 9 § 3 st. och 2 kap. 10 § 1 st. TF, se prop. 1975/76:160 om nya grundlagsbestämmelser angående allmänna handlingars offentlighet.
[15] Prop. 1975/76:160 s. 87 om nya grundlagsbestämmelser angående allmänna handlingars offentlighet.
[16] Prop. 1975/76:160. s. 87 om nya grundlagsbestämmelser angående allmänna handlingars offentlighet. I propositionen görs uttalandet i samband med att föredraganden ger uttryck för att motsvarande ordning som gäller när andra myndigheter tar teknisk befattning med upptagningar bör gälla också i den situation då myndigheter utför teknisk bearbetning för enskildas räkning.
[17] Prop. 2016/17:198, Utökat sekretesskydd i verksamhet för teknisk bearbetning och lagring, s 28-29. och prop. 2022/23:97, Sekretessgenombrott vid utlämnande för teknisk bearbetning eller teknisk lagring av uppgifter, s. 16.
[18] Prop. 2019/20:201, Tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter, s. 22.
[19] Jmf. definitionen av handling i 2 kap. 3 § TF.
[20] Se prop. 2022/23:97 Sekretessgenombrott vid utlämnande för teknisk bearbetning eller teknisk lagring, s. 11 respektive 2019/20:201 Tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter, s. 16.

3.1.2 Åtgärder som enligt förarbeten omfattas av begreppet teknisk bearbetning eller teknisk lagring

I förarbetena till 2 kap. 9 § 3 st. och 13 § 1 st. TF redovisas ett antal exempel på sådana behandlingar som enligt lagstiftaren borde anses utgöra teknisk bearbetning eller teknisk lagring. Bland annat överföring av information från ett medium till ett annat, såsom överföring av ljudupptagning på magnetband till grammofonskiva, överföring från pappershandling till magnetband eller framkallning av fotografi. Ett annat exempel på denna typ av bearbetning är mångfaldigande av information såsom tryckning och kopiering. Även tekniska procedurer som redigering av en myndighets ljudupptagning på magnetband nämns. Det beskrivs dock inte närmare vad redigeringen ska bestå i. I fråga om lagring nämns sådana former av lagring som kräver särskilda tekniska anordningar såsom t.ex. lagring av information i skrivminne eller på magnetband.[21] Exemplen var relevanta vid tidpunkten för förarbetena vid mitten av 1970-talet, men är fortfarande relevanta för att bedöma den karaktär på tjänster som kan anses utgöra teknisk bearbetning eller teknisk lagring.

I förarbetena till tystnadspliktslagen[22] anges grundläggande it-driftstjänster och it-baserade funktioner som en generell beskrivning av tjänster som kan komma ifråga som teknisk bearbetning eller teknisk lagring. Som närmare förklaring anges att det t.ex. kan vara en teknisk infrastruktur eller en teknisk plattform för it-drift. Det kan också vara fråga om att tillhandahålla en it-baserad funktion, t.ex. en applikation eller en standardiserad eller anpassad digital tjänst.[23] Den typ av tjänster som kan kvalificera för begreppet är myndigheters grundläggande behov av it-driftstjänster och andra it-baserade funktioner.[24]

I förarbetena[25] till den sekretessbrytande bestämmelsen i 10 kap. 2 a § OSL anges diarie- och ärendehanteringssystem, system för kontorsstöd vilket kan inkludera e-post, kalender och dokumenthanteringsstöd som exempel på it-drift som kan bli föremål för utkontraktering. Det anges inte specifikt att de angivna exemplen är att betrakta som exempel på teknisk bearbetning eller teknisk lagring. Avsikten med att ange dessa exempel får dock antas ha varit att peka på möjliga tjänster för teknisk bearbetning eller teknisk lagring. Härutöver beskrivs endast översiktligt att de grundläggande it-driftstjänster som myndigheter har behov av kan utgöra teknisk bearbetning eller teknisk lagring.

[21] Prop. 1975/76:160 om nya grundlagsbestämmelser angående allmänna handlingars offentlighet, s. 137.
[22] Prop. 2019/20:201 Tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter.
[23] Prop. 2019/20:201 Tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter, s. 6 och 22.
[24] Prop. 2019/20:201 Tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter, s. 16.
[25] Prop. 2022/23:97 Sekretessgenombrott vid utlämnande för teknisk bearbetning eller teknisk lagring, s. 7.

I förarbetena till både tystnadspliktslagen och till 10 kap. 2 a § OSL lämnas utförliga beskrivningar av åtgärder som en tjänsteleverantör kan vidta i anslutning till de tjänster som denne tillhandahåller. Här nämns bl.a. att leverantören kan, avseende en utkontrakterad tjänst som avser teknisk bearbetning eller teknisk lagring, införa, förvalta, utveckla och avveckla en it-driftstjänst. Under dessa olika faser kan en mängd olika åtgärder vidtas för att upprätthålla tillgänglighet, funktionalitet och prestanda i den utkontrakterade tjänsten. Åtgärderna kan bestå i förändringar och tillägg i en befintlig tjänsts funktionalitet, etablering av en tilläggstjänst, integration med andra tjänster, konfiguration, test och utveckling samt tillhandahållande av supporttjänster. Säkerhetstester och andra säkerhetshöjande åtgärder som uppgradering, uppdatering, säkerhetskopiering, kryptering, anonymisering, pseudonymisering och incidenthantering kan också vara åtgärder som omfattas av ett uppdrag om teknisk bearbetning eller teknisk lagring. Vid avveckling av en tjänst kan myndighetens uppgifter behöva migreras eller exporteras tillbaka till myndigheten eller till en annan tjänsteleverantör.[26] Beskrivningen avser i det närmast olika typer av förvaltningsåtgärder som tjänsteleverantören utför för att förvalta och utveckla den tjänst som tillhandahålls.

I både förarbetena till OSL och tystnadspliktslagen påpekas att under samtliga moment av teknisk bearbetning eller teknisk lagring kan det förekomma att personal hos tjänsteleverantören tar del av de uppgifter som hanteras för den uppdragsgivande myndighetens räkning. Att tjänsteleverantören behöver ta del av uppgifter kan vara nödvändigt för att leverantören ska kunna utföra sina arbetsuppgifter såsom led i den tekniska bearbetningen eller lagringen. Normalt sett bör det vara fråga om drifts- och säkerhetsrelaterad information, t.ex. uppgifter om användarkonton, loggar, krypteringsnycklar, lösenord och säkerhetsinställningar. Men det kan också röra sig om uppgifter i läsbar form.[27]

Vilka tjänster eller åtgärder som en tjänsteleverantör kan utföra inom ramen för begreppet teknisk bearbetning eller teknisk lagring är inte en gång för alla bestämt. I förarbetena till 10 kap. 2 a § OSL och till 4 § tystnadspliktslagen påtalas det att vilka slags åtgärder som kan omfattas av begreppet teknisk bearbetning eller teknisk lagring kan komma att förändras över tid med anledning av den tekniska utvecklingen.

[26] Prop. 2019/20:201 Tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter, s. 23 och prop. 2022/23:97 Sekretessgenombrott vid utlämnande för teknisk bearbetning eller teknisk lagring, s. 17.
[27] Prop. 2019/20:201 Tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter, s. 22 f och prop. 2022/23:97 Sekretessgenombrott vid utlämnande för teknisk bearbetning eller teknisk lagring, s. 17.

3.1.3 Praxis kring begreppet teknisk bearbetning eller teknisk lagring

Det finns viss rättspraxis i fråga om tillämpningen av 2 kap. 13 § 1 st. TF, som gäller när en myndighet är den part som tillhandahåller en tjänst eller funktion för teknisk bearbetning eller tekniskt lagring av uppgifter för någon annans räkning, se RÅ 1994 ref. 64, HFD 2011 ref. 52 och HFD 2018 ref. 48.

I RÅ 1994 ref. 64 ansågs Riksrevisionsverkets (RRV) tillhandahållande av systemet Cosmos utgöra sådan teknisk bearbetning eller teknisk lagring som avsågs i 2 kap. 10 § TF (motsvarande reglering som nuvarande 2 kap. 13 § TF). RRV disponerade inte över myndigheternas redovisningsdata och myndighetens tillhandahållna centrala lagring av data var en teknisk lösning.

I HFD 2011 ref. 52 och 2018 ref. 48 ansåg Högsta förvaltningsdomstolen att den bearbetning som Rikspolisstyrelsen respektive Borås kommun utförde för sina respektive uppdragsgivare inte kunde anses utgöra enbart teknisk bearbetning eller teknisk lagring i den mening som avses i 2 kap. 10 § TF.[28] I båda avgörandena fanns uppgifterna i myndigheternas tekniska system och användes där, vid sidan av för uppdragsgivarens räkning, också för statistikframställning och, ifråga om Rikspolisstyrelsen, för att rapportera till Arbetsmiljöverket.

I HFD 2018 ref. 48 angav domstolen att det av den myndighet som tillhandahåller en tjänst endast för teknisk bearbetning eller teknisk lagring också bör krävas att myndigheten såväl tekniskt som administrativt har begränsat den egna personalens tillgång till uppgifterna så att dessa inte är tillgängliga i läsbart skick. Myndighetens personal ska enligt domstolen enbart kunna ta del av den drifts- och säkerhetsrelaterade informationen.

I prop. 2019/20:201 s. 7 uttalas att det är oklart i vilken utsträckning de avgöranden som nämns ovan, som avser myndigheter, kan tjäna som vägledning när en privat aktör har i uppdrag att tekniskt bearbeta eller tekniskt lagra handlingar för en myndighets räkning, eftersom inte samma insynsintresse (offentlighetsprincipen) gör sig gällande som när en myndighet utför motsvarande uppdrag.

[28] Regleringen i nu gällande 2 kap. 13 § TF fanns vid tidpunkten för respektive rättsfall i 2 kap. 10 § TF.

3.1.4 Endast för teknisk bearbetning eller teknisk lagring och för den uppdragsgivande myndighetens räkning

I samtliga lagrum[29] där begreppet teknisk bearbetning eller teknisk lagring används tydliggörs att den uppdragstagande parten ska tillhandahålla verksamhet *endast* för den tekniska bearbetningen eller tekniska lagringen *för en annan myndighets räkning* eller *på uppdrag av en myndighet*. Den hantering som avses ske i den upphandlade tjänsten ska alltså till alla delar ske för att tillgodose den uppdragsgivande myndighetens behov. Om tjänsteleverantören vill använda uppgifterna för att skapa statistik eller för att förbättra sina tekniska lösningar så kommer avgränsningen att tjänsten ska ske för annans räkning inte att uppfyllas.[30] Det är i lagtexten tydligt att den rättsföljd som är kopplad till respektive lagrum ställer krav på att tjänsteleverantörens leverans måste inskränkas till sådan teknisk befattning som omfattas av begreppet teknisk bearbetning eller teknisk lagring. Den tekniska befattningen ska dessutom ske utifrån ett uppdrag från en myndighet eller för en myndighets räkning.

I förarbetena till tystnadspliktslagen[31] behandlas frågan om hur existensen av den författningsreglerade tystnadsplikten påverkas av om en tjänsteleverans innehåller moment av både teknisk bearbetning respektive teknisk lagring och andra tjänster. Om ett uppdrag innehåller annat än enbart sådana tekniska moment som kan definieras som teknisk bearbetning eller teknisk lagring så faller utkontrakteringen utanför tillämpningsområdet för tystnadspliktslagen. Det anges vidare att om en myndighet utkontrakterar flera uppdrag till samma tjänsteleverantör som innebär dels sådan teknisk befattning med uppgifterna och dels andra moment, så är tystnadspliktslagen endast tillämplig i det första fallet och, om utkontrakteringen helt eller delvis avser samma uppgifter, endast i den mån som uppgifterna som är föremål för teknisk befattning inte ingår i den andra tjänsten.

I förarbetena till 10 kap. 2 a § OSL[32] klargörs tillämpningen av den sekretessbrytande regeln. Det anges att syftet med bestämmelsen är att utvidga myndigheters möjligheter att lämna ut uppgifter som omfattas av sekretess endast vid utkontraktering av it-drift. Den syftar alltså inte till att möjliggöra andra former av utkontraktering med digitala inslag som en myndighet kan ha behov av. För att tydliggöra den avsedda avgränsningen används i lagtexten begreppet endast teknisk bearbetning eller teknisk lagring.

Utfallen i praxis visar att tjänsteleverantörens befattning med uppgifterna helt ska avse att tillgodose myndighetens intressen och att utrymmet för att behandla uppgifterna för

[29] Här avses lagrummen 2 kap. 9, 13 §§ TF, 10 kap. 2a §, 11 kap. 4a § och 40 kap. 5 § OSL och 4 § lag (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter.
[30] Se också SOU 2021:1 Säker och kostnadseffektiv it-drift, s. 296.
[31] Prop. 2019/20:201 Tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter, s. 22.
[32] Prop. 2022/23:97 Sekretessgenombrott vid utlämnande för teknisk bearbetning eller teknisk lagring, s. 11.

egna ändamål,[33] hur begränsade de än må vara, inte är möjligt för att rekvisitet ska anses uppfyllt, jfr HFD 2011 ref. 52 och 2018 ref 48 (se avsnitt 3.1.3).

3.2 Vilka it-tjänster omfattas av begreppet teknisk bearbetning eller teknisk lagring?

Vilka tjänster ska då anses omfattas av begreppet teknisk bearbetning eller lagring? I propositionen till tystnadspliktslagen[34] konstaterar regeringen att begreppet teknisk bearbetning eller teknisk lagring är både teknikneutralt och etablerat. Det anges vidare i propositionen att tillämpningen av begreppet kan orsaka vissa svårigheter i förhållande till dagens och framtidens teknikanvändning och teknikutveckling när det gäller myndigheters grundläggande behov av it-driftstjänster och andra it-baserade funktioner. Regeringens inställning är dock att begreppet är tillräckligt tydligt och att det inte bör vålla några större tillämpningssvårigheter i praktiken. I förarbetena till 10 kap. 2 a § OSL anges att vilka slags åtgärder som kan omfattas av begreppet teknisk bearbetning eller teknisk lagring kan komma att förändras över tid med anledning av den tekniska utvecklingen.

Till ledning för vilka it-tjänster som omfattas av begreppet teknisk bearbetning eller teknisk lagring får utgångspunkt tas i de exempel som räknats upp i de olika förarbetena till tryckfrihetsförordningen, OSL och tystnadspliktslagen, se ovan redovisning i avsnitt 3.1.2.

3.2.1 It-tjänstens karaktär

En utgångspunkt för den sekretessbrytande regeln i 10 kap. 2 a § OSL och för regleringen i tystnadspliktslagen är att utkontrakteringen ska avse it-drift. Även om begreppet it-drift inte är definierat ger det ändå ledning om vilken karaktär av tjänster som avses.

Enligt eSams uppfattning finns det ett relativt stort utrymme för vilka it-tjänster som kan innefattas i begreppet teknisk bearbetning eller teknisk lagring. De traditionella infrastrukturtjänsterna där it-leverantören tillhandahåller drift, underhåll, lagring och säkerhetskopiering med tillhörande säkerhets- och övervakningstjänster bör typiskt sett vara tjänster som kan omfattas. Även systemleveranstjänster och it-baserade funktioner (se 3.1.2) kan utgöra teknisk bearbetning eller teknisk lagring. Molnbaserad teknik bör kunna användas för tillhandahållande av nämnda infrastrukturtjänster.

[33] Detta är viktigt även ur personuppgiftssynpunkt. Om leverantören behandlar uppgifter för eget ändamål blir det fråga om utlämnande för en personuppgiftsansvarig till en annan personuppgiftsansvarig.
[34] Prop. 2019/20:201 Tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter, s. 16.

Det finns dock anledning att vara försiktig med att utgå från hur it-tjänsten är rubricerad. En it-driftstjänst kan tillhandahållas paketerad med en eller flera tilläggstjänster som kan ha en karakteristik som inte kan inrymmas i begreppen teknisk bearbetning eller lagring. I detta sammanhang kan det vara av värde att granska tjänsteleverantörens affärsmodell. Om denna är uppbyggd utifrån informationshantering och exempelvis omfattar analys eller försäljning av information så kan detta ge en vägledning om att tjänstens karakteristik inte kan rymmas inom teknisk bearbetning eller teknisk lagring.

Istället för att utgå från tjänstens rubricering förspråkar eSam att bedömningen av vad som bör karakterisera en it-tjänst för att den ska definieras som teknisk bearbetning eller teknisk lagring utgår från tjänstens tekniska natur och tjänsteleverantörens befattning.

3.2.2 Tjänsteleverantörens befattning

Av de exempel som finns i förarbetena till TF[35] så framgår det tydligt att leverantörernas tjänster måste vara av teknisk natur. Den behandling som leverantören ska tillhandahålla innebär endast hantering av den information som myndigheten har tillhandahållit. Någon förädling av informationen och informationsinnehållet omfattas inte av exemplen från 1970-talet. Exemplen antyder att leverantören kan överföra befintlig information från ett medium till ett annat, tillhandahålla sökbar lagring, kopiering m.m., men det förefaller inte vara aktuellt att låta leverantören tillföra informationen något nytt eller kompletterande innehåll.

Enligt eSams uppfattning ska en tjänsteleverantörs förhållningssätt och befattning med informationsmängden i en utkontraktering alltså vara av teknisk natur och uteslutande för den utkontrakterande myndighetens räkning. Någon behandling av tjänsteleverantören för egen räkning kan inte tillåtas. Om tjänsteleverantörens befattning med uppgifterna är av teknisk natur är det acceptabelt att denne tar del av nödvändiga uppgifter i klartext, dvs. eSam gör bedömningen att förarbetsuttalandena till tystnadspliktslagen och 10 kap. 2 a § OSL och även tidigare förarbetsuttalanden till TF (avsnitt 3.1.2) ger ett vidare utrymme att "ta del" av uppgifter än vad tidigare praxis (avsnitt 3.1.3) uttryckt.

Det bör inte vara aktuellt för leverantören att ta del av information som omfattas av uppdraget om teknisk bearbetning eller lagring annat än då det krävs för att utföra leverantörens uppgifter enligt avtalet.

eSam anser således att för att det ska vara fråga om teknisk bearbetning eller teknisk lagring ska informationsbehandlingen ske för den utkontrakterade myndighetens räkning

[35] Prop. 1975/76:160 om nya grundlagsbestämmelser angående allmänna handlingars offentlighet, s 137.

och behandlingen får inte innebära att informationen förädlas genom att något tillförs innehållsmässigt.

Vid utkontraktering är det sannolikt att tjänsteleverantören erbjuder tjänster där vissa delar kan definieras som teknisk bearbetning eller teknisk lagring och andra inte. Frågan inställer sig då hur den rättsliga regleringen i TF respektive OSL förhåller sig till detta.

I rekvisitet "endast" ligger att uppgifterna inte får hanteras på annat sätt än för teknisk bearbetning eller teknisk lagring. Om samma uppgifter hanteras i ett annat informationsflöde behöver dessa flöden enligt eSams uppfattning hållas åtskilda, annars riskerar hela utkontrakteringen att inte anses vara teknisk bearbetning eller teknisk lagring, jfr förarbetsuttalandena till tystnadspliktlagen (se avsnitt 3.1.4). Myndigheten behöver därmed säkerställa en åtskild hantering av leverantören, i de fall leverantören också tillhandahåller andra tjänster där uppgifterna hanteras. Detta behöver hanteras särskilt i avtalsregleringarna och tekniska begränsningar såsom behörighetsbegränsningar.

4. Allmänna handlingar

Enligt 2 kap. 1 § TF ska var och en ha rätt att ta del av allmänna handlingar. Hos alla svenska myndigheter finns allmänna handlingar, dvs. handlingar som *förvaras* hos myndigheten och är att anse som *inkomna*[36] till eller *upprättade*[37] hos myndigheten.[38] Med handling avses enligt 2 kap. 3 § TF en framställning i skrift eller bild samt en upptagning som endast med tekniska hjälpmedel kan läsas, avlyssnas eller uppfattas på annat sätt.

En handling som förvaras hos en myndighet endast som ett led i en teknisk bearbetning eller teknisk lagring för någon annans räkning anses enligt 2 kap. 13 § 1 st. TF inte som allmän handling hos den myndigheten. En sådan handling omfattas således inte av bestämmelserna om handlingsoffentlighet hos den mottagande myndigheten. På motsvarande sätt följer det av 2 kap. 9 § 3 st. TF att en handling som återkommer till en myndighet efter teknisk bearbetning eller teknisk lagring utanför myndigheten inte anses som en inkommen handling. Rimligen bör det ursprungliga exemplaret då inte heller anses vara expedierat från, och därmed en upprättad allmän handling hos, den avsändande myndigheten. En annan tolkning skulle leda till att undantaget i 2 kap. 9 § 3 st. TF helt skulle förlora sin funktion.[39]

Om tjänsteleverantören även vidtar andra åtgärder än teknisk bearbetning eller lagring, är dock undantaget i 2 kap. 9 § 3 st. TF inte tillämpligt. I sådana situationer torde handlingen också anses expedierad och därmed utgöra en upprättad allmän handling i samma stund som den görs tekniskt tillgänglig för tjänsteleverantören. Det finns undantag vad gäller osjälvständiga uppdragstagare, se avsnitt 5.3.2.

Vid en utkontraktering måste myndigheten således ta ställning till om utlämnandet av vissa handlingar till en extern tjänsteleverantör medför att dessa expedieras vilket bedöms utifrån vad leverantören ska göra med uppgifterna, se avsnitt 3 om teknisk bearbetning eller teknisk lagring.

4.1 Utkontraktering av hantering av allmänna handlingar

Vid utkontraktering som innefattar hantering av allmänna handlingar till en extern tjänsteleverantör måste myndigheten beakta de krav som ställs gällande gallring och

[36] Av 2 kap. 9 § 1 st. TF framgår att en handling anses ha kommit in till en myndighet, när den har anlänt till myndigheten eller kommit behörig befattningshavare till handa. I fråga om upptagning gäller i stället att den anses ha kommit in till myndigheten när någon annan har gjort den tillgänglig för myndigheten på sätt som anges i 6 §.
[37] Enligt 2 kap. 10 § TF anses en handling upprättad hos en myndighet när den har expedierats, eller om den inte har expedierats, när det ärende som den hänför sig till har slutbehandlats eller, om den inte hänför sig till visst ärende, när den har justerats av myndigheten eller färdigställts på annat sätt.
[38] 2 kap. 4 §, 6 § och 9-10 §§ TF.
[39] HFD 2011:52, jfr uttalanden i prop. 2019/20:201 Tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter, s. 7 och prop. 1975/76 om nya grundlagsbestämmelser angående allmänna handlingars offentlighet, s. 137.

arkivering av sådana handlingar. Sådana bestämmelser hittas bland annat i arkivlagen (1990:782), arkivförordningen (1991:446), TF, OSL, myndighetsspecifik registerlagstiftning samt Riksarkivets föreskrifter och allmänna råd.[40]

Huvudregeln är att allmänna handlingar ska bevaras och att gallring endast ska ske om det framgår av lag, förordning eller Riksarkivets föreskrifter och beslut. Om det finns en bestämmelse eller föreskrift som säger att vissa handlingar ska gallras är det viktigt att myndigheten ser till att detta görs, vilket även omfattar att se till att detta följs av tjänsteleverantören som hanterar uppgifterna. Detsamma gäller om de allmänna handlingarna ska bevaras.[41] Myndigheten måste då säkerställa att den tilltänkta tjänsteleverantören erbjuder långtidsbevaring. Det kan vara olämpligt att lägga mer långsiktigt bevarande av diarieuppgifter och handlingar i en molntjänst och det behöver övervägas om bevarandehandlingar vid ärendens avslut istället bör föras över till myndighetens ordinarie system (t.ex. vid ärenden om rekrytering). Det behöver säkerställas möjlighet till uttag och migrering, dvs. att myndigheten vid behov har möjlighet att ta tillbaka handlingarna eller byta leverantör. Det måste också vara möjligt för både myndigheten själv och allmänheten att på ett smidigt sätt få tillgång till handlingarna. Myndigheten måste även kunna garantera handlingarnas riktighet. Det är myndighetens ansvar att säkerställa så att gallring och bevarande av handlingar sker på ett korrekt sätt även hos tjänsteleverantören, genom att utforma avtalsvillkoren så att detta möjliggörs. De krav som ställs på arkivering och gallring enligt arkivlagen, relevanta föreskrifter samt registerförfattningar måste således beaktas tidigt i upphandlingsprocessen. Behandlingen behöver finnas med i myndighetens arkivförteckning.

Utöver detta bör myndigheten även analysera vilka risker som är förknippade med att överlåta hanteringen av allmänna handlingar till en extern tjänsteleverantör. Om denne går i konkurs eller dylikt skulle det kunna leda till att de allmänna handlingarna förloras eller obehörigen sprids.

[40] T.ex. 1 kap. 3 § Föreskrifter om ändring av Riksarkivets föreskrifter (RA–FS 1991:1) och allmänna råd om arkiv hos statliga myndigheter (RA-FS 2019:2).
[41] Se t.ex. Riksarkivets föreskrifter och allmänna råd (RA-FS 2009:1) om elektroniska handlingar (upptagningar för automatiserad behandling).

5. Sekretess

5.1 Utkontraktering och sekretess

Vid en utkontraktering som medför att information hos myndigheten blir tillgänglig även för tjänsteleverantören måste begränsningarna i OSL beaktas. Grundprincipen är att varje myndighet ansvarar för sin egen verksamhet. En myndighet som tänker genomföra utkontraktering måste därför utreda vilka slags uppgifter som ska överlämnas till tjänsteleverantören och, i de fall det är fråga om sekretessreglerade uppgifter, behöver myndigheten noga överväga om det är tillåtet enligt OSL. Myndigheten behöver också överväga om det är lämpligt med en utkontraktering utifrån att det är fråga om sekretessreglerade uppgifter.

Sekretess innebär inte bara begränsningar av rätten att ta del av allmänna handlingar[42] utan även ett förbud att röja en uppgift, oavsett om det görs muntligen, genom utlämnande av allmän handling eller på något annat sätt, 3 kap. 1 § OSL. Sekretess innebär således både handlingssekretess och tystnadsplikt och gäller inte bara för uppgifter i allmänna handlingar, utan även för uppgifter som finns hos en myndighet i sådana handlingar som ännu inte blivit allmänna. Otillåtet röjande av en sekretessbelagd uppgift är straffsanktionerat som brott mot tystnadsplikt, 20 kap. 3 § brottsbalken, BrB. Något krav på att ett avslöjande har skett ska inte läggas in i ordet röja.[43]

Enligt 2 kap. 1 § 1 st. OSL gäller för *myndigheter* förbud mot att röja eller utnyttja en uppgift. Av övriga bestämmelser i kapitlet och bilagan till OSL följer att vissa organ som inte är myndigheter ska jämställas med sådana vid tillämpningen av 2 kap. TF och OSL.

Sekretess gäller som huvudregel inte bara i förhållande till enskilda utan också mellan myndigheter, samt inom en myndighet om det finns olika verksamhetsgrenar som är att betrakta som självständiga i förhållande till varandra, 8 kap. 1 och 2 §§ OSL.

Sekretess gäller även i förhållande till utländska myndigheter och mellanfolkliga organisationer, för vilka särskilda regler införts i 8 kap. 3 § OSL.

I 21 kap. 7 § OSL föreskrivs dessutom ett generellt förbud mot att lämna ut personuppgifter om det kan antas att mottagaren efter ett utlämnande kan komma att

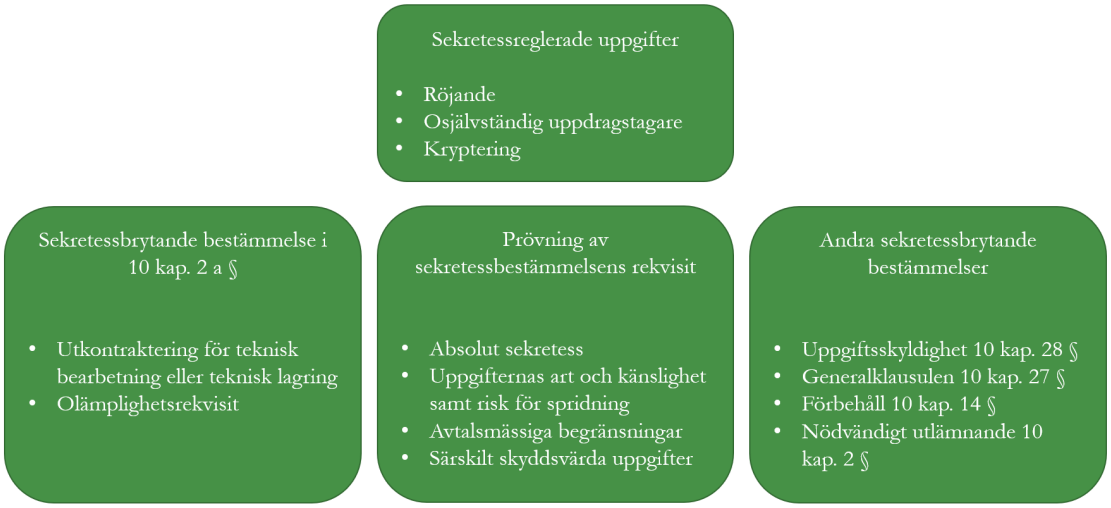
[42] Rätten att ta del av allmänna handlingar får enligt 2 kap. 2 § 1 st. TF begränsas bara om det är nödvändigt med hänsyn till vissa, särskilt angivna, intressen. En sådan begränsning ska anges noga i en bestämmelse i en särskild lag eller, om det i ett visst fall anses lämpligare, i en annan lag som den förstnämnda lagen hänvisar till. Den särskilda lag som avses är OSL.
[43] Brottsbalken, En kommentar, Bäcklund m.fl. och prop. 1979/80:2 med förslag till sekretesslag m.m. del A, s. 402 ff., s. 488 och s. 504.

behandla uppgiften i strid med dataskyddsförordningen, dataskyddslagen eller lagen (2003:460) om etikprövning.

5.2 Inledande överväganden inför en utkontraktering

Det finns i OSL ingen fastslagen metod vid bedömning inför en utkontraktering. Vanligtvis[44] bör en sekretessprövning bestå av stegen; är uppgifterna sekretessreglerade, föreligger sekretess i det enskilda fallet eller kan utlämnande ske efter en skadeprövning, finns en sekretessbrytande bestämmelse.

Vid en utkontraktering är det ofta fråga om en stor mängd uppgifter och myndigheten vet sällan vid varje givet tillfälle exakt vilka uppgifter det rör sig om. Det kan följaktligen i praktiken vara omöjligt för myndigheten att vid varje utlämnande av uppgifter göra en individuell sekretessbedömning. Den sekretessbrytande bestämmelsen i 10 kap. 2 a § OSL, som är tillämplig enbart vid teknisk bearbetning eller lagring, är tänkt att kunna tillämpas även när sekretessen inte kan bedömas för varje enskild uppgift. Det kan därför vara mer ändamålsenligt att inför en utkontraktering att först pröva om denna sekretessbrytande bestämmelse kan tillämpas, innan myndigheten ger sig in på att pröva om sekretess föreligger för uppgifterna i det enskilda fallet. Sådan utgångspunkt har fått ligga till grund för strukturen i följande avsnitt, dvs. efter avsnittet om det är sekretessreglerade uppgifter följer ett avsnitt om förutsättningar för tillämpning av 10 kap. 2 a § OSL. Därefter följer ett avsnitt om prövning utifrån sekretessbestämmelsens rekvisit och slutligen ett avsnitt om andra sekretessbrytande bestämmelser som i vissa fall kan tillämpas.



[44] Karlsson Rikard och Atle Morseth Edvinsson, Molntjänster och staten – En diskussion om röjandebegreppet i offentlighets- och sekretesslagen.

5.3 Sekretessreglerade uppgifter

De sekretessöverväganden som beskrivs i detta avsnitt är endast nödvändiga om de uppgifter som görs tillgängliga är *sekretessreglerade.*[45] Den första fråga som myndigheten måste ställa sig är därför om det över huvud taget finns någon sekretessbestämmelse i OSL som avser de aktuella uppgifterna och som är tillämplig hos myndigheten. Är uppgifterna inte sekretessreglerade behöver inga sekretessöverväganden göras. Däremot behöver fortfarande regler om behandling av personuppgifter och informationssäkerhet m.m. övervägas.

5.3.1 Röjande

Som anförts ovan definieras sekretess i 3 kap. 1 § OSL som ett förbud mot att röja en uppgift, vare sig det sker muntligen, genom utlämnande av en allmän handling eller på något annat sätt. I förarbetena till sekretesslagen anges att innebörden av röjandeförbudet är att ”befattningshavaren inte får låta någon ta del av hemlig uppgift vare sig detta sker genom att allmän handling företes eller att någon får ta del av handling som inte är allmän eller att uppgiften meddelas i brev. Också andra former av röjande av en uppgift kan tänkas, t.ex. att någon förevisar ett hemligt föremål för annan.”[46]

Enligt förarbetena till 10 kap. 2 a § OSL ska en uppgift som omfattas av sekretess och som görs tillgänglig för en tjänsteleverantör betraktas som utlämnad eller röjd i OSL:s mening.[47] [48] Detta gäller även uppgifter som görs tillgängliga för teknisk bearbetning eller teknisk lagring. Ett sådant röjande är bara tillåtet om inte sekretess hindrar att uppgiften lämnas ut.

En uppgift anses inte röjd om kryptering är möjlig, se 5.3.3.

5.3.2 Osjälvständig uppdragstagare

Myndigheten behöver fundera över om det verkligen är fråga om en utkontraktering eller om det är fråga om att lämna uppgifter till en part som inte är självständig i

[45] En *sekretessreglerad* uppgift är enligt definitionen i 3 kap. 1 § OSL en uppgift för vilken det finns en bestämmelse om sekretess. En sekretessreglerad uppgift för vilken sekretess gäller i ett enskilt fall är en *sekretessbelagd* uppgift.
[46] Prop. 1979/80:2 med förslag till sekretesslag m.m., del A s 119.
[47] Prop. 2022/23:97 Sekretessgenombrott vid utlämnande för teknisk bearbetning eller teknisk lagring, s 7.
[48] eSam har tidigare i ett rättsligt uttalande från 2015 framhållit uppfattningen att det inte är fråga om ett röjande om tjänsteleverantören enligt avtal med uppdragsgivaren inte får del av eller vidarebefordra de uppgifter som görs tekniskt tillgängliga för denne och omständigheterna i övrigt medför att det är osannolikt att detta ändå sker. Detta ställningstagande har kompletterats med två ytterligare uttalanden 2018 och 2019 där slutsatsen var att sekretessreglerade uppgifter får anses vara röjda om de görs tekniskt tillgängliga för en tjänsteleverantör som till följd av ägarförhållanden eller annars är bunden av regler i ett annat land enligt vilka tjänsteleverantören kan bli skyldig att överlämna information utan att internationell rättshjälp anlitats eller annan laglig grund föreligger enligt svensk rätt. Det räcker inte med en sannolikhetsbedömning av om ett röjande kan komma att ske. Först måste den rättsliga regleringen av parternas mellanhavande ha utformats på ett hållbart sätt så att en juridiskt bindande och sanktionerad avtalssekretess föreligger. Dessutom får leverantören av tjänsten inte vara bunden av regler i främmande rätt om att lämna ut uppgifter utan en föregående sekretessprövning eller annan laglig grund enligt svensk rätt för ett utlämnande. Dessa uttalanden är överspelade utifrån lagstiftarens uttryck i förarbetena till 10 kap. 2 a § OSL.

förhållande till myndigheten. Detta kan t.ex. vara aktuellt vid vissa typer av konsulttjänster. Sekretess behöver inte beaktas vid överlämnande av uppgifter till en fysisk person som på grund av uppdrag eller på annan liknande grund deltar i myndighetens verksamhet och därför själv omfattas av samma tystnadsplikt som myndighetens anställda enligt 2 kap. 1 § OSL. Av bestämmelsens andra stycke framgår att lagens förbud mot att röja eller utnyttja en uppgift också gäller för en *person* som fått kännedom om uppgiften genom att för det allmännas räkning delta i en myndighets verksamhet

- på grund av anställning eller uppdrag hos myndigheten,
- på grund av tjänsteplikt, eller
- på annan liknande grund.

Ett överlämnande av en handling eller en uppgift till en sådan person utgör således inte ett utlämnande enligt TF eller ett röjande enligt OSL och i dessa fall behöver myndigheten därför inte fundera över sekretessen enligt detta avsnitt. Ett personuppgiftsbiträde (se avsnitt 6.4.2) finns alltid utanför den ansvariges egna organisation och kan därmed inte anses delta i myndighetens verksamhet.

5.3.3 Kryptering

Myndigheten behöver också överväga om uppgiften är möjlig att kryptera på ett sådant sätt att mottagaren saknar teknisk kapacitet att forcera krypteringen. När en uppgift skyddas av en kryptografisk funktion som hindrar mottagaren att ta del av uppgiftens informationsbärande innehåll, bör den inte betraktas som röjd enligt OSL.[49] Många gånger kan det vara svårt att uppnå kryptering för alla uppgifter som hanteras i t.ex. i samarbetsplattformar[50] med kontorsstöd och dokumenthantering. Även i digital infrastruktur[51] kan begränsningar finnas, t.ex. när krypteringsnycklarna behandlas i klartext i molnet eller tjänsteleverantören råder över behörigheterna till nyckelhanteringssystemet. För att informationen inte ska betraktas som röjd kan hela kedjan, från avsändaren till mottagaren vid överföring samt lagringen, behöva krypteras. Det kan många gånger vara svårt att säkerställa en sådan total kryptering.

För att säkerställa en kryptering och att uppgifterna inte blir röjda i OSLs mening bör kraven på de tekniska begränsningarna regleras i avtal.

[49] Prop. 2022/23:97 Sekretessgenombrott vid utlämnande för teknisk bearbetning eller teknisk lagring, s 7.
[50] S.k. SaaS-tjänster.
[51] S.k. IaaS-tjänster.

Om kryptering inte är möjligt behöver det övervägas om det finns en tillämplig sekretessbrytande bestämmelse eller att det efter en prövning av skaderekvisitet ändå bedöms vara möjligt att lämna ut uppgifterna till tjänsteleverantören.

5.4 Utkontraktering för teknisk bearbetning eller teknisk lagring enligt 10 kap. 2 a § OSL

Av 10 kap. 2 a § OSL följer att sekretess inte hindrar att en uppgift lämnas till en enskild eller till en annan myndighet som för den utlämnande myndighetens räkning har i uppdrag att endast tekniskt bearbeta eller tekniskt lagra uppgiften, om det med hänsyn till omständigheterna inte är olämpligt att uppgiften lämnas ut. Bestämmelsen syftar till att ge förutsättningar för myndigheter att utkontraktera sin it-drift.[52]

I och med att bestämmelsen gäller uppgifter som mottagaren erhåller för teknisk bearbetning eller teknisk lagring omfattas uppgifterna även av sekretess hos mottagaren, se 11 kap. 4 a § och 40 kap. 5 § OSL eller av tystnadsplikt enligt 4 § tystnadspliktslagen.

Av 11 kap. 4 a § följer att om en myndighet får, i verksamhet för enbart teknisk bearbetning eller teknisk lagring för en annan myndighets räkning, en uppgift som hos den senare myndigheten är sekretessreglerad av hänsyn till ett allmänt intresse, blir sekretessbestämmelsen tillämplig även hos den mottagande myndigheten (överförd sekretess). Vidare gäller enligt 40 kap. 5 § OSL sekretess beträffande uppgifter om en enskilds personliga eller ekonomiska förhållanden (absolut sekretess).

Av 4 § tystnadspliktslagen framgår att den som på grund av anställning eller på något annat sätt deltar i eller har deltagit i en tjänsteleverantörs verksamhet att på uppdrag av en myndighet endast tekniskt bearbeta eller tekniskt lagra uppgifter inte obehörigen får röja eller utnyttja dessa uppgifter. Tystnadsplikt gäller enligt 3 § även för anställda m.fl. hos underleverantörer till tjänsteleverantören, som medverkar till att fullgöra dennes uppdrag.[53] Lagen är begränsad till teknisk bearbetning eller lagring av uppgifter i samband med utkontraktering, varför uppdrag som innehåller annat än enbart sådana tekniska moment faller utanför lagens tillämpningsområde i dessa delar.

I förarbetena[54] till 10 kap. 2 a § OSL anges att bestämmelsen endast kan tillämpas av de myndigheter och med myndigheter jämställda organ som omfattas av OSLs tillämpningsområde, och en privat tjänsteleverantör, som inte omfattas av OSL, kan därmed inte tillämpa bestämmelsen när denne avser att exempelvis överföra uppgifter till en underleverantör. Enligt eSams uppfattning innebär inte detta ett hinder mot att

[52] Prop. 2022/23:97 Sekretessgenombrott vid utlämnande för teknisk bearbetning eller teknisk lagring, s 1 och 10.
[53] Prop. 2019/20:201 Tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter, s 16.
[54] Prop. 2022/23:97 Sekretessgenombrott vid utlämnande för teknisk bearbetning eller teknisk lagring, s 10.

utkontraktera till en leverantör som använder underleverantörer. Förekomsten av underleverantörer är däremot något som måste beaktas vid myndighetens olämplighetsprövning, se bl.a. avsnitt 5.4.2.3 och 5.4.2.4.

5.4.1 Teknisk bearbetning eller teknisk lagring

Det finns ingen tydlig definition av teknisk bearbetning eller teknisk lagring enligt vad som framgår i lag och andra rättskällor. Som redogjors för i avsnitt 3 är eSams bedömning och tolkning av begreppet teknisk bearbetning eller teknisk lagring att det inte bör vara aktuellt att låta leverantören tillföra informationen något nytt eller kompletterande innehåll. Bedömningen behöver ske utifrån it-tjänstens karaktär. En tjänsteleverantörs förhållningssätt och befattning med informationsmängden i en utkontraktering ska vara av teknisk natur och uteslutande för den utkontrakterande myndighetens räkning.

Det är inte ovanligt att tjänsterna innebär att data också används för tjänsteleverantörens egna behov (metadata, diagnostisk data m.m.). Myndigheten behöver noga analysera att tjänsten inte medför att uppgifterna används för annat sätt än *endast* för teknisk bearbetning eller teknisk lagring. En granskning av leverantörens affärsmodell kan vara ett sätt att undersöka detta. Detta behöver även beaktas i kravställningen vid en upphandling.

5.4.2 Olämplighetsrekvisit

Av andra ledet i 10 kap. 2 a § OSL framgår att det myndigheten vid prövning inför en utkontraktering av sekretessreglerade uppgifter ska bedöma om det med hänsyn till omständigheterna *inte är olämpligt* att uppgifterna lämnas ut. Det innebär att en myndighet, innan en uppgift lämnas ut, ska pröva om det finns skäl som talar emot att uppgiften lämnas ut. Lagrådet[55] har påpekat att det är en viss skillnad mellan begreppet ”inte är olämpligt” och det omvända, som skulle ha inneburit att uppgifterna fick lämnas om det ”vore lämpligt”. Enligt eSam bör detta kunna tolkas som att utredningsbördan är något lägre för myndigheten vid en olämplighetsbedömning än en lämplighetsbedömning, se 5.4.2.5 om avvägning utifrån kända faktorer.

eSams uppfattning är att vid en olämplighetsprövning är det av vikt att beakta de intressen som sekretessen avser att skydda och hur de kan tillgodoses. Likt vid prövning som sker av en sekretessbestämmelses rekvisit (se avsnitt 5.5) bör uppgifternas art, deras känslighet och hur uppgifterna hos mottagaren skyddas mot ytterligare spridning kunna tillmätas betydelse.

[55] Utdrag ur protokoll Lagrådets sammanträde 2023-02-14.

En olämplighetsbedömning bör avse samtliga omständigheter som är relevanta i en specifik utkontrakteringssituation. I förarbetena till 10 kap. 2 a § OSL framhålls att jämfört med en intresseavvägning,[56] som endast avser en prövning av om intresset av att lämna ut en uppgift väger tyngre än det intresse som sekretessen ska skydda, är en bedömning av om ett utlämnande är olämpligt mer omfattande till sin karaktär och även andra omständigheter bör beaktas, som leverantörens förmåga att skydda uppgifterna. Omständigheter att beakta kan vara kopplade till den uppgiftslämnande myndigheten, till uppgiftsmottagaren eller till de uppgifter som lämnas ut. Det kan också röra sig om omständigheter som rör den aktuella it-driftstjänsten, avtalsförhållandet mellan den uppdragsgivande myndigheten och uppgiftsmottagaren eller det allmänna säkerhetsläget nationellt eller internationellt. Det ska alltså göras en allsidig prövning av samtliga omständigheter som har relevans i det enskilda fallet för att uppgiftshanteringen ska vara säker och förutsebar.[57]

5.4.2.1 Uppgifter av känsligt slag

Inom vissa områden förekommer uppgifter vars röjande kan få mycket allvarliga och långtgående konsekvenser. En omständighet som med viss tyngd kan innebära att ett utlämnande är olämpligt är att det är fråga om uppgifter av särskilt känsligt slag, exempelvis uppgifter av synnerlig betydelse för rikets säkerhet när det gäller totalförsvaret.[58]

I säkerhetsskyddslagen finns bestämmelser om särskilda bedömningar, lämplighetsprövningar och krav på samråd med tillsynsmyndigheter om en utomstående aktör under vissa förutsättningar kan få tillgång till säkerhetsskyddsklassificerade uppgifter eller annan säkerhetskänslig verksamhet.

5.4.2.2 Aggregerad och samlokaliserad information

Det kan vara olämpligt att lämna ut en mycket stor mängd uppgifter där de flesta enskilda uppgifter inte är känsliga, men där den totala informationsmängden i sig är tillräckligt skyddsvärd. Med en oinskränkt tillgång till stora informationsmängder kan det finnas risk för åtgärder och analyser som av säkerhetsskäl inte bör få förekomma.[59] Det kan behövas säkerhetsskyddsavtal även om uppgifterna var för sig inte är säkerhetsskyddsklassade, om uppgifterna på en aggregerad nivå ändå når upp till en högre säkerhetsskyddsklass.[60] Det kan t.ex. handla om situationer där uppgifter som

[56] SOU 2021:1 It-driftsutredningens delbetänkande Säker och kostnadseffektiv it-drift – rättsliga förutsättningar för utkontraktering.
[57] Prop. 2022/23:97 Sekretessgenombrott vid utlämnande för teknisk bearbetning eller teknisk lagring, s 13 och 16.
[58] Prop. 2022/23:97 Sekretessgenombrott vid utlämnande för teknisk bearbetning eller teknisk lagring, s 13 och 17.
[59] SOU 2018:25 Juridik som stöd för förvaltningens digitalisering (Digitaliseringsrättsutredningen), s 378-379.
[60] Jfr prop. 2017/18:89 Ett modernt och stärkt skydd för Sveriges säkerhet – ny säkerhetsskyddslag, s. 45.

sammanställts har bearbetats eller kan bearbetas så att man av sammanställningen kan utvinna en annan och mer känslig information än av uppgifterna var för sig.

Myndigheten bör ta ställning till om utkontrakteringen kan innebära en ökad riskexponering för de uppgifter som lämnas ut, exempelvis genom att uppgifter samlokaliseras med uppgifter som tillhör andra myndigheter eller organisationer. Det kan vara olämpligt om flera myndigheters system och information samlas i en tjänst, då det kan innebära en ökad riskexponering för känsliga uppgifter.[61]

Om utkontrakteringen innebär att svenska myndigheter avhänder sig kontrollen över uppgifter i den samhällsbärande verksamheten är detta enligt eSams uppfattning en omständighet av tyngd att beakta vid olämplighetsprövningen.[62] Detta utifrån krav på myndigheten att genomföra sitt uppdrag, men också utifrån påverkan på Sveriges digitala suveränitet, dvs. förutsättningar att kontrollera myndighetens egna digitala data och hur den används.

5.4.2.3 Leverantörsförhållanden, tystnadsplikt och avtalsvillkor

Enligt förarbetena bör myndigheten granska tjänsteleverantörens affärsmodell.[63] Myndigheten behöver beakta avtalsrelationen med leverantören och då i synnerhet avtalsvillkor som riskerar att frånta myndigheten kontrollen över uppgifterna. Det kan ha betydelse om underleverantörer potentiellt kan få tillgång till uppgifterna. Om leverantören har många underleverantörer med olika lokalisering kan detta försvåra en överblick av hur uppgifterna kan riskera att spridas och vilket skydd som kan upprätthållas. I detta sammanhang kan framhållas att i ett upphandlingsunderlag behöver myndigheten säkerställa att samma krav ställs på underleverantörer som på huvudleverantören.

Det bör också beaktas vilka åtgärder som uppgiftsmottagaren vidtar för att skydda uppgifterna och om denne omfattas av en lag- eller avtalsreglerad tystnadsplikt (se avsnitt 5.5.4). I förarbetena till tystnadspliktslagen påtalas att riskerna med en utkontraktering inte alltid elimineras eller ens minimeras med hjälp av bestämmelsen i tystnadspliktslagen.[64] eSams uppfattning är dock att det straffrättsliga ansvaret som leverantörens anställda har enligt en lagstadgad tystnadsplikt ändå bör ha viss tyngd vid olämplighetsbedömningen. Även en avtalsreglerad tystnadsplikt bör kunna vägas in.[65]

---

[61] Prop. 2022/23:97 Sekretessgenombrott vid utlämnande för teknisk bearbetning eller teknisk lagring, s 17, SOU 2018:25 Juridik som stöd för förvaltningens digitalisering (Digitaliseringsrättsutredningen), s 378-379.
[62] Försäkringskassans har i sin Vitbok Molntjänster i samhällsbärande verksamhet – risker, lämplighet och vägen framåt beskrivit den ökade sårbarhet som följer med digitaliseringen av samhällsbärande funktioner. I vitboken uttrycks att Sveriges digitala suveränitet behöver säkras och den offentliga förvaltningen måste bibehålla eller ta tillbaka kontrollen över samhällsbärande digitala funktioner och data.
[63] Prop. 2022/23:97 Sekretessgenombrott vid utlämnande för teknisk bearbetning eller teknisk lagring, s 12.
[64] Prop. 2019/20:201 Tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter, s 12.
[65] Jfr även avsnitt 5.5.5 denna vägledning.

Hur tystnadsplikten är reglerad och möjligheten att utdöma straffrättsligt ansvar är särskilt intressant vid utkontraktering till utländska leverantörer eller underleverantörer. I förarbetena[66] till tystnadspliktslagen framhålls att frågan om ett brott mot tystnadsplikt som begås utanför Sveriges gränser kan bedömas av svensk domstol eller inte avgörs utifrån den generella regleringen av tillämpligheten av svensk lag i 2 kap. BrB. Det innebär normalt, för sådana brott mot tystnadsplikten som begås utomlands, att svensk domsrätt kommer att finnas om brottet begås av en svensk medborgare eller av en någon med hemvist i Sverige. Som ett ytterligare krav gäller att gärningen ska vara straffbar även på gärningsorten, s.k. dubbel straffbarhet. Enligt 2 kap. 3 § 1 st. 4 BrB är svensk domstol behörig att döma över ett brott som har begåtts utomlands trots att det inte föreligger dubbel straffbarhet, om brottet har riktats mot ett svenskt allmänt intresse. Det kan finnas många situationer där det kan sättas i fråga om ett röjande av uppgifter är att anse som ett brott riktat mot svenska intressen, exempelvis röjande av enstaka namn eller adressuppgifter. Enligt eSams uppfattning är det därför viktigt att fortsatt reglera tystnadsplikt i avtal för de fall där brott mot tystnadsplikten inte kan beivras.

Här behöver också övervägas effekten av en avtalsreglerad tystnadsplikt och vilket skydd den innebär för uppgifterna, detta särskilt i förhållande till extraterritoriell lagstiftning (se avsnitt 5.4.2.4).

5.4.2.4 Geografisk lokalisering och extraterritoriell lagstiftning

Var uppgifterna kommer att hanteras geografiskt kan ha betydelse. En viss geografisk lokalisering hos en leverantör kan vara olämplig, avseende vissa känsliga uppgifter.[67]

Det finns länder och rättsordningar som inte har samma syn som Sverige på mänskliga rättigheter såsom skyddet för privatlivet, vilket kan påverka möjligheten till skydd för uppgifterna. I samband med utkontraktering och i synnerhet då uppgifterna riskerar att överföras till tredjeland behöver vid olämplighetsbedömningen beaktas om utkontrakteringen innebär att det kan antas att personuppgifterna efter utlämnandet kommer att behandlas i strid med dataskyddsförordningen eller dataskyddslagen, jfr det sekretesskydd som finns i 21 kap. 7 § OSL.

Territorialprincipen har fått en något annan innebörd än vad den haft historiskt sett vad gäller en stats möjlighet att bereda sig tillgång till elektronisk information som är lagrad i andra länder. Detta bland annat mot bakgrund av hur globala leverantörer tillhandahåller it-tjänster, såsom molntjänster, närmast oberoende av nationsgränser.

[66] Prop. 2019/20:201 Tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter, s 20.
[67] SOU 2018:25 Juridik som stöd för förvaltningens digitalisering (Digitaliseringsrättsutredningen), s 378-379.

Förutsättningarna har ändrats så att beslut om att ett företag ska lämna uppgifter i vissa fall kan fattas av ett utländskt offentligt organ med bindande verkan enligt utländsk rätt och riktas direkt mot ett företag som enligt utländsk rätt anses vara omfattat av utländsk jurisdiktion, oberoende av var i världen data finns lagrade eller annars tillgängliga. Det kan således avse information som en svensk myndighet har utkontrakterat till ett företag som omfattas av ett sådant beslut. Den svenska myndigheten skulle i vissa fall inte ens få vetskap om att informationen har lämnats ut till annan stats offentligrättsliga organ från leverantören och har ingen möjlighet att överklaga ett sådant belsut. Som exempel på sådana extraterritoriella lagstiftningar kan nämnas US CLOUD Act[68] och sektion 702 av Foreign Intelligence Surveillance Act (FISA 702).[69]

En aspekt som myndigheten måste beakta är således också om det finns lagar och regler i andra länder som kan påverka möjlighetena att skydda uppgifterna. Det kan uppstå en situation där reglerad tystnadsplikt ställs mot andra länders lagstiftning, vilket gör det svårt för en tjänsteleverantör eller underleverantör att efterleva lagstadgad tystnadsplikt eller uppfylla en avtalsreglerad tystnadsplikt. I avsaknad av prejudicerade fall förespråkar eSam en försiktighet i en situation av nämnda slag. Uppgifternas karaktär och det intresse som sekretessen avser att skydda behöver noga övervägas. Utkontraktering av sekretessreglerade uppgifter till en leverantör som omfattas av extraterritoriell lagstiftning som kan innebära att uppgifterna röjs för utomstående är enligt eSams uppfattning en omständighet av vikt som behöver beaktas i olämplighetsbedömningen.

Diskussionerna i samband med utkontraktering till utländska aktörer har ofta avsett länder utanför EU/EES med extraterritoriell lagstiftning och särskilt har lyfts den amerikanska lagstiftningen såsom Cloud Act och FISA 702. Ur sekretesshänseende är det dock inte bara länder utanför EU/EES som är problematiska och i synnerhet inte när den utkontrakterande myndigheten ska göra bedömningen av om det är olämpligt enligt 10 kap. 2 a § OSL eller vid en prövning av sekretessbestämmelsens rekvisit om det saknas en sekretessbrytande bestämmelse (se avsnitt 5.5). Skälet till det är att det med stor sannolikhet finns lagstiftning i andra länder som ger myndigheter i dessa länder rätt att ta del av uppgifter som finns i landet oavsett om uppgifterna lagras där för en utländsk myndighets räkning. Även här behöver beaktas risk för att tystnadsplikten inte kan efterlevas på grund av motstridiga lagstiftningar. I sammanhanget behöver

[68] U.S. CLOUD Act och anknytande reglering ger amerikanska myndigheter möjlighet att begära att bl.a. leverantörer av elektroniska kommunikationstjänster och molntjänster som är underkastade amerikansk jurisdiktion, bevarar eller lämnar ut data som är under leverantörens kontroll.

[69] Sektion 702 i den aktuella rättsakten möjliggör för amerikanska underrättelsemyndigheter att samla in information om icke-amerikanska medborgare som rimligen kan antas befinna sig utanför USA. Amerikanska myndigheter kan efter ett domstolsbeslut inhämta och spara en EU-medborgares personuppgifter utan att bevisa sannolika skäl till behörig domstol. De företag som ska verkställa besluten att lämna ut information måste hemlighålla sin delaktighet. Det saknas juridiska eller administrativa vägar för individer vars personuppgifter inhämtas att få kännedom om inhämtningen.

myndigheten dock beakta att det inte ställs krav gentemot aktörerna som inte är förenliga med upphandlingslagstiftningen.

En del av bedömningen blir således att ta ställning till var myndigheten kan godta att uppgifterna lagras och om det bedöms vara godtagbart att uppgifterna lagras utomlands och i så fall i vilka länder det inte kan anses vara olämpligt. Även om uppgifterna lagras i Sverige behöver den utkontrakterande myndigheten fundera över och kravställa kring leverantörens bolagsstruktur så att uppgifterna inte kan begäras direkt från leverantören enligt utländsk rätt.

5.4.2.5 Avvägning utifrån kända faktorer och upphandlingskrav

Det är således en mycket bred och omfattande bedömning som den enskilda myndigheten ska företa. Enligt eSams uppfattning måste ändå en viss avvägning göras med avseende på vad som är rimligt att beakta i en olämplighetsbedömning. Detta bör även kunna uttolkas av lagrådets uttalande kring lämpligt jämfört med olämpligt. En myndighet kan endast beakta för denne kända förhållanden. Den sekretessbrytande bestämmelsen är införd för att hjälpa myndigheter att säkert utföra utkontraktering av it-drift. Ett exempel på ett förhållande som kan vara svårt för den utkontrakterande myndigheten att värdera är vid samordnad it-drift hos en annan myndighet och frågor om hur den levererande myndigheten hanterar andra myndigheters uppgifter. Även om den myndighet som ska utkontraktera frågar hur uppgifterna kommer att hanteras mer specifikt hos leverantören kan leverantören inte alltid precist tillhandhålla den informationen, eventuellt på grund av egen tystnadsplikt kring det mer allmänna förhållandet av driften. Med det sagt ska en olämplighetsbedömning naturligtvis inbegripa samtliga kända faktorer och myndigheten får anses ha en rimlig undersökningsplikt. I undersökningspliken får anses ligga att efterfråga och samla in information och utifrån den värdera om det finns anledning till ytterligare undersökning.

I sammanhanget ska också framhållas att en myndighet som avser att genomföra en upphandling avseende utkontraktering måste göra dessa överväganden på ett generellt plan och i upphandlingen ställa krav på leverantören och tjänsten för att säkerställa att utkontrakteringen inte är olämplig, oavsett leverantör.

5.4.2.6 Dokumentation

Ett viktigt moment i utkontrakteringen är att den utkontrakterande myndigheten på ett tillförlitligt sätt dokumenterar den utredning och bedömning som myndigheten företagit inför utkontrakteringen. Svåra avvägningar kan behöva göras men om det finns ett

noggrant underlag som en bedömningsgrund för de respektive val myndigheten har gjort är det en mycket bra grund för en robust och säker utkontraktering.[70]

5.5 Prövning av sekretessbestämmelsens rekvisit

Om uppgifter inte kan lämnas ut med stöd av 10 kap. 2 a § OSL måste myndigheten utreda om den information som genom utkontrakteringen röjs för tjänsteleverantören är *sekretessbelagd*. Myndigheten måste alltså avgöra om sekretess gäller i det enskilda fallet, dvs. i förhållande till den tänkta tjänsteleverantören. Med andra ord måste myndigheten pröva om sekretessbestämmelsens rekvisit är uppfyllda.

En sekretessbestämmelse består i regel av tre huvudsakliga rekvisit, dvs. förutsättningar för bestämmelsens tillämplighet. Dessa rekvisit anger sekretessens föremål,[71] dess räckvidd[72] och dess styrka. Styrkan bestäms i regel med hjälp av s.k. skaderekvisit, vilket innebär en prövning av om ett utlämnande kan ske utan att det medför skada eller men för det intresse som sekretessen avser att skydda. Man skiljer i detta sammanhang mellan raka och omvända skaderekvisit. Vid rakt skaderekvisit är utgångspunkten att uppgiften är offentlig och att sekretess gäller bara om det kan antas att en viss skada uppstår om uppgiften lämnas ut. Vid omvänt skaderekvisit är utgångspunkten den motsatta, dvs. att uppgiften som utgångspunkt är sekretessbelagd. Uppgiften får då lämnas ut endast om det står klart att uppgiften kan röjas utan att viss skada uppstår.

5.5.1 Absolut sekretess

Sekretessen kan även vara absolut, vilket innebär att sekretessbestämmelsen är utformad så att den saknar skaderekvisit.

Uppgifter som omfattas av absolut sekretess får inte röjas utan stöd av en sekretessbrytande bestämmelse, även om det i det enskilda fallet skulle kunna konstateras att ett röjande inte skulle skada det intresse som sekretessen avser att skydda. Sådan sekretess gäller alltså även gentemot en utförare i samband med utkontraktering. Om utkontrakteringen innefattar uppgifter som omfattas av absolut sekretess är det således inte möjligt att genomföra utkontrakteringen, såvida det inte finns en sekretessbrytande bestämmelse till stöd för utlämnandet eller om uppgifterna kan krypteras så att röjande inte sker (se avsnitt 5.3.3).

[70] Prop. 2022/23:97 Sekretessgenombrott vid utlämnande för teknisk bearbetning eller teknisk lagring, s 17.
[71] Sekretessens *föremål* är den information som kan hemlighållas och anges i lagen genom ordet ”uppgift” tillsammans med en mer eller mindre precisering av uppgiftens art.
[72] Räckvidden bestäms normalt genom att det i bestämmelsen preciseras att sekretessen för de angivna uppgifterna gäller i viss typ av ärende, i en viss typ av verksamhet eller hos viss myndighet. Några sekretessbestämmelser gäller utan att räckvidden är begränsad.

5.5.2 Prövning av skaderekvisit

Konstruktionen med skaderekvisit innebär att vetskap om vem som är mottagare, vad mottagaren ska göra med uppgiften och hur uppgiften kommer att hanteras kan påverka bedömningen av om skaderekvisitet i sekretessbestämmelsen är uppfyllt eller inte.

Vid utkontraktering som kräver eller innebär att en större mängd uppgifter av samma typ görs tillgänglig för utföraren, kan prövningen av om den aktuella sekretessbestämmelsens skaderekvisit är uppfyllt i det enskilda fallet ske enligt en schabloniserad prövningsmodell.[73] Myndigheten vet vem utföraren är, hur denne kommer att hantera uppgifterna och vilken risk för ytterligare spridning som finns. Dessa kunskaper, tillsammans med en bedömning av den skaderisk som *typiskt sett* är förbunden med uppgifter av aktuellt slag, kan i de allra flesta fall ge fullt tillräckligt underlag för bedömningen av om sekretessbestämmelsens skaderekvisit är uppfyllt och om sekretess därmed gäller gentemot utföraren i fråga.

Avgörande betydelse bör alltså som regel tillmätas de *aktuella uppgifternas art och deras känslighet*.[74] Av särskilt intresse vid prövningen av om ett skaderekvisit är uppfyllt är också *hur uppgifterna hos mottagaren skyddas mot ytterligare spridning*, dvs. om mottagaren får lämna uppgiften vidare och själv utnyttja den eller om dessa befogenheter är begränsade.

Sådana begränsningar kan framgå bl.a. av författning (t.ex. bestämmelser som tystnadsplikt se avsnitt 5.5.4) eller beslut om utlämnande med förbehåll enligt 10 kap. 14 § OSL (se avnitt 6.5.2). Myndigheten kan också sluta avtal med privata tjänsteleverantörer innehållande begränsningar, se avsnitt 5.5.3. Dessa begränsningar kan innebära att det kan bedömas att skaderekvisiten inte är uppfyllda och utkontraktering därmed är möjlig.

Vid en prövning av sekretessbestämmelsens rekvisit behöver den utkontrakterande myndigheten fundera över vilka krav som ska ställas beträffande var uppgifterna kan lagras och huruvida en utländsk leverantör kan godtas. I denna del bör liknande överväganden som vid olämplighetsbedömningen enligt 10 kap. 2 a § OSL kunna aktualiseras, se avsnitt 5.4.2.

5.5.3 Avtalsrättsliga och tekniska begränsningar

Myndigheten kan sluta avtal med privata tjänsteleverantörer med begränsningar i klausuler om tystnadsplikt eller behandlingsförbud, kompletterade med sekretessförbindelser med tjänsteleverantörens personal avseende tystnadsplikt. Det kan

[73] Jfr. prop. 2022/23:97 Sekretessgenombrott vid utlämnande för teknisk bearbetning eller teknisk lagring, s 7-8.
[74] Prop. 1979/80:2 med förslag till sekretesslag m.m., del A s. 80 f.

också regleras vilken personal hos leverantören som ska ges åtkomst till uppgifterna, samt krav på noggranna processer och rutiner för denna personals hantering av det system som omgärdar uppgifterna. Vidare bör tekniska begränsningar, såsom begränsningar i åtkomsten göras. Begränsningar kan också finnas i instruktioner om hur uppgifter får eller ska behandlas enligt personuppgiftsbiträdesavtal och säkerhetsskyddsavtal. Avtalsbestämmelserna kan variera beroende på uppgifternas art och känslighet och kan utformas på olika sätt, men generellt kan bestämmelser i avtalet med tjänsteleverantören om kännbart vite vara lämpligt.

5.5.4 Reglering av tystnadsplikt och behandlingsförbud

Författningsbestämmelser om tystnadsplikt för personal i privaträttsligt bedriven verksamhet finns exempelvis i 8 kap. 4 § rättegångsbalken avseende advokater samt i 29 kap. 14 § skollagen (2010:800), 15 kap. 1 § socialtjänstlagen (2001:453), 6 kap. 12 § patientsäkerhetslagen och 15 § lagen (1997:736) om färdtjänst, avseende enskilt bedriven skolverksamhet, socialtjänst, hälso- och sjukvård respektive färdtjänst. Som nämnts i avsnitt 5.4 finns också bestämmelser i tystnadspliktslagen, men som är begränsade till utkontraktering av uppgifter för teknisk bearbetning eller teknisk lagring.

För offentliga funktionärer kan tystnadsplikt bara regleras i lag eller, efter bemyndigande i lag, i annan författning. Inskränkningar för mottagande myndighet i rätten att behandla en viss uppgift kan däremot i princip införas genom överenskommelse med den myndigheten, men får inte tillämpas om det t.ex. skulle stå i strid med mottagande myndighets skyldighet att pröva en begäran om utlämnande av allmän handling. Sådana överenskommelser saknar således rättslig verkan i fråga om utlämnande av allmän handling med stöd av offentlighetsprincipen.

Tystnadsplikt för privatanställda kan med bindande verkan regleras i avtal.[75] På motsvarande sätt kan privatanställdas rätt att behandla en uppgift inskränkas genom avtal.

5.5.5 Särskilt skyddsvärda uppgifter

En avtalsreglerad tystnadsplikt bör i många fall vara tillräckligt för att skaderekvisitet inte ska anses vara uppfyllt gentemot tjänsteleverantören.[76] Enbart en avtalsreglerad tystnadsplikt, som alltså inte är straffsanktionerad, skulle dock sannolikt betraktas som otillräcklig för att skydda *särskilt skyddsvärda, mycket integritetskänsliga, uppgifter*, se JO:s beslut den 9 september 2014, dnr 3032-2011. I de av JO granskade avtalen ingick i

[75] Av prop. 1979/80:2 med förslag till sekretesslag m.m., del A s. 128 följer att då mottagaren inte omfattas av någon lagreglerad tystnadsplikt och det heller inte är möjligt att lämna ut uppgifterna med förbehåll enligt offentlighets- och sekretesslagen, får behovet av tystnadsplikt när det är möjligt tillgodoses i civilrättslig ordning genom avtal om tystnadsplikt.
[76] E-delegationen, Fi 2009:01/2015/4, s. 5 och 57.

uppdraget att leverantörens personal skulle ta del av uppgifter med sekretess med omvänt skaderekvisit. På motsvarande sätt skulle avtalsreglerad tystnadsplikt kunna anses otillräcklig för att skydda sådana uppgifter som har ett särskilt uttalat skyddsbehov med hänsyn till Sveriges internationella relationer eller rikets säkerhet, se dock 19 kap. BrB.

Det har för sådana situationer resonerats kring om det skulle kunna vara möjligt att även beakta om mottagaren är bunden av någon annan straffsanktionerad bestämmelse som i praktiken får samma effekt som tystnadsplikt, dvs. en motsvarande *straffsanktionerad befogenhetsinskränkning*. Bland annat har resonerats kring bestämmelsen i 10 kap. 5 § BrB om trolöshet mot huvudman och dataintrång enligt 4 kap. 9 c § BrB.[77]

Vid bedömningen av vilka uppgifter som är av sådant särskilt skyddsvärt slag att avtalsreglerad tystnadsplikt kan anses vara otillräcklig, bör enligt eSams mening viss ledning kunna hämtas från de resonemang som förts i samband med den aktuella sekretessbestämmelsens införande. Sekretessens styrka, dvs. om skaderekvisitet är rakt eller omvänt, kan också ge vissa indikationer i detta avseende, även om långt ifrån alla uppgifter som skyddas av omvänt skaderekvisit kan anses vara av denna särskilt skyddsvärda karaktär.

5.6 Andra sekretessbrytande bestämmelser

Om en prövning enligt 10 kap. 2 a § OSL, eller en prövning av sekretessbestämmelsens rekvisit, inte ger stöd för ett utlämnande får prövning ske om det finns någon annan sekretessbrytande bestämmelse som skulle kunna tillämpas för att möjliggöra en utkontraktering.

5.6.1 Uppgiftsskyldighet eller tillämpning av generalklausulen

Om utkontrakteringen innebär att sekretessbelagda uppgifter ska lämnas till en annan *myndighet* kan 10 kap. 28 § OSL eller 10 kap. 27 § OSL bli aktuella. Det vill säga om det föreligger en skyldighet enligt lag eller förordning för myndigheten att lämna ut uppgifterna eller om det är uppenbart att intresset av att uppgifterna lämnas ut har företräde framför det intresse som sekretessen ska skydda, utlämnande med stöd av den s.k. generalklausulen. Det bör noteras att 10 kap. 27 § OSL inte är tillämplig om sekretess gäller enligt de i 10 kap. 27 § 2 st. OSL angivna bestämmelserna. Bestämmelsen ska inte heller användas rutinmässigt annat än i undantagsfall.[78]

[77] E-delegationen, Fi 2009:01/2015/4, s 46 ff.
[78] Prop. 1979/80:2 med förslag till sekretesslag m.m., del A s. 327.

5.6.2 Förbehåll

Om det vid utkontraktering till en *enskild aktör* uppstår ett behov av att tjänsteleverantören vidtar en *enstaka* åtgärd som kräver att denne faktiskt tar del av sekretessbelagda uppgifter, kan myndigheten överväga möjligheten att lämna ut uppgifterna med stöd av 10 kap. 14 § OSL, dvs. med förbehåll om att mottagaren inte får lämna uppgifterna vidare eller utnyttja dem. Ett sådant *förbehåll kan inte meddelas i förväg för en viss typ av information*, utan ska föregås av en prövning i varje särskilt fall. Vidare är konstruktionen över huvud taget möjlig endast om

- tjänsteleverantören är en enskild aktör,
- utlämnandet sker till en utpekad fysisk person, t.ex. en anställd hos tjänsteleverantören,
- det kan konkretiseras vilka uppgifter som lämnas ut,
- uppgifterna skyddas av en sekretessbestämmelse som är försedd med skaderekvisit (dvs. inte av absolut sekretess) och det kan konstateras att den risk för skada, men eller annan olägenhet som kan antas uppstå vid ett utlämnande undanröjs genom förbehållet, och
- förbehållet meddelas som ett formligt beslut och inte ges karaktären av ett civilrättsligt avtal.

Dessa begränsningar medför att förbehållslösningen endast i undantagsfall kan tillämpas vid utlämnande av uppgifter i samband med utkontraktering.

5.6.3 Nödvändigt utlämnande

Sekretess hindrar inte 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*, dvs. de uppgifter som följer av myndighetens instruktion, andra författningar, regleringsbrevet eller andra särskilda regeringsbeslut. Detta framgår av den sekretessbrytande bestämmelsen i 10 kap. 2 § OSL. Bestämmelsen ska dock användas restriktivt. Enbart en bedömning att effektiviteten i myndighetens handlande nedsätts på grund av sekretess får enligt uttalanden i förarbetena inte leda till att sekretessen åsidosätts.[79]

Att bestämmelsen ska tillämpas restriktivt är dock enligt eSams mening inte detsamma som att den ska tillämpas endast i situationer av undantagskaraktär. Enligt förarbetena

[79] Lagrådets yttrande, se prop. 1979/80:2 med förslag till sekretesslag m.m., del A s. 465.

kan det t.ex. i särskilda fall vara ”nödvändigt” för en tjänsteman att vända sig till en utomstående expert och att då upplysa om hemliga omständigheter.[80]

Det bör dock poängteras att myndigheten alltid noggrant måste överväga sådana alternativ som innebär ett röjande av sekretessbelagda uppgifter. Även om utkontraktering skulle medföra något lägre kostnader eller något högre effektivitet än ett annat fullt genomförbart alternativ, torde inte det vara tillräckligt för att utkontrakteringen, och därmed tillgängliggörandet av uppgifter, skulle anses vara ”nödvändig” i den mening som avses i 10 kap. 2 § OSL. För detta krävs i praktiken att utkontraktering framstår som den enda realistiska lösningen.

[80] Prop. 1979/80:2 med förslag till sekretesslag m.m., del A s. 122.

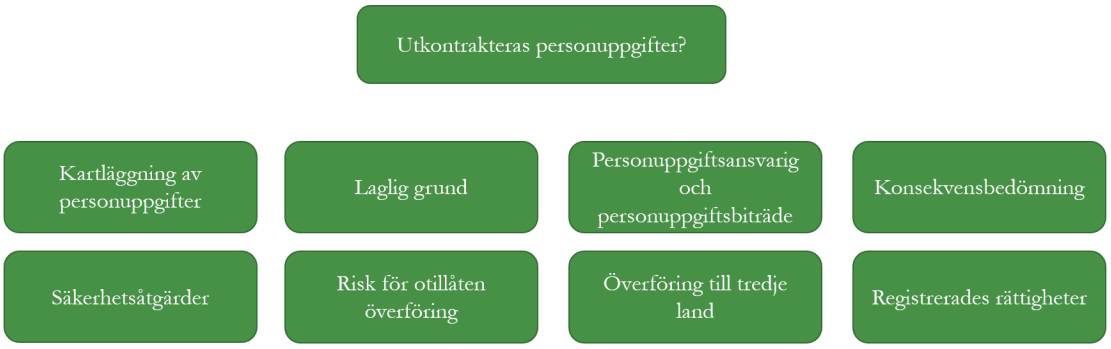
6. Skydd av personuppgifter

6.1 Utkontraktering och personuppgifter

Skyddet för den enskildes personliga integritet och respekten för privatlivet är viktiga grundläggande rättigheter som kommer till uttryck i både 2 kap. 6 § regeringsformen (RF) och artikel 8 i Europakonventionen.[81] Bestämmelser om behandling av personuppgifter finns i dataskyddsförordningen, dataskyddslagen (2018:218) med tillhörande förordning samt myndighetsspecifika registerförfattningar. Reglering finns också i brottsdatalagen (2018:1177), avsnitt 6 har dock avgränsats till en genomgång utifrån dataskyddsförordningen. Med personuppgifter avses varje upplysning som avser en identifierad eller identifierbar nu levande fysisk person (en registrerad).[82]

Vid all utkontraktering som innebär att personuppgifter behandlas av tjänsteleverantören måste regelverket rörande behandling av personuppgifter beaktas.

Vid sådan utkontraktering som är av särskilt intresse för e-förvaltningen, kan det antas att det mer eller mindre regelmässigt är så att tjänsteleverantören ska utföra vissa behandlingar av personuppgifter. Det gäller även om uppdraget bara avser teknisk lagring, eftersom även lagring av personuppgifter är en åtgärd som enligt artikel 4.2 i dataskyddsförordningen utgör behandling.



6.2 Kartläggning av personuppgifter inför utkontraktering

Inför en utkontraktering behöver det göras en kartläggning av den personuppgiftsbehandling som utkontrakteringen medför. Kartläggningen är en förutsättning för att bedöma *rättslig grund*, bedöma om personuppgifter behandlas i *förenlighet* med de grundläggande principerna för dataskydd, avgöra vilka *riskminimerande*

[81] Se även artikel 7 och 47 Europeiska unionens stadga om de Grundläggande rättigheterna.
[82] Av definitionen i artikel 4.1 följer vidare att en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller online-identifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

åtgärder som krävs för att behandlingen ska kunna genomföras, fastställa vilka *ytterligare bestämmelser* som behöver uppfyllas i dataskyddsförordningen, exempelvis bestämmelser om när känsliga personuppgifter får behandlas, och om när en *konsekvensbedömning* ska genomföras, samt avgöra vilka av de *registrerades rättigheter* som gäller för den aktuella behandlingen och tillgodose dessa.

6.2.1 Vilka personuppgifter kommer att behandlas?

Exempel på uppgifter som kan utgöra personuppgifter och som kan förekomma vid en utkontraktering, men som lätt kan missas, är kontaktuppgifter till arbetsplatsen, uppgifter som skapas vid användande av vissa tjänster samt uppgifter som har att göra med driften av tjänsterna, så kallad metadata, telemetridata och diagnostisk data.[83] Även IP-adresser är ofta personuppgifter.

Personuppgifter kan indelas i kategorier utifrån hur de regleras i dataskyddsförordningen, till dataskyddsförordningen kompletterande lagstiftning eller i OSL. Vissa personuppgifter behöver även särskiljas utifrån att de har en personlig karaktär som medför särskilda integritetsrisker. Myndigheten bör i kartläggningen urskilja följande kategorier;[84] känsliga personuppgifter,[85] personuppgifter som rör lagöverträdelser,[86] personnummer och samordningsnummer,[87] personuppgifter som omfattas av sekretess eller tystnadsplikt som syftar till att skydda enskildas personliga eller ekonomiska förhållanden, integritetskänsliga personuppgifter[88] och personuppgifter som rör särskilt skyddsvärda kategorier av registrerade, det kan t.ex. röra sig om barn eller patienter.

6.2.2 Hur omfattande är personuppgiftsbehandlingen?

Om personuppgifter som rör ett stort antal personer kommer att behandlas ökar riskerna med behandlingen, liksom om ett större antal uppgifter om varje person behandlas. Myndigheten behöver bedöma om det finns möjligheter att kartlägga en persons vanor, agerande eller annat med hjälp av de personuppgifter som behandlas och vara vaksam på om behandlingen innefattar geolokalisering eller insamling av metadata som kan avslöja saker om användare. Myndigheten behöver också vara uppmärksamma

[83] Se avsnitt 3.7 i rapporten 2022 Coordinated Enforcement Action, Use of cloud-based services by the public sector, Adopted on 17 January 2023. Telemetridata, eller diagnostisk information, definieras där som data som rör användningen av infrastrukturer eller tjänster, till exempel resursidentifierare, taggar, informations- och behörighetsroller, användarstatistik om olika typer av användare. När uppgifterna kan hänföras till en identifierad eller identifierbar nu levande fysisk person är de personuppgifter.
[84] Se även Integritetsskyddsmyndighetens beskrivning av kategorierna på myndighetens webbplats.
[85] Detta är aktuellt om uppgifterna avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening eller om de utgörs av biometriska uppgifter, uppgifter om hälsa eller om sexualliv eller sexuell läggning. Se vidare i artikel 9 i dataskyddsförordningen.
[86] Artikel 10 dataskyddsförordningen, kallas ibland särskilt skyddsvärda personuppgifter.
[87] 3 kap. 10-11 §§ dataskyddslagen, kallas ibland särskilt skyddsvärda personuppgifter.
[88] Integritetskänsliga personuppgifter är sådana personuppgifter som ligger nära den personliga sfären. Det kan t.ex. röra sig om privata ekonomiska uppgifter, utvärderingar såsom skriftliga omdömen, sociala förhållanden med mera. Se även skäl 75 i dataskyddsförordningen.

på att sök- och sammanställningsmöjligheter kan göra att personuppgifter blir mer känsliga än om de personuppgifter som behandlas ses ur ett isolerat perspektiv.

6.2.3 Vad händer med personuppgifterna?

Myndigheten behöver veta vad som händer med personuppgifterna inom ramen för utkontrakteringen. På vilket sätt kommer leverantören att behandla personuppgifterna? Styr myndigheten fortfarande över ändamål och medel för behandlingen i alla delar eller kommer leverantören i någon del att behandla personuppgifterna för egna syften?

Myndigheten behöver också ta reda på vilka som kommer att få del av personuppgifterna, t.ex. om personuppgifter överförs till underleverantörer, vilka dessa är och vad de gör med personuppgifterna. Det behöver särskilt noteras om personuppgifter överförs till tredjeland och därvid vara observanta på om underleverantörernas behandling medför en tredjelandsöverföring eller om tjänsten innefattar support som medför tredjelandsöverföring. Om en tjänsteleverantör eller underleverantör har säte i ett tredjeland bör myndigheten ta reda på om detta medför en risk för tillämpning av extraterritoriell lagstiftning som kan resultera i att personuppgifter överlämnas till myndigheter i tredjeland.

6.3 Rättslig grund och ändamål för myndighetens personuppgiftsbehandling

Efter att myndigheten har kartlagt personuppgiftsbehandlingen behöver den fastställa ändamålen med behandlingen, vilket styr med vilken rättslig grund de behandlas och gör det möjligt att bedöma om de grundläggande principerna i dataskyddsförordningen uppfylls.

Det är av vikt att myndigheten undersöker om rättslig grund föreligger i enlighet med dataskyddsförordningen för personuppgiftshanteringen som ska utkontrakteras. För att kunna göra detta behöver myndigheten vara klar över vad ändamålet är med personuppgiftsbehandlingen, eftersom det styr vilket stöd som finns i lagstiftningen. Frågan myndigheten ska ställa sig är: varför ska dessa personuppgifter behandlas? Som myndighet behöver behandlingen av personuppgifter kunna knytas till myndighetens uppdrag och den mer specifika lagstiftning som bestämmer hur myndigheten ska bedriva sin verksamhet. Anknytningen till myndighetens uppdrag kan innebära att det är en behandling som behövs för att myndigheten ska kunna fungera, såsom t.ex. rekrytering av medarbetare. Ändamålet får inte formuleras för brett eftersom det skulle innebära brist på träffsäkerhet i den rättsliga grunden och i uppfyllandet av de grundläggande principerna.

Den rättsliga grunden handlar om skäl som gör personuppgiftsbehandling för ett visst ändamål tillåten. Personuppgiftsbehandlingen måste vara nödvändig att utföra av dessa skäl. De vanligaste rättsliga grunderna för personuppgiftsbehandling som följer på myndigheters verksamhet är rättslig förpliktelse, myndighetsutövning och utförande av en uppgift av allmänt intresse. Enligt grunden rättslig förpliktelse ska myndigheten vara ålagd att uppfylla förpliktelsen genom lag eller annan regel, vilket kan gestaltas i EU-rätt, svensk rätt eller kollektivavtal. Ännu en grund utgörs av myndighetsutövning och uppgifter av allmänt intresse. Myndighetsutövning ska grundas på lag, förordning eller andra författningar i form av EU-rätt eller svensk rätt. Även uppgifter av allmänt intresse ska ha stöd i lag eller annan författning, kollektivavtal eller beslut som meddelats med stöd av lag eller annan författning.

Om den lagliga grunden handlar om *varför* personuppgifter behandlas, handlar de grundläggande principerna om *hur* de får behandlas. Några viktiga grundläggande principer för behandlingen av personuppgifter är att den måste ske i enlighet med de ursprungliga ändmålen för vilka personuppgifterna samlades in, fler personuppgifter får inte behandlas än vad som är nödvändigt utifrån ändamålen och personuppgifterna får inte sparas längre än vad som behövs i förhållande till ändamålen.

Myndigheten behöver också säkerställa att den tänkta behandlingen är förenlig med eventuell registerlagstiftning.

6.4 Personuppgiftsansvarig och personuppgiftsbiträde

Innan behandlingen påbörjas behöver det vara klart vilken part som är personuppgiftsansvarig[89] för behandlingen av personuppgifter och vilken part som är personuppgiftsbiträde. Det kan även vara fråga om ett gemensamt ansvar.[90] Ofta är den utkontrakterande myndigheten personuppgiftsansvarig och leverantören ett personuppgiftsbiträde. En utkontraktering kan även innebära att den personuppgiftsansvarige myndigheten överlämnar personuppgifter till en annan personuppgiftsansvarig och i vissa fall kan det vara svårt att bedöma vilken situation som är för handen.[91] Bedömningen behöver ske utifrån faktiska förhållanden. Om leverantören i någon del behandlar personuppgifter för egna syften, detta kan exempelvis gälla i förhållande till telemetri eller diagnostisk data[92] såsom framställande av

[89] Enligt artikel 4.7 i dataskyddsförordningen menas med personuppgiftsansvarig en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter. Om två eller flera personuppgiftsansvariga tillsammans fastställer ändamål och medel för personuppgiftsbehandlingen är de gemensamt personuppgiftsansvariga, artikel 26 dataskyddsförordningen.
[90] Artikel 26 i dataskyddsförordningen.
[91] Se EDPB:s riktlinjer 07/2020 angående begreppen personuppgiftsansvarig och personuppgiftsbiträde i GDPR samt Svenskt Näringslivs skrift Rollfördelning för korrekt personuppgiftsansvar (2019).
[92] Avsnitt 3.7 i rapporten 2022 Coordinated Enforcement Action, Use of cloud-based services by the public sector, Adopted on 17 January 2023.

användningsstatistik, och är att se som personuppgiftsansvarig, behöver myndigheten kunna visa att den har en rättslig grund för utlämnande av personuppgifter till leverantören för sådan behandling.

6.4.1 Personuppgiftsansvarig

Den som bestämmer över ändamålen och medlen för en personuppgiftsbehandling är personuppgiftsansvarig.

Det är primärt den personuppgiftsansvarige som ansvarar för att behandlingen av personuppgifter sker i enlighet med dataskyddsförordningens bestämmelser. Den personuppgiftsansvarige kan delegera uppgifter till personuppgiftsbiträdet, såsom att ge information till de registrerade, men är även i sådana fall den som är ansvarig för att dataskyddsförordningen uppfylls vid behandlingen.

Både den personuppgiftsansvarige och personuppgiftsbiträdet är ansvariga för att vidta tillräckliga tekniska och organisatoriska åtgärder för att skydda personuppgifterna.[93] Det är viktigt att myndigheten försäkrar sig om att tjänsteleverantören har förmåga att vidta lämpliga säkerhetsåtgärder och att detta verkligen sker. Det har föreskrivits i artikel 28.1 i dataskyddsförordningen att den personuppgiftsansvarige endast får anlita personuppgiftsbiträden som ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i förordningen och säkerställer att den registrerades rättigheter skyddas. Den personuppgiftsansvarige ansvarar för att det personuppgiftsbiträde den anlitar (med påföljande underbiträden) endast behandlar personuppgifter i enlighet med den ansvariges instruktioner.

6.4.2 Personuppgiftsbiträde

Den som behandlar personuppgifter för den personuppgiftsansvariges räkning utan att arbeta under dennes direkta ledning är ett personuppgiftsbiträde. Ett personuppgiftsbiträde befinner sig alltid utanför den personuppgiftsansvariges organisation.

Enligt artikel 28 i dataskyddsförordningen ska det finnas ett skriftligt avtal om personuppgiftsbiträdets behandling av personuppgifter för den ansvariges räkning. Det framgår av artikel 28.3 i dataskyddsförordningen vilka villkor som måste finnas med i

[93] Artikel 32 i dataskyddsförordningen.

personuppgiftsbiträdesavtalet. EU-kommissionen har också publicerat standardavtalsklausuler för hur ett personuppgiftsbiträdesavtal kan vara utformat.[94]

Personuppgiftsbiträdet har i dataskyddsförordningen getts ett självständigt ansvar för att vidta lämpliga tekniska och organisatoriska åtgärder,[95] att den som arbetar under biträdets ledning endast behandlar personuppgifter i enlighet med den personuppgiftsansvariges instruktioner,[96] att den personuppgiftsansvarige underrättas om personuppgiftsincidenter,[97] att föra en enklare förteckning över behandlingar som utförs för den personuppgiftsansvariges räkning,[98] att samarbeta med tillsynsmyndigheten[99] samt i vissa fall att utnämna dataskyddsombud.[100] I inget fall inskränks den personuppgiftsansvariges ansvar av personuppgiftsbiträdets ansvar. Både den personuppgiftsansvarige och personuppgiftsbiträdet kan bli skyldiga att betala ersättning till en registrerad som lidit skada till följd av en överträdelse av dataskyddsförordningen. För att ett personuppgiftsbiträde ska bli ersättningsskyldig måste det dock antingen handla om en överträdelse av någon av de bestämmelser som riktar sig direkt till personuppgiftsbiträden eller om personuppgiftsbiträdet inte följt den personuppgiftsansvariges instruktioner.

6.4.3 Underbiträde

Ett personuppgiftsbiträde kan i sin tur under vissa förutsättningar anlita s.k. underbiträden för att utföra personuppgiftsbehandling.[101] Det ska framgå av personuppgiftsbiträdesavtalet att anlitande av ett underbiträde antingen måste godkännas skriftligt av den ansvarige, eller att den ansvarige måste informeras innan ett underbiträde anlitats.[102] Underbiträden ska genom avtal åläggas samma skyldigheter avseende dataskydd gentemot den personuppgiftsansvarige som personuppgiftsbiträdet har. I likhet med personuppgiftsbiträdet ska underbiträdet ge tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder.[103]

Den personuppgiftsansvarige ansvarar för att kontrollera att såväl personuppgiftsbiträdet som underbiträden följer villkoren i personuppgiftsbiträdesavtalet och de krav som framgår av dataskyddsförordningen avseende bl.a. säkerhet. Det är därför viktigt att ta reda på förhållanden om underbiträden, såsom vilken lagstiftning de omfattas av.

---

[94] Kommissionens genomförandebeslut (EU) 2021/915 av den 4 juni 2021 om standardavtalsklausuler mellan personuppgiftsansvariga och personuppgiftsbiträden enligt artikel 28.7 i Europaparlamentets och rådets förordning (EU) 2016/679 och artikel 29.7 i Europaparlamentets och rådets förordning (EU) 2018/1725.
[95] Artikel 32.1 i dataskyddsförordningen.
[96] Artikel 32.4 i dataskyddsförordningen.
[97] Artikel 33 i dataskyddsförordningen.
[98] Artikel 30.2 i dataskyddsförordningen.
[99] Artikel 31 i dataskyddsförordningen.
[100] Artikel 37 i dataskyddsförordningen.
[101] Artikel 28.4 i dataskyddsförordningen.
[102] Artikel 28.3 i dataskyddsförordningen.
[103] Artikel 28.4 i dataskyddsförordningen.

Datainspektionen (numer Integritetsskyddsmyndigheten) har i tillsynsärendet 574-2011 uttalat att tredjepartsrevision kan vara ett sätt att kontrollera en tjänsts säkerhets- och kvalitetskrav men att detta inte fråntar den personuppgiftsansvariges ansvar att kontrollera att personuppgiftsbiträdet verkligen vidtar de säkerhetsåtgärder som krävs.[104]

6.5 Konsekvensbedömningar

För typer av behandlingar som innebär särskilt höga risker i relation till enskildas fri- och rättigheter ska en konsekvensbedömning (DPIA)[105] göras i enlighet med artikel 35 i dataskyddsförordningen. Konsekvensbedömningen ska genomföras innan behandlingen påbörjas och syftar till att åtgärda de risker som förknippas med behandlingen.[106]
När en myndighet utkontrakterar en del av sin verksamhet som innefattar behandling av personuppgifter kan det ofta röra sig om en behandling i stor omfattning (dvs. som rör mycket information om en personkrets eller många personer). Om personuppgifterna då även är känsliga eller av annat skäl särskilt skyddsvärda, talar det starkt för att en konsekvensbedömning ska genomföras inför utkontrakteringen. De enskilda medborgare som många myndigheter arbetar mot, t.ex. socialnämndernas brukare eller skattebetalare, har en utsatt ställning gentemot myndigheten och redan av det skälet bör behandling av deras personuppgifter (om den sker i större skala) föranleda en konsekvensbedömning. Vidare kan utkontraktering ofta involvera ny teknik, vilket nämns som ett observandum i artikel 35. Dessutom innebär utkontraktering i vissa fall att myndigheten förlorar en del kontroll över personuppgiftsbehandlingarna eftersom de blir exponerade för en kedja av personuppgiftsbiträden och underbiträden. Det senare kan ses som en generell ökning av risken vid behandling av personuppgifterna. Även andra faktorer vid en utkontraktering kan medföra höga risker och en skyldighet att göra en konsekvensbedömning.

6.6 Säkerhetsåtgärder enligt artikel 32 dataskyddsförordningen

Dataskyddsförordningen föreskriver som en av de grundläggande principerna för dataskydd att personuppgifter ska behandlas på ett sätt som säkerställer lämplig säkerhet, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av tekniska eller organisatoriska åtgärder.[107]

[104] Avsnitt 4.5 Kammarkollegiets Förstudierapporten Webbaserat kontorsstöd (dnr 23.2-6283-18).
[105] Data protection impact assessment.
[106] För en mer ingående vägledning, se Integritetsskyddsmyndighetens hemsida, www.imy.se.
[107] Artikel 5.1 f i dataskyddsförordningen (principen om integritet och konfidentialitet).

Principen har preciserats i artikel 32 i dataskyddsförordningen. När den personuppgiftsansvarige bestämmer en lämplig säkerhetsnivå ska denne beakta behandlingens art, omfattning, sammanhang och ändamål samt risken för fysiska personers fri- och rättigheter. Bland annat utgör behandling av känsliga eller integritetskänsliga personuppgifter en särskild risk.[108]

Exempel på åtgärder som kan vidtas för att skydda fysiska personers rättigheter och friheter mot risker vid behandlingen av personuppgifter är bland annat att uppgiftsbehandlingen minimeras, att personuppgifter pseudonymiseras och att öppenhet inför den registerade vidtas.[109] Åtgärderna bör säkerställa en lämplig säkerhetsnivå, med beaktande av den senaste utvecklingen och genomförandekostnaderna i förhållande till riskerna och vilken typ av personuppgifter som ska skyddas.[110]

6.7 Risk för otillåten tredjelandsöverföring

Dataskyddsförordningen ställer upp särskilda krav för att tredjelandsöverföringar ska vara tillåtet. Om det är fråga om en överföring tillämpas bestämmelserna i kapitel V i dataskyddsförordningen, se avsnitt 6.8.

Är det inte fråga om en överföring behöver den personuppgiftsansvarige ändå bedöma riskerna med behandlingen och lämpliga säkerhetsåtgärder med utgångspunkt från bland annat känsligheten hos personuppgifterna, jfr artikel 32 och 28 dataskyddsförordningen.[111] Om den personuppgiftsansvarige planerar att använda molninfrastruktur är ägandeförhållandena och förekomsten av extraterrioriell lagstiftning något som särskilt behöver bedömas.

Att uppgifter överförs till ett bolag i ett land inom EU/EES som har ett moderbolag i ett tredjeland, innebär inte att uppgifterna genom detta överförs till tredjeland enligt bestämmelserna i kapitel V i dataskyddsförordningen. Däremot kan det föreligga en risk för att personuppgifter otillåtet kan komma att föras över till tredjeland, t.ex. på grund av att molntjänstleverantören är bunden av lagstiftning i tredjeland som innebär att denne kan komma att behöva lämna ut personuppgifter till myndigheter i tredjeland, i strid med dataskyddsförordningen. Sådan lagstiftning finns t.ex. i USA, Kina och Ryssland. Om ett företag har ett moderbolag i någon av dessa länder är det möjligt att ländernas myndigheter skulle kunna bereda sig tillgång till personuppgifter som överförs till företaget inom ramen för tjänsten. Den personuppgiftsansvarige behöver utreda om en sådan risk föreligger, hur stor den är och vilken skada som en realisering av risken skulle

[108] Se skäl 75 i dataskyddsförordningen.
[109] Skäl 78 i dataskyddsförordningen.
[110] Skäl 83 i dataskyddsförordningen.
[111] Rekommendationer 01/2020 om åtgärder som komplement till överföringsverktyg för att säkerställa överensstämmelsen med EU-nivån för skydd av personuppgifter, Version 2.0, Antagna den 18 juni 2021, fotnot 42.

medföra för de registrerade. Om en risk för otillåten överföring föreligger behöver den personuppgiftsansvarige bedöma om det går att vidta tillräckliga säkerhetsåtgärder i enlighet med artikel 32 för att uppnå en lämplig säkerhetsnivå i förhållande till risken eller om behandlingen inte kan genomföras eftersom risken för de registrerades fri och rättigheter är för stor.

Om personuppgiftsbiträdet, eller underleverantörer som denne anlitar, lyder under lagstiftning som innebär att uppgifter måste lämnas ut till myndigheter i tredjeland kan det ifrågasättas om biträdet kan ge tillräckliga garantier för att personuppgifterna skyddas, så som föreskrivs i artikel 28.1 i dataskyddsförordningen. eSam menar att artikel 28.1 ska tolkas så att personuppgiftsbiträdet ska ge tillräckliga garantier för att en lämplig säkerhetsnivå (artikel 32) uppnås i förhållande till risken. För att bedöma om en lämplig säkerhetsnivå föreligger trots risken för olovlig överföring till tredjeland behöver den personuppgiftsansvarige i det enskilda fallet bland annat bedöma om de utländska myndigheterna genom personuppgiftsombudet faktiskt kan få tillgång till uppgifterna, sannolikhet för att de utländska myndigheter skulle begära åtkomst till uppgifterna och vilken skada för registrerades fri och rättigheter en otillåten åtkomst skulle kunna medföra. Offentliga uppgifter eller uppgifter som redan är kända kan generellt sett anses medföra en mindre risk i detta sammanhang, medan uppgifter som omfattas av sekretess eller annars integritetskänsliga uppgifter generellt kan anses medföra en stor risk.

Om risken med ett eventuellt utlämnande skulle vara för stor och den personuppgiftsansvarige och personuppgiftsbiträdet inte skulle kunna vidta tillräckliga åtgärder för att minska risken skulle behandlingen av personuppgifter inom ramen för det tjänsteavtalet även strida mot artikel 32.

Det är viktigt att i avtalet med tjänsteleverantören ha med regleringar som förbjuder tredjelandsöverföring och att förena detta med ett kännbart vite. Det är också önskvärt att reglera vad som gäller vid ett uppköp av den personuppgiftsansvarige som påverkar bedömningen av risken för otillåten tredjelandsöverföring (change of control-klausul).

6.8 Överföring av personuppgifter till tredjeland

Vid utkontraktering som innebär att personuppgifter förs över till tredjeland krävs att villkoren i kapitel V dataskyddsförordningen är uppfyllda, artiklarna 44-55.[112] Överföring får bara ske om:

1. EU-kommissionen har beslutat att landet säkerställer en adekvat skyddsnivå för personuppgifter enligt artikel 45 (s.k. adekvansbeslut),

[112] Med tredje land avses ett land som inte är medlem i EU/EES och därför inte omfattas av dataskyddsförordningens bestämmelser.

2. ett överföringsverktyg enligt artikel 46 används, eller
3. något av de undantag i särskilda situationer som anges i artikel 49 kan användas.

Vid alla överföringar till tredjeland behöver dessutom åtgärder vidtas i enlighet med artikel 32 för att skydda personuppgifterna vid överföringen.

Villkoren för överföring behandlas i följande avsnitt. En första fråga att bedöma är dock om det handlar om en överföring, dvs. om bestämmelserna i kapitel V dataskyddsförordningen är tillämpliga.

6.8.1 Överförs personuppgifter till tredjeland?

I dataskyddsförordningen definieras inte begreppet överföring till tredjeland närmare. Europeiska dataskyddsstyrelsen har däremot antagit en riktlinje som behandlar denna frågeställning.[113] För att utkontraktering ska anses medföra en överföring enligt dataskyddsförordningens kapitel V krävs:

1. att personuppgifterna överförs eller görs tillgängliga för en annan personuppgiftsansvarig eller ett personuppgiftsbiträde, och

2. att denne befinner sig i ett tredjeland.

Det krävs alltså att uppgifterna genom utkontrakteringen faktiskt överförs till ett tredjeland eller görs tillgängliga för en personuppgiftsansvarig eller ett personuppgiftsbiträde som befinner sig i ett tredjeland för att dataskyddsförordningens kapitel V ska vara tillämplig. Det senare innebär att även fjärråtkomst till uppgifterna utgör en överföring.[114] Som angetts i avsnitt 6.7 är det inte fråga om att uppgifter överförs till tredjeland om uppgifter överförs till ett bolag i ett land inom den EU/EES som har ett moderbolag i ett tredjeland, t.ex. USA.[115] Det är inte heller fråga om en överföring när en person som är anställd inom EU/EES arbetar från sin dator i ett tredjeland.[116]

En myndighet som utkontrakterar verksamhet måste vara mycket noggrann i sin analys av vilka uppgifter som kan komma att överföras till tredjeland vid anlitande av personuppgiftsbiträdet, även om biträdet finns inom EU/EES. Det förekommer t.ex. att support lämnas från ett moderbolag i tredjeland, vilket kan innebära att personuppgifter

[113] Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR.
[114] Rekommendationer 01/2020 om åtgärder som komplement till överföringsverktyg för att säkerställa överensstämmelsen med EU-nivån för skydd av personuppgifter, Version 2.0, Antagna den 18 juni 2021.
[115] Ägarförhållandena kan dock vara något som behöver beaktas i den riskanalys som beskrivs i det avsnittet.
[116] Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR.

görs tillgängliga på ett sätt som innebär överföring till tredjeland, eller att personuppgifter i personuppgiftsbiträdets verksamhet överförs till tredjeland för t.ex. analys eller statistik som ett led i utveckling och uppföljning av en molntjänst.

6.8.2 Överföring till tredjeland med adekvat skyddsnivå (adekvansbeslut)

Enligt artikel 45 dataskyddsförordningen får personuppgifter föras över till ett tredjeland om EU-kommissionen har beslutat att landet säkerställer en adekvat skyddsnivå för personuppgifter. Personuppgifter får då överföras utan något särskilt tillstånd och kan ske på samma sätt som om uppgifterna överfördes inom EU/EES. En förteckning över vilka länder som EU-kommissionen har beslutat säkerställer en adekvat skyddsnivå finns på EU-kommissionens webbplats.[117] Ett adekvansbeslut kan gälla ett visst territorium, en internationell organisation eller en eller flera sektorer i ett tredjeland.[118] Sådant beslut kan också vara utformat på olika sätt, i vissa fall kan tillämpningen av adekvansbeslutet vara förenat med en certifiering av företag, till vilka överföring är tillåten.[119]

Beslut om adekvat skyddsnivå är till alla delar bindande för samtliga medlemsstater och organ i medlemsstaterna och så länge som det inte har ogiltigförklarats.[120] I detta sammanhang kan nämnas att EU-domstolen i mål C-311/18 Schrems II underkänt ett beslut om adekvat skyddsnivå utifrån att övervakningslagstiftningen i USA ansågs vara för omfattande, oproportionerlig, och att det saknades rättsmedel för europeiska medborgare.[121]

För att EU-kommissionen ska kunna meddela ett adekvansbeslut ska landets (eller sektorns) skyddnivå bedömas vara väsentligen likvärdig med den skyddsnivå som gäller inom EU/EES. Därav krävs att landets lagstiftning uppfyller artiklarna 7, 8 och 45 i EU:s rättighetsstadga. När EU-kommissionen fattar beslut om adekvat skyddsnivå undersöks landets lagar och internationella åtaganden, vilka möjligheter den registrerade har att få rättslig prövning och om landet respekterar de mänskliga rättigheterna och de grundläggande friheterna. Vidare kontrollerar EU-kommissionen också att det finns oberoende tillsynsmyndigheter som ansvarar för att dataskyddsreglerna följs och som kan hjälpa de registrerade.[122] EU-kommissionen bedömer således genom sitt beslut att

[117] https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
[118] För närvarande har Kanada ett adekvansbeslut som gäller när landets lagstiftning för skydd av personuppgifter i privat sektor är tillämplig på mottagarens personuppgiftsbehandling, se Hur vet vi om ett tredjeland har adekvat skyddsnivå? (imy.se).
[119] Detta har varit fallet vid tidigare utformningar av adekvansbeslut som gäller för USA, och även för det senaste utkastet till ett sådant beslut.
[120] Se Schrems II st. 117, 118 och 156 samt 119, 120 och 157 om tillsynsmyndighet rätt att väcka talan i domstol för att få förhandsavgörande från EU-domstolen.
[121] EU-kommissionen har i december 2022 färdigställt ett förslag till beslut om adekvat skyddsnivå baserat på EU-USA Data Privacy Framework (ramverket), det vill säga EU:s överenskommelse med USA om åtgärder för att komma till rätta med bristerna som konstaterades i Schrems II samt inrättande av organisationers möjlighet till självcertifiering. Förslaget har beretts med Europaparlamentet (LIBE) och EDPB som lämnat en del kritiska synpunkter. EU-kommissionen har föreslagit att beslutet om adekvat skyddsnivå inte ska träda i kraft förrän förutsättningarna finns att genomföra den exekutiva ordern EO 14086 fullt ut i USA.
[122] Artikel 45.2 i dataskyddsförordningen.

det föreligger en adekvat skyddsnivå och det finns inte utrymme för den personuppgiftsansvariga att själv avgöra om det finns en adekvat skyddsnivå eller inte. EU-kommissionens beslut kan däremot prövas i EU-domstolen.

6.8.3 Överföring till tredjeland med stöd av lämpliga skyddsåtgärder

Enligt artikel 46 i dataskyddsförordningen får personuppgifter överföras till ett tredjeland som inte omfattas av ett beslut om adekvat skyddsnivå endast om lämpliga skyddsåtgärder vidtagits och på villkor att lagstadgade rättigheter och effektiva rättsmedel för registrerade finns tillgängliga.

Artikel 46 innehåller en förteckning över ett antal överföringsverktyg med ”lämpliga skyddsåtgärder” som personuppgiftsansvarige kan använda för att överföra personuppgifter till tredjeländer i avsaknad av ett beslut om adekvat skyddsnivå.

De viktigaste typerna av överföringsverktyg i artikel 46 är

- standardiserade dataskyddsbestämmelser, standardavtalsklausuler, som antagits av EU-kommissionen eller av tillsynsmyndighet och godkänts av EU-kommissionen. EU-kommissionen har publicerat antagna standardavtalsklausuler[123]
- uppförandekoder, (artikel 40, utarbetade av sammanslutningar som företräder kategorier av personuppgiftsansvariga eller personuppgiftsbiträden och godkända av behörig tillsynsmyndighet eller EU-kommissionen)
- certifieringsmekanismer (artikel 42, utfärdade av behörigt certifieringsorgan eller behörig tillsynsmyndighet)
- avtalsklausuler mellan personuppgiftsansvarig och personuppgiftsbiträdet som godkänts av behörig tillsynsmyndighet (IMY)

Vid överföring av personuppgifter med stöd av artikel 46 krävs det enligt EU-domstolens praxis (Schrems II) att den som gör överföringen säkerställer att personuppgifter som överförs får en väsentligen likvärdigt skydd som inom EU/EES. Den som överför personuppgifterna måste därför göra en konsekvensbedömning av dataöverföringar (TIA).[124] Konsekvensbedömningen ska bland annat innehålla en bedömning av tredjelandets lagar och praxis, om det finns oberoende tillsynsmyndigheter där och eventuella internationella åtaganden från tredjelandet. EDPB har gett ut rekommendationer 01/2020 om åtgärder som komplement till

[123] https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en
[124] Transfer Impact Assessment.

överföringsverktyg för att säkerställa överensstämmelsen med EU-nivån för skydd av personuppgifter.[125]

6.9 Registrerades rättigheter

Den personuppgiftsansvarige ansvarar för att den registrerades rättigheter enligt dataskyddsförordningen kan uppfyllas efter utkontrakteringen och måste därför se till att ha rådighet över detta. Vid all personuppgiftsbehandling ska de registrerade få information om behandlingen, både genom den personuppgiftsansvariges eget initiativ eller på begäran, om inte något undantag är tillämpligt.[126] Den registrerade har också alltid rätt att få felaktiga personuppgifter rättade.[127] Vad gäller rätt till radering, begränsning av behandling, och rätt att göra invändningar gäller de endast i begränsad omfattning när behandlingen stödjer sig på någon av de rättsliga grunder som vanligen gäller i myndigheters verksamhet.[128] Rätten till dataportabilitet[129] är endast aktuell för behandlingar som grundar sig på samtycke eller avtal med den registrerade. Vissa automatiserade beslut som inte har stöd i lagstiftningen får inte fattas.[130]

Myndigheten behöver tillse att myndighetens behandlingar är upptagna i registerförteckningen, artikel 30.

[125] Rekommendationer 01/2020 om åtgärder som komplement till överföringsverktyg för att säkerställa överensstämmelsen med EU-nivån för skydd av personuppgifter, Version 2.0, Antagna den 18 juni 2021.
[126] Artiklarna 12-15 i dataskyddsförordningen.
[127] Artikel 16 i dataskyddsförordningen.
[128] Artiklarna 17, 18, och 21 i dataskyddsförordningen.
[129] Artikel 20 i dataskyddsförordningen.
[130] Artikel 22 i dataskyddsförordningen.

7. Informationssäkerhet

Inför en utkontraktering måste regler om informationssäkerhet beaktas. Informationssäkerhet handlar om att skydda myndighetens information och fokuserar på tre principer.

- **Konfidentialitet**, att endast behöriga har åtkomst till informationen.
- **Riktighet**, att informationen är fullständig och att endast behöriga kan ändra den.
- **Tillgänglighet**, att behöriga har åtkomst till informationen när den behövs.

Vid en informationsklassning kartläggs vilka informationsmängder som kommer att hanteras vid en utkontraktering. Klassningen utmynnar i en värdering av risken (sannolikheten) samt konsekvensen om konfidentialitet, riktighet och tillgänglighet förloras för respektive informationsmängd. Det görs också en bedömning av vilka åtgärder som myndigheten kan och vill vidta för att minska risken för förlust samt för att minska skadeverkningarna om så ändå sker.

Informationssäkerhet handlar främst om riskvärdering och de tre principerna ska beaktas oavsett om informationen innehåller personuppgifter eller inte. Många gånger kan liknande riskbedömningar behöva göras som vid en prövning enligt dataskyddsreglerna och det kan finnas ett värde i att samköra processerna. Det är emellertid viktigt att förstå att prövningen görs ur olika perspektiv och utifrån olika regleringar. Förenklat uttryckt görs informationssäkerhetsprövningen ur ett myndighetsperspektiv, medan dataskyddsprövningen görs ur de registrerades perspektiv. Utfallet behöver därför inte bli detsamma.

Bestämmelser om informationssäkerhet finns i flera olika regelverk. I säkerhetsskyddslagen med tillhörande förordning finns regler som gäller för verksamhetsutövare av säkerhetskänslig verksamhet. Det är myndigheten själv som ska bedöma om den bedriver säkerhetskänslig verksamhet och det föreligger då en anmälningsskyldighet till tillsynsmyndigheten. Vilken myndighet som utövar tillsyn framgår av 8 kap. 1 § säkerhetsskyddsförordningen. Vid utkontraktering av säkerhetsskyddsklassificerade uppgifter finns särskilda regler att beakta, se bl.a. 4 kap. säkerhetsskyddslagen. I lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-lagen) med tillhörande förordning beskrivs allmänt de säkerhetsåtgärder som ska vidtas och de skyddsnivåer som ska uppnås i samhällsviktiga respektive digitala tjänster. De aspekter som ska beaktas av leverantörer av digitala

tjänster specificeras i en genomförandeförordning.[131] I NIS-lagen finns vidare föreskrifter om incidentrapportering, tillsyn och sanktioner. I slutet av år 2022 beslutade EU om ett nytt och bredare direktiv, NIS2-direktivet, som kommer införlivas i svensk lag under år 2024. NIS2-direktivet ersätter NIS-direktivet, som ligger till grund för nuvarande NIS-lag. Ytterligare regelverk om informationssäkerhet är förordningen (2022:524) om statliga myndigheters beredskap samt eIDAS-förordningen.[132] Enligt artikel 19 i eIDAS-förordningen ska tillhandahållare av betrodda tjänster vidta lämpliga tekniska och organisatoriska åtgärder för att hantera riskerna för säkerheten hos de betrodda tjänster de tillhandahåller.

Från ett övergripande perspektiv ser informationssäkerhetskraven i dessa författningar ut att vara likartade. Eftersom det handlar om ramlagstiftning är det inte möjligt att utläsa vilka konkreta krav på säkerhet som ställs. Det som regleras är i stället bestämmelser om övergripande mål, ansvarsförhållanden och allmänna krav på åtgärder i berörda verksamheter. Det vill säga att myndigheter och andra organ använder vissa arbetssätt – systematiskt och riskbaserat informationssäkerhetsarbete – och vidtar vissa åtgärder, t.ex. rapporterar incidenter.

I flera av regleringarna finns bemyndiganden för tillsynsmyndigheter att meddela närmare föreskrifter på området. För att komplettera lagstiftning på området och därmed underlätta tillämpning har flera sådana föreskrifter också tagits fram bland annat av Säkerhetspolisen, Försvarsmakten och Myndigheten för samhällsskydd och beredskap (MSB). Därutöver har även ytterligare stödjande material getts ut av tillsynsmyndigheterna. Säkerhetspolisen har gett ut vägledningar på säkerhetsskyddsområdet som kan fungera som stöd för verksamhetsutövare i tillämpningen av säkerhetsskyddsregelverket. Försvarsmakten har tagit fram kommentarer till sina föreskrifter och MSB har tagit fram vägledningar som ger stöd vid tillämpningen av NIS-regelverket. Det finns också standarder för ledningssystem för informationssäkerhet, bl.a. ISO/IEC 27001 och 27002.

[131] Kommissionens genomförandeförordning (EU) 2018/151 av den 30 januari 2018.
[132] Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG.

Bilaga 1 Checklista

Checklista, hantering av allmänna handlingar vid utkontraktering

- Innebär utkontrakteringen att allmänna handlingar uppstår?
- Innefattar utkontrakteringen hantering av allmänna handlingar?
  - Kan handlingarna bevaras på tillfredställande sätt?
  - Finns möjligheter till gallring?
  - Har myndigheten smidig tillgång till handlingarna?
  - Kan myndigheten vid behov ta tillbaka handlingarna?
  - Finns det risk att de allmänna handlingarna förloras eller obehörigen sprids?

Checklista, sekretessöverväganden vid utkontraktering

Är det fråga om sekretessreglerade uppgifter?

- Kommer uppgifterna att röjas?
- Är det fråga om en osjälvständig uppdragstagare?
- Kan uppgifterna krypteras på ett fullgott sätt gentemot leverantören?

Kan utkontraktering ske med stöd av den sekretessbrytande bestämmelsen i 10 kap. 2 a § OSL?

- Gäller det utkontraktering för teknisk bearbetning eller teknisk lagring?
  - Hanteras överlämnad information endast för uppdragsgivande myndighets räkning?
  - Är it-tjänstens karaktär enbart av teknisk natur?
  - Tillförs informationen något nytt eller kompletterande innehåll?
  - Förekommer hantering av samma uppgifter i något annat flöde hos leverantören och är det i så fall möjligt att hålla dessa flöden helt åtskilda?
- Är det olämpligt att utkontraktera för teknisk bearbetning eller teknisk lagring?
  - Är det fråga om uppgifter av känsligt slag?
  - Kan aggreggering innebära att den totala informationsmängden blir mer skyddsvärd?

- Finns det risk för att myndigheten avhänder sig kontroll över uppgifter i den samhällsbärande verksamheten?
- Förekommer underleverantörer och kan i så fall skyddet upprätthållas hos dessa?
- Finns det risk för att lag- eller avtalsreglerad tystnadsplikt inte kan efterföljas?
- Är den interna åtkomsten hos leverantören begränsad med tekniskt eller med organisatoriska rutiner?
- Kan leverantörens geografiska lokalisering påverka möjligheten att upprätthålla skyddet för uppgifterna?
- Är leverantören eller dess underleverantörer bundna av extraterritoriell lagstiftning eller annan lagstiftning som innebär att skyddet för uppgifterna inte kan upprätthållas?
- Har myndigheten tagit hänsyn till kända faktorer och vilka krav som är möjliga att ställa i en upphandling?
- Ger en allsidig bedömning utfallet att ett utlämnande inte är olämpligt?

Kan utkontraktering ske efter prövning av en sekretessbestämmelses rekvisit?

- Gäller s.k. absolut sekretess eller är sekretessbestämmelsen reglerad med ett skaderekvisit?
- Hur skyddsvärda är uppgifterna, typiskt sett?
  - Är det uppgifter av känslig art?
  - Har mottagaren rätt att lämna uppgifterna vidare eller själv utnyttja dem (dvs risk för spridning)
  - Kan avtalsmässiga och tekniska begränsningar göras?

Kan utkontraktering ske med stöd av någon annan sekretessbrytande bestämmelse?

- Om tjänsteleverantören är en myndighet, är utlämnandet en följd av en lag- eller förordningsreglerad uppgiftsskyldighet eller kan utlämnandet ske med stöd av den s.k. generalklausulen eller någon sektorsspecifik sekretessbrytande bestämmelse?
- Om tjänsteleverantören är en enskild aktör, kan uppgifterna lämnas med förbehåll att uppgifterna inte får lämnas vidare eller nyttjas av leverantören?
  - Är det fråga om en enstaka åtgärd?
- Oavsett om tjänsteleverantören är en myndighet eller en privaträttslig aktör, kan utlämnandet anses vara ”nödvändigt”?

- Kan myndighetens uppdrag rimligen fullgöras utan att utlämnande sker?
- Motiveras utlämnandet även av andra skäl än rent ekonomiska?
- Har alla alternativ till utlämnande övervägts noggrant?
- Framstår utkontrakteringen som den enda realistiska lösningen?

Checklista, dataskydd vid utkontraktering

- Ska tjänsteleverantören behandla personuppgifter?
  - Vilka personuppgifter kommer att behandlas?
  - Hur omfattande är behandlingen?
  - Vad händer med personuppgifterna?
- Finns laglig grund för utkontraktering av personuppgifterna?
- Finns det ett personuppgiftsbiträdesavtal enligt artikel 28 i dataskyddsförordningen?
  - Finns det tydliga instruktioner för varför och hur biträdet får behandla personuppgifter?
  - Får tjänsteleverantören anlita underleverantörer för behandling av personuppgifter?
- Behöver det göras en konsekvensbedömning?
- Har säkerhetsåtgärder enligt artikel 32 vidtagits?
- Föreligger risk för tredjelandsöverföring?
  - Kan biträdet ge tillräckliga garantier för att personuppgifterna skyddas, så som föreskrivs i artikel 28.1?
  - Går det att vidta tillräckliga säkerhetsåtgärder i enlighet med artikel 32?
  - Kan behandlingen genomföras eller är risken för stor?
- Är det fråga om överföring till tredjeland?
  - Finns ett adekvansbeslut?
  - Om inte adekvansbeslut finns, har lämpliga skyddsåtgärder vidtagits så att överföring är möjligt?
- Kan de registrerades rättigheter tillgodoses?

Checklista, informationssäkerhet vid utkontraktering

- Har informationsklassning och riskvärdering gjorts?
- Omfattas uppgifterna av säkerhetsskyddslagen?

Bilaga 2 Sekretessförbindelse avseende [Tjänsteleverantörens] anställda och uppdragstagare

Observera att denna mall till sekretessförbindelse endast kan tillämpas för privata leverantörer. Myndighetsanställdas tystnadsplikt regleras i OSL. Tänk på att förbindelsen kan behöva anpassas till regleringen i det enskilda avtalet med tjänsteleverantören.

Jag förbinder mig härmed gentemot [Tjänsteleverantören], till tystnadsplikt m.m. enligt följande:

Tystnadsplikten innebär att jag inte, vare sig under arbetstid eller på fritiden, nu eller senare, får avslöja sådan Konfidentiell information som jag har fått kännedom om till följd av [Tjänsteleverantörens] avtal med [Myndigheten] eller mitt arbete med [Myndigheten]. Jag får inte heller själv utnyttja sådan Konfidentiell information för egna eller andras syften.

Med "Konfidentiell information" avses dels varje uppgift som hos [Myndigheten] är sekretessreglerad enligt offentlighets- och sekretesslagen (2009:400), dels varje annan upplysning, oavsett om informationen lämnats skriftligen eller muntligen och oberoende av format, som jag erhåller, från [Myndigheten] eller någon anställd, annan befattningshavare eller rådgivare till [Myndigheten], i samband med mitt arbete med [Myndigheten]. Som Konfidentiell information anses inte information som,
a) vid tiden för förfogandet var allmänt känd, eller
b) jag kan visa redan var tillgänglig för mig vid tiden för förfogandet och som jag inte, direkt eller indirekt, har erhållit genom överträdelse av denna sekretessförbindelse.

Jag förbinder mig att inte medvetet ta fram information ur [Myndighetens] informationssystem, databaser eller handlingar utan uttryckligt tillstånd från [Myndigheten].

Jag är skyldig att följa [Tjänsteleverantörens] säkerhetsregler, exempelvis vad gäller rätten att ha tillgång till eller på olika sätt hantera utrustning och information.

Jag förbinder mig även att tillse att till mig anförtrott material inte kommer obehörig till del. Med obehörig avses alla (således även familjemedlem och kollega), som inte bedöms

behöva information inom ramen för [Tjänsteleverantörens] uppdrag gentemot [Myndigheten].

När mitt uppdrag upphör, kommer jag att återlämna allt som tillhandahållits mig i form av dokument, foton, elektronisk media, datafiler samt apparater och tilldelad utrustning. Jag förbinder mig vidare att radera alla elektroniska filer innehållande Konfidentiell Information.

Jag är fullt införstådd med ovanstående och är medveten om att brott mot denna tystnadsplikt m.m. kan medföra stor skada för enskilda individer och företag, liksom för [Tjänsteleverantörens] och [Myndighetens] verksamhet, och att det för mig personligen kan innebära straffansvar och skadeståndsskyldighet, samt skadeståndsskyldighet för [Tjänsteleverantören] och för [Myndigheten].

Bilaga 3 Nationella utredningar och ställningstaganden

Utkontraktering har behandlats i flera myndighetsrapporter, ställningstaganden och utredningar. Exempelvis kan nämnas:

- Pensionsmyndighetens rapport ”Molntjänster i staten, en ny generation av outsourcing” (VER 2015-157)
- Statens servicecenters rapport år 2017 ”En gemensam statlig molntjänst för myndigheternas it-drift”.
- eSams rättsliga uttalanden 2015, 2018 och 2019.[133]
- Rättsutredning om röjande vid användning av globala molntjänster av Setterwalls Advokatbyrå på uppdrag av Sveriges Kommuner och Regioner (SKR).
- Förstudierapport av Statens inköpscentral vid Kammarkollegiet om ”Webbaserat kontorsstöd” (dnr 23.2-6283-18)
- Försäkringskassans vitbok, Molntjänster i samhällsbärande verksamhet – risker, lämplighet och vägen framåt (dnr 013428-2019)
- Promemoria om ersättning av Skype i Skatteverkets och Kronofogdens verksamhet (Skatteverkets dnr 8-958696)
- It-driftsutredningens delbetänkande Säker och kostnadseffektiv it-drift – rättsliga förutsättningar för utkontraktering (SOU 2021:1).

[133] VER 2015-190, VER 2018:57 och Promemoria Kompletterande information om molntjänster, 2019-09-20.

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

Alla stöddokument finns på esamverka.se

I eSam ingår Arbetsförmedlingen, Arbetsmiljöverket, Bolagsverket, Boverket, Centrala Studiestödsnämnden, Domstolsverket, E-hälsomyndigheten, Ekonomistyrningsverket, Folkhälsomyndigheten, Försäkringskassan, Havs- och vattenmyndigheten, Inspektionen för vård och omsorg, Jordbruksverket, Kemikalieinspektionen, Kriminalvården, Kronofogdemyndigheten, Lantmäteriet, Länsstyrelserna, Migrationsverket, Naturvårdsverket, Patent- och Registreringsverket, Pensionsmyndigheten, Riksarkivet, Rättsmedicinalverket, Sida, Skatteverket, Skolverket, Statens institutionsstyrelse, Statens servicecenter, Statens tjänstepensionsverk, Statistiska centralbyrån, Tillväxtverket, Trafikverket, Transportstyrelsen, Tullverket och Universitets- och högskolerådet (feb 2023).