Outsourcing – en vägledning om sekretess och persondataskydd

2016-01-27

Innehåll

Fakta om eSam

eSamverkansprogrammet (eSam) är en frivillig fortsättning efter E-delegationen och består av 18 medlemmar. Syftet med programmet är att vara ett forum för fortsatt samverkan mellan myndigheter och SKL och ska bygga vidare på de kunskaper och erfarenheter som byggts upp inom ramen för E-delegationen. En viktig uppgift för programmet är att ge ut vägledningar som skapar förutsättningar för att öka den digitala samverkan inom offentlig förvaltning.

Medlemmar är: Arbetsförmedlingen, Bolagsverket, Centrala Studiestödsnämnden, eHälsomyndigheten, Ekonomistyrningsverket, Försäkringskassan, Jordbruksverket, Kronofogdemyndigheten, Lantmäteriet, Migrationsverket, Pensionsmyndigheten, Polisen, Riksarkivet, Skatteverket, Sveriges Kommuner och Landsting, Tillväxtverket, Transportstyrelsen och Tullverket. (januari 2016).

1. Inledning

1.1 Syfte

Outsourcing eller utkontraktering, dvs. att låta externa tjänsteleverantörer utföra funktioner som annars skulle skötas i egen regi, är en viktig del i myndigheternas strategier för att utveckla e-förvaltningen. Många myndigheter har t.ex. utkontrakterat drift och förvaltning av myndighetens informationssystem, tekniskt stöd såsom it-support och teknisk bearbetning såsom skanning, tryck och postbefordran av dokument.

I vissa fall innebär en sådan utkontraktering att tjänsteleverantören och dennes personal får tillgång till uppgifter som hos myndigheten är sekretessreglerade och därmed inte utan särskild prövning får lämnas ut. Myndigheten måste i sådana situationer göra vissa juridiska överväganden för att säkerställa att utkontrakteringen är laglig och lämplig. Detta gäller även då tjänsteleverantören fungerar som personuppgiftsbiträde åt myndigheten. I vissa fall krävs nämligen att praktiska åtgärder vidtas eller att den planerade tjänsten justeras för att utkontrakteringen alls ska kunna äga rum.

Denna vägledning är avsedd att ge myndigheterna juridiskt stöd i de överväganden rörande sekretess och skydd av personuppgifter som måste göras inför en planerad utkontraktering samt att ge handfasta förslag på åtgärder som kan vidtas i syfte att säkerställa en korrekt hantering av sekretessreglerad information. Vägledningen bygger på den förstudie som E-delegationen gjorde under våren 2015, Sekretess och outsourcing (Fi2009:01/2015/4).

1.2 Målgrupp

Denna vägledning vänder sig i första hand till jurister och andra som i sitt arbete inom statliga myndigheter, kommuner och landsting deltar i utformningen av en planerad utkontraktering eller har att bedöma lagligheten och lämpligheten i att utkontrakteringen genomförs.

1.3 Avgränsning

De statliga myndigheterna, kommunerna och landstingen har relativt stort utrymme att själva avgöra på vilket sätt deras respektive uppdrag ska fullgöras, dvs. hur och av vem arbetsuppgifterna ska utföras. Outsourcing skulle därför i princip kunna aktualiseras avseende flertalet av de uppgifter som en myndighet ansvarar för, låt vara att överlämnande av arbetsuppgifter som innefattar myndighetsutövning kräver stöd av lag. Denna vägledning fokuserar dock på utkontraktering av sådana uppgifter som är av särskilt intresse för myndigheternas e-förvaltning, såsom it-drift, vissa administrativa stödtjänster och it-relaterad infrastruktur. Detta utesluter inte att utkontraktering även av vissa andra arbetsuppgifter kräver liknande förberedelser som dem som beskrivs i denna vägledning.

Oavsett vilka uppgifter som ska utkontrakteras, med andra ord vilka tjänster som ska köpas in, krävs att myndigheten gör juridiska överväganden av olika slag. Detta förutsätter att myndigheten har tillräckliga resurser i form av kompetens och förmåga rörande bl.a. kontraktsrätt och regelverken kring offentlig upphandling. Denna vägledning behandlar dock enbart *frågor rörande handlingsoffentlighet och sekretess* samt närliggande frågor kring *persondataskydd*.[1] Vägledningen är därmed relevant bara avseende sådan utkontraktering som innebär att *information som finns hos myndigheten blir tillgänglig även för tjänsteleverantören*.

1.4 Medverkande

Arbetet med att ta fram vägledningen har genomförts av eSams rättsliga expertgrupp. Ledamöter i expertgruppen är Johan Bålman, Per Furberg, Sven Granlund, Gustaf Johnssén, Jan Sjösten, Gunnar Svensson, Mikael Westberg, Staffan Wikell, Tomas Öhrn och Christina Wikström. Adjungerade ledamöter i expertgruppen är Maria Sertcanli, Nils Fjelkegård och Maria Jonsson. I arbetet har även eSams rättsliga referensgrupp deltagit.

[1] De särskilda juridiska frågor som uppkommer i samband med molntjänster omfattas t.ex. inte av vägledningen. Pensionsmyndigheten har emellertid, i enlighet med ett regeringsuppdrag, tagit fram rapporten Molntjänster i staten, en ny generation av outsourcing. Den innehåller en bilaga, Juridisk analys, se Pensionsmyndighetens diarienummer VER 2015-157.

2. Gällande rätt

2.1 Allmänna handlingar

Enligt 2 kap. 1 § tryckfrihetsförordningen (TF) ska varje svensk medborgare ha rätt att ta del av allmänna handlingar. En handling är enligt 2 kap. 3 § första stycket TF allmän om den *förvaras* hos en myndighet och är att anse som *inkommen* till eller *upprättad* hos myndigheten. En upptagning, t.ex. en elektronisk handling, anses enligt andra stycket i samma paragraf förvarad hos myndigheten om upptagningen är 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 2 kap. 6 § första stycket TF framgår att en handling anses inkommen till en myndighet när den har anlänt till myndigheten eller kommit behörig befattningshavare till handa. I fråga om upptagning gäller i stället att den anses inkommen till myndighet när annan har gjort den tillgänglig för myndigheten på sätt som anges i 3 § andra stycket. Enligt 2 kap. 7 § TF anses en handling upprättad hos en myndighet när den har expedierats, eller om den inte har expedierats, när det ärende till vilken den hänför sig har slutbehandlats eller, om den inte hänför sig till visst ärende, när den har färdigställts av myndigheten.

En handling som förvaras hos en myndighet endast som led i teknisk bearbetning eller teknisk lagring för annans räkning anses emellertid enligt 2 kap. 10 § första stycket TF inte som allmän handling hos den myndigheten. En sådan handling omfattas således inte alls av bestämmelserna om handlingsoffentlighet. På motsvarande sätt följer det av 2 kap. 6 § 3 st. TF att en handling som återkommer till en myndighet efter teknisk bearbetning eller lagring utanför myndigheten inte anses som en inkommen handling.

2.2 Sekretess

Rätten att ta del av allmänna handlingar får enligt 2 kap. 2 § första stycket TF begränsas bara om det är nödvändigt med hänsyn till vissa, särskilt angivna, intressen. En sådan begränsning ska anges noga i en bestämmelse i en särskild lag eller, om det i ett visst fall anses lämpligare, i en annan lag som den förstnämnda lagen hänvisar till. Den särskilda lag som avses är offentlighets- och sekretesslagen (2009:400, OSL).

2.2.1 Vad innebär sekretess?

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 (3 kap. 1 § OSL). Förbudet att röja uppgifter träffar alltså varje form av röjande. Sekretess innebär således både handlingssekretess och tystnadsplikt

och gäller inte bara för uppgifter i allmänna handlingar, utan även för uppgifter som finns hos en myndighet i sådana handlingar som ännu inte blivit allmänna. Otillåtet röjande av en sekretessbelagd uppgift är straffsanktionerat som brott mot tystnadsplikt (20 kap. 3 § brottsbalken, BrB). Enligt kommentaren till brottsbalken ska något krav på att ett avslöjande har skett inte läggas in i ordet röja.[2]

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).

2.2.2 Offentlighets- och sekretesslagens tillämpningsområde

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

I bestämmelsens andra stycke anges att lagens förbud mot att röja eller utnyttja en uppgift också gäller för en *person* som fått kännedom om uppgiften genom att för det allmännas räkning delta i en myndighets verksamhet

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

Röjandeförbudet enligt lagen gäller alltså inte bara för myndighetens anställda, utan också för sådana personer som på grund av uppdrag hos myndigheten eller på annan liknande grund deltar i myndighetens verksamhet.

2.2.3 Sekretessbestämmelsers uppbyggnad

En sekretessbestämmelse består i regel av tre huvudsakliga rekvisit, dvs. förutsättningar för bestämmelsens tillämplighet. Dessa rekvisit anger sekretessens föremål, dess räckvidd och dess styrka.

Sekretessens *föremål* är den information som kan hemlighållas och anges i lagen genom ordet "uppgift" tillsammans med en mer eller mindre långtgående precisering av uppgiftens art, t.ex. uppgift om enskilds personliga förhållanden.

---

[2] Brottsbalken. En kommentar, Leijonhufvud m.fl.

En sekretessbestämmelses *räckvidd* bestäms normalt genom att det i bestämmelsen preciseras att sekretessen för de angivna uppgifterna bara gäller i en viss typ av ärende, i en viss typ av verksamhet eller hos en viss myndighet. Några få sekretessbestämmelser gäller utan att räckvidden är begränsad. Uppgiften kan då hemlighållas oavsett i vilket ärende, i vilken verksamhet eller hos vilken myndighet den förekommer.

Sekretessens *styrka* bestäms i regel med hjälp av 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.

2.2.4 Sekretessbrytande bestämmelser

Som tidigare nämnts gäller sekretess inte bara i förhållande till enskilda utan också mot andra svenska myndigheter, utländska myndigheter och mellanfolkliga organisationer, samt mellan olika självständiga verksamhetsgrenar inom en myndighet. I vissa fall måste dock myndigheter kunna lämna ut uppgifter för att kunna utföra sina uppgifter. Vidare kan enskilda i vissa fall ha ett berättigat behov av att få ta del av uppgifter som annars omfattas av sekretess. Sekretessregleringen innehåller därför särskilda sekretessbrytande bestämmelser. Dessa har utformats efter en intresseavvägning mellan myndigheternas eller enskildas behov av att ta del av uppgifterna och de intressen som de aktuella sekretessbestämmelserna avser att skydda.

Sådana sekretessbrytande bestämmelser som bryter all sekretess eller sekretess enligt väldigt många sekretessbestämmelser har samlats i lagens tredje avdelning (10 kap.). Sekretessbrytande bestämmelser som endast bryter sekretessen enligt en viss sekretessbestämmelse eller enligt några få sekretessbestämmelser har normalt placerats i anslutning till berörda sekretessbestämmelser i lagens fjärde och femte avdelning.

2.2.5 Överföring av sekretess och tystnadsplikt

Överlämnande till annan myndighet

Som huvudregel gäller att sekretess inte följer med en uppgift när den lämnas till en annan myndighet. Det beror bl.a. på att behovet av och styrkan i en sekretess inte kan bestämmas enbart med hänsyn till sekretessintresset. Offentlighetsintresset kan kräva att uppgifter som behandlas som hemliga hos en myndighet är offentliga hos en annan myndighet.

Vissa bestämmelser om överföring av sekretess med begränsade och överblickbara tillämpningsområden har dock införts. Sådana bestämmelser innebär att en *primär sekretessbestämmelse*[3] som är tillämplig hos en myndighet ska tillämpas på uppgiften även av en myndighet som uppgiften har lämnats till eller som har elektronisk tillgång till uppgiften hos den förstnämnda myndigheten (s.k. direktåtkomst). En och samma sekretessbestämmelse kan således vara en primär sekretessbestämmelse hos den utlämnande myndigheten och en *sekundär sekretessbestämmelse*[4] hos den mottagande myndigheten.

Om en sekretessreglerad uppgift lämnas från en myndighet till en annan gäller sekretess för uppgiften hos den mottagande myndigheten antingen om sekretess följer av en primär sekretessbestämmelse som är tillämplig hos den mottagande myndigheten eller om sekretess följer av en bestämmelse om överföring av sekretess. Om ingen av dessa förutsättningar är uppfyllda blir uppgiften offentlig hos den mottagande myndigheten.

Överlämnande till ett privat subjekt

Offentlighets- och sekretesslagen innehåller ingen allmän bestämmelse om tystnadsplikt för en utomstående[5] fysisk eller juridisk person som har tagit del av en sekretessbelagd uppgift. I enskilda fall kan dock tystnadsplikt enligt offentlighets- och sekretesslagen ändå gälla, nämligen då uppgiften lämnats ut med förbehåll som inskränker den enskildes rätt att lämna uppgiften vidare eller utnyttja den. Sådana förbehåll kan bl.a. meddelas med stöd av 10 kap. 14 § OSL.

I vissa andra fall av utlämnande till privata subjekt träder tystnadsplikt enligt andra författningar in, såsom den tystnadsplikt som gäller för advokater enligt 8 kap. rättegångsbalken (RB) eller inom enskilt bedriven hälso- och sjukvård enligt 6 kap. 12 § patientsäkerhetslagen (2010:659).

I situationer då mottagaren inte omfattas av någon lagreglerad tystnadsplikt och det heller inte är möjligt att lämna ut uppgifterna med förbehåll enligt offentlighets- och sekretesslagen, får behovet av tystnadsplikt tillgodoses i rent civilrättslig ordning genom avtal om tystnadsplikt (prop. 1979/80:2 Del A s. 128).

---

[3] En primär sekretessbestämmelse är enligt 3 kap. 1 § OSL en bestämmelse om sekretess som en myndighet ska tillämpa på grund av att bestämmelsen riktar sig direkt till myndigheten, omfattar en viss verksamhetstyp eller en viss ärendetyp som hanteras hos myndigheten, eller omfattar vissa uppgifter som finns hos myndigheten.

[4] En sekundär sekretessbestämmelse är enligt 3 kap. 1 § OSL en bestämmelse om sekretess som ska tillämpas på grund av en bestämmelse om överföring av sekretess.

[5] Med utomstående menas här ett organ eller en person som inte är skyldig att tillämpa de sekretessbestämmelser som gäller för myndigheten. Se avsnitt 3.3 angående vilka personer som omfattas av offentlighets- och sekretesslagens tillämpningsområde enligt 2 kap. 1 § OSL.

2.3 Skydd av personuppgifter

Skyddet för den enskildes personliga integritet och respekten för privatlivet är viktiga grundläggande rättigheter som kommer till uttryck i både 2 kap. 6 § regeringsformen (RF) och art. 8 i Europakonventionen. När det gäller automatiserad behandling av personuppgifter har dessa grundläggande rättigheter preciserats i det så kallade dataskyddsdirektivet, 95/46/EG. Dataskyddsdirektivet har genomförts i svensk rätt genom personuppgiftslagen (1998:204; PuL) och myndigheternas registerförfattningar.

Med personuppgifter avses all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet, 3 § PuL.

2.3.1 Personuppgiftsansvar

Enligt 3 § PuL är personuppgiftsansvarig den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter. Den personuppgiftsansvarige är den som ansvarar för att behandlingen av personuppgifter är förenlig med personuppgiftslagen och med andra hos den ansvarige tillämpliga författningar, t.ex. offentlighets- och sekretesslagen. Ansvaret innebär bl.a. 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, 48 § PuL. Enligt 31 § PuL ansvarar den personuppgiftsansvarige även för att vidta lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifterna som behandlas.

I registerförfattningar anges ofta vilken myndighet som bär personuppgiftsansvaret för de behandlingar som omfattas av författningen. Varje myndighet är också personuppgiftsansvarig för den behandling av personuppgifter som sker internt för t.ex. personaladministrativa ändamål.

2.3.2 Personuppgiftsbiträde

En aktör som behandlar personuppgifter för den personuppgiftsansvariges räkning kallas personuppgiftsbiträde, 3 § PuL. Ett personuppgiftsbiträde får behandla personuppgifterna bara i enlighet med de instruktioner som den ansvarige har utfärdat för uppdraget, 30 § första stycket PuL.

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

Den personuppgiftsansvarige har i förhållande till den registrerade ett fortsatt skadeståndssanktionerat ansvar för att personuppgiftslagen följs även när personuppgiftsbehandlingen utförs av ett personuppgiftsbiträde. Den personuppgiftsansvarige 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. Biträdet kan bli skadeståndsskyldigt gentemot den personuppgiftsansvarige för eventuella brott mot dennes

instruktioner, men då på kontraktsrättslig grund och inte i enlighet med personuppgiftslagens skadeståndsregel.

Personuppgiftsbiträdesavtal

Enligt 30 § andra stycket PuL ska det finnas ett skriftligt avtal om personuppgiftsbiträdets behandling av personuppgifter för den personuppgiftsansvariges räkning. I det avtalet ska det särskilt föreskrivas att biträdet får behandla personuppgifterna 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 biträdet inte kan utföra någon otillåten behandling av uppgifterna utan att det strider mot avtalsvillkoren.

Med personuppgiftsbiträdesavtalet följer en form av tystnadsplikt för den som är anställd hos biträdet och som behandlar personuppgifter för den personuppgiftsansvariges räkning. Tystnadsplikten är emellertid inte straffsanktionerad.

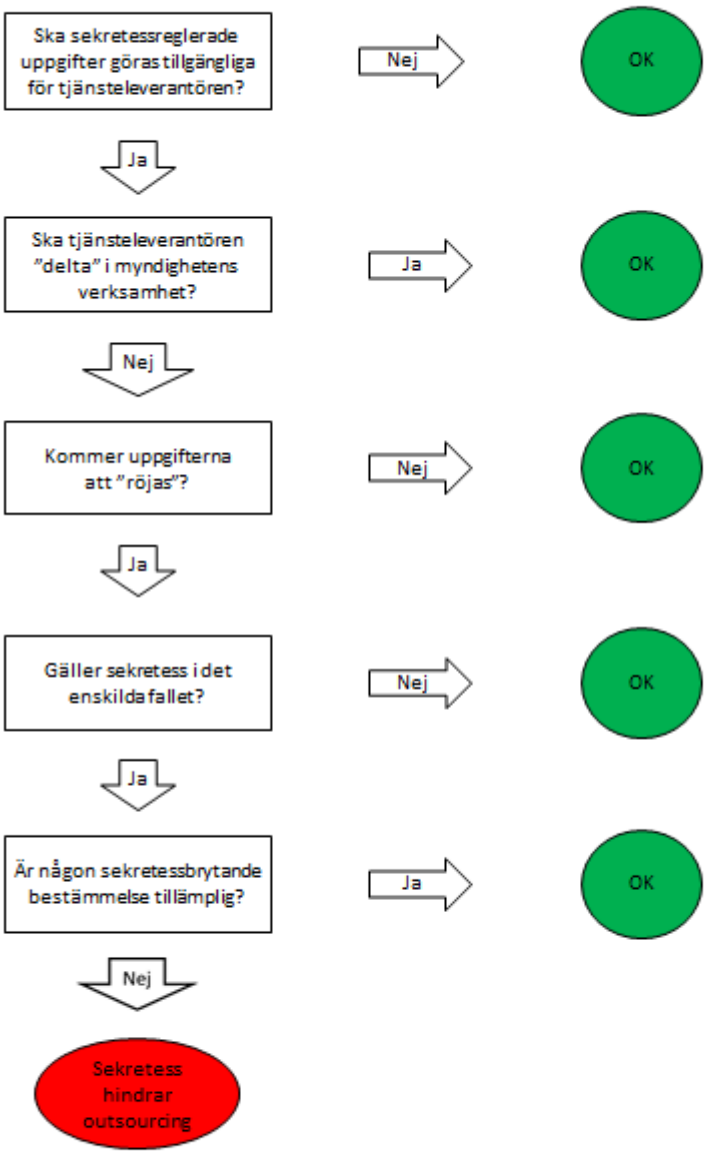
När en personuppgiftsansvarig uppdrar åt ett personuppgiftsbiträde att behandla personuppgifter måste den ansvarige se till att eventuella underleverantörer till biträdet, som också behandlar personuppgifterna, blir bundna av samma avtalsvillkor som personuppgiftsbiträdet.

3. Sekretessöverväganden

3.1 Inledning

Vid en utkontraktering som medför att information hos myndigheten blir tillgänglig även för tjänsteleverantören måste offentlighets- och sekretesslagens begränsningar beaktas. Grundprincipen är att varje myndighet ansvarar för sin egen verksamhet. En myndighet som tänker genomföra en sådan utkontraktering måste därför utreda vilka slags uppgifter som ska överlämnas till tjänsteleverantören och bedöma om denna åtgärd är tillåten enligt offentlighets- och sekretesslagen. I detta kapitel redogörs för de olika frågor som myndigheten måste ställa sig vid denna bedömning. Det ges också exempel på hur man kan resonera i olika konkreta situationer. Redogörelsen illustreras även schematiskt.

Utgör sekretess ett hinder för outsourcing?



3.2 Ska sekretessreglerade uppgifter göras tillgängliga för tjänsteleverantören?

Sekretessfrågorna måste beaktas om det finns en sekretessbestämmelse i offentlighets- och sekretesslagen som avser de uppgifter som görs tillgängliga för tjänsteleverantören.

Denna vägledning behandlar de överväganden som en myndighet kan behöva göra då en utkontraktering innebär att information som finns hos myndigheten blir tillgänglig även för tjänsteleverantören. De sekretessöverväganden som beskrivs i detta kapitel är dock bara nödvändiga om de uppgifter som görs tillgängliga är *sekretessreglerade*[6]. Den första fråga som myndigheten måste ställa sig är därför om det över huvud taget finns någon sekretessbestämmelse i offentlighets- och sekretesslagen som avser de aktuella uppgifterna och som är tillämplig hos myndigheten. Är uppgifterna däremot inte sekretessreglerade saknar detta kapitel i vägledningen relevans. Om outsourcingen innebär att tjänsteleverantören ska behandla personuppgifter måste dock regelverket rörande persondataskydd beaktas av myndigheten, se kapitel 5. Detta gäller oavsett om uppgifterna är sekretessreglerade eller inte.

Checklista – sekretessreglerade uppgifter enligt OSL

Finns det någon sekretessbestämmelse i offentlighets- och sekretesslagen som avser de aktuella uppgifterna? Med andra ord, kommer tjänsteleverantören att få tillgång till uppgifter som är sekretessreglerade hos myndigheten?

3.3 Ska tjänsteleverantören ”delta” i myndighetens verksamhet?

Sekretess behöver inte beaktas vid överlämnande av uppgifter till en fysisk person som på grund av uppdrag eller på annan liknande grund deltar i myndighetens verksamhet och därför själv omfattas av samma tystnadsplikt som myndighetens anställda.

Ett personuppgiftsbiträde finns alltid utanför den ansvariges egen organisation och kan därmed inte anses delta i myndighetens verksamhet.

Som tidigare har nämnts gäller offentlighets- och sekretesslagens röjande-förbud inte bara för myndighetens egna anställda, utan enligt 2 kap. 1 § OSL även för andra fysiska personer som på grund av uppdrag hos myndigheten, eller på annan liknande grund, för det allmännas räkning deltar i myndighetens verksamhet. Ett överlämnande av en handling eller en uppgift till en sådan person utgör varken ett utlämnande enligt tryckfrihetsförordningen eller ett röjande enligt offentlighets- och sekretesslagen. De sekretessöverväganden

[6] En *sekretessreglerad* uppgift är enligt definitionen i 3 kap. 1 § OSL en uppgift för vilken det finns en bestämmelse om sekretess. En sekretessreglerad uppgift för vilken sekretess gäller i ett enskilt fall är en *sekretessbelagd* uppgift.

som beskrivs i denna vägledning behöver därför inte göras i en sådan situation. Det blir alltså av avgörande betydelse om den planerade utkontrakteringen sker till en helt extern aktör eller om tjänsteleverantören i stället är en sådan fysisk person som deltar i myndighetens verksamhet på det sätt som avses i 2 kap. 1 § OSL.

Det är dock inte helt enkelt att dra en tydlig gräns för när en uppdragstagare eller likställd ska anses delta i en myndighets verksamhet på ett sådant sätt att denne omfattas av offentlighets- och sekretesslagen. Viss ledning för gränsdragningen, av relevans för frågan om outsourcing, ges i de ursprungliga förarbetena till den numera upphävda sekretesslagen (1980:100), prop. 1979/80:2 Del A s. 127 f. Av dessa uttalanden kan man dra slutsatsen att de avgörande faktorerna är dels graden av självständighet hos uppdragstagaren, dels uppdragets koppling till myndighetens egentliga verksamhet.

3.3.1 Självständiga uppdragstagare

Självständiga uppdragstagare, som visserligen har fått uppgifter sig anförtrodda av en myndighet men som handlar i eget namn och som utåt framstår som utrustade med egen kompetens, anses inte delta i myndighetens verksamhet enligt 2 kap. 1 § OSL. Detsamma gäller om uppdragets samband med myndighetens egentliga verksamhet är så löst att det skulle vara främmande att beteckna uppdragstagaren som en offentlig funktionär.

Exempel 1

Myndigheten A ska måla om ett rum i sina lokaler. Efter direktupphandling tecknas kontrakt med en målare som har F-skattsedel. Målaren omfattas inte av offentlighets- och sekretesslagen, trots att han har ett personligt uppdragsavtal med myndigheten, eftersom målningsarbeten inte ingår i myndighetens egentliga verksamhet.

3.3.2 Osjälvständiga uppdragstagare

Mer osjälvständiga uppdragstagare, dvs. sådana fysiska personer som har ett personligt uppdrag hos en myndighet och som har en sådan anknytning till myndigheten att de kan sägas delta i dennas verksamhet, omfattas däremot av personkretsen enligt 2 kap. 1 § OSL. Med en myndighets verksamhet avses den egentliga verksamheten, den som framgår eller kan utläsas av myndighetens instruktion eller av annan författning. I förarbetena anges att det i allmänhet kan antas att en uppdragstagare har den behövliga anknytningen till en viss myndighet, om den uppgift som han eller hon utför vanligen ska fullgöras av en tjänsteman eller någon annan befattningshavare vid myndigheten eller i varje fall naturligen skulle kunna handhas av en sådan befattningshavare.

Exempel 2

Myndigheten B anlitar ett företag för översättningstjänster. Myndigheten tecknar samtidigt ett uppdragsavtal med en av företagets anställda, som

vid översättning av texter som innehåller särskilt integritetskänsliga uppgifter ska arbeta under myndighetens direkta ledning. Vid utförandet av sådana uppdrag kommer alltså översättaren i fråga att delta i myndighetens verksamhet och omfattas av tystnadsplikt enligt offentlighets- och sekretesslagen.

3.3.3 Annan liknande grund

Offentlighets- och sekretesslagen gäller i princip inte för den som är anställd hos ett företag som i sin tur har ett uppdragsavtal med myndigheten. I förarbetena till sekretesslagen anges dock att om en myndighet har träffat avtal med ett enskilt företag, kan det i undantagsfall te sig naturligt att arbetstagare hos motparten får lyda under lagens bestämmelser, nämligen då arbetstagaren ställs till myndighetens förfogande och deltar i dess verksamhet på samma sätt som om myndigheten hade ingått uppdragsavtal med vederbörande själv. Med tanke på sådana och liknande fall gäller lagens röjandeförbud även den som på ”annan liknande grund” deltar i myndighets verksamhet. Detsamma gäller utomstående experter som rådfrågas av myndighet utan att något egentligt uppdragsavtal föreligger.

Exempel 3

Myndigheten C bestämmer sig för att utkontraktera vissa it-tjänster till ett stort it-företag. Företaget avsätter två av sina anställda att utföra uppdraget, i myndighetens lokaler. Trots att dessa personer inte har personliga uppdragsavtal med myndigheten omfattas de av personkretsen enligt offentlighets- och sekretesslagen, eftersom de deltar i myndighetens verksamhet på annan liknande grund. (Se även Exempel 10, avsnitt 3.6.4.)

3.3.4 Personuppgiftsbiträde

Den som behandlar personuppgifter för den personuppgiftsansvariges räkning är enligt 3 § PuL personuppgiftsbiträde. Ett sådant biträde ska alltid finnas utanför den ansvariges egen organisation. Anställda och andra personer i den ansvariges egen organisation behandlar i stället personuppgifterna under den ansvariges direkta ledning och är alltså inte personuppgiftsbiträde enligt personuppgiftslagen. Därmed kan ett personuppgiftsbiträde inte heller anses ”delta i myndighetens verksamhet” på det sätt som avses i 2 kap. 1 § OSL.

Checklista – personkretsen enligt OSL

1. Ska tjänsteleverantören utföra en uppgift som annars skulle ha utförts av någon av myndighetens egna anställda?
2. Är tjänsteleverantören en fysisk person som på grund av uppdraget kan sägas delta i myndighetens verksamhet?
3. Kan tjänsteleverantörens anställda anses delta i myndighetens verksamhet på annan liknande grund än anställning eller uppdrag?

3.4 Kommer uppgifterna att "röjas"?

Om avtalet med tjänsteleverantören hindrar denne och dennes personal från att faktiskt ta del av eller vidarebefordra de uppgifter som görs tillgängliga och det förefaller osannolikt att detta ändå sker, bör uppgifterna inte anses vara röjda i offentlighets- och sekretesslagens mening.

Vid sådan outsourcing som kräver eller innebär att sekretessreglerade uppgifter görs tillgängliga för en självständig tjänsteleverantör, dvs. för någon som inte deltar i myndighetens verksamhet enligt 2 kap. 1 § OSL, måste myndigheten ta ställning till om tillgängliggörandet är tillåtet enligt offentlighets- och sekretesslagen. Rent systematiskt gäller lagens röjandeförbud endast för sekretessbelagda uppgifter, dvs. sådana uppgifter för vilka sekretess gäller i det enskilda fallet. Vid utkontraktering av sådana uppgifter som är av särskilt intresse för myndigheternas e-förvaltning är det dock, av praktiska skäl, ofta lämpligt att myndigheten först utreder om några uppgifter alls kommer att tillgängliggöras för den externa aktören på ett sådant sätt att uppgifterna anses vara "röjda" i offentlighets- och sekretesslagens mening. Om något sådant röjande inte är aktuellt behöver nämligen myndigheten inte göra de ibland svåra överväganden som krävs för att bestämma om sekretess gäller i det enskilda fallet.

3.4.1 Röjandebegreppet

Sekretess definieras i 3 kap. 1 § OSL som ett förbud mot att röja en uppgift, vare sig det sker muntligen, genom utlämnande av en allmän handling eller på något annat sätt. Röjandebegreppet har däremot inte getts någon legaldefinition i offentlighets- och sekretesslagen.

Otillåtet röjande av en sekretessbelagd uppgift är enligt 20 kap. 3 § BrB straffsanktionerat som brott mot tystnadsplikt. I förarbetena till straffbestämmelsen anges bl.a. att det som brott mot tystnadsplikt kan betraktas även att någon röjer något som han ska hemlighålla genom att förete en icke allmän handling eller genom att visa upp en hemlig allmän handling.[7] I vissa sammanhang har det därför antagits att det alltid utgör ett röjande att göra en uppgift tillgänglig för en utomstående, oavsett om något avslöjande av informationsinnehållet har skett eller inte.[8] En sådan utgångspunkt var rimlig och oproblematisk på slutet av 1970-talet när sekretesslagen och den nuvarande lydelsen av straffbestämmelsen kom till. Avsikten med att göra en uppgift tillgänglig för en utomstående var då sannolikt regelmässigt att mottagaren skulle ta del av uppgiften i fråga.

Sedan dess har den elektroniska informationsmängden växt närmast explosionsartat, parallellt med att den tekniska utvecklingen rusat. Detta ställer krav på myndigheternas informationshantering som man nog inte ens kunde

---

7 A. prop. s. 402. Se även Lagrådets kommentar, a. prop. s. 488.

8 Brottsbalken. En kommentar, Leijonhufvud m.fl.

föreställa sig för 35 år sedan. Det är idag knappast någon myndighet som kan utföra sitt uppdrag helt utan att utkontraktera vissa tekniska arbetsuppgifter och därmed göra uppgifter tekniskt tillgängliga för en utomstående tjänsteleverantör. Avsikten med ett sådant tillgängliggörande är dock inte att mottagaren ska tillgodogöra sig informationsinnehållet. Vid outsourcing av till exempel it-drift, scanning eller kommunikationstjänster är syftet i stället att mottagaren ska tekniskt bearbeta själva informationsmassan, oavsett dess innehåll. Enligt eSams mening finns det därför, i vart fall i dessa sammanhang, skäl att överväga en nyanserad tolkning av offentlighets- och sekretesslagens röjandebegrepp.

I förarbetena till sekretesslagen anges att innebörden av röjandeförbudet är att ”befattningshavaren inte får låta någon *ta del av* hemlig uppgift vare sig detta sker genom att allmän handling *företes* eller att någon får *ta del av* handling som inte är allmän eller att uppgiften meddelas i brev. Också andra former av röjande av en uppgift kan tänkas, t.ex. att någon *förevisar* ett hemligt föremål för annan.”[9] Enligt eSams bedömning indikerar denna formulering att ett röjande innebär inte bara att befattningshavaren gör uppgiften tillgänglig för annan, utan också att mottagaren förutsätts ta del av uppgiften i fråga eller åtminstone har rätt att göra det. Översatt till en elektronisk kontext skulle man kunna säga att ett röjande innebär inte bara att data görs tekniskt tillgängliga för mottagaren, utan också att denne förutsätts ta del av det faktiska informationsinnehållet eller åtminstone har rätt att göra det.

I rättsfallet NJA 1991 s. 103 behandlas innebörden av uttrycket ”röjer uppgift” i 19 kap. 9 § BrB (vårdslöshet med hemlig uppgift), vilket kan vara vägledande också vid tillämpningen av offentlighets- och sekretesslagen och när det gäller brott mot tystnadsplikt.[10] Högsta domstolen uttalade i den domen att det avgörande för straffansvar främst bör vara om uppgiften har blivit tillgänglig för någon obehörig ”under sådana omständigheter att man måste räkna med att den obehörige kommer att ta del av uppgiften”. Enligt eSams bedömning torde detta innebära att straffansvar för sekretessbrott knappast skulle komma i fråga om uppgifter gjorts tillgängliga för en tjänsteleverantör under sådana omständigheter att myndigheten tvärtom inte har anledning att räkna med att denne eller någon annan obehörig kommer att ta del av uppgifterna.

Det måste emellertid finnas en viss marginal mellan det utrymme för utlämnande som följer av offentlighets- och sekretesslagen och området där straffansvar för sekretessbrott föreligger.[11] Det bör alltså finnas situationer då ett tillgängliggörande utgör en överträdelse av offentlighets- och sekretesslagens röjandeförbud, utan att för den skull utgöra en straffbar gärning enligt brottsbalken. Enligt eSams bedömning tas tillräcklig höjd för en sådan marginal om mottagaren inte får ta del av eller vidarebefordra de uppgifter som görs tillgängliga och omständigheterna i övrigt är sådana att det förefaller osannolikt att detta ändå sker. Då torde enligt eSams bedömning ett röjande i offentlig-

---

9 Prop. 1979/80:2 Del A s. 119 (vår kursivering).

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

11 Jfr prop. 1979/80:2 Del A s. 85.

hets- och sekretesslagens mening inte anses ha ägt rum. Det bör dock noteras att rättsläget ännu inte kan anses vara klarlagt i detta avseende.

3.4.2 Begränsningar genom avtal

Ibland är det oundvikligt att uppgifter blir tekniskt tillgängliga för utföraren, trots att denne inte behöver ta del av själva informationsinnehållet för att kunna utföra sitt uppdrag. Så är exempelvis fallet vid outsourcing av kommunikationstjänster eller arbetsuppgifter som enbart avser teknisk bearbetning eller teknisk lagring av information, såsom ren it-drift. I sådana situationer kan det vara möjligt och lämpligt att i avtalet införa krav på tekniska och/eller rättsliga begränsningar som hindrar utföraren och dennes personal från att faktiskt ta del av eller vidarebefordra de uppgifter som myndigheten har gjort tillgängliga genom outsourcingen. Förutsatt att dessa begränsningar är tillräckligt tydliga och möjliga att kontrollera, exempelvis genom loggning av alla transaktioner, samt att missbruk kan beivras med kännbara sanktioner, torde det vara osannolikt att någon obehörig ändå skulle ta del av de aktuella uppgifterna. Enligt eSams uppfattning bör ett röjande i offentlighets- och sekretesslagens mening inte anses ha skett vid denna typ av tillgängliggörande av uppgifter. Det bör dock observeras att om tjänsteleverantören är en annan myndighet, skulle denna typ av begränsningar inte ha någon rättslig verkan för det fall att informationen utgör allmänna handlingar hos den myndigheten. Skyldigheten enligt tryckfrihetsförordningen att pröva en begäran om utlämnande skulle då ha företräde framför avtalets begränsningar. Endast om samtliga uppgifter i den handling som efterfrågas omfattas av absolut sekretess kan myndigheten i en sådan situation underlåta att ta fram och granska handlingen.

Myndigheten bör alltså ta ställning till om tjänsteleverantören måste ta del av de tillgängliggjorda uppgifterna för att kunna utföra sitt uppdrag. I så fall står det klart att uppgifterna kommer att röjas för tjänsteleverantören. Om så däremot inte är fallet bör avtalet förbjuda tjänsteleverantören och dennes personal att faktiskt ta del av eller vidarebefordra uppgifterna. Om det mot bakgrund av avtalets kontroll- och sanktionsklausuler kan antas vara osannolikt att detta ändå sker, bör det tekniska tillgängliggörandet enligt eSams bedömning inte anses utgöra ett röjande i offentlighets- och sekretesslagens mening.

Exempel 4

Inför de målningsarbeten som beskrivs i Exempel 1 måste målaren ges tillgång till myndighetens lokaler, där handlingar som innehåller sekretessreglerade uppgifter förvaras. Myndigheten A konstaterar dock att målaren inte behöver ta del av några sekretessreglerade uppgifter för att kunna utföra sitt uppdrag. Eftersom myndigheten har goda rutiner kring hanteringen av känsliga handlingar bedömer myndigheten att det är osannolikt att målaren faktiskt tar del av sådana uppgifter.

Exempel 5

Myndigheten D överväger att utkontraktera sin it-drift, inklusive driften av e-tjänsten eget utrymme. Man gör bedömningen att uppdraget kan skötas utan att tjänsteleverantören behöver ta del av eller vidarebefordra några uppgifter i myndighetens it-system. Genom att i avtalet förbjuda att det ändå sker, kräva kontroller av att förbudet efterlevs och reglera kännbara sanktioner vid eventuella överträdelser bedömer myndigheten D att det är osannolikt att tjänsteleverantören eller någon annan obehörig faktiskt kommer att ta del av några uppgifter vid utförandet av it-driften. Eftersom myndigheten D anser att det därmed inte kan anses ske något röjande i offentlighets- och sekretesslagens mening, kan utkontrakteringen ske utan hinder av sekretess.

Checklista – röjandebegreppet enligt OSL

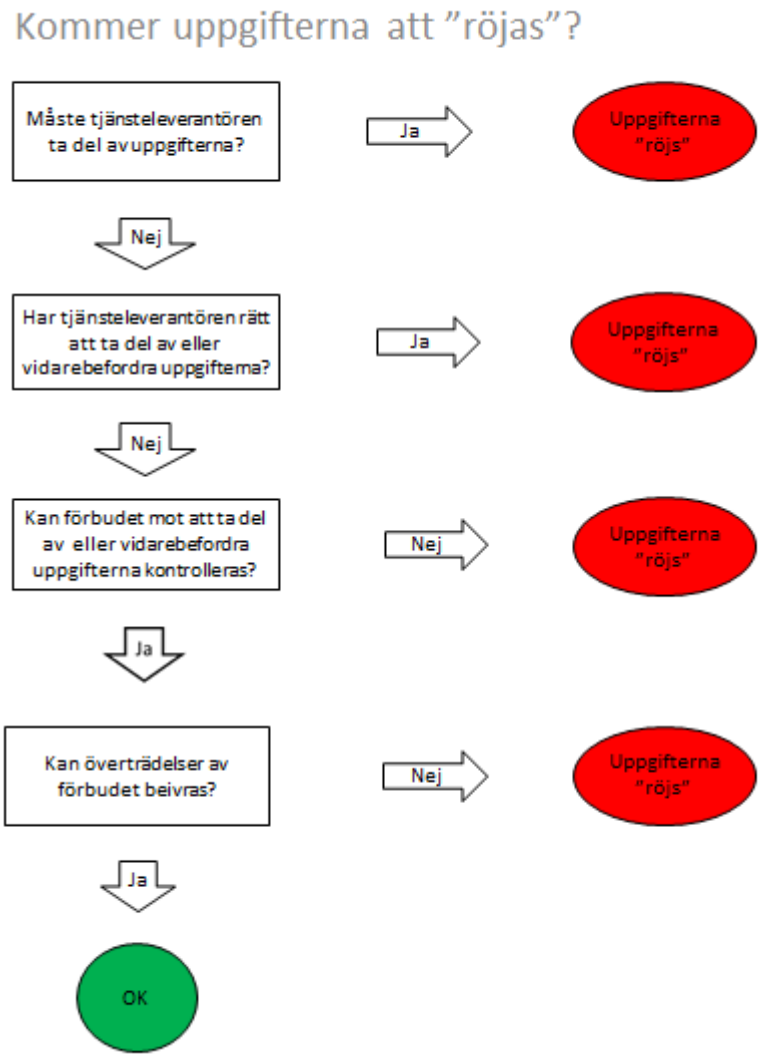
1. Måste tjänsteleverantören faktiskt ta del av de tillgängliggjorda uppgifterna för att kunna utföra sitt uppdrag?

2. Innehåller avtalet tydliga krav på tekniska och/eller rättsliga begränsningar som hindrar tjänsteleverantören och dennes personal från att faktiskt ta del av eller vidarebefordra uppgifterna?

3. Hur sannolikt är det att tjänsteleverantören eller någon annan obehörig ändå faktiskt tar del av de tillgängliggjorda uppgifterna?

a. Innehåller avtalet krav på kontroll av att begränsningarna efterlevs, exempelvis genom loggning av alla transaktioner samt uppföljning av denna?

b. Innehåller avtalet kännbara sanktioner vid överträdelser av begränsningarna?


Kommer uppgifterna att ”röjas”?
Måste tjänsteleverantören ta del av uppgifterna?
Ja
Uppgifterna ”röjs”
Nej
Har tjänsteleverantören rätt att ta del av eller vidarebefordra uppgifterna?
Ja
Uppgifterna ”röjs”
Nej
Kan förbudet mot att ta del av eller vidarebefordra uppgifterna kontrolleras?
Nej
Uppgifterna ”röjs”
Ja
Kan överträdelser av förbudet beivras?
Nej
Uppgifterna ”röjs”
Ja
OK

3.5 Gäller sekretess för de uppgifter som röjs?

För vissa särskilt skyddsvärda uppgifter om enskildas personliga förhållanden kan sekretess anses gälla även gentemot en tjänsteleverantör, om dennes personal inte omfattas av straffsanktionerad tystnadsplikt eller av någon motsvarande straffsanktionerad befogenhetsinskränkning. Däremot bör avtalsreglerad tystnadsplikt anses ge ett tillräckligt skydd för mindre integritetskänsliga uppgifter som röjs i samband med outsourcing. Detsamma bör i normalfallet gälla i fråga om uppgifter som sekretessreglerats till skydd för allmänna eller kommersiella intressen.

Om det inte är osannolikt att tjänsteleverantören faktiskt tar del av eller vidarebefordrar sekretessreglerade uppgifter, dvs. att uppgifter ”röjs” i offentlighets- och sekretesslagens mening, måste myndigheten utreda om den information som genom utkontrakteringen röjs för tjänsteleverantören är *sekretessbelagd*[12]. Myndigheten måste alltså avgöra om sekretess gäller i det enskilda fallet, dvs. i förhållande till den tilltänkta tjänsteleverantören. Med andra ord måste myndigheten pröva om sekretessbestämmelsens rekvisit är uppfyllda. Om sekretess gäller i det enskilda fallet förutsätter ett genomförande av den planerade utkontrakteringen att det finns en tillämplig sekretessbrytande bestämmelse, se avsnitt 3.6.

3.5.1 Absolut sekretess

Ett fåtal sekretessbestämmelser i offentlighets- och sekretesslagen är utformade så att de saknar skaderekvisit. I sådana fall säger man att sekretessen är *absolut*. Sådan sekretess gäller exempelvis inom beskattningsverksamheten, 27 kap. OSL, och till följd av vissa internationella avtal och EU-rättsakter, se t.ex. 30 kap. 24 § OSL. Absolut sekretess gäller även i verksamhet för enbart teknisk bearbetning eller teknisk lagring för någon annans räkning av personuppgifter, för uppgift om enskilds personliga och ekonomiska förhållanden (40 kap. 5 § OSL). Enligt eSams bedömning gäller därför absolut sekretess för sådana uppgifter om enskilds personliga och ekonomiska förhållanden som förvaras i ett s.k. eget utrymme.

Uppgifter som omfattas av absolut sekretess får aldrig ”röjas” utan stöd av en sekretessbrytande bestämmelse, även om det i det enskilda fallet skulle kunna konstateras att ett röjande inte skulle skada det intresse som sekretessen avser att skydda. Sådan sekretess gäller alltså även gentemot en utförare i samband med outsourcing. Absolut sekretess utgör dock inget hinder för sådan outsourcing som kan ske utan att uppgifterna ”röjs” i offentlighets- och sekretesslagens mening, se avsnitt 3.4, eller då utlämnandet är ”nödvändigt” för att myndigheten ska kunna fullgöra sin verksamhet, se avsnitt 3.6.3.

---

[12] En *sekretessbelagd* uppgift är enligt definitionen i 3 kap. 1 § OSL en sekretessreglerad uppgift för vilken sekretess gäller i ett enskilt fall.

3.5.2 Prövning av skaderekvisit

Flertalet sekretessbestämmelser i offentlighets- och sekretesslagen är försedda med *skaderekvisit*, vilket innebär att det måste göras en prövning av om ett utlämnande kan ske utan att det medför skada eller men för det intresse som sekretessen avser att skydda.

Konstruktionen med skaderekvisit innebär att vetskap om vem som är mottagare av en uppgift kan ha betydelse när sekretessfrågan ska avgöras. Vad mottagaren ska göra med uppgiften, hur den kommer att hanteras och vilken risk för ytterligare spridning som finns är sådana omständigheter som kan påverka bedömningen av om skaderekvisitet i sekretessbestämmelsen är uppfyllt eller inte.

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

Avgörande betydelse bör alltså som regel tillmätas de aktuella *uppgifternas art, deras känslighet*.[13] Av särskilt intresse vid prövningen av om ett skaderekvisit är uppfyllt är också *hur uppgifterna hos mottagaren skyddas mot ytterligare spridning*, dvs. om mottagaren får lämna uppgiften vidare och själv utnyttja den eller om dessa befogenheter är begränsade. Sådana begränsningar kan framgå bl.a. av

- författning, i form av bestämmelser om tystnadsplikt eller bestämmelser som inskränker rätten att behandla en viss uppgift,
- beslut om utlämnande med förbehåll enligt 10 kap. 14 § OSL,
- klausuler om tystnadsplikt eller behandlingsförbud i avtal med mottagaren, i detta fall tjänsteleverantören, kompletterade med sekretessförbindelser avgivna av tjänsteleverantörens personal avseende tystnadsplikt eller behandlingsförbud, eller
- instruktioner om hur uppgifter får eller ska behandlas enligt personuppgiftsbiträdesavtal och säkerhetsskyddsavtal, m.m.

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

Reglering av tystnadsplikt för mottagaren

Författningsbestämmelser om tystnadsplikt för personal i privaträttsligt bedriven verksamhet finns exempelvis i 8 kap. 4 § RB avseende advokater samt i 29 kap. 14 § skollagen (2010:800), 15 kap. 1 § socialtjänstlagen (2001:453), 6 kap. 12 § patientsäkerhetslagen och 15 § lagen (1997:736) om färdtjänst, avseende enskilt bedriven skolverksamhet, socialtjänst, hälso- och sjukvård respektive färdtjänst. Tystnadsplikt för privatanställda kan med bindande verkan också regleras i avtal. På motsvarande sätt kan privatanställdas rätt att behandla en uppgift inskränkas genom avtal.

För offentliga funktionärer kan tystnadsplikt bara regleras i lag eller, efter bemyndigande i lag, i annan författning. Detta följer av att tystnadsplikt i det fallet, till skillnad från när en privaträttslig aktör ålägger sina anställda tystnadsplikt, utgör en begränsning av den yttrandefrihet som var och en är tillförsäkrad gentemot det allmänna. Avtal om tystnadsplikt för offentliga funktionärer har därmed ingen rättslig verkan och kan inte påverka prövningen av skaderekvisitet.

Inskränkningar i rätten att behandla en viss uppgift kan däremot i princip införas genom avtal med en myndighet, men får inte tillämpas om det t.ex. skulle stå i strid med myndighetens skyldighet att pröva en begäran om utlämnande av allmän handling. Sådana avtal saknar således rättslig verkan i fråga om handlingar som är allmänna hos myndigheten.

Om mottagaren är en myndighet eller något annat organ som omfattas av offentlighets- och sekretesslagen är det i stället relevant att ta hänsyn till i vilken mån sekretess enligt offentlighets- och sekretsslagen, och därmed tystnadsplikt, kommer att gälla för uppgifterna även hos mottagaren. Om uppgifterna skulle sakna sekretesskydd hos den mottagande myndigheten och därmed bli offentliga där, torde sekretess regelmässigt gälla gentemot den myndigheten. Följden av att sekretess gäller gentemot mottagaren är att den planerade outsourcingen inte kan ske utan stöd av en sekretessbrytande bestämmelse, se avsnitt 3.6.

Särskilt skyddsvärda uppgifter

Vid outsourcing som innebär att uppgifter görs tillgängliga för privaträttsliga aktörer krävs normalt att myndigheten i avtal reglerar sekretessfrågan i förhållande till det utförande företaget och bland annat ställer krav på att det företaget ska sluta *avtal om tystnadsplikt* med sin personal. Det är i de allra flesta fall tillräckligt för att skaderekvisitet inte ska anses vara uppfyllt gentemot tjänsteleverantören. Enbart sådan avtalsreglerad tystnadsplikt, som alltså inte är straffsanktionerad, kan dock betraktas som otillräcklig för att skydda *särskilt skyddsvärda, mycket integritetskänsliga, uppgifter*, se JO:s beslut den 9 september 2014, dnr 3032-2011. På motsvarande sätt skulle avtalsreglerad tystnadsplikt kunna anses otillräcklig för att skydda sådana uppgifter som har ett särskilt uttalat skyddsbehov med hänsyn till Sveriges internationella relationer eller rikets säkerhet, se dock 19 kap. BrB.

Enligt eSams mening bör dock i sådana situationer även beaktas om mottagaren är bunden av någon annan straffsanktionerad bestämmelse som i praktiken får samma effekt som tystnadsplikt, dvs. en motsvarande

straffsanktionerad befogenhetsinskränkning. Sekretess bör därför enligt eSams mening inte anses gälla gentemot en tjänsteleverantör som har fått i uppdrag att självständigt handha kvalificerad teknisk uppgift eller övervaka skötseln av sådan angelägenhet eller uppgift. En sådan utförare verkar nämligen under straffansvar enligt bestämmelsen i 10 kap. 5 § BrB om trolöshet mot huvudman.

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

Exempel 6

Socialnämnden i E kommun överväger att anlita ett privat företag för att utvärdera barn- och ungdomsenhetens insatser enligt socialtjänstlagen (2001:453; SoL). Nämnden konstaterar att uppgifter som är sekretessreglerade enligt 26 kap. 1 § OSL måste röjas för tjänsteleverantören. Vidare gör nämnden bedömningen att dessa uppgifter, som rör barnen och deras familjer, är av särskilt skyddsvärd karaktär. Eftersom tjänsteleverantörens personal omfattas av straffsanktionerad tystnadsplikt enligt 15 kap. 1 § SoL, och dessutom enligt personuppgiftsbiträdesavtalet bara får behandla personuppgifterna i enlighet med nämndens instruktioner, bedömer nämnden att det står klart att uppgifterna kan röjas utan att den enskilde eller någon närstående till denne lider men. Det omvända skaderekvisitet i 26 kap. 1 § OSL är alltså inte uppfyllt, vilket innebär att sekretess inte gäller gentemot tjänsteleverantören.

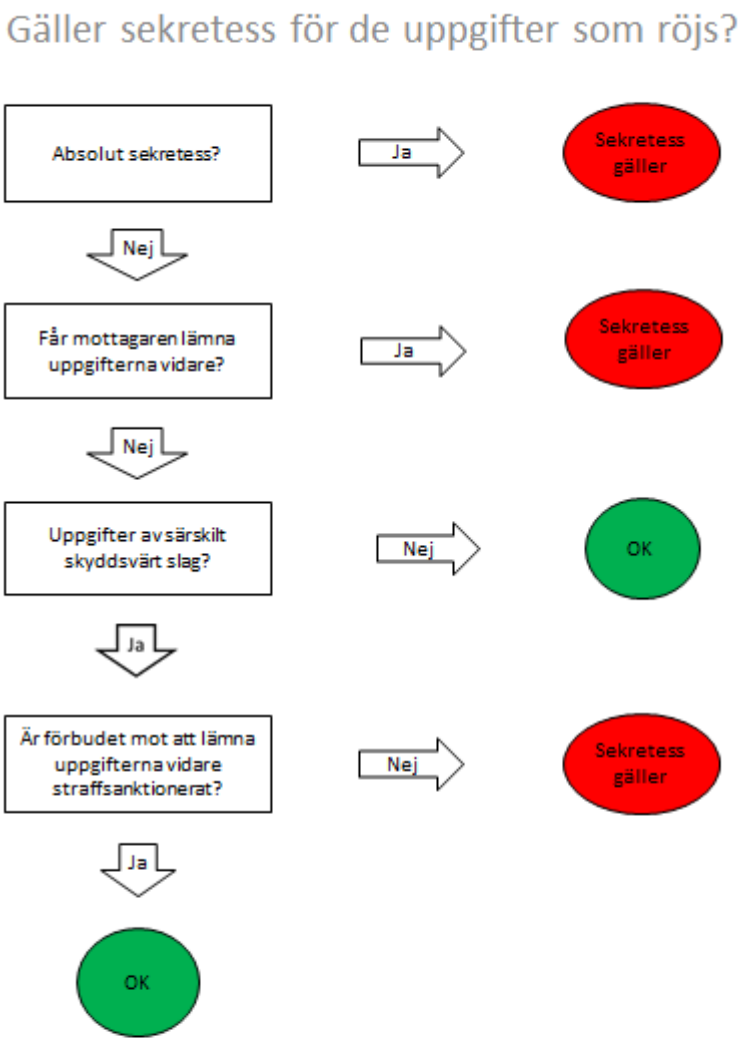
Exempel 7

Myndigheten F tänker utkontraktera vissa personaladministrativa sysslor till en privaträttslig tjänsteleverantör. Av 39 kap. 3 § andra stycket OSL och 10 § offentlighets- och sekretessförordningen (2009:641) framgår att sekretess med omvänt skaderekvisit gäller just hos myndigheten F för vissa uppgifter om de anställda. Bland annat mot bakgrund av vad som anges i förarbetena konstaterar dock myndigheten att presumtionen för sekretess inte motiveras av att uppgifterna i sig typiskt sett är av särskilt integritetskänsligt slag. Myndigheten F finner därför att skaderekvisitet inte är uppfyllt, eftersom tjänsteleverantörens anställda är avtalsrättsligt bundna av tystnadsplikt och inskränkningar av rätten att behandla uppgifterna. Sekretess gäller alltså inte gentemot tjänsteleverantören.

Checklista – prövning av skaderekvisit

1. Hur skyddsvärda är uppgifterna, typiskt sett?
2. Har mottagaren rätt att lämna uppgifterna vidare eller själv utnyttja dem?

3. Om uppgifterna är av särskilt skyddsvärt slag, är den befogenhets-inskränkning som gäller för mottagaren straffsanktionerad?



3.6 Kan röjandet ske med stöd av en sekretessbrytande bestämmelse?

Röjande av uppgifter i samband med sådan outsourcing som sker i syfte att dra nytta av utförarens expertkompetens eller tekniska utrustning, bör i särskilda fall anses utgöra ett sådant ”nödvändigt utlämnande” som kan ske utan hinder av sekretess.

Om utkontrakteringen innebär att sekretessreglerade uppgifter ska göras tekniskt tillgängliga för en aktör som inte behöver ta del av uppgifterna i fråga, kan som tidigare nämnts kontraktet utformas så att det är osannolikt att tjänsteleverantören eller någon annan obehörig faktiskt kommer att ta del av uppgifterna. I en sådan situation bör uppgifterna enligt eSams uppfattning inte betraktas som röjda i offentlighets- och sekretesslagens mening, se avsnitt 3.4. Någon sekretessbrytande bestämmelse behövs då inte för att outsourcingen ska kunna ske, oavsett hur en eventuell sekretessprövning gentemot tjänsteleverantören skulle utfalla.

I vissa fall är det dock så att en planerad outsourcing kräver eller innebär ett faktiskt ”röjande”, dvs. att tjänsteleverantören måste ta del av sekretessreglerade uppgifter för att kunna utföra sitt uppdrag eller att det i vart fall inte är osannolikt att så sker. Om uppgifterna i en sådan situation skulle vara sekretessbelagda gentemot tjänsteleverantören, dvs. om sekretess skulle gälla i det enskilda fallet, krävs stöd av en sekretessbrytande bestämmelse för att utlämnande av uppgifterna ska kunna ske och outsourcingen komma till stånd. Annars riskerar myndigheten att göra ett otillåtet röjande.

3.6.1 Om tjänsteleverantören är en annan myndighet

Om utkontrakteringen innebär att sekretessbelagda *uppgifter ska lämnas till en annan myndighet* ligger det närmast till hands att ställa sig följande frågor:

1. Är myndigheten enligt lag eller förordning skyldig att lämna ut uppgifterna, dvs. kan utlämnandet ske med stöd av den sekretessbrytande bestämmelsen i 10 kap. 28 § OSL?

2. Är det uppenbart att intresset av att uppgiften lämnas ut har företräde framför det intresse som sekretessen ska skydda, dvs. kan utlämnandet ske med stöd av den s.k. generalklausulen, 10 kap. 27 § OSL? Det bör noteras att bestämmelsen inte är tillämplig om sekretess gäller enligt vissa angivna bestämmelser.

3.6.2 Om tjänsteleverantören är en enskild aktör

Om det vid outsourcing till en enskild aktör uppstår ett behov av att tjänsteleverantören vidtar en enstaka åtgärd som kräver att denne faktiskt tar del av sekretessbelagda uppgifter, kan myndigheten överväga möjligheten att lämna ut uppgifterna med stöd av 10 kap. 14 § OSL, dvs. med förbehåll om att mottagaren inte får lämna uppgifterna vidare eller att utnyttja dem. Ett sådant

förbehåll kan inte meddelas i förväg för en viss typ av information, utan ska föregås av en prövning i varje särskilt fall. Vidare är konstruktionen över huvud taget möjlig endast om

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

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

3.6.3 Om utlämnandet är nödvändigt

Sekretess hindrar inte att en uppgift lämnas till en enskild eller till en annan myndighet, om det är *nödvändigt för att den utlämnande myndigheten ska kunna fullgöra sin verksamhet*, dvs. de uppgifter som följer av myndighetens instruktion, andra författningar, regleringsbrevet eller andra särskilda regeringsbeslut. Detta framgår av den sekretessbrytande bestämmelsen i 10 kap. 2 § OSL. Bestämmelsen ska dock användas restriktivt. Enbart en bedömning att effektiviteten i myndighetens handlande nedsätts pga. sekretess får enligt uttalanden i förarbetena inte leda till att sekretessen åsidosätts, Lagrådets yttrande, se prop. 1979/80:2 Del A s. 465.

Att bestämmelsen ska tillämpas restriktivt är dock enligt eSams mening inte detsamma som att den ska tillämpas endast i situationer av undantagskaraktär. Enligt förarbetena kan det t.ex. i särskilda fall vara ”nödvändigt” för en tjänsteman att vända sig till en utomstående expert och att då upplysa om hemliga omständigheter, prop. 1979/80:2 Del A s. 122. Detta bör enligt eSams bedömning gälla även då inhämtandet av expertkunskap sker i effektivitetsfrämjande syfte, förutsatt att åtgärden sker inom ramen för vad som utgör myndighetens egen verksamhet, dess uppdrag. Som exempel kan nämnas outsourcing av support-/help desk-funktioner samt kontraktering av rekryteringskonsulter eller upphandlingsexperter. Det kan enligt eSams bedömning också 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 kan detta visa sig vara aktuellt 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.

Det bör dock poängteras att myndigheten alltid noggrant 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, torde inte det vara tillräckligt för att outsourcingen, och därmed tillgängliggörandet av uppgifter, skulle anses vara ”nödvändig” i den mening som avses i 10 kap. 2 § OSL. För detta krävs i praktiken att outsourcing framstår som den enda realistiska lösningen.

Exempel 8

Myndigheten G avser att utkontraktera den interna it-supporten. Man inser att det emellanåt kan vara nödvändigt för tjänsteleverantören att spegla en av myndighetens datorer för att kunna ge bästa möjliga hjälp. Om den medarbetare som behöver hjälpen råkar arbeta med sekretessreglerade uppgifter kan dessa då komma att röjas för tjänsteleverantören. Myndigheten G bedömer dock att myndigheten inte kan fullgöra sitt uppdrag utan kvalificerad it-support och att myndigheten inte själv har förmåga att upprätthålla önskvärd kompetens på området. Det är därför nödvändigt att anlita externa experter, till vilka sekretessreglerade uppgifter vid behov kan lämnas ut med stöd av den sekretessbrytande bestämmelsen i 10 kap. 2 § OSL. Utkontrakteringen av supporttjänster kan därmed ske utan hinder av sekretess.

Exempel 9

Myndigheten H avser att överlåta all skanning av inkommande post på en privat tjänsteleverantör. Leverantören använder en teknik som innebär att innehållet i papperet förblir dolt för operatören. Vid eventuella tekniska problem måste dock manuella åtgärder vidtas, vilket kan medföra att innehållet i ett papper blir synligt för operatören. Myndigheten H bedömer dock att utkontrakteringen av skanningtjänster måste anses vara nödvändig för att myndigheten ska kunna fullgöra sin verksamhet, eftersom varje enskild myndighet inte rimligen kan förväntas anskaffa all den tekniska utrustning som krävs för en modern dokumenthantering.

Checklista – nödvändigt utlämnande enligt OSL

1. Kan myndighetens uppdrag rimligen fullgöras utan att utlämnande sker?
2. Motiveras utlämnandet även av andra skäl än rent ekonomiska?
3. Har alla alternativ till utlämnande övervägts noggrant?

3.6.4 Är förfarandet lämpligt?

Även om en sekretessbrytande bestämmelse är tillämplig och tillåter utlämnande av uppgifter, kan det i vissa fall betraktas som olämpligt att ett utlämnande sker.

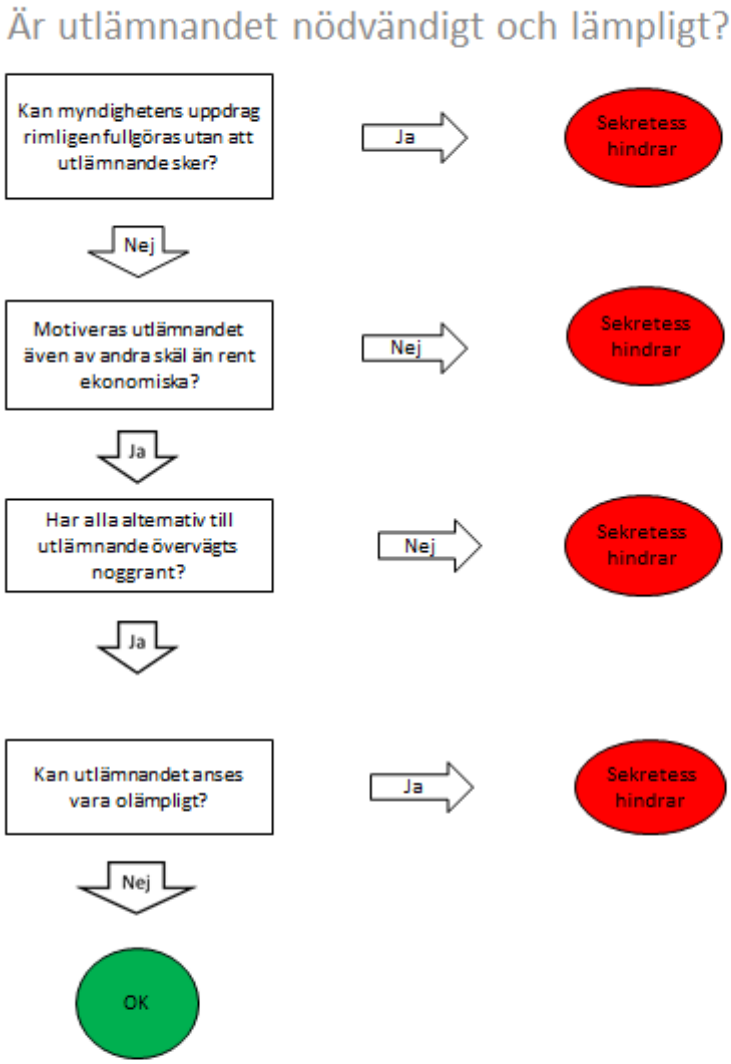
Av avgörande vikt vid lämplighetsbedömningen är att *beakta hur de intressen som sekretessen avser att skydda tillgodoses, främst huruvida tystnadsplikt gäller för mottagaren*.

Detta innebär vid outsourcing till andra myndigheter bl.a. att den s.k. generalklausulen i 10 kap. 27 § OSL bör utnyttjas med större försiktighet om informationen inte är sekretesskyddad hos den mottagande myndigheten, särskilt i fråga om uppgifter som är hemliga med hänsyn till enskilds intressen. Om en uppgift inte alls skyddas av sekretess hos den mottagande myndigheten kan risken för att skada ska uppkomma vara så stor att uppgiften inte bör lämnas ut. För säkerhets skull är också vissa särskilt känsliga uppgifter undantagna från generalklausulens tillämpningsområde, se bestämmelsens andra stycke.

Vid utlämnande i samband med outsourcing till en enskild aktör kan myndigheten däremot både ställa upp förbehåll i enskilda fall enligt 10 kap. 14 § OSL och teckna bindande avtal som inskränker mottagarens rätt att lämna uppgifterna vidare eller att utnyttja dem. Mot den bakgrunden framstår möjligheterna för myndigheten att värna de intressen som sekretessen avser att skydda snarast som större vid utlämnande till en enskild aktör än till en myndighet där sekretessen är svag eller alls inte gäller.

Exempel 10

Myndighet I har drabbats av dataintrång och har därför slagit på särskilda loggar för att händelsen ska kunna analyseras. Eftersom myndigheten inte har den särskilda expertkompetens som krävs för denna brådskande analys har myndigheten vänt sig till informationssäkerhetskonsulten Per Persson, som har en för ändamålet särskild anpassad utrustning. Per Persson bedriver sin verksamhet i aktiebolagsform. Myndigheten behöver överlämna det krypterade materialet till Per Persson, men vet inte vilka slags uppgifter materialet innehåller. Det är dock inte osannolikt att det förekommer såväl särskilt skyddsvärda uppgifter som uppgifter som omfattas av absolut sekretess. Myndighet I bedömer att ett skyndsamt överlämnande av sekretessbelagda uppgifter till Per Persson visserligen kan anses vara nödvändigt för att myndigheten ska kunna fullgöra sin verksamhet. Mot bakgrund av att myndigheten inte känner till vad materialet innehåller bedömer dock myndigheten att det skulle kunna anses olämpligt att tillämpa 10 kap. 2 § OSL. I stället informeras Per Persson om att han anses delta i myndighetens verksamhet ”på annan liknande grund” och därför omfattas av straffsanktionerad tystnadsplikt enligt 2 kap. 1 § andra stycket tredje punkten OSL (se avsnitt 3.3.3).


Är utlämnandet nödvändigt och lämpligt?
Kan myndighetens uppdrag rimligen fullgöras utan att utlämnande sker?
Ja
Sekretess hindrar
Nej
Motiveras utlämnandet även av andra skäl än rent ekonomiska?
Nej
Sekretess hindrar
Ja
Har alla alternativ till utlämnande övervägts noggrant?
Nej
Sekretess hindrar
Ja
Kan utlämnandet anses vara olämpligt?
Ja
Sekretess hindrar
Nej
OK

3.7 Hur kan tjänsten eller avtalet anpassas?

Som tidigare har nämnts måste den myndighet som överväger att outsourca en viss arbetsuppgift beakta de begränsningar som sekretessregleringen innebär. Detta medför att en planerad utkontraktering ibland måste anpassas på ett visst sätt, för att undgå att olagliga eller annars olämpliga röjanden av sekretessbelagda uppgifter sker.

Som en allmän utgångspunkt bör myndigheten enligt eSams mening sträva efter att *undvika att sekretessreglerade uppgifter görs tillgängliga* för en extern utförare. Begränsningar i detta avseende kan i den traditionella miljön ofta åstadkommas genom praktiska åtgärder, såsom att förvara skyddsvärt material i låsta skåp då det inte står under behörig tjänstemans uppsikt. I den elektroniska miljön krävs i stället tekniska hinder, såsom kryptering, vilket dock i praktiken är en kostsam metod. I vissa fall, t.ex. vid test som tjänst, kan däremot en sortering av det material som överlämnas till utföraren säkerställa att endast offentliga uppgifter lämnas ut. Vid outsourcing av it-drift kan det på motsvarande sätt övervägas om myndigheten själv ska ombesörja driften av de system där sekretessreglerade uppgifter behandlas, i stället för att överlåta all it-drift på en extern aktör. Detsamma gäller vid outsourcing av andra administrativa stödfunktioner där det är möjligt att urskilja olika typer av tjänster utifrån den information som berörs. Det är t.ex. oproblematiskt att utkontraktera tryckning och utskick till allmänheten av offentlig information, medan utskick som innehåller sekretessskyddade uppgifter om mottagaren kräver större försiktighet.

Ett annat sätt att undvika att sekretessreglerade uppgifter görs tillgängliga för en extern utförare är att genom anställnings- eller uppdragsavtal knyta den fysiska person som ska utföra uppgiften till myndigheten på ett sådant sätt att denne enligt 2 kap. 1 § OSL kan anses *delta i myndighetens verksamhet*. Detta utgör dock inte outsourcing i begreppets egentliga betydelse, eftersom arbetsuppgiften då alltjämt utförs i myndighetens egen regi.

Krav på att leverantören sluter avtal med sin personal om tystnadsplikt och förbud mot obehörigt utnyttjande av uppgifter bör alltid ingå i tjänsteavtal rörande sådan outsourcing som innebär att sekretessreglerade uppgifter görs tillgängliga för utföraren. När utföraren ska utgöra personuppgiftsbiträde åt myndigheten bör också instruktionerna för denna behandling vara så tydliga som möjligt. Om leverantören för myndighetens räkning självständigt ska handha kvalificerad teknisk uppgift eller övervaka skötseln av sådan angelägenhet eller uppgift kan det i tjänsteavtalet finnas skäl att erinra om straffansvaret enligt 10 kap. 5 § BrB rörande trolöshet mot huvudman.

I vissa fall kräver eller innebär outsourcing att sekretessreglerade uppgifter görs (tekniskt) tillgängliga för utföraren, utan att själva informationsinnehållet har någon betydelse för åtgärdens utförande. Som exempel kan nämnas flertalet typer av it-drift. I sådana situationer bör myndigheten *begränsa mottagarens rätt att ta del av eller vidarebefordra informationen*. Detta kan ske genom krav på tekniska begränsningar, men också genom förbudsklausuler i tjänsteavtalet, som bör kombineras med krav på kontrollmekanismer, såsom loggning, och kännbara civilrättsliga sanktioner vid överträdelser. I de fall där den typen av begränsningar införs på ett ändamålsenligt sätt torde det få anses osannolikt att utföraren eller någon annan obehörig faktiskt tar del av uppgifterna. Dessa bör

därmed, enligt eSams uppfattning, inte anses vara röjda i offentlighets- och sekretesslagens mening. Dessutom skulle en överträdelse av förbudet kunna aktualisera straffrättsligt ansvar för dataintrång eller trolöshet mot huvudman.

Ibland ligger det dock i arbetsuppgiftens natur att utföraren ska ta del av myndighetens information, antingen pga. att informationsinnehållet i sig påverkar arbetsuppgiftens genomförande, vilket t.ex. kan vara fallet vid outsourcing av vissa personal- eller ekonomiadministrativa göromål, eller pga. att det krävs en mänsklig kontroll av att utförandet inte har råkat förvanska informationen, såsom vid skanning. I sådana situationer bör myndigheten överväga om utlämnandet av de sekretessreglerade uppgifterna kan ske med stöd av någon sekretessbrytande bestämmelse, t.ex. om det kan anses vara ett *"nödvändigt" utlämnande* på det sätt som avses i 10 kap. 2 § OSL. Ett sådant resonemang kan i särskilda fall vara relevant i samband med sådan outsourcing som sker i syfte att dra nytta av utförarens expertkompetens eller av dennes tekniska utrustning, dvs. då den arbetsuppgift som ska utkontrakteras kräver omfattande investeringar och personal med särskild kompetens.

Om ingen sekretessbrytande bestämmelse är tillämplig kan det i vissa situationer vara möjligt för myndigheten att undanröja den risk för skada eller dylikt som hindrar ett utlämnande genom att fatta ett formellt beslut om *utlämnande med förbehåll*, i enlighet med 10 kap. 14 § OSL, till förmån för den fysiska person som ska utföra den utkontrakterade arbetsuppgiften. Denna lösning, som inte kan användas om uppgifterna omfattas av s.k. absolut sekretess, torde främst bli aktuell beträffande arbetsuppgifter som är väl avgränsade såväl i tid som sak, men skulle också kunna komma till användning vid viss felsökning, undersökning av misstankar om dataintrång och liknande it-driftsrelaterade arbetsuppgifter. Om denna typ av arbetsuppgifter är mer regelbundet förekommande framstår det emellertid som ett bättre alternativ att myndigheten posterar en anställd i tjänsteleverantörens lokaler eller att personliga uppdragsavtal tecknas med en eller flera av tjänsteleverantörens anställda, så att just dessa arbetsuppgifter kan utföras under myndighetens direkta ledning.

3.8 Sammanfattning – sekretessöverväganden

En utkontraktering kan ske utan hinder av sekretess om ett eller flera av följande påståenden stämmer:

1. Inga sekretessreglerade uppgifter kommer att göras ens tekniskt tillgängliga för tjänsteleverantören.
2. Tjänsteleverantören kommer att delta i myndighetens verksamhet enligt 2 kap. 1 § OSL.
3. Avtalet förbjuder tjänsteleverantören och dennes personal att faktiskt ta del av eller vidarebefordra de uppgifter som görs tekniskt tillgängliga och det är osannolikt att detta ändå sker.
4. De uppgifter som röjs är inte sekretessbelagda gentemot tjänsteleverantören.
5. Det finns en sekretessbrytande bestämmelse och det är inte olämpligt att tillämpa den.

Avtal om tystnadsplikt ska alltid ingås med en extern, privaträttslig tjänsteleverantör som får tillgång till sekretessreglerade uppgifter. Avtalet ska omfatta krav på att tjänsteleverantörens personal undertecknar personliga sekretessförbindelser.

Sekretessbelagda uppgifter, dvs. uppgifter för vilka sekretess gäller även gentemot tjänsteleverantören, får inte utan stöd av en sekretessbrytande bestämmelse göras tekniskt tillgängliga för tjänsteleverantören, om inte omständigheterna är sådana att uppgifterna inte ”röjs” i offentlighets- och sekretesslagens mening.

Om avtalet med tjänsteleverantören hindrar denne och dennes personal från att faktiskt ta del av eller vidarebefordra de uppgifter som görs tillgängliga och det förefaller osannolikt att detta ändå sker, bör uppgifterna enligt eSams bedömning inte anses vara röjda i offentlighets- och sekretesslagens mening. Detta förutsätter att avtalet innehåller

1. tydliga krav på tekniska och/eller rättsliga begränsningar som hindrar utföraren och dennes personal från att ta del av eller vidarebefordra de uppgifter som myndigheten gjort tillgängliga genom outsourcingen,
2. krav på kontroll av att begränsningarna efterlevs, exempelvis genom loggning av alla transaktioner samt uppföljning av denna, och
3. bestämmelser om kännbara sanktioner vid överträdelse av begränsningarna.

Sekretess gäller gentemot tjänsteleverantören om

1. absolut sekretess gäller för uppgifterna i fråga,

2. tjänsteleverantören är en myndighet och det inte finns någon sekretessbestämmelse i offentlighets- och sekretesslagen som kan tillämpas för de aktuella uppgifterna hos den mottagande myndigheten, eller

3. uppgifterna är av sådan särskilt skyddsvärd karaktär att de är sekretessbelagda även gentemot tjänsteleverantören, trots att denne är bunden av en avtalsreglerad tystnadsplikt.

Om det finns en tillämplig *sekretessbrytande bestämmelse*, kan annars sekretessbelagda uppgifter lämnas ut utan att det utgör ett otillåtet röjande, även om tjänsteleverantören måste ta del av uppgifterna för att kunna utföra sitt uppdrag eller det i vart fall inte kan anses osannolikt att så sker.

4. Allmänna handlingar

Genom åtgärden att göra myndighetens informationssamling tillgänglig för en utomstående tjänsteleverantör kan arbetsmaterial komma att bli upprättade, allmänna handlingar hos myndigheten. Detta gäller dock inte om tjänsteleverantörens uppdrag endast är att tekniskt bearbeta eller tekniskt lagra informationen för myndighetens räkning.

4.1 Inledning

Hos alla svenska myndigheter finns allmänna handlingar, dvs. handlingar som *förvaras* hos myndigheten och är att anse som *inkomna* till eller *upprättade* hos myndigheten. Sekretessbestämmelserna i offentlighets- och sekretesslagen gäller emellertid inte bara för uppgifter i allmänna handlingar, utan även för uppgifter som finns hos en myndighet i sådana handlingar som ännu inte blivit allmänna. För uppgifter som finns i handlingar som inte är allmänna är handlingssekretessen och tystnadsplikten dessutom inte tidsbegränsad. Röjandeförbudet gäller således också för sekretessbelagda uppgifter i exempelvis utkast och andra dokument som varken har expedierats eller på annat sätt kommit att bli upprättade i tryckfrihetsförordningens mening. Myndighetens sekretessöverväganden inför en planerad outsourcing måste därför även omfatta uppgifter i handlingar som inte är allmänna och som ska överlämnas till tjänsteleverantören.

Även om sekretess inte hindrar en planerad outsourcing, kan åtgärden att göra delar av myndighetens informationssamling tillgänglig för en utomstående tjänsteleverantör leda till att handlingars status förändras. Att göra en elektronisk handling tekniskt tillgänglig för någon annan utgör nämligen normalt en expediering som medför att handlingen anses upprättad och därmed allmän. Om tjänsteleverantören är en myndighet blir handlingen dessutom inkommen dit och därmed allmän även hos denna, fastän handlingen inte är färdigställd och kanske aldrig kommer att bli det.

4.2 Teknisk bearbetning/lagring

Om den mottagande myndighetens uppdrag endast är att tekniskt bearbeta eller tekniskt lagra handlingen för avsändarmyndighetens räkning, anses handlingen inte som en allmän handling där. Det framgår av en uttrycklig undantagsbestämmelse i tryckfrihetsförordningen, 2 kap. 10 § TF. Av en annan undantagsbestämmelse, 2 kap. 6 § 3 st. TF, framgår att en handling som återkommer till en myndighet efter teknisk bearbetning eller lagring inte anses som en inkommen handling. Rimligen bör det ursprungliga exemplaret då inte heller anses vara expedierat från, och därmed en upprättad allmän handling hos, den avsändande myndigheten. En annan tolkning skulle leda till att undantaget i 2 kap. 6 § 3 st. TF helt skulle förlora sin funktion, i vart fall då fråga är om enbart teknisk lagring utanför myndigheten.

En handling som inte är allmän hos den avsändande myndigheten blir således enligt eSams bedömning inte att betrakta som allmän bara för att den överlämnas till en tjänsteleverantör för teknisk bearbetning eller teknisk lagring. Detta bör rimligen gälla oavsett om tjänsteleverantören är en myndighet eller en privaträttslig aktör.

Om tjänsteleverantören även vidtar andra åtgärder än teknisk bearbetning eller lagring, är dock undantaget i 2 kap. 6 § 3 st. TF inte tillämpligt. I sådana situationer torde handlingen också anses expedierad och därmed upprättad i samma stund som den görs tekniskt tillgänglig för tjänsteleverantören. I och med det blir handlingar som tidigare inte varit allmänna hos myndigheten att betrakta som allmänna handlingar som omfattas av tryckfrihetsförordningens bestämmelser om handlingsoffentlighet.

Som exempel på teknisk bearbetning anges i de något ålderstigna förarbetena bl.a. tryckning, kopiering, redigering av ljudupptagningar och överföring av sådana upptagningar till grammofonskiva (prop. 1975/76:160 s. 171 som hänvisar till s. 137). Som exempel på teknisk lagring nämns sådana former av lagring som kräver tekniska anordningar, t.ex. lagring av information i skivminne eller på magnetband.

Exakt vilka åtgärder som utgör enbart teknisk bearbetning eller teknisk lagring i dagens elektroniska verklighet är i någon mån osäkert. Av praxis står det dock klart att åtgärder som mottagaren utför *för egen räkning* och som innebär en bearbetning av handlingarnas faktiska innehåll, t.ex. genom att uppgifter används för framställning av statistik eller arbetsmiljörapporter, inte omfattas av undantaget (jfr HFD 2011 ref. 52). Åtgärder som helt eller till övervägande del utförs elektroniskt och automatiserat för uppdragsmyndighets räkning, såsom exempelvis ren it-drift och skanning av dokument, bör dock enligt eSams bedömning i normalfallet omfattas av undantaget för teknisk bearbetning och teknisk lagring. I sammanhanget kan nämnas att Kammarrätten i Stockholm i en dom den 26 oktober 2015 (mål nr. 7369-15) har funnit att handlingar i eget utrymme inte är att anse som allmänna och att det därvid ligger i sakens natur att vissa anställda har åtkomst till berörd databas för att administrera den. För ett utförligt resonemang kring undantaget för teknisk bearbetning och teknisk lagring hänvisas till E-delegationens betänkande Så enkelt som möjligt för så många som möjligt, SOU 2014:39 s. 44 ff.

5. Skydd av personuppgifter

Myndigheten är personuppgiftsansvarig för den behandling av personuppgifter som tjänsteleverantören utför för myndighetens räkning. Tjänsteleverantören utgör då personuppgiftsbiträde åt myndigheten. Det ska finnas ett skriftligt personuppgiftsbiträdesavtal mellan parterna och tydliga instruktioner från myndigheten om varför och hur biträdet får behandla personuppgifterna.

5.1 Inledning

Vid all outsourcing som innebär att personuppgifter överlämnas till tjänsteleverantören måste regelverket rörande persondataskydd beaktas, dvs. personuppgiftslagen och tillämpliga registerförfattningar. Vid sådan outsourcing som är av särskilt intresse för e-förvaltningen, kan det antas att det mer eller mindre regelmässigt är så att tjänsteleverantören ska utföra vissa behandlingar av personuppgifter. Det gäller även om uppdraget bara avser teknisk lagring, eftersom även lagring av personuppgifter är en åtgärd som enligt 3 § PuL utgör behandling i personuppgiftslagens mening.

5.2 Personuppgiftsansvar och personuppgiftsbiträde

Även om en viss arbetsuppgift som innebär behandling av personuppgifter utkontrakteras till en extern tjänsteleverantör är det myndigheten som bär *personuppgiftsansvaret* enligt personuppgiftslagen eller tillämplig registerförfattning. Tjänsteleverantören, som utför behandlingarna för myndighetens räkning, är *personuppgiftsbiträde* åt myndigheten.

Enligt 30 § PuL ska det finnas ett skriftligt avtal om personuppgiftsbiträdets behandling av personuppgifter för den ansvariges räkning. I det avtalet ska det anges att biträdet får behandla personuppgifterna bara i enlighet med instruktioner från den ansvarige och att biträdet är skyldigt att vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas.

Tjänsteleverantören har i egenskap av personuppgiftsbiträde bara ett avtalsrättsligt ansvar gentemot myndigheten. Ansvaret enligt personuppgiftslagen gentemot den registrerade, dvs. den person som en viss personuppgift är hänförlig till, liksom ansvaret gentemot Datainspektionen, ligger alltså ändå på myndigheten. Om de säkerhetsåtgärder som biträdet vidtar visar sig vara otillräckliga, så att personuppgifter t.ex. sprids till obehöriga, är det därmed myndigheten som bär ansvaret gentemot den registrerade och kan bli skyldig att betala skadestånd till denne.

För att myndigheten ska kunna ta sitt personuppgiftsansvar även för de behandlingar som utförs av tjänsteleverantören är det viktigt att myndigheten ger tjänsteleverantören instruktioner om varför och hur personuppgifter får behandlas. Instruktionerna ska de vara så tydliga att otillåten behandling inte kommer att utföras. Sådana instruktioner kan exempelvis gälla ändamålen med behandlingen, tredjelandsöverföring och utlämnande till tredje man.

Det är också viktigt att myndigheten försäkrar sig om att tjänsteleverantören har förmåga att vidta lämpliga säkerhetsåtgärder och att detta verkligen sker.

5.2.1 Underentreprenörer

Myndighetens personuppgiftsansvar omfattar även de behandlingar som en underleverantör till tjänsteleverantören utför för myndighetens räkning. Även underentreprenören utgör i en sådan situation personuppgiftsbiträde åt myndigheten.

En grundläggande förutsättning för att den myndigheten ska kunna uppfylla sitt personuppgiftsansvar är att myndigheten har kännedom om vilka personuppgiftsbiträden som behandlar personuppgifter för dennes räkning. Myndigheten bör därför se till att avtalet inte ger tjänsteleverantören rätt att anlita sådana underentreprenörer utan myndighetens godkännande. Ger myndigheten ändå tjänsteleverantören ett sådant mandat måste det framgå i avtalet att varje underbiträde har samma skyldigheter som huvudbiträdet.

5.2.2 Förhållandet mellan TF, OSL och PuL

Allmänhetens rätt att få tillgång till allmänna handlingar framgår av tryckfrihetsförordningen, en av Sveriges grundlagar. Denna rätt har företräde framför dataskyddsbestämmelserna i personuppgiftslagen och myndigheternas registerförfattningar. Detta innebär bl.a. att en myndighet alltid måste *pröva* en begäran om utlämnande av handling, även om handlingen finns hos myndigheten bara på grund av att myndigheten utgör personuppgiftsbiträde åt en annan myndighet. Den omständigheten att den biträdande myndigheten, enligt personuppgiftslagen, bara får behandla personuppgifter enligt den ansvariga myndighetens instruktioner har i den situationen ingen betydelse. Om den handling som begäran avser utgör en allmän handling hos den biträdande myndigheten, vilket är fallet om uppdraget inte enbart avser teknisk bearbetning eller teknisk lagring av handlingar, måste den biträdande myndigheten dessutom lämna ut handlingen till sökanden, i den mån den inte innehåller uppgifter för vilka sekretess gäller enligt offentlighets- och sekretesslagen.

Trots att delar av offentlighets- och sekretesslagen kan sägas ha samma syfte som personuppgiftslagen, nämligen att skydda den enskildes integritet, är regelverken inte alls likstämmiga eller utbytbara. Den myndighet som i samband med en utkontraktering gör personuppgifter tillgängliga för tjänsteleverantören måste därför beakta såväl sekretesslagstiftningen som dataskyddslagstiftningen och se till att åtgärden är förenlig med båda dessa regelverk. Dessutom måste myndigheten överväga vilka konsekvenser åtgärden får för handlingarnas status enligt tryckfrihetsförordningen.

Ett personuppgiftsbiträde utgör inte en tredje man i personuppgiftslagens mening, 3 § PuL. Överlämnandet av personuppgifter till en tjänsteleverantör, som för myndighetens räkning ska behandla uppgifterna, utgör därför inte ett utlämnande i dataskyddshänseende. I 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 som deltar i myndighetens verksamhet. Ett överlämnande av uppgifter till en tjänsteleverantör kan därför utgöra ett röjande enligt offentlighets- och sekretesslagen, även om tjänsteleverantören är personuppgiftsbiträde åt myndigheten. Röjandebegreppet enligt offentlighets- och sekretesslagen är i sin tur delvis skilt från vad som utgör ett utlämnande eller en expediering enligt tryckfrihetsförordningen, bl.a. på grund av att offentlighets- och sekretesslagen avser uppgifter, medan tryckfrihetsförordningen avser handlingar. Detta illustrerar de tre regelverkens olika utgångspunkter och tydliggör behovet av att myndigheten analyserar utkontrakteringens förenlighet med vart och ett av dem.

Checklista – persondataskydd

1. Ska tjänsteleverantören behandla personuppgifter?
2. Finns det ett personuppgiftsbiträdesavtal enligt 30 § PuL?
3. Finns det tydliga instruktioner för varför och hur biträdet får behandla personuppgifter?
4. Får tjänsteleverantören anlita underleverantörer för behandling av personuppgifter?
5. Är personuppgiftsbehandlingen förenlig även med andra regelverk, såsom TF, OSL och arkivlagen?

Bilaga 1

Checklista, sekretessöverväganden

Ska sekretessreglerade uppgifter göras tillgängliga för tjänsteleverantören?

1. Finns det någon sekretessbestämmelse i offentlighets- och sekretesslagen som avser de aktuella uppgifterna?

Ska tjänsteleverantören ”delta” i myndighetens verksamhet?

1. Ska tjänsteleverantören utföra en uppgift som annars skulle ha utförts av någon av myndighetens egna anställda?

2. Är tjänsteleverantören en fysisk person som på grund av uppdraget kan sägas delta i myndighetens verksamhet?

3. Kan tjänsteleverantörens anställda anses delta i myndighetens verksamhet på annan liknande grund än anställning eller uppdrag?

Kommer uppgifter att ”röjas”?

1. Måste tjänsteleverantören ta del av de tillgängliggjorda uppgifterna för att kunna utföra sitt uppdrag?

2. Innehåller avtalet tydliga krav på tekniska och/eller rättsliga begränsningar som hindrar tjänsteleverantören och dennes personal från att faktiskt ta del av eller vidarebefordra uppgifterna?

3. Hur sannolikt är det att tjänsteleverantören eller någon annan obehörig ändå faktiskt tar del av uppgifterna?

    a. Innehåller avtalet krav på kontroll av att begränsningarna efterlevs, exempelvis genom loggning av alla transaktioner samt uppföljning av denna?

    b. Innehåller avtalet kännbara sanktioner vid överträdelser av begränsningarna?

Gäller sekretess för de uppgifter som röjs för tjänsteleverantören?

1. Är sekretessbestämmelsens rekvisit uppfyllda?

    a. Gäller s.k. absolut sekretess?

    b. Är sekretessen reglerad med skaderekvisit?

i. Hur skyddsvärda är uppgifterna, typiskt sett?

ii. Har mottagaren rätt att lämna uppgifterna vidare eller själv utnyttja dem?

iii. Om uppgifterna är av särskilt skyddsvärt slag, är den befogenhetsinskränkning som gäller för mottagaren straffsanktionerad?

Kan röjandet ske med stöd av någon sekretessbrytande bestämmelse?

1. Om tjänsteleverantören är en myndighet, är utlämnandet en följd av en lag- eller förordningsreglerad uppgiftsskyldighet eller kan utlämnandet ske med stöd av den s.k. generalklausulen eller någon sektorsspecifik sekretessbrytande bestämmelse?

2. Oavsett om tjänsteleverantören är en myndighet eller en privaträttslig aktör, kan utlämnandet anses vara ”nödvändigt”?

    a. Kan myndighetens uppdrag rimligen fullgöras utan att utlämnande sker?

    b. Motiveras utlämnandet även av andra skäl än rent ekonomiska?

    c. Har alla alternativ till utlämnande övervägts noggrant?

3. Kan utlämnandet anses vara lämpligt, särskilt med tanke på hur de intressen som sekretessen avser att skydda tillgodoses av mottagaren?

Bilaga 2

Sekretessförbindelse avseende [Tjänsteleverantörens] anställda och uppdragstagare

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

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

Med "Konfidentiell information" avses dels varje uppgift som hos [Myndigheten] är sekretessreglerad enligt offentlighets- och sekretesslagen (2009:400), dels varje annan upplysning. oavsett om informationen lämnats skriftligen eller muntligen och oberoende av format, som jag erhåller, från [Myndigheten] eller någon anställd, annan befattningshavare eller rådgivare till [Myndigheten], i samband med mitt arbete med [Myndigheten]. Som Konfidentiell information anses inte information som,

a) vid tiden för förfogandet var allmänt känd, eller

b) jag kan visa redan var tillgänglig för mig vid tiden för förfogandet och som jag inte, direkt eller indirekt, har erhållits genom överträdelse av denna sekretessförbindelse.

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

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

Jag förbinder mig även att tillse att till mig anförtrott material inte kommer obehörig till del. Med obehörig avses alla (således även familjemedlem), som inte bedöms behöva information inom ramen för [Tjänsteleverantörens] uppdrag gentemot [Myndigheten].

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

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

skyldighet, samt skadeståndsskyldighet för [Tjänsteleverantören] och för [Myndigheten].