Avtal om dataskydd och sekretess till skydd för enskildas personliga förhållanden

*Gustaf Johnssén**

1. Inledning

Statliga myndigheter, kommuner och regioner anlitar i betydande omfattning externa leverantörer för IT-tjänster och behandling av uppgifter.[1] Ramavtal finns och har funnits för många sådana tjänster. De rättsliga förutsättningarna för offentliga myndigheters outsourcing av olika IT-tjänster har under de senaste åren varit föremål för särskild uppmärksamhet. Diskussionen har rört både sekretess och dataskydd. När det gäller dataskydd har den diskussion som rör myndigheternas outsourcing varit en del av en mer allmän diskussion rörande tredjelandsöverföringar, som rör hela samhället. Sekretessfrågorna är däremot specifika för den offentliga sektorns outsourcing. Syftet med detta bidrag är att peka på några skillnader och likheter mellan bestämmelserna om dataskydd och bestämmelser om sekretess för enskilds personliga förhållanden, särskilt när det gäller förutsättningarna för att genom avtal säkerställa att uppgifterna får det skydd som lagen kräver. Jag menar att dataskyddsområdet har en större mognad när det gäller avtal som verktyg för att skydda uppgifter. Myndigheterna skulle därför kunna hämta inspiration från dataskyddsområdet när det gäller avtal om hantering av sekretessuppgifter. Jag har inga anspråk på att här göra någon djupare genomlysning, utan vill framför allt peka på några frågor som skulle kunna bli föremål för en djupare analys och vara en del av ett utvecklat sätt att arbeta med reglering av sekretess i outsourcingsituationer.[2]

* Gustaf Johnssén är verksam vid advokatbyrån Wikström & Partners. Han har tidigare arbetat med dataskydd och andra IT-rättsliga frågor i olika roller i myndigheter och regeringskansli.

[1] I viss lagstiftning kallas detta för utkontraktering. Jag har valt att i huvudsak använda den mer vedertagna termen outsourcing. Ingen skillnad i sak är avsedd. Termen myndigheter avser genomgående statliga och kommunala myndigheter.

[2] De tankar och idéer som framförs i detta kapitel har vuxit fram i diskussioner genom åren med kollegor, oftast klokare än jag själv. Jag vill särskilt nämna advokaten Christina Wik-

2. Dataskydd och sekretess vid outsourcing

Den enskildes integritet och privatlivets helgd skyddas i flera internationella överenskommelser.[3] Skyddet säkerställs genom nationell lagstiftning och unionslagstiftning på olika områden. Jag fokuserar här dels på Dataskyddsförordningen, GDPR[4], dels på de bestämmelser om sekretess till skydd för enskildas personliga förhållanden som finns i avd. V i offentlighets- och sekretesslagen (2009:400), OSL. Ytterst syftar båda dessa regleringar till att skydda den enskildes integritet. Båda regleringarna handlar om att undvika att skyddsvärda uppgifter kommer i fel händer eller används på ett felaktigt sätt. De utmynnar ofta i delvis samma åtgärder för att skydda uppgifterna, t.ex. olika informationssäkerhetsåtgärder. De innebär också båda att särskilda överväganden behöver göras såväl när organisation och arbetssätt utformas inom en myndighet som i samband med att en myndighet outsourcar behandling av uppgifter till en kommersiell leverantör.[5] Utöver likheterna finns skillnader mellan de båda regelverken som gör att det kan vara intressant att jämföra hur de tillämpas i samband med outsourcing.

Båda regelverkens implementering i praktiken innebär att ett antal tekniska och organisatoriska åtgärder behöver vidtas för att säkerställa att uppgifterna får ett tillräckligt och ändamålsenligt skydd. De båda regelverken innebär att särskilda överväganden behöver göras i samband med att uppgifter lämnas till en annan organisation. Organisationens gränser är avgörande för bestämmelserna, och de åtgärder som vidtas i samband med att uppgifter korsar sådana gränser är avgörande för om behandlingen är tillåten. När en extern leverantör anlitas för behandling av uppgifter behöver avtalet mellan myndigheten och leverantören innehålla bestämmelser som säkerställer att uppgifterna hos leverantören får ett sådant skydd som krävs med hänsyn till både dataskydd och sekretess. Sådana krav kan vara organisatoriska, tekniska och

---

ström, Wikström & Partners och enhetschefen Mikael Vall, Statens servicecenter. Den sistnämnde utvecklar tillsammans med mig delvis samma teman som i föreliggande bidrag i avsnittet ”Förutsättningar för att utkontraktera it-verksamhet” i Cecilia Magnusson Sjöberg (red.): *Rättsinformatik – Juridiken i det digitala informationssamhället* (4 uppl. Lund 2021), s. 516–538.

[3] Art. 7 och 8 Europeiska unionens stadga om de grundläggande rättigheterna (2010/C 83/02), art. 8 Europeiska konventionen om skydd för de mänskliga rättigheterna.

[4] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

[5] Även när en myndighet anlitar en annan myndighet för informationsbehandling uppkommer många intressanta rättsfrågor och rättsliga komplikationer. Jag uppehåller mig här helt vid outsourcing till privaträttsliga subjekt, när relationen mellan kund (myndighet) och leverantör styrs av civilrättsliga avtal.

rättsliga. Det kan t.ex. vara fråga om krav på åtkomstbegränsningar, krav på skydd mot intrång, krav på viss kompentens hos personalen, eller krav på att personalen ska ha tecknat sekretessförbindelser. De åtgärder som vidtas för att säkerställa att man uppfyller rättsliga krav kan också ha sitt ursprung i och stödja mer allmänna säkerhets- och verksamhetsöverväganden, t.ex. krav på att information ska vara tillgänglig och inte kunna förvanskas.

Den generella frågan vid outsourcing av behandling av sekretessuppgifter gäller om det är tillåtet att lämna ut uppgifterna till leverantören eller om detta hindras av sekretess. Sekretess innebär att uppgifter inte obehörigen får röjas. Ett röjande kan ske genom att en uppgift delges någon som inte är en del av myndigheten. I vissa fall kan också sekretess gälla mellan självständiga verksamhetsgrenar i en myndighet.[6] Den som är en del av myndigheten är i första hand den som genom ett anställningsavtal är knuten till myndigheten. Utöver anställda kan även andra uppdragstagare vara inordnade i myndighetens organisation på ett sådant sätt att uppgifter inte röjs när uppdragstagaren tar del av dem. Både anställda och andra uppdragstagare inordnas i myndigheten genom avtal (anställnings- eller uppdragsavtal). En leverantör knyts också till myndigheten genom avtal. En leverantör och dess anställda har normalt en sådan självständig ställning i förhållande till myndigheten att de inte kan anses inordnade i myndigheten på ett sådant sätt att sekretessreglerna inte ska tillämpas. I en situation när uppgifter lämnas till en leverantör behöver därför myndigheten säkerställa att de inte är sekretessbelagda i förhållande till leverantören.

Om uppgifter i den aktuella informationsmängden är sekretessreglerade kan det vara tillåtet att lämna ut uppgifterna på olika alternativa grunder.[7] Huvudalternativet är att uppgifterna görs tillgängliga för leverantören efter att myndigheten vid en sekretessprövning funnit att uppgifterna inte är sekretessbelagda i förhållande till leverantören. De flesta sekretessbestämmelser innehåller ett skaderekvisit. Om detta skaderekvisit är uppfyllt gäller sekretess. Om skaderekvisitet inte är uppfyllt gäller inte sekretess. Sekretessbestämmelserna är utformade och i första hand tänkta att tillämpas i situationer där någon efterfrågar en handling eller uppgifter hos en myndighet. En sekretessprövning görs då i det enskilda fallet. På motsvarande sätt görs vid en outsourcingsituation en generell sekretessprövning av de aktuella uppgifterna. Om myndigheten finner att de säkerhetsåtgärder som enligt avtal ska

[6] 8 kap. 2 § OSL.

[7] En god beskrivning av de allmänna överväganden som behöver göras vid outsourcing av sekretessuppgifter finns i E-sams vägledning Utkontraktering – sekretess och dataskydd ES2023-06.

vidtas för att skydda uppgifterna är tillräckliga för att skaderekvisiten inte ska vara uppfyllda, får uppgifterna lämnas ut till leverantören. Detta har förmodligen varit det vanligaste i samband med outsourcing av myndigheters IT-drift och informationshantering.

Det kan också vara tillåtet att lämna ut sekretessreglerade uppgifter till en leverantör om tjänsten är utformad så att uppgifterna över huvud taget inte röjs för leverantören. Just detta alternativ har varit föremål för särskild uppmärksamhet under de senaste åren. Mer om det nedan.

Slutligen kan det vara tillåtet att lämna ut uppgifter till en leverantör även om de omfattas av sekretess, om det finns en sekretessbrytande bestämmelse som innebär att uppgifterna får lämnas ut.

I GDPR finns bestämmelser som behöver beaktas om uppgifter lämnas från en organisation till en annan. Om en personuppgiftsansvarig anlitar en annan organisation för att behandla uppgifter är den senare organisationen ett personuppgiftsbiträde. GDPR innehåller då regler om krav på ett sådant biträde och på det personuppgiftsbiträdesavtal som ska upprättas mellan den personuppgiftsansvarige och biträdet. Liknande bestämmelser fanns tidigare i personuppgiftslagen. Gällande dataskyddsregleringen uppkommer därför normalt inte samma principiella fråga om det över huvud taget är tillåtet att lämna ut uppgifter till externa leverantörer. Däremot ställer lagstiftningen krav på åtgärder som den personuppgiftsansvarige behöver vidta när en leverantör anlitas samt på att den externa leverantören kan säkerställa att uppgifterna får ett tillräckligt skydd och i övrigt hanteras på ett korrekt sätt. I annat fall får leverantören inte anlitas.[8]

När det gäller användningen av externa leverantörer för behandling av uppgifter finns det alltså likheter mellan de två regelkomplexen när det gäller vilka typer av krav som behöver ställas. Däremot finns en avgörande skillnad i det att dataskyddsbestämmelserna förutsätter och tar höjd för att en personuppgiftsansvarig ska kunna anlita en extern leverantör. Det finns ju t.o.m. ett särskilt rättsinstitut för detta i form av personuppgiftsbiträdet. Sekretessbestämmelserna, däremot, är inte utformade med en outsourcingsituation för ögonen. Några lagstiftningsåtgärder, som diskuteras närmare nedan, har på senare år genomförts för att underlätta outsourcing. Behovet av dessa ändringar understryker att reglerna i grunden inte är utformade med outsourcing för ögonen. Sekretessrelaterade överväganden vid outsourcing är också styvmoderligt behandlade i både litteratur och praxis. I stort sett varje handbok om dataskydd innehåller ett avsnitt om personuppgiftsbiträden och biträdesavtal. På sekretessområdet är inte överväganden vid

[8] Art. 28.1 GDPR.

outsourcing alls lika närvarande, och i allmänna handböcker omnämns det ofta inte alls.[9] Detta trots att det inte är något ovanligt att myndigheter outsourcar behandling av sekretessuppgifter.

3. Sekretess vid outsourcing sedan 2014

Justitieombudsmannen (JO) meddelade den 9 september 2014 beslut i ett ärende rörande hantering av sekretessreglerade uppgifter när myndigheter outsourcar informationsbehandling.[10] Detta beslut kom att ha stor påverkan på synen på myndigheters outsourcing.

Några landsting hade anlitat en extern leverantör av läkarsekreterare. Sekreterarnas uppgift var att föra in journalanteckningar från inspelade diktat. JO fann att de känsliga uppgifter som hanterades inte var tillräckligt skyddade och att hanteringen av sekretessreglerade uppgifter var otillåten. JO lyfte bl.a. fram att leverantörens anställda, till skillnad från landstingsanställda, inte omfattades av en lagstadgad och straffsanktionerad tystnadsplikt. Utfallet av den ovan nämnda sekretessprövningen blev då enligt JO att sekretess rådde mellan myndigheten och leverantören, varför uppgifterna inte fick lämnas ut. Även om omständigheterna i ärendet var speciella kom beslutet att få långtgående konsekvenser. Det ledde till en stor osäkerhet i både statlig och kommunal förvaltning om de rättsliga förutsättningarna för outsourcing av IT-tjänster. Beslutet gjorde många myndigheter osäkra på om och när outsourcing var tillåten. Många olika aktörer kom att ge sig in i diskussionen om tillåten outsourcing, och debatten kom att röra både tolkning av OSL och övergripande policyfrågor rörande myndigheters outsourcing, framtida former för statlig it-drift m.m. Både inom statlig och kommunal sektor gavs det ut vägledningar om hur sekretessbestämmelserna borde tolkas för att möjliggöra outsourcing.[11] Olika tolkningar debatterades och ifrågasattes.[12] I detta sammanhang räcker egentligen att konstatera att det rått stor osäkerhet hos myndigheter om förutsättningarna för att på ett tillåtet sätt anlita externa leverantörer för behandling av sekretessreg-

[9] Jag har, utan att i och för sig ha gjort en genomgång av all tillgänglig litteratur, inte hittat något exempel på att en allmän handbok om sekretess tar upp frågan om outsourcing.

[10] Beslut 2014-09-09, dnr 3032-2011, Allvarlig kritik mot vissa vårdgivare inom dels Västra Götalandsregionen, dels Stockholms läns landsting för att man har ingått avtal om journalföring med ett företag trots att detta inte varit förenligt med regelverket om sekretess inom hälso- och sjukvården.

[11] T.ex. E-sam, E-sam, Outsourcing 2.0 – En vägledning om sekretess och dataskydd (2019).

[12] Se t.ex. Rikard Karlsson och Atle Morseth Edvinsson: Molntjänster och staten – En diskussion om röjandebegreppet i offentlighets- och sekretesslagen, Förvaltningsrättslig tidskrift 2021, s 855–888, Per Furberg och Mikael Westberg: Måste myndigheter följa lagarna? Om utkontraktering och legalitet i digital miljö, JT 2020/21 s. 406–417, Cirio advokatbyrå AB: Molntjänster, offentlighet och sekretess i offentlig sektor (2020)

lerade uppgifter. Samtidigt är sådan utkontraktering mycket vanlig, och det har sedan decennier funnits statliga ramavtal för IT-tjänster som innefattar behandling av sekretessuppgifter, t.ex. personal- och löneadministrativa system.

Mycket av diskussionen kom att handla om huruvida uppgifterna röjs när de lämnas ut till leverantören. Man kan få intrycket att i vart fall vissa myndigheter eller debattörer har uppfattningen att all outsourcing som innebär att uppgifter röjs skulle vara otillåten. Däremot kom frågan om vilka krav som bör ställas för att ett utlämnande ska vara tillåtet efter sekretessprövning att få mindre utrymme. Det som enligt JO-avgörandet är huvudfallet kom alltså i praktiken att framstå som en avvikelse.[13] Detta kan enligt min mening ha bidragit till att frågan om hur man genom avtal säkerställer skydd för sekretessuppgifter inte har fått den uppmärksamhet den kunde ha förtjänat.

Flera förslag på författningsändringar lades fram för att undanröja den osäkerhet som följde på JO-avgörandet och underlätta outsourcing av behandling av sekretessreglerade uppgifter även när uppgifterna är särskilt känsliga.[14] Dessa förslag grundande sig delvis på olika tolkningar av rättsläget. År 2020 infördes en särskild lag om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter.[15] Enligt denna lag har den som på grund av anställning eller på något annat sätt deltar i eller har deltagit i en tjänsteleverantörs verksamhet på uppdrag av en myndighet tystnadsplikt för de uppgifter som personen tagit del av. Denna tystnadsplikt gäller enbart när tjänsterna avser teknisk bearbetning eller teknisk lagring av uppgifter. För tjänster som går utöver teknisk bearbetning och teknisk lagring gäller ingen tystnadsplikt enligt lagen.

För att ytterligare tydliggöra förutsättningarna för outsourcing infördes 2023 en sekretessbrytande regel i 10 kap. 2 a § OSL som föreskriver att uppgifter utan hinder av sekretess får lämnas ut till en leverantör för teknisk bearbetning och teknisk lagring.[16] Detta innebär att de uppgifter som enligt 2020 års lag omfattas av tystnadsplikt får lämnas

[13] En bra redogörelse för olika tolkningar finns på s. 231–267 i SOU 2021:1 Säker och kostnadseffektiv it-drift – rättsliga förutsättningar för utkontraktering. Utredningen redogör för olika uppfattningar om röjandebegreppet och förordar en viss tolkning, som inte är okontroversiell. Utredningens överväganden och förslag förutsätter såvitt jag förstår saken att outsourcing i normalfallet bygger på att uppgifter lämnas ut efter sekretessprövning, dvs. att de röjs på ett tillåtet sätt.

[14] SOU 2018:25 Juridik som stöd för förvaltningens digitalisering, SOU 2015:66 En förvaltning som håller ihop, SOU 2021:1 Säker och kostnadseffektiv it-drift.

[15] Lag (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter, proposition 2019/20:201 Tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter.

[16] Prop. 2022/23:97 Sekretessgenombrott vid utlämnande för teknisk bearbetning eller teknisk lagring av uppgifter.

ut till en leverantör utan föregående sekretessprövning. Detta förutsatt att det inte är olämpligt att uppgifterna lämnas ut. Om outsourcingen omfattar tjänster som går utöver teknisk bearbetning och teknisk lagring, t.ex. användarsupport, gäller att uppgifterna kan lämnas ut efter en sekretessprövning. Vid denna sekretessprövning blir tystnadsplikten en faktor som ska vägas in vid skadeprövningen.

Diskussionen om förutsättningarna för myndigheters outsourcing har också påverkats av den generella uppmärksamhet som varit på frågor om tredjelandsöverföringar av personuppgifter och EU-domstolens domar rörande den frågan. Enligt GDPR gäller samma regler för myndigheter som för andra personuppgiftsansvariga. Frågan om utländska myndigheters tillgång till personuppgifter som behandlas hos leverantörer har dock en särskild dimension när det gäller sekretess. Utöver frågan om den registrerades ställning har det diskuterats om utländska myndigheters möjlighet att bereda sig tillgång till uppgifter innebär att uppgifterna är röjda i OSL:s mening.[17]

4. Avtalad och lagstadgad sekretess

En avgörande fråga i diskussionen om sekretess vid utkontraktering gäller skillnaden mellan avtalad och lagstadgad tystnadsplikt eller sekretess. I JO-avgörandet är frågan om lagstadgad och straffsanktionerad tystnadsplikt central för slutsatserna. Enligt JO är det normalt tillräckligt att avtala om tystnadsplikt med en leverantör för att det ska vara tillåtet att outsourca behandling av sekretessreglerade uppgifter. JO stödjer sig här på uttalanden i förarbetena till sekretesslagen.[18] Avsaknaden av en lagstadgad och straffsanktionerad tystnadsplikt för leverantörens anställda var enligt JO huvudskälet till att den aktuella outsourcingen inte var tillåten. Skälet till att en avtalad tystnadsplikt inte var tillräcklig var att uppgifterna i detta fall ansågs särskilt skyddsvärda.

Häri finns också en avgörande skillnad mellan regelverken för sekretess och dataskydd. Röjande av en sekretessbelagd uppgift är straffbart enligt 20 kap. 3 § brottsbalken. Någon liknande bestämmelse finns inte för personuppgifter. Med hänsyn till den vikt som frågan om en lagstadgad och straffsanktionerad tystnadsplikt har fått finns det skäl att närmare granska skillnaderna mellan en lagstadgad och en avtalad tystnadsplikt.

Leverantören är personuppgiftsbiträde och omfattas som sådant av olika både avtalade och lagstadgade förpliktelser, bl.a. att inte behandla

[17] Se källor i not 9.
[18] Prop. 1979/80:2 med förslag till sekretesslag m.m. Del A s. 128.

uppgifterna i strid med instruktioner eller för egna ändamål. Någon lagstadgad tystnadsplikt följde dock inte av personuppgiftslagen. Någon sådan tystnadsplikt föreskrivs inte heller i GDPR. I sammanhanget kan dock noteras att datalagen innehöll i 13 § en bestämmelse om tystnadsplikt för envar som tagit befattning med personregister. Skulle behandlingen ha omfattats av den lagen skulle en lagstadgad tystnadsplikt ha funnits.

På arbetsmarknaden är det brukligt att en anställd ingår någon form av förbindelse med arbetsgivaren om tystnadsplikt. En sådan förbindelse blir en del av avtalet mellan arbetsgivaren och arbetstagaren. Arbetstagaren är även i övrigt skyldig att följa de säkerhetsbestämmelser och andra anvisningar som ges. Det är genom sådana anvisningar som arbetsgivaren säkerställer att uppgifter skyddas. Det gäller både sekretessuppgifter och personuppgifter. I det senare avseendet är de styrande åtgärderna en del av de organisatoriska åtgärder som en personuppgiftsansvarig eller ett personuppgiftsbiträde ska vidta.

För en offentliganställd gäller att tystnadsplikt inte kan åläggas genom avtal.[19] Så har dock inte alltid varit fallet. Genom sekretesslagens tillkomst 1980 samordnades regleringen av tystnadsplikt och regleringen av handlingssekretess. Innan dess var framför allt regleringen av tystnadsplikt mer spretig. Reglering förekom på flera olika författningsnivåer. Vidare kunde arbetsgivaren ålägga medarbetarna tystnadsplikt. Förhållandena kan sägas likna de som än idag gäller för den om är anställd i ett privat företag. Även om inte tystnadsplikt för offentliganställda kan åläggas genom avtal har anställningsavtalet och de arbetsrättsliga förutsättningarna betydelse för skyddet av uppgifter som omfattas av sekretess (och andra uppgifter). Arbetsgivaren ska vidta de säkerhetsåtgärder som behövs för att skydda uppgifter. I detta ingår t.ex. bestämmelser på arbetsplatsen om förutsättningar för att ta del av uppgifter som finns i system och handlingar, samt för hur sådana uppgifter får användas.

Ett leveransavtal för IT-tjänster innehåller typiskt sett bestämmelser om att anställda hos leverantören ska ingå sekretessförbindelser med sin arbetsgivare. På det sättet binds den civilrättsliga regleringen ihop med den offentligrättsliga hela vägen från myndighet till enskild anställd hos leverantören.

Det kan framstå som självklart att en avtalad sekretess ger ett sämre skydd för uppgifter än en lagstadgad tystnadsplikt. En avtalad sekretess kan dock på många sätt ge ett mer förutsebart, heltäckande och långtgående skydd för uppgifter än en lagstadgad sekretess, även om

[19] Prop. 1979/80:2 med förslag till sekretesslag m.m. Del A s 52 och s 336–339.

den senare är straffsanktionerad. Den avhållande verkan som en straffsanktion har saknas förstås vid avtalad sekretess. Det kan i och för sig diskuteras vilken praktisk betydelse detta har för skyddet av uppgifterna. För en anställd kan risken att åtalas och fällas för ett brott mot sekretess antagligen framstå som abstrakt och möjligen osannolik. Risken att förlora anställningen på grund av ett brott mot anställningsavtalet kan säkert framstå som en i vart fall nästan lika kännbar risk. I de fall behandlingen utförs av personer utanför Sverige är betydelsen av straffsanktionen förmodligen mycket begränsad.

Sekretessbestämmelserna i OSL är generella till sin karaktär. Ett avtal måste förstås tolkas, men det innehåller typiskt sett mer detaljerade bestämmelser om hur en tjänst kan utformas och parterna har möjlighet att utforma mer detaljerade bestämmelser om sekretessens föremål, räckvidd och styrka. En avtalad sekretess med en leverantör är inte heller bunden av OSL:s begränsningar. Parterna kan avtala om vilket skydd uppgifterna ska ha och med vilka metoder de ska skyddas utan hinder av lagbestämmelser. En avtalad sekretess kan sålunda ge ett mer omfattande skydd än en lagstadgad sekretess. När det gäller styrka är en avtalad sekretess i praktiken normalt absolut. Ett avtal om sekretess kan (och bör) också innehålla bestämmelser om vilken information myndigheten ska lämna till leverantören om uppgifterna, processer för kommunikation mellan myndighet och leverantör, för uppföljning m.m. Avtalsbestämmelser krävs därför för att säkerställa sekretessen, men de kan också användas för att skapa ett förutsebart skydd för uppgifterna hos leverantören som är mer långtgående och tydligt än en lagstadgad sekretess är.

Även i de fall när det finns en straffsanktionerad tystnadsplikt hos leverantören behövs sekretessbestämmelser i avtal. Att enbart förlita sig på straffsanktionerad tystnadsplikt för leverantörens anställda och inte ställa andra krav skulle inte framstå som ett ansvarsfullt agerande av en myndighet. I realiteten skulle förmodligen ingen myndighet heller ens överväga detta.

5. Avtal om sekretess i praktiken

De avtalade kraven om skydd för de uppgifter som en myndighet gör tillgängliga för en leverantör är avgörande för förutsättningarna för att outsourcingen ska ske på ett rättsenligt sätt. Detta gäller oavsett på vilka grunder de sekretessreglerade uppgifterna lämnas ut. Om myndigheten lämnar ut uppgifterna efter en sekretessprövning, måste villkoren vara sådana att myndigheten kan förvissa sig om att uppgifterna

har ett sådant skydd att skaderekvisiten inte är uppfyllda. Om avtalskrav på organisatoriska och tekniska åtgärder är avsedda att säkerställa att uppgifterna över huvud taget inte är röjda för leverantören, måste det finnas villkor som på ett trovärdigt sätt säkerställer att så verkligen är fallet. Även om uppgifter lämnas ut med stöd av en sekretessbrytande bestämmelse måste de ha ett tillräckligt skydd hos leverantören, bl.a. för att det inte ska vara olämpligt att lämna ut uppgifterna. I praktiken behöver förmodligen de krav som ställs på leverantören när uppgifter lämnas ut med stöd av den nya sekretessbrytande bestämmelsen vara i stort sett desamma som behöver ställas på leverantören för att uppgifter ska kunna lämnas ut efter en sekretessprövning.

Som framgått ovan är de avtalskrav som ska säkerställa sekretess väsentliga för att det ska vara tillåtet att outsourca behandling av sekretessuppgifter. Det gäller dels i de fall myndigheten behövt göra en sekretessbedömning när uppgifterna lämnas till leverantören, dels när en olämplighetsbedömning ska göras enligt den nya sekretessbrytande bestämmelsen. Man kunde mot den bakgrunden möjligen vänta sig att myndigheters avtal skulle innehålla genomarbetade och detaljerade sekretessbestämmelser. Den som studerar exempelvis äldre statliga ramavtal finner att sekretess ofta är övergripande reglerad. Typiskt sett kan en avtalsbestämmelse innehålla ett åliggande att säkerställa att personal känner till sekretessbestämmelser och att anställda ska underteckna sekretessförbindelser. Ibland innehåller de också ett krav på att leverantören ska ha rutiner för att säkerställa att bestämmelserna följs. Denna typ av övergripande sekretessbestämmelser motsvarar hur sekretess traditionellt reglerats i IT-avtal i allmänhet.[20]

Det finns också avtalsmallar med mer utvecklade sekretessbestämmelser, t.ex. de som tagits fram inom ramen för myndighetssamverkansprogrammet e-sam. I de villkor som publicerades 2020 föreskrivs bl.a. att leverantörens anställda inte får ta del av sekretessreglerade uppgifter utan skriftligt medgivande. Syftet med denna bestämmelse är att uppgifterna som huvudregel inte ska anses röjda för leverantören. Dvs. att outsourcingen är tillåten på den grunden att uppgifterna inte röjs.[21]

Tidigare har avtal typiskt sett inte innehållit bestämmelser om att leverantören inte får ta del av uppgifter. Den outsourcing som har skett måste därför ha grundat sig på att uppgifter lämnats ut till leverantörer efter sekretessprövning. I praktiken har det förmodligen varit vanligt att myndigheter inte har gjort några djupare rättsliga överväganden eller analyser. Sekretessbestämmelserna är som nämnts utformade med helt

[20] Se t.ex. TechSverige IT-infrastrukturtjänster (2021), allmänna bestämmelser 16.1 och 16.2.
[21] E-sam. Allmänna villkor för it-drift (2023-02-24).

andra situationer för ögonen, och det är inte otänkbart att den myndighet som outsourcar IT-drift eller informationshantering inte ser outsourcingen som en situation som ens är relevant ur ett sekretessperspektiv. Det faktum att frågan fått så lite uppmärksamhet kan möjligen tyda på detta. De tolkningar som har gjorts under de senaste årens diskussion har därför enligt min mening i viss mån haft karaktären av efterhandskonstruktion. Med det avser jag att myndigheterna förmodligen historiskt inte alltid har gjort de detaljerade och kvalificerade analyser som gjorts på senare år. Detta innebär dock inte att jag menar att outsourcing tidigare skett på ett lättvindigt sätt eller med sämre säkerhet. Däremot tror jag att myndigheter i många fall inte har varit vana att utforma och ställa krav på sekretess vid outsourcing och inte minst att analysera tjänster ur ett sekretessperspektiv.

Även mer utvecklade sekretessbestämmelser i avtal kan dock innebära risker för att myndighetens uppgifter inte hanteras på ett tillräckligt säkert sätt. Exempelvis kan det uppstå en situation där myndigheten i praktiken överlåter åt leverantören att bedöma vilka sekretessbestämmelser som gäller i myndighetens verksamhet. Ett rimligt krav från en leverantör bör vara att myndigheten ska kunna redovisa vilka sekretessbestämmelser som enligt lag gäller för vilka uppgifter hos myndigheten, så att leverantören vet vilka uppgifter som är skyddsvärda och kan behöva omfattas av särskilda åtgärder. Vidare är det lämpligt att upprätta gemensamma rutiner för hur den avtalade tystnadsplikten ska upprätthållas, eller i vart fall att den outsourcande myndigheten ska veta vilka rutiner som leverantören tillämpar. Att rutiner finns och hur de följs bör också följas upp av myndigheten.

En god avtalsreglering av sekretess förutsätter att myndigheten analyserar inte bara vilken information som ska lämnas ut, utan också hur tjänsterna faktiskt produceras. En sådan analys behövs t.ex. för att förstå vilka begränsningar i tillgången till behandlade uppgifter som är möjliga att föreskriva. Sedan 2020 gäller dessutom att myndigheten tillsammans med leverantören behöver tydliggöra i vilka delar tjänsten avser teknisk bearbetning och teknisk lagring. En sådan analys är nödvändig för att avgöra om det råder tystnadsplikt, vilket i sin tur är ett underlag för myndighetens bedömning av om uppgifterna lämnas ut efter en sekretessbedömning eller med stöd av den sekretessbrytande bestämmelsen. Eftersom det är en viktig förutsättning för avtalet om det är fråga om teknisk bearbetning och teknisk lagring bör det framgå av avtalet i vilka delar tjänsten faller under detta begrepp. Även om det ytterst är en domstol som avgör, så bör parterna ha en tydlig gemensam uppfattning om vilken lagstiftning som gäller för tjänsten. Såvitt jag känner till innehåller avtal sällan några bestämmelser om eller någon

dokumentation av i vilka delar en tjänst faller under teknisk lagring eller teknisk bearbetning. I vilken mån sådana analyser förekommer skiljer sig säkert mellan olika myndigheter. Det kan dock konstateras att det inte finns några allmänt förekommande metoder för sådana analyser.

I en i år aktuell förstudie från Kammarkollegiet om upphandling av IT-drift ägnas utrymme åt säkerhetsfrågor och visst utrymme åt dataskyddsfrågor. Det sägs dock inget särskilt om överväganden med anledning av sekretess. När det gäller utvecklingsområden pekas säkerhet ut. Man pekar särskilt på rättsliga krav med anledning av GDPR.[22] En av myndighetens slutsatser är att kravställningen avseende informationssäkerhet bör utökas.[23] I resonemang och beskrivningar av den rättsliga bakgrunden bakom kraven nämns inte sekretess annat än i förbigående i anslutning till säkerhetsskydd. De nya reglerna i OSL som börjat gälla i år berörs inte alls. Det återstår att se hur avtalsvillkoren kommer att se ut och på vilket sätt de kommer att ta hänsyn till reglerna om tystnadsplikt vid utkontraktering och sekretessgenombrott, bl.a. när det gäller gränsdragningen mellan teknisk lagring och bearbetning och annan informationshantering.

Sammantaget kan konstateras att avtalsreglering av sekretess vid myndigheters outsourcing har utvecklats, men att det finns en potential för utveckling och förbättring. Det finns inte en tradition av utarbetade avtalskrav på sekretessområdet, inte heller av strukturerad uppföljning av sekretesskrav i avtal. Jag menar att sättet att ingå och förvalta avtal på dataskyddsområdet kan tjäna som förebild även på sekretessområdet.

6. Avtal om dataskydd som inspiration?

Dataskyddsreglering är, till skillnad från sekretessregleringen, en helhetsreglering av behandling av personuppgifter. I lagstiftningen i sig finns krav på att bestämmelserna ska beaktas vid utformning av system och arbetssätt. Detta skiljer reglerna från t.ex. sekretessbestämmelserna. I lagstiftningen finns också krav på att den ansvarige ska kunna visa att reglerna följs. I detta ligger ett ansvar för att dokumentera ställningstaganden. Detta krav på dokumenterade ställningstaganden gäller både när man organiserar behandlingen och i enskilda fall, t.ex. vid incidenter. Denna relativt omfattande administrativa reglering saknar motsvarighet i sekretessregleringen.

[22] Kammarkollegiet, Förstudierapport inom området IT-drift 2023-05-01 dnr 23.2-14663-2022, avsnitt 14.5 s. 37.
[23] Ibid. s. 38.

När det gäller förhållandet mellan sekretess och outsourcing är det otydligare vad som historiskt har gällt. Lagstiftningen ger inget tydligt stöd för outsourcing på det sätt som dataskyddsregleringen gör. Det finns ingen tydlig reglering av roller och ansvar. Det finns heller inga utvecklade och etablerade former för praktisk hantering, uppföljning etc. av sekretess på samma sätt som för personuppgiftshantering.

Till skillnad från vad som gäller på sekretessområdet är avtalet en integrerad och självklar del av regleringen av dataskydd. Dataskyddslagstiftningen förutsätter och bygger på att det är tillåtet och möjligt att överlåta behandlingar till någon annan. Det finns inget generellt hinder för att anlita ett biträde för behandlingar och lagstiftningen kan snarast sägas främja att så sker. Just förutsättningarna för att outsourca, hur man avtalar med och följer upp leverantörer har varit föremål för aktiv utveckling på marknaden. Både leverantörer, kunder och tillsynsmyndighet har bidragit till utvecklingen ur olika perspektiv. Utvecklingen av former för outsourcing har därmed varit mer strukturerad, ordnad och transparent. Det har heller aldrig rått något tvivel om att det är tillåtet att anlita externa leverantörer för att behandla personuppgifter. Det har också varit tydligt vad som förväntas av någon som anlitar ett biträde för hantering av personuppgifter. Dataskyddet har därför ett tydligt ramverk för outsourcing. Lagen tillhandahåller en terminologi och en begreppsapparat för att förstå och hantera de förfoganden som är aktuella vid en kommersiell outsourcingsituation.

JO noterar i det nämnda beslutet att myndigheterna i sina yttranden lade stor vikt vid avtalskrav rörande personuppgiftsbehandling men mindre uppmärksamhet vid själva sekretessfrågan. Mot bakgrund av att avtalande om personuppgifter är mer utvecklat i samhället är det enligt min mening inte särskilt förvånande.

På dataskyddsområdet finns vidare en mer utbredd användning av standarder och standardiserade förfaranden. Området har på senare år kommit att präglas av tänkande från compliance, ibland kallat regelefterlevnad. Detta sätter fokus mer på administrativa rutiner, styrdokument och liknande. Det innebär också ett större fokus på uppföljning av sådana rutiner. Samverkan med och kontroll av leverantörer är därför en naturlig del av arbetet med dataskydd på annat sätt än vad som gäller för en myndighets arbete med sekretess. Användning av standarder och formaliserad regelefterlevnad kan ha nackdelar i den offentliga förvaltningen. Men oavsett det står det klart att standardiserade och formaliserade metoder underlättar avtalskrav och uppföljning av sådana krav.

En annan skillnad som kan ha betydelse för skillnaderna i hanteringen av dataskydd och sekretess i avtal har att göra med lagstiftningens koppling till teknik och teknisk utveckling. Dataskyddsregleringen

har en tydlig historisk koppling till teknikutveckling. Skälet till att lagstiftningen kom var risken för enskildas integritet som den utvecklade datatekniken medförde.[24] Detta innebär att regleringen alltid har hängt ihop med och associerats med den konkreta tekniska behandlingen av uppgifterna. Sekretessregleringen har sitt ursprung i ämbetsmäns, läkares och prästers tystnadsplikt och myndigheternas hantering av pappershandlingar. Det har handlat om att skydda handlingarna hos myndigheten och informationen i tjänstemännens huvud. Sekretessreglerna är tänkta att tillämpas när någon begär ut en handling. Tekniska system har inte på samma sätt varit en självklar del av regleringens utveckling och utformning. Det är möjligt att den närmare anknytning mellan lagstiftning och teknik som finns på dataskyddsområdet inneburit att det varit mer närliggande att omsätta de rättsliga kraven i tekniska och organisatoriska krav i avtal. Det kan också ha underlättat den kommunikation mellan professioner som är nödvändig för att utforma goda avtalskrav på system och tjänster.

7. Framtida utveckling

Säkerhet i allmänhet och dataskydd i synnerhet har de senaste åren fått stor uppmärksamhet i samhället. Dataskyddsfrågor har fått en större uppmärksamhet i samhället sedan dataskyddsförordningens tillkomst. Detta har utan tvivel inneburit att även skyddet för sekretess uppmärksammats mer och förbättrats, inte minst i outsourcingsituationer. Detta är förstås positivt. Som framgått menar jag att användningen av avtalsreglering av sekretess behöver utvecklas. Min bild är att myndigheter generellt hanterar sin outsourcing på ett ansvarsfullt sätt. Men jag är också övertygad om att många myndigheter saknar både tid och resurser att göra alla de analyser och lägga den tid på avtalsförvaltning som skulle behövas. Jag tror bl.a. att myndigheterna behöver lägga mer möda på att analysera hur IT-tjänster faktiskt produceras. Detta är nödvändigt för att avgöra vilka regler som gäller (dvs. i vilka delar tjänsterna avser teknisk bearbetning och teknisk lagring) dels för att avgöra vilka krav som kan ställas, och för att avgöra hur kraven kan följas upp. Just de uppföljningarna är ett annat område som generellt skulle behöva utvecklas i förvaltningen.

Det kan också finnas anledning att överväga om förutsättningarna för outsourcing kan förtydligas och förbättras genom förändringar i lagstiftningen. En fråga som skulle kunna utredas är om rollfördelningen

[24] Se t.ex. gällande bakgrunden till datalagen, prop. 1973:33 Kungl. Maj:ts proposition med förslag till ändringar i tryckfrihetsförordningen m.m., s. 16–18, 40–52 och 89–96.

skulle kunna förtydligas på ett sätt som liknar förhållandet mellan personuppgiftsansvarig och personuppgiftsbiträde. En annan fråga är om det behövs en särskild avtalsform om sekretess på samma sätt som personuppgiftsbiträdesavtalet, eller för den delen säkerhetsskyddsavtalet.

I avvaktan på eventuella lagstiftningsinitiativ finns det dock goda möjligheter för både myndigheter och leverantörer att förbättra avtalsregleringen av behandling av sekretessuppgifter med inspiration från regleringen av personuppgiftsbehandling. Min ambition har varit att peka på några sådana möjligheter.