Tjänsteutlåtande
Utfärdat 2021-05-25
Diarienummer
0227/21

Handläggare: Ove Hellmers Eberhard, Jan Gustavsson, Per Gustavsson, Fredrik Andersson
Telefon: 070-3479009
E-post: ove.hellmers@intraservice.goteborg.se

Redogörelse för Intraservice arbetssätt och metod för utveckling av Kommungemensamma interna tjänster med stöd av molntjänstleverantörer

Förslag till beslut

I nämnden för Intraservice:

1. Informationen om hur förvaltningen arbetar med bedömning och utveckling av molntjänster antecknas.
2. Nämnden antecknar också att rättsläget är osäkert och att det i hög grad påverkar på vilket sätt som nya tjänster kan startas.
3. Nämnden önskar fortlöpande information om förändringar i rättsläget.

Sammanfattning

Europeisk och svensk lagstiftning styr på vilket sätt förvaltningen kan använda molntjänster i leveransen av Kommungemensamma interna tjänster. Att förhålla sig till är främst Dataskyddsförordningen och Offentlighets –och sekretesslagstiftningen. Användningen påverkas också av viss amerikansk lagstiftning. 2020-07-16 förändrades förutsättningarna då Schrems II-domen ogiltigförklarade den tidigare möjligheten att avtala om överföring av personuppgifter via Privacy Shield. Efter domen är rättsläget delvis oklart. Det gäller, främst överföring av personuppgifter till tredjeland, det vill säga, hur Kommungemensamma interna tjänster kan överföra personuppgifter för behandling utanför EU/EES.

Sammantaget påverkar detta hur Göteborgs Stad förvaltningar och bolag kan behandla personuppgifter som överförs i Kommungemensamma interna tjänster. I Dataskyddsförordningen regleras vem som har ansvaret för behandlingen genom rollerna Personuppgiftsansvarig och Personuppgiftsbiträde. Enligt styrdokumentet ”Göteborgs Stads riktlinjer för styrning av Kommungemensamma interna tjänster” är de nämnder och styrelser för de förvaltningar och bolag som använder Kommungemensamma interna tjänster personuppgiftsansvariga. Nämnden för Intraservice är personuppgiftsbiträde.

I Kommungemensamma interna tjänster använder Intraservice flera leverantörer. Tjänsterna levereras via Intraservice egen drift, via licensavtal med leverantörer, via olika typer av molntjänster samt i hybridlösningar mellan egen drift och molntjänster. Exempel på molntjänster från leverantörer är Microsoft som leverantör av Office 365 och Azure, via Google som leverantör av utbildningsområdets Google Workspace for Education. För de skoladministrativa tjänsterna är IST och Skola24 leverantörer. Med Kommungemensamma interna tjänster skapas förutsättningar för att medborgare, elever, vårdnadshavare och medarbetare i hög grad kan samarbeta, arbeta flexibelt, kommunicera digitalt och ha effektivt verksamhets- och kontorsstöd. Leveransen i molntjänsten kan liknas vid ett sammanhållet ekosystem med samverkande funktionalitet. I tjänsterna förekommer olika typer av data, innehållsdata, funktionsdata och diagnosdata. De olika typerna av data och dess innehåll påverkar på vilket sätt en personuppgift kan behandlas.

Molntjänster levereras i olika former, IaaS, PaaS, SaaS, On-Prem och som supporttjänst. I de olika formerna levereras olika delar av den funktionalitet som efterfrågas. Intraservice använder samtliga dessa former. Molntjänstleverantörer finns på olika geografiska platser och i olika länder. Bearbetning och lagring av olika typer av data i olika länder styr på vilket sätt data behöver skyddas, antingen via tekniska skyddsåtgärder eller via avtal. Kraven på de tekniska skyddsåtgärderna utgår ifrån interna och externa krav på hur informationstillgångarna ska skyddas. Kraven uttrycks i konfidentialitet, riktighet, tillgänglighet samt integritet. Olika åtgärder kan beskrivas utifrån administrativa, organisatoriska, tekniska, fysiska och juridiska skydd.

En omvärldsanalys av hur andra kommuner tillämpar och använder molntjänster visar en gemensam bild av ett arbetssätt som motsvarar förvaltningens sätt att hantera de juridiska frågeställningarna gällande molntjänster och överföring av personuppgifter. Analysen visar också att två myndigheter avstått från att införa funktionalitet levererad från Microsoft i Office365 och en region avvaktar ett införande. På uppdrag av förvaltningen har advokatfirman Lindahls gjort en bedömning av rättsläget. Två prövningar har genomförts i fransk domstol och fler prövningar väntas.

Intraservice använder tjänster för egen räkning men är framför allt leverantör till stadens förvaltningar och bolag. I förvaltningens arbetssätt finns en tydlighet i vem som ansvarar för analys av molntjänst inom Kommungemensam intern tjänst och vem som ansvarar för att säkerställa att det utförs en bedömning i respektive förvaltning och bolag.

Processen för att bedöma en tjänst består av flera olika steg och i en slutlig bedömning avgörs om det finns ett starkt verksamhetsintresse som överväger risken med överföringen av personuppgifter. Av sammanlagt 225 tjänster är bedömningen att 199 inte utgör någon risk utifrån Schrems II-domen. Utredning och bedömning av återstående 26 tjänster pågår. Intraservice har en kommunikationsplan med definierade intressenter. I utvecklingsinitiativ inom tjänsteplan använder förvaltningen samma arbetssätt och metod för att bedöma behandlingen av personuppgifter i förhållande till lagstiftning.

Molntjänster levereras ofta som sammanhållna ekosystem med funktioner som hjälper användaren att till exempel lagra information på endast ett ställe och göra det möjligt att återanvända information. Funktioner används integrerade och utnyttjar oberoende av varandra lagrad information. Det är svårt att hitta ersättning för den funktionalitet som ett ekosystem tillhandahåller och det är inte kostnadseffektivt. Leverantörer utvecklar inte solitära program, utvecklingen går mot ekosystem i molntjänster. Ökade licenskostnader,

högre supportkostnader, dålig kostnadseffektivitet och svårigheter att hitta kompetens är exempel på sådana konsekvenser att frångå ekosystem för leverans i Kommungemensamma interna tjänster.

Avveckling av en molntjänst är genomförbar men har stor påverkan på möjligheterna att utveckla och digitalisera inom Göteborgs Stads verksamheter.

Bedömning ekonomiska konsekvenser att ersätta en molntjänst

Användning av molntjänster möjliggör för användare i Göteborgs Stad att arbeta flexibelt med hög grad av mobilitet. En molntjänst är nåbar oavsett geografiska placering. Molntjänster utgör många gånger hela ekosystem med funktioner som ger användare möjlighet att samverka och utbyta information på ett enkelt sätt. Exempel på två ekosystem är Microsoft Office 365 och Google Workspace for Education. Båda leverantörernas ekosystem omfattar funktioner som är sammanhållna och ger användaren en möjlighet att samverka flexibelt och effektivt med andra användare, både i den egna organisationen och med externa aktörer.

Att ersätta ett ekosystem med fristående lösningar är möjligt men det innebär kraftigt ökade kostnader och kraftigt minskad funktionalitet. Trenden är att leverantörer överger enskilda solitära program som ger begränsad funktionalitet till förmån för molntjänstbaserade sammanhållna tjänster. Följdeffekten är att kostnader för tillgängliga licenser och licensmodeller blir avsevärt högre beroende på att utveckling av enskilda funktioner inte stödjer leverantörens utvecklingsstrategi, det vill säga, leverantörer satsar inte på produkter som inte främjar arbete i sammanhållna ekosystem.

Supportkostnader för enskilda funktioner blir höga och leverantörers egna kostnader för att upprätthålla kompetens ökar. Marknaden för solitära tjänster och funktioner är på sikt liten. Utvecklingen i omvärlden går mot sammanhållna ekosystem med inbyggd förmåga till samarbete vilket innebär att mindre resurser finns tillgängliga för utveckling av enskilda fristående funktioner.

Funktioner utanför ett ekosystem har också mycket sämre förmåga att samverka med existerande molntjänster vilket bidrar till försämrad användarupplevelse och effektivitet vilket på sikt kan leda till högre kostnader för personal.

På uppdrag från Kommunfullmäktige ska nämnden för Intraservice kraftigt dämpa kostnadsutvecklingen för drift, förvaltning och utveckling. Utan användning av molntjänster och dess kostnadsfördelar och möjlighet till effektiva arbetssätt blir det mycket svårt att nå detta mål. Nya medarbetare förväntas kunna använda de vanligaste molntjänsterna och nya medarbetare ställer krav på oss som arbetsgivare att tillhandahålla moderna och effektiva digitala hjälpmedel.

Förvaltningen ser en risk i att parallella organisationer kommer att uppstå i de förvaltningar och bolag som använder Kommungemensamma interna tjänster som oberoende av varandra adresserar frågan om vad som ska ersätta en avvecklad befintlig molntjänst. Detta leder till ökade kostnader i Göteborgs Stad, sämre måluppfyllelse och försämrad informationssäkerhet.

Det är mycket svårt att lämna någon uppfattning om vad det innebär för kostnad att lämna en molntjänst. Varje molntjänst kräver en unik studie som bland annat behöver visa vilken påverkan det har på befintliga Kommungemensamma interna tjänster, på det specifika användningsområdet och hur det eventuellt kan ersättas. Påverkan på organisation, på befintlig och ny kompetens behöver också utredas för varje specifik molntjänst.

Bedömning ur ekologisk dimension

För alla strategier är innovation, **digitalisering**, kommunikation och samverkan centrala möjliggörare för att lyckas. Förvaltningen refererar till följande tre styrande dokument som viktiga utgångspunkter:

Göteborgs Stads innovationsprogram:
Syftet med detta program är att skapa ett strukturerat arbete med innovation i Göteborgs Stads verksamheter och utgör därför en utgångspunkt för allt innovationsarbete i Göteborgs Stad. Att tänka nytt både vad gäller tekniska och institutionella lösningar är centralt för att lyckas nå målen i miljö- och klimatprogrammet.

Göteborgs Stads policy för digitalisering och IT:
Göteborg Stad ska vara en attraktiv stad där alla ges chansen att forma sina liv och där en ekonomisk stabilitet lägger grunden för en hållbar utveckling av Göteborgs Stad. Digitaliseringens möjligheter behöver tillvaratas utifrån aktuella och nya utmaningar för att lyckas med att vara en hållbar stad.

Göteborgs Stads policy för kommunikation:
Göteborgs Stad ska på ett systematiskt och öppet sätt sprida data, kunskaper och erfarenheter internt och externt. Vi utvecklar och effektiviserar kommunikationen kring Göteborgs Stads strategiska miljöarbete genom att använda en gemensam kommunikationsplattform för alla förvaltningar och bolag.

Men digitaliseringens påverkan på den ekologiska dimensionen är komplex. I delbetänkandet till den statliga utredningen SOU 2016:85 *Digitaliseringens effekter på individ och samhälle - fyra temarapporter* (Statens Offentliga utredningar, 2016) framgår att

> ”digitalisering kan ha såväl positiva som negativa effekter på miljön, och båda aspekterna behöver analyseras för att bedöma digitaliseringens nettoeffekt. Nettoeffekten av en it-produkt eller applikation är summan av alla interaktioner med miljön. Detta innebär till exempel att man behöver balansera de utsläpp av växthusgaser som sker till följd av utveckling, produktion och drift av it-produkter mot de utsläppsminskningar som kan hänföras till att användningen av produkterna förbättrar effektiviteten på annat håll, t.ex. i byggnader, transportsystem eller eldistribution.”

Bedömning ur social dimension

”Digitalt först” var regeringens program för digital förnyelse av det offentliga Sverige som genomfördes under 2015–2018. Nuvarande mål handlar om att Sverige ska vara bäst i världen på att ta tillvara digitaliseringens möjligheter. Rätt använd kan digitaliseringen öka möjligheten till smart och klok interaktion och samverkan direkt mellan boende, besökare och näringsliv och med Göteborgs Stad. Genom ökad kommunikation och tillgänglighet skapas möjligheter att öka transparens och insyn i information och beslut, vilket stärker demokratin. Digitala tjänster och infrastruktur skapar möjlighet till nya sätt att leverera välfärd där det senaste goda exemplet är omställningen under pågående pandemi. Något som visar att den digitala infrastrukturen i många fall är minst lika viktigt som den fysiska. Vi behöver bygga säkra och robusta tjänster som skapar digital trygghet och inkluderar samhällets alla medborgare

Samverkan

Samverkan med de fackliga organisationerna i FSG sker 2021-06-15

Bilagor

1. O365 bedömning SLK
2. Yttrande från IMY på samråd Stockholm Stad gällande AD i Azure
3. Konsekvenser och risker beskrivna i effektkedjor

Ärendet

Ärendet syftar till att informera nämnden om det rådande rättsläget och dess påverkan på molntjänster. Ärendet avser också att tydliggöra det arbetssätt som förvaltningen använder för att utveckla Kommungemensamma interna tjänster med funktionalitet som levereras via molntjänst.

Bakgrund

Intraservice har en roll inom Göteborgs Stad att vara intern leverantör av tjänster. Tjänster levereras som olika it-tjänster till andra bolag och förvaltningar inom Göteborgs Stad. Av 2 § i reglementet som styr uppdraget för Intraservice framgår att Intraservice ska utveckla, leverera, och följa upp samordnade interna tjänster med it-stöd i Göteborgs Stad. Detta ska ske i enlighet med de av kommunfullmäktige fastställda riktlinjer för styrning av Kommungemensamma interna tjänster. Nämnden för Intraservice ska också besluta om ärenden gällande stadsgemensamma it-stöd och vid behov bereda ärenden inom detta område till kommunstyrelsen och kommunfullmäktige.

I tjänsteutlåtande från 2019-12-10 (dnr 0189/19) lämnade förvaltningen förslag till nämnden för Intraservice att besluta om den fortsatta användningen och utvecklingen av Microsoft Office 365. Nämnden bedömde att ärendet var av sådan principiell betydelse för kommunen och beslutade 2019-12-19 § 204 att begära kommunstyrelsens yttrande i frågan. Kommunstyrelsen beslutade 2021-01-13 § 20 (dnr 0189/19) att återsända ärendet till nämnden för Intraservice med motiveringen att ärendet ligger inom ramen för Intraservice uppdrag att leverera Kommungemensamma interna tjänster i Göteborgs Stad.

Förvaltningens arbete avseende en fortsatt utveckling av molntjänster, i Kommungemensamma interna tjänster, där behandling av personuppgifter sker måste omfatta samtliga de leverantörer som ingår i leveranser av Kommungemensamma interna tjänster. I utvecklingsinitiativ kan inte Office 365 hanteras annorlunda. Hänsyn måste vid beslut tas till roller och ansvar utifrån både stadens styrande dokument och dataskyddsförordningens regelverk.

Molntjänster inom Göteborgs Stad

Ansvar och roller inom Göteborgs Stad vid tillhandahållandet och användandet av molntjänster som Kommungemensam intern tjänst.

Sammanfattning

Intraservice har två roller att hantera ur ett dataskyddsperspektiv. Intraservice är i sin egen verksamhet *personuppgiftsansvarig*. I sin roll som leverantör är Intraservice ett *personuppgiftsbiträde*. Intraservice kan bara besluta om sin egen behandling av personuppgifter. För att förstå roller och ansvar är det viktigt att känna till och förstå begreppen personuppgiftsansvarig, personuppgiftsbiträde, underbiträde och att veta vad ett personuppgiftsbiträdesavtal är.

Intraservice är själv användare av molntjänster (tex. Microsoft Office 365) för sin egen verksamhet och är då personuppgiftsansvarig. Intraservice har samtidigt rollen som leverantör (personuppgiftsbiträde) till andra verksamheter inom Göteborgs Stad. Dataskyddsförordningen har tydliga regler rörande ansvar och roller vid behandling av personuppgifter. Begreppen förklaras i detta avsnitt.

Kommungemensamma interna tjänster

Uppdraget att leverera Kommungemensamma interna tjänster regleras främst av ”Göteborgs Stads riktlinjer för styrning av Kommungemensamma interna tjänster. Riktlinjerna är antagna av kommunfullmäktige. Riktlinjerna kompletteras dels av Göteborgs stads regler för Kommungemensamma interna tjänster, dels Göteborgs stads generella regler för Kommungemensamma interna tjänster. Kommunstyrelsen har enligt riktlinjerna ett uppdrag att ha ett lednings- och samordningsansvar för dessa tjänster. Enligt dessa styrande dokument är det stadsdirektören, på delegation av kommunstyrelsen efter samråd med förvaltnings- och bolagsledningar, som beslutar om vilka tjänster som ska vara Kommungemensamma interna tjänster samt fastställer de kompletterande reglerna.

Intraservice tillhandahåller tjänster som förvaltningen använder själva i sin egen verksamhet, de största användarna av tjänsterna är dock övriga verksamheter inom Göteborgs Stad. Det innebär att Intraservice i förhållande till andra delar av Göteborgs Stad är att betrakta som leverantör.

I den förordning som reglerar skyddet för personuppgifter, dataskyddsförordningen, regleras relationer och ansvar mellan olika parter i samband med tjänster där personuppgifter behandlas för en annan parts räkning, typiskt sett just inom en kund – leverantörs situation. Mer om dataskyddsförordningen följer nedan, men förordningen är relevant att belysa redan inledningsvis för förståelsen av rollfördelning och ansvar.

Roller och ansvar ur ett dataskyddsperspektiv

Intraservice är ansvarig för de personuppgifter som behandlas för den egna verksamheten och kallas då ”Personuppgiftsansvarig”. När Intraservice är leverantör och behandlar personuppgifter för andra förvaltningars och bolags räkning så är respektive nämnd personuppgiftsansvarig och Intraservice kallas i rollen som leverantör för ”Personuppgiftsbiträde”. Om Intraservice i sin tur anlitar underleverantör som också behandlar personuppgifter för andra delar av Göteborgs Stad så är underleverantören ”Underbiträde”. I förhållande till andra förvaltningar och bolag inom staden så är alltså Intraservice leverantör av Microsoft Office 365 och Google Workspace for Education. Microsoft och Google är underbiträden och allt som dessa underbiträden gör kan i princip läggas Intraservice till last.

De olika rollerna har getts olika ansvar i dataskyddsförordningen. Som regel är den som är personuppgiftsansvarig den som är skyldig att följa dataskyddsförordningen och som måste kunna bevisa att så har skett, men även personuppgiftsbiträdet kan drabbas av ansvar och sanktioner i vissa fall. När den personuppgiftsansvarige anlitar ett personuppgiftsbiträde är det därför ett krav att parterna reglerar sin relation i ett särskilt avtal ”Personuppgiftsbiträdesavtal”. I detta ska den personuppgiftsansvarige lämna personuppgiftsbiträdet instruktioner om hur de personuppgifter som biträdet hanterar för den personuppgiftsansvariges räkning ska behandlas och skyddas.

Biträdet har ingen egen beslutanderätt rörande uppgifterna och får inte behandla uppgifterna på ett sätt som strider mot avtalet och instruktionerna. Om så sker så kan biträdet anses ha tagit på sig rollen som personuppgiftsansvarig och därmed det ansvar som följer med rollen.

I förhållandet mellan Intraservice och övriga Göteborgs Stads verksamheter är personuppgiftsbiträdesavtalet infogat som en bilaga till Göteborgs stads generella regler för Kommungemensamma interna tjänster (Kommunstyrelsen, 2018). Intraservice är skyldigt att följa personuppgiftsbiträdesavtalet och de instruktioner som vid var tid meddelats av verksamheterna. Av biträdesavtalet framgår bland annat att Intraservice ska följa förordningen, att överföring till ett land utanför EU/EES inte får ske utan verksamheternas skriftliga samtycke i förväg och efter säkerställande av att överföringen sker i överenstämmelse med lag samt att anlitandet av underbiträden ska godkännas i förväg.

Intraservice tecknar i sin tur personuppgiftsbiträdesavtal med underbiträden, vilka ska åläggas minst samma skyldigheter som Intraservice har i förhållande till Göteborgs Stads verksamheter. Intraservice ska informera de personuppgiftsansvariga verksamheterna om eventuella planer på att anlita nya underbiträden eller ersätta underbiträden, så att den personuppgiftsansvarige har möjlighet att göra invändningar mot sådana förändringar. För de fall det finns rimligt fog för invändningen har personuppgiftsansvarige rätt att med bindande verkan motsätta sig anlitandet av visst nytt underbiträde.

Val av personuppgiftsbiträden och underbiträden

Enligt förordningen får den personuppgiftsansvarige endast anlita personuppgiftsbiträden som ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller förordningens krav och ger tillräckligt skydd för personuppgifter. Detta innebär att den verksamhet som vill uppdra åt någon annan att behandla personuppgifter för deras räkning har en omsorgsplikt vid val av biträde, som innefattar att göra en riskbedömning. De överväganden som görs bör dokumenteras på lämpligt sätt.

Mandat att besluta om vilken behandling som ska ske i molntjänsterna

Ovan sagda innebär att Intraservice endast kan besluta och ta ställning till de behandlingar som Intraservice gör i form av personuppgiftsansvarig, dvs för den egna verksamheten. Övriga personuppgiftsansvariga behöver informeras och konsulteras enligt personuppgiftsbiträdesavtalet och de måste själva besluta om sin användning av de tjänster som Intraservice erbjuder. Förvaltningens expertkompetens kan bedöma och utvärdera molntjänster och bistå andra förvaltningar och bolag med sin bedömning men beslut om användning av molntjänst där behandling av personuppgifter sker måste

beslutas av respektive personuppgiftsansvarig nämnd i Göteborgs Stad. Intraservice bedömningen görs alltså i egenskap av personuppgiftsbiträde och det är upp till varje personuppgiftsansvarig att förlita sig på bedömningen eller göra en egen.

Förekomst av personuppgifter i olika typer av data

Personuppgifter kan förekomma i innehållsdata, i diagnosdata och i funktionsdata eller vid support. Begreppen definieras enligt nedan:

- **Innehållsdata** (kund data, Content data, Customer data) är data som användare skapar med ett *kontorsstöd* eller *verksamhetssystem*, till exempel via texten i ett Worddokument, innehållet i ett e-postmeddelanden, informationen i de skoladministrativa systemen, i patientjournaler eller i kontaktinformation som användaren kompletterar med i Delve, chatten i Teams eller i Google Meet.
- **Diagnosdata** (telemetridata) är data som leverantören samlar in för att analysera hur tjänster, applikationer och operativsystem används. Datat är en förutsättning för analys av funktionaliteten och för att utveckla och uppdatera applikationen. Diagnosdata samlas även i vissa fall in för att säljas vidare till andra leverantörer.
- **Funktionsdata** är data som är till för att säkerställa de grundläggande funktionerna i en applikation och är till exempel identiteter och inloggningsinformation, autentiseringsinformation, konfigurationsinformation, accessrättigheter, och versionshantering av filer som innehåller innehållsdata. Funktionsdata är data som leverantören tillfälligt måste bearbeta för att låta användare ansluta till internet och använda onlinetjänster.

Utkontraktering

Utkontraktering[1] av drift, underhåll, support eller molntjänster är vanligt inom statliga myndigheter, kommuner och regioner. Utkontrakteringen innebär att en leverantör utför teknisk bearbetning och teknisk lagring av en it-tjänst.

Teknisk bearbetning och lagring är aktiviteter inom it-drift och dit räknas underhåll och teknisk support av hård- och mjukvara. Till it-drift räknas också underhåll och hantering av it-arbetsplats, mjukvarusystem, förvaltning, utveckling samt avveckling och förändringar av en it-tjänst. Likaså förändringar av funktioner och införande av tilläggstjänster och supporttjänster[2]. Teknisk bearbetning och lagring kan levereras i form av molntjänster:

Molntjänster

En molntjänst levereras från en leverantör i form av infrastruktur som tjänst (IaaS), plattform som tjänst (PaaS) och mjukvara som tjänst (SaaS). Även andra tjänster som till exempel support kan ingå. I tjänsterna finns olika grad av innehållsdata, diagnosdata och funktionsdata.

- **IaaS** är en leverans av hårdvara där kunden själv ansvarar för vad som körs på hårdvaran. IaaS omfattar serverutrymme, nätverk, lastbalansering, lagring och säkerhet. Virtuella datacenter bestående av flera fysiska servrar kan finnas på olika geografiska platser. Majoriteten data är funktionsdata.

[1] Utkontraktering – definition från SOU202:1
[2] Från regeringens proposition (2019/20:201) och SOU 202:1

- **PaaS** är en leverans av plattformen där operativsystem och annan underliggande programvara kan konfigureras med automatik. Majoriteten av data är funktionsdata och diagnosdata.
- **SaaS** är en leverans av mjukvara där distribution av applikationer till användare eller klienter sker över internet. Leveransen görs via en webbläsare till en dator eller till en telefon. I Kommungemensamma interna tjänster och stödtjänster är exempel på SaaS: Microsoft Office 365, Google Workspace For Education, samt Service Now. Majoriteteten av data är innehållsdata och diagnosdata.
- **On-Prem** är en leverans av IaaS, PaaS, SaaS eller support via den egna organisationen. I tjänsterna finns olika grad av innehållsdata, diagnosdata och funktionsdata.
- **Supporttjänster** är när en leverantör, oavsett om den levereras som en molntjänst, via sin support får tillgång till personuppgifter. Exempel är support från Microsoft, från Google eller från ServiceNow. Även support via underleverantörer för en tjänst som till exempel Benify omfattas. I tjänsterna finns olika grad av innehållsdata, diagnosdata och funktionsdata.

I Intraservice leverans av Kommungemensamma interna tjänster används samtliga former av utkontraktering och molntjänster.

Geografisk placering och leverantörens tillgång till informationen

Flera leverantörer av molntjänster är internationella och har datacenter på olika geografiska platser och i olika länder. Data och information flödar generellt sett fritt mellan datacentren för att skapa hög tillgänglighet och redundans. Data och information kan som konsekvens överföras till länder som inte omfattas av europeisk och svensk lagstiftning. Det innebär att hänsyn måste tas till den nationella lagstiftningen där teknisk bearbetning och lagring utförs samt vilka juridiska och tekniska skyddsåtgärder som ger adekvat skydd enligt europeisk och svensk lagstiftning.

För att en avancerad SaaS tjänst som Google Workspace for Education eller Microsoft Office 365 ska kunna användas via en webbläsare måste all bearbetning av data finnas hos leverantören. Det innebär att data är okrypterad hos leverantören vid bearbetning. Vid lagring är den krypterad men leverantören känner till krypteringsnyckeln.

För en SaS tjänst som endast erbjuder fillagring kan data krypteras lokalt innan den överförs till leverantören. Detta är säkert så länge som krypteringsnyckeln endast är känd av kunden (tex. Intraservice, Göteborgs Stad) och att all kryptering och dekryptering görs på den egna enheten innan data skickas till leverantörens molntjänst.

För IaaS och PaaS innebär det att man själv kontrollerar sitt data och sitt system. Men tillgången till hårdvaran eller operativsystem gör det möjligt för leverantör att få tillgång till data.

Överblick över hur olika scenarion överensstämmer med lagstiftningen

I tabell 1 nedan presenteras scenarion som beskriver när ett godkänt förhållande uppstår beroende på var bearbetning och lagring utförs i en tjänst och gäller oavsett om det är personuppgifter i innehållsdata, diagnosdata, funktionsdata eller vid support.

Ett X i kolumner för respektive scenario markerar var bearbetning och lagring utförs, antingen av den egna organisationen eller av en leverantör som inte är bunden till amerikansk lagstiftning. Med Sverige avses i de fall bearbetning eller lagring utförs av

egen organisation eller av en svensk leverantör (det vill säga att leverantören lyder svensk lagstiftning först). För några scenarion finns förbehåll.

Tabell 1- Scenarion i förhållande till var bearbetning och lagring utförs

Scenario	Bearbetning			Lagring			Godkänd användning
	Sverige	EU/EES	Tredjeland	Sverige	EU/EES	Tredjeland	
1A	X			X			Ja
1B	X				X		Ja
1C	X					X	Ja med förbehåll
2A		X		X			Ja
2B		X			X		Ja
2C		X				X	Ja med förbehåll
3A			X	X			Nej, men förbehåll finns
3B			X		X		Nej, men förbehåll finns
3C			X			X	Nej, men förbehåll finns

Förbehåll

1C, 2C – Förbehåll

Godkänt om data krypteras innan den skickas till tredjeland och att nycklar endast är kända av den egna organisationen eller leverantör. Alternativt att artikel 46 eller artikel 49 tillsammans med kompletterande skyddsåtgärder medför Väsentligt likvärdigt skydd i enlighet med dom i mål C-311/18 kan detta förhållande vara godkänt.

(artikel 46 förklaras i avsnitt Andra lämpliga skyddsåtgärder sid 27)

3A, 3B, 3C - Förbehåll

Bearbetning i tredjeland (innebär att informationen är överförd) är generellt inte godkänt men om artikel 46 eller artikel 49 tillsammans och kompletterande skyddsåtgärder medför Väsentligt likvärdigt skydd i enlighet med dom i mål C-311/18 kan detta förhållande vara godkänt.

(artikel 46 förklaras i avsnitt Andra lämpliga skyddsåtgärder sid 27)

Informationssäkerhet, dataskydd, säkerhetsskydd och cybersäkerhet

Informationssäkerhet, dataskydd, säkerhetsskydd och cybersäkerhet är fyra sammanflätande områden som delvis överlappar och delvis skiljer sig åt.

1. Informationssäkerhet innefattar skydd av all information i både fysisk och digital form. Utgångspunkten är att samtliga tänkbara risker, hot, konsekvenser och sannolikheter ska bedömas ur alla perspektiv.
2. Dataskydd fokuserar på personuppgifter och har sin utgångspunkt i dataskyddsförordningen och risker för kränkningar av enskilda individers fri- och rättigheter.
3. Säkerhetsskydd handlar om att skydda information och verksamheter som är av betydelse för Sveriges säkerhet och tar sin utgångspunkt i säkerhetskyddslagstiftningarna och risker mot antagonistiska hot som till exempel spioneri, sabotage, terroristbrott.

4. Cybersäkerhet innefattar skydd av tekniska hjälpmedel och information som bearbetas, överförs, lagras med hjälp av olika tekniska hjälpmedel (dvs oftast digitala).

De interna och externa kraven en organisation har för skydd gällande informationstillgångar grupperas inom de fyra kategorierna konfidentialitet, riktighet, tillgänglighet, och integritet.

- Konfidentialitet (Confidentialitity) är krav på att information ska skyddas mot obehöriga.
- Riktighet (Integrity) är krav på att information som skyddas inte kan manipuleras eller förstöras.
- Tillgänglighet (Availability) är krav på att information är tillgänglig för den som är behörig.
- Integritet (Privacy) är krav på att personuppgifter ska skyddas mot otillåten behandling, obehöriga, mot förlust, förstöring eller skada genom olyckshändelser.

Inom informationssäkerhet är det främst fokus på kategorierna konfidentialitet, riktighet och tillgänglighet. Inom dataskydd är det främst fokus på kategorierna integritet och riktighet. Inom säkerhetsskydd är det främst fokus på kategorien konfidentialitet. Inom cybersäkerhet är det främst fokus på kategorien konfidentialitet och tillgänglighet.

Kraven på skydd realiseras sedan genom att man kopplar säkerhetsåtgärder till varje konsekvensnivå. Säkerhetsåtgärder indelas typiskt i organisatoriska, administrativa, tekniska, fysiska och juridiska åtgärder. Oftast är det en kombination av skyddsåtgärder som skapar ett anpassat säkerhetsskydd.

- Organisatoriska skyddsåtgärder är hur man utformar sitt säkerhetsarbete i en organisation, till exempel via organisationsbeskrivningar, befattningsbeskrivningar, styrdokument, arbetsordning och delegationsbeslut.
- Administrativa skyddsåtgärder är process och metodstöd för genomförandet av vad som står i styrdokument och arbetsordningar. Styrdokument omfattar till exempel personalsäkerhet, informationskartläggning, informationsklassning, riskanalyser, konsekvensbedömningar, riskhantering, val av säkerhetsåtgärder, implementera och följa upp säkerhet, kontinuitetshantering, incidenthantering samt att implementera ledningssystem för informationssäkerhet och dataskydd.
- Tekniska skyddsåtgärder är hur infrastruktur, hårdvara, mjukvara och information skyddas. Typiska skyddsåtgärder är styrning av åtkomst, kryptering, driftsäkerhet, skydd mot skadlig kod, säkerhetskopiering, loggning och övervakning, styrning av driftsystem, hantering av tekniska sårbarheter, kommunikations och nätverkssäkerhet.
- Fysiska skyddsåtgärder är hur man skyddar till exempel utrustning och områden.
- Juridiska skyddsåtgärder är hur man efterlever lagar, avtal och regler. Typiska skyddsåtgärder är avtal och försäkringar.

Juridiska frågeställningar och molntjänster

Relevant amerikansk lagstiftning i sammandrag

Sammanfattning:

Vid användning av utländska leverantörer så står dessa leverantörer under kontroll av en annan nations lagstiftning. Flera av de tjänster som Intraservice använder sig av tillhandahålls av amerikanska leverantörer. Amerikansk lagstiftning måste därför beaktas för att förstå vilken påverkan den har på avtalsrelationen, tjänsten och om lagstiftningen är förenligt med den nationella lagstiftningen så som offentlighet- och sekretesslagstiftningen och dataskyddsförordningen.

Att förstå jurisdiktionsrisken vid molntjänster

Vid användning av molntjänster tillhandahållna av utländska leverantörer och/eller tjänster som tillhandahålls utanför rikets gränser finns alltid en risk för att de uppgifter och handlingar som omfattas av leverantörens åtagande också kommer att bli föremål för den reglering som följer av den lagstiftning som gäller inom den jurisdiktion där leverantören är verksam eller informationen finns. De flesta länder bedriver någon form av kommunikationssignalspaning. Det kan vara i syfte att kartlägga främmande makters förhållanden, avvärja säkerhetshot som terrorism, spridning av massförstörelsevapen eller hot mot infrastruktur.

Med tanke på den ökade frekvensen av terrorhot och ett osäkert säkerhetsläge i omvärlden har behovet av en effektiv försvarsunderrättelseverksamhet ökat. Samtidigt så innebär kommunikationssignalspaning ett intrång i kommunikationen mellan individer, vilket i sig också kan bli problematiskt exempelvis i förhållande till frågor som rör skyddet för sekretessbelagda uppgifter men också i upprättandet av skyddet för den enskildes integritet.

De flesta länder bedriver någon form av signalspaning, varav kommunikationssignalspaning utgör en väsentlig del. Hur sådan spaning får gå till och om den ska vara nationell eller exterritorial avgörs av varje lands egen lagstiftning. Lagstiftning i andra länder kan alltså innebära att andra länders myndigheter kan ha rätt att direkt från leverantörer av exempelvis molntjänster utkräva åtkomst till uppgifter som leverantören hanterar för kundens räkning. Detta kan därför påverka svenska myndigheters möjligheter till användningen av molntjänster.

Eftersom det framför allt är amerikanska leverantörer som är aktuella för de tjänster som Intraservice använder så är det relevant att ha med en kort beskrivning av vad dessa lagar innebär eftersom de påverkar både hanteringen ur ett sekretessperspektiv och ett dataskyddsperspektiv. Liknande regleringar förekommer dock också i andra länder så som exempelvis Indien, Kina och Storbritannien.

Amerikansk lagstiftning och regelverk

Bestämmelser om amerikansk försvarsunderrättelseverksamhet och signalspaning återfinns i ett flertal olika regleringar. Detta beror bland annat på att det i amerikansk rätt görs en tydlig uppdelning mellan signalspaning som bedrivs inom USA och sådan som bedrivs utanför landet.

US CLOUD Act

CLOUD Act (Clarifying Lawful Overseas Use of Data Act) (115th US Congress , 2018) möjliggör att amerikanska myndigheter under vissa förutsättningar och efter beslut av amerikansk domstol kan begära ut data som lagras utanför USA från tjänsteleverantörer (exempelvis telekomoperatörer och molntjänstleverantörer) som omfattas av amerikansk jurisdiktion. Alla amerikanska bolag omfattas av amerikansk jurisdiktion. När information begärs ut på detta sätt så innebär det att information (både personuppgifter och andra hemliga handlingar) rörande både europeiska fysiska och juridiska personer hamnar hos amerikanska myndigheter. En begäran att få ut information kan i vissa fall bestridas av tjänsteleverantören. Men begäran att utfå informationen kan förenas med sekretesskrav innebärande att tjänsteleverantören inte får informera den enskilde eller sin kund om att informationen lämnas ut.

Executive Order 12333

Vid signalspaning utanför USA tillämpas Executive Order 12333 (Reagan, 1981). Ordern utfärdades av Ronald Reagan år 1981 och har uppdaterats fler gånger sedan dess. Ordern förtydligar det ramverk under vilket amerikanska myndigheter bedriver underrättelseverksamhet. Ordern ger bland annat National Security Agency (NSA) behörighet att bedriva signalspaning för insamlandet av försvarsunderrättelseinformation.

FISA 702

När signalspaning bedrivs inom USA:s territorium gäller Foreign Intelligence Surveillance Act (FISA) (110th Congress, 2008). FISA är en amerikansk lag från 1978 som reglerar insamling av försvarsunderrättelseinformation. Under FISA får signalspaning riktas mot utländska makter eller utländska agenter samt mot icke-amerikaner för att inhämta försvarsunderrättelseinformation. Amerikanska myndigheter tillåts enligt lagen att använda verktyg som avlyssning av kommunikation och tillgång till data som lagras i exempelvis molntjänster. NSA tillämpar olika tekniker vid inhämtning av information under vissa övervakningsprogram. Ett sådant program är Planning Tool for Resource Integration, Synchronization and Management (PRISM) (Gellman & Poitras, 2013) som innebär att vissa företag anslutna till programmet, är skyldiga att leverera viss data som kunderna har hos leverantören. Det kan exempelvis vara information relaterad till en viss e-postadress eller användare. En annan form av insamling sker av internationell kommunikation när den färdas in och ut från USA. Informationen samlas in då när den passerar kablar i nätet. Detta innebär en *bulkinsamling* av information baserad på vissa urvalskriterier. Företag som tillhandahåller elektroniska kommunikationstjänster är skyldiga att erbjuda den efterfrågade informationen samt tillhandahålla den assistans som krävs för att inhämtningen ska kunna genomföras utan att kunna informera sina kunder.

FISA gör en tydlig distinktion mellan amerikanska och utländska medborgare, då amerikanska medborgare ges visst skydd av USA:s konstitution i form av rätt till privatliv vilket inte gäller för utländska medborgare. I princip saknas effektiva rättsmedel och bindande rättigheter för utländska medborgare som kan göras gällande mot amerikanska myndigheter.

Molntjänster ur ett offentlighets- och sekretessperspektiv

Relevant sekretesslagstiftning i sammandrag

Sammanfattning:

Offentliga verksamheter är bundna av Tryckfrihetsförordningens regler om handlingars offentlighet. Eftersom offentliga verksamheter också hanterar uppgifter som inte lämpligen är offentliga ska dessa verksamheter också tillämpa offentlighets- och sekretesslagen (2009:400) för att avgöra när och på vilket sätt uppgifter ska hållas hemliga eller får lämnas ut. Lagstiftningen är tillskapad före de stora digitala molntjänsternas tid och den är därför inte helt tydlig med hur utkontrakterad it-drift (molntjänster) ska hanteras. Det har gjorts många utredningar av olika aktörer och olika tolkningar förekommer. Stadsledningskontoret, genom stadsjuristerna har tagit ställning till frågan rörande Microsoft Office 365 för Göteborgs Stads räkning. För att underlätta för offentliga aktörer att i större utsträckning kunna använda sig av utkontrakterad it-drift har ett lagförslag presenterats i delbetänkandet SOU 2021:1 Säker och kostnadseffektiv it-drift – rättsliga förutsättningar för utkontraktering (Statens Offentliga utredningar, 2021). Delbetänkandet tolkar sekretesslagstiftningen på delvis ett annat sätt än vad Stadsledningskontoret har gjort, men lämnar också ett förslag till en lösning (genom nya lagregler tänkta att träda i kraft 1/1 2022) för att lösa de oklarheter som finns i dagens regelverk. Delbetänkandet har ännu inte antagits. Dagens användning av Microsoft Office 365 inom Göteborgs Stad baserar sig därför alltjämt på den bedömning som Stadsledningskontoret har gjort.

Hantering av offentliga verksamheters handlingar i molnet

I samband med så kallade *molntjänster* eller utkontrakterad it-drift diskuteras ofta om sådan utkontraktering är tillåten eller olaglig enligt offentlighets- och sekretesslagen (2009:400) (“**OSL**”). Frågan adresseras ofta under benämningen *röjandefrågan*. För att förstå problematiken är det viktigt att ha viss kunskap om hur lagstiftningen fungerar.

Offentlighet och sekretess – regelverket i korthet

För att en handling ska vara allmän krävs det att den är upprättad eller inkommen och förvarad på myndigheten. Varje nämnd ses som en egen myndighet. Så snart en handling passerar en myndighetsgräns så är den, som huvudregel, att anse som upprättad och/eller inkommen till myndigheten och blir därmed en allmän handling. En handling är en bärare av information. Det är inte bara dokument utan exempelvis också filmer, bilder, sms, e-post och andra typer av framställningar. I princip anses alla framställningar som finns i bild eller skrift eller som man på annat sätt kan läsa, se på, lyssna på eller på annat sätt kan uppfatta med tekniska hjälpmedel anses vara handlingar i Tryckfrihetsförordningens (1949:105) mening.

Mycket av det som produceras är internt arbetsmaterial medan andra framställningar skickas till någon annan mottagare i kommunen, eller någon utomstående organisation eller privatperson. Annan information tar förvaltningen emot. Enligt en av våra grundlagar, tryckfrihetsförordningen, så är alla handlingar som förvaras på förvaltningen och som är antingen inkomna till eller skickade från förvaltningen allmänna handlingar. Också interna handlingar blir i vissa fall allmänna handlingar då de färdigställs exempelvis handlingar som ligger till grund för beslut, protokoll som justeras eller handlingar som läggs i diariet. Som huvudregel så har allmänheten rätt att få ta del av handlingar som är allmänna.

En del av den information som hanteras inom det offentliga är känslig och därför är det inte lämpligt att allmänheten får ta del av den. Även annan information, som i och för sig inte finns i en allmän handling, kan vara mycket känslig och måste skyddas från spridning. För att hindra att känslig information sprids finns OSL. Den skyddar alltså både allmänna handlingar och andra handlingar som finns i offentliga verksamheter.

OSL pekar ut vilka slags uppgifter med visst innehåll som ska skyddas. Det är endast den information som skyddas av en sekretessbestämmelse som omfattas av sekretess. Sekretess definieras i lagen som ”ett förbud att röja en uppgift, vare sig det sker muntligen, genom utlämnande av en allmän handling eller på något annat sätt”.

Sekretess kan alltså gälla oavsett om det är uppgifter som finns i en allmän handling eller inte. Det är också själva uppgifterna som skyddas - inte hela handlingar. Uppgifterna skyddas både genom bestämmelser om tystnadsplikt och förbud mot att lämna ut allmänna handlingar.

Sekretessbestämmelserna tar sikte på uppgifternas innehåll eller förekomsten i ett visst sammanhang. Bestämmelserna skyddar också olika intressen. Det kan exempelvis röra sig om enskildas personliga eller ekonomiska förhållanden eller det allmännas intressen.

Varje bestämmelse är utformad på ett sätt så att skyddet inte blir mer långtgående än vad som är motiverat av skyddsintresset. Därför finns det olika grader av sekretess. Ett beslut att inte lämna ut uppgifter kan överklagas till kammarrätten.

Man kan dela in sekretessnivåerna på följande sätt:

1. Ingen sekretess dvs. det finns inget undantag i OSL från huvudregeln om offentlighet

2. Uppgifter där man utgår ifrån att offentlighet råder om det inte kan antas att viss skada eller visst men uppkommer om uppgiften röjs. Det är upp till myndigheten att argumentera för att det kan vara förenat med skada att lämna ut handlingen.

Exempel: Sekretess gäller för uppgift om en enskilds affärs- eller driftförhållanden när denne har trätt i affärsförbindelse med tex. kommunalt bolag, om det kan antas att den enskilde lider skada om uppgiften röjs

3. Uppgifter där man utfår ifrån att sekretess råder om det inte står klart att uppgiften kan röjas utan skada eller men.

   Exempel: Sekretess gäller inom hälso- och sjukvården för uppgift om en enskilds hälsotillstånd eller andra personliga förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till denne lider men.

4. Absolut sekretess dvs. sekretess råder och det finns inte utrymme för prövning.

   Exempel: Sekretess gäller inom kommunal familjerådgivning för uppgift som en enskild har lämnat i förtroende eller som har inhämtats i samband med rådgivningen.

Eftersom sekretessbestämmelserna är utformade på detta sätt så krävs alltid att förvaltningen gör en sekretessprövning av varje enskild uppgift för att avgöra om ett utlämnande kan göras utan att skyddsintresset tar skada innan en handling får lämnas ut.

Sekretesslagstiftningen gäller inte för alla verksamheter utan för myndigheter och vissa andra verksamheter som jämställs med myndigheter i lagtexten, exempelvis kommunala bolag. Lagen omfattar inte privata aktörer. Däremot så omfattas den som är anställd i verksamheten eller på uppdrag i verksamheten. En konsult anställd i en privat verksamhet som genom ett uppdragsavtal tjänstgör på en myndighet så denne i praktiken deltar i verksamheten omfattas alltså också. Även den som är där på grund av tjänsteplikt eller annan liknande grund omfattas. Det finns möjligheter att i avtal komma överens om sekretess men det betyder inte att leverantören omfattas av den lagstadgade sekretessen i OSL.

Den 1 januari 2021 trädde lagen (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter i kraft (”**Tystnadspliktslagen**”). Lagen är tillämplig när en myndighet uppdrar åt ett företag eller en annan enskild (tjänsteleverantör) att endast tekniskt bearbeta eller tekniskt lagra uppgifter. Lagen innebär inte att tjänsteleverantörerna (och deras personal) omfattas av OSL men lagen skapar en lagreglerad och därmed straffsanktionerad tystnadsplikt för anställda i den verksamhet som omfattas.

Sekretess innebär att sekretessbelagda uppgifter inte får röjas till varken till fysiska eller juridiska personer. Det finns dock undantag från kravet på tystnadsplikt när uppgifter lämnas för publicering i media (meddelarfrihet).

Det finns också många andra undantag där sekretessbelagda uppgifter, med stöd av lagen, får lämnas ut. Sådana undantagsbestämmelser kallas för sekretessbrytande bestämmelser. Vissa sådana sekretessbrytande bestämmelser innebär exempelvis att uppgifter i vissa fall får lämnas mellan olika myndigheter.

Överlämnandet av sekretessbelagda uppgifter till utländsk myndighet eller mellanfolkliga organisationer är särskilt reglerat i OSL genom en sekretessbrytande bestämmelse som innebär att ett överlämnande av sekretessbelagd information bara får ske i enlighet med

föreskrift i lag eller förordning eller om uppgiften i motsvarande fall skulle få lämnas ut till en svensk myndighet och det enligt den utlämnande myndighetens prövning står klart att det är förenligt med svenska intressen att uppgiften lämnas ut.

Om en uppgift är sekretessbelagd så får den inte lämnas ut, varken muntligen eller på annat sätt, såvida inte något undantag är tillämpligt eller den bedömts möjlig att lämna ut efter skadeprövning. För att säkerställa följsamhet mot lagen så är överträdelser straffsanktionerade i Brottsbalken (1962:700). Där framgår att om någon röjer en uppgift som denne var skyldig att hålla hemlig enligt lag eller annan författning eller om någon på annat sätt utnyttjar sådan hemlig uppgift så ska denne dömas för brott mot tystnadsplikten till böter eller fängelse i högst ett år. Om röjandet sker av oaktsamhet så är följden böter och om det rör sig om ett ringa fall så ska ansvar inte utdömas. Den som uppmanar någon annan att röja en uppgift eller på annat sätt medverkar till att hemliga uppgifter röjs kan dömas för sin medverkan. Att felaktigt lämna ut en handling som på grund av sekretess inte får lämnas ut kan även utgöra tjänstefel.

Offentlighet och sekretesslagen och ”molntjänster”

Det finns framför allt tre frågeställningar som har väckt mycket uppmärksamhet och som ansetts mer eller mindre problematiska när det gäller hanteringen av information innehållandes uppgifter som omfattas av sekretess i molntjänster. De är *röjandefrågan, sekretessprövning* och *utländska myndigheters möjlighet att bereda sig tillgång till information.*

Ett flertal utredningar har utförts, men eftersom rättsläget är oklart så finns inget entydigt svar.

Tekniskt röjd är ett begrepp som används av eSamverkansprogrammet (eSam, 2015; eSam, 2016; eSam, 2018; eSam, 2019; eSam, 2021) och innebär utkontraktering av teknisk bearbetning och behandling. I en molntjänst betraktas informationen som delad med leverantören om man inte tydligt kan visa motsatsen. Leverantören av molntjänsten har teknisk insyn i hela sin tjänst. Detta gäller även vid specifika skyddslösningar framtagna av samma leverantör för samma molntjänst (eSam, 2021). Det innebär att om sekretessreglerade uppgifter görs tekniskt tillgängliga för en tjänsteleverantör som till följd av ägarförhållanden eller annars är bunden av regler i ett annat land, enligt vilka tjänsteleverantören kan bli skyldig att överlämna information utan att internationell rättshjälp anlitats eller annan laglig grund föreligger enligt svensk rätt, får uppgifterna anses vara röjda. (eSam, 2018). Kammarkollegiet gör samma bedömning som eSam i att sekretessreglerade och säkerhetskänsliga uppgifter som finns tillgängliga i en utländsk molntjänst, på det sätt som eSamverkansprogrammet uttalat, är att anse som röjda (Kammarkollegiet, 2019).

Faktiskt röjd är ett begrepp som används av SKR och innebär att även om information är tekniskt tillgänglig för leverantören så är den inte är röjd förrän den verkligen lämnas ut till obehöriga (Sveriges Kommuner och Regioner, 2019; Sveriges Kommuner och Regioner, 2019; Sveriges Kommuner och Regioner, 2019). I Försäkringskassans vitbok (Försäkringskassan, 2019) så beskrivs detta med det ska finnas en juridiskt bindande och sanktionerad avtalssekretess för leverantören. Leverantören får inte heller vara bunden av regler i främmande rätt om att lämna ut uppgifter utan en föregående sekretessprövning eller annan laglig grund enligt svensk rätt för ett utlämnande och därefter att

omständigheterna i övrigt medför att det är osannolikt att tjänsteleverantören ändå tar del av eller vidarebefordrar uppgifterna.

De tre frågeställningar som framför allt uppfattats som oklara i förhållande till molntjänster

1. Röjandefrågan

Det råder en oklarhet i hur ordet ”röja” ska tolkas och när en uppgift ska anses vara ”röjd”. En del menar att man med ”röja” helt enkelt avser att en uppgift har lämnats till någon annan utanför organisationen. Ett sådant röjande kan alltså vara tillåtet om handlingen inte var hemlig. Denna definition kallas *tekniskt röjd* och används av eSam (eSam, 2015; eSam, 2016; eSam, 2018; eSam, 2019). Andra menar att ordet ”röja” tar sikte på att man har lämnat en sekretessbelagd uppgift till någon annan i strid mot lagen. Hur man tolkar begreppet kan spela roll för om det kan anses vara tillåtet eller inte att lämna information till en molntjänstleverantör överhuvudtaget. Denna definition kallas *faktiskt röjd* och används av Göteborgs Stad av SKR (Sveriges Kommuner och Regioner, 2019; Sveriges Kommuner och Regioner, 2019; Sveriges Kommuner och Regioner, 2019)

2. Kravet på att göra en prövning av enskilda uppgifter (sekretessprövning)

En annan fråga som aktualiseras i samband med molntjänster är hur en offentlig verksamhet ska hantera kravet på att bedöma enskilda uppgifter genom en skadeprövning innan en uppgift lämnas ut. Ett överlämnande till en molntjänstleverantör innebär ju per automatik att en stor mängd uppgifter förs över till leverantören på ett sådant sätt att skadeprövning av enskilda uppgifter omöjliggörs.

Istället krävs att någon form av schabloniserad bedömning sker av om uppgifterna typiskt sett är offentliga eller hemliga samt om uppgifterna kommer att vara skyddade på ett sådant sätt att skyddsintresset inte skadas av överlämnandet.

3. Utländska myndigheters möjlighet att bereda sig tillgång till information

Ytterligare en faktor som komplicerarat diskussionen om molntjänster är frågan om vilken påverkan utländsk lagstiftning kan få om det i tjänsteleverantörens hemvist finns nationella regler som möjliggör för utländska myndigheter att få åtkomst till sekretessbelagd information. Frågan om överlämnande till utländska myndigheter är särskilt reglerad i OSL.

Göteborgs Stads bedömning

Stadsledningskontoret, genom stadsjuristerna, har haft att ta ställning till de aktuella frågeställningarna i förhållande till ett specifikt system, Microsoft Office 365 (O365) (Stadsledningskontoret, 2017; Stadsledningskonret, 2019). Slutsatserna sammanfattas endast i korthet men bifogas i sin helhet, *se bilaga 1*.

1.Röjandefrågan

När det gäller själva begreppet *röjande* så tolkar stadsledningskontoret ordet så att det anses ta sikte på när sekretessbelagda uppgifter avslöjas utan stöd i lag. Stadsledningskontorets bedömning är att ett röjande i offentlighets- och sekretesslagens mening sker när uppgifterna lämnas över till leverantören oavsett om leverantören tar del av informationen eller inte. Det är tillräckligt att leverantören har en faktisk åtkomst till uppgifter som kan vara sekretessreglerade för att de ska anses röjda. Faktisk tillgång har ansetts föreligga även vid krypterad information när Microsofts personal och dess

underleverantörer har tillgång till krypteringsnycklar. Genom att tekniskt och avtalsmässigt säkerställa att ingen, verken leverantör eller underleverantör, får tillgång till Göteborgs Stads information utan föregående sekretessprövning ska information som lagras i Office 365 inte anses röjd.

2. Kravet på att göra en prövning av enskilda uppgifter (sekretessprövning)
Eftersom leverantören inte har åtkomst till uppgifterna så föreligger i praktiken inget krav på att vidta någon sekretessprövning. I tjänsten Office 365 hanteras inte heller någon känslig information (klass II) dvs. ingen information som lyder under absolut sekretess utan endast information där det är Göteborgs Stad som har att bedöma om uppgifterna kan lämnas ut utan skada. Genom att ha ett obligatoriskt informationsklassningssystem inom Göteborgs Stad säkerställs att de förvaltningar och bolag som använder tjänsten har tagit ställning till informationens sekretessnivå innan information överförs till Office 365.

3. Utländska myndigheters möjlighet att bereda sig tillgång till information
Frågan om utländska myndigheters möjlighet att bereda sig tillgång till information är prövad i förhållande till CLOUD Act[3]. Där gör stadsledningskontoret följande bedömning:

”När det gäller frågan om CLOUD Acts betydelse bedömer stadsledningskontoret att uppgifter som omfattas av sekretess som överförts till O365 inte ska anses som röjda, med mindre att en amerikansk myndighet getts *faktisk åtkomst* till uppgifterna inom ramen för ett förfarande för CLOUD Act, samtidigt som dessa uppgifter i motsvarande fall inte skulle få lämnas ut till en svensk myndighet. Genom att sannolikheten är så liten att en amerikansk myndighet kommer att ges faktisk åtkomst till sådana uppgifter bedömer stadsledningskontoret att CLOUD Act inte hindrar att Intraservice fortsätter att införa O365 i hela staden.”

SOU 2021:1 Säker och kostnadseffektiv it-drift – rättsliga förutsättningar för utkontraktering

Syfte och lagändringar som möjliggör en lösning av sekretessfrågan
I januari 2021 presenterades delbetänkandet rörande säker och kostnadseffektiv it-drift – rättsliga förutsättningar för utkontraktering. I delbetänkandet presenteras en lösning av frågeställningarna rörande sekretesslagstiftningen i form av två konkreta lagförslag.

Syftet med delbetänkandet var att ”skapa bättre förutsättningar för den offentliga förvaltningen att få tillgång till säker och kostnadseffektiv it-drift genom antingen samordnad statlig it-drift eller genom tydligare rättsliga förutsättningar för att kunna anlita privata leverantörer av it-drift.”

I betänkandet avses med utkontraktering när en verksamhetsutövare lägger ut hela eller delar av sin it-drift på en extern aktör. I betänkandet konstateras inledningsvis att ”en säker och kostnadseffektiv it-drift är en förutsättning för den offentliga förvaltningens digitalisering. Statliga myndigheter, kommuner och regioner ansvarar för att verksamhetens it-driftslösningar stödjer en effektiv verksamhetsutveckling och uppfyller

[3] Se tidigare avsnitt om amerikansk lagstiftning

krav på säkerhet (säkerhetsskydd, sekretess och dataskydd) och kostnadseffektivitet. it-drift kan bedrivas i egen regi, genom utkontraktering till tjänsteleverantör eller genom samordnad it-drift. Vilken it-driftslösning som är den mest lämpade beror på verksamhetens uppdrag och vilka uppgifter som hanteras i verksamheten".

I delbetänkandet redovisat en undersökning som gjorts bland 158 svarande myndigheter. I undersökningen har 33, 32 och 95 procent av myndigheterna uppgett att de använder någon form av IaaS[4], PaaS[5]- respektive SaaS[6]-tjänst. I Myndigheten för samhällsskydd och beredskaps rapport *Outsourcing av it-tjänster i kommuner* (2014) uppgav 80 procent av drygt 120 kommuner att de utkontrakterat it-tjänster (MSB, 2014).
Ett slutbetänkande kommer presenteras senast den 15 oktober 2021 och det kommer att fokusera på en samordnad statlig it-drift och förutsättningarna för det. "en säker och kostnadseffektiv it-drift är en förutsättning för den offentliga förvaltningens digitalisering. Statliga myndigheter, kommuner och regioner ansvarar för att verksamhetens it-driftslösningar stödjer en effektiv verksamhetsutveckling och uppfyller krav på säkerhet (säkerhetsskydd, sekretess och dataskydd) och kostnadseffektivitet. it-drift kan bedrivas i egen regi, genom I delbetänkandet redovisat en undersökning som gjorts bland 158 svarande myndigheter. I undersökningen har 33, 32 och 95 procent av myndigheterna uppgett att de använder någon form av utkontraktering.

Delbetänkandet och sekretessfrågorna

1. Röjandefrågan
I delbetänkandet görs bedömningen att med röjande avses all typ av överlämnande av information, såväl tillåten som otillåten. Därav följer att det inte krävs att mottagaren har tagit del av uppgifteren för att den ska betraktas som röjd. Har en uppgift lämnat organisationen så har den röjts oavsett om mottagaren fått faktiskt tillgång eller ej. Delbetänkandet menar att det inte spelar någon roll för bedömningen av röjandefrågan om det finns en avtalad sekretess eller om uppgiften är krypterad eller pseudonymiserad. Detta eftersom det dels inte finns några nu kända säkerhetsåtgärder som gör det omöjligt i teori och praktik för tjänsteleverantören att få del av uppgifterna och dels då det inte heller är lätt för myndigheterna att kunna verifiera säkerhetsåtgärderna. (En annan sak är att avtalad sekretess eller säkerhetsåtgärder kan spela roll vid skadebedömningen.)

2. Kravet på att göra en prövning av enskilda uppgifter (sekretessprövning)
Utifrån den tolkning av röjandebegreppet som görs i delbetänkandet krävs, för att en utkontraktering ska vara förenlig med OSL, att utlämnande sker efter en av myndigheten utförd skadeprövning som utmynnat i slutsatsen att uppgifterna kan lämnas ut alternativt att så kan ske med stöd av en sekretessbrytande bestämmelse. Delbetänkandet konstaterar att den prövning som sker vid beslut om outsourcing inte är samma som när någon begär ut en allmän handling. Delbetänkandet anser inte att det finns några betänkligheter mot att en myndighet gör mer övergripande skadeprövningar för att konstatera om det finns något hinder mot att uppgifter lämnas ut eller inte och att en utkontraktering av it-drift därmed kan basera sig på ett mer schablonmässigt övervägande. Delbetänkandet skiljer dock på

[4] IaaS – Infrastructure as a Service
[5] PaaS - Plattform as a Service
[6] SaaS – Software as a Service

möjligheterna beroende på graden av sekretess.

Delbetänkandet menar att utrymmet för en utkontraktering är vidare i de fall uppgifterna är sådana att man utgår ifrån att offentlighet råder om det inte kan antas att skada uppkommer om uppgiften röjs. Sekretessen är i dessa fall svag. Förekomsten av ett sekretessavtal mellan den utkontrakterande myndigheten och en privat tjänsteleverantör kan då också tillmätas betydelse vid skadeprövningen.

I de fall då en uppgift antas vara sekretessbelagd om det inte står klart att den kan lämnas ut utan skada krävs det mer för att en utkontraktering ska få ske. I dessa fall är det tveksamt om avtalad sekretess är tillräckligt. Om däremot mottagarna av uppgifterna omfattas av en straffsanktionerad tystnadsplikt borde skadeprövningen oftare kunna mynna ut i att utkontraktering är möjlig. Kryptering och andra tekniska åtgärder som försvårar för personalen hos en tjänsteleverantör att ta del av uppgifterna bör också enligt betänkandet kunna tillmätas betydelse vid skadeprövningen.

När det gäller uppgifter som omfattas av absolut sekretess finns det ingen möjlighet för myndigheten att göra någon skadeprövning. I de fall uppgifter som omfattas av absolut sekretess ska lämnas till en leverantör måste det därmed finnas en sekretessbrytande bestämmelse som tillåter utlämnandet. Finns det ingen tillämplig sekretessbrytande bestämmelse så saknas det stöd för att lämna uppgifter till en leverantör. Eftersom någon bedömning av skada inte ska ske spelar här ingen roll om det finns krypteringsmöjligheter eller andra säkerhetslösningar.

3. Utländska myndigheters möjlighet att bereda sig tillgång till information

Delbetänkandets synsätt innebär att en uppgift är röjd redan genom att den har lämnats till en leverantör. Röjandet kan vara tillåtet eller otillåtet, men oaktat så sker röjandet från myndigheten till leverantören och inte från myndigheten direkt till en utländsk myndighet. Själva prövningen av om ett tillåtet röjande är förenligt med lag måste alltså redan ha skett före överlämnandet till leverantören. Delbetänkandet menar att bestämmelsen i OLS endast tar sikte på den situationen att en myndighet lämnar en uppgift direkt till en utländsk myndighet. Bestämmelsen är därför inte tillämplig. Eftersom uppgifterna redan är röjda för leverantören menar delbetänkandet också att det inte är relevant ur ett OSL-perspektiv att se till vad som eventuellt kan hända i ett senare led mellan leverantören och eventuell utländsk myndighet eftersom leverantören inte omfattas av reglerna i OSL. Om en leverantör måste överlämna uppgifterna vidare till en utländsk myndighet så blir det därför inte ett röjande enligt sekretesslagens mening. Överlämnandet kan dock vara otillåtet enligt annan reglering, tex. tystandspliktslagen, eller genom att det blir ett avtalsbrott.

Delbetänkandets förslag till lösning;

Delbetänkandet föreslår följande:

- I OSL införs en sekretessbrytande bestämmelse som tar sikte på fall då uppgifter lämnas ut till företag eller en annan enskild (tjänsteleverantör) eller till en annan myndighet som har i uppdrag att utföra endast teknisk bearbetning eller teknisk lagring av de uppgifter som lämnas ut för den utlämnande myndighetens räkning.

- Ett utlämnande– enligt den föreslagna bestämmelsen – inte ska ske om övervägande skäl talar för att det intresse som sekretessen ska skydda har företräde framför intresset av utkontraktering.
- Att meddelarfriheten enligt tryckfrihetsförordningen och yttrandefrihetsgrundlagen inskränks för den krets av personer som träffas av tystnadspliktslagen.

Den sekretessbrytande bestämmelsen

Den avgränsning som gjorts innebär att den nya sekretessbrytande bestämmelsen endast träffar den hantering av uppgifter som sker *för myndighetens räkning*. Sådan hantering av uppgifter som en privat tjänsteleverantör utför för ändamål kopplade till den egna verksamheten, exempelvis utvecklingen av egna produkter och tjänster baserat på hantering av kundens uppgifter, faller utanför tillämpningsområdet. Det betyder inte att uppgifter aldrig kan lämnas ut till leverantören i sådana syften men prövningen får ske utifrån de regler som gäller idag. Det får inte heller glömmas att förenlighet med annan lagstiftning alltjämt också måste beaktas vid utkontraktering, exempelvis dataskyddslagstiftning eller säkerhetsskyddslagstiftning.

Förslaget till sekretessbrytande bestämmelse tar sikte på såväl utkontraktering av it-drift till privata tjänsteleverantörer som utkontraktering av it-drift myndigheter emellan.

Intresseavvägningen

En utkontraktering innebär ett utlämnande av uppgifter som sker på myndighetens eget initiativ och är inte att betrakta som ett utlämnande med grund i offentlighetsprincipen. Utlämnandet syftar istället till att åstadkomma en fungerande it-driftlösning för myndigheten. Vid utkontraktering är det inte möjligt att närmare granska varje enskild uppgift som ska lämnas ut. Prövningen måste istället bli mer övergripande. Det kan vara förenat med svårigheter eftersom det i en stor mängd information kan finnas uppgifter som regleras av olika sekretessbestämmelser. En intresseavvägning kan skapa förutsättningar för myndigheten att göra en mer övergripande prövning och skulle därmed innebära en förenkling för myndigheterna jämfört med dagens reglering som i princip kräver skadebedömningar på uppgiftsnivå.

Om delbetänkandets förslag antas skulle det bli tydligare att sådana schablonmässiga överväganden får göras. Samtidigt uppges i delbetänkandet att det finns ett behov av att skapa en reglering som möjliggör hänsynstagande till sekretessintresset i det enskilda fallet där det framstår som nödvändigt. Detta kan åstadkommas genom att den utkontrakterande myndigheten åläggs att, innan ett beslut fattas, göra en avvägning mellan intresset av en utkontraktering och de intressen som sekretessen avser att skydda. Kravet på intresseavvägning skulle innebära att myndigheterna tvingas att, i sina överväganden inför ett beslut om utkontraktering av it-drift, beakta sekretessintresset. Kravet på intresseavvägning innebär också ytterst att ansvar för brott mot tystnadsplikt enligt 20 kap. 3 § brottsbalken kan komma i fråga, i de fall utkontraktering skett trots att sekretessintresset vägde tyngre.

Delbetänkandet anger inte hur själva intresseavvägningen ska gå till men uppger att ”vilka intressen som föranlett sekretessen, med vilken styrka som sekretessen är reglerad liksom uppgifternas art och omfattning är faktorer av betydelse. Det kan också vara av betydelse vilken sekretess eller tystnadsplikt som gäller hos mottagaren av uppgifterna, och vilken styrka den sekretessen eller tystnadsplikten har.

Delbetänkandet anger också att ”Dataskyddsregelverket innebär i viss utsträckning en tystnadsplikt för personuppgifter som också kan vara relevant att ta i beaktande i bedömningen. Detsamma gäller förekomsten av avtalsreglerad tystnadsplikt samt förekomsten av tekniska säkerhetsåtgärder, som t.ex. kryptering, som gör det svårare för någon obehörig att ta del av uppgifterna.”

Avskaffad meddelarfrihet för leverantörer som omfattas av Tystnadspliktslagen

Syftet med Tystnadspliktslagen var att den tystnadsplikt som i lagen åläggs tjänsteleverantörer som verkar för det allmänna så långt som möjligt skulle överensstämma med den tystnadsplikt som gäller enligt OSL för myndigheten och dess egen personal. Det innebär att tystnadsplikt hos tjänsteleverantören gäller för en uppgift som hos myndigheten skulle ha omfattats av sekretess till skydd för allmänna intressen enligt 11 kap. 4 a § OSL eller till skydd för enskilds personliga och ekonomiska förhållanden enligt 40 kap. 5 § OSL. Den grundlagsstadgade meddelarfriheten innebär en rätt att lämna uppgifter, även sådana som omfattas av sekretess eller tystnadsplikt, för offentliggörande i tryckt skrift, program eller genom tekniska upptagningar. Meddelarfriheten omfattar alltså inte bara dem som verkar inom det offentliga utan även dem som har tystnadsplikt enligt Tystnadspliktslagen.

I OSL finns dock vissa bestämmelser som innebär att tystnadsplikten väger tyngre än meddelarfriheten men en sådan inskränkning finns inte enligt Tystnadspliktslagen. Delbetänkandet resonerar som så ” Offentliga funktionärers tystnadsplikt för uppgift om enskilds personliga eller ekonomiska förhållanden som hanteras i verksamhet för endast teknisk bearbetning eller teknisk lagring inskränker meddelarfriheten (40 kap. 5 och 8 §§ OSL). Meddelarfriheten är även inskränkt för uppgift som är sekretessreglerad av hänsyn till ett allmänt intresse enligt en bestämmelse som har företräde framför meddelarfriheten och som hanteras i verksamhet för endast teknisk bearbetning eller teknisk lagring för en annan myndighets räkning. Det gäller dock inte om en annan primär sekretessbestämmelse till skydd för samma intresse, som inte har företräde framför meddelarfriheten, är tillämplig hos den uppgiftsmottagande myndigheten (jfr 11 kap. 4 a och 8 §§ OSL). Det kan ifrågasättas om det är en rimlig ordning att den tystnadsplikt som gäller för de offentliga funktionärerna har företräde framför meddelarfriheten samtidigt som meddelarfriheten har företräde framför den tystnadsplikt som följer av tystnadspliktslagen.”

Eftersom den föreslagna sekretessbrytande bestämmelsen dessutom syftar till att utöka möjligheterna till utkontraktering föreslår delbetänkandet att meddelarfriheten inskränks för den krets av personer som omfattas av Tystnadspliktslagen.

Göteborgs Stads bedömning

Göteborgs Stad har lämnat remissvar (Kommunstyrelsen Göteborgs Stad, 2021) och tillstyrker delbetänkandets författningsförslag att införa en sekretessbrytande bestämmelse i offentlighets- och sekretesslagen (2009:400) avseende utkontraktering av teknisk bearbetning och teknisk lagring av uppgifter och tillägget avseende inskränkt meddelarfrihet för den krets av personer som träffas av lagen (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgiften. Göteborgs Stad anser den föreslagna sekretessbrytande bestämmelsen inte bara bör utan ska kompletteras med central vägledning och stöd till statliga myndigheter, kommuner och regioner. Det är positivt att den sekretessbrytande bestämmelsen villkoras så att en avvägning mellan

intresset av en utkontraktering och de intressen som sekretessen avser att skydda beaktas innan utkontraktering.

Molntjänster ur ett dataskyddsperspektiv

Relevant dataskyddslagstiftning i sammandrag

Sammanfattning

Fram till sommaren 2020 var det möjligt att ingå avtal med amerikanska leverantörer under Privacy Shield – efter ett beslut från EU-kommissionen. Under 2020 underkände emellertid EU-domstolen EU-kommissionens beslut med hänvisning till att det i USA saknas tillräckligt skydd för personuppgifter och möjligheter för de registrerade att ta tillvara sina rättigheter. Framför allt sågs de lagar som möjliggör för amerikanska myndigheter att tillkräva sig åtkomst till personuppgifter från leverantörer som svårförenliga med dataskyddsförordningen. Domen har efterlämnat en rad oklarheter och tolkningsfrågor rörande förenligheten med lagstiftningen, även i de avtalsrelationer som tidigare ingåtts under Privacy Shield. EDPB avser att publicera en vägledning som kan komma att klargöra rättsläget. Förhandlingar mellan EU-kommissionen och USA har också startat för att söka komma till en ny lösning. Det finns i dagsläget ett antal frågor är oklara vilka en personuppgiftsansvarig behöver ta ställning till och agera efter.

Syftet med dataskyddsförordningen

Dataskyddsförordningen (DSF) är till för att skydda enskildas grundläggande fri- och rättigheter, särskilt rätten till skydd av personuppgifter. DSF är en förordning som gäller inom hela EU. Syftet med en gemensam reglering är att säkerställa ett likvärdigt skydd och samma rättigheter för att på så sätt möjliggöra ett fritt följde inom hela EU/EES. DSF är tillämpligt på de behandlingar som görs av verksamheter etablerade inom unionen, oavsett om uppgifterna behandlas inom eller utanför unionens geografiska område. Under vissa omständigheter är förordningen även tillämplig på aktörer utanför unionen när behandlingarna är riktade mot registrerade inom unionen.

Det finns många bestämmelser i DSF som berör användningen av molntjänster och som måste beaktas. De frågor som dock framför allt har aktualiserats det senaste halvåret handlar om överföring av uppgifter till USA. Sådan överföring kunde tidigare ske med EU-kommissionens godkännande men spelplanen ritades delvis om efter en dom i EU-domstolen sommaren 2020. Nedanstående text avser att försöka skapa klarhet i problematiken på en övergripande nivå.

Särskilda regler när personuppgifter överförs till ett land utanför EU/EES – ett ”Tredjeland”

Inom EU/EES värnas den personliga integriteten genom DSF men utanför finns inte motsvarande generella regler. Vissa länder har ett starkt skydd och möjligheter för fysiska personer att ta tillvara sina rättigheter genom rättsliga förfaranden medan andra länder har mycket svaga rättigheter för individen. (De fysiska personer vars personuppgifter är föremål för behandling kallas nedan för ”**de registrerade**”.)

För att skydda de registrerades rättigheter och inte urholka det skydd som förordningen avser att ge, är huvudregeln att överföring av personuppgifter till tredjeland är förbjuden. I DSF finns dock ett antal undantag som kan göra det tillåtet att överföra personuppgifter till ett tredjeland.

Undantag till förbudet av tredjelandsöverföringar genom EU-kommissionens beslut om adekvat skyddsnivå

EU-kommissionen kan fatta beslut om att ett land har en tillräcklig hög skyddsnivå för att de registrerades rättigheter ska vara skyddade, så kallad adekvat skyddsnivå. Om EU-kommissionen fattat ett sådant beslut så är överföring av personuppgifter möjlig utan att något tillstånd behövs.

För att EU-kommissionen ska kunna fatta ett beslut om adekvat skyddsnivå måste ett antal förutsättningar beaktas. Dessa är bland annat i) det tredjelandets efterlevnad av rättsstatsprincipen och respekten för mänskliga rättigheter och grundläggande friheter, att det finns relevant lagstiftning och regler samt faktiska och verkställbara rättigheter för registrerade, inbegripet tillgång till effektiv administrativ och rättslig prövning för de registrerade vars personuppgifter överförs, ii) att det finns en eller flera effektivt fungerande oberoende tillsynsmyndigheter i det tredjelandet som har ansvar för att säkerställa och kontrollera att dataskyddsregler följs samt innehar lämpliga verkställighetsbefogenheter och möjligheter att lämna råd och assistans till de registrerade för att kunna tillvarata sina rättigheter samt iii) om det finns internationella åtaganden som det berörda tredjelandet gjort avseende skyddet av personuppgifter.

EU-kommissionen har fattat beslut om att skyddsnivån i ett antal länder är adekvat. Dessa länder är Andorra, Argentina, Bailiwick of Guernsey, Färöarna, Isle of Man, Israel, Japan, Jersey, Nya Zeeland, Schweiz och Uruguay. EU-kommissionen har också bedömt att Kanada omfattas av en adekvat skyddsnivå under förutsättning att deras lagstiftning för skydd av personuppgifter i privat sektor är tillämplig på mottagarens personuppgiftsbehandling.

Avseende USA antog kommissionen ett beslut år 2000. Beslutet innebär inte någon generell möjlighet till överföring av uppgifter till USA utan endast till de organisationer som anslutit sig till principerna om Safe Harbor och som fanns upptagna i en särskild förteckning som offentliggjordes och förvaltades av USA:s handelsministerium. Det var alltså ett slags system för självcertifiering där de organisationer som anslöt sig åtog sig att upprätthålla ett visst skydd för personuppgifter. År 2015 ogiltigförklarade EU-domstolen beslutet i en uppmärksammad dom – Schrems I.

Efter nya förhandlingar mellan EU-kommissionen och USA beslutade kommissionen på nytt om att adekvat skyddsnivå var uppnådd för de organisationer som anslöt sig till ett nytt självcertifieringssystem, kallat Privacy Shield. Även detta beslut är numera upphävt sedan 2020 av EU-domstolen genom den uppmärksammade domen Schrems II. Privacy Shield går alltså inte länge att åberopa som grund för överföring av uppgifter till USA.

Det finns också andra undantag från förbudet om tredjelandsöverföring som kan tillämpas om det inte finns något beslut om adekvat skyddsnivå. Överföring kan då istället ske efter att andra lämpliga skyddsåtgärder vidtagits och på villkor att lagstadgade rättigheter för registrerade och effektiva rättsmedel för registrerade finns att tillgå. Eftersom andra

undantag påverkas av domen i Schrems II är det först relevant att redogöra för vad domen handlade om.

EU-domstolens avgörande i Schrems II-målet

Målet behandlade den österrikiska medborgaren Max Schrems bestridande av Facebooks europeiska dotterbolag Facebook Ireland:s rätt att föra över hans personuppgifter till USA. Målet kom att handla om den massöverföring till USA som Facebook Ireland gjorde av europeiska medborgares personuppgifter. Målet inleddes vid irländsk domstol som hänsköt frågan till EU-domstolen. Den 16 juli 2020 ogiltigförklarade EU-domstolen i sin dom (C-311/18 Schrems II) EU-kommissionens beslut om att adekvat skyddsnivå säkerställdes genom Privacy Shield.

Ogiltigförklaringen berodde i korthet på att skyddet för personuppgifter i Privacy Shield var för svagt och inte erbjöd de registrerade något skydd mot de övervakningsprogram som enligt amerikansk lagstiftning gör det möjligt för amerikanska myndigheter att skaffa sig åtkomst till europeiska medborgares personuppgifter. Domstolen ansåg att de amerikanska lagarna, så som FISA 702 och Executive Order 12333, inte är förenliga med DSF proportionalitetsprincip eftersom bestämmelserna går utöver vad som är nödvändigt i ett demokratiskt samhälle.

EU-domstolen ansåg inte heller att europeiska medborgare hade tillgång till effektiva rättsmedel eller rätt till prövning. De registrerade kunde därmed inte ta tillvarata sina rättigheter gentemot de amerikanska myndigheter som bedrev övervakningen. Eftersom kraven på en adekvat skyddsnivå inte kunde säkerställas beslutade EU-domstolen att med omedelbar verkan ogiltigförklara EU-kommissionens beslut om att Privacy Shield utgjorde grund för adekvat skyddsnivå.

Domstolen förtydligade också att det krävs samma nivå av skydd för fysiska personer oavsett vilken grund enligt DSF som åberopas för överföring av personuppgifter, det vill säga oavsett om det handlar om ett adekvansbeslut av EU-kommissionen eller något annat undantag där det är den personuppgiftsansvarige som ska göra bedömningen.

Av domen framgår att för att kravet på ”adekvat skyddsnivå”, ska vara uppfyllt krävs inte att skyddsnivån i det tredjelandet är identisk med det skydd som garanteras inom unionen men det ska säkerställa en nivå som är väsentligen likvärdig med det skydd som ges i DSF.

EU-domstolen ogiltigförklarade inte andra skyddsåtgärder som är möjliga att åberopa som undantag för tredjelandsöverföring. Domen förtydligade dock att ytterligare skyddsåtgärder kan vara nödvändiga för att garantera att kraven i DSF uppfylls.

Domen innebar att alla verksamheter som åberopat Privacy Shield som rättslig grund för tredjelandsöverföring omedelbart behövde upphöra med överföringen alternativt hitta en annan rättslig rund, eftersom överföringen i och med domen blev lagstridig.

Andra lämpliga skyddsåtgärder

En annan möjlighet för tillåten överföring är att den personuppgiftsansvarige vidtar lämpliga skyddsåtgärder. Den möjlighet som främst står till buds är att ingå ett särskilt avtal med mottagaren av uppgifterna genom användning av ”standardavtalsklausulerna” (SCC) som EU-kommissionen har fastställt. Ett krav för att tillämpa SCC som lämplig

skyddsåtgärd är att lagstadgade rättigheter för registrerade och effektiva rättsmedel för registrerade finns tillgängliga.

Resonemanget i domen Schrems II ställer krav på att den personuppgiftsansvarige gör en bedömning av om lagstiftningen i det mottagande landet garanterar ett väsentligen likvärdigt skydd som gäller enligt DSF. För det fall ett väsentligen likvärdigt skydd inte kan åstadkommas kan standardavtalsklausulerna behöva kompletteras med ytterligare skyddsåtgärder för att utgöra en giltig grund för överföring.

Schrems-II domen har skapat stor osäkerhet kring i vilken utsträckning SCC kan användas för överföringar till USA överhuvudtaget med tanke på domstolens resonemang om amerikansk lagstiftning och bristen på skydd för de registrerade i landet. Den personuppgiftsansvarige och en leverantör kan ju inte avtala om att leverantören inte ska vara bunden av amerikansk lagstiftning. EU-domstolen poängterar dessutom att de europeiska tillsynsmyndigheterna har en skyldighet att förbjuda överföring med hjälp av SCC till länder som inte erbjuder tillräckligt skydd för personuppgifter.

Särskilda situationer och enstaka fall

Utöver ovanstående undantag finns ytterligare undantag för särskilda situationer och enstaka fall. Överföring är i vissa fall möjlig då den inte är repetitiv, om den endast gäller ett begränsat antal registrerade, och om den är nödvändig för ändamål som rör den personuppgiftsansvariges berättigade intressen och den registrerades intressen i sådana fall inte väger tyngre. Samtliga omständigheter kring överföringen ska beaktas och även i detta fall ska lämpliga skyddsåtgärder finnas på plats. Både tillsynsmyndigheten och de registrerade ska informeras om överföringen och om de tvingande berättigade intressen som personuppgiftsansvarige vill uppnå. EDPB har tagit fram riktlinjer som beskriver tillfällen då denna undantagsbestämmelse kan bli aktuell.

Europeiska dataskyddsstyrelsens vägledning

Med anledning av Schrems II-domen har den europeiska dataskyddsstyrelsen (EDPB) publicerat två vägledningar. EDPB:s vägledningar är inte bindande men tänkta att fungera som en slags rekommendation. Den första rekommendationen redogör för hur den personuppgiftsansvarige ska gå tillväga för att avgöra om ett tredjeland erbjuder ”ett väsentligen likvärdigt skydd”. Den andra rekommendationen innefattar en beskrivning om vilka ”ytterligare skyddsåtgärder” som kan användas för att komplettera standardavtalsklausulerna.

EDPB menar att det kan vara nödvändigt att kombinera olika åtgärder. Om det är mottagarlandets nationella lagar som är otillräckliga kan åtgärderna behöva vara sådana att de i praktiken säkerställer att utländska myndigheter inte kan få åtkomst. Det kan därmed innebära att varken kontraktuella eller organisatoriska åtgärder är tillräckliga utan dessa kan behöva kombineras med tekniska åtgärder, så som kryptering eller pseudonymisering, där nyckeln inte är åtkomlig för mottagaren av personuppgifterna. Därmed kan inte heller uppgifterna lämnas ut till en utländsk myndighet. Å andra sidan kan den typen av tekniska åtgärder i princip göra vissa typer av tjänster obrukbara för den personuppgiftsansvarige.

Vägledningen rörande ytterligare skyddsåtgärder har varit på remiss men ett antagande har dröjt. Vägledningen har fått mycket kritik för att ha tolkat Schrems II allt för vittgående. Rättsläget är därmed alltjämt till viss del oklart. Å andra sidan så måste den

personuppgiftsansvarige som inte kan säkerställa ett tillräckligt skydd för personuppgifter avbryta överföringen till tredjeland. Även tillsynsmyndigheten har möjlighet att avbryta överföringen om skyddet för personuppgifter och de registrerades rättigheter inte säkerställts.

EU-kommissionens beslut om SCC

2021-06-04 beslutade EU-kommissionen om två nya Standardavtalsklausuler (SCC) för tredjelandsöverföringar. Förvaltningen behöver ta ställning till hur detta påverkar Kommungemensamma interna tjänster och molnlösningar.

När överförs personuppgifter till ett tredjeland?

Frågan om vad som ska anses vara en tredjelandsöverföring är inte uttryckligen definierad i lagstiftningen. I princip är dock innebörden att en överföring av personuppgifter sker till tredjeland när personuppgifter blir tillgängliga för någon i ett land utanför EU/EES-området. Uppgifterna måste alltså inte aktivt ha skickats till ett annat land utan det räcker att någon i ett tredjeland kan ta del av uppgifterna. EDPB anser att en fjärråtkomst från tredjeland eller en lagring i en molntjänst utanför EU/EES ska betraktas som tredjelandsöverföringar. Då e-post sänds till en mottagare i ett annat land är ett annat exempel på en tredjelandsöverföring liksom situationen då en supporttjänst i ett annat land ges tillgång till information som lagras inom EU/EES enligt tillsynsmyndigheten. Samtidigt så har EU-domstolen i ett rättsfall, till viss del motsatsvis, konstaterat att en publicering av uppgifter på internet som blev tillgängliga i hela världen inte skulle anses vara en tredjelandsöverföring, så länge webbhotellsleverantören var etablerad inom unionen. bestå. Enligt uppgift från tillsynsmyndigheten så är frågan om vad som utgör en överföring av personuppgifter till tredjeland för närvarande under behandling inom EDPB, bland annat inom ramen för kommande riktlinje.

Det förs en diskussion om Schrems II-domen ska tolkas så att en tredjelandsöverföring sker redan genom att amerikanska bolag kan bli beordrade att lämna information till amerikanska myndigheter. Frågan berördes i tidigare nämnd SOU 2021:1 och i den görs tolkningen att det inte är frågan om tredjelandsöverföring när personuppgifter behandlas uteslutande inom EU, även om personuppgiftsbiträdet är bundet av tredjelandets lagstiftning. Utredningen anser dock att en tredjelandsöverföring föreligger när personuppgiftsansvarig eller ett personuppgiftsbiträde behandlar personuppgifter genom användning av utrustning som finns i tredjeland. I delbetänkandet står att ”oavsett hur kort eller lång tid utrustningen har använts, samt om uppgifterna är krypterade eller pseudonymiserade, så ska det alltjämt vara fråga om personuppgifter och en överföring av sådana uppgifter. Detta innebär att även om personuppgifterna konstant är under den personuppgiftsansvariges kontroll är det fråga om en överföring när de förs över till tredjeland eller en internationell organisation. Någon tredjelandsöverföring ska dock inte anses ha skett förrän uppgifter rent faktiskt överförs från en leverantör till ett tredjeland.

Ytterst så kan inte frågan besvaras av svenska lagstiftare. DSF är en EU-rättslig reglering och därför är det utanför nationell kontroll hur rättsutvecklingen i frågan kommer att ske. (Även om den svenska tillsynsmyndigheten för visso är med inom EDPB och på det sättet kan påverka tidigare nämnd vägledning när den slutligen antas.) I slutändan är det dock EU-domstolen som avgör hur dataskyddsförordningens bestämmelser ska tolkas.

Den personuppgiftsansvariges omsorgsplikt vid val av lämpligt personuppgiftsbiträde

Vid den tolkning av tredjelandsöverföringar, som redovisats i föregående punkt, så möter det inget hinder att anlita en amerikansk leverantör, så länge personuppgifterna behandlas uteslutande inom EU/EES. En fråga som då istället har väckts är om valet av en amerikansk leverantör, som uppenbarligen är bunden av amerikansk lagstiftning, är

olämplig utifrån den omsorgsplikt som den personuppgiftsansvarige har vid valet av personuppgiftsbiträde.

Tillsynsmyndigheten Integritetsmyndigheten, IMY, har i sitt remissvar över SOU 2021:1 redovisat sin uppfattning i frågan. Av yttrandet framgår att omsorgsplikten innefattar en riskbedömning för att bedöma om garantierna som biträdet presenterar är tillräckliga. IMY skriver att ”Riskbedömningen behöver göras i varje enskilt fall utifrån behandlingens art, omfattning, ändamål och riskerna för fysiska personers rättigheter och friheter. För att avgöra om personuppgiftsbiträdet kan ställa tillräckliga garantier måste den personuppgiftsansvariga göra en bedömning av bland annat personuppgiftsbiträdets expertkunskaper, pålitlighet och resurser. Den personuppgiftsansvariga bör vara särskilt uppmärksam om personuppgiftsbiträdet har verksamhetsställen i tredjeland eller för avsikt att delegera behandlingar till exempelvis underbiträden i tredjeland. IMY anser att den omständigheten att personuppgiftsbiträdet omfattas av tredjelands lagstiftning, enligt vilken personuppgifter kan komma att lämnas ut till det tredjelandets myndigheter i strid med bestämmelserna om tredjelandsöverföring enligt dataskyddsförordningen, är något som den personuppgiftsansvariga behöver ta i beaktande vid bedömningen om personuppgiftsbiträdet kan ge tillräckliga garantier. Skyldigheten för den personuppgiftsansvariga att endast använda sig av personuppgiftsbiträden som ger tillräckliga garantier enligt artikel 28.1 i dataskyddsförordningen är också något som den personuppgiftsansvariga kontinuerligt behöver följa upp, exempelvis genom revision eller inspektion om det är lämpligt.”

Frågor att beakta

Det är den personuppgiftsansvarige som ska ta ställning till om den personuppgiftsbehandling som sker lever upp till kravet på tillräckligt hög nivå och efterlevnaden av DSF. Den personuppgiftsansvarige har en ansvarsskyldighet och ska kunna bevisa följsamhet till lagen. Att inte följa lagstiftningen innebär en risk för att drabbas av såväl sanktioner som skadestånd, tvång att upphöra med överföringen och förtroendeskador.

Intraservice är personuppgiftsansvarig i förhållande till den egna behandlingen av personuppgifter men är också personuppgiftsbiträde i förhållande till Göteborgs Stads övriga förvaltningar och i förekommande fall bolag. De leverantörer som Intraservice har avtal med är därmed både personuppgiftsbiträden och underbiträden.

- Enligt Bilaga 1 till Regler om Kommungemensamma interna tjänster (Kommunstyrelsen, 2018), avseende Intraservice behandling av personuppgifter på uppdrag av nämnder och/eller styrelser stadgas följande:
  Intraservice får inte överföra några personuppgifter till land utanför EU/EES-området eller till land som inte omfattas av undantagen till förbud mot överföring till tredje land enligt Dataskyddsförordningen, utan att ha den Personuppgiftsansvariges skriftliga samtycke i förväg och ha säkerställt att sådan överföring sker i överensstämmelse med tillämplig lag.

Intraservice behöver därmed beakta frågorna för egen del men också överväga vilka skyldigheter som föreligger i rollen som personuppgiftsbiträde.

1. Är det frågan om en tredjelandsöverföring att anlita en amerikansk leverantör?
Den tolkning som tycks ha blivit den rådande är att så inte är fallet så länge behandlingen av personuppgifter sker uteslutande inom EU/EES (Integritetsskyddsmyndigheten, 2021, s. 4 (stycke 3)). Det betyder också att ingen fjärråtkomst från USA får vara möjlig. Det går inte med säkerhet att säga om denna tolkning kommer bestå. Frågan behandlas just nu inom ramen för kommande rekommendationer av EDPB. För att säkerställa att behandling uteslutande sker inom EU/EES måste detta tydligt framgå av avtalet mellan den personuppgiftsansvarige och leverantören (personuppgiftsbiträdet/underbiträdet). Först om en leverantör faktiskt skulle tvingas lämna uppgifter till amerikanska myndigheter sker en tredjelandsöverföring. Om biträdet överfört uppgifterna i strid med avtalet och lämnade instruktioner bör personuppgiftsbiträdet kunna hållas ansvarigt för den skada som drabbar den registrerade om överföringen saknade lagligt stöd.

Om den ansvarige hade vetskap om eller skäl att misstänka att personuppgiftsbiträdet överför personuppgifter till tredjeland trots att parterna avtalat om annat så bör dock den ansvarige inte kunna undkomma i alla fall visst ansvar. Detta eftersom den personuppgiftsansvarige bara kan undgå ansvar om denne kan visa att den inte på något sätt är ansvarig för den händelse som orsakade skadan. Här blir frågan om omsorgsplikten relevant enligt punkten 4 nedan.

2. Om det är frågan om en tredjelandsöverföring – går det att använda SCC?
Av Schrems II-domen framgår att SCC går att använda men endast om skyddsnivån är väsentligen likvärdig med det skydd som ges inom DSF. Domstolen konstaterade i domen att tillräckligt skydd för personuppgifter saknas i USA. Därmed behöver SCC förenas med ytterligare skyddsåtgärder för att uppnå tillräckligt skydd. Enligt det utkast till vägledning som EDPB publicerat så skulle det troligtvis krävas, förutom kontraktuella och organisatoriska åtgärder, att uppgifterna krypteras eller pseudonymiseras så leverantören inte själv kan få åtkomst till uppgifterna (och därmed inte heller kan lämna ut dem i läsbart skick). Vägledningen har ännu ej publicerats i sin slutliga version så viss osäkerhet finns om tolkningen kommer att bestå oförändrad.

3. Om det inte går att tillämpa SCC – finns det något annat tillämpligt undantag?
De undantag som finns i övrigt är inte direkt tillämpbara på överföring i större skala så som vid utkontraktering av it-drift men skulle möjligen kunna tillämpas vid enstaka eller unika fall efter analys av den specifika behandlingssituationen och de krav som kan vara förknippade därmed.

4. Strider det mot omsorgsplikten att välja ett personuppgiftsbiträde som är en amerikansk leverantör?
En sådan tolkning är möjlig och framförs som trolig i SOU 2021:1. EU-domstolen har inte tagit ställning till frågeställningen men den svenska tillsynsmyndigheten har uttalat sig i frågan. Tillsynsmyndigheten (Integritetsskyddsmyndigheten, 2021) betonar vikten av skyldigheten för den personuppgiftsansvariga att endast använda sig av personuppgiftsbiträden som ger tillräckliga garantier för skyddet av personuppgifter. Vilka garantier som omfattas av parternas avtal är viktigt men också andra omständigheter som biträdets expertkunskaper, pålitlighet och resurser. Tillsynsmyndigheten anser att den omständigheten att personuppgiftsbiträdet omfattas av tredjelands lagstiftning, enligt vilken personuppgifter kan komma att lämnas ut till det tredjelandets myndigheter i strid med bestämmelserna om tredjelandsöverföring enligt DSF, är något som den personuppgiftsansvariga behöver ta i beaktande vid bedömningen

om personuppgiftsbiträdet kan ge tillräckliga garantier. Riskbedömningen behöver göras i varje enskilt fall utifrån behandlingens art, omfattning, ändamål och riskerna för fysiska personers rättigheter och friheter.

Slutsatser Microsoft Office 365

Allmänt

En av leveransen Kommungemensamma interna tjänster är Office 365 som levereras via Microsoft. Nedan redovisas förvaltningens bedömning specifikt för den tjänsten.

Avtal

Det kommersiella avtalet är med Microsoft Irland, DPA är med Microsoft USA. (Advokatfirman Lindahl KB, 2021)

Data

Innehållsdata för majoriteten av tjänsterna lagras och bearbetas inom EU/EES, Diagnosdata behandlas och lagras i USA, Funktionsdata behandlas i EU/EES och USA, Support ges från hela världen. (Advokatfirman Lindahl KB, 2021; Intraservice, 2021; Intraservice, 2020)

OSL i relation till Office 365

Stadsjuristerna har i beskrivet att information är tekniskt röjd men inte faktiskt röjd och ger rekommendationen att endast information som klassats till 1 i konfidentialitet hanteras i Office 365 och att ingen sekretessreglerad information får hanteras i Office 365 (se Göteborgs Stads bedömning sid 19) promemorior (Stadsledningskontoret, 2017; Stadsledningskontoret, 2019).

Dataskydd i relation Office 365

Är det fråga om tredjelandsöverföring?
Ja.

I Microsofts *Online Services Data Protection Addendum (DPA)* står det under dataöverföringar

> *Kunddata och Personuppgifter som Microsoft behandlar å Kundens vägnar får inte överföras till, eller lagras och behandlas på en geografisk plats förutom enligt DPA-villkoren och de säkerhetsåtgärder som tillhandahålls nedan i detta avsnitt. Med beaktande av sådana säkerhetsåtgärder ger Kunden Microsoft i uppdrag att överföra Kunddata och Personuppgifter till USA eller något annat land där Microsoft eller dess Underbiträden är verksamma och att lagra och behandla Kunddata och Personuppgifter för att tillhandahålla Onlinetjänsterna, med undantag för beskrivningen på andra ställen i DPA-villkoren.* (Microsoft, 2020)
>
> Enligt juridisk analys å är det fråga om tredjelandsöverföring (Advokatfirman Lindahl KB, 2021, s. 1.2)

Detta innebär att innehållsdata, diagnosdata och funktionsdata enligt avtal överförs till tredjeland.

Om det är frågan om en tredjelandsöverföring – går det att använda Standardklausuler?

Standardklausuler går att använda enligt dataskyddsförordningen (Europaparlamentet och Europiska unionens råd, 2016, s. Artikel 46), EU-domstolens dom i mål C-311/18 (Court of Justice of the European Union (CJEU), 2020, ss. 148, 149) och Dataskyddsstyrelsens rekommendationer (Dataskyddstyrelsen (EDPB), 2020).

För att standardklausuler ska kunna användas krävs att överföringen omfattas av lämpliga skyddsåtgärder, och på villkor att lagstadgade rättigheter för registrerade och effektiva rättsmedel för registrerade finns tillgängliga. (Europaparlamentet och Europiska unionens råd, 2016, s. Artikel 46). EU-domstolen kom i sin analys och dom fram till att skölden för skydd av privatlivet (Privacy Shield) strider mot artikel 45.1 i dataskyddsförordningen när den jämförs med artiklarna 7, 8 och 47 i Eu-stadgan, vilket innebär att amerikansklagstiftning inte är väsentligt likvärdig Unionens. (Court of Justice of the European Union (CJEU), 2020, ss. 196-199 (168-202)). I dataskyddsstyrelsen rekommendationer (Dataskyddstyrelsen (EDPB), 2020, ss. 44, 76) beskrivs att amerikansklagstiftning inte är väsentlig likvärdig med europeisk.

I Dataskyddstyrelsen rekommendationer (Dataskyddstyrelsen (EDPB), 2020, s. 44) sägs att om överföringsverktyget inte säkerställer en väsentligen likvärdig skyddsnivå. Uppgiftsinföraren kan inte fullgöra sina skyldigheter på grund av tredjelandets tillämpliga lagstiftning och/eller praxis för överföringen. I de fall där överföringsverktygen i artikel 46 i dataskyddsförordningen inte är tillräckliga fastslog EU-domstolen att det är uppgiftsutförarens ansvar att antingen införa effektiva kompletterande åtgärder eller avstå från att överföra personuppgifterna.

Finns det effektiva kompletterande åtgärder?

Nej, det finns inga effektiva kompletterande åtgärder

För innehållsdata

Nej, det finns inga effektiva kompletterande åtgärder

Perspektiv	Åtgärder
Juridiskt	De åtgärder som Microsoft har beskriver i *Online Services Data Protection Addendum (DPA)* (Microsoft, 2020) är inte effektivt då överföring av personuppgifter sker till tredjeland enligt juridisk analys (Advokatfirman Lindahl KB, 2021)
Tekniskt	Det går att kryptera information inom den egna organisation, men det innebär att Office 365 inte längre är en tjänst som går att använda i webbläsare. Det krävs en tillförlitlig uppkoppling för att till exempel öppna och redigera filer.

Diagnosdata / Funktionsdata

Nej, det finns inga effektiva kompletterande åtgärder

Perspektiv	Åtgärder
Juridiskt	De åtgärder som Microsoft har beskriver i *Online Services Data Protection Addendum (DPA)* (Microsoft, 2020) är inte effektiva då överföring av personuppgifter sker till tredjeland enligt juridisk analys (Advokatfirman Lindahl KB, 2021, s. 1.2)
Tekniskt	Det går att stänga av diagnosdata för desktopversioner men inte för Microsoft 365 Online (när Office 365 används via en webbläsare).

Finns andra undantag då det inte går att tillämpa SCC?

De undantag som finns i övrigt är inte direkt tillämpbara på överföring i större skala så som vid utkontraktering av it-drift men skulle möjligen kunna tillämpas vid enstaka eller unika fall efter analys av den specifika behandlingssituationen och de krav som kan vara förknippade därmed. Det kan därmed anses inte vara tillämpbart på Office 365.

Är Microsoft Europa bundna till amerikansk lagstiftning?

Stadsjuristerna har inte gjort ett ställningstagande i frågan (se sid 35). Men har avseende Cloud Act och OSL gjort bedömningen att Microsoft Europa lyder under amerikansk lagstiftning (Stadsledningskontoret, 2017; Stadsledningskontoret, 2019). Förvaltningens bedömning är att Microsoft Europa i sin behandling av Göteborgs Stads personuppgifter är bunden av EU-lagstiftning. Samtidigt är Microsoft Europa bunden av amerikansk lagstiftning eftersom man genom sitt amerikanska moderbolag kan tvingas överföra personuppgifter till den amerikanska staten.

Förvaltningens bedömning

Förvaltningen har via arbetssätt, rekommenderat av EDPB, så långt det är möjligt säkrat underlag för att kunna göra en bedömning av användningen av Office 365 utifrån gällande lagstiftning och nuvarande rättsläge.

Förvaltningen bedömer att överföring av diagnosdata och funktionsdata är nödvändiga för att tjänsten Office 365 ska fungera och att det innebär att personuppgifter överförs till USA. Intraservice bedömning är att Office 365 är av sådan vikt för Intraservice och Göteborgs Stads verksamhet att den måste fortsätta användas trots ovan beskrivna potentiella risker. Intraservice kan inte fatta beslut om användning för hela Göteborgs Stad utan ansvaret för vilka personuppgiftsbehandlingar som utförs i Office 365 är respektive nämnd och styrelses ansvar i de förvaltningar och bolag som använder tjänsten.

Genomförda analyser och omvärld

Stadsjuristen vid Göteborgs Stad har ännu inte tagit ställning till eller tagit fram någon riktlinje för hur Göteborgs Stad ser på användningen av molntjänster och överföring av personuppgifter ställt i relation till Schrems II-domen.

Analys av advokatbyrån Lindahls

Förvaltningen Intraservice inom Göteborgs Stad(“Staden”) har gett Advokatfirman Lindahl i uppdrag göra en fördjupad juridisk analys av Stadens användning av programvaran Microsoft Office 365. Utgångspunkten för analysen är de utredningar som Staden sedan tidigare låtit utföra avseende användning av Office 365, vilka sammantaget funnit att användningen - i vart fall före EU-domstolens dom i mål C-311/18 (“Schrems II”) från den 16 juli 2020 – var förenlig med gällande lagar och regler. Denna PM är således inriktad mot det förändrade rättsläge som domen i Schrems II inneburit vad gäller tillåtligheten av överföringar till tredjeland och hur det påverkar Stadens tidigare slutsatser.

Analys av Microsofts hantering av diagnostikdata – underlag för konsekvensbedömning

Analysen är genomförd våren 2021 och omfattar diagnostikdata, som genereras vid användning av Microsofts tjänster både online och via Windows lokalt. Diagnostikdata skiljer sig från innehållsdata, som är den information användare tillhandahåller via bild, ljud, filer, mejl, kalenderbokningar och annan data som kunden laddar upp eller sparar lokalt. (Intraservice, 2021)

Syftet med analysen är att fungera som underlag för konsekvensbedömning av tjänsterna, eftersom diagnostikdata kan innefatta indirekta personuppgifter, som till exempel IP-nummer.

De viktigaste slutsatserna är att:

1. Olika tjänster skickar diagnostikdata i olika omfattning. Vissa tjänster kan inte begränsas alls, som Office för webben.
2. Diagnostikdata går inte att stänga av helt.
3. Diagnostikdata lagras i USA, vilket innebär överföring till tredjeland.
4. Det går att blockera delar av överföring av diagnostikdata, men detta kan leda till kraftigt försämrad funktionalitet.
5. Till tjänsterna finns det ansluta funktioner, där Microsoft i vissa fall agerar som personuppgiftsansvarig.
6. Microsoft har i arbetet med analysen varit transparenta och öppna med hur de hanterar diagnostikdata och vad denna används till.

För att minska överföring av diagnosdata som del av Microsofts produkter ger analysen ett antal rekommendationer. Emellertid innebär varje minskning eller blockering en avvägning mot nyttan av användningen. Påverkan på tjänster kan innebära att avstå från funktionalitet.

Hur hanterar andra offentliga organisationer molntjänster

Denna sektion sammanfattar omvärldsbevakning av vad andra organisationer gör och har gjort avseende molntjänster som man är på väg att använda eller redan använder.

Stockholms Stad
Stockholms Stad arbetar med Schrems II på samma sätt som Intraservice och följer dataskyddstyrelsen rekommendationer avseende process (samtal den 7 maj 2021 med CISO Stockholms Stad).

Kommunstyrelsen i Stockholms Stad har begärt förhandssamråd med Integritetsmyndigheten för att samråda gällande hög integritetsrisk för den registrerade vid tredjelandsöverföring. Samrådet omfattar om de mitigerande åtgärder som kommunstyrelsen planerar att införa fortfarande innebär att hög risk föreligger för individens rättigheter och friheter. Det är angeläget att få klarhet i möjligheterna att införa tjänsterna Azure AD och Teams med begränsad funktionalitet.

(Stockholms Stad, 2021; Stockholms Stad, 2021; Stockholms Stad).

Malmö Stad
Malmö Stad arbetar med Schrems II på samma sätt som Intraservice och följer dataskyddstyrelsen rekommendationer avseende (samtal den 6 maj 2021 med informationssäkerhetssamordnare och signalskyddschef för Malmö Stad). Generellt kan sägas att Malmö stad inte fattat några övergripande beslut eller ställningstaganden avseende användandet av Microsoft Office 365 eller molntjänst - relaterat till tredjelands överföringar. Malmö Stad arbetar i kortfattat enligt följande;

- Respektive förvaltning har gjort en inventering av eventuella tredjelands överföringar (DSO skickade ut detta under okt/nov 2020)
- Förvaltningar har dokumenterade genomförda risk-och konsekvensbedömningar och genomför löpande bedömningar som dokumenteras.
- I de fall nya system ska upphandlas där det förekommer tredjelandsöverföring och verksamheten (Personuppgiftsansvarig) ändå vill använda systemet/tjänsten så rekommenderas att verksamheten dokumenterar beslut, ställningstaganden och genomförda riskanalyser och konsekvensbedömningar.

Boråsregionen
CISO Intraservice har haft möte med DSO för Boråsregionen och Boråsregionen följer dataskyddstyrelsens rekommenderade arbetsprocess från november 2020.

Grannkommuner till Göteborgs Stad
Vid möte den 17 maj 2021 med digitaliseringsansvariga i grannkommunerna till Göteborgs Stad och CISO Intraservice diskuterades samarbete avseende Schrems II. Flera av grannkommunerna har påbörjat sitt arbete och följer dataskyddstyrelsens rekommendationer. Som ett led i arbetet har Göteborgs Stad Intraservice delat med sig av arbetsprocesser, analyser mm till Ale, Alingsås, Härryda, Kungsbacka, Kungälv, Lerum, Lilla Edet, Mölndal, Partille, Stenungssund, Tjörn, Öckerö samt Västkom.

Google Analytics och över 100 organisationers anmälan av personuppgiftsincidenter[7]
Åklagarmyndigheten och 100 andra organisationer (däribland Göteborgs Stad) stoppade Google Analytics för användning i slutet av februari 2021. Diagnosdata skickades direkt till USA för bearbetning eller anonymiserades hos leverantören Google på Irland. Det

[7] Sveriges radio 2021-03-05 https://sverigesradio.se/artikel/kommuner-anmaler-sig-sjalva-efter-ekots-granskning

finns en osäkerhet om Google Irland är bunden till Google USA. Om överföring i ett sådant förhållande är genomförd är osäkert, men Göteborgs Stad valde att stoppa tjänsten.

Skatteverket och Kronofogsmyndigheten

Beslut inför användande av Teams på Skatteverket och Kronofogden (3 maj 2021)

I promemoria från Skatteverket (8-958696) och Kronofogden (KFM 10419–2021) 2021-05-03 har myndigheterna fattat beslut om att inte införa användning av Teams.

Beslut att inte införa Teams är fattat på nedan grunder.

1. Det finns ingen möjlighet för Skatteverket och Kronofogden att förhindra en olovlig personuppgiftsöverföring till USA genom tekniska åtgärder och organisatoriska åtgärder är inte tillräckliga i detta sammanhang,
2. Det finns skäl att anta uppgifterna skulle vara av intresse för de amerikanska myndigheterna eftersom de inte är tillgängliga på annat sätt, dvs. det finns en reell risk för att uppgifterna faktiskt överförs,
3. Myndigheterna har inga kontrollmöjligheter för att upptäcka om sådan överföring sker,
4. Omfattningen av personuppgifterna är stor,
5. Personuppgifterna, i synnerhet i Skatteverkets verksamhet, är känsliga, och
6. En olovlig personuppgiftsbehandling och överföring innebär stora negativa konsekvenser för de enskilda vars personuppgifter behandlas i respektive myndighets verksam

Mot den bakgrunden anser Skatteverket och Kronofogden att det inte finns förutsättningar för användning av Teams i myndigheternas verksamhet som huvudsakligt verktyg för video- och samarbeten.

Genomförda prövningar i domstol

Frågan om lagring inom EU av ett amerikanskt molntjänstföretag har prövats av den franska högsta förvaltningsdomstolen (Conseil d'État) i två fall, vilka båda var kortfattade beslut tagna i summariska förfaranden. Prejudikatvärdet av dessa avgöranden är därför begränsat.

Det första avgörandet rörande denna fråga kom i oktober 2020 och rörde en centraliserad hälsoplattform som upprättats i samband med coronavirusets utbrott (Health Data Hub) som driftades av Microsoft Irland på plattformen Azure. Enligt avtalet med Microsoft skulle data inte överföras till USA, dock med undantag av vissa diagnosdata och faktureringsdata. Den data som lagrades i tjänsten var krypterad och pseudonymiserad. Domstolen konstaterade i målet att det trots detta fanns en risk att Microsoft skulle kunna tvingas att lämna ut personuppgifter till amerikanska myndigheter och att det därmed fanns en risk för överträdelser av Dataskyddsförordningen. Prövningen i målet var dock inriktad på om det förelåg en uppenbar och allvarlig överträdelse. Detta fann domstolen inte att det förelåg. [8]

Det andra avgörandet kom i mars 2021 och rörde också en hälsorelaterad webbplattform, denna gång för vaccinationsbokningar (DoctoLib). Driften sköttes av Amazon i

[8] Health Data Hub (CE - N° 444937) https://gdprhub.eu/index.php?title=CE_-_N%C2%B0_444937

Luxemburg och bolaget hade därtill lovat att inte överföra uppgifter utanför EU. Därutöver förekom inga känsliga uppgifter, data var krypterad med nyckeln hos tredje part och uppgifterna skulle raderas efter tre månader. Domstolen gjorde även i detta fall prövningen baserat på att det förelåg en risk att uppgifterna skulle hamna i amerikansk myndigheternas händer, men fann även i detta fall att det inte förelåg någon uppenbar eller allvarlig överträdelse av Dataskyddsförordningen och användningen stoppades inte. Viss vikt föreföll ha fästs vid att tjänsten ifråga tillkommit med anledning av pandemin.[9]

Förvaltningens reflektion över omvärld och analyser

Förvaltningens reflektion av Lindahls Analys av Microsoft

Innan ytterligare vägledning kommer från EU-domstolen eller europeiska dataskyddsmyndigheter är det inte möjligt att med säkerhet uttala sig om vilka skyddsåtgärder som är nödvändiga vid överföringar av personuppgifter till USA och andra tredjeländer – och därmed om Microsofts överföring av personuppgifter till USA är förenlig med europeisk dataskyddslagstiftning eller inte. Vår bedömning är emellertid att de skyddsåtgärder som nu vidtagits ensamt inte är tillräckliga för att Microsofts överföring till USA som utgångspunkt ska anses godtagbar. Detsamma gäller om Microsoft garanterar behandling inom EU.

Det medför emellertid inte med automatik att anlitande av Microsoft för personuppgiftsbehandling omöjliggörs. Varje personuppgiftsansvarig måste göra sin egen bedömning med hänsyn tagen till vilka uppgifter som behandlas, under hur lång tid det sker, förekomsten av andra möjliga lösningar samt utrymmet för tillämpning av undantag. I en sådan bedömning bör enligt vår bedömning sannolikheten för att Göteborgs Stads data faktiskt lämnas ut till amerikanska myndigheter vägas in.

Förvaltningens reflektion på Analys av Microsofts hantering av diagnosdata

Diagnosdata som innehåller personuppgifter bedöms skickas direkt till USA för behandling och lagring. Att insamling av diagnosdata med de inställningar som gjorts i Göteborgs Stad inte innebär en hög risk för den registrerades fri och rättigheter.

Förvaltningens reflektion på Stockholms Stad

Stockholms stad arbetar på ett likartat sätt som Göteborgs Stad Intraservice och har i analyser identifierat samma utmaningar med användandet av Microsoft Office 365.

2021-06-02 fick Stockholm Stad svar från IMY (DI-2021-1513). Dokumentet bifogas i sin helhet, bilaga2. Nedan en kort sammanfattning;

1) Konsekvensbedömning av Stockholm stad är inte tillräcklig

2) IMY anser att skyddsåtgärder behöver utredas mer

3) IMY rekommenderar Stockholm Stad att inte använda Azure AD och Teams

Förvaltningen har inte analyserat vad beslut från IMY gällande Stockholms Stads samråd innebär för leveransen i Kommungemensamma interna tjänster. Förvaltningen bedömer att Intraservice genomförda konsekvensbedömning tar hänsyn till den fortsatta behandlingen av personuppgifter vid användningen av tjänsterna. IMY konstaterar att rättsläget vad gäller möjligheten att anlita amerikanska personuppgiftsbiträden inte är helt

[9]Doctolib (CE – 450163) https://gdprhub.eu/index.php?title=CE_-_450163

klart idag. IMY pekar på att de europeiska dataskyddsmyndigheterna arbetar med att ta fram vägledning till personuppgiftsansvariga kring detta.

Förvaltningens reflektion på Malmö Stad

Malmö stad arbetar på ett likartat sätt som Göteborgs Stad Intraservice och har i analyser identifierat samma utmaningar med användandet av Microsoft Office 365.

Förvaltningens reflektion på Boråsregionen

Borås regionen arbetar på ett likartat sätt som Göteborgs Stad Intraservice och har i analyser identifierat samma utmaningar med användandet av Microsoft Office 365. Boråsregionen var på väg att införa Microsoft 365 men valde att avvakta utveckling av rekommendationer från dataskyddstyrelsen.

Förvaltningens reflektion på Grannkommuner till Göteborgs Stad

Grannkommunerna Ale, Alingsås, Härryda, Kungsbacka, Kungälv, Lerum, Lilla Edet, Mölndal, Partille, Stenungssund, Tjörn, Öckerö samt Västkom fortsätter sitt arbete i linje med dataskyddstyrelsens rekommendationer och kommer följa Göteborgs Stad avseende Microsoft och andra stora molntjänster.

Förvaltningens reflektion på promemorian 8-958696 från de två myndigheterna

Skatteverket och Kronofogden fattade beslut att inte införa Teams, en funktion de inte använder. Göteborgs Stad använder redan Teams integrerat i Microsoft Office 365. De båda myndigheternas bedömning är i sak korrekt med hänsyn till lagstiftningen.

Skatteverkets och kronofogdemyndighetens analys samstämmer med den analys av Microsoft som Intraservice genomfört. Intraservice gör bedömningen att överföring av funktionsdata inte innebär en hög risk för den registrerades fri och rättigheter.

Förvaltningens reflektion av Genomförda prövningar i domstol

Några säkra slutsatser om molntjänster i allmänhet kan inte dras från dessa avgöranden då de båda omfattade mycket omfattande tekniska säkerhetsåtgärder Båda prövningarna hade en koppling till pandemin (och därmed möjlighet till undantag enligt artikel 49). De bedömdes dessutom summariskt utifrån frågan om det förelåg en uppenbar och allvarlig överträdelse.

Enligt vår bedömning kan dock sägas att avgörandena indikerar två saker vad gäller bedömningen: i) att den amerikanska övervakningslagstiftningens extraterritoriella tillämpning inte ifrågasätts utan ska ses som en reell risk, ii) att förekomsten av en sådan risk med nödvändighet inte innebär att anlitande av biträdet är uteslutet.

Förvaltningens arbetssätt, ansvar och metodik

En arbetsgrupp bestående av tjänstemän från Intraservice; dataskyddsombud, förvaltningsjurist, CIO, CISO, kommunikationschef, enhetschef för it-säkerhet och kanslichef har tagit fram ett arbetssätt. Arbetssättet stödjer arbetet med att hantera dom i mål C-311/18 (SchremsII-domen). Arbetssättet följer Göteborgs Stads styrande dokument och Intraservice interna processer och beslutades den 10 augusti 2020.

I samverkansmöte 19 augusti 2020 med SLK, representerad av Göteborgs Stads CISO och stadsjurist, Intraservice representerad av CISO och förvaltningsjurist gjordes en fördelning av ansvar;

1. Intraservice ansvarar för analys av Kommungemensamma interna tjänster
2. SLK informerar övriga förvaltningar och bolag om att kartlägga och bedöma sina egna it-system och tjänster

Dataskyddstyrelsens rekommendation om arbetsprocess från 11 november 2020 innebar inte någon förändring i arbetssätt.

Arbetssätt

- Respektive förvaltning gör sin kartläggning enligt dataskyddstyrelsens rekommendationer från den 11 november 2020.
- Intraservice som levererar Kommungemensamma interna tjänster ansvarar för kartläggningen av Kommungemensamma interna molnbaserade tjänsterna. Kartläggningen sker både utifrån Intraservice roll som Personuppgiftsansvarig (PUA) och Personuppgiftsbiträde (PUB).
- Kartläggningen kan innebära nya förhållanden. Ny kunskap om rättsläget, nya rekommendationer eller att andra kommuner och myndigheter gör att ställningstaganden kan påverka resultatet av kartläggningen.
- Ett ställningstagande och eventuella åtgärder genomförs enligt dataskyddstyrelsens rekommendationer

Intraservice arbetar sedan 20 juli 2020, efter dom i mål C-311/18 (SchremsII-domen), med att hantera och åtgärda berörda Kommungemensamma interna molnbaserade tjänster.

Det innebär att:

- Intraservice inventerar och ser över personuppgiftsbiträdesavtal med leverantörer och deras underbiträden.
- Intraservice identifierar om det sker tredjelandsöverföringar
- Intraservice ser över vilken ”mekanism” som används. Om det är adekvat beslut (artikel 45) eller Dataskyddsförordningen kapitel V och artiklarna 45 och 46 som är tillämpbara
- Intraservice ser över och bedömer behovet av kompletterande tekniska skyddsåtgärder
- Intraservice tillsammans med stadsledningskontoret bedömer behovet av kompletterande juridiska åtgärder
- Intraservice meddelar personuppgiftsansvarig om tjänsten inte uppfyller krav enligt lagstiftningen. Personuppgiftsansvarig bedömer om verksamhetsintressen

värderas högre än riskerna och om tjänsten kan användas eller om den ska avvecklas.

Intraservice arbetar med frågeställningar och åtgärder enligt nedan. Metoden följer dataskyddstyrelsens (EDPBs) rekommendationer.

Frågeställning	**Svar**	**Åtgärd**
1. Överförs personuppgifter till leverantör?	Nej	Godkänt för användning.
2. Överförs personuppgifter av leverantör utanför EU/EES?	Nej	Godkänt för användning.
Om Ja på de 2 första frågorna	**Svar**	**Åtgärd**
Frågeställning		
3. Avtalsform vid överföringen? (Adekvat beslut)	Gällande Adekvat beslut finns	Godkänt för användning.
4. Avtalsform vid överföringen? (Privacy Shield eller standardavtalsklausuler)	Privacy Shield används	Byt till standardavtalsklausuler och ta fram ytterligare skyddsåtgärder om det är möjligt.
5. Standardavtalsklausuler används?	Ja	Utred vilka skyddsåtgärder som finns på plats och bedöm om skyddsåtgärderna är tillräckliga.
6. Skyddsåtgärder är tillräckliga?	Ja	Godkänt för användning.
7. Skyddsåtgärder är otillräckliga?	Ja	Samråd genomförs med dataskyddsombud och personuppgiftsansvarig. Personuppgiftsansvarig avgör om verksamhetsintressen finns som gör att tjänsten fortsätter att användas. Personuppgiftsansvarig avgör om kontakt med Integritetsmyndigheten ska ske eller inte.
8. Verksamhetsintresse överväger inte risken?	Nej	Ta fram underlag för beslut för att initiera avveckling

Riskminimering

För att minska risken för felaktig behandling av personuppgifter finns instruktioner. Och regler. Tekniskt beskrivs detta i genomförd riskanalys gällande dataskydd för specifikt Office 365. Kommunikation om resultatet har genomförts via Tjänsteforum och till forum för it-chefer och utvecklingsledare.

I rollen som personuppgiftsansvarig är det ytterst respektive nämnd för förvaltningar och bolag som har det slutgiltiga beslutet om användning. Vidare finns i ”Göteborgs Stads regler för it-användare” uttryckta regler (paragraf1) att respektive medarbetare har skyldighet att informera sig om gällande instruktioner och i ”Göteborgs Stads regler för chefers informationssäkerhetsansvar står det (paragraf2) att chefer ska informera sin anställda. I Göteborgs Stads ”Råd för säkerhet i molntjänster” är det uttryckt

säkerhetskrav för molntjänst som hanterar information med personuppgifter. Den som använder en molntjänst för sin personuppgiftsbehandling är personuppgiftsansvarig för behandlingen även om den utförs av molntjänstleverantören eller dess underleverantörer. Leverantören, och alla dess underleverantörer som anlitas för behandlingen, är den personuppgiftsansvariges personuppgiftsbiträden. Det är den personuppgiftsansvarige som ansvarar för att personuppgiftslagen följs.

Innan lagring och bearbetning av personuppgifter i en molntjänst ska den personuppgiftsansvariga bland annat säkerställa att:

- personuppgifter inte kommer att behandlas för andra ändamål än de ursprungliga
- en eventuell överföring av personuppgifter till ett land utanför EU/EES har stöd i personuppgiftslagen
- säkerställa att personuppgiftsbiträdesavtal upprättas med leverantören
- bedöma vilka säkerhetsåtgärder som måste vidtas för att skydda de personuppgifter som behandlas
- förvissa sig om att leverantören kan genomföra de stipulerade säkerhetsåtgärderna samt att leverantören vidtar åtgärderna. Detta sker genom granskning och verifiering, företrädesvis med hjälp av en tredje oberoende part.

Förvaltningen har en tjänst, “Informationssäkerhet och dataskydd”, där förvaltningen erbjuder stöd till Göteborgs Stads verksamheter för stöd i arbetet med bedömning av molnbaserade tjänster. För nyanskaffning av system vid upphandling har vi kontrollpunkter, kravställning, riskbedömningar och konsekvensbedömningar utifrån nuvarande rättsläge.

Återrapportering Göteborgs Stad – nämnder och styrelser

Sedan den 2020-07-20 har information om status för de olika tjänsterna genomförts via tjänsteforum till dataskyddskontakter och personuppgiftsansvariga i respektive förvaltning. Intraservice har koordinerat och samrått med Stadsledningskontorets CISO och stadsjurist, samt informerat Intraservice nämnd vid olika tillfällen. Nedan är den kommunikationsplan och lista med de betydande genomförda aktiviteterna.

Kommunikationsplan	Intressenter	Via
Intraservice	Nämnden för Intraservice	Presidiet
	Intraservice ledningsgrupp	ILG-möten
	Koordinerande projektet ”Att arbeta digitalt”	Möten och e-post
	Tjänsteansvariga	Möten och e-post
	Projekt och portföljstyrning, Projektledare, Projektägare	Möten och e-post
	Supporten	Möten och e-post
	Övriga chefer och medarbetare Intraservice	Intranätet
Göteborgs Stad	Kommunstyrelsen	SLK CISO
	SLK direktörer	SLK CISO
	Förvaltnings -och bolagsdirektörer	SLK CISO
	it-chefer, Utvecklingsledare	Etablerade forum, 3F/ULIT
	Kontaktcenter	Möten och e-post

Kommunikationsplan	Intressenter	Via
	Tjänsteforum	Möten
	Utvecklingsorganisationen	Månadsmöten
	Skolprojekten inom område välfärd	Via PL
Externt	Media	Vid kontakt från media
	Datainspektionen	Vid eventuell självanmälan eller samråd med personuppgiftsansvarig
	SKR	Via kontakt mellan Intraservice CISO och SKR CIO
	Andra kommuner och organisationer	Via kontakt mellan Intraservice CISO samt CISO och CIOer i andra kommuner

Förteckning genomförd Information

Datum	Till vem	Information om
2021-02-09	Nämnden för Intraservice	Customer Lockbox
2021-01-27	VLG IT	Status Schrems II, Customer Lock Box
2021-01-26	Intraservice presidie	Customer Lockbox
2020-12-17	Nämnden för Intraservice	§ 197 Information om Schrems II Säkerhetsarkitekt Per Gustavsson informerar om EU-domen och överföringar av personuppgifter till USA. Per Gustavsson ger en bakgrundinformation samt en statusuppdatering kring hur Intraservice jobbar med frågorna. Nämnden för Intraservice antecknar informationen.
2020-08-28	ULIT3F (forum i Göteborgs Stad)	Information om Schrems II och Microsoft och hur Intraservice arbetar med frågan
2020-08-26	Intraservice internt samtliga medarbetare (EU-dom dataskydd infomöte 26 augusti.pptx	Information om Schrems II och hur Intraservice arbetar med frågan
2020-08-19	Information från Intraservice till SLK (samverkansmöte) (2020-08-19 EU-dom dataskydd baspresentation.pptx)	Information om Schrems II och hur Intraservice arbetar med frågan. Rollen och vilket ansvar Intraservice har i form av Personuppgiftsbiträde som leverantör av Kommungemensamma interna tjänster lyfts fram.
2020-08-19	Intraservice ILG	Information Schrems II och hur Intraservice arbetar med frågan
2020-08-10	Intraservice arbetsgrupp (2020-08-10 Status pågående arbete avseende CJEU Schrems ii.pptx	Information om Schrems II och hur Intraservice arbetar med frågan

Status Kommungemensamma interna tjänster

I tabell 2, nedan beskriver vi status den 5 maj 2021 för Kommungemensamma interna tjänster. Status kan komma att ändras när mer information inhämtats om leverantörer och dess underleverantörer. Totalt är det 225 tjänster och system som kartlagts och analyserats.

Av de 225 tjänsterna och systemen bedömer vi att 199 inte har några risker avseende Schrems II. 26 Tjänster och system har kvarstående risker. Arbetet med kartläggning och eventuella åtgärder pågår för de tjänster och system där tredjelandsöverföringar eventuellt sker. Respektive personuppgiftsansvarig är informerad via tjänsteforum. Respektive personuppgiftsansvarig i förvaltning och bolag har det slutgiltiga ansvaret att avgöra lämpligheten i att använda molntjänsterna.

Tabell 2- Samanställning av kartläggning av Kommungemensamma interna tjänster 5 maj 2021

Typ	Beskrivning	Antal
Inte IT objekt	Manuella tjänster	8
Inte molntjänster	Lösning där Intraservice driftar system och tjänster inom egna organisationen	135
Molntjänster	Ett antal tjänster och system hanterar inte personuppgifter. Det är 2 system inom HR och 7 system inom IT.	9
	Bearbetning och lagring av personuppgifter sker inom Sverige eller Europa	47
	Bearbetning och lagring av personuppgifter sker inom Sverige eller Europa med potentiell överföring till USA. Leverantör eller underleverantör har amerikanskt moderbolag eller att Data Processing Amandment (DPA) innebär att bearbetning och lagring kan ske i tredjeland	19
	Bearbetning och lagring av personuppgifter sker inom Sverige eller Europa med överföring till USA	3
	Bearbetning och lagring av personuppgifter sker i USA	3
	Bearbetning och lagring av personuppgifter som har avslutats	1
Totalt		225

19 molntjänster inom EU/EES med möjlig överföring på grund av att leverantör eller underleverantör kan anses vara bunden till amerikansklagstiftning.

Pågående utveckling

I tjänsteplaner för 2021 och 2022 pågår initiativ som använder olika typer av molntjänster. Arbetet med initiativ inom tjänsteplan regleras enligt riktlinjer för Kommungemensamma interna tjänster, i detta arbete kartläggs verksamhetens behov och målsättning med de enskilda tjänsterna inom respektive tjänsteområde. I kartläggningen av behoven ingår att förstå vilken typ av behandling av information som verksamheten ämnar göra och vilken typ av information som ingår i behandlingen.

När arbete sedan påbörjas att ta fram tjänsten är ett av stegen att ta fram ett lösningsförslag. I de fall tjänsten i sin lösning har någon form av system skall en riskanalys genomföras för att säkerställa att lösningen utifrån ett dataskyddsperspektiv kan upprätthålla de krav som ställs. Arbetet genomförs enligt framtagen process och medverkande är bland annat dataskyddsombud, CISO, leveransansvariga för de olika delarna i tjänsten samt tjänsteansvarig.

Behov av kompletterande arbetssätt -Office 365 som exempel

Office 365, precis som andra molntjänster, uppdateras kontinuerligt med ny funktionalitet under tiden den är tillgänglig för användarna. Processen för framtagning tjänsteplanen och genomförande av initiativen där i har 12-36 månaders cykler, vi har därför här sett ett behov av att komplettera arbetssätt och processer för att hantera de snabba förändringarna.

En process och en organisation, bestående av representanter från Intraservice samt verksamheter i Göteborgs Stad, har därför etablerats. Syftet är att snabbt kunna fånga upp förändringar ifrån leverantör, men också att kunna fånga upp verksamhetens behov av förändringar i tjänsten. Gällande informationssäkerhet innebär detta att vi tidigt identifierar sådana förändringar i tjänsten som kan innebära ändrad informationshantering och de förändrade behandlingar som verksamheten kan tänkas vilja göra med stöd av nytillkommen funktionalitet eller tjänst.

Oavsett om förändringen gäller diagnosdata, funktionsdata eller innehållsdata startar ett arbete med utgång ifrån riskanalysprocessen. När lösningsförslaget arbetas fram ingår det att, utifrån den informationshantering vi utför i tjänsten eller den nya behandling som skulle kunna uppstå, utvärdera de tekniska samt de administrativa skyddsåtgärderna. Detta är riskanalysen som vi genomför som PUB och leverantör av tjänsten och som verksamheten tar del av när de gör sin konsekvensbedömning som PUA.

Genom detta arbetssätt, har vi i många fall möjligheten att dels stänga av vissa tjänster eller avvakta med lansering av ny funktionalitet, till dess att arbetet är genomfört och en analys är klar. Detta skapar bättre förutsättningar för varje enskild verksamhet att informera sina användare om förändringen, besluta hur tjänsten skall användas eller välja att den inte skall användas.

Ekosystem och kontorsstöd i molnet eller egen regi

Generellt

En förändring som skett under de senaste decennierna är att organisationer, både privata och offentliga, väljer att i allt högre grad fokusera på sin kärnverksamhet. Detta innebär att organisationer i högre utsträckning köper tjänster för det som inte direkt kan kopplas till verksamhetens direkta mål och syfte. I takt med detta har även leverantörer av system och applikationer förändrat på vilket sätt de tillhandahåller sina produkter till kunderna.

En tydlig trend på marknaden är att erbjuda applikationer som paketerade tjänster där leverantörerna vill ta ett helhetsansvar för att möta kundernas behov. Detta gäller inte

bara system och applikationer utan samma trend går även se inom plattforms- och infrastrukturtjänster.

En konsekvens av denna förflyttning är att leverantörerna fokuserar på utveckling av molntjänsten vilket medför att den licensbaserad produkten får en långsammare utvecklingstakt eller på sikt uteblir.

Inom vissa områden kommer det troligen finnas alternativ för lokal drift under en överskådlig framtid. Det kan bland annat handla om sådana områden eller system kopplade till specifika verksamhetsprocesser, där kunden behöver ha god kontroll över informationen som hanteras i systemet eller där andra typer av krav gör att det endast går att lösa med fysisk kontroll över systemen.

Strategi för att välja leveransform

I valet av leveransform gäller det att analysera förstå vilken typ av tjänst du skall leverera.

- vilken typ av information kommer bearbetas,
- vilka alternativ finns för att göra leveransen
- vilket tidsperspektiv du har på att leverera tjänsten

Utifrån dessa och ytterligare faktorer välja den mest lämpliga leveransformen. Det behöver också göras en analys om möjligheter att förändra leveransformen i framtiden då förutsättningarna kan förändras under den livslängd som tjänsten har.

Resultatet av analysen kan dessutom ge att det är en kombination av leveransformer som krävs för att leverera tjänsten. I moln och/eller egen regi i kombination.

Drift och support

Att hantera en fysisk drift och supportmiljö innebär att ha ansvar för allt ifrån fysiska lokaler till servrar. Att kunna svara på användarnas frågor och hantera avbrott under den tiden på dygnet som tjänster och funktioner förväntas vara tillgängliga.

När vi väljer leveransform är även detta frågor att beakta, vill vi ha tjänster som är tillgängliga över fler av dygnets timmar krävs extra personal och kompetens. En kostnad som vi bär helt själva som både kunde och leverantör. Men om en istället väljer att köpa en tjänst så delar vi istället på vissa av dessa kostnader med andra kunder. Även om kostnaden kanske inte nödvändigtvis blir lägre så ger det andra fördelar. En leverantör som är aktiv på flera marknader globalt har ofta flera driftsorganisationer tillgängliga, dessa blir då tillgängliga för oss. Felsökning och support blir tillgängligt utanför våra kontorstider

Kompetensutveckling

En annan aspekt som en behöver beakta vid val av leveransform är hur tillgängligheten är av den kompetens som behövs för att ta hand om tjänsten. Utifrån den generella utvecklingen som sker på marknaden där mer och mer förflyttas till molnet och den teknik som då används där, kommer det ske en ökning av tillgängliga jobb i den sfären och därmed kommer också människor att söka sig både kompetensmässigt och anställningsmässigt åt det hållet. Även om en då kan välja att hantera tjänsten/systemet själv kanske det kan finnas utmaningar att hitta personal som vill vara anställda. Detta skulle kunna driva upp de personalkostnader som uppstår att hantera tjänsten, något som du delar med andra kunder när du istället köper det från leverantör.

Innovation genom moln

En annan anledning till att leverantörerna väljer att erbjuda sina applikationer och plattformar som moln är för att höja innovationstakten. Istället för att ha cykler som skall förhålla sig till varje kunds olika förutsättningar att ta emot en förändring, ansvarar leverantören för hela kedjan. Genom att allt erbjuds på en egen standardiserad plattform med minimalt med lokala förutsättningar att förhålla sig till skapas en mer kontrollerad miljö att både testa och leverera nya funktioner på. Samtidigt skapas en gemensam plattform med alla kunder, där behov kan tas emot, prioriteras, utvecklas och testas med betydligt kortare tidsperspektiv än om de skall ta hänsyn till att produkten skall levereras till olika kunder och olika miljöer. Resultatet av detta är snabbare innovation då den ske i kontrollerade miljöer, snabbare distribution till slutanvändare då detta sker direkt hos leverantör.

Ekosystemsbaserade kontorsstöd och arbetsströmmens betydelse för effektivitet

System och applikationer för kontorsstöd har funnits under en lång tid. Från att i början handlat om enkla ordbehandlingssystem och kalkylark, till att nu handla mer om hur vi som individer och organisationer samarbetar kring informationen som vi producerar i dessa verktyg. Istället för att lagra filer på enkla tjänster där vi som individ måste dela via andra funktioner så som e-post. Finns nu vår information i tjänster där användaren inte bara själv enkelt kan dela, utan där det också stöttas av sammanvävda funktioner för att föra dialog i text/ljud/bild, skapa möten, påminnelser och andra händelser.

I ekosystem hänger alla dessa olika funktioner ihop, information delas mellan de olika tjänsterna för att stötta användaren, gränssnitten är strömlinjeformade för att lyfta fram det viktigaste och skapa enkelhet.

Ekosystem svårare att skapa själv

I ekosystem kring kontorstjänster finns ett antal tjänster och funktioner som samverkar. Det finns dessutom ofta ett antal grundläggande beståndsdelar som binder ihop dessa, det kan vara sådant som inloggningen och den profil som är kopplad till användaren. Det kan också handla om att information som skapas i del olika tjänsterna delas, på detta sätt finns den tillgänglig för alla delarna i ekosystemet och jag som användare slipper hantera dubbletter eller att behöva ange samma information på flera ställen.

Att sätta samman ekosystemet är något som molnleverantörerna tar ansvar för, att se till att allt ifrån konton till information hanteras på ett sätt som gör att de blir tillgängliga och samverkar sömnlöst för användare. Samma upplevelse är svårare att skapa i egen regi med motsvarande funktionalitet. Att ställa krav på flera leverantörer som var och en ansvarar för att leverera in sin del till ett ekosystem är komplext och i vissa fall inte görbart. Det ställer högre krav på kunden att förstå och ställa krav på de integrationer och användarupplevelser och en kommer ofta att få sätta dessa lägre på prioriteringslistan i jämförelse med de funktioner som ligger närmare själva kärnan av vad som skall lösas.

Det är inte heller säkert att alla de funktioner och tjänster som du får tillgång till via ett molnbaserat ekosystem finns tillgängliga för lokal drift. En aspekt att förhålla sig till när en försöker uppnå önskad effekt.

Aktiviteter vid avveckling av molntjänst

Förvaltningen ser ett omfattande arbete att ersätta en molntjänst och vi behöver ta fram en övergripande plan för beslut som beskriver hur förvaltningen tänker ta sig an ett sådant uppdrag från nämnden.

I nästa steg behöver flera initiala beslutsunderlag skapas;

- Urval kritiska molntjänster
- påverkan på befintliga Kommungemensamma interna tjänster,
- påverkan på Göteborgs Stad,
- för vilka molntjänster som behöver ersättas,
- för behov av målmiljöer för att ersätta befintliga tjänster,
- som innehåller kostnader för nya målmiljöer,
- för hur ett genomförande ska gå till

Förvaltningens slutsats

Förvaltningen har i detta TU beskrivit det faktiska nuvarande rättsläget och redovisat hur förvaltningen arbetar med pågående utveckling i Kommungemensamma interna tjänster där hela eller delar av tjänsten levereras via molntjänst. Förvaltningen har via arbetssätt, rekommenderat av EDPB, så långt det är möjligt säkrat underlag för att kunna göra en bedömning av Kommungemensamma interna tjänster utifrån gällande lagstiftning och nuvarande rättsläge. För närvarande är rättsläget framförallt gällande tredjelandsöverföringar oklart. Den gemensamma nämnaren är att flertalet av leverantörerna är amerikanska bolag.

Tills rättsläget klargörs avser förvaltningen att följa nuvarande arbetssätt och fortsätter därmed att utreda och bedöma molntjänster i Kommungemensamma interna tjänster.

Förvaltningen redovisar vad det innebär att avveckla en molntjänst samt några av de risker och konsekvenser förvaltningen ser i samband med detta. Förvaltningen redovisar några av de risker och konsekvenser förvaltningen ser i att vara kvar i nuvarande arbetssätt.

Förvaltningen avser att återkomma till nämnden för Intraservice med ett uppdaterat rättsläge. Förvaltningen anser att nämnden för Intraservice är informerad.

Underskrifter

Ove Hellmers	Lena Eineving
Enhetschef	Verksamhetschef

Definitioner och förkortningar

De ord och termer som i förklaringarna har kursivstil har egna definitioner i tabellen.

Förkortning eller uttryck	Förklaring	Källa
Administrativ bearbetning och lagring	Administrativ bearbetning och lagring är alla tjänster som kan ingå i leverans och utförande av administrativa tjänster. Innebär att den som utför tjänsten alltid har tillgång till informationen. Se även *Teknisk bearbetning och lagring*	Branschstandard
Bearbetning och lagring	Bearbetning och lagring är ett samlingsbegrepp för *administrativ bearbetning och lagring* samt *teknisk bearbetning och lagring.*	Branschstandard
Dataskyddsförordningen	Dataskyddsförordningen (*DSF*)	(Europaparlamentet och Europiska unionens råd, 2016)
Dataskyddsstyrelsen	Se *Europeiska dataskyddsstyrelsen*	IMYs webbplats EDPB | European Data Protection Board (europa.eu)
Datatillsynsmannen	Se *Europeiska datatillsynsmannen*	IMYs webbplats EDPS Homepage | European Data Protection Supervisor (europa.eu)
DSF	Dataskyddsförordningen	(Europaparlamentet och Europiska unionens råd, 2016)
EDBP	European Data Protection Board: *Europeiska Dataskyddsstyrelsen*	IMYs webbplats EDPB | European Data Protection Board (europa.eu)
EDPS	European Data Protection Supervisor: *Europeiska datatillsynsmannen*	IMYs webbplats EDPS Homepage | European Data Protection Supervisor (europa.eu)
Europeiska dataskyddsstyrelsen	Den Europeiska dataskyddsstyrelsen (European Data Protection Board,	IMYs webbplats

Förkortning eller uttryck	Förklaring	Källa
	EDPB) är ett oberoende europeiskt organ som bidrar till en enhetlig tillämpning av dataskyddsreglerna inom hela EU/EES samt främjar samarbetet mellan dataskyddsmyndigheterna.	EDPB | European Data Protection Board (europa.eu)
Europeiska datatillsynsmannen	Europeiska datatillsynsmannen (European Data Protection Supervisor (*EDPS*)) är tillsynsmyndighet för Europeiska unionens institutioner, organ och byråer. Det innebär att EDPS har till uppgift att säkerställa att personuppgifter behandlas på ett lagligt och korrekt sätt inom EU.	IMYs webbplats EDPS Homepage | European Data Protection Supervisor (europa.eu)
GDPR	General Data Protection Regulation (GDPR): Dataskyddsförordningen (*DSF*)	(Europaparlamentet och Europiska unionens råd, 2016)
Hybridmoln (Hybrid Cloud)	Kombination av *on-prem* (levereras av den egna organisationen), *privata moln* (levereras av tredje part) och *publika moln* (levereras av tredje part)	Branschstandard What Is Hybrid Cloud? Everything You Need to Know (techtarget.com)
IaaS	Infrastructure as a Service: Infrastruktur som tjänst är en molntjänst där en leverantör är värd för hårdvara iform av lagrings-, server- och nätverksresurser. IaaS är under PaaS och SaaS.	Branschstandard What is IaaS? Infrastructure as a Service Definition (techtarget.com)
IMY	Integritetsmyndigheten	www.imy.se
Molninfrastruktur	Se molntjänster och IaaS, PaaS, SaaS	Branschstandard
Molntjänster	Molntjänster är ett samlingsnamn för tjänster som nås av en applikation eller webbläsare via internet till en server där *bearbetning och lagring* sker. En molntjänst kan antingen levereras av en extern leverantör eller myndighet, eller av den egna organisationen (*on-Prem*), det förekommer även *hybridmoln* (som är en kombination av extern och intern leverans) Molntjänster delas in i följande huvudgrupper:	Branschstandard

Förkortning eller uttryck	Förklaring	Källa
	SaaS: Software as a Service *IaaS: Infrastructure as a Service* *PaaS: Platform as a Service*	
On-prem	On-premises: Den egna organisationen sköter it-drift, underhåll och support.	Branschstandard
OSL	Offentlighets- och sekretesslag	(200:400) (Sveriges riksdag, 2009)
PaaS	Plattform as a Service: Plattform som tjänst är en molntjänst där en leverantör är värd för programverktyg till användare över internet (och den underliggande infrastrukturen Iaas). Tex operativsystem, databaser, integrationstjänster mm. PaaS är mellan Iaas (infrastruktur) och SaaS (Mjukvara)	Branschstandard What is PaaS? Platform as a Service Definition (techtarget.com)
Privata moln (Private Cloud)	Privat moln är en molninfrastruktur som drivs enbart för en enda organisation och levereras av en tredje part. Ett privat moln som levereras av den interna organisationen är en *on-prem* lösning	Branschstandard What is a Private Cloud and What are its Advantages? (techtarget.com)
Publika moln (Public Cloud)	Publika molntjänster är en molninfrastruktur som drivs för flera organisationer och levereras av en tredje part	Branschstandard What Is Public Cloud? Everything You Need to Know (techtarget.com)
SaaS	Software as a Service: Mjukvara som tjänst är en molntjänst där en leverantör är värd för applikationer och mjukvarusystem och gör dem tillgängliga för användare via internet (och underliggande plattformar (PaaS) och infrastruktur (IaaS). Exempel: Microsoft Office 365, Azure, Google Suite for Education, Service Now	Branschstandard What is SaaS (Software as a Service)? Everything You Need to Know (techtarget.com)

Förkortning eller uttryck	Förklaring	Källa
Teknisk bearbetning och lagring	Teknisk bearbetning och lagring är alla tjänster som kan ingå i leverans och utförande av it-drift. Det inkluderar IaaS, PaaS, SaaS, supportpersonal som via fjärrstyrning kan ta del av information samt andra tekniska hjälpmedel för att leverera den tekniska tjänsten. Begreppet används bla i *OSL* kap11, 4a §, Teknisk bearbetning och lagring Se även *Administrativ bearbetning och lagring*	*OSL* kap11, 4a §, Teknisk bearbetning och lagring SOU 2021:1 (ej definierat, utan beskrivs i flera olika stycken)
Utkontraktering	Utkontraktering (engelska Outsourcing) är utläggning av verksamhet på entreprenad och innebär att ett företag eller organisation låter tredje part sköta en eller flera processer. På det sättet kan företaget fokusera på sin kärnverksamhet. Utkontraktering av it-drift är när en tredje part sköter om drift, underhåll och support. Ofta används *molntjänster* för utkontrakteringen av *teknisk bearbetning och lagring av information*	Branschstandard Svenska akademins ordlista (SAOL) SOU2021:1
Vitbok	En prövning görs om tjänsteleverantören enligt avtal med uppdragsgivaren inte får ta del av eller vidarebefordra de uppgifter som görs tekniskt tillgängliga för leverantören. Detta innebär att det ska finnas en juridiskt bindande och sanktionerad avtalssekretess för leverantören. Leverantören får inte heller vara bunden av regler i främmande rätt om att lämna ut uppgifter utan en föregående sekretessprövning eller annan laglig grund enligt svensk rätt för ett utlämnande. Om detta första villkor är uppfyllt, ska i ett andra steg en bedömning göras av om omständigheterna i övrigt medför att det är osannolikt att tjänsteleverantören ändå tar del av eller vidarebefordrar uppgifterna.	

Referenser

110th Congress. (2008, oktober 7). FISA section 702 - H.R.6304 - FISA Amendments Act of 2008 (50 USC 1881a). Retrieved from https://www.congress.gov/bill/110th-congress/house-bill/6304

115th US Congress . (2018, mars 24). H.R.4943 - CLOUD Act. USA. Retrieved from https://www.congress.gov/bill/115th-congress/house-bill/4943

Advokatfirman Lindahl KB. (2021, april 14). Göteborg stads användning av Microsoft Office 365. Göteborg, Sverige: Intraservice. doi:Intraservice 0193/21

Bundesamt für Sicherheit in der Informationstechnik. (2017). *Projekt „SiSyPHuS Win10: Studie zu Systemaufbau, Protokollierung, Härtung und Sicherheitsfunktionen in Windows 10“ - Work Package 4: Telemetry.* Bonn.

Court of Justice of the European Union (CJEU). (2020, juli 16). Judgement of the court: Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems. Retrieved from http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=SV&mode=lst&dir=&occ=first&part=1&cid=11388612

Dataskyddsstyrelsen (EDPB). (2020, juli 23). *Vanliga frågor om EU-domstolens dom i mål C-311/18 – Data Protection Commissioner mot Facebook Ireland och.* Retrieved from https://edpb.europa.eu/our-work-tools/our-documents/other/frequently-asked-questions-judgment-court-justice-european-union_en

Dataskyddstyrelsen (EDPB). (2020, november 10). *Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.* Retrieved from https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf

Dataskyddstyrelsen (EDPB). (2020, 11 10). *Rekommendationer 01/2020 om åtgärder som komplement.* Retrieved from https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_sv.pdf

eSam. (2015, december 17). Röjandebegreppet enligt offentlighets- och sekretesslagen (VER 2015-190). Retrieved from https://www.esamverka.se/download/18.1d126bc174ad1e6c39cafe/1464274177874/R%C3%A4ttsligt%20uttalande%20r%C3%B6jandebegreppet.pdf

eSam. (2016, januari). Outsourcing – en vägledning om sekretess och persondataskydd. Retrieved from https://www.esamverka.se/download/18.1d126bc174ad1e6c39cae2/1598467797623/Outsourcing%20-%20en%20v%C3%A4gledning%20om%20sekretess%20och%20persondataskydd.pdf

eSam. (2018, oktober 23). Rättsligt uttalande om röjande och molntjänster (VER 2018:57). Retrieved from https://www.esamverka.se/download/18.1d126bc174ad1e6c39cac3/15420078241

43/eSam%20-%20Ra%CC%88ttsligt%20uttalande%20om%20ro%CC%88jande%20och%20molntj%C3%A4nster.pdf

eSam. (2019, september 20). Kompletterande information om molntjänster. Retrieved from https://www.esamverka.se/download/18.1d126bc174ad1e6c39caf4/1568977769756/Kompletterande%20information%20om%20molnfr%C3%A5gan%202019-09.pdf

eSam. (2019, december). Outsourcing 2.0 En vägledning om sekretess och dataskydd. Retrieved from https://www.esamverka.se/download/18.1d126bc174ad1e6c39c4db/1576749838091/Outsourcing%202.0%20sekretess%20och%20dataskydd%202019.pdf

eSam. (2021, januari 26). Molngruppens redovisning - Teknik, produkter och säkerhetslösningar. Retrieved from https://www.esamverka.se/download/18.2592ea441774291f4c756db/1611825241932/PM%20Teknik%20och%20molntj%C3%A4nster%201.0%202021.pdf

Europaparlamentet och Europiska unionens råd. (2016, april 27). Dataskyddsförordningen: 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/. Retrieved from https://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=CELEX:32016R0679

Försäkringskassan. (2019, november 18). *Vitbok - Molntjänster i samhällsbärande verksamhet.* Retrieved from https://www.forsakringskassan.se/wps/wcm/connect/30cc57bd-b5cd-4e04-94cd-1f7a02a9ae1a/vitbok.pdf?MOD=AJPERES&CVID=

Gellman, B., & Poitras, L. (2013, juni 6). US Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program. *The Washington Post*. Retrieved from https://www.webcitation.org/6Hhl2Lwpl?url=http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html

Google. (2021). *Data processing Amendment (Version 2.3).* Retrieved maj 11, 2021, from https://gsuite.google.com/terms/dpa_terms.html

Integritetsskyddsmyndigheten. (2021, maj 3). Yttrande över Säker och kostnadseffektiv it-drift –rättsliga förutsättningar för utkontraktering (SOU 2021:1). doi:DI-2021-956

Intraservice. (2018, maj 17). Bedömning av Customer Lockbox.

Intraservice. (2018, oktober 10). Bedömning av Microsofts grundsäkerhetsnivå gällande Office 365.

Intraservice. (2019, december 10). Intraservice fortsatta utveckling av tjänster baserade på Office 365 (Dnr 0189/19). *Tjänsteutlåtande*.

Intraservice. (2020, juli 29). *Riskanalys Dataskydd - Bedömning av tjänsteleverans O365.* Retrieved from Sharepoint: Intraservice-KomODem-Office365-informationssakerhet

Intraservice. (2021, maj 3). Rapport – Analys av Microsofts hantering av diagnostikdata.pdf.

Kammarkollegiet. (2019, 02 22). *Förstudierapport Webbaserat kontorsstöd.* Retrieved from https://www.avropa.se/globalassets/forstudierapporter-vt--it/forstudierapport-webbaserat-kontorsstod2.pdf

Kommunfullmäktige. (2021, maj 25). Göteborgs Stads miljö- och klimatprogram 2021–2030 (H 2021 nr 43, P 2021-03-25 § 18, Dnr 0409/19). *Stadens styrande dokuument*. Göteborg: Götebrogs Stad. Retrieved from https://intranat.goteborg.se/wps/portal/int?uri=gbglnk:Intranat.styrandedokument&dominoURL=https://www5.goteborg.se/prod/Stadsledningskontoret/LIS/Verksamhetshandbok/Forfattn.nsf/0/6B3CA866EF066429C12586B200449D53?OpenDocument

Kommunstyrelsen. (den 5 juni 2014). *Riktlinjer för styrning av kommungemensamma interna tjänster (H 2014 nr 80, P 2014-06-05, § 25).* doi:KS, 2015-03-11, § 142

Kommunstyrelsen. (2018, februari 18). Göteborgs Stads generella regler för kommungemensamma interna tjänster (dnr 0110/20). *Stadens styrande dokument*. Retrieved from https://intranat.goteborg.se/wps/portal/int?uri=gbglnk:Intranat.styrandedokument&dominoURL=https://www5.goteborg.se/prod/Stadsledningskontoret/LIS/Verksamhetshandbok/Forfattn.nsf/0/77BE1C5EBA9911A3C1257E3C0033C7B2?OpenDocument

Kommunstyrelsen. (2018, februari 18). Göteborgs Stads regler för kommungemensamma interna tjänster (2020-06-25, Dnr 0014/20). *Stadens styrande dokument*. Retrieved from https://intranat.goteborg.se/wps/portal/int?uri=gbglnk:Intranat.styrandedokument&dominoURL=https://www5.goteborg.se/prod/Stadsledningskontoret/LIS/Verksamhetshandbok/Forfattn.nsf/0/1DB9F7E0588DB5AEC1257E3C0031EC1B?OpenDocument

Kommunstyrelsen. (2019, december 19). Göteborgs Stads riktlinje för informationssäkerhet (Dnr 0019/19). *Stadens styrande dokument*. Retrieved from Styrande dokumment: https://intranat.goteborg.se/wps/portal/int?uri=gbglnk:Intranat.styrandedokument&dominoURL=https://www5.goteborg.se/prod/Stadsledningskontoret/LIS/Verksamhetshandbok/Forfattn.nsf/0/2A8DE6AB694CF7BFC1257C230027B5CF?OpenDocument

Kommunstyrelsen Göteborgs Stad. (2021, maj 5). Göteborgs Stads yttrande gällande remiss av delbetänkande Säker och kostnadseffektiv it-drift – rättsliga förutsättningar för utkontraktering (SOU 2021:1). doi:Dnr: 0400/21

Microsoft. (20-01-2021). *The Microsoft 365 apps: Data management and privacy.* Microsoft.

Microsoft. (2020, december 9). Microsoft Onlinetjänster - Dataskyddstillägg / Microsoft Online Services - Data Protection Addendum. USA: Microsoft. Retrieved from https://www.microsoft.com/en-us/licensing/product-licensing/products

MSB. (2014, augusti). Outsourcing av it-tjänster i kommuner. *Myndigheten för samhällskydd och beredskap*. Retrieved from https://www.msb.se/sv/publikationer/outsourcing-av-it-tjanster-i-kommuner/

Reagan, T. 4. (1981, december 4). Executive Order 12333--United States intelligence activities. Retrieved from https://www.archives.gov/federal-register/codification/executive-order/12333.html

Stadsledningskonret. (2019, novemeber 14). Office 365 – bedömning om röjande enligt OSL (Dnr 1408/17). doi:Stadsledningskontorets diarie

Stadsledningskontoret. (2017, oktober 20). Promemoria avseende Office. Retrieved from http://www5.goteborg.se/prod/Intraservice/Namndhandlingar/SamrumPortal.nsf/93ec9160f537fa30c12572aa004b6c1a/8da819e1af971507c12582940044d0d7/$FILE/Bilaga_2_Promemoria_avseende_Office365.pdf

Stadsledningskontoret. (2019, 11 14). *Stadsledningskontoret Promemoria avseende Office 365 – bedömning om röjande enligt OSL.*

Statens Offentliga utredningar. (2016). *Digitaliseringens effekter på individ och samhälle - fyra temarapporter (SOU 2016:85).* Retrieved from https://www.regeringen.se/4af25c/contentassets/bf87c5fce6fc4f9a889d57ea2e46a27d/sou-2016_85_webb-pdf-med-framsida.pdf?_t_id=1B2M2Y8AsgTpgAmY7PhCfg%3D%3D&_t_q=eh%C3%A4lsa&_t_tags=language%3Asv%2Csiteid%3Ac5a774ab-a6e3-4456-8f59-3bde614ae911&_t_ip=66.249.70

Statens Offentliga utredningar. (2021, januari). delbetänkandet SOU 2021:1 Säker och kostnadseffektiv it-drift – rättsliga förutsättningar för utkontraktering. Retrieved from https://www.riksdagen.se/sv/dokument-lagar/dokument/statens-offentliga-utredningar/saker-och-kostnadseffektiv-it-drift_ZZB31

Stockholms Stad . (n.d.). Kompletteringar till förhandssamråd med IMYs dnr DI-2021-1513. 16.

Stockholms Stad. (2021, februari). Begäran om förhandssamråd (dnr DI-2021-1513).

Stockholms Stad. (2021, februari 18). Konsekvensbedömning avseende dataskydd för tjänsten Azure AD och Teams med begränsad funktionalitet.

Sveriges Kommuner och Regioner (SKR). (2019, maj 5). *Molntjänster och konfidentialitetsbedömning.* Retrieved from https://skr.se/download/18.5024007816e4121cb57c4271/1573646970091/Molntjänster%20och%20konfidentialitetsbedömning_191024_JT_02%20LI%20slutlig%20191019_LI%20rev%20191105.pdf

Sveriges Kommuner och Regioner. (2019, november 11). Molntjänster Cloud Act. Retrieved from https://skr.se/download/18.4d3d64e3177db55b1663107c/1615462780595/Molntj%C3%A4nster%20v%C3%A4gledning%20Cloud%20Act%20191025%20LI%20slutlig.pdf

Sveriges Kommuner och Regioner. (2019, novenber 11). Molntjänster i verksamheten. Retrieved from https://skr.se/download/18.4d3d64e3177db55b1663107e/1615462780788/Molntj%C3%A4nster%20i%20verksamheten_191104_slutlig%20LI%20191104_rev%20191111.pdf

Sveriges Kommuner och Regioner. (2019, 11 27). *Vägledning för molntjänster.* Retrieved from https://skr.se/naringslivarbetedigitalisering/digitalisering/arkitektursakerhet/molntjanster/vagledningarmolntjanster.29885.html

Sveriges riksdag. (2009). *Offentlighets- och sekretesslag (2009:400).* Retrieved from Svensk författningsamling: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/offentlighets--och-sekretesslag-2009400_sfs-2009-400

Sveriges riksdag. (2018). Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning. *Svensk författningsamling*. Justitiedepartementet. Retrieved from https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2018218-med-kompletterande-bestammelser_sfs-2018-218

Sveriges riksdag. (n.d.). Brottsbalk (1962:700). *Svensk författningssamling*. Retrieved from https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/brottsbalk-1962700_sfs-1962-700

Sveriges riksdag. (n.d.). Lag (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter. *Svensk författningssamling*. Retrieved from https://riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2020914-om-tystnadsplikt-vid_sfs-2020-914

Sveriges Riksdag. (n.d.). Tryckfrihetsförordningens (1949:105). Retrieved from https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/tryckfrihetsforordning-1949105_sfs-1949-105