Juridisk analys

Innehåll

Bilaga 1 Juridisk analys av myndigheters informationshantering i molnet

Syftet med att placera den juridiska analysen i en bilaga är att på ett mer utförligt sätt kunna redogöra för vilka juridiska förutsättningar som måste vara uppfyllda för att en myndighet ska kunna hantera sin information i en molntjänst. Genomgången av relevanta författningar har emellertid inga ambitioner att vara uttömmande eftersom varje myndighet alltid, utifrån omständigheterna i det specifika fallet, måste utreda vilka lagar och regler som är tillämpliga vid myndighetens hantering av sin information. Urvalet av de lagar som analyseras här har gjorts mot bakgrund av att de i princip alltid aktualiseras när en myndighet avser att hantera sin information i en molntjänst. Trots bilagans omfattande sidantal innehåller redogörelsen i stort sett bara de bestämmelser i respektive lag som är särskilt relevanta i förhållande till molntjänster.

Framställningen följer i stora drag den legala prövning en myndighet behöver göra vid en bedömning av om det är lagligt och lämpligt att behandla en viss typ av information i en molntjänst.

1.1 Offentlighets- och sekretesslagstiftningen

En myndighet som anlitar en utomstående aktör, t.ex. en molntjänstleverantör, för att bearbeta, lagra eller på annat sätt hantera myndighetens information måste pröva om det är tillåtet att lämna ut informationen till leverantören i fråga och vilka eventuella konsekvenser ett utlämnande kan få. Utlämnandet måste vara förenligt med gällande sekretesslagstiftning för att vara lagligt. Vidare måste myndigheten ta ställning till om handlingarnas status kan komma att förändras i och med att de lämnas ut till en utomstående part.

1.1.1 Offentlighets- och sekretesslagen

Offentlighets- och sekretesslagen (2009:400, OSL) avser att ge en gemensam reglering av handlingssekretess och tystnadsplikt i den offentliga verksamheten. Sekretess innebär inte bara begränsningar av rätten att ta del av allmänna handlingar utan även ett förbud att röja en uppgift, oavsett om det görs muntligen, genom utlämnande av allmän handling eller på något annat sätt. Sekretessbestämmelserna i offentlighets- och sekretesslagen gäller således inte bara för uppgifter i allmänna handlingar, utan även för uppgifter som finns hos en myndighet i sådana handlingar som ännu inte har blivit allmänna. Röjandeförbudet aktualiseras därmed även för sekretessbelagda uppgifter i exempelvis arbetsmaterial, utkast och andra dokument som varken har expedierats eller på annat sätt kommit att bli upprättade i tryckfrihetsförordningens mening. För uppgifter som finns i handlingar som inte är allmänna är handlingssekretessen och tystnadsplikten dessutom inte tidsbegränsad.

Sekretess gäller som huvudregel inte bara i förhållande till enskilda utan också mellan myndigheter samt inom en myndighet, om där 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, 8 kap. 3 § OSL.

Sekretessbelagda uppgifter får inte röjas för utomstående, om inte annat anges i offentlighets- och sekretesslagen eller i lag eller förordning som offentlighets- och sekretesslagen hänvisar till. Detta gäller oavsett syftet bakom utlämnandet och oavsett om utlämnandet ska ske till en enskild person, ett företag eller en myndighet. Det

saknar betydelse om utlämnandet görs till en extern aktör som inte *behöver* ta del av innehållet i den information som görs tillgänglig, men det är oundvikligt att detta ändå kan komma att ske.

1.1.2 Allmänt om offentlighets- och sekretesslagen och molntjänster

En myndighet som har för avsikt att hantera sin information i en molntjänst måste göra vissa särskilda avvägningar. Vid en sekretessprövning är det t.ex. inte tillräckligt att myndigheten enbart prövar om sekretess gäller gentemot molntjänstleverantören. Myndigheten måste också ta ställning till om sekretess gäller gentemot eventuella underleverantörer som anlitas av molntjänstleverantören. Det kan antas vara förenat med stora svårigheter, om ens möjligt, för en utlämnande myndighet att göra en sådan bedömning i flera led. Generellt sett har en myndighet små möjligheter till insyn och kontroll av en molntjänstleverantörs hantering av myndighetens information. Detta gäller i synnerhet när informationen hanteras av globala molntjänstleverantörer. Om molntjänstleverantören dessutom använder sig av underleverantörer blir myndighetens möjlighet till insyn och kontroll i det närmaste obefintlig.

Om molntjänstleverantören kommer att lagra informationen utanför Sveriges gränser måste myndigheten också beakta att andra länders myndigheter, med stöd i sin egen nationella rättsordning, kan få åtkomst till informationen som lagras i det aktuella landet. Myndigheten måste därför ta ställning till om ett sådant potentiellt tillgängliggörande är förenligt med gällande sekretessbestämmelser.

Beroende på vilket uppdrag en molntjänstleverantör har för hanteringen av myndighetens information behöver myndigheten också ta ställning till om överföringen av uppgifter till leverantören innebär att handlingarna kommer att anses som expedierade och därmed upprättade, allmänna handlingar i tryckfrihetsförordningens (TF) mening. Om molntjänstleverantören utför annan behandling än enbart teknisk lagring eller bearbetning kan överföringen av information medföra att handlingar som tidigare inte varit allmänna hos myndigheten ändrar status.

I det följande redogörs för de allmänna och särskilda avvägningar i förhållande till sekretess m.m. som en myndighet måste göra vid användningen av molntjänster.

1.1.3 Skaderekvisit och skadeprövning

Vid sekretessreglernas utformning har man strävat efter att inte ge sekretessen större omfattning än nödvändigt. Sekretessen är till för att skydda vissa intressen och den bör gälla endast i den mån offentlighet skulle äventyra dessa intressen. Sekretessens styrka bestäms i regel med hjälp av ett s.k. skaderekvisit. 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 är sekretessbelagd. Uppgiften får då lämnas ut endast om det står klart att uppgiften kan röjas utan att viss skada uppstår. Sekretessen kan även vara absolut, vilket innebär att de uppgifter som omfattas av bestämmelsen ska hemlighållas utan någon skadeprövning, om uppgifterna begärs ut.

1.1.3.1 Rakt skaderekvisit

Det raka skaderekvisitet innebär att tillämparen kan göra sin bedömning inom ganska vida ramar. Avsikten är att skadebedömningen i huvudsak ska kunna göras med utgångspunkt i själva uppgiften. Det innebär att frågan huruvida sekretess gäller eller inte i första hand inte behöver knytas till en skadebedömning i det enskilda fallet.

Avgörande bör istället vara om uppgiften som sådan är av den arten att ett utlämnande typiskt sett kan vara ägnat att medföra skada för det intresse som ska skyddas genom bestämmelsen. Om uppgiften är sådan att den genomsnittligt sett måste betraktas som harmlös, ska den alltså normalt anses falla utanför sekretessen. Avgörande betydelse bör som regel tillmätas arten av den uppgift som efterfrågas. Konstruktionen med skaderekvisit innebär emellertid att även vem som begär en uppgift eller ändamålet med begäran kan få betydelse när sekretessfrågan prövas.[1]

1.1.3.2 Omvänt skaderekvisit

Det omvända skaderekvisitet innebär en presumtion om att sekretess gäller för uppgiften. Att sekretess gäller, om det inte står klart att uppgiften kan röjas utan skada, betyder att tillämparen har ett ganska begränsat utrymme för sin bedömning.

I praktiken innebär detta att tillämparen många gånger inte kan lämna ut en uppgift som omfattas av en sådan sekretessregel utan att ha kännedom om mottagarens identitet och dennes avsikter med uppgifterna.[2]

1.1.3.3 Schabloniserad skadeprövning vid massutlämnande

När det gäller utlämnande av en stor mängd uppgifter till en molntjänstleverantör är det av naturliga skäl inte möjligt för en tjänsteman att bilda sig en uppfattning om den särskilda skaderisk som kan vara förbunden med en enskild uppgift. Vid ett sådant massutlämnande torde myndigheten å andra sidan ha kännedom om mottagaren av uppgifterna. Den utlämnande myndigheten kan vid skadeprövningen därför väga in vilket sekretesskydd uppgifterna ifråga kommer att åtnjuta hos mottagaren. Dessa kunskaper i förening med en bedömning av den skaderisk som typiskt sett är förbunden med de aktuella uppgifterna bör i många fall ge fullt tillräckligt underlag för bedömningen av om sekretessregleringen ska anses hindra ett utlämnande eller inte.[3] En myndighets möjlighet till schabloniserad skadeprövning i förhållande till molntjänstleverantörer försvåras avsevärt när leverantören anlitar egna underleverantörer. Myndighetens prövning måste i dessa fall omfatta samtliga aktörer som kommer att ta del av uppgifterna.

1.1.3.4 Röjandebegreppet

Av 2 kap. 1 § OSL följer att det är förbjudet för myndigheter och för vissa uppräknade personer, som har tystnadsplikt, att röja eller utnyttja uppgifter som är sekretessbelagda enligt offentlighets- och sekretesslagen. Innebörden av att röja en uppgift kan kopplas till definitionen av begreppet sekretess i 3 kap. 1 § OSL, vilka sekretessen gäller mot enligt 8 kap. 1 § OSL och rekvisiten i 20 kap. 3 § brottsbalken (BrB) om brott mot tystnadsplikten. Förbudet att röja en uppgift gäller oavsett om uppgiften i fråga förekommer i en allmän handling eller inte.

Högsta domstolen har i ett rättsfall gått närmare in på vad som krävs för att en uppgift ska anses vara röjd.[4] HD uttalade att uttrycket ”röjer uppgift” enligt vanligt språkbruk innebär att en uppgift avslöjas eller uppenbaras. Detta förutsätter att det finns någon

---

[1] Prop. 1979/80:2 Del A s. 80-81.

[2] Prop. 1979/80:2 Del A s. 82.

[3] Prop. 1979/80:2 Del A s. 81.

[4] NJA 1991 s. 103.

person, för vilken uppgiften görs tillgänglig. Det torde dock inte alltid kunna krävas att denne faktiskt har fått kännedom om uppgiften. Det bör sålunda som regel vara tillräckligt att en handling med hemliga uppgifter har kommit i någon obehörigs besittning. Även vissa andra närliggande situationer bör omfattas. Däremot kan inte varje möjlighet att ta del av en uppgift, som har beretts någon obehörig, medföra att uppgiften ska anses ha röjts. Avgörande för straffansvar bör främst vara om uppgiften har blivit tillgänglig för någon under sådana omständigheter, att man måste räkna med att den obehörige kommer att ta del av uppgiften.

1.1.3.5 Straffsanktionerad och avtalsreglerad tystnadsplikt

Den som omfattas av tystnadsplikt som har författningsstöd, t.ex. enligt offentlighets- och sekretesslagen, och som felaktigt röjer en uppgift kan i vissa fall dömas för brott mot tystnadsplikten. Straffbestämmelsen finns i 20 kap. 3 § BrB.

När uppgifter lämnas ut till en privaträttslig aktör, t.ex. en molntjänstleverantör, torde det vara sällsynt att personalen omfattas av en straffsanktionerad tystnadsplikt. Här får myndigheten i stället förlita sig på en avtalsreglerad tystnadsplikt. I förarbetena till den tidigare gällande sekretesslagen (1980:100) anfördes bl.a. följande angående avtalsreglerad tystnadsplikt för en mottagare som t.ex. behandlar uppgifter för en myndighets räkning.

Mot bakgrund av det anförda kan konstateras att t.ex. personal från en kontoristförening eller ett bevakningsföretag som regel inte torde vara bundna av sekretesslagen. Jag vill emellertid erinra om att det oftast är möjligt att undvika olägenheter som kan uppkomma till följd härav antingen genom att det enskilda företaget sluter avtal med sina anställda om tystnadsplikt eller genom att en myndighet ställer upp förbehåll om att uppgifter som arbetstagare som inte är offentliga funktionärer får kännedom om i sin verksamhet inte får röjas för utomstående (jfr 14 kap. 9 § SekL).[5] *Detta förfarande kan tillämpas t.ex. när en myndighet anlitar en skrivbyrå för utskrift av handlingar som innehåller sekretessbelagda uppgifter.*[6]

JO har i ett beslut från 2014 tagit ställning till frågan om en avtalsreglerad tystnadsplikt var tillräcklig för att ett landsting skulle kunna lämna ut enskildas patientuppgifter till en privaträttslig aktör. JO uttalade följande i sin bedömning.

Jag bedömer att risken för att patientuppgifter – som ofta är av mycket integritetskänsligt slag – felaktigt lämnas ut är större när den personal som behandlar uppgifterna inte arbetar under en straffsanktionerad tystnadsplikt. Det är därmed enligt min mening tydligt att journalföring enligt avtalen innebär att patientuppgifter har ett svagare skydd än om personal som har tystnadsplikt enligt OSL utför journalföringen.

Mot bakgrund av det nu anförda anser jag att varken den avtalsreglerade tystnadsplikten som gäller för biträdets personal eller den form av tystnadsplikt som följer av regleringen i PuL medför att det kan anses stå klart att patientuppgifter kan lämnas ut

[5] Motsvaras i OSL av 10 kap. 14 §, utlämnande med förbehåll.

[6] Prop. 1981/82:186 s. 41-42.

till företagets personal för journalföring utan att den enskilde eller någon närstående lider men.[7]

Av det ovan anförda kan man dra slutsatsen att uppgifter som är av mycket integritetskänsligt slag är sekretessbelagda i förhållande till en molntjänstleverantör, vars personal enbart omfattas av en avtalsreglerad tystnadsplikt. När en avtalsreglerad tystnadsplikt kan antas vara tillräcklig i övrigt torde få avgöras med beaktande av omständigheterna i varje enskilt fall. En försvårande omständighet vid utlämnande av uppgifter till en molntjänstleverantör är givetvis om leverantören anlitar egna underleverantörer för hanteringen av uppgifterna. I sådana fall måste avtal om krav på tystnadsplikt för personalen slutas med samtliga aktörer som kan komma att hantera uppgifterna i fråga, vilket sannolikt är mycket svårt att genomföra i praktiken, i synnerhet om informationen hanteras utanför Sveriges gränser. Myndigheten har dessutom ytterst små möjligheter att kontrollera att avtalsvillkoren faktiskt efterlevs.

1.1.4 E-delegationens förstudie Sekretess vid outsourcing

E-delegationen har i en förstudie[8] utrett i vilken mån sekretesslagstiftningen begränsar myndigheters möjligheter att göra sekretessreglerade uppgifter tillgängliga för en tjänsteleverantör i samband med outsourcing. I förstudien framhåller E-delegationen att offentlighets- och sekretesslagen kan tolkas på ett sätt som ger ett relativt och normalt sett tillräckligt stort utrymme för att utlämnanden till tjänsteleverantörer ska kunna ske, under förutsättning att tjänsteavtalet tydligt anger leverantörens befogenheter och skyldigheter i fråga om tystnadsplikt, behandling av personuppgifter, rätten att ta del av information och egenkontroll av överträdelser. E-delegationen poängterar att det inte finns några prejudicerande rättsfall eller vägledande förarbetsuttalanden som tydliggör exakt i vilka avseenden eller under vilka omständigheter som gällande rätt hindrar ett utlämnande av sekretessreglerade uppgifter till en tjänsteleverantör i samband med outsourcing. Rättsläget måste därför i någon mån, i vissa avseenden, bedömas som osäkert.[9]

I det följande redogörs för hur E-delegationen har tolkat sekretesslagstiftningens begränsningar och möjligheter vid utlämnande av sekretessreglerade uppgifter till en tjänsteleverantör. Det är dock viktigt att framhålla att E-delegationens tolkningar enbart avser utlämnande av uppgifter till en tjänsteleverantör som är etablerad i Sverige och som hanterar informationen inom landets gränser.

E-delegationen har inte heller tagit ställning till hur en sekretessbedömning påverkas av det förhållandet att en tjänsteleverantör använder sig av underleverantörer för hanteringen av myndighetens information.

1.1.4.1 Prövning av skaderekvisit och röjandebegreppet

Inför ett utlämnande av sekretessreglerade uppgifter måste myndigheten pröva om sekretessen gäller gentemot mottagaren, dvs. den aktuella leverantören. Om sekretessen är reglerad utan skaderekvisit gäller s.k. absolut sekretess, vilket innebär att uppgifterna kan röjas endast med stöd av en sekretessbrytande bestämmelse. Om den aktuella sekretessbestämmelsen däremot är försedd med skaderekvisit ska myndig-

[7] JO:s beslut den 9 september 2014, dnr 3032-2011.

[8] Sekretess vid outsourcing – en förstudie, Fi 2009:01/2015/4, 2015-03-19.

[9] A.a. s. 8-9.

heten göra en sekretessprövning, *dels* utifrån den skaderisk som typiskt sett är förbunden med uppgifter av det slag som avses, *dels* med beaktande av de kunskaper som myndigheten har om mottagaren, dvs. hur denne kommer att hantera uppgifterna och vilken spridningsrisk som finns. En aspekt som enligt JO är särskilt viktig att beakta vid denna sekretessprövning är huruvida leverantören omfattas av en tystnadsplikt som är straffsanktionerad.[10]

När det gäller sådana sekretessreglerade uppgifter om enskilda som inte kan anses vara av särskilt integritetskänsligt slag anser E-delegationen att utgångspunkten vid sekretessprövningen bör vara att en avtalsreglerad tystnadsplikt räcker för att man ska kunna konstatera att skaderekvisitet inte är uppfyllt och att sekretess därmed inte gäller gentemot tjänsteleverantören. På motsvarande sätt bör en avtalsreglerad tystnadsplikt i normalfallet ge ett tillräckligt skydd för sådana uppgifter som sekretessreglerats till skydd för allmänna eller kommersiella intressen, med undantag för vissa uppgifter som har ett särskilt uttalat skyddsbehov med hänsyn till Sveriges internationella relationer eller rikets säkerhet.[11]

För den sistnämnda typen av särskilt känsliga uppgifter, liksom för vissa särskilt skyddsvärda uppgifter om enskildas personliga förhållanden, kan det däremot antas att sekretess skulle anses gälla gentemot en tjänsteleverantör, om utförarens personal varken omfattas av en straffsanktionerad tystnadsplikt eller av någon motsvarande straffsanktionerad befogenhetsinskränkning.[12]

Om det kan konstateras att en planerad outsourcing kräver ett tillgängliggörande av uppgifter för vilka sekretess gäller även gentemot tjänsteleverantören, måste myndigheten ta ställning till om uppgifterna kommer att göras tillgängliga på ett sådant sätt att uppgifterna kan anses vara ”röjda” i offentlighets- och sekretesslagens mening. Enligt E-delegationens uppfattning bör det i vart fall inte betraktas som ett röjande i offentlighets- och sekretesslagens mening om en hemlig uppgift har gjorts tillgänglig för en utomstående på ett sådant sätt att det förefaller *osannolikt* att mottagaren faktiskt tar del av uppgifterna. Vid outsourcing av exempelvis it-drift skulle en sådan situation kunna föreligga om tjänsteavtalet har försetts med ett tydligt förbud för leverantören och dennes personal att ta del av den information som hanteras i systemen, krav på kontrollmekanismer och kännbara civilrättsliga sanktioner vid överträdelser.[13]

1.1.4.2 Kan E-delegationens tolkningar tillämpas av en myndighet som avser att anlita en molntjänstleverantör?

Det är inte möjligt att på ett enhetligt sätt beskriva molntjänstleverantörer. En molntjänstleverantör kan vara en nationell aktör, utan underleverantörer, med ett fåtal anställda och där all hantering av informationen sker inom Sveriges gränser. En molntjänstleverantör kan också vara en global aktör, med datacenter utspridda över

---

[10] A.a. s. 4, (E-delegationen förespråkar att även andra straffrättsliga bestämmelser ska kunna beaktas vid bedömningen av om uppgifter kan anses åtnjuta ett tillförlitligt skydd hos en privaträttslig mottagare. De exempel som ges torde dock inte vara aktuella vid utlämnande av uppgifter till molntjänstleverantörer varför de har utelämnats här).

[11] A.a. s. 5.

[12] A.a. s. 5-6.

[13] A.a. s. 6-7.

alla kontinenter, med ett stort antal anställda och underleverantörer i olika länder. Vilken typ av molntjänstleverantör som anlitas kan vara avgörande för hur en myndighets sekretessprövning utfaller. En sekretessprövning inför utlämnande av uppgifter till en global molntjänstleverantör ställer givetvis högre krav på myndigheten än motsvarande prövning gentemot en mindre nationell aktör.

En myndighet som anlitar en molntjänstleverantör måste ofta göra en s.k. schabloniserad sekretessprövning. Vid denna bedömning ska myndigheten bedöma om sekretess gäller gentemot samtliga mottagare av uppgifterna, dvs. såväl molntjänstleverantören som eventuella underleverantörer. I många fall är det sannolikt förenat med stora svårigheter, om ens möjligt, för en utlämnande myndighet att göra en sådan schabloniserad sekretessprövning. I synnerhet torde detta vara fallet när uppgifterna omfattas av ett omvänt skaderekvisit och/eller molntjänstleverantören anlitar egna underleverantörer.

Myndigheten lär ställas inför samma svårigheter när det gäller att ta ställning till om det går att lämna ut sekretessbelagda uppgifter till en molntjänstleverantör utan att uppgifterna röjs i offentlighets- och sekretesslagens mening. Det kan förvisso finnas förutsättningar för en myndighet som anlitar en mindre, nationell molntjänstleverantör, utan underleverantörer, att förhandla fram avtalsvillkor som förhindrar leverantörens personal att ta del av uppgifterna som hanteras och ger myndigheten tillräckliga kontrollmekanismer för att granska att avtalet efterlevs. När det gäller globala molntjänstleverantörer är det dock osannolikt att en myndighet kan förhandla fram avtalsvillkor som tryggar myndighetens rätt till insyn och kontroll.

Ett alternativ som diskuteras emellanåt är möjligheten att krypteringsskydda uppgifter innan de lämnas ut till t.ex. en molntjänstleverantör. Ett tillförlitligt krypteringsskydd, som medför att leverantören inte kan ta del av uppgifterna i läsbart format eller uppfatta innehållet på annat sätt, torde innebära att uppgifterna inte röjs för leverantören. Givetvis är en förutsättning för detta att uppgifterna även är krypteringsskyddade hos eventuella underleverantörer. Vidare behöver lämpliga avtalsvillkor upprättas mellan parterna, dels för att förhindra att leverantören tar del av uppgifterna om en sådan möjlighet trots allt skulle uppstå och dels för att ge myndigheten tillgång till konkreta verktyg för att kunna utöva kontroll över leverantörens hantering.

1.1.5 Sekretessbrytande bestämmelser

Bland annat i 10 kap. OSL finns ett antal sekretessbrytande bestämmelser som innebär att ett utlämnande av en uppgift i vissa fall är möjligt även om uppgiften är sekretessbelagd. En sekretessbrytande bestämmelse som skulle kunna vara tillämplig vid utlämnande av uppgifter till en molntjänstleverantör är 10 kap. 2 § OSL, dvs. i situationer när det är fråga om ett nödvändigt utlämnande.

1.1.5.1 Nödvändigt utlämnande, 10 kap. 2 § OSL

Bestämmelsen innebär att sekretess inte hindrar att en myndighet lämnar ut uppgifter om det är nödvändigt för att myndigheten ska kunna fullgöra sin verksamhet. Syftet med bestämmelsen är att förhindra att sekretessregleringen gör det omöjligt för en myndighet och dess personal att sköta de uppgifter som myndigheten har ansvar för. Sekretessen får efterges bara i sådana fall då ett utlämnande av sekretessbelagda uppgifter är en nödvändig förutsättning för att myndigheten ska kunna fullgöra ett

visst åtagande.[14] Av förarbetena framgår att bestämmelsen ska tillämpas restriktivt. Enbart en bedömning att effektiviteten i myndighetens handlande sätts ner genom en föreskrift om sekretess får inte leda till att sekretessen åsidosätts.[15]

Bestämmelsen har aktualiserats i flera ärenden hos JO. Det tidigare nämnda JO-beslutet från år 2014 förtjänar att redogöras för närmare.

Ärendet gällde offentliga vårdgivare som ingått avtal med ett företag om hjälp med journalföring av patientuppgifter. Enligt avtalen tillät vårdgivare att läkarsekreterare, anställda av företaget, på distans lyssnade av inlästa diktat och skrev in uppgifterna i patientens journal. De uppgifter som hanterades av läkarsekreterarna omfattades av en presumtion för sekretess, dvs. omvänt skaderekvisit. Enligt JO är utgångspunkten att 10 kap. 2 § OSL ska tillämpas restriktivt och att det i praktiken handlar om situationer av undantagskaraktär. JO konstaterar därefter att det inte framkommit något som tyder på att vårdgivarna i och för sig skulle ha varit förhindrade att lösa journalföringen på ett sätt som inte hade riskerat att komma i konflikt med sekretessbestämmelserna t.ex. genom omfördelning av personal eller genom anställning av ny personal. Enbart en effektivisering av vårdgivarens journalföring i samband med ett ansträngt arbetsläge innebär inte att bestämmelsen blir tillämplig. Enligt JO:s mening var det således inte fråga om ett sådant ”nödvändigt utlämnande” som medför att bestämmelserna i 10 kap. 2 § OSL kan tillämpas.[16]

E-delegationen, som närmare har granskat detta JO-beslut, anser att det förhållandet att bestämmelsen i 10 kap. 2 § OSL ska tillämpas restriktivt inte är detsamma som att den ska tillämpas endast i ”situationer av undantagskaraktär”.[17] E-delegationen menar, med hänvisning till lagens förarbeten, att för att bestämmelsen inte ska sakna praktisk relevans måste den tolkas så att det i särskilda fall kan anses vara nödvändigt att lämna ut uppgifter till en utomstående expert även då utlämnandet sker av effektivitetsskäl, förutsatt att åtgärden sker inom ramen för vad som utgör myndighetens egen verksamhet, dess uppdrag.[18] Vidare anser E-delegationen att det torde finnas situationer då det måste anses vara ”nödvändigt” för en myndighet att vända sig till en utomstående aktör för att dra nytta av dennes tekniska utrustning. Framför allt gäller detta vid åtgärder för teknisk bearbetning och teknisk lagring av myndighetsinformation, såsom storskalig skanning av dokument, tryckeriverksamhet, it-drift och e-arkivering samt funktioner för t.ex. elektronisk legitimering, elektroniska underskrifter och stöd mot intrång och andra angrepp i myndighetens it-miljö.[19] E-delegationen poängterar dock att myndigheten måste överväga sådana alternativ som innebär att ett röjande av sekretessbelagda uppgifter kan undvikas. Även om outsourcing skulle medföra något lägre kostnader eller något högre effektivitet än ett annat fullt genomförbart alternativ

[14] Lenberg m.fl., Offentlighets- och sekretesslagen, En kommentar, 10 kap. 2 § OSL.

[15] Prop. 1979/80:2 Del A s. 465 och 494.

[16] JO:s beslut den 9 september 2014, dnr 3032-2011.

[17] E-delegationens förstudie s. 73, se även refererade JO-beslut s. 19 och prop. 1979/80:2 Del A s. 121 ang. utlämnande till utomstående expert.

[18] A.a. s. 74.

[19] A.a. s. 74.

torde inte det vara tillräckligt för att outsourcingen, och därmed tillgängliggörandet av uppgifter, skulle anses vara ”nödvändigt” i den mening som avses i 10 kap. 2 § OSL.[20]

Sammanfattningsvis kan det konstateras att rättsläget fortfarande är förhållandevis oklart när det gäller vad som kan anses vara ett nödvändigt utlämnande enligt 10 kap. 2 § OSL. Bestämmelsen torde emellertid endast undantagsvis kunna vara tillämplig när en myndighet lämnar ut uppgifter till en molntjänstleverantör. Även om utlämnandet är tillåtet med stöd av 10 kap. 2 § OSL är det viktigt att myndigheten binder leverantören vid en avtalsreglerad tystnadsplikt för att det skyddsintresse som offentlighets- och sekretesslagen tar sikte på ska tillgodoses.

1.1.6 Teknisk bearbetning och lagring

Hos alla svenska myndigheter finns allmänna handlingar, dvs. handlingar som *förvaras* hos myndigheten och är att anse som *inkomna* till eller *upprättade* hos myndigheten. Även om sekretess inte hindrar en myndighet från att lämna ut uppgifter kan dock åtgärden att göra delar av myndighetens informationssamling tillgänglig för exempelvis en molntjänstleverantör leda till att handlingars status förändras. Att göra en elektronisk handling tekniskt tillgänglig för någon annan utgör nämligen en expediering som enligt huvudregeln medför att handlingen blir upprättad och därmed allmän. Att handlingen blir allmän innebär att den omfattas av offentlighetsprincipen och kan begäras utlämnad. Tryckfrihetsförordningen innehåller emellertid undantag från när en handling ska anses vara en allmän handling.

Enligt 2 kap. 7 § första stycket TF anses en handling upprättad hos en myndighet när den har expedierats. En upptagning, dvs. en elektronisk handling, anses expedierad när myndigheten har vidtagit de tekniska åtgärder som erfordras för att någon utomstående ska få tillgång till informationen i läsbar form, eller då den har översänts till annan, t.ex. med e-post. Handling som inte har expedierats anses upprättad när det ärende till vilket den hänför sig har slutbehandlats hos myndigheten eller, om handlingen inte hänför sig till visst ärende, när den har justerats av myndigheten eller på annat sätt färdigställts.

Enligt 2 kap. 6 § andra stycket TF anses en upptagning inkommen till myndighet när annan gjort den tillgänglig för myndigheten med tekniskt hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att den kan läsas, avlyssnas eller på annat sätt uppfattas. Av tredje stycket i samma paragraf framgår dock att en handling som återkommer till en myndighet efter teknisk bearbetning eller teknisk lagring inte anses som en inkommen handling. Rimligen bör det ursprungliga exemplaret då inte heller anses vara expedierat från, och därmed inte en upprättad allmän handling hos, den avsändande myndigheten. En annan tolkning skulle leda till att undantaget i 2 kap. 6 § 3 stycket TF helt skulle förlora sin funktion, i vart fall då fråga är om enbart teknisk lagring utanför myndigheten.

En tolkning enligt ovan ger vid handen att en myndighet som uppdrar åt en molntjänstleverantör att enbart tekniskt lagra eller tekniskt bearbeta viss information inte anses ha expedierat handlingar i tryckfrihetsförordningens mening. En handling som inte är allmän hos den avsändande myndigheten blir således inte att betrakta som allmän bara för att den överlämnas till en molntjänstleverantör för teknisk bearbetning

[20] A.a. s. 74.

eller lagring. Enligt undantagsbestämmelsen i 2 kap. 6 § tredje stycket TF anses handlingarna inte heller ha kommit in till myndigheten när molntjänstleverantören tillhandahåller myndigheten den tekniskt bearbetade eller lagrade informationen.

Om molntjänstleverantörens uppdrag i stället går utöver teknisk lagring eller teknisk bearbetning, exempelvis analys av data eller framställning av statistik, är undantaget inte tillämpligt. Samma sak bör gälla om molntjänstleverantören behandlar informationen för egna ändamål. Myndigheten anses då i stället ha expedierat handlingarna i och med att de lämnas ut till molntjänstleverantören och handlingarna blir att betrakta som inkomna när de tillgängliggörs för myndigheten av leverantören. Detta innebär att handlingar som tidigare inte varit allmänna hos den avsändande myndigheten blir att betrakta som allmänna handlingar som omfattas av tryckfrihetsförordningens bestämmelser om handlingsoffentlighet i samma stund de överlämnas till molntjänstleverantören.

Undantag från vad som utgör allmän handling finns även för information som tekniskt lagras eller bearbetas av myndigheter. Enligt 2 kap. 10 § TF anses en handling, som förvaras hos en myndighet endast som led i teknisk bearbetning eller teknisk lagring för annans räkning, inte som allmän handling hos den myndigheten. Bestämmelsen tar sikte på myndigheter som utför teknisk bearbetning eller lagring för en annan myndighets eller en enskilds räkning. Liksom i exemplet ovan ska handlingen inte heller anses vara expedierad från eller inkommen till den avsändande myndigheten.[21] Om den mottagande myndigheten i sin tur anlitar en molntjänstleverantör för att utföra den tekniska bearbetningen eller lagringen borde detta rimligen medföra att handlingen bevarar sin status som icke allmän, dvs. handlingen blir inte expedierad när den överlämnas till molntjänstleverantören.

Undantaget i 2 kap. 10 § TF är bara tillämpligt under förutsättning att molntjänstleverantören inte vidtar några andra åtgärder än teknisk lagring eller bearbetning. Om leverantören utför andra åtgärder eller behandlar informationen för egna ändamål anses handlingen vara expedierad i samma stund som den görs tekniskt tillgänglig för denne. Handlingen är därmed att betrakta som allmän och kan bli föremål för utlämnande enligt tryckfrihetsförordningens bestämmelser om allmänna handlingar.

1.1.7 Sammanfattning offentlighets- och sekretesslagstiftningen

1.1.7.1 Sekretessregleringen

En myndighet måste pröva om det är förenligt med offentlighets- och sekretesslagen att lämna ut sin information till den tänkta molntjänstleverantören. Om molntjänstleverantören anlitar egna underleverantörer som kommer att ta del av myndighetens information ska sekretessprövningen ske gentemot var och en av dessa underleverantörer. Även om myndigheten kan konstatera att det inte finns något generellt hinder i offentlighets- och sekretesslagen mot att uppgifterna lämnas ut bör myndigheten också ta ställning till om det är lämpligt att lämna ut informationen. I lämplighetsbedömningen bör myndigheten exempelvis beakta var molntjänstleverantören kommer att lagra informationen geografiskt och i förekommande fall ta ställning till vilka konsekvenserna kan bli av att informationen exponeras mot andra länders rättsordningar.

[21] Prop. 1975/76:160 s. 137.

I kölvattnet av JO:s beslut från år 2014[22] har en debatt blossat upp rörande frågan om det över huvud taget är möjligt att lämna ut sekretessbelagda uppgifter till personuppgiftsbiträden och i synnerhet till molntjänstleverantörer som personuppgiftsbiträden. E-delegationen har i sin förstudie[23] gjort en grundlig genomgång av offentlighets- och sekretesslagens förarbeten och praxis och lagt fram förslag på en tolkning av sekretessregleringen. Förstudien har emellertid fokuserat på traditionell outsourcing ur ett nationellt perspektiv där en myndighet som regel anlitar en leverantör som är etablerad i Sverige. Förstudien tar inte heller upp frågan om hur en myndighet ska kunna utföra en tillförlitlig sekretessprövning i förhållande till underleverantörer som kan finnas i flera led eller hur myndigheten ska kunna kontrollera underleverantörers avtalsefterlevnad. Mot denna bakgrund torde E-delegationens bedömningar, inom ramen för denna analys, vara användbara endast när myndigheten upphandlar en molntjänstleverantör vars verksamhetsupplägg motsvarar eller påminner om traditionell outsourcing.

1.1.7.2 Vilka förutsättningar ger offentlighets- och sekretesslagen att anlita en molntjänstleverantör?

En myndighet kan lämna ut sin information till en molntjänstleverantör, under förutsättning att informationen inte är sekretessreglerad och att det inte är olämpligt av andra skäl att lämna ut informationen till leverantören i fråga.

En myndighet som har för avsikt att anlita en molntjänstleverantör för att behandla sekretessreglerad information måste pröva om informationen kan lämnas ut eller om sekretess hindrar ett utlämnande. Under vissa omständigheter kan eventuellt en tystnadspliktförbindelse i avtal vara tillräcklig för att myndigheten ska kunna konstatera att sekretess inte gäller mot leverantören. Myndigheten bör dock iaktta stor försiktighet vid en sådan bedömning och vinnlägga sig om att informationen t.ex. inte är av särskilt integritetskänsligt slag i förhållande till enskilda individer eller har ett särskilt uttalat skyddsbehov med hänsyn till Sveriges internationella relationer eller rikets säkerhet.[24] Vidare ska myndigheten också beakta om det finns andra omständigheter som gör att det är olämpligt att lämna ut informationen till molntjänstleverantören i fråga.

Under alla omständigheter torde det alltid vara olämpligt att lämna ut sekretessreglerade uppgifter till en molntjänstleverantör som anlitar fler än någon enstaka underleverantör eller som regelbundet anlitar nya underleverantörer. Myndighetens möjlighet att säkerställa att samtliga underleverantörer blir bundna av samma avtalsvillkor som molntjänstleverantören och myndighetens möjlighet att kontrollera att samtliga leverantörer efterlever avtalsvillkoren torde minska i takt med ett ökat antal underleverantörer hos molntjänstleverantören.

1.1.7.3 Allmänna handlingar – teknisk bearbetning och lagring

En myndighet som uppdrar åt en molntjänstleverantör att hantera myndighetens information måste vara uppmärksam på att handlingars status kan komma att förändras när uppgifterna lämnas ut till en leverantör. Om leverantörens uppdrag går

---

[22] JO:s beslut den 9 september 2014, dnr 3032-2011.

[23] Sekretess vid outsourcing - en förstudie, Fi 2009:01/2015/4, 2015-03-19.

[24] A.a. s. 5.

utöver enbart teknisk lagring eller teknisk bearbetning anses de upptagningar/ handlingar som myndigheten överlämnar till leverantören vara expedierade i tryckfrihetsförordningens mening. Detta innebär att handlingarna blir att anse som allmänna hos myndigheten och kan begäras ut enligt tryckfrihetsförordningen.

1.2 Säkerhetsskyddslagstiftningen

Syftet med säkerhetsskyddslagen (1996:627) är bl.a. att ge säkerhetsskydd för statlig verksamhet som är av betydelse för rikets säkerhet eller som särskilt behöver skyddas mot terrorism. Till säkerhetsskyddslagen finns den anslutande säkerhetsskyddsförordningen (1996:633) som bl.a. reglerar hur myndigheter på en mer detaljerad nivå ska arbeta med sitt säkerhetsskydd. Säkerhetspolisen har därutöver utfärdat förskrifter och allmänna råd om säkerhetsskyddet (PMFS 2015:3). Föreskrifterna innehåller utförliga bestämmelser om hur uppgifter, som omfattas av sekretess enligt offentlighets- och sekretesslagen och som rör rikets säkerhet, ska hanteras när det gäller t.ex. informationssäkerhet för it-system.

1.2.1 Informationssäkerhet

Säkerhetsskyddet ska bl.a. skydda uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen och som rör rikets säkerhet, 6 § punkten 2 säkerhetsskyddslagen. En av säkerhetsskyddsåtgärderna i lagen är informationssäkerhet, 7 § punkten 1, säkerhetsskyddslagen.

Informationssäkerhet ska förebygga att uppgifterna obehörigen röjs, ändras eller förstörs. Vilka åtgärder en myndighet är skyldig att vidta i informationssäkerhetshänseende regleras såväl i säkerhetsskyddslagen som i förordningen och i Säkerhetspolisens föreskrifter (PMFS 2015:3).

Av 9 § säkerhetsskyddslagen framgår att behovet av skydd vid automatisk informationsbehandling ska beaktas särskilt vid utformningen av informationssäkerheten. Förordningen ställer bl.a. krav på att ett system som av flera personer ska användas för automatiserad behandling av hemliga uppgifter[25] ska vara försett med funktioner för behörighetskontroll och registrering av händelser i systemet som är av betydelse för säkerheten, 12 § säkerhetsskyddsförordningen. Av 13 § säkerhetsskyddsförordningen följer att myndigheter innan de sänder hemliga uppgifter i ett datanät utanför deras kontroll, ska förvissa sig om att det för uppgifterna där finns en fullgod informationssäkerhet. Vidare får hemliga uppgifter krypteras endast med kryptosystem som har godkänts av Försvarsmakten, 13 § säkerhetsskyddsförordningen. I 4 kap. i föreskrifterna (PMFS 2015:3) finns ytterligare detaljreglering av informationssäkerhet för it-system.

1.2.2 Säkerhetsprövning

Säkerhetsprövning är en säkerhetsskyddsåtgärd som ska vidtas i syfte att förhindra att personer som inte är pålitliga ur säkerhetssynpunkt deltar i verksamhet som har betydelse för rikets säkerhet, 7 § punkten 3, säkerhetsskyddslagen. Säkerhetsprövning ska göras innan en person genom anställning eller på annat sätt deltar i verksamhet som har betydelse för rikets säkerhet, 11 § säkerhetsskyddslagen. Alla personer som

[25] Med hemliga uppgifter avses enligt definitionen i 4 § punkten 1 säkerhetsskyddsförordningen, uppgift som omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) och som rör rikets säkerhet.

ska delta i ett uppdrag och som kan antas få del av hemliga uppgifter, eller delta i verksamhet av betydelse för rikets säkerhet ska säkerhetsprövas.[26] Om uppdraget är placerat i säkerhetsklass ska även en registerkontroll göras. De som får del av hemliga uppgifter eller deltar i verksamheten ska upplysas om den tystnadsplikt som gäller.

1.2.3 Säkerhetsskyddad upphandling

När staten avser att begära in anbud eller träffa avtal om upphandling där det förekommer uppgifter som med hänsyn till rikets säkerhet omfattas av sekretess, ska staten träffa ett skriftligt avtal (säkerhetsskyddsavtal) med anbudsgivaren eller leverantören om det säkerhetsskydd som behövs i det särskilda fallet, 8 § första stycket säkerhetsskyddslagen. Syftet med säkerhetsskyddsavtalet är att skyddet för hemliga uppgifter ska vara detsamma oberoende av i vilken verksamhet de förekommer.

Myndigheten ska alltså ställa samma krav på säkerhetsskydd hos leverantörer som de ställer i sin egen verksamhet. Detta gäller både huvudleverantör och eventuella underleverantörer som tar del av hemliga uppgifter eller deltar i verksamhet med betydelse för rikets säkerhet. I avtalet ska bl.a. regleras hur leverantören ska utforma sitt säkerhetsskydd avseende informationssäkerhet, tillträdesbegränsningar och säkerhetsprövning.

När ett säkerhetsskyddsavtal har ingåtts ska leverantören upprätta en säkerhetsskyddsinstruktion. I instruktionen ska denne redovisa vilka säkerhetsskyddsåtgärder leverantören kommer att vidta under uppdraget för att uppfylla kraven i säkerhetsskyddsavtalet. Om leverantören ska hantera och förvara hemliga uppgifter i sina egna lokaler ska myndigheten besöka företaget för att kontrollera att lokaler och övriga förhållanden är lämpliga från säkerhetsskyddssynpunkt.

1.2.4 Sammanfattning säkerhetsskyddslagstiftningen

Det finns inget uttryckligt hinder i säkerhetsskyddslagen för en myndighet att anlita externa leverantörer, t.ex. en molntjänstleverantör, för hantering av information som omfattas av lagen. En förutsättning är emellertid att det är förenligt med offentlighets- och sekretesslagen, och i övrigt lämpligt, att lämna ut informationen till leverantören i fråga. Vidare krävs att myndigheten tecknar ett säkerhetsskyddsavtal med leverantören och att leverantören upprättar en säkerhetsinstruktion vari framgår vilka åtgärder leverantören ska vidta för att uppfylla kraven i säkerhetsskyddsavtalet. Om molntjänstleverantören har sin personal, sin verksamhet och sina serverhallar utanför Sveriges gränser måste myndigheten beakta att möjligheten att säkerhetspröva personal och utnyttja svenska kontrollinstrument är mycket starkt begränsade i utlandet.

Sammantaget kan det konstateras att säkerhetsskyddslagen och dess anslutande förordning och föreskrifter ställer långtgående krav på hanteringen av hemliga uppgifter. En myndighet som har för avsikt att anlita en molntjänstleverantör för hantering av information som omfattas av säkerhetsskyddslagen måste kontrollera att leverantören har förutsättningar att uppfylla samtliga krav som ställs på hanteringen. Myndigheten måste därutöver kontrollera att leverantören har faktisk möjlighet att

[26] Bestämmelser om säkerhetsprövning finns i 11-13 §§ och 17-19 §§ säkerhetsskyddslagen, 14 § och 18-19 §§ säkerhetsskyddsförordningen samt i kap. 6 och 8 PMFS 2015:3.

efterleva samtliga krav. Förutsättningarna för att hantera information som omfattas av säkerhetsskyddslagen i en molntjänst torde i realiteten vara synnerligen begränsade. Det kan exempelvis antas vara vare sig lagligt eller lämpligt att hantera hemliga uppgifter i en publik molntjänst eller i en tjänst som tillhandahålls av en global aktör eller en leverantör som anlitar fler än någon enstaka underleverantör.

1.3 Integritetsskyddslagstiftningen

Skyddet för den enskildes personliga integritet och respekten för privatlivet är viktiga grundläggande rättigheter som i svensk lag kommer till uttryck i både 2 kap. 6 § regeringsformen (RF) och art. 8 Europakonventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna. Bestämmelsen i Europakonventionen innefattar en skyldighet för det offentliga att avhålla sig från ingrepp i den enskildes privat– och familjeliv och en offentlig myndighets inskränkning av den enskildes rätt får endast ske med stöd av lag. Härutöver ska även Europeiska unionens stadga om de grundläggande rättigheterna beaktas.[27] När det gäller automatiserad behandling av personuppgifter har dessa grundläggande rättigheter preciserats i det så kallade dataskyddsdirektivet 95/46/EG.[28] Att integritetsskyddet har sin grund även i data-skyddsdirektivet innebär att de bestämmelser om behandling av personuppgifter som finns i vår nationella lagstiftning inte får ge en lägre skyddsnivå än vad direktivet föreskriver.

Enligt 2 kap. 6 § andra stycket RF är var och en gentemot det allmänna skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. En begränsning av rättigheterna i 2 kap. 6 § andra stycket RF ska, för att vara tillåten, stadgas i lag och får inte gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett begränsningen, 2 kap. 20 och 21 §§ RF. En förutsättning för att få behandla personuppgifter automatiserat är därför att det integritetsintrång som behandlingen innebär för den enskilde har stöd i lag och dessutom är väl avvägt och står i proportion till behovet av behandlingen.

1.3.1 Personuppgiftslagen

Behandling av personuppgifter regleras i personuppgiftslagen (1998:204, PuL). Personuppgiftslagen grundar sig på dataskyddsdirektivet och syftet med lagen är att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter, 1 § PuL. Av 2 § PuL följer att om det i lag eller förordning finns bestämmelser som avviker från lagen ska dessa bestämmelser gälla. Således har särregler i myndigheters registerförfattningar företräde i förhållande till bestämmelserna i personuppgiftslagen. Registerförfattningar är sektors- eller myndighetsspecifika regleringar om databehandling av personuppgifter. För de myndigheter vars verksamhetsrelaterade personuppgiftsbehandling inte är särreglerad genom registerförfattning gäller enbart personuppgiftslagen och den anslutande personuppgiftsförordningen (1998:1191, PuF).

---

[27] Europeiska unionens stadga om de grundläggande rättigheterna (2010/C 83/02).

[28] Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.

En myndighet som har för avsikt att behandla personuppgifter i en molntjänst ska följa samtliga aktuella bestämmelser i personuppgiftslagen eller eventuellt tillämplig registerförfattning. Inom ramen för denna rapport kommer emellertid enbart redogöras för de bestämmelser som är av särskilt intresse vid myndigheters behandling av personuppgifter i en molntjänst.

1.3.2 Personuppgifter

Med personuppgifter avses all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet, 3 § PuL. Personuppgifter kan t.ex. vara personnummer, uppgift om namn och adress, beskrivande information eller uppgifter som på annat sätt indirekt pekar ut en specifik individ såsom exempelvis lägenhetsnummer, ett fordons registreringsnummer m.m. Även uppgifter som har krypterats, pseudonymiserats eller anonymiserats är personuppgifter så länge det finns en kodnyckel sparad. Det saknar betydelse om den aktör som behandlar uppgifterna inte har, eller kan få, tillgång till kodnyckeln. Avgörande är i stället om det finns en faktisk möjlighet att återkoppla uppgifterna till en fysisk person.

Enligt 13 § PuL är vissa typer av personuppgifter att betrakta som känsliga i lagens mening. Det rör sig om personuppgifter som avslöjar

- ras eller etniskt ursprung,
- politiska åsikter,
- religiös eller filosofisk övertygelse,
- medlemskap i fackförening samt
- personuppgifter som rör hälsa eller sexualliv.

Den som behandlar personuppgifter är skyldig att vidta lämpliga säkerhetsåtgärder för att skydda uppgifterna i fråga. När känsliga personuppgifter behandlas ställs högre krav på de åtgärder som ska vidtas för att skydda uppgifterna.

Även uppgifter som inte klassificeras som känsliga enligt 13 § PuL kan vara särskilt integritetskänsliga och därför kräva samma höga skyddsnivå som känsliga personuppgifter. Vissa typer av uppgifter räknas regelmässigt som integritetskänsliga t.ex. uppgifter om

- lagöverträdelser,
- ekonomisk hjälp eller vård inom socialtjänsten,
- enskilds personliga och ekonomiska förhållanden inom bank- och försäkringsväsendet, och
- uppgifter inom kreditupplysning eller inkassoverksamhet.

Ett uttryck för att det är fråga om känsliga personuppgifter kan också vara att uppgifterna omfattas av sekretess till skydd för enskildas personliga förhållanden, enligt offentlighets- och sekretesslagen.[29]

Personuppgifter kan även under andra omständigheter anses vara integritetskänsliga exempelvis när en omfattande mängd uppgifter om en och samma individ behandlas

[29] Datainspektionens allmänna råd Säkerhet för personuppgifter, s. 18.

eller om uppgifterna är av rent privat natur eller på annat sätt rör en individs egenskaper eller personliga förutsättningar t.ex. omdömen. För att avgöra om uppgifter är integritetskänsliga eller inte krävs i regel en bedömning i varje enskilt fall.

En behandling av personuppgifter är varje åtgärd eller serie av åtgärder som vidtas i fråga om personuppgifter, vare sig det sker på automatisk väg eller inte. I 3 § PuL ges som exempel på vad som avses med behandling, bl.a. insamling, registrering, lagring, bearbetning, utlämnande, spridning etc.

1.3.3 Personuppgiftsansvarig och personuppgiftsbiträde

Enligt 3 § PuL är personuppgiftsansvarig den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter. Den personuppgiftsansvarige har ett skadeståndsrättsligt ansvar gentemot de registrerade, dvs. de enskilda vars uppgifter behandlas, 48 § PuL. Ansvaret innebär att den personuppgiftsansvarige ska ersätta den registrerade för skada och kränkning av den personliga integriteten som en behandling av personuppgifter i strid med personuppgiftslagen har orsakat.

I registerförfattningar finns ofta ett utpekat personuppgiftsansvar. Exempelvis är Arbetsförmedlingen personuppgiftsansvarig för den behandling av personuppgifter som Arbetsförmedlingen utför, 3 § lagen (2002:546) om behandling av personuppgifter i den arbetsmarknadspolitiska verksamheten och Skatteverket är personuppgiftsansvarigt för den behandling av personuppgifter som verket ska utföra, 6 § lagen (2001:181) om behandling av uppgifter i Skatteverkets beskattningsverksamhet.

Varje myndighet är också personuppgiftsansvarig för den behandling av personuppgifter som sker internt för t.ex. personaladministrativa ändamål. Det förhållandet att myndigheten har uppdragit åt en utomstående aktör, exempelvis Statens servicecenter, att hantera personaladministrationen fråntar inte den uppdragsgivande myndigheten dess personuppgiftsansvar.

En aktör som behandlar personuppgifter för den personuppgiftsansvariges räkning kallas personuppgiftsbiträde, 3 § PuL. Ett personuppgiftsbiträde är en osjälvständig part i förhållande till den personuppgiftsansvarige och får behandla personuppgifterna bara i enlighet med de instruktioner som den ansvarige har utfärdat för uppdraget, 30 § första stycket PuL. Den personuppgiftsansvarige har i förhållande till den registrerade ett fortsatt skadeståndssanktionerat ansvar för att personuppgiftslagen följs även när personuppgiftsbehandlingen utförs av ett personuppgiftsbiträde. Den personuppgiftansvarige kan således uppdra den faktiska behandlingen av personuppgifterna till biträdet, men aldrig avsäga sig personuppgiftsansvaret. I förhållande till den registrerade har personuppgiftsbiträdet inget direkt ansvar för personuppgiftsbehandlingens lagenlighet. Det är en annan sak att biträdet kan bli skadeståndsskyldigt gentemot den personuppgiftsansvarige för eventuella brott mot dennes instruktioner, men då på kontraktsrättslig grund och alltså inte i enlighet med personuppgiftslagens skadeståndsregel.[30]

Om personuppgiftsbiträdet behandlar personuppgifterna för egna ändamål eller behandlar dem på ett sätt som går utöver vad som har avtalats blir biträdet normalt

[30] Myndighetsdatalag, SOU 2015:39 s. 335.

ansvarig för den behandlingen. Är personuppgiftsbiträdet biträde till fler än en personuppgiftsansvarig, kan uppgifterna som biträdet behandlar inte sammanblandas utan att det blir frågan om en ny uppgiftssamling. Den nya uppgiftssamlingen blir personuppgiftsbiträdet själv ansvarig för. Det gäller dock inte om sammanblandningen sker på uppdrag av någon av de personuppgiftsansvariga, då blir denne i stället ansvarig. För att kunna ge ett sådant uppdrag måste den personuppgiftsansvarige själv ha behörighet att behandla dessa personuppgifter, i annat fall är behandlingen otillåten.

När en myndighet behandlar personuppgifter i en molntjänst har molntjänst-leverantören rollen som personuppgiftsbiträde. Detta gäller även när en myndighet under förenklade former köper eller använder t.ex. en SaaS-tjänst direkt över internet. Den leverantör som tillhandahåller tjänsten är myndighetens personuppgiftsbiträde om denne behandlar personuppgifter åt myndigheten.

Det är inte ovanligt att en molntjänstleverantör anlitar underleverantörer för t.ex. underhåll och support av tjänsten. Underleverantörerna kan vara företag som ingår i molntjänstleverantörens egen koncern eller fristående bolag. Oavsett vilket marknads-mässigt förhållande en underleverantör har till molntjänstleverantören så är under-leverantören ett personuppgiftsbiträde till den personuppgiftsansvarige om underleve-rantören behandlar den ansvariges uppgifter inom ramen för sitt uppdrag. Den person-uppgiftsansvarige myndigheten har således också ett skadeståndsrättsligt ansvar för den personuppgiftsbehandling som utförs av underleverantören.

1.3.4 Personuppgiftsbiträdesavtal

Enligt 30 § andra stycket PuL ska det finnas ett skriftligt avtal om personuppgifts-biträdets behandling av personuppgifter för den personuppgiftsansvariges räkning. I det avtalet ska det särskilt föreskrivas att personuppgiftsbiträdet får behandla person-uppgifterna bara i enlighet med instruktioner från den personuppgiftsansvarige och att biträdet är skyldigt att vidta säkerhetsåtgärder enligt 31 § PuL. Instruktionerna till ett personuppgiftsbiträde ska vara så pass tydliga att personuppgiftsbiträdet inte kan utföra någon otillåten behandling av uppgifterna utan att det strider mot avtals-villkoren.

Personuppgiftsbiträdesavtalet är ett av de verktyg som den personuppgiftsansvarige har till sitt förfogande för att förvissa sig om att personuppgiftsbiträdet vidtar nödvändiga säkerhetsåtgärder och i övrigt följer givna instruktioner för person-uppgiftsbehandlingen. Med personuppgiftsbiträdesavtalet följer en form av tystnads-plikt för den som är anställd hos ett personuppgiftsbiträde och som behandlar person-uppgifter för den personuppgiftsansvariges räkning. Tystnadsplikten är emellertid inte straffsanktionerad.

Personuppgiftsbiträdesavtalet ska vidare innehålla instruktioner till biträdet om att denne ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda uppgifterna som behandlas. Utgångspunkten är att uppgifterna inte ska få ett sämre skydd för att behandlingen utförs av ett biträde. Biträdet är därför skyldigt att vidta samma säkerhetsåtgärder som den ansvarige hade behövt vidta om denne själv hade utfört behandlingen. Biträdesavtalet ska också innehålla villkor som garanterar den personuppgiftsansvarige rätt till insyn och kontroll av biträdets behandling av personuppgifter för den ansvariges räkning.

I lagtexten finns inte närmare angivet vilken typ av instruktioner ett personuppgiftsbiträdesavtal ska innehålla.[31] Datainspektionen har i ett tillsynsbeslut angett att instruktionerna till biträdet ska vara så pass tydliga att otillåten behandling av uppgifterna inte kommer att utföras och att instruktionerna bl.a. ska omfatta ändamålen med behandlingen av personuppgifterna och anvisning om när biträdet ska radera personuppgifterna.[32] Datainspektionen har i sina granskningar funnit brister i personuppgiftsbiträdesavtal som tillhandhålls av molntjänstleverantörer. Bristerna har bl.a. varit hänförliga till avtalsvillkor som har varit alltför svårtolkade och otydligt formulerade. Enligt Datainspektionen har avtalsvillkoren bl.a. lämnat utrymme för molntjänstleverantören att behandla den ansvariges personuppgifter för egna ändamål och saknat fastställda tidsramar för molntjänstleverantörens radering av personuppgifterna.[33]

Hur pass tydliga och detaljerade den personuppgiftsansvariges instruktioner till en molntjänstleverantör behöver vara avgörs bl.a. med hänsyn till

- vilka personuppgifter som behandlas,
- vilken typ av molntjänst behandlingen ska utföras i, och
- vilken typ av molntjänstleverantör som ska utföra behandlingen, t.ex. en stor global eller en mindre, nationell aktör.

Om den ansvarige har liten möjlighet till insyn i molntjänstleverantörens personuppgiftsbehandling är det viktigt att instruktionerna i biträdesavtalet är detaljerade och otvetydiga.

1.3.4.1 Underleverantörer som personuppgiftsbiträden

När en personuppgiftsansvarig uppdrar åt en molntjänstleverantör, som personuppgiftsbiträde, att behandla personuppgifter och molntjänstleverantören anlitar egna underleverantörer ska den ansvarige se till att samtliga underleverantörer, som behandlar personuppgifterna, blir bundna av samma avtalsvillkor i biträdesavtalet som personuppgiftsbiträdet. Detta kan göras på olika sätt t.ex. genom att den personuppgiftsansvarige

- självständigt tecknar personuppgiftsbiträdesavtal med samtliga underleverantörer, eller
- i avtal samtycker till att molntjänstleverantören anlitar underleverantörer under förutsättning att denne tecknar avtal med underleverantörerna vari framgår att dessa har samma skyldigheter som det personuppgiftsbiträde, dvs. molntjänstleverantören, som den personuppgiftsansvarige har ingått avtal med.

---

[31] Viss vägledning ges i Datainspektionens informationsblad Molntjänster och personuppgiftslagen. http://www.datainspektionen.se/Documents/faktablad-molntjanster.pdf

[32] Datainspektionens beslut den 31 maj 2013, dnr 1351-2012, (fastställt av Förvaltningsrätten i Stockholm den 1 juli 2014 i mål nr 15410–13).

[33] Datainspektionens beslut den 31 maj 2013, dnr 1351-2012, den 10 juni 2014, dnr 358-2014 och den 18 juli, dnr 988-2014.

Artikel 29-arbetsgruppens[34] uppfattning är att personuppgiftsbiträden endast får lägga ut sin verksamhet på underentreprenad med den personuppgiftsansvariges samtycke, vilket generellt kan lämnas när tjänsten börjar tillhandahållas.[35] En molntjänstleverantör som personuppgiftsbiträde måste ge den ansvarige tillgång till information om vilka underleverantörer som anlitas, beskriva vilken typ av tjänst underleverantören utför, vilka egenskaper nuvarande eller potentiella underleverantörer har och vilka garantier underleverantörerna erbjuder molntjänstleverantören för att dataskyddsdirektivet kommer att följas.[36] Molntjänstleverantören har också en tydlig skyldighet att informera den personuppgiftsansvarige om eventuella planerade ändringar, t.ex. att underleverantörer läggs till eller tas bort. Om den personuppgiftsansvarige motsätter sig att en viss underleverantör anlitas ska denne ha möjlighet att, på skäliga grunder, invända mot ändringarna eller säga upp avtalet.[37] Information till den personuppgiftsansvarige om samtliga underleverantörer som lagrar eller behandlar uppgifter och var dessa är lokaliserade kan molntjänstleverantören t.ex. tillhandahålla i ett offentligt digitalt register.[38]

1.3.5 Säkerheten för personuppgifter

Den personuppgiftsansvarige ansvarar, enligt 31 § PuL, för att vidta lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifterna som behandlas. Åtgärderna ska åstadkomma en säkerhetsnivå som är lämplig med beaktande av

a) de tekniska möjligheter som finns,

b) vad det skulle kosta att genomföra åtgärderna,

c) de särskilda risker som finns med behandlingen av personuppgifterna, och

d) hur pass känsliga de behandlade personuppgifterna är.

När den personuppgiftsansvarige anlitar ett personuppgiftsbiträde, ska denne förvissa sig om att personuppgiftsbiträdet kan genomföra de säkerhetsåtgärder som måste vidtas och se till att personuppgiftsbiträdet verkligen vidtar åtgärderna.

Med organisatoriska säkerhetsåtgärder avses bl.a.

- genomförande av en riskanalys,
- fungerande administrativa rutiner för behandlingen av personuppgifter,
- en fastställd säkerhetspolicy, samt
- rutiner för rapportering och uppföljning av säkerhetsincidenter.

För att kunna avgöra om en personuppgiftsbehandling kan göras i en molntjänst måste den personuppgiftsansvarige genomföra en riskanalys innan den planerade

---

[34] Artikel 29-arbetsgruppen är inrättad enligt artikel 29 i direktiv 95/46/EG. Den är ett oberoende rådgivande EU-organ i frågor som rör dataskydd och integritet.

[35] Se även klausulerna 5 h) och 11.1 i kommissionens standardavtalsklausuler rörande krav på skriftligt förhandstillstånd/samtycke för att ett personuppgiftsbiträde ska få anlita underleverantörer.

[36] Artikel 29-arbetsgruppen yttrande 5/2012 om datormoln (cloud computing), antaget den 1 juli 2012, 010371/12/SV, WP 196, avsnitt 3.3.2 (härefter refererat som WP 196).

[37] WP 196 avsnitt 3.3.2.

[38] WP 196 avsnitt 4.1.

behandlingen påbörjas. Analysen ska omfatta molntjänstleverantörens hantering av uppgifterna och en bedömning av om de säkerhetsåtgärder leverantören erbjuder är tillräckliga för att säkerställa skyddet för den enskildes personliga integritet. Den personuppgiftsansvarige ska också, i samband med riskanalysen, pröva om behandlingen är förenlig med den integritetsskyddslagstiftning myndigheten har att följa och analysera hur integritetsskyddet för personuppgifterna påverkas av den planerade behandlingen.[39]

Med tekniska säkerhetsåtgärder avses bl.a.

- kryptering,
- loggning (uppföljning av behandlingshistorik),
- behörighetsstyrning,
- inloggningslösningar,
- säkerhetskopiering (backup),
- skydd mot skadliga program m.m.

Syftet med de tekniska och organisatoriska säkerhetsåtgärderna är att skydda personuppgifter från förstöring genom olyckshändelse eller otillåtna handlingar eller förlust genom olyckshändelse samt mot ändringar, otillåten spridning av eller otillåten tillgång till uppgifterna.[40]

De risker som generellt brukar aktualiseras vid behandling av personuppgifter i en molntjänst är förknippade med bristande kontroll och insyn i leverantörens behandling av personuppgifterna. En molntjänstleverantör ska därför kunna visa den personuppgiftsansvarige att leverantören har rutiner för

- behörighetsstyrning, dvs. att endast de personer som behöver ta del av personuppgifterna för att kunna utföra sina arbetsuppgifter har tillgång till uppgifterna,
- tillförlitliga loggningsmekanismer,
- att bistå den personuppgiftsansvarige med att tillgodose de registrerades rätt till registerutdrag och att få rättelse, [41] och
- att hjälpa kunden att flytta över eller hämta hem data (portabilitet). [42]

För att tillgodose den personuppgiftsansvariges behov av insyn och kontroll är det viktigt att de tekniska och organisatoriska säkerhetsåtgärder som biträdet ska vidta specificeras skriftligen i avtal. Den personuppgiftsansvarige måste också följa upp att molntjänstleverantören verkligen vidtar de avtalade säkerhetsåtgärderna.

---

[39] I den nya dataskyddsförordningen förslås en s.k. Data Protection Impact Assessment (DPIA) att bli ett obligatoriskt moment när en personuppgiftsbehandling medför särskilda risker för den registrerade.

[40] Art. 17.1 dataskyddsdirektivet.

[41] 26 och 28 §§ PuL.

[42] WP 196 avsnitt 3.4.3 – 3.4.3.6.

1.3.5.1 Underleverantörer

Eftersom ansvaret för att säkerhetsåtgärderna faktiskt vidtas vilar på den personuppgiftsansvarige måste denne också kunna kontrollera att samtliga underleverantörer verkligen vidtar de säkerhetsåtgärder som har avtalats eller som den ansvarige på annat sätt har lämnat instruktioner om. För att det överhuvudtaget ska finnas realistiska möjligheter för insyn, uppföljning och kontroll av underleverantörerna måste den ansvarige ha grundläggande kännedom om vilka dessa är och vilka uppdrag de utför.[43] Den personuppgiftsansvarige måste också se till att avtalsvillkoren i personuppgiftsbiträdesavtalet ger förutsättningar för kontroll av samtliga personuppgiftsbiträden.

1.3.5.2 Kontroll genom tredjepartsrevision

I praktiken torde det vara praktiskt ogörligt för en personuppgiftsansvarig att på plats granska och kontrollera personuppgiftsbehandlingen hos en global molntjänstleverantör. Ur säkerhetsmässig synvinkel kan det också diskuteras om det över huvudtaget är lämpligt att en personuppgiftsansvarig molntjänstkund har möjlighet att, på plats, granska leverantörens utrustning och databehandling. En sådan granskning skulle sannolikt utsätta leverantörens övriga kunder för onödiga risker. Den personuppgiftsansvarige kan istället anlita en oberoende tredje part för att granska biträdets personuppgiftsbehandling. Det förhållandet att kontrollen utförs av en tredje part fråntar dock inte den personuppgiftsansvarige ansvaret för att kontrollerna utförs och för eventuell uppföljning av konstaterade brister.

1.3.6 Tillåten behandling

I 9 § PuL anges de grundläggande kraven på behandlingen av personuppgifter. För att en personuppgiftsbehandling ska vara tillåten ska den personuppgiftsansvarige se till att samtliga villkor som stadgas i 9 § är uppfyllda. Nedan redogörs för de villkor i 9 § PuL, samt motsvarande bestämmelser i registerförfattningar, som är av särskilt intresse vid myndigheters behandling av personuppgifter i en molntjänst.

1.3.6.1 Ändamålen med behandling av personuppgifter och finalitetsprincipen

I registerförfattningar är det ofta särskilt reglerat för vilka ändamål en myndighet får behandla personuppgifter, s.k. ändamålsbestämmelser. Det förekommer att ändamålen delas upp i primära och sekundära sådana. De primära ändamålen syftar till att tillgodose den behandling som behövs i myndighetens egen verksamhet medan de sekundära ändamålen tar sikte på myndighetens utlämnande av uppgifter för att tillgodose andras behov. Syftet är således att göra det tydligt hur uppgifterna får användas i den egna verksamheten och för vilka syften de får lämnas ut till andra. Ett utlämnande av personuppgifter som sker som ett led i den egna verksamheten, inte i syfte att tillgodose andras behov, anses vanligtvis omfattas av de primära ändamålen.[44]

I registerförfattningar förekommer dels uttömmande bestämningar av samtliga ändamål – såväl primära som sekundära – för vilka behandling får ske, dels den

[43] Datainspektionen har i sina granskningar funnit brister i personuppgiftsansvarigas insyn i vilka underleverantörer som anlitas av en molntjänstleverantör, se t.ex. Datainspektionens beslut den 31 maj 2013, dnr 1351-2012 och den 25 april 2014, dnr 1475-2013.

[44] Myndighetsdatalag, SOU 2015:39, s. 269

varianten att de i författningen angivna ändamålen kompletteras med en möjlighet att vidarebehandla redan insamlade uppgifter även för ändamål som inte är oförenliga med insamlingsändamålet. Skillnaden består således i att lagstiftaren i det senare fallet har gett den personuppgiftsansvariga myndigheten utrymme att själv bestämma kompletterande ”sekundära” ändamål. Det är alltså myndigheten själv som måste beakta finalitetsprincipen. Man brukar då tala om att ”finalitetsprincipen tillämpas” men vad som i strikt rättslig mening avses är snarare en tillämpning av bestämmelsen i 9 § första stycket d) PuL.[45]

Enligt 9 § första stycket d) PuL ska den personuppgiftsansvarige se till att personuppgifter inte behandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in. Bestämmelsen ger uttryck för den ovan nämnda finalitetsprincipen. Finalitetsprincipen kan aktualiseras vid en myndighets behandling av personuppgifter i en molntjänst. När myndigheten är personuppgiftsansvarig måste all behandling av personuppgifter som sker under myndighetens ansvar, oavsett om myndigheten själv utför behandlingen eller uppdrar åt ett biträde att göra den, omfattas av myndighetens tillåtna ändamål för behandling eller av finalitetsprincipen. En myndighet kan inte instruera ett biträde att utföra en personuppgiftsbehandling som inte myndigheten lagligen skulle kunna utföra själv.[46]

1.3.6.2 Laglig behandling

Enligt 9 § första stycket a) PuL ska den personuppgiftsansvarige se till att personuppgifter behandlas bara om det är lagligt. Att behandlingen ska vara laglig innebär både att den ska vara förenlig med personuppgiftslagen men också att den ska vara tillåten enligt annan tillämplig lagstiftning t.ex. offentlighets- och sekretesslagen. När en personuppgiftsansvarig lämnar ut personuppgifter till en annan personuppgiftsansvarig får de ändamål för vilka mottagaren ska behandla uppgifterna, inte vara oförenliga med avsändarens ursprungliga ändamål för vilka uppgifterna initialt samlades in. Om så är fallet torde mottagarens behandling av personuppgifterna (insamlingen) för ett oförenligt ändamål strida mot kravet på att behandlingen ska vara laglig i 9 § första stycket a). En personuppgiftsansvarig får inte heller lämna ut personuppgifter till någon annan om det kan antas att denne ska behandla personuppgifterna på ett sätt som inte är tillåtet enligt personuppgiftslagen eller annan tillämplig lagstiftning. Då strider redan själva utlämnandet mot kravet i 9 § första stycket a) PuL om att den personuppgiftsansvarige ska se till att personuppgifter bara behandlas om det är lagligt.[47]

Den faktiska tillämpningen av bestämmelserna om ändamål, finalitetsprincipen och laglig behandling kan bäst illustreras genom ett par beskrivande exempel.

Myndighet A uppdrar åt en molntjänstleverantör att lagra personuppgifter åt myndigheten i en molntjänst. Av myndighetens instruktioner till molntjänstleverantören i personuppgiftsbiträdesavtalet framgår tydligt att leverantören inte får utföra någon annan behandling av uppgifterna utöver lagringen. Den lagring av personuppgifter som myndigheten är personuppgiftsansvarig för omfattas av myndig-

[45] Myndighetsdatalag, SOU 2015:39 s. 270-271

[46] Datainspektionens beslut den 3 juli 2015, dnr 518-2015 och 643-2015

[47] Personuppgiftslagen, En kommentar, Sören Öman och Hans-Olof Lindblom, fjärde upplagan, 2011, s. 196.

hetens tillåtna ändamål för behandling av personuppgifter, leverantören följer instruktionerna i biträdesavtalet, och behandlingen är förenlig med 9 § första stycket a) PuL.

Myndighet B anlitar en molntjänstleverantör för tillhandahållande av en dokumenthanteringstjänst. De personuppgifter som kommer att hanteras i tjänsten är begränsade till vissa uppgifter som myndighetens anställda måste uppge för att skapa användarkonton. Av personuppgiftsbiträdesavtalet, som har upprättas av molntjänstleverantören, framgår att leverantören, i eget syfte, kommer att behandla personuppgifterna som hanteras i tjänsten för marknadsföringsändamål.[48] Den personuppgiftsbehandling som leverantören utför i detta syfte ligger utanför myndighetens kontroll och leverantören är sannolikt att betrakta som personuppgiftsansvarig för den behandlingen. Myndigheten måste, som personuppgiftsansvarig, ta ställning till om det är förenligt med myndighetens ändamålsbestämmelser eller med finalitetsprincipen att lämna ut uppgifterna till leverantören för att behandlas i marknadsföringssyfte.[49] Om myndigheten bedömer att leverantörens behandling av personuppgifter för marknadsföringsändamål inte omfattas av myndighetens egna ursprungliga ändamål för behandling och inte heller är förenlig med finalitetsprincipen är utlämnandet av uppgifterna till leverantören inte förenligt med PuL:s ändamålsbestämmelser eller finalitetsprincipen. Molntjänstleverantörens planerade behandling torde då i sin tur vara i strid med kravet på laglig behandling i 9 § första stycket a) PuL.

Myndighet C anlitar en molntjänstleverantör för bearbetning av uppgifter som rör enskildas hälsa. Den bearbetning som utförs av leverantören omfattas av myndighetens tillåtna ändamål för behandling av personuppgifterna. Myndigheten gör bedömningen att hanteringen är förenlig med integritetsskyddslagstiftningen, tecknar ett personuppgiftsbiträdesavtal med tydliga instruktioner och påbörjar överföringen av uppgifterna till leverantören. I detta skede har dock myndigheten missat att göra en sekretessprövning för att kontrollera om uppgifterna över huvudtaget kan lämnas ut eller om de omfattas av sekretess i förhållande till molntjänstleverantören. En förutsättning för att behandlingen av personuppgifter ska vara laglig enligt 9 § första stycket a) PuL är att behandlingen är förenlig med övriga tillämpliga lagar, i detta fall offentlighets- och sekretesslagen. I samband med att en sekretessprövning utförs bedömer myndigheten att uppgifterna är sekretessbelagda och inte kan lämnas ut till leverantören. Eftersom den pågående personuppgiftsbehandlingen inte är förenlig med offentlighets- och sekretesslagen är den inte heller laglig enligt 9 § första stycket a) PuL.

1.3.7 Överföring av personuppgifter till tredje land

Dataskyddsdirektivet kräver att samtliga medlemsstater, och EES-stater, har ett likvärdigt skydd för personuppgifter och personlig integritet. Därför kan personuppgifter fritt överföras mellan dessa länder utan några juridiska begränsningar. Eftersom det inte finns några generella regler som ger motsvarande garantier utanför EU/EES har det ansetts att överföring till sådana länder behöver begränsas. Personuppgifter får därför föras över till tredje land om det finns en adekvat skydds-

[48] I exemplet beaktas inte annan lagstiftning som kan vara tillämpligt utöver personuppgiftslagen.

[49] Myndigheten måste också pröva om utlämnandet är förenligt med 21 kap. 7 § OSL.

nivå i mottagarlandet eller om det finns särskilda garantier för att uppgifterna och de enskilda individernas personliga integritet skyddas.

Enligt huvudregeln i 33 § PuL är det förbjudet att till tredje land föra över personuppgifter som är under behandling om landet inte har en adekvat nivå för skyddet av personuppgifterna. Förbudet gäller också överföring av personuppgifter för behandling i tredje land. Frågan om en skyddsnivå är adekvat ska bedömas mot bakgrund av samtliga omständigheter kring överföringen. Särskild vikt ska läggas vid uppgifternas art, ändamålet med behandlingen, hur länge behandlingen ska pågå, ursprungslandet, det slutliga bestämmelselandet och de regler för behandlingen som finns i det tredje landet.

I 34 § PuL anges ett antal undantag från förbudet mot överföring av personuppgifter till tredje land. Dessa undantag, som är strikt avgränsade, rör främst fall där riskerna för den registrerade är förhållandevis små, där andra intressen har företräde framför den registrerades rätt till skydd för den personliga integriteten eller där den registrerade har lämnat sitt samtycke till överföringen. Utan att gå in i detalj på varje enskilt undantag kan det kortfattat konstateras att det ytterst sällan torde komma ifråga att en överföring av personuppgifter till tredje land i en (global) molntjänst kan ske med stöd av något av undantagen i 34 § PuL. Molntjänster utmärks ofta av att den information som behandlas flödar över nationsgränserna på ett sätt som är omöjligt för den personuppgiftsansvarige att ha insyn i och utöva kontroll över. Informationen kan finnas i ett datacenter på förmiddagen och vara på andra sidan jordklotet på eftermiddagen. Det är osannolikt att en molnkund i realtid känner till var dennes information behandlas, lagras eller överförs. Mot denna bakgrund ter det sig varken praktiskt eller realistiskt möjligt för en molnkund att vid varje överföringstillfälle avgöra om det mottagande landet har en adekvat skyddsnivå för skyddet av personuppgifter eller att bedöma om någon av undantagsbestämmelserna i 34 § PuL är tillämpliga. Vidare anser artikel 29-arbetsgruppen att undantagen endast ska tillämpas när överföringarna varken är återkommande, omfattande eller strukturella.[50]

De rättsliga instrument som vanligtvis används som lagligt stöd för att överföra personuppgifter till ett personuppgiftsbiträde i tredje land är hänförliga till 35 § PuL. Enligt denna bestämmelse får regeringen meddela föreskrifter om undantag från förbudet i 33 § för överföring av personuppgifter till vissa stater. Regeringen får också meddela föreskrifter om att överföring av personuppgifter till tredje land är tillåten om överföringen regleras av ett avtal som ger tillräckliga garantier till skydd för de registrerades rättigheter. Regeringen eller den myndighet som regeringen bestämmer får vidare meddela föreskrifter om undantag från förbudet i 33 §, om det behövs med hänsyn till ett viktigt allmänt intresse eller om det finns tillräckliga garantier till skydd för den registrerades rättigheter. Regeringen får under de förutsättningar som nämns i andra stycket i enskilda fall besluta om undantag från förbudet i 33 §. Regeringen får överlåta åt tillsynsmyndigheten att fatta sådana beslut.

Med stöd av 35 § PuL finns bl.a. följande rättsliga instrument tillgängliga för att möjliggöra överföring av personuppgifter till tredje land:

---

[50] Article 29 Working Party, Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995 (WP 114, 2093/05/EN), 25 November 2005, s. 9

- Regeringens föreskrifter i enlighet med 13 § punkten 1 PuF, att personuppgifter får föras över till tredje land om och i den utsträckning som Europeiska kommissionen har konstaterat att landet har en adekvat nivå för skyddet av personuppgifter.[51]
- EU-kommissionens standardavtalsklausuler.[52]
- Datainspektionens beslut i enskilda fall om den personuppgiftsansvarige ställer tillräckliga garantier till skydd för de registrerades rättigheter.[53]
- Binding Corporate Rules.[54]

Ett lagligt stöd som har använts frekvent för överföring av personuppgifter till USA är det numera ogiltigförklarade Safe Harbor. Nedan följer en mer detaljerad genomgång av de ovan uppräknade rättsliga instrumenten inklusive Safe Harbor-beslutet. Det bör nämnas att personuppgiftslagen kan medge överföring av personuppgifter till tredje land även under andra omständigheter. Dessa redogörs inte för här eftersom bedömningen gjorts att de inte är relevanta som rättsligt stöd för tredjelandsöverföring vid behandling av personuppgifter i en molntjänst.

1.3.7.1 EU-kommissionens beslut om adekvat skyddsnivå

Regeringen har getts behörighet att meddela föreskrifter om generella undantag från förbudet för överföring av personuppgifter till vissa stater. Bakgrunden är att dataskyddsdirektivet kräver att överföring av personuppgifter tillåts till stater som i viss ordning har en adekvat skyddsnivå. Länder som har konstaterats ha en adekvat skyddsnivå är bl.a. Schweiz, Argentina, Nya Zeeland och Uruguay. En personuppgiftsansvarig behöver inte vidta några särskilda åtgärder för att föra över personuppgifter till länder som omfattas av ett beslut av EU-kommissionen om adekvat skyddsnivå.

1.3.7.2 Safe Harbor-principerna

Safe Harbor-principerna är en samling integritetsskyddsprinciper som har utfärdats av Förenta Staternas handelsministerium (US Department of Commerce). Den 26 juli 2000 antog EG-kommissionen beslut 2000/520/EG (Safe Harbor-beslutet) som erkänner att Safe Harbor-principerna och de frågor och svar som Förenta staternas handelsministerium har utfärdat medger en adekvat nivå för skyddet av person-

[51] Enligt art. 25.6 i Dataskyddsdirektivet kan kommissionen konstatera att ett tredje land genom sin interna lagstiftning eller på grund av de internationella förpliktelser som åligger landet har en skyddsnivå som är adekvat. Medlemsstaterna ska vidta de åtgärder som är nödvändiga för att följa kommissionens beslut. Kommissionens beslut har genomförts i Sverige genom 13 § punkten 1 personuppgiftsförordningen och bilaga 1 till förordningen vari kommissionens beslut om adekvat skyddsnivå anges.

[52] Kommissionens beslut om standardavtalsklausuler har genomförts genom 13 § punkten 2 personuppgiftsförordningen och bilaga 2 till förordningen.

[53] Regeringen har genom 14 § personuppgiftsförordningen överlåtit åt Datainspektionen att meddela beslut i enskilda fall om det finns tillräckliga garantier till skydd för de registrerades rättigheter.

[54] Regeringen har genom 14 § personuppgiftsförordningen överlåtit åt Datainspektionen att meddela beslut i enskilda fall om det finns tillräckliga garantier till skydd för de registrerades rättigheter.

uppgifter som överförs från EU till en mottagare i USA som har anslutit sig till principerna.[55]

Safe Harbor-systemet bygger på att anslutna företag årligen genomför en självcertifiering som lämnas in till Förenta staternas handelsministerium och att företagen har en allmänt tillgänglig integritetsskyddspolicy vari anges att företaget är anslutet till, och efterlever, Safe Harbor-principerna. Safe Harbor-principerna innehåller krav på både det materiella skyddet av personuppgifter och de registrerades processuella rättigheter. I Safe Harbor-beslutet finns emellertid undantag för när efterlevnaden av principerna kan begränsas om det är befogat med hänsyn till krav i fråga om nationell säkerhet, allmänintresset och rättsefterlevnaden eller till lagar, myndighetsföreskrifter eller rättspraxis.

På senare år har det framkommit allt större farhågor rörande skyddsnivån för personuppgifter som överförs inom ramen för Safe Harbor-systemet, i synnerhet efter att Förenta staternas övervakningsprogram Prism avslöjades i juni 2013. EU-kommissionen har den 27 november 2013 antagit två meddelanden om hur Safe Harborprinciperna fungerar och hur förtroendet för dataflöden mellan EU och Förenta staterna kan återskapas.[56] I kommissionens meddelanden ifrågasätts bl.a. skyddsnivån som Safe Harbor-systemet erbjuder. Det förhållandet att systemet bygger på frivillighet och självcertifiering innebär t.ex. att vissa företag inte efterlever principerna, trots att de är anslutna. Det framförs också kritik mot bristande insyn, transparens och tillsyn av anslutna företag och ifrågasätts huruvida den storskaliga insamlingen och behandlingen av personuppgifter inom ramen för de amerikanska övervakningsprogrammen är nödvändig och proportionerlig med hänsyn till de nationella säkerhetsintressena.[57]

De farhågor som funnits under de senaste åren konkretiserades den 6 oktober 2015 när EU-domstolen i ett förhandsavgörande[58] ogiltigförklarade kommissionens Safe Harbor-beslut. Domstolen fastställde vidare att det förhållandet att kommissionen har fattat beslut i enlighet med art. 25.6 i dataskyddsdirektivet, såsom t.ex. Safe Harborbeslutet, inte hindrar eller inskränker nationella dataskyddsmyndigheters rätt att pröva en persons begäran om skydd för sina fri- och rättigheter när denne person gör gällande att ett sådant beslut inte säkerställer en adekvat skyddsnivå i mottagarlandet.

Av skälen till domstolens beslut att ogiltigförklara kommissionens Safe Harbor-beslut framgår bl.a. följande. Safe Harbor-principerna är uteslutande tillämpliga på självcertifierade amerikanska organisationer som erhåller personuppgifter från unionen. Det finns inget krav på att amerikanska myndigheter ska iaktta Safe Harbor-

---

[55] På amerikanska handelsdepartementets webbplats finns en lista över företag som är anslutna till Safe Harborprinciperna. https://safeharbor.export.gov/list.aspx

[56] Meddelande från Kommissionen till Europaparlamentet och Rådet COM(2013) 846 final Återskapande av förtroendet för dataflöden mellan EU och Förenta staterna" och COM(2013) 847 final Om hur principerna om integritetsskydd (safe harbour) fungerar när det gäller EU:s medborgare och företag som är etablerade i EU, antagna den 27 november 2013. Meddelandena åtföljdes av Report on Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection, 27 November 2013.

[57] COM(2013) 846 final s. 4.

[58] Mål C-362/14 den 6 oktober 2015

principerna. I Safe Harbor-beslutet stadgas ett antal undantag för när en ansluten organisation kan göra avsteg från principerna. Undantagen härrör till vad som är nödvändigt för att uppfylla krav i fråga om [amerikansk] nationell säkerhet, allmänintresset och rättsefterlevnaden. Vidare understryks i Safe Harbor-beslutet att ”självklart måste amerikanska organisationer, om de i amerikansk lag har en motstridig skyldighet, oberoende av om de anslutit sig till Safe Harbor eller inte, följa lagen”. De angivna undantagen i Safe Harbor-beslutet innebär att amerikanska krav i fråga om nationell säkerhet, allmänintresset och rättsefterlevnaden har företräde framför Safe Harbor-principerna. Till detta kommer den omständigheten att det i Safe Harbor-beslutet inte anges att det finns något effektivt rättsmedel för enskilda att få prövat lagligheten av de ingrepp i de grundläggande rättigheterna som uppstår på grund av statliga åtgärder. Sammanfattningsvis menar EU-domstolen att de begränsningar som medges av undantagen i Safe Harbor-beslutet strider mot den grundläggande rätten till respekt för privatlivet, skydd för personuppgifter och rätten till ett effektivt rättsmedel.[59]

EU-domstolens dom innebär att Safe Harbor-beslutet inte längre kan åberopas som ett lagligt stöd för överföring av personuppgifter till Safe Harbor-anslutna bolag i USA. För närvarande pågår förhandlingar mellan EU-kommissionen och amerikanska handelsdepartementet för att reformera Safe Harbor-principerna. Kommissionens målsättning är att förhandlingarna ska vara avslutade i februari 2016.[60] EU-domstolens dom klargör också på ett tydligt sätt att enskilda kan vända sig till de nationella dataskyddsmyndigheterna för att få prövat om en överföring av dennes personuppgifter till tredje land, som sker med stöd av ett beslut från EU-kommission, uppfyller kraven på adekvat skyddsnivå.

1.3.7.3 EU-kommissionens standardavtalsklausuler

Regeringen har getts behörighet att meddela föreskrifter om generella undantag från förbudet mot tredjelandsöverföring när överföringen regleras av ett avtal som ger tillräckliga garantier till skydd för de registrerades rättigheter. Bakgrunden är här att EG-direktivet kräver att överföring ska tillåtas om överföringen regleras av ett avtal som innehåller vissa standardavtalsklausuler till skydd för de registrerades rättigheter.

EU-kommissionen har bl.a. fattat beslut om standardavtalsklausuler som kan användas vid överföring av personuppgifter till ett personuppgiftsbiträde i tredje land. [61] Standardavtalsklausulerna är en uppsättning avtalsklausuler som innehåller skyldigheter dels för personuppgiftsansvariga som vill föra över uppgifter till tredje land, dels för personuppgiftsbiträden som tar emot sådana uppgifter.[62] Klausulerna reglerar

---

[59] Art. 7, 8 och 47 Europeiska unionens stadga om de grundläggande rättigheterna, 2012/C 326/02 (EU-stadgan).

[60] Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgement by the Court of Justice in Case C-362/14 (Schrems), Brussels, 6.11.2015, COM(2015) 566 final, s. 15.

[61] Kommissionens beslut, 2010/87/EU, den 5 februari 2010 om standardavtalsklausuler för överföring av personuppgifter till registerförare etablerade i tredjeland i enlighet med Europarådet och rådets direktiv 95/46/EG.

[62] Standardavtalsklausulerna använder begreppen ”uppgiftsutförare” och ”uppgiftsinförare” i stället för personuppgiftsansvarig och personuppgiftsbiträde. För enkelhetens skull används dock enbart de sistnämnda begreppen i denna rapport.

också andra frågor kring överföringen, som till exempel de registrerades rättigheter och hur tvister med anledning av avtalet ska lösas. Syftet med avtalsklausulerna är att ge tillräckliga garantier för att enskildas rättigheter ska skyddas vid överföring av personuppgifter till länder som inte har en adekvat skyddsnivå.

Vid användning av standardavtalsklausulerna måste bl.a. följande beaktas.

- Den personuppgiftsansvarige ska teckna standardavtalsklausuler med ett personuppgiftsbiträde som är etablerat i tredje land. Det är relativt vanligt att större molntjänstföretag har dotterbolag som är etablerade inom EU/EES-området och som är den huvudsakliga avtalsparten till kunden. Standardavtalsklausulerna ska emellertid ingås med ett bolag som är etablerat utanför EU/EES-området. Alternativt kan den personuppgiftsansvarige, t.ex. i personuppgiftsbiträdesavtalet, ge det EU-baserade personuppgiftsbiträdet i uppdrag att ingå standardavtalsklausuler med ett biträde i tredje land för den ansvariges räkning.[63]
- Avtalsparterna får, enligt klausul 10, inte göra några ändringar i standardavtalsklausulerna.
- Eventuella tillägg i standardavtalsklausulerna får inte, direkt eller indirekt, motsäga avtalsvillkoren eller påverka den registrerades grundläggande fri- och rättigheter.[64]
- I tillägg 1 och 2 till standardavtalsklausulerna förväntas parterna bl.a. föra in information om vilken typ av uppgifter som överförs och hur de kommer att behandlas samt vilka säkerhetsåtgärder personuppgiftsbiträdet ska vidta.

I standardavtalsklausulerna finns avtalsvillkor som rör personuppgiftsbiträdets möjlighet att använda sig av underleverantörer för att utföra behandlingen av personuppgifter. För att ett personuppgiftsbiträde ska kunna anlita underleverantörer måste den personuppgiftsansvarige ha lämnat sitt samtycke till detta enligt klausul 11.1. Ett sådant samtycke kan vara generellt och lämnas på förhand, t.ex. skriftligt i huvudavtalet eller i personuppgiftsbiträdesavtalet. En ytterligare förutsättning för att det ska vara tillåtet att anlita underleverantörer är att dessa genom ett skriftligt avtal, åläggs samma skyldigheter som enligt standardavtalsklausulerna åligger personuppgiftsbiträdet. Detta kan ske genom att underleverantören undertecknar de standardavtalsklausuler som ingåtts mellan den ansvarige och dess biträde eller genom att personuppgiftsbiträdet tecknar ett separat avtal med underleverantören vari i denna åläggs samma skyldigheter som biträdet. Enligt klausul 5 j) är personuppgiftsbiträdet skyldigt att omedelbart översända en kopia av ett sådant avtal till den personuppgiftsansvarige.

Det finns ytterligare ett par villkor i standardavtalsklausulerna som hänför sig till personuppgiftsbiträdets skyldigheter som kan vara värda att nämna.

- Enligt klausul 5 d) i) – iii) ska personuppgiftsbiträdet utan dröjsmål underrätta den personuppgiftsansvarige om

---

[63] Article 29 Data Protection Working Party, WP 176, FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC, Adopted on 12 July 2010, s. 4.

[64] Frequently asked questions relating to transfers of personal data from the EU/EEA to third countries, s. 28. http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf

i) varje rättsligt bindande begäran från rättsliga myndigheter om utlämnande av personuppgifterna, om inte detta är förbjudet på grund av exempelvis ett straffrättsligt förbud som syftar till att bevara sekretessen vid brotts-utredningar,

ii) varje oavsiktlig eller otillåten åtkomst, och

iii) varje förfrågan direkt från de registrerade, utan att svara på dem om han inte givits tillstånd till det.

Vidare ska personuppgiftsbiträdet enligt klausul 5 f) godta och garantera att på den personuppgiftsansvariges begäran ställa sin databehandlingsutrustning till förfogande för granskning av den uppgiftsbehandling som dessa klausuler avser; granskningen ska genomföras av den personuppgiftsansvarige eller av ett inspektionsorgan med oberoende och sakkunniga ledamöter; de av tystnadsplikt bundna ledamöterna utses av den personuppgiftsansvarige.

I klausul 12 regleras parternas skyldigheter efter det att behandlingen av person-uppgifter har upphört. Enligt punkten 1 är personuppgiftsbiträdet skyldigt att, beroende på vad den personuppgiftsansvarige beslutar, antingen återlämna alla överförda personuppgifter och kopior av dessa till den ansvarige eller förstöra alla personuppgifter och intyga för den ansvarige att så skett. Enligt punkten 2 ska personuppgiftsbiträdet och underleverantören garantera att de på den ansvariges och/eller tillsynsmyndighetens begäran kommer att ställa sin databehandlings-utrustning till förfogande för en granskning av de åtgärder som anges i punkten 1.

Klausulerna 3 och 6 reglerar tredjepartsberättigande och ansvarsfrågan och mot vilken part en registrerad, som har lidit skada, kan rikta ersättningskrav. Huvudregeln är att den registrerade ska rikta ersättningskrav till den personuppgiftsansvarige. I undantagsfall, t.ex. när den ansvarige har upphört att existera i faktisk eller rättslig mening eller hamnat på obestånd, har den registrerade rätt att väcka talan och erhålla skadestånd från personuppgiftsbiträdet eller, under ytterligare undantagsförhållanden, en underleverantör.

Vissa avtalsvillkor i standardavtalsklausulerna är dåligt anpassade för förhållanden mellan en molntjänstleverantör och den personuppgiftsansvarige. Det vore troligen olämpligt ur säkerhetssynpunkt att t.ex. ge en personuppgiftsansvarig tillträde till molntjänstleverantörens lokaler för att kontrollera ”databehandlingsutrustningen” på sätt som anges i klausulerna 5 f) och 12.2.

Avtalsvillkor som rör bl.a. revision, ansvarsfördelning, incidentrapportering och andra skyldigheter som ankommer på personuppgiftsbiträdet regleras ofta i det (standard)avtal som tillhandahålls av molntjänstleverantören. För att undvika förekomsten av motstridiga avtalsvillkor i standardavtalsklausulerna i förhållande till molntjänstleverantörens egna standardavtal är det av stor vikt att en personuppgifts-ansvarig granskar leverantörens egna avtal och jämför dessa med villkoren i standard-avtalsklausulerna. I synnerhet i förhållande till de avtalsklausuler som har refererats ovan.

Med beaktande av EU-domstolens ogiltigförklarande av Safe Harbor-beslutet bör slutligen klausul 5 b) i standardavtalsklausulerna nämnas. Av denna klausul framgår att personuppgiftsbiträdet godtar och garanterar att han inte har anledning att förmoda att den lagstiftning som är tillämplig på honom hindrar honom från att fullfölja den personuppgiftsansvariges instruktioner och sina skyldigheter enligt detta avtal; om

lagstiftningen ändras på ett sätt som sannolikt har en avsevärt skadlig inverkan på de garantier som klausulerna innebär, ska han anmäla ändringen till den personuppgiftsansvarige, varvid personuppgiftsbiträdet har rätt att avbryta överföringen av uppgifter och/eller häva avtalet.

Standardavtalsklausulerna ställer långtgående krav på skyddet för personuppgifter, krav som inte i alla delar är faktiskt och praktiskt tillämpbara i förhållandet mellan en personuppgiftsansvarig och en molntjänstleverantör. Standardavtalsklausulerna ställer också höga krav på insyn och transparens till förmån för den ansvarige när biträdet avser att anlita underleverantörer för behandlingen av personuppgifter. Datainspektionens granskningar har visat att dessa krav på transparens och insyn i vissa fall förbigås, vilket medför förlust av kontroll för den personuppgiftsansvarige. Trots de brister som redovisats här torde standardavtalsklausulerna vara det instrument som mest frekvent används av en personuppgiftsansvarig som vill överföra personuppgifter till en molntjänstleverantör som är etablerad i tredje land. Det förtjänar dock att poängteras att avtalsparterna måste följa samtliga avtalsvillkor i standardavtalsklausulerna för att personuppgifterna ska anses åtnjuta en adekvat skyddsnivå.

EU-domstolens ogiltigförklarande av Safe Harbor-beslutet[65] ger anledning att fundera över om standardavtalsklausulerna, under alla förhållanden, kan garantera en adekvat skyddsnivå för uppgifter som överförs till tredje land. En personuppgiftsansvarig bör i vart fall inte per automatik kunna förlita sig på att användningen av standardavtalsklausulerna säkerställer en adekvat skyddsnivå för personuppgifterna som överförs. Den personuppgiftsansvarige måste också räkna med att den nationella dataskyddsmyndigheten kan komma att pröva om de överförda personuppgifterna omgärdas av adekvat skydd. För att säkerställa ett adekvat skydd för personuppgifterna torde den personuppgiftsansvarige, utöver att teckna standardavtalsklausuler, även behöva ta ställning till andra omständigheter som kan påverka skyddet för personuppgifterna, t.ex. mottagarlandets nationella lagstiftning och utländska myndigheters möjlighet att ta del av uppgifterna i fråga, mottagarlandets geopolitiska förutsättningar och den politiska stabiliteten i landet överlag.

1.3.7.4 Datainspektionens beslut i enskilda fall

Enligt 14 § PuF får Datainspektionen i enskilda fall besluta om undantag från förbudet att föra över personuppgifter till tredje land om det finns tillräckliga garantier till skydd för de registrerades rättigheter. Sådana garantier kan exempelvis framgå av lämpliga avtalsklausuler. För att en personuppgiftsansvarig ska beviljas undantag i enlighet med 14 § PuF måste ansökan ställas till Datainspektionen. Datainspektionen beslutar, efter granskning av de garantier som ställs till skydd för de registrerades rättigheter, om undantag ska beviljas eller inte. Ett beslut om undantag är specificerat till en typ av överföring och till en specificerad mottagare. Datainspektionen kan inte på förhand besluta om undantag för framtida överföringar till okända mottagare i tredje land. En avtalslösning som svarar mot kraven i 14 § PuF måste således rikta in sig på en noggrann specifikation och lämplig anpassning till överföringen i fråga. Att avtalet måste anpassas noggrant till varje enskild överförings särdrag innebär att

[65] Mål C-362/14 den 6 oktober 2015.

avtalsreglering passar särskilt bra när uppgiftsöverföringarna är likartade eller upprepas.

Mot bakgrund av att undantag enligt 14 § PuF enbart beviljas i enskilda fall till en angiven mottagare och för specificerade överföringar torde det endast vara i sällsynta fall som en personuppgiftsansvarig molntjänstkund anser det lämpligt att ansöka om undantag enligt bestämmelsen.

1.3.7.5 Binding Corporate Rules – Företagsinterna regler

Regeringen får under vissa förutsättningar i enskilda fall besluta om undantag från förbudet mot överföring av personuppgifter till tredje land. Regeringen får överlåta åt tillsynsmyndigheten att fatta sådana beslut, 35 § tredje stycket PuL. Regeringen har genom 14 § PuF överlåtit åt Datainspektionen att meddela beslut om undantag i enskilda fall om det finns tillräckliga garantier till skydd för de registrerades rättigheter. Datainspektionen kan fatta beslut om undantag från överföringsförbudet om en internationell koncern har tagit fram Binding Corporate Rules (BCR) dvs. enhetliga och bindande företagsinterna regler, som ger ett tillräckligt skydd för personuppgifter som överförs inom företagets internationella koncern. Artikel 29-gruppen har utarbetat ett system för de europeiska tillsynsmyndigheternas granskning av enhetliga, bindande företagsinterna regler.

Initialt var det endast möjligt att ansöka om undantag för BCR för överföring av uppgifter till personuppgiftsansvariga inom samma koncern. Sedan den 1 januari 2013 är det emellertid möjligt för internationella koncerner att ta fram BCR för den behandling av personuppgifter som koncernbolagen utför i rollen som personuppgifts-biträden. Syftet är att personuppgiftsansvariga som anlitar bolag i internationella koncerner som personuppgiftsbiträden ska kunna förlita sig på att överföringar av personuppgifter till tredje land inom koncernen omgärdas av tillräckliga säkerhets-åtgärder. Vid användning av BCR för personuppgiftsbiträden, som lagligt stöd för tredjelandsöverföring, måste BCR biläggas avtalet mellan den ansvarige och biträdet.

Institutet med BCR för personuppgiftsbiträden är nytt och ansökningsproceduren är förhållandevis tidsödande. Enligt den lista som tillhandahålls på kommissionens webbplats synes ännu ingen global molntjänstleverantör har fått beslut om undantag med stöd av BCR.[66]

1.3.8 Förhållandet mellan tryckfrihetsförordningen, offentlighets- och sekretesslagen och personuppgiftslagen

Allmänhetens rätt att få tillgång till allmänna handlingar framgår av tryckfrihets-förordningen. Denna rätt har företräde framför dataskyddsbestämmelserna i person-uppgiftslagen och myndigheternas registerförfattningar. Personuppgiftslagen och delar av offentlighets- och sekretesslagen har samma syfte, nämligen att skydda den enskildes integritet. Trots detta är regelverken inte alls likstämmiga eller utbytbara. En myndighet som uppdrar åt ett personuppgiftsbiträde, t.ex. en molntjänstleverantör, att behandla personuppgifter för myndighetens räkning måste därför beakta såväl

[66] På EU-kommissionens webbplats finns en lista över de företag som har fått beslut om undantag för tredjelandsöverföring av personuppgifter med stöd av BCR. http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm

sekretesslagstiftningen som integritetsskyddslagstiftningen och se till att åtgärden är förenlig med båda dessa regelverk.

Ett personuppgiftsbiträde utgör inte en tredje man i personuppgiftslagens mening, 3 § PuL. Överlämnandet av personuppgifter till en molntjänstleverantör, som ska behandla uppgifter för myndighetens räkning, utgör därför inte ett utlämnande (behandling) i integritetsskyddshänseende. Ur sekretesshänseende förhåller det sig emellertid annorlunda. Ett personuppgiftsbiträde ska alltid finnas utanför den personuppgiftsansvariges organisation och ingår därmed inte i den personkrets som enligt 2 kap. 1 § OSL deltar i myndighetens verksamhet. Ett överlämnande av uppgifter till en molntjänstleverantör kan därför utgöra ett röjande enligt offentlighets- och sekretesslagen även om leverantören är personuppgiftsbiträde åt myndigheten. Röjandebegreppet är i sin tur delvis skilt från vad som utgör ett utlämnande eller en expediering enligt tryckfrihetsförordningen.

Ett överlämnande av personuppgifter till ett personuppgiftsbiträde är inte en behandling enligt personuppgiftslagen och utgör således inte ett ”utlämnande” av personuppgifter till biträdet enligt personuppgiftslagen. Eftersom biträdet finns utanför den personuppgiftsansvariges egen organisation måste den ansvarige dock pröva om det är tillåtet enligt offentlighets- och sekretesslagen att lämna ut uppgifterna till biträdet eller om sekretess utgör hinder för ett sådant utlämnande. Slutligen måste myndigheten beakta om personuppgiftsbiträdet kommer att utföra annan hantering än enbart teknisk lagring eller teknisk bearbetning av myndighetens handlingar. Om så är fallet har myndigheten att räkna med att handlingarnas status kan komma att förändras i och med att de lämnas ut till biträdet. Ett sådant förfarande innebär att handlingarna kommer att bli expedierade från myndigheten och därmed allmänna och kan bli föremål för utlämnande i enlighet med offentlighetsprincipen.

1.3.9 Sammanfattning integritetsskyddslagstiftningen

Integritetsskyddslagstiftningen är tillämplig ur två perspektiv när en myndighet behandlar personuppgifter i en molntjänst. För det första måste myndighetens egen behandling av personuppgifterna vara tillåten enligt personuppgiftslagen eller tillämplig registerförfattning. För det andra måste den behandling av personuppgifter som utförs av molntjänstleverantören, dvs. personuppgiftsbiträdet, vara tillåten enligt samma lagstiftning. Inom ramen för detta arbete är det det sistnämnda förhållandet som är i fokus, dvs. hur, och i vissa fall även var, molntjänstleverantören behandlar personuppgifterna.

Integritetsskyddslagstiftningen innehåller flera legala utmaningar för den myndighet som vill behandla personuppgifter i molnet. Utmaningar som kan kopplas till begreppen kontroll, insyn och transparens. Myndigheten måste ha tillräcklig insyn i molntjänstleverantörens hantering för att kunna utöva nödvändig kontroll över personuppgiftsbehandlingen. Molntjänstleverantören måste vinnlägga sig om att dess behandling av personuppgifter sker med största möjliga transparens i förhållande till den personuppgiftsansvarige myndigheten. Den personuppgiftsansvarige myndigheten måste dessutom ha i åtanke att det alltid är myndigheten som bär det skadeståndsrättsliga ansvaret gentemot de registrerade oavsett om den kränkning som den registrerade har utsatts för har förorsakats av att dess personuppgiftsbiträde har behandlat personuppgifterna på ett otillåtet sätt.

Det främsta verktyget, och ibland det enda, myndigheten har till sitt förfogande för att få insyn i molntjänstleverantörens behandling av personuppgifter och kunna utöva kontroll av densamma, är personuppgiftsbiträdesavtalet. I biträdesavtalet ska det finnas tydliga och avgränsade instruktioner om hur molntjänstleverantören får behandla personuppgifter. Av biträdesavtalet ska framgå vilka säkerhetsåtgärder molntjänstleverantören ska vidta och hur myndigheten ska kunna kontrollera att leverantören faktiskt vidtar de avtalade säkerhetsåtgärderna. Om myndigheten accepterar att molntjänstleverantören anlitar underleverantörer ska detta framgå av avtalet liksom det ska vara tydligt reglerat vem som ansvarar för att se till att underleverantörerna binds av motsvarande avtalsvillkor som gäller för molntjänst-leverantören. Myndighetens rätt till insyn och kontroll gäller hos underleverantörerna på samma sätt som för molntjänstleverantören.

Om molntjänstleverantören eller någon av dess underleverantörer kommer att behandla personuppgifterna i tredje land ska det finnas ett lagligt stöd för att överföringen av personuppgifter till det tredje landet ska vara tillåten. I skrivande stund är det i praktiken bara EU-kommissionens standardavtalsklausuler som kan bli aktuella för sådan överföring. Den personuppgiftsansvarige myndigheten måste förvissa sig om att samtliga parter, dvs. såväl molntjänstleverantören som dess underleverantörer, som behandlar personuppgifterna i tredje land är bundna av standardavtalsklausulerna för att överföringen ska vara tillåten. Den personuppgifts-ansvarige behöver också kontrollera att det finns realistiska förutsättningar för samtliga parter att efterleva regleringen i standardavtalsklausulerna.

Trots det ovan sagda finns det faktiska möjligheter för en myndighet att behandla personuppgifter i molntjänster på ett lagligt sätt i förhållande till integritetsskydds-lagstiftningen. För att avgöra vilka personuppgifter som kan behandlas i vilken typ av moln, t.ex. privat eller publikt, och i vilken typ av tjänst, t.ex. SaaS, PaaS eller IaaS, måste myndigheten, inför sin upphandling eller anlitande av leverantör, klargöra vilka krav myndigheten måste ställa på leverantören. Kraven ska följa regleringen i den integritetsskyddslagstiftning som myndigheten har att följa men bör också ha sin grund i en gedigen riskanalys. Myndigheten måste förvissa sig om att det avtal som tecknas med molntjänstleverantören återspeglar samtliga krav som följer av lagstiftningen och att det finns möjligheter för myndigheten att utöva nödvändig kontroll över leverantörens behandling av personuppgifterna.

1.4 Arkivlagstiftningen

De bestämmelser som styr statliga myndigheters registrering, arkivering, hantering m.m. av allmänna handlingar finns framför allt i tryckfrihetsförordningen, offentlighets- och sekretesslagen, arkivlagen (1990:782), arkivförordningen (1991:446) samt i Riksarkivets föreskrifter och allmänna råd. Syftet med regleringen är bl.a. att allmänheten ska kunna utnyttja sina demokratiska rättigheter genom att kunna få tillgång till information om myndigheternas ärendehandläggning och verksamhet. Allmänheten måste kunna lita på att den information som finns hos myndigheter är tillgänglig och riktig och att den inte obehörigen har ändrats eller till och med raderats eller förstörts.

1.4.1 God offentlighetsstruktur

Vilka allmänna åtgärder en myndighet ska vidta för att underlätta sökandet efter allmänna handlingar m.m. regleras i 4 och 5 kap. OSL samt i 6 § arkivlagen. I

myndighetens ansvar för allmänna handlingar ingår att upprätthålla en god offentlighetstruktur. Myndigheten ska veta vilka handlingar som är allmänna, hålla en beskrivning över dessa allmänna handlingar tillgänglig och ge allmänheten möjlighet att själv söka bland de allmänna handlingarna (genom arkivbeskrivningen, arkivförteckningen, diariet, registerförteckningen eller andra register). Syftet med en god offentlighetsstruktur är att ge faktiska garantier för insyn genom god ordning och överskådlighet hos myndighetens informationsbehandling. Strukturen ska också leda till att reglerna om sekretess verkligen ger det skydd mot insyn som är avsett. Kraven på en god offentlighetsstruktur och möjligheten att kunna söka efter allmänna handlingar gäller självklart även för handlingar som lagras i en molntjänst.

1.4.2 Arkivlagen

Arkivbestämmelserna omfattar allt material som är att anse som allmän handling hos en myndighet. Definitionen i tryckfrihetsförordningen av vad som utgör en handling är synnerligen vid och innefattar även t.ex. loggar, trafikuppgifter och liknande. Enligt arkivlagen ska allmänna handlingar bevaras, hållas ordnade och vårdas för att tillgodose rätten att ta del av allmänna handlingar, behovet av information för rättsskipning och förvaltning samt forskningens behov, 3 § arkivlagen. Presumtionen är således att allmänna handlingar ska bevaras och gallring får endast ske i enlighet med föreskrifter eller beslut av Riksarkivet, om inte särskilda gallringsföreskrifter finns i lag eller förordning, 10 § arkivlagen och 14 § arkivförordningen. Att gallra handlingar innebär enligt Riksarkivets definition i 2 kap. 1 §, RA-FS 1991:1, att förstöra allmänna handlingar eller uppgifter i allmänna handlingar; förstöring av sådana handlingar/uppgifter i samband med överföring till annan databärare räknas som gallring om överföringen medför

- informationsförlust,
- förlust av möjliga informationssammanställningar,
- förlust av sökmöjligheter, eller
- förlust av möjligheter att fastställa informationens autenticitet.

Gallring är en aktiv och oåterkallelig åtgärd som innebär att uppgifter förstörs och resulterar i en slutlig förlust av information. Att föreskriven gallring faktiskt utförs är viktigt bl.a. av integritetsskäl. Många myndigheter har också att följa sina särskilda registerförfattningar, i vilka gallring av personuppgifter är huvudregel och ett eventuellt undantagsbevarande måste föreskrivas av regeringen eller Riksarkivet.

En myndighet som upphandlar en molntjänst för att hantera allmänna handlingar måste beakta arkivlagens krav på bevarande och gallring. Detta gäller oavsett vilken typ av molntjänst som upphandlas och för vilken planerad avtalstid. Myndigheten måste kontrollera att avtalen som tecknas med leverantören ger förutsättningar för att både bevara de handlingar som ska bevaras och gallra de handlingar som ska gallras. I praktiken innebär detta att myndigheten måste förvissa sig om att det är möjligt att antingen långtidsbevara handlingarna hos leverantören eller hämta hem eller flytta informationen i ett hanterbart format, till en annan leverantör. När det gäller handlingar för vilka gallring är föreskriven måste myndigheten kontrollera att den gallring av uppgifter som genomförs av myndigheten också slutförs hos leverantören. Om uppgifterna fortsätter att lagras på leverantörens servrar, trots att myndigheten har gallrat uppgifterna i fråga, är kravet på gallringens oåterkallelighet inte uppfyllt.

1.4.3 Särskilt om elektroniska handlingar

Riksarkivet har tagit fram föreskrifter och allmänna råd om elektroniska handlingar (upptagningar för automatiserad behandling) (RA-FS 2009:1). Föreskrifterna är tämligen detaljerade och ställer relativt långtgående krav på myndighetens hantering av sina elektroniska handlingar. Av föreskrifterna framgår bl.a. att en myndighet som upphandlar program eller tjänster för utveckling eller drift av ett system, ska överenskomma med leverantören om tillgång till program och dokumentation i den utsträckning som krävs för tillämpningen av denna författning, 1 kap. 9 §, RA-FS 2009:1. Om myndigheten genom uppdrag överlåter teknisk framställning, bearbetning eller bevarande av elektroniska handlingar till en annan myndighet eller enskild ska dessa genom skriftlig överenskommelse åläggas skyldighet att följa de bestämmelser som är tillämpliga, 1 kap. 10 §, RA-FS 2009:1. Av överenskommelsen ska framgå att såväl myndigheten som arkivmyndigheten har rätt att vid behov kontrollera efterlevnaden av bestämmelserna. I 3 kap. RA-FS 2009:1 stadgas att myndigheten ska ha en strategi för bevarande av elektroniska handlingar, vad denna strategi ska innehålla samt att myndigheten redan i planeringsstadiet ska ta ställning till hur bevarande och gallring samt överföring till bevarande ska ske. Myndigheten ska också, i enlighet med 5 kap. RA-FS 2009:1, dokumentera sina elektroniska handlingar för att handlingarna ska kunna framställas, överföras, hanteras, förvaras och vårdas på ett tillfredsställande sätt under den tid de ska bevaras. Vilka krav som ställs på informationssäkerhet regleras i 6 kap. RA-FS 2009:1. För att bedöma behovet av säkerhetsrutiner ska myndigheten t.ex. genomföra en riskanalys innan driftsättning eller innan uppdrag ges till annan myndighet eller enskild.

Riksarkivet har också tagit fram föreskrifter och allmänna råd om tekniska krav för elektroniska handlingar (upptagningar för automatiserad behandling) (RA-FS 2009:2). I föreskrifterna anges bl.a. vilka format som ska användas i databaser, register, textfiler, e-postmeddelanden m.m. Enligt 1 kap. 4 §, RA-FS 2009:2 ska myndigheten framställa elektroniska handlingar i enlighet med kraven i denna författning. Om detta inte är möjligt ska handlingarna senast vid överföring till bevarande uppfylla kraven i denna författning.

Sammantaget kan det konstateras att Riksarkivets föreskrifter ställer långtgående krav på myndighetens förbyggande och löpande hantering av allmänna handlingar i elektronisk form. Många av kraven är av sådan art att de måste beaktas i myndighetens förberedande upphandlingsarbete, t.ex. vid genomförandet av en riskanalys. Andra krav måste framgå i myndighetens kravställning för att myndigheten därefter, i avtalet med en molntjänstleverantör, ska kunna få garantier för att samtliga krav motsvaras av lämpliga avtalsvillkor med leverantören.

Myndigheten måste också förvissa sig om att det i avtalet med en molntjänstleverantör finns förutsättningar att uppfylla samtliga relevanta bestämmelser i arkivlagen, arkivförordningen samt därtill hörande föreskrifter, t.ex. att informationen lagras i rätt format eller i vart fall kan konverteras till ett sådant format samt att det finns förutsättningar för myndigheten att kontrollera molntjänstleverantörens efterlevnad av bestämmelserna.

1.4.4 Sammanfattning arkivlagstiftningen

Lagring av allmänna handlingar i molnet ställer bl.a. krav på tillförlitlighet och autenticitet/riktighet. En myndighet som är skyldig att bevara allmänna handlingar måste kunna garantera handlingarnas autenticitet över tid oavsett var och i vilken form

handlingarna lagras. En myndighet som lagrar allmänna handlingar i en molntjänst måste förvissa sig om att den molntjänst, vari handlingarna lagras, är tillförlitlig och att det finns förutsättningar för myndigheten, och i förlängningen även för enskilda, att få ständig tillgång till de allmänna handlingarna. På motsvarande sätt måste myndigheten kontrollera att det finns förutsättningar att oåterkalleligt gallra allmänna handlingar som lagras hos en molntjänstleverantör.

Arkivförfattningarnas krav måste genomlysas innan en myndighet anlitar en molntjänstleverantör för hantering av allmänna handlingar. Redan i det inledande upphandlingsförfarandet måste myndigheten analysera vilka krav som molntjänst-leverantören ska uppfylla för att myndigheten ska kunna efterleva bestämmelserna i arkivlagen, anslutande föreskrifter och eventuellt tillämplig registerförfattning. Myndigheten bör inte enbart förvissa sig om att det finns garantier för att bevara eller gallra allmänna handlingar. Myndigheten bör också fundera över vilka generella risker som finns med att lagra sina allmänna handlingar i molnet. Vad händer om molntjänst-leverantören t.ex. försätts i konkurs, blir uppköpt eller på annat sätt avvecklar sin verksamhet? För att så långt som möjlighet undvika risken att allmänna handlingar går förlorade, sprids till obehöriga, förstörs etc. måste myndigheten säkerställa att det i avtalet med molntjänstleverantören finns villkor som ger myndigheten garantier för att arkivlagens regler kan uppfyllas.

1.5 Upphandlingslagstiftningen

Genom EG-direktiv är regelverket för offentlig upphandling detsamma inom EU och EES-området över de gällande tröskelvärdena. Under tröskelvärdena har medlems-staterna större möjlighet att utforma sin lagstiftning för offentlig upphandling. Även regler om upphandling under tröskelvärdena ska dock vara utformade i enlighet med de grundläggande principerna för offentlig upphandling som utgör grundstenarna i direktiven. Dessa principer är proportionalitetsprincipen, principen om ömsesidigt erkännande, principen om likabehandling av anbudsgivare, icke-diskriminerings-principen och principen om öppenhet (förutsebarhet och transparens).

De direktiv som är av intresse för denna framställning är direktivet avseende den s.k. klassiska sektorn (2004/18/EG) och direktivet avseende den s.k. försörjningssektorn (2004/17/EG). Det förra har implementerats i lagen (2007:1091) om offentlig upphandling (LOU) och det senare i lagen (2007:1092) om upphandling inom områdena vatten, energi, transporter och posttjänster (LUF).

I det följande kommer vi att belysa vissa särskilda upphandlingsrättsliga frågor som kan aktualiseras vid myndigheters upphandling av molntjänster. Det ska inledningsvis framhållas att LOU inte innehåller någon specifik reglering om offentlig upphandling av molntjänster. Inte heller finns, såvitt är känt, några vägledande avgöranden från svenska domstolar eller EU-domstolen avseende offentliga upphandlingar av moln-tjänster. Eftersom LUF inte innehåller någon avvikande reglering i förhållande till LOU kommer regleringen i LUF inte att kommenteras vidare. Slutligen ska det också framhållas att nu gällande CPV-förordning (213/2008/EG) inte har några specifika koder för offentliga upphandlingar där en tjänst anskaffas och där tillhandahållandet av tjänsten sker genom en molnlösning.

1.5.1 Val av upphandlingsförfarande

Redan under planeringsfasen av en molntjänstupphandling, är det tillåtet för den upphandlande myndigheten att föra en dialog med potentiella leverantörer, enligt skäl

8 i direktivet 2004/18/EG. Däri anges att ”Innan ett upphandlingsförfarande inleds får den upphandlande myndigheten genom en "teknisk dialog" söka eller godta råd som kan användas när specifikationerna utarbetas, dock under förutsättning att sådana råd inte leder till hinder för konkurrensen.” Med anledning av molntjänsters relativa nykommenhet på marknaden kan det vara lämpligt för en upphandlande myndighet att utnyttja möjligheten till teknisk dialog.

När det gäller myndighetens val av möjliga och lämpliga upphandlingsförfaranden bör myndighetens möjlighet att använda undantagsförfaranden framhållas. En myndighet kan t.ex. använda sig av ett förhandlat förfarande med föregående annonsering enligt 4 kap. 2 § punkterna 2 och 3 LOU, om det som ska upphandlas är av sådant slag eller förenat med sådana risker att det på grund av särskilda omständigheter inte går att ange något totalpris i förväg eller för finansiella och intellektuella tjänster som är av sådan art att det inte går att utarbeta tillräckligt exakt förfrågningsunderlag för att kunna genomföra upphandlingen genom att välja det bästa anbudet enligt bestämmelserna för öppna eller selektiva förfaranden. Myndigheten bör även kunna använda sig av en konkurrenspräglad dialog enligt 4 kap. 10 – 21 § § LOU vid upphandling av en molntjänst när det är fråga om komplexa kontrakt. Om upphandlingen understiger tröskelvärdet finns det alltid en möjlighet att förhandla (förenklat förfarande eller urvalsförfarande).

Myndighetens möjlighet att använda förhandlat förfarande utan föregående annonsering enligt 4 kap. 5 – 9 § § LOU är i och för sig begränsad.[67] Men om det som ska upphandlas av tekniska eller konstnärliga skäl eller på grund av ensamrätt kan fullgöras av endast en viss leverantör kan det finnas förutsättningar för en myndighet att tillämpa ett sådant förfarande. Givet nuvarande inställning hos domstolarna har dock detta undantag ett mycket begränsat tillämpningsområde.

Om kontraktets värde är under gällande tröskelvärde kan myndigheten direktupphandla. En upphandlande myndighet har under ett räkenskapsår rätt att genom direktupphandling upphandla varor och tjänster av ”samma slag” upp till ett till ett belopp om 505 800 kr exklusive mervärdesskatt (2015). Antalet kontrakt eller antalet leverantörer som upphandlas av ”samma slag” saknar betydelse. Det är anskaffningar av ”samma slag” hittills under räkenskapsåret som är av relevans. Vad som utgör ”samma slag” enligt 15 kap. 3 a § LOU saknar närmare reglering i LOU och i förarbetena.

Konkurrensverket har gett ut en vägledning för beräkning av kontraktsvärdet vid direktupphandlingar av samma slag.[68] Utifrån de hjälpregler som finns i vägledningen torde man inte kunna dra slutsatsen att endast det förhållandet att den efterfrågade tjänsten tillhandahålls i form av en molntjänst innebär att det ska anses vara av ”samma slag”. Detta då molntjänster kan vara av vitt skilda slag t.ex. arkiveringstjänster, rekryteringsverktyg m.m. Det saknas dock vägledande avgöranden i detta

---

[67] Se även hänvisningen i 15 kap. 3 § LOU för upphandlingar under tröskelvärdena.

[68] *Är inköpen av samma slag? Hjälpregler för beräkning av kontraktsvärdet vid direktupphandlingar av samma slag,* Vägledning från Konkurrensverket 1(2015). http://www.konkurrensverket.se/globalassets/publikationer/vagledningar/vagledning_2015-1_inkop-av-samma-slag.pdf

avseende. Det ska vidare poängteras att även om direktupphandling oftast kan ske formlöst, uppställer lagstiftningen krav på att myndigheten ska ha riktlinjer för direktupphandling och dokumentera direktupphandlingar som överstiger 100 000 kronor, 15 kap. 3 och 18 §§ LOU.

En myndighet som direktupphandlar en molntjänst genom att t.ex. teckna kontrakt direkt över internet måste förvissa sig om att kontraktets värde i realiteten inte kommer att överstiga gränsvärdet för direktupphandlingen. Vid beräkningen av kontraktets värde måste myndigheten beakta samtliga kostnader som kan komma att betalas för tjänsten. Även sådana kostnader som kan vara svåra att förutse och beräkna ska räknas in. Det kan t.ex. röra sig om kostnader för att hämta hem eller flytta över myndighetens information till en annan leverantör vid kontraktets upphörande eller kostnader för utökad användning av tjänsten. Om en direktupphandling har genomförts i strid med bestämmelserna i LOU kan det leda till flera negativa konsekvenser för den upphandlande myndigheten. Avtalet kan komma att ogiltigförklaras och myndigheten kan bli skyldig att betala skadestånd eller en sanktionsavgift (s.k. upphandlingsskadeavgift). Detta oavsett vilken grund för direktupphandling som åberopats.

Många molntjänster på marknaden tillhandahålls gratis eller till en mycket låg kostnad i monetära termer. Det kan röra sig om tjänster som myndigheter kan använda som ett komplement till sina redan befintliga it-system, t.ex. sociala medier, men även tjänster som i praktiken kan ersätta befintliga it-system, t.ex. e-post- och kalendertjänster. En tjänst som tillhandahålls helt utan ekonomisk ersättning faller utanför det reglerade området och behöver sålunda inte upphandlas enligt LOU. Det är emellertid av största betydelse att det står klart att tjänsten verkligen är kostnadsfri för den upphandlande myndigheten för att myndigheten inte ska behöva tillämpa LOU.

1.5.2 Kravställning

Vid upphandling av molntjänster är 6 kap. LOU och de grundläggande principerna styrande för vilka tekniska krav som kan ställas på tjänsten. Den tekniska specifikationen ska innehålla kraven på molntjänstens egenskaper. Hänvisningar till fabrikat, med angivande av att likvärdiga fabrikat accepteras, får endast göras när det inte är möjligt att beskriva föremålet genom angivande av t.ex. funktion eller prestanda eller genom att hänvisa till en standard, 6 kap. 2 – 4 §§ LOU. Enligt principen om öppenhet (förutsebarhet/transparens) bör en teknisk beskrivning vara så tydligt formulerad att det står klart för leverantörerna vilka krav den upphandlande myndigheten ställer. Dagens lagstiftning stipulerar inga direkta krav på avtalsvillkoren i övrigt, till skillnad från kommande lagstiftning.[69] Avtalsvillkoren måste dock utformas i överensstämmelse med de grundläggande principerna. Enligt EU-domstolens praxis måste även principerna för ersättning, i vart fall i huvuddrag, återfinnas i förfrågningsunderlaget för att uppfylla kravet på att upphandlingsföremålet ska vara tillräckligt tydligt definierat.

Det är inte tillåtet att beskriva kontraktsföremålet, i form av avtalsvillkor eller tekniska krav, på ett sätt som innebär att varor och tjänster med ursprung i andra EU-medlemsländer diskrimineras. Mot bakgrund av icke-diskrimineringsprincipen kan det

[69] Se avsnitt 1.8.5

ifrågasättas om en myndighet t.ex. kan ställa ett uttryckligt krav på att myndighetens information måste lagras på servrar i Sverige. EU-domstolen har i ett flertal domar ställt sig negativ till att uppställa krav på att anbudsgivaren ska ha sitt produktionsställe på en viss geografisk plats och till premiering av anbudsgivare utifrån avståendet mellan denne och den upphandlande myndigheten. Kammarrätten i Stockholm behandlade nyligen ett mål som rörde ett krav om att leverantörer inte fick behandla personuppgifter utanför EU/EES-området.[70] Av domskälen följer att det förvisso finns utrymme för en upphandlande myndighet att kräva att en it-miljö inte driftas utanför EU men att detta får avgöras från fall till fall. Det anförda innebär dock att en myndighet med största säkerhet inte torde kunna ställa ett explicit krav på att myndighetsinformation måste lagras på servrar i Sverige annat än möjligen när det är fråga om rikets säkerhet. Att däremot uppställa krav på att support, tekniskt stöd och tillhandahållande av handlingar sker på svenska språket anses inte strida mot icke-diskrimineringsprincipen.

Utöver ovanstående redovisade aspekter av upphandlingslagstiftningen återfinns inga direkta bestämmelser i LOU som kan sägas vara särpräglade för upphandling av molntjänster. Det är dock både tillåtet och lämpligt att ställa väl motiverade krav på tidigare erfarenhet hos anbudsgivarna, t.ex. vad avser ett tillfredställande utfall av migrering av uppgifter av viss omfattning, känslighet eller i övrigt av viss karaktär, för att säkerställa att en molntjänst upphandlas på ett adekvat sätt.[71] Vid upphandling över tröskelvärdena gäller dock den begräsningen att de kvalificerande uppdragen ska ha slutförts inom de tre senaste åren räknat från dagen för ingivandet av anbud i den nu aktuella upphandlingen. Det ska vidare framhållas att det varken enligt nuvarande eller kommande lagstiftning föreligger något hinder mot att upphandla flera leverantörer varav en som huvudleverantör och en som back-up för det fall avtalet nödgas avslutas med huvudleverantören.

1.5.3 Ändringar i tilldelade kontrakt

Upphandlingslagstiftningen reglerar själva upphandlingsförfarandet fram till tilldelning av kontrakt. Av en omfattande nationell rättspraxis och av EU-domstolens rättspraxis följer emellertid att ett tilldelat kontrakt inte under avtalstiden får bli föremål för ändringar på så sätt att det *väsentligen ändras*. En väsentlig ändring i ett avtal kan medföra att ett nytt kontrakt anses ha ingåtts utan föregående upphandling, vilket innebär att den upphandlande myndigheten förmodligen har gjort en otillåten direktupphandling. Vad som utgör en väsentlig ändring av ett kontrakt är en fråga som avgörs från fall till fall utifrån den aktuella ändringen, t.ex. av omfattningen eller enskilda villkor. En ändring av ett kontrakt som medför att en annan anbudsgivande leverantör hade kunnat tilldelas det aktuella kontraktet är emellertid typiskt sett att anse som en väsentlig ändring, såsom t.ex. tillåtandet av prishöjningar hos den antagne leverantören. Detta gäller upphandlingar som slutförts efter ett annonserat förfarande.

När det gäller direktupphandling av molntjänster är det relativt vanligt att det är leverantörens standardavtal m.m. som reglerar förhållandet mellan parterna dvs.

---

[70] Kammarrätten i Stockholm, mål 8972-12, avgjort den 23 april 2013

[71] Se bl.a. Kammarrätten i Stockholm, mål 9894-14, avgjort den 6 maj 2015, angående krav på genomförda projekt och proportionalitetsbedömning avseende referensprojektets innehåll

förfrågan från den upphandlande myndigheten innehåller inte avtalsvillkoren såsom vid annonserade upphandlingar. I dessa fall förekommer att leverantören i sitt standardavtal för tjänsten lämnar utrymme för att ensidigt införa ändringar i avtalsvillkoren. Att leverantören förbehåller sig rätten att ensidigt ändra i avtalsvillkoren från tid till annan är givetvis olämpligt för en upphandlande myndighet av många anledningar men det behöver inte vara i strid mot upphandlingslagstiftningen.

1.5.4 Sammanfattning upphandlingslagstiftningen

Upphandlingslagstiftningen kan sägas utgöra det nav som en myndighet har att förhålla sig till vid inköp av en molntjänst. Samtliga legala krav som myndigheten har identifierat vid den rättsliga analysen av den lagstiftningen som är tillämplig på myndighetens planerade informationshantering i molnet ska återspeglas i upphandlingsunderlaget. Av denna anledning är det av stor vikt att myndigheten utför ett gediget analysarbete som utmynnar i en kravställning som uppfyller alla myndighetens behov såväl ur juridiskt perspektiv som ur övriga verksamhetsperspektiv.

En myndighet som upphandlar en molntjänst i standardutförande har ofta att acceptera att det är molntjänstleverantörens eget standardavtal som reglerar förhållandet mellan parterna. Det gäller i synnerhet vid direktupphandling av publika SaaS-tjänster. Myndigheten måste under sådana förutsättningar granska avtalet noggrant för att kontrollera att det överensstämmer med de rättsliga krav lagstiftningen ställer på myndighetens hantering av sin information.

Sammanfattningsvis innehåller inte upphandlingslagstiftningen någon särreglering för upphandling av molntjänster. Att utforma ett upphandlingsunderlag som motsvarar samtliga myndighetens krav ställer emellertid höga krav på myndighetens upphandlingskompetens varför myndigheten behöver utföra ett grundligt arbete i den förberedande upphandlingsfasen.

1.6 Soft Law – instrument för självreglering

Inom molntjänstområdet pågår ett omfattande arbete med att utveckla olika typer av självreglerande instrument t.ex. standarder, certifieringar och uppförandekoder. Syftet med dessa instrument är att underlätta för potentiella molntjänstkunder att t.ex. kunna kontrollera vilka säkerhetsåtgärder en leverantör vidtar eller hur leverantören behandlar kundernas information och personuppgifter. En molntjänstkund kan emellertid inte nöja sig med att konstatera att en leverantör är certifierad enligt en viss modell eller ansluten till en viss uppförandekod. Myndigheten måste också granska innehållet i certifieringen eller uppförandekoden, göra en jämförelse med den nationella lagstiftningen myndigheten har att följa och kontrollera hur väl innehållet i certifieringen eller uppförandekoden överensstämmer med kraven i den nationella lagstiftningen. Myndigheten bör också kontrollera om molntjänstleverantörens anslutning till ett självreglerande instrument har föregåtts av en självutvärdering eller genom att leverantören har granskats av en oberoende tredje part. En certifiering som grundas på leverantörens egen självutvärdering äger givetvis inte samma tyngd som en certifiering som har utfärdats efter en granskning av en oberoende tredje part.

I det följande redogörs kortfattat för ett par olika instrument för självreglering som är av särskilt intresse, i huvudsak i förhållande till de rättsliga krav i integritetsskyddshänseende som ställs vid behandling av personuppgifter i molntjänster. Det bör dock poängteras att även om s.k. Soft Law kan ge en indikation på hur en molntjänst-

leverantör skyddar och behandlar personuppgifter så kan ett sådant instrument aldrig ersätta en juridisk bedömning i det enskilda fallet.

- **Privacy Level Agreement [V2]**

Organisationen Cloud Security Alliance har tagit fram ett s.k. Privacy Level Agremeent [V2] (PLA).[72] PLA är utformad för att överensstämma med kraven i dataskyddsdirektivet 95/46/EG och artikel 29-arbetsgruppens yttrande om datormoln (WP196). Syftet med PLA är att en ansluten molntjänstleverantör ska kunna visa potentiella kunder att leverantörens behandling av personuppgifter sker i enlighet med dataskyddsdirektivets grundläggande krav. Det är emellertid upp till respektive kund att granska innehållet i PLA och kontrollera molntjänstleverantörens efterlevnad.

- **Data Protection Code of Conduct for Cloud Service Providers**

C-SIG on Code of Conduct[73] har i samarbete med bl.a. representanter från molntjänstmarknaden utvecklat en uppförandekod för molntjänstleverantörer i syfte att stödja en enhetlig tillämpning av EU:s dataskyddsbestämmelser. Arbetet har initierats av EU-kommissionen inom ramen för satsningen på en europeisk molntjänststrategi.[74] Uppförandekoden innehåller en uppsättning krav som ska följas av en ansluten molntjänstleverantör i dess roll som personuppgiftsbiträde. Artikel 29-arbetsgruppen har yttrat sig över uppförandekoden i enlighet med artikel 30.1 d) i dataskydds-direktivet. [75] Artikel 29-arbetsgruppen anför i yttrandet att uppförandekoden i och för sig kommer att bidra till större transparens och rättsäkerhet för samtliga parter men att den inte i alla hänseenden uppfyller dataskyddsdirektivets rättsliga krav. I skrivande stund pågår arbete med att justera uppförandekoden för att den till alla delar ska överensstämma med dataskyddsdirektivet.

- **Cloud Certification Schemes List**

C-SIG on Certification[76] har i samarbete med Enisa[77] tagit fram en lista över certifieringar och verktyg som har utarbetats inom ramen för satsningen på en europeisk molnstrategi. Cloud Certification Schemes List[78] ger en översikt över olika certifieringar som finns tillgängliga för molntjänstleverantörer. Syftet med listan är bl.a. att ge molntjänstkunder en bättre överblick över befintliga certifieringar och innehållet i dessa och att kunna jämföra certifieringarna sinsemellan.

---

[72] Privacy Level Agreement [V2]: A Compliance Tool for Providing Cloud Services in the European Union. https://downloads.cloudsecurityalliance.org/assets/research/pla/downloads/2015_05_28_PrivacyLevelAgreementV2_FINAL_JRS5.pdf

[73] Cloud Select Industry Group (C-SIG) on Code of Conduct är en arbetsgrupp i EU-kommissionen som har i uppdrag att utveckla en uppförandekod inom ramen för satsningen på en europeisk molnstrategi.

[74] https://ec.europa.eu/digital-agenda/en/european-cloud-initiative, sidan är hämtad den 1 december 2015.

[75] Opinion on C-SIG Code of Conduct on Cloud Computing, 2588/15/EN, WP 232, antaget den 22 september 2015. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp232_en.pdf

[76] Cloud Select Industry Group (C-SIG) on Certification Schemes är en arbetsgrupp i EU-kommissionen som har i uppdrag att bidra till utvecklingen av certifieringar inom ramen för satsningen på en europeisk molnstrategi.

[77] European Union Agency for Network and Information Security (Enisa).

[78] https://resilience.enisa.europa.eu/cloud-computing-certification

- **SS-ISO/IEC 27018:2014 (ISO 27018)**

ISO 27018 innehåller riktlinjer för skydd av personuppgifter i publika molntjänster. En molntjänstleverantör kan välja att ansluta sig till standarden och åta sig att följa riktlinjerna däri. Det är emellertid inte möjligt för en leverantör att bli certifierad enligt ISO 27018. Den avgörande skillnaden är att en certifiering medför att leverantören regelbundet granskas av en oberoende tredje part för att kontrollera att leverantören faktiskt lever upp till de krav som leverantören har åtagit sig att följa.

1.7 Förslag och utredningar som kan påverka myndigheters användning av molntjänster

1.7.1 EU:s dataskyddsreform

I mars 2012 presenterade Europeiska kommissionen ett förslag till nya regler om dataskydd och personuppgiftsbehandling. Syftet är att modernisera reglerna i dataskyddsdirektivet från 1995 och få till stånd en mer enhetlig tillämpning inom EU. Förslaget till reform innehåller dels en generell dataskyddsförordning, dels ett särskilt dataskyddsdirektiv för brottsbekämpande myndigheter.

I mitten av december 2015 nådde parterna en överenskommelse om den nya dataskyddsförordningen. Förordningen kommer att antas i början av år 2016 och träder i kraft två år därefter. Det exakta innehållet i den nya förordningen är i skrivande stund inte känt men det kan förutsättas att den, på en genomgripande nivå, kommer att förändra spelplanen för såväl personuppgiftsansvariga som personuppgiftsbiträden. En stor omställning i molntjänstsammanhang är att även personuppgiftsbiträden, dvs. molntjänstleverantörer kommer att åläggas visst ansvar för att förordningen efterlevs. En konsekvens av detta torde bli att molntjänstleverantörer måste anpassa sina avtal så att de är utformade i överensstämmelse med förordningens regler. Vidare införs en skyldighet för personuppgiftsansvariga att utföra en s.k. Data Protection Impact Assessment (DPIA) när en planerad personuppgiftsbehandling medför särskilda risker för den registrerade. Det kommer också införas en skyldighet för personuppgiftsansvariga att anmäla integritetsincidenter (personal data breach) till tillsynsmyndigheten och på motsvarande sätt ska personuppgiftsbiträden anmäla integritetsincidenter till den personuppgiftsansvarige. Vidare förstärks de nationella dataskyddsmyndigheternas möjlighet att utfärda sanktionsavgifter vid bristande uppfyllelse av regelverket.

Dataskyddsförordningen kommer att gälla direkt som lag i Sverige. Det innebär att den svenska personuppgiftslagen som den ser ut nu inte kommer att finnas kvar. De regler som personuppgiftsansvariga och andra måste följa kommer, i huvudsak, att finnas direkt i EU-förordningen istället. I vissa delar kan förordningen trots allt komma att ge utrymme för mer preciserade bestämmelser i nationell lagstiftning. Svenska regler som rör personuppgiftsbehandling kan därför komma att finnas även i fortsättningen på vissa områden t.ex. personuppgiftsbehandling hos myndigheter.

1.7.2 Myndighetsdatalag (SOU 2015:39)

Informationshanteringsutredningen har haft i uppdrag att se över den s.k. registerlagstiftningen och utreda förutsättningarna för att skapa en generell, enhetlig och – helt eller i vart fall delvis – samlad reglering för myndigheternas behandling av personuppgifter. Utredningen föreslår en ny lag – myndighetsdatalagen – som innehåller bestämmelser som kan gälla generellt för alla statliga och kommunala myndigheters personuppgiftsbehandling bortsett från den brottsbekämpande sektorn. Vissa

verksamheter är dock undantagna från lagens tillämpningsområde nämligen en myndighets administrativa verksamhet och dess verksamhet som personuppgiftsbiträde.

Lagen ska gälla i stället för personuppgiftslagen men innehåller hänvisningar till vissa bestämmelser i personuppgiftslagen som ska tillämpas vid myndigheters behandling av personuppgifter enligt den nya lagen. I det följande redogörs för ett par bestämmelser i förslaget till myndighetsdatalag som kan vara relevanta vid myndigheters behandling av personuppgifter i en molntjänst.

1.7.2.1 Säkerhet vid behandlingen

I 17 § förslaget till myndighetsdatalag regleras personuppgiftsansvarigas skyldighet att skydda personuppgifter med lämpliga säkerhetsåtgärder. I jämförelse med 31 § PuL innehåller den föreslagna regleringen ett tydliggörande om att säkerhetsarbetet ska ske systematiskt och omfatta samtliga led i personuppgiftsbehandlingen, dvs. arbetet ska inbegripa förebyggande, löpande och uppföljande åtgärder. Vidare framgår att säkerhetsarbetet ska bedrivas så att det inriktas på åtgärder som behövs för att skydda registrerades integritet och så långt som möjligt samordnas med övrigt informationssäkerhetsarbete som sker i enlighet med t.ex. arkivlagstiftningen och andra föreskrifter om informationssäkerhet hos myndigheter.[79]

Bakgrunden till att utredningen har valt att precisera hur myndigheterna ska bedriva sitt säkerhetsarbete är att det för närvarande bedöms förekomma brister i myndigheternas systematiska säkerhetsarbete. Av denna anledning är det önskvärt att det tydliggörs i lagen att detta sätt att arbeta med säkerhetsfrågorna är av central betydelse.[80] För en myndighet som avser att upphandla en molntjänst är det positivt att det på ett tydligare sätt klargörs inom vilka ramar myndigheten ska bedriva sitt säkerhetsarbete samt att säkerhetsarbetet som sker i förhållande till myndighetsdatalagen ska integreras med myndighetens övriga informationssäkerhetsarbete. Detta är ytterligare ett incitament för myndigheten att förstå vikten av att ha ett systematiskt säkerhetsarbete för att skydda sin information.

1.7.2.2 Personuppgiftsbiträde

Bestämmelserna om personuppgiftsbiträden finns i 19 – 21 §§ förslaget till myndighetsdatalag. Den föreslagna regleringen motsvarar 30 § och 31 § andra stycket PuL men klargör därutöver vissa övriga förutsättningar som ska vara uppfyllda för att det ska vara tillåtet att anlita ett personuppgiftsbiträde. Det rör sig främst om förtydliganden av redan gällande praxis t.ex. att biträden som anlitas av ett personuppgiftsbiträde (dvs. underleverantörer) får behandla personuppgifter bara i enlighet med instruktioner från den personuppgiftsansvariga myndigheten (19 § andra meningen), att myndigheten ska förvissa sig om att biträdet inte anlitar ett annat biträde utan godkännande från myndigheten (20 § punkten 4) och att det ska finnas ett skriftligt avtal om personuppgiftsbiträdets behandling av personuppgifter för myndighetens räkning. Avtalet ska innehålla instruktioner och villkor om biträdets skyldig-

[79] Myndighetsdatalag, SOU 2015:39, s. 711

[80] A.a. s. 383.

heter i frågor som avses i 19 och 20 §§ och motsvarande avtal ska finnas med ett biträde som anlitas av ett personuppgiftsbiträde (21 §). [81]

1.7.2.3 Korrigering av felaktiga personuppgifter eller annars otillåten behandling

Enligt 25 § förslaget till myndighetsdatalag ska en personuppgift på begäran av den registrerade avskiljas från fortsatt behandling och inte lämnas ut till en enskild annat än med stöd av 2 kap. tryckfrihetsförordningen eller utplånas, om uppgiften rör honom eller henne och den inte får behandlas enligt denna lag.

Genom paragrafen görs klart att en myndighet är skyldig att agera om en registrerad påpekar att en behandling av personuppgifter som rör honom eller henne inte uppfyller lagens krav. Det ska vara fråga om påpekanden som kan bekräftas överensstämma med de krav som gäller för den aktuella behandlingen först efter en bedömning från myndighetens sida och som inte kan åtgärdas genom att uppgifterna rättas eller kompletteras. Det ska alltså vara fråga om påpekanden från den registrerade om att behandlingen av de aktuella personuppgifterna i något avseende inte alls är tillåten (jämför 9 § a) PuL och kravet på att en behandling ska vara laglig). Som exempel på när bestämmelsen skulle kunna bli tillämplig nämns bl.a. att personuppgifter har behandlats under för lång tid eller att uppgifterna inte kan anses relevanta för det ändamål för vilket behandlingen äger rum. [82] Den föreslagna bestämmelsen kan tänkas bli tillämplig om en molntjänstleverantör, som personuppgiftsbiträde, t.ex. ges utrymme att behandla personuppgifterna för egna ändamål eller om den personuppgiftsansvariga myndigheten har lämnat bristfälliga instruktioner om när biträdet ska radera uppgifter och detta leder till att biträdet bevarar uppgifterna längre än vad som kan bedömas vara nödvändigt med hänsyn till ändamålen med behandlingen av personuppgifterna.

1.7.3 En ny säkerhetsskyddslag (SOU 2015:25)

Syftet med förslaget till en ny säkerhetsskyddslag är bl.a. att utvidga det skyddsvärda området till *säkerhetskänslig verksamhet.* Säkerhetskänslig verksamhet är dels verksamhet som är av betydelse för *Sveriges säkerhet* och dels verksamhet som avses i ett för Sverige förpliktande åtagande om säkerhetsskydd (internationellt säkerhetsskyddsåtagande).

Vidare föreslår utredningen att säkerhetsskyddet ska inriktas mot verksamhet som innebär *hantering av säkerhetsskyddsklassificerade uppgifter.* Det ska innefatta skydd av uppgifter som är av betydelse för Sveriges säkerhet eller som ska skyddas enligt ett internationellt säkerhetsskyddsåtagande och som till sin natur är sådana uppgifter som avses i bestämmelser om sekretess. Det innebär således en vidare ram än enligt den nuvarande säkerhetsskyddslagen som utgår från begreppet hemliga uppgifter dvs. uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen *och* rör rikets säkerhet.

Därutöver ska säkerhetsskyddet inriktas mot verksamheter som av annan anledning behöver ett säkerhetsskydd (*i övrigt säkerhetskänslig verksamhet).* Det skyddsvärda området ska utformas så att det även kan innefatta annan säkerhetskänslig verksamhet,

---

[81] A.a. s. 712-713.

[82] A.a. s. 717.

t.ex. hantering av it-system eller sammanställningar av uppgifter som är av central betydelse för ett fungerande samhälle eller verksamhet som behöver skyddas på den grunden att den kan utnyttjas för att skada nationen.

1.7.4 Informations- och cybersäkerhet i Sverige (SOU 2015:23)

Utredningen föreslår en strategi som innehåller förslag till åtgärder inom de områden utredningen har bedömt som strategiska för att uppnå en god informationssäkerhet inom staten. Åtgärderna ska bl.a. säkerställa att de statliga myndigheterna har ett gemensamt förhållningsätt till informationssäkerhetsfrågor och behovet av skyddad kommunikation samt säkra it-lösningar. I det följande lyfts ett par av utredningens förslag fram som kan komma att ha betydelse för myndigheternas informationssäkerhetsarbete vid anlitandet av en molntjänstleverantör.

- **Styrning och tillsyn av informationssäkerheten i staten stärks**

Utredningen föreslår att en nationell styrmodell för informationssäkerhet etableras för att skapa ett systematiskt informationssäkerhetsarbete i statlig verksamhet. Vidare föreslås att ett statligt myndighetsråd för informationssäkerhet inrättas. För att tydliggöra myndigheternas ökade ansvar för det praktiska säkerhetsarbetet inom myndigheterna införs en ny förordning; förslag till förordning för statliga myndigheters informationssäkerhet.

- **Staten ställer tydliga krav som upphandlare av tjänster som innehåller informationshantering eller av it-tjänster**

Utredningen föreslår att statlig upphandling på it-området bör innehålla hänvisning till för staten gällande standarder och krav på certifiering i de situationer där säkerhetsnivåer har fastställts för respektive verksamhet. Vidare föreslås att det bör införas ett krav på att rapportera vilken leverantör som en statlig myndighet har valt då ramavtal rörande it-lösningar används. Vidare bör regeringen fördjupa dialogen mellan privata och offentliga aktörer samt utbildnings- och forskningsinstitutioner på informationssäkerhetsområdet.

- **Samtliga statliga myndigheter rapporterar it-incidenter**

Utredningen föreslår att det bör inrättas ett system för obligatorisk it-incidentrapportering för samtliga statliga myndigheter. Ett system för obligatorisk it-incidentrapportering skulle bidra till förmågan att förebygga och hantera it-incidenter.

Regeringen beslutade i december 2015 om en obligatorisk it-incidentrapportering för statliga myndigheter. När förslaget nu realiseras innebär det att en myndighet, vid upphandling av en molntjänst, måste säkerställa att avtalet med leverantören ger förutsättningar för myndigheten att uppfylla skyldigheten att rapportera it-incidenter. Myndigheten kan under sådana förhållanden inte överlåta till leverantören att avgöra vilka it-incidenter som ska rapporteras tillbaka till myndigheten.

Sammantaget innebär utredningens förslag ökade krav på att myndigheterna anlägger ett systematiskt och processinriktat arbetssätt för att upprätthålla en god informationssäkerhet. Förslag till förordning för statliga myndigheters informationssäkerhet innehåller såväl generella som specifika krav på hur myndigheterna informationssäkerhetsarbete ska genomföras. I den föreslagna förordningen, 15-16 §§, klargörs bl.a. vilka åtgärder en myndighet måste vidta för att trygga en god informationssäkerhet vid upphandling och utveckling av it-system och it-produkter.

1.7.5 En ny upphandlingslagstiftning

Den förändring av upphandlingslagstiftningen som kommer att träda i kraft i april 2016 grundar sig dels på en revidering av nu gällande direktiv och dels på ett nytt direktiv om offentlig upphandling av koncessioner.[83] I det följande kommer vi att nämna ett par förändringar i den kommande lagstiftningen som kan ha viss inverkan vid en myndighets upphandling av en molntjänst.

När det gäller möjligheten till dialog med marknadens aktörer förtydligas i artikel 40 i det nya LOU-direktivet att ”Innan en upphandlande myndighet inleder ett upphandlingsförfarande kan den genomföra marknadsundersökningar för att förbereda upphandlingen och för att informera de ekonomiska aktörerna om den planerade upphandlingen och kraven för denna. I detta syfte får den upphandlande myndigheten till exempel rådfråga eller godta råd från oberoende experter eller myndigheter eller från marknadsaktörer. Dessa råd får användas vid planering och genomförande av upphandlingsförfarandet, under förutsättning att deras råd inte snedvrider konkurrensen eller bryter mot principerna om icke-diskriminering och öppenhet.” Direktivbestämmelsen föreslås inte införas i nya LOU. Men den nya lagstiftningen kommer att innehålla reglering för situationer där en potentiell leverantörs deltagande i förberedelserna av upphandlingen innebär att denne erhållit fördelar, som inte kan läkas i den kommande upphandlingen. I sådana fall ska den upphandlande myndigheten utesluta denne leverantör. Det införs dessutom en skyldighet för den upphandlande myndigheten att informera i förfrågningsunderlaget om eventuella leverantörers deltagande i den förberedande fasen.

Det kommer vidare att införas regler om att en upphandlande myndighet får bruka tilldelning av kontrakt i separata delar med en rätt för den upphandlande myndigheten att begränsa möjligheten till tilldelning. Vinnaren tar alltså inte hem allt. Det blir alltså möjligt för den upphandlande myndigheten att ha parallella leverantörer för olika områden varvid de leverantörer som har antagits för ett område kan träda in för det fall avtalet upphör med en leverantör för ett annat område. Det föreligger ingen skyldighet att dela upp kontrakt, men det ska övervägas och om så inte sker, ska skälen för detta motiveras i upphandlingsdokumenten.

Vidare införs ett betydligt utökat tillämpningsområde för förhandlat förfarande med föregående annonsering och konkurrenspräglad dialog jämte ett helt nytt upphandlingsförfarande – innovationspartnerskap. En upphandlande myndighet får använda ett förfarande för inrättande av innovationspartnerskap om den t.ex. behöver en tjänst för att tillfredsställa behov som den upphandlande myndigheten bedömer inte kan tillgodoses genom lösningar som finns på marknaden, något som skulle kunna bli aktuellt vid upphandling av molntjänster.

Avseende tekniska specifikationer anges i den nya lagstiftningen att de egenskaper som anges får också avse

---

[83] Europaparlamentets och rådets direktiv 2014/24/EU av den 26 februari 2014 om offentlig upphandling och om upphävande av direktiv 2004/18/EG, Europaparlamentets och rådets direktiv 2014/25/EU av den 26 februari 2014 om upphandling av enheter som är verksamma på områdena vatten, energi, transporter och posttjänster och om upphävande av direktiv 2004/17/EG, samt Europaparlamentets och rådets direktiv 2014/23/EU av den 26 februari 2014 om tilldelning av koncessioner.

1. den specifika processen eller metoden för att producera eller tillhandahålla varorna, tjänsterna eller byggentreprenaderna, eller
2. en specifik process som avser ett annat skede i varornas, tjänsternas eller byggentreprenaderans livscykel.

Detta gäller även när de egenskaper som anges inte utgör en del av de berörda varorna, tjänsterna eller byggentreprenaderna i sig. I de tekniska specifikationerna får det också anges om överlåtelse av immateriella rättigheter kommer att krävas.

Upphandlande myndigheter får, enligt den nya lagstiftningen, besluta att vissa uppgifter som är avgörande för kontraktet ska utföras direkt av leverantörerna, om kontraktet avser tjänstekontrakt, byggentreprenadkontrakt eller monterings- eller installationsarbeten inom ramen för ett varukontrakt. Direktiven använder här begreppet ”kritiska uppgifter”. Av säkerhetsskäl torde det många gånger vid upphandling av molntjänster vara motiverat att nyttja denna rätt att begränsa möjligheten för den antagne leverantören att nyttja underleverantörer.

Slutligen bör uppmärksammas de regler om fullgörande av kontrakt som införs i den nya lagstiftningen och som utgör en kodifiering av EU-domstolens rättspraxis. Regleringen avser vilka åtgärder som kan vidtas avseende ett ingånget kontrakt. Utifrån de nya reglerna torde i många fall tilläggsavtal till ingångna avtal innefattandes tillhandahållande av molntjänster vara tillåtna förutsatt att det inte ändrar avtalets övergripande karaktär vare sig i form av ändringar och kompletterande beställningar.

1.8 Att teckna avtal med en molntjänstleverantör

1.8.1 Avtal

Vikten av tydliga, klart avgränsade och noga genomtänkta avtalsvillkor kan inte tillräckligt betonas för den myndighet som planerar att anlita en molntjänstleverantör. Innehållet i avtalsvillkoren är avgörande för att en myndighet ska kunna göra en sekretessprövning, bedöma om det finns förutsättningar att bevara och/eller gallra handlingar, kontrollera om integritetsskyddsbestämmelserna kommer att efterlevas, säkerställa att det finns skäliga sanktioner att ta till vid bristande avtalsuppfyllelse m.m. I avtalsvillkoren ska samtliga relevanta förhållanden, skyldigheter och rättigheter mellan parterna regleras. Det innebär att villkoren inte enbart måste vara förenliga med de lagar och regler myndigheten har att följa. Myndigheten måste också beakta det civilrättsliga förhållandet mellan parterna, t.ex. rätt till ersättning eller skadestånd på grund av bristande avtalsuppfyllelse, ansvarsbegränsningar, forum för tvistelösning etc.

Att teckna avtal med en molntjänstleverantör kan innebära så vitt skilda förfaranden som att klicka i en ”Jag godkänner”-box på en webbplats eller att genomföra en sedvanlig avtalsförhandling med leverantören. I många fall har myndigheten att räkna med att det är molntjänstleverantörens standardavtal som kommer att reglera förhållandet mellan parterna och myndigheten har vanligtvis inga eller mycket små möjligheter att förhandla om innehållet i avtalsvillkoren. Oavsett hur ett avtal ingås är det myndighetens ansvar att kontrollera att det finns förutsättningar att använda tjänsten i enlighet med gällande lagstiftning och att samtliga nödvändiga avtals-dokument och villkor är på plats. Det ställs således höga krav på myndighetens kompetens, erfarenhet och affärsmognad vid avtalstecknandet. I det följande kommer

vi att gå igenom vad en myndighet bör uppmärksamma särskilt innan ett avtal ingås med en molntjänstleverantör.

1.8.1.1 Avtalsparter

Utgångspunkten är här att det är en myndighet som tecknar avtal med en molntjänstleverantör och att det är dessa parter som blir bundna av avtalsvillkoren. I realiteten kan emellertid långt fler parter än dessa komma att beröras eller omfattas av avtalsvillkoren. Om molntjänstleverantören t.ex. anlitar underleverantörer måste myndigheten kontrollera att även dessa blir bundna av samma avtalsvillkor som gäller för molntjänstleverantören. Detta gäller i synnerhet när underleverantörerna behandlar personuppgifter.

Molntjänstleverantören kan i vissa fall kräva att slutanvändarna, dvs. myndighetens anställda, godkänner leverantörens användarvillkor för att få tillgång till den aktuella tjänsten. Sådana villkor innebär att slutanvändarna blir avtalsparter till leverantören och kan t.ex. åläggas personligt ansvar för att de efterlever användarvillkoren. När leverantören kräver att slutanvändarna accepterar användarvillkor måste myndigheten noggrant granska innehållet i dessa villkor för att kontrollera att de inte strider mot den lagstiftning myndigheten har att följa. Det förekommer t.ex. att leverantören i användarvillkoren inhämtar samtycke från slutanvändarna att behandla deras personuppgifter för egna ändamål. Slutanvändaren har i praktiken inget annat val än att godkänna användarvillkoren när det rör sig om en tjänst som denne måste använda för att kunna utföra sina arbetsuppgifter. Samtycket torde emellertid inte kunna utgöra ett lagligt stöd för behandling av personuppgifter eftersom den anställde inte har lämnat samtycket frivilligt.[84] Anställda befinner sig i ett beroendeförhållande till sin arbetsgivare och kan ha svårt att neka att godkänna användarvillkoren när detta innebär att den aktuella tjänsten inte kan användas av den anställde och denne därmed inte kan utföra de arbetsuppgifter han eller hon är anställd för att utföra. Ytterligare en aspekt av leverantörens inhämtande av samtycke och behandling av personuppgifter för egna ändamål är att uppgifterna anses utlämnade av myndigheten till leverantören. Ett sådant utlämnande måste vara förenligt med offentlighets- och sekretesslagen och integritetsskyddslagstiftningen. Sammanfattningsvis måste myndigheten noggrant kontrollera eventuella användarvillkor då innehållet i dessa kan strida mot gällande lag och under sådana förutsättningar kan molntjänsten inte användas.

Det är relativt vanligt att en myndighet som planerar att använda en molntjänst tecknar avtal med en it-leverantör som är etablerad i Sverige men som tillhandahåller tjänster från en annan, global, molntjänstleverantör. Under sådana förhållanden måste myndigheten vara medveten om att vissa avtal, t.ex. personuppgiftsbiträdesavtalet, ska reglera inte bara den nationella it-leverantörens behandling av personuppgifter utan även den faktiska molntjänstleverantörens behandling av personuppgifter.

Slutligen när det gäller avtalsparter ska också nämnas det förhållandet att en myndighetsanställd på eget initiativ tecknar avtal med en molntjänstleverantör för att använda en tjänst i syfte att utföra sina arbetsuppgifter. Vanligtvis har en myndighet tydliga föreskrifter om vem på myndigheten som har rätt att ingå avtal för

[84] Enligt definitionen i 3 § PuL är samtycke varje slag av frivillig, särskild och otvetydig viljeyttring genom vilken den registrerade, efter att ha fått information, godtar behandling av personuppgifter som rör honom eller henne.

myndighetens räkning. Gratistjänster som levereras direkt över internet kan emellertid användas av vem som helst och för vilka ändamål som helst. Detta kan medföra att myndighetsanställda, i god tro, väljer att ta hjälp av molntjänster för att utföra sina arbetsuppgifter. Om detta innebär att personuppgifter kommer att behandlas i molntjänsten faller den behandlingen i regel under den personuppgiftsansvarige myndighetens ansvar. Myndigheten torde då bli bunden av det avtal som har ingåtts, i vart fall rörande den personuppgiftsbehandling som utförs i tjänsten. För att undvika dylika situationer är det angeläget att myndigheten inte bara har tydliga riktlinjer om hur det är tillåtet att använda molntjänster. Riktlinjerna måste också regelbundet kommuniceras ut i verksamheten.

1.8.1.2 Vad kan ingå i ett avtalspaket?

För att en myndighet ska kunna ta ställning till om det finns lagliga förutsättningar att anlita en molntjänstleverantör måste myndigheten veta vilka dokument som ingår i avtalspaketet. Har myndigheten inte möjlighet att förhandla om avtalsvillkoren måste myndigheten noggrant granska samtliga dokument som ingår i avtalspaketet för att kunna ta ställning till om det är juridiskt möjligt att hantera myndighetens information i tjänsten. Granskning av avtal kan vara en grannlaga uppgift och det kan finnas många fallgropar på vägen. Första steget i en avtalsgranskning är att få en överblick över vilka dokument som ingår i själva avtalspaketet. Det kan vara värt att notera att den omständigheten att ett dokument har en viss benämning inte alltid innebär att dokumentets innehåll är det som förespeglas. Eftersom en molntjänstleverantör ofta tillhandahåller sina avtal via webben måste granskaren också ta hänsyn till om det i dokumenten finns andra länkade dokument och bedöma vilken status de länkade dokumenten har i avtalet med leverantören.

Avtalspaketet kan utöver huvudavtalet även innehålla:

1. personuppgiftsbiträdesavtal,
2. EU-kommissionens standardavtalsklausuler för överföring av personuppgifter till tredje land,
3. Service Level Agreement (SLA),
4. säkerhetspolicy,
5. integritetspolicy,
6. användarvillkor (för slutanvändarna) m.m.

Det är inte alltid helt klart för den avtalstecknande myndigheten vilken juridisk status de ovan uppräknade dokumenten har. Vissa dokument utgörs av leverantörens ambitioner och målsättningar utan att innehålla några konkreta utfästelser från leverantörens sida eller krav gentemot kunden. Även om ett dokument inte är juridiskt bindande är det viktigt att den avtalstecknande myndigheten sätter sig in i och förstår innehållet då det kan ge en fingervisning om hur molntjänstleverantören t.ex. kommer att behandla personuppgifter eller under vilka förutsättningar leverantören ensidigt kan ändra i dokumentet.

1.8.1.3 Avtalsvillkor som bör uppmärksammas särskilt

Generellt sett vilar ett stort ansvar på en myndighet som vill teckna avtal med en molntjänstleverantör. Avtalen är ofta författade på engelska och det kan vara svårt att utläsa och tolka innebörden av villkoren. Det är utomordentligt viktigt att en

myndighet granskar avtalsvillkoren noga för att förvissa sig om att villkoren är rimliga och säkerställer en hantering av myndighetens information som är förenlig med svensk lagstiftning såväl under den tid kontraktet löper som vid dess upphörande. Det är emellertid inte tillräckligt att myndigheten granskar de befintliga villkoren utan myndigheten bör också fundera över om det är något förhållande som har lämnats oreglerat i avtalet till nackdel för myndigheten. Nedan listas några exempel på avtalsvillkor som en myndighet bör ägna lite extra uppmärksamhet innan ett avtal ingås med en molntjänstleverantör. Uppräkningen är enbart exemplifierande och inte på något sätt uttömmande.

- **Tillämplig lag och tvistelösningsforum**

De flesta avtal innehåller klausuler om vilket lands lag som ska tillämpas och vilken domstol som är behörig vid en eventuell tvist mellan parterna eller om tvisten ska lösas genom skiljeförfarande. En myndighet måste vara uppmärksam på dessa villkor då det inte är självklart att svensk lag är tillämplig eller att tvister ska lösas i Sverige. Att driva rättsprocesser utanför Sveriges gränser kan bli mycket kostsamt och tidskrävande för en myndighet.

När det gäller eventuella tvister med anledning av brister i behandlingen av personuppgifter är det tvärtom ganska vanligt att personuppgiftsbiträdesavtalet fastställer att dataskyddsdirektivet eller personuppgiftslagen är tillämplig men även detta bör givetvis kontrolleras av myndigheten.

- **Rätt att ändra i avtalsvillkoren**

En molntjänstleverantör kan förbehålla sig rätten att ensidigt införa ändringar i avtalet eller i andra dokument som hör till avtalspaketet. I vissa fall ges myndigheten rätt att frånträda avtalet om ändringarna t.ex. påtagligt påverkar myndighetens möjlighet att utnyttja tjänsten. Hur avtalsändringarna förmedlas till myndigheten kan vara reglerat i avtalet och sker ibland genom att leverantören postar information om ändringarna på sin webbplats eller genom att ett e-postmeddelande skickas till myndigheten. Rätten att införa ändringar kan skilja sig mellan t.ex. huvudavtal och personuppgifts-biträdesavtal jämfört med t.ex. policydokument och användarvillkor. I policy-dokument och liknande har leverantören ofta större utrymme att införa ändringar jämfört med i huvudavtalet och biträdesavtalet.

- **Ansvarsbegränsning och rätt till ersättning vid skada**

I molntjänstleverantörens standardavtal kan det finnas klausuler som i stor utsträckning begränsar leverantörens ansvar för eventuell skada som åsamkas den avtalstecknande myndigheten. Det kan röra sig om att leverantören endast ersätter direkt skada som har åsamkats myndigheten när leverantören har agerat grovt vårdslöst. Den eventuella skadeersättningen som kan komma myndigheten till del har ibland en övre gräns som är förhållandevis låg. Ersättningen kan också vara begränsad i förhållande till den avgift myndigheten har erlagt för tjänsten för en viss angiven period. Mot bakgrund av att molntjänster kan tillhandahållas gratis eller relativt billigt kan den ersättning som myndigheten har rätt till i kontanta medel vara mycket låg.

- **Leverantörens hantering av personuppgifter**

Den myndighet som använder en molntjänst är personuppgiftsansvarig för de personuppgifter som hanteras i tjänsten. Molntjänstleverantören får inte, som personuppgiftsbiträde, behandla personuppgifterna för egna ändamål.

Det är inte ovanligt att en molntjänstleverantör har otydliga avtalsvillkor när det gäller hur leverantören behandlar de personuppgifter som en myndighet hanterar i en molntjänst. I vissa avtal framgår till och med explicit att leverantören har för avsikt att behandla personuppgifterna för egen räkning. Som huvudregel är det inte förenligt med de integritetsskyddsbestämmelser en myndighet har att följa att låta ett personuppgiftsbiträde behandla personuppgifter för egna ändamål. Utgångspunkten ska i stället vara att avtalsvillkoren måste innehålla tydliga och klart avgränsande instruktioner för hur molntjänstleverantören får behandla personuppgifterna.

- **Portabilitet och radering**

En myndighet som har för avsikt att hantera allmänna handlingar i en molntjänst måste kontrollera att det finns förutsättningar att uppfylla arkivlagens bestämmelser om bl.a. bevarande och gallring. Molntjänstleverantörens standardavtal kan innehålla villkor om hur informationen som hanteras i en tjänst kommer att hanteras när avtalstiden har löpt ut. Vissa leverantörer erbjuder sig att återlämna information i ett hanterbart format, ibland mot en avgift, medan andra överlämnar helt åt myndigheten att se till att den hämtar hem den information som ska bevaras. När det gäller gallring måste myndigheten kontrollera att leverantören åtar sig att gallra uppgifter såväl under avtalstidens gång som när kontraktet har löpt ut och myndigheten har hämtat hem eller flyttat sin information till en annan leverantör. Det är inte enbart arkivlagen som kan ställa krav på att uppgifter ska gallras. Även i registerförfattningar kan det finnas bestämmelser om när personuppgifter ska avskiljas eller raderas och enligt 9 § i) PuL ska myndigheten se till att uppgifter inte bevaras längre än vad som är nödvändigt med hänsyn till ändamålen med behandlingen.

- **Incidentrapportering**

Myndigheter som använder molntjänster ansvarar för att personuppgifter som behandlas i tjänsten omgärdas av tillräckliga säkerhetsåtgärder enligt personuppgiftslagen. Även när information inte innehåller personuppgifter måste myndigheten säkerställa att informationen är tillräckligt skyddad i förhållande till dess känslighet. För närvarande har Myndigheten för samhällsskydd och beredskap (MSB) ett system för frivillig incidentrapportering för myndigheter. Inom kort kan det dock komma att införas en obligatorisk it-incidentrapportering för statliga myndigheter.[85] En förutsättning för att en myndighet ska kunna rapportera en it-incident till MSB är givetvis att myndigheten själv, från sin molntjänstleverantör, har fått information om *att* det har förekommit en it-incident.

En myndighet kan inte förutsätta att en molntjänstleverantör kommer att rapportera eventuella it-incidenter till myndigheten. I vissa fall lämnas denna fråga oreglerad i avtalet vilket torde innebära att leverantören avgör själv om och när den vill rapportera en incident. Även då leverantörens rapportering av it-incidenter regleras i avtalet är det relativt vanligt att [avtalsvillkoren är formulerade på ett sådant sätt att] det [fortfarande] är upp till leverantören att avgöra vilka eventuella incidenter som ska rapporteras. Detta är givetvis inte acceptabelt ur ett säkerhetsperspektiv utan myndigheten måste förvissa sig om att samtliga eventuella it-incidenter som inträffar och som

[85] *Informations- och cybersäkerhet i Sverige*, SOU 2015:23 s. 19.

har betydelse för myndigheten ur något perspektiv rapporteras tillbaka till myndigheten.

- **Underleverantörer**

Det är vanligt att en molntjänstleverantör anlitar egna underleverantörer för att tillhandahålla en molntjänst. En myndighet som i avtalet godtar ett sådant förfarande måste vara medveten om att alla avtalsvillkor rörande personuppgiftsbehandlingen som gäller i förhållande till molntjänstleverantören också ska gälla för samtliga underleverantörer. Har myndigheten överlåtit till molntjänstleverantören att se till att underleverantören blir bunden av avtalsvillkor som motsvaras av dem som har upprättats i personuppgiftsbiträdesavtalet mellan myndigheten och molntjänstleverantören ska detta framgå av avtalet mellan myndigheten och leverantören. Vidare ska det finnas avtalsvillkor som garanterar att myndigheten får tillräcklig information om vilka underleverantörer som anlitas. Om leverantören avser att anlita en ny underleverantör ska myndigheten informeras om detta innan underleverantören påbörjar behandling av myndighetens personuppgifter. Är underleverantören etablerad i tredje land ska det finnas ett lagligt stöd för att överföra personuppgifterna till detta land.

- **Granskning av molntjänstleverantören och dess underleverantörer**

Myndighetens skyldighet att kontrollera den behandling av personuppgifter som utförs av ett personuppgiftsbiträde framgår av 31 § PuL. Kontrollskyldigheten omfattar såväl molntjänstleverantören som alla dess underleverantörer som behandlar personuppgifter. Om myndigheten har tecknat EU-kommissionens standardavtalsklausuler med personuppgiftsbiträden i tredje land framgår kraven på kontroll och revision även av detta avtal. Kontroll och revision behöver inte nödvändigtvis utföras av myndigheten själv utan den kan anlita en oberoende tredje part för att utföra kontrollen.

Molntjänstleverantörens standardavtal reglerar ofta hur revision ska utföras och i praktiken utses i regel granskaren av molntjänstleverantören. En myndighet kan sällan eller aldrig påverka förutsättningarna för granskningen eller vad som ska granskas. Myndighetens rätt till insyn i kontrollerna och resultatet av dessa är ofta begränsad till att ta del av en revisionsrapport. Det kan starkt ifrågasättas om detta förfarande är tillräckligt för att uppfylla de kontrollkrav som framgår av personuppgiftslagen.

1.8.2 Sammanfattning avtal

Som framgått ovan är avtalsgranskning, eller avtalsförhandling när sådan är möjlig, ett av de viktigaste momenten för en myndighet som avser att anlita en molntjänstleverantör. Det är genom avtalet myndigheten ska ges förutsättningar att uppfylla alla legala krav som åvilar myndigheten och också i övrigt se till att förhållandet mellan avtalsparterna är rimligt och skäligt ur alla perspektiv såväl vad gäller ansvar för skada som tillämplig lag och forum för tvistelösning etc. I ett upphandlingsförfarande är det emellertid inte tillräckligt att myndigheten blir varse vilka krav som måste ställas på leverantören i samband med granskningen eller förhandlingen av avtalet. Myndigheten måste redan i sin kravställning i upphandlingens förberedande arbete klargöra vilka oavvisliga krav myndigheten har på avtalsvillkoren och när det finns utrymme att anpassa avtalsvillkoren efter de särskilda omständigheter som råder mellan myndigheten och molntjänstleverantören.

1.9 Risker med att hantera myndighetsinformation i andra länder

Information som lagras utanför Sveriges gränser kommer att exponeras för andra länders nationella rättsordningar. Om en myndighet t.ex. anlitar en molntjänst-leverantör som lagrar myndighetens information på servrar i USA, kan den amerikanska lagstiftningen t.ex. ge stöd för att dess nationella brottsutredande myndigheter, under vissa förutsättningar, kan få tillgång till informationen i fråga.

Prism-skandalen som briserade i juni 2013 i och med visselblåsaren Edward Snowdens avslöjanden är ett exempel på när en främmande stat, på ett storskaligt sätt, har tagit del av information som lagras i molntjänster. Prism är ett signalspanings-program som används av amerikansk underrättelseverksamhet för insamling av uppgifter från hela världen. Dokument som Edward Snowden läckte visar att programmet har gett National Security Agency (NSA) och Federal Bureau of Intelligence (FBI) tillgång till realtidskommunikation såväl som lagrad information från människor över hela världen via nio internetföretag bl.a. Microsoft, Google och Apple.[86]

Det ovan sagda är ett exempel på när ett annat land, i detta fall USA, har fått tillgång till information för att informationen hanterades i USA av amerikanska bolag. För närvarande pågår en domstolsprocess i USA där den rättsliga fråga som ska prövas är om en amerikansk brottsutredande myndighet, med stöd i sin nationella lagstiftning, har rätt att få tillgång till informationen i ett e-postkonto som lagras på Irland av ett amerikanskt bolag.[87] Domstolens avgörande kan få stor påverkan på den europeiska molntjänstmarknaden. Om domstolen bedömer att den amerikanska myndigheten har laglig rätt att få åtkomst till informationen som lagras på Irland kan det innebära att det saknar betydelse var information lagras geografiskt. Så länge informationen i fråga hanteras av ett amerikanskt bolag kan den vara åtkomlig för amerikanska myndig-heter.

De exempel som redogjorts för ovan gäller USA och amerikanska bolag. En svensk myndighet som utreder möjligheten att hantera sin information utanför Sveriges gränser måste dock beakta att oavsett i vilket land informationen hanteras kan den bli åtkomlig för myndigheterna i det landet. Även när informationen hanteras inom gränserna för EU/EES kan leverantören bli skyldig att lämna ut uppgifter till myndig-heterna i det land där uppgifterna lagras. För en svensk myndighetsjurist kan det te sig svårt att sätta sig in i andra staters rättsordningar och göra en välgrundad analys av vilka förutsättningar som gäller för att leverantören ska vara skyldig att lämna ut myndighetens information till en myndighet i det land där uppgifterna lagras. Av denna anledning bör en svensk myndighet helt enkelt utgå ifrån att information som lagras i ett annat land kan komma att bli tillgänglig för det landets myndigheter. Med denna utgångspunkt måste myndigheten ta ställning till vilka konsekvenser ett sådant

[86] https://sv.wikipedia.org/wiki/Prism_(%C3%B6vervakningsprogram) Sidan är hämtad den 24 november 2015.

[87] En mer utförlig beskrivning av målet finns här. https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/07/23/does-it-matter-who-wins-the-microsoft-ireland-warrant-case/ http://www.computing.co.uk/ctg/analysis/2389869/why-i-hope-microsoft-loses-court-case-against-the-nsa-privacy-campaigner Sidorna är hämtade den 24 november 2015.

tillgängliggörande kan få och därefter avgöra var informationen bör hanteras geografiskt.

Avslutningsvis kan det nämnas att även Sverige, genom Försvarets radioanstalt (FRA), har laglig rätt att utöva signalspaning på bl.a. datatrafik som flödar över Sveriges gränser. Signalspaningen sker bl.a. på uppdrag av regeringen, regeringskansliet och Säkerhetspolisen. Under vilka förutsättningar signalspaning får utföras regleras av lagen (2008:717) och förordningen (2008:923) om signalspaning i underrättelseverksamhet.

1.10 Avslutande sammanfattning

Ur ett juridiskt perspektiv skiljer sig inte användningen av molntjänster från traditionell outsourcing. Det är samma lagar som aktualiseras och myndigheten måste göra samma typer av avvägningar och bedömningar som vid vanlig outsourcing. För att myndigheten ska kunna avgöra om en planerad användning av en molntjänst är förenlig med gällande rätt krävs att myndigheten gör en s.k. laglighetskontroll. En förutsättning för att myndigheten ska kunna göra en tillförlitlig laglighetskontroll är att myndigheten har kartlagt vilken typ av information som myndigheten har för avsikt att behandla i molnet.

I laglighetskontrollen räcker det inte att myndigheten konstaterar att sekretess inte utgör ett hinder för att lämna ut uppgifterna till molntjänstleverantören. Myndigheten måste också pröva om behandlingen av personuppgifter är tillåten. Även om det finns förutsättningar att uppfylla kraven i personuppgiftslagen eller tillämplig registerförfattning måste myndigheten ta ställning till om det rör sig om material som ännu inte är allmänna handlingar och som kan komma att ändra status för att molntjänstleverantören utför andra behandlingar av uppgifterna än vad som omfattas av begreppen teknisk bearbetning eller teknisk lagring enligt tryckfrihetsförordningen. Om myndigheten kommer att hantera allmänna handlingar i molntjänsten måste myndigheten förvissa sig om att det finns förutsättningar att uppfylla kraven på en god offentlighetsstruktur och arkivlagens krav på bevarande och gallring m.m. Bedömer myndigheten att det inte finns några lagliga hinder mot att hantera den aktuella informationen i en molntjänst bör myndigheten ändå göra en avvägning om det är lämpligt att anlita en molntjänstleverantör. I denna bedömning bör myndigheten bl.a. väga in vilka konsekvenserna kan bli av att informationen exponeras för andra länders rättsordningar om den hanteras utanför Sveriges gränser.

Resultatet av myndighetens laglighetskontroll ska utgöra de krav som myndigheten ställer på molntjänstleverantörens hantering av myndighetens information. Det kan t.ex. röra sig om att leverantören och dess anställda, som kommer att få tillgång till myndighetens information, måste ingå försäkran om tystnadsplikt eller att leverantören måste garantera att det finns förutsättningar att långtidsbevara myndighetens information eller överflytta informationen i ett hanterbart format till en annan leverantör. Myndigheten kan också behöva ställa krav på hur leverantören behandlar personuppgifterna och kräva att eventuella underleverantörer bara får anlitas efter myndighetens utryckliga godkännande. Myndigheten ska vidare ställa krav på tillförlitliga kontrollmekanismer för att kunna kontrollera att leverantören efterlever de avtalsvillkor som ingås mellan parterna. Det kan innebära att myndigheten ska ha rätt att granska loggar för kontrollera att ingen obehörig åtkomst till informationen har skett och att myndigheten själv, eller genom en av myndigheten utsedd oberoende tredje part, kan utföra regelbundna revisioner hos leverantören m.m.

Myndighetens samlade kravsammanställning ska återspeglas i det upphandlingsunderlag som ska ligga till grund för myndighetens upphandling av molntjänsten. Att myndigheten vinnlägger sig om att utföra noga genomtänkta och väl förberedda upphandlingar har således avgörande betydelse för att myndigheten ska ha förutsättningar att anlita en molntjänstleverantör som kan tillgodose myndighetens krav.

Källförteckning

Lag, förordning, direktiv mm samt kommentarer till lag

Direktiv 95/46/EG (Dataskyddsdirektivet)

Arkivlagen (1990:782)

Europakonventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna, EU (1950 samt därefter ändringar genom protokoll)

EU-kommissionens beslut av den 5 februari 2010 om standardavtalsklausuler (2010/87/EU)

Europaparlamentets och rådets direktiv 1995/46/EG av den 24 oktober 1995

Europaparlamentets och rådets direktiv 2014/24/EU av den 26 februari 2014 om offentlig upphandling och om upphävande av direktiv 2004/18/EG

Europaparlamentets och rådets direktiv 2014/25/EU av den 26 februari 2014 om upphandling av enheter som är verksamma på områdena vatten, energi, transporter och posttjänster och om upphävande av direktiv 2004/17/EG

Europaparlamentets och rådets direktiv 2014/23/EU av den 26 februari 2014 om tilldelning av koncessioner

Europeiska unionens stadga om de grundläggande rättigheterna (2010/C 83/02)

NJA 1991

Lagen (2007:1091) om offentlig upphandling

Offentlighet- och sekretesslag (2009:400)

Offentlighets- och sekretesslagen, En kommentar, Lenberg m.fl.

Personuppgiftsförordningen (1998:1191)

Personuppgiftslagen (1998:204)

Personuppgiftslagen, En kommentar, Sören Öman och Hans-Olof Lindblom, fjärde upplagan, 2011

Regeringsformen (1974:152)

Säkerhetspolisens föreskrifter och allmänna råd om säkerhetsskydd (PMFS 2015:3)

Säkerhetsskyddsförordningen (1996:633)

Säkerhetsskyddslagen (1996:627)

Mål och Beslut

Datainspektionens beslut den 31 maj 2013, dnr 1351-2012, fastställt av Förvaltningsrätten i Stockholm den 1 juli 2014 i mål nr 15410–13

Datainspektionens beslut den 10 juni 2014, dnr 358-2014 och den 18 juli 2014, dnr 988-2014

Datainspektionens beslut den 3 juli 2015, dnr 518-2015 och 643-2015

EU-domstolen Mål C-362/14 den 6 oktober 2015

JO:s beslut den 9 september 2014, dnr 3032-2011

Kammarrätten i Stockholm, mål 8972-12, angående krav på tillgängliggörande av personuppgifter endast i EU/EES-länder eller länder som EU-kommissionen bedömt ha en adekvat skyddsnivå för personuppgifter

Kammarrätten i Stockholm, mål 9894-14, angående krav på genomförda projekt och proportionalitetsbedömning avseende referensprojektets innehåll

Propositioner

Prop. 1975/76:160 om nya grundlagsbestämmelser angående allmänna handlingars offentlighet

Prop. 1979/80:2 (Del A) med förslag till sekretesslag m.m.

Prop. 1981/82:186 om ändring i sekretesslagen (1980:100), m.m.

Offentliga utredningar

Informations- och cybersäkerhet i Sverige (SOU 2015:23)

Myndighetsdatalag (SOU 2015:39)

Rapporter och yttranden, information och artiklar

Artikel 29-arbetsgruppens yttrande 5/2012 om datormoln (cloud computing), antaget den 1 juli 2012, 010371/12/SV (WP196)

Artikel 29-arbetsgruppens "Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995 (WP 114, 2093/05/EN)"

Does it matter who wins the Microsoft Ireland warrant case?, the Washington Post, https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/07/23/does-it-matter-who-wins-the-microsoft-ireland-warrant-case/ (sida hämtad 20151124)

EU-kommissionens meddelande "Återskapande av förtroendet för dataflöden mellan EU och Förenta staterna", COM(2013) 846 final, och "Om hur principerna om integritetsskydd (safe harbour) fungerar när det gäller EU:s medborgare och företag som är etablerade i EU", COM(2013) 847 final

EU-kommissionens meddelande "Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgement by the Court of Justice in Case C-362/14 (Schrems)", COM(2015) 566 final

EU-kommissionens rapport "Report on Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection", november 2013

Lista över företag som har fått beslut om undantag för tredjelandsöverföring av personuppgifter med stöd av BCR, http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm

Molntjänster och personuppgiftslagen, informationsblad från Datainspektionen

Opinion on C-SIG Code of Conduct on Cloud Computing, 2588/15/EN, WP 232, september 2015

Prism övervakningsprogram, https://sv.wikipedia.org/wiki/Prism_(%C3%B6vervakningsprogram) (sida hämtad 151124)

Privacy campaigner: Why I hope Microsoft loses court case against the NSA, Computing, http://www.computing.co.uk/ctg/analysis/2389869/why-i-hope-microsoft-loses-court-case-against-the-nsa-privacy-campaigner (Sida hämtad 151124)

Privacy Level Agreement [V2]: A Compliance Tool for Providing Cloud Services in the European Union. Cloud Security Alliance, maj 2015

Sekretess vid outsourcing – en förstudie, Fi 2009:01/2015/4, 2015-03-19

Säkerhet för personuppgifter, Datainspektionens allmänna råd, november 2008

U.S.-EU SAFE HARBOR LIST, lista över företag som är anslutna till Safe Harbor-principerna, https://safeharbor.export.gov/list.aspx

Är inköpen av samma slag? Hjälpregler för beräkning av kontraktsvärdet vid direktupphandlingar av samma slag, Vägledning från Konkurrensverket 1(2015)