Förstudierapport Webbaserat kontorsstöd

23.2-6283-18

KAMMARKOLLEGIET

Sammanfattning

Digitaliseringstakten ökar inom offentlig sektor och behovet av moderna it-baserade stöd för fillagring, dokumenthantering, ordbehandling, samarbetsverktyg, e-post och andra funktioner väntas öka. Med den ökade digitaliseringstakten riktas också ljuset allt mer mot offentlig sektors särställning och juridiska förutsättningar.

Statens inköpscentral vid Kammarkollegiet har under lång tid upphandlat ramavtal för programvaror och molntjänster där denna typ av funktioner kan köpas genom avrop. Ramavtalen ger avropande myndigheter stor frihet att beskriva sina behov med vetskap om att ramavtalsleverantörerna kan leverera en stor bredd av lösningar. Samtidigt måste den som avropar ta hänsyn till de juridiska förutsättningar som på olika sätt är speciella för offentlig sektor. Utöver lagen om offentlig upphandling gäller exempelvis regler om arkivering, offentlighet och sekretess samt skyddet för privatlivet. Ytterst ansvarar varje myndighet för att en viss it-lösning kan införas och användas. Det gäller i synnerhet när it-lösningen medför att en extern part ska hantera myndighetens information.

Under 2018 har tre betydande rättsliga förändringar skett i form av EU:s dataskyddsförordning (GDPR), genomförandet av EU:s NIS-direktiv i svensk lag samt den amerikanska lagen CLOUD Act. I spåren av detta kom ett uttalande från eSamverkansprogrammets juridisk expertgrupp som noterade att problem kan uppstå kring sekretess för uppgifter i molntjänster. Vidare ersätts under 2019 säkerhetsskyddslagen med en lag som dels är mer långtgående, dels berör långt fler.

Komplexiteten i den kravställning som krävs, såväl tekniskt som juridiskt, har ökat markant. Utgångspunkten i förstudien har därför varit att undersöka om ett nytt ramavtal, som redan på ramavtalsnivå kravställer på rätt sätt, skulle underlätta för myndigheter att anskaffa och använda de funktioner som i förstudien benämns Webbaserat kontorsstöd.

Svensk offentlig sektor är i hög grad decentraliserad där kommuner, regioner och statliga myndigheter var för sig fattar sina egna beslut när det gäller it. Lagstiftning som säkerhetsskyddslagen och dataskyddsförordningen ställer skarpare krav när en leverantör ska hantera en större uppgiftsmängd. En ytterligare utgångspunkt har därför varit att bedöma hur olika regelverk skulle kunna påverka Webbaserat kontorsstöd vid utbredd användning i offentlig sektor.

Förstudien visar att det framstår som möjligt att upphandla Webbaserat kontorsstöd som både är tekniskt och rättsligt godtagbart. Det förutsätter dock att offentlig sektor tillsammans med marknaden först har tagit tillräckliga initiativ för att påvisa ett konkret behov och investeringsvilja. Statens inköpscentral ser positivt på att bidra till sådana initiativ med sin kompetens och erfarenhet. Det föreslås att Statens inköpscentral tillsvidare, och innan andra initiativ är etablerade, genomför en fördjupad dialog med offentlig sektor samt företrädare från it-branschen som på egen hand har förmåga att leverera hela eller stora delar av Webbaserat kontorsstöd. Projektgruppen rekommenderar att Statens inköpscentral, när en marknad har etablerats, upphandlar ramavtal för Webbaserat kontorsstöd som kan användas av hela offentlig sektor.

Summary

The pace of digitalisation in Sweden's public sector is accelerating and the need for modern IT-based tools for file storage, document management, word processing, collaboration, e-mail and other functions is only expected to grow.

The National Procurement Services is a major central purchasing body for Sweden's public sector, and a department of Kammarkollegiet, the Swedish Legal, Financial and Administrative Services Agency. The National Procurement Services has for a long time concluded framework agreements for software and services, which facilitate the purchasing of office suites through call-offs. The framework agreements give the procuring public sector entities great leeway to describe their specific needs, in the knowledge that the framework agreement vendors can deliver a wide range of solutions. Meanwhile, the procurer must observe the legal requirements which apply in different ways to the public sector in particular. Besides the public procurement act, there are regulations concerning for example, long-term archiving, data privacy and public access to information and secrecy. Ultimately, each public sector entity is responsible for making sure an envisaged IT solution may be implemented and used. This applies in particular when the IT solution may involve an external party processing the public sector entity's data.

During 2018, three significant legal changes took place in the form of the EU General Data Protection Regulation, the EU Network and Information Security directive's transposition into Swedish law as well as the enactment of the American legislation CLOUD Act. Following this, a legal expert group within the eSamverkansprogrammet collaboration between 23 central government agencies and the Swedish Association of Local Authorities and Regions, made a statement about potential issues concerning secrecy for public sector data in cloud services. Furthermore, during 2019, the Swedish Security Protection Act is replaced with a new, more demanding law which will also affect a greater number of organisations. The required complexity in specifying procurement requirements, both technical and legal, has increased significantly. The starting point of this pre-study has therefore been to investigate whether a new framework agreement, which defines the correct requirements at a framework level, would facilitate public sector procurement and use of a web-based office suite.

Sweden's public sector is to a high degree decentralised, where municipalities, regions and central government agencies each make their own independent decisions regarding IT. Legislation such as the Swedish Security Protection Act and the GDPR impose more stringent requirements when a vendor is handling a large amount of data. Another starting point has therefore been to assess how different rules could affect a web-based office suite if used at a large scale in the public sector.

The pre-study shows that it appears possible to procure a web-based office suite which is both technically and legally acceptable. This presupposes that the public sector together with market actors take the required initiatives to demonstrate a substantial need and willingness to invest. The National Procurement Services looks forward to contributing to such initiatives with its competence and experience. Going forward, and until other

initiatives are established, it is proposed that the National Procurement Services conducts a deeper dialogue with the public sector and IT industry representatives which on their own have the capacity to either deliver an envisaged web-based office suite in its entirety or in great part. The project group recommends that the National Procurement Services, when a market is established, conducts a public procurement process resulting in a framework agreement where vendors can offer web-based office suites usable by all parts of the public sector.

Innehåll

1 Inledning

1.1 Bakgrund till förstudien

Förstudien om Webbaserat kontorsstöd är genomförd av Statens inköpscentral vid Kammarkollegiet. Webbaserat kontorsstöd omfattar fillagring, dokumenthantering, samarbetsverktyg, ordbehandling, e-post och andra funktioner som tillhandahålls slutanvändaren i en webbläsare. I förstudien har utgångspunkten varit att den bakomliggande driften ska kunna skötas antingen hos en leverantör eller av myndigheten själv.

Enligt förordning (1998:796) om statlig inköpssamordning ska det finnas ramavtal eller andra gemensamma avtal som effektiviserar upphandlingar av varor och tjänster som myndigheterna upphandlar ofta, i stor omfattning eller som uppgår till stora värden. Statens inköpscentral ansvarar för upphandlingsverksamheten inom den statliga inköpssamordningen och för att dessa ramavtal ingås.

Statens inköpscentral har uppfattat att myndigheter har ett stort behov av att använda den typ av verktyg som Webbaserat kontorsstöd utgör men att det föreligger viss osäkerhet gällande rättsläget för t.ex. hantering av känslig eller sekretessbelagd information. Statens inköpscentral har i dagsläget inget specifikt ramavtal för Webbaserat kontorsstöd som kravställts för att tillgodose de komplexa funktionella, tekniska och rättsliga krav som myndigheter har att ta hänsyn till. De nuvarande ramavtalen inom familjen ”Program-varor och tjänster” är upphandlade utifrån perspektivet att ramavtals-leverantörerna ska kunna tillhandahålla flera olika typer av programvaror och moln-tjänster. En myndighet som vill avropa funktionalitet motsvarande Webbaserat kontors-stöd behöver inför avrop genomföra ett eget kravställningsarbete med hänsyn till gällande lag och förordning. Ett sådant arbete kan mynna ut i att regelverken rörande handlingars sekretess, Sveriges säkerhet och den personliga integriteten förhindrar nyttjandet av befintliga molntjänster på marknaden, eller åtminstone gör dem olämpliga att använda på önskat sätt.

Statens inköpscentral initierade därför denna förstudie för att försöka klarlägga vilka behov myndigheterna har, vilka tjänster marknaden erbjuder samt vilka rättsliga utmaningar som finns inom området. Om tillräckligt stort behov finns, om ett nytt ramavtal skulle effektivisera för myndigheter samt om marknaden kan erbjuda rätt lösningar, kan det vara lämpligt att genomföra en ramavtalsupphandling. Ett eventuellt kommande ramavtal för Webbaserat kontorsstöd är tänkt att kunna användas för avrop av statliga myndigheter under regeringen samt andra upphandlande myndigheter som lämnar bekräftelse på att vara avropsberättigade, främst kommuner och regioner. I denna förstudierapport benämns samtliga dessa som ”myndigheter”.

1.2 Mål med förstudien

Syftet med förstudien har varit att samla information och kunskap om Webbaserat kontorsstöd, samt om de behov som myndigheterna har. Förstudien belyser även på ett övergripande plan hur en ramavtalsupphandling skulle kunna genomföras, i vilken uträckning det skulle krävas stöd från Statens inköpscentral samt samverkan med leverantörer och myndigheter gällande upplägg och kravställning.

Samtliga rekommendationer som lämnas i samband med denna förstudie kan komma att prövas på nytt, ändras och anpassas inför eller under en kommande ramavtalsupphandling då ny information kan tillkomma och förutsättningar kan ändras med tiden.

1.3 Avgränsningar

Syftet med förstudierapporten har inte varit att ta fram en kravspecifikation till en kommande ramavtalsupphandling varför eventuella kravställningar endast är beskrivna på en övergripande nivå.

Förstudierapporten gör inte heller anspråk på att vara en heltäckande analys av teknik, marknad, juridik eller behov. Framförallt gäller detta de rättsliga analyserna. Dessa är strikt avgränsade till Webbaserat kontorsstöd och tar endast upp delar som projektgruppen uppfattat som relevanta. Det finns därför sannolikt ytterligare regelverk som dock inte berörs i förstudierapporten.

1.4 Målgrupp

Förstudien riktar sig i första hand till följande målgrupper:

- Statens inköpscentral
- Statliga myndigheter, kommuner, regioner och andra upphandlande myndigheter
- Leverantörer

1.5 Metod för förstudien

Förstudiearbetet har utförts i enlighet med Statens inköpscentrals projektstyrnings-metodik.

Informationsinsamlingen till förstudien har skett genom möten med olika leverantörer, externa experter och företrädare för expertmyndigheter. Därtill har en referensgrupp med deltagare från olika myndigheter deltagit och bidragit med värdefull information och synpunkter.

I förstudierapporten görs en samlad bedömning av all information som inkommit för att på så sätt undersöka om en ramavtalsupphandling inom området är lämplig. Det kan innebära att förslag från enskilda intressenter inte alltid har beaktats.

1.6 Projektgrupp

Förstudiens projektgrupp har bestått av Daniel Melin (projektledare), Arman Borghem och Karl Ekman. Emma Dufva var projektets jurist.

I beredningen har enhetscheferna Hans Sundström och Anna Ekberg deltagit. Förstudierapporten är därefter fastställd av avdelningschef Anna Clara Törnvall Wittgren.

Projektgruppen vill tacka referensgruppen och särskilt tacka Eva Maria Broberg Lennartsson, Monica Kruseke och Pontus Blomqvist för värdefulla bidrag och detaljgranskning.

2 Omfattning

2.1 Omfattning

Med Webbaserat kontorsstöd avses en hel kontorsarbetsplats som tillhandahålls slutanvändaren i en webbläsare. Grundnivå på funktioner i kontorsarbetsplatsen är minst:

- Chatt
- Dokumenthantering
- E-post
- Fillagring
- Kalender
- Kalkylark
- Kontakter
- Ordbehandling
- Presentationsverktyg
- Videokonferens

Förstudierapporten utgår från att en tjänsteman ska kunna använda all funktionalitet i Webbaserat kontorsstöd oavsett val av operativsystem eller webbläsare. Ingen programvara, utöver webbläsare, ska krävas för slutanvändaren. För mobila enheter kan dock appar behövas som komplement.

Webbaserat kontorsstöd skulle principiellt kunna levereras som en publik molntjänst, privat molntjänst eller programvaror som myndigheten installerar i eget datacenter. I förstudierapporten är perspektivet oftast att en leverantör tillhandahåller Webbaserat kontorsstöd som publik molntjänst.

Ett grundläggande krav på alla funktioner i Webbaserat kontorsstöd är att de ska stödja ett modernt kollaborativt arbetssätt där tjänstemän på myndigheter enkelt och säkert ska

kunna skapa och dela information. Det innebär t.ex. att funktionen för ordbehandling ska möjliggöra att flera tjänstemän arbetar i samma dokument samtidigt och att handlingar enkelt och säkert kan flöda genom myndigheten.

Ett ytterligare grundläggande synsätt i förstudien är att se offentlig sektor som en helhet för att kunna bedöma hur olika regelverk påverkar Webbaserat kontorsstöd. Offentlig sektor i Sverige är i hög grad decentraliserad där kommuner, regioner och statliga myndigheter var för sig fattar sina egna beslut när det gäller it. Lagstiftning som t.ex. den nya säkerhetsskyddslagen och dataskyddsförordningen ställer upp högre krav när mängden information ökar.

Förstudierapporten innehåller både myndigheters och leverantörers synpunkter på Webbaserat kontorsstöd samt en analys av myndigheters behov och marknadens utbud.

Slutligen sammanfattas all information i ett antal slutsatser och en rekommendation.

3 Myndighetsperspektiv

3.1 Inledning

För att kartlägga behovet hos myndigheter gällande Webbaserat kontorsstöd har det i förstudien genomförts två referensgruppsmöten med deltagare från statliga myndigheter, regioner, kommuner och närliggande organisationer vilka återges i avsnitt 14.1. Detta kapitel berör den information projektgruppen inhämtat från dessa.

3.2 Referensgrupp

De myndigheter som anmält intresse att medverka i referensgruppen bjöds in till möten med projektgruppen. Sammanlagt deltog 20 myndigheter i referensgruppen. Referensgruppens deltagare bestod av bl.a. verksjurister, it-chefer, it-säkerhetsansvariga, it-arkitekter samt informationssäkerhetsansvariga.

Syftet med referensgruppsmötena var att diskutera myndigheternas behov och uppfattning rörande de juridiska, tekniska och funktionella behoven kopplade till Webbaserat kontorsstöd.

3.3 Nuläge

Alla myndigheter behöver de funktioner som ingår i Webbaserat kontorsstöd eftersom dessa funktioner är helt grundläggande för en myndighet. De flesta myndigheter använder

i nuläget lokalt installerade programvaror för de funktioner som ingår i Webbaserat kontorsstöd, men det finns många som redan idag använder Webbaserat kontorsstöd i form av en publik molntjänst.

Den absoluta merparten av myndigheterna använder, oavsett lokalt installerade programvaror eller publik molntjänst, Microsoft som leverantör för funktionerna som omfattas av Webbaserat kontorsstöd. Andra förekommande leverantörer är t.ex. Alfresco, Google, IBM, Libreoffice och Micro Focus.

Många myndigheter ser fördelar i att slippa lokalt installerade programvaror som ska underhållas samt att de återkommande är föremål för licensrevision av licensgivarna. Noteras kan också att trenden hos flera licensgivare är att molntjänster ska vara den enda leveransformen alternativt den primära leveransformen. Flera licensgivare har upphört med nyförsäljning av lokalt installerade programvaror, andra har aviserat att dessa snart kommer att upphöra att säljas. Många myndigheter upplever därför att de inte har något egentligt val gällande byte från lokalt installerade programvaror till molntjänster alternativt byte till andra programvaror.

Hos myndigheter där det förekommer viss säkerhetskänslig verksamhet används ofta ett helt avskilt nätverk i avskilda lokaler. Sådana myndigheter behöver väl fungerande kontorsstöd även i dessa avskilda miljöer, men eftersom anslutning till internet inte får finnas kan varken en privat eller publik molntjänst användas. I en skyddad och avskild it-miljö kan inte allt fungera likadant som i den öppna it-miljön men behovet av bra kontorsstöd finns likväl. Det vore därför bra om Webbaserat kontorsstöd även fanns för leverans där myndigheten själv sköter driften.

Alla myndigheters verksamhet ska bedrivas effektivt och säkert för att medborgarna ska ha tillit till det allmänna och att samhället i stort ska fungera väl. Referensgruppen ansåg att kraven på effektivitet och hushållande med resurser ibland ställs mot krav på t.ex. säkerhet och regelefterlevnad.

En reflektion av referensgruppen var att it-funktionen på en myndighet typiskt sett ska erbjuda moderna och säkra verktyg till verksamheten, men verksamheten är ibland missnöjd med verktygen och skaffar egna verktyg utanför it-funktionens kontroll. En vanligt förekommande typ av sådana verktyg är fillagring som molntjänst. Det är därför positivt om Webbaserat kontorsstöd kan erbjuda ett effektivt och juridiskt hållbart verktyg för t.ex. fillagring.

3.4 Funktionalitet

Referensgruppen ansåg att den grundnivå på funktioner som projektgruppen föreslagit är lämplig. Grundnivån ansågs innehålla alla väsentliga delar som alla myndigheter i princip behöver. Funktioner som referensgruppen ansåg vore positivt om de tillkom var någon form av enklare projekthantering, t.ex. för agila projekt eller interna projekt av enklare karaktär, digitala signaturer, möjlighet att informationsklassa handlingar samt enklare ärendehantering där t.ex. ett dokument kan flöda mellan handläggare.

Referensgruppen ansåg att det är kritiskt att Webbaserat kontorsstöd skyddas mot t.ex. dataläckage, intrång, virus och spam.

3.5 Tillgänglighet

Referensgruppen ombads fundera över vilka konsekvenser över tid det skulle få för deras respektive myndighet om Webbaserat kontorsstöd var otillgängligt. Vissa myndigheter skulle få mycket stora problem att sköta sin verksamhet redan efter en arbetsdag medan andra når en kritisk punkt efter ungefär en vecka. De myndigheter som absolut inte klarar någon större otillgänglighet har ofta någon form av sekundär lösning för att hjälpligt kunna fortsätta arbeta. Regioner som går in i stabsläge uppgav att de inte bör ha något beroende till Webbaserat kontorsstöd för det som är vårdrelaterat, men för övrig verksamhet inom regionen blir det kritiskt efter 1 – 2 dygn.

Referensgruppen gjorde ett generellt antagande att om en kommun har hela sitt kontorsstöd i en molntjänst, innebärande att lokalt installerad kontorsstödsprogramvara är borta samt lokal fillagring har upphört, påverkas de administrativa funktionerna redan efter en arbetsdag. Skolan påverkas, vård och omsorg kan drabbas av problem och även kommunens kontakter med medborgare och andra berörs. Efter två dygn accelererar problemen för administrationen och kommunens handläggning av ärenden får problem. Även utbyte av information mellan olika vård- och omsorgsgivare kan bli problematisk. Efter en vecka har allt som tidigare angetts ovan blivit ännu värre, den politiska processen står i princip stilla då ärendehanteringen är kraftigt påverkad, flera administrativa kommunala funktioner fungerar inte alls och det blir stora störningar i alla övriga delar av kommunen då nästan all kommunikation med såväl externa som interna parter går via e-post. Om en majoritet av Sveriges kommuner använder samma molntjänst blir det sannolikt snabbt en väldigt allvarlig situation om den blir otillgänglig. En kommun kan i denna situation hitta på olika temporära lösningar för att försöka få det mesta att fungera, t.ex. telefon, fax, privat e-post, fysiska möten och USB-minnen. Däremot kan detta innebära att tillämpliga lagar och regler kringgås, i synnerhet sådana som syftar till att upprätthålla säkerhet och sekretess.

Delar av referensgruppens resonemang bekräftas av Myndigheten för samhällsskydd och beredskaps (MSB) studie ”Säkerhet vid molnlösningar”. I studien framkommer hur olika kommuner och statliga myndigheter bedömer konsekvenserna av avbrott i molntjänster vid olika tidsintervall. Efter ett dygn bedömer kommuner att det överlag får få konsekvenser, dock beroende på specifika tider på året och verksamhetsområde. Inom vård och omsorg kan det få stora konsekvenser. Statliga myndigheter bedömer att det överlag får få konsekvenser men allvarsgraden varierar beroende på myndighetens verksamhet och vilka system som berörs. Efter två dygn bedömer kommuner att det börjar bli kännbart, men beroende på verksamhet kan det bli kritiskt. Statliga myndigheter bedömer att det börjar bli kritiskt. Efter en vecka bedömer kommuner att det är kritiskt för flera delar av verksamheten, medan statliga myndigheter bedömer att det för vissa myndigheter är kritiskt.

Referensgruppen påtalade att avtalsvillkoren gällande tillgänglighet hos flera molntjänstleverantörer innebär att leverantören förbundit sig att göra sitt bästa för att

hålla tjänsten tillgänglig men att det inte lämnas några garantier. Dessutom kan leverantören ensidigt förändra tjänsten under avtalstiden. Referensgruppen såg detta som ett övergripande problem för offentlig sektor om många myndigheter använder samma molntjänst för Webbaserat kontorsstöd.

3.6 Sekretess

Myndigheter samlar in och hanterar stora mängder information som inte sällan är känslig. Sekretessreglerna finns för att skydda uppgifter som myndigheter hanterar, och som lagstiftaren bedömt inte ska vara offentliga. Enskilda personer kan inte välja eller påverka om uppgifter ska lämnas till eller hanteras av en myndighet varför det är av stor vikt att tjänster som används för myndigheters informationshantering gör det enkelt att följa de regelverk som finns för att skydda enskildas integritet, såsom sekretessregler och dataskyddsförordningen.

Referensgruppen noterade att eftersom myndigheter kan komma att hantera både personuppgifter och sekretessbelagd information bör Webbaserat kontorsstöd kravställas utifrån det.

3.7 Informationsklassning

Informationsklassning görs utifrån aspekterna konfidentialitet, riktighet och tillgänglighet och är en metod för att identifiera vilken skada en organisation och andra kan få om informationen inte hanteras utifrån organisationens och andras behov. Statliga myndigheter och leverantörer av samhällsviktiga tjänster måste genomföra informationsklassning utifrån konfidentialitet, riktighet och tillgänglighet enligt MSB:s föreskrifter MSBFS 2016:1 och MSBFS 2018:8. Övriga myndigheter genomför ofta informationsklassning efter rekommendationer från egna samverkansorganisationer, t.ex. erbjuder Sveriges kommuner och landsting ett verktyg för att genomföra informationsklassning.

Referensgruppen uppgav att ett vanligt förhållningssätt bland myndigheter är att information först klassificeras som t.ex. öppen information, begränsat öppen information, känslig information eller mycket känslig information. Har information klassificerats som mycket känslig kan den, men måste inte, dessutom säkerhetsskyddsklassificeras och därmed hamna inom säkerhetsskyddslagens område. Informationen behöver då klassificeras i enlighet med nivåerna som anges i säkerhetsskyddslagen.

Klassificeringen behöver ibland göras om, eftersom informationsklassningen kan ändras över tid. Aggregering av information kan också påverka informationsklassningen. Det går därför inte att förhålla sig till informationsklassning som något statiskt eller som något som bedöms vid en given tidpunkt.

Referensgruppen ansåg att Webbaserat kontorsstöd bör ha inbyggt stöd för informationsklassificering.

3.8 Statens inköpscentrals roll

Referensgruppen såg ett behov av omfattande revision hos leverantörer för att kunna säkerställa att ramavtalet efterlevs, särskilt hanteringen av personuppgifter och sekretessreglerade uppgifter. För att effektivisera revision framfördes önskemålet att Statens inköpscentral, om möjligt, skulle kunna genomföra revision åt hela offentlig sektor.

Referensgruppen påtalade att det kan vara problematiskt att säkerställa vilka underleverantörer som deltar i en tjänsteleverans samt hur revision och uppföljning av dessa ska kunna hanteras. Referensgruppen ansåg därför att det är en fördel om Statens inköpscentral ställer krav på leverantörernas användande av underleverantörer. Förslag från referensgruppen var att antalet underleverantörer hålls nere, revisioner även sker hos underleverantörer samt långtgående krav på leverantören när denne vill anlita en underleverantör.

3.9 Sammanfattning

Referensgruppen upplevde utvecklingen på marknaden, bort från lokalt installerade programvaror, som mycket påtaglig. Referensgruppen menade att oavsett vad de helst skulle önska, behöver de förr eller senare byta ut nuvarande lokalt installerade programvaror och ersätta dem med någon form av Webbaserat kontorsstöd.

Referensgruppen är också generellt sett positiv till ett mer modernt verktyg som också möjliggör ett modernare arbetssätt. De legala farhågorna och orosmomenten upplevdes dock som stora. Det rådde enighet om att mer vägledning behövs och att ett särskilt ramavtal avseende Webbaserat kontorsstöd troligen skulle kunna vara till stor nytta.

4 Personuppgiftsbehandling

4.1 Inledning

Personuppgiftsbehandling är en integrerad och självklar del av Webbaserat kontorsstöd. Myndighetsanställda som använder Webbaserat kontorsstöd behöver personliga konton som möjliggör exempelvis autentisering, e-postadresser, identiteter vid samverkan, styrning av behörigheter samt spårbarhet kring vem som gjort vad. Varje personligt konto är då knutet till en specifik individ vilket i sig innebär personuppgiftsbehandling när Webbaserat kontorsstöd hanterar dessa personliga konton. Utöver denna personuppgiftsbehandling tillkommer personuppgiftsbehandling inom ramen för myndighetens verksamhet, främst när personuppgifter hanteras i handlingar som inkommer till, skapas i eller lagras i Webbaserat kontorsstöd. Inkommande e-post innebär oundvikligen att

myndigheten regelmässigt tar emot personuppgifter som hanteras i Webbaserat kontorsstöd.

Vid behandling av personuppgifter tillämpas framför allt dataskyddsförordningen (GDPR, General Data Protection Regulation) som skyddar rätten till privatlivet. Dataskyddsförordningen gäller i hela EU och EES och ska för de ingående ländernas medborgare tillförsäkra en enhetlig nivå för skyddet av personuppgifter.

4.2 Rättslig grund, ansvarig och biträde

Enligt dataskyddsförordningen måste behandling av personuppgifter vila på en av flera i förordningen angivna rättsliga grunder. I annat fall är behandlingen inte laglig. Utifrån den konkreta personuppgiftsbehandlingens art och omfattning måste dessutom lämpliga tekniska och organisatoriska åtgärder vidtas. Webbaserat kontorsstöd bör därför utformas så att samtliga rättsliga, tekniska och organisatoriska krav kan uppfyllas av en myndighet vid alla former av personuppgiftsbehandling som krävs dels för att myndighetens anställda kan använda Webbaserat kontorsstöd, dels för den personuppgiftsbehandling som myndigheten har rätt att utföra inom ramen för sitt uppdrag.

Personuppgiftsansvarig är den som ensam eller tillsammans med andra bestämmer ändamålen och medlen för behandling av personuppgifter. En myndighet är således personuppgiftsansvarig och ger då leverantören instruktioner om i vilka syften och på vilket sätt personuppgifterna ska behandlas. Leverantören är i sin tur personuppgiftsbiträde i den utsträckning leverantören behandlar personuppgifter för den personuppgiftsansvariges räkning. Skulle leverantören bestämma ändamålen och medlen för någon del av personuppgiftsbehandlingen i Webbaserat kontorsstöd, antingen själv eller genom att leverantören anses ha ett delat personuppgiftsansvar tillsammans med myndigheten, kräver även sådan personuppgiftsbehandling en rättslig grund för leverantörens del. Det är därför viktigt att understryka att Webbaserat kontorsstöd inte får leda till behandling av personuppgifter för leverantörens egna syften, exempelvis där leverantören gör analyser i syfte att skapa eller tillhandahålla andra tjänster.

Det finns exempel där myndighetsanställda vid användning av en upphandlad programvara eller molntjänst ombetts lämna samtycke för personuppgiftsbehandling direkt mot leverantören. Sannolikt är dock samtycke olämpligt som rättslig grund när myndighetsanställda ska använda en tjänst av Webbaserat kontorsstöds karaktär. Myndighetsanställda behöver då som individer ta ställning till en behandling där leverantören har ett personuppgiftsansvar som eventuellt delas med myndigheten. Samtycke enligt dataskyddsförordningen bygger dock på verklig frivillighet och den anställde kan svårligen anses göra ett frivilligt val gentemot sin arbetsgivare. I vart fall framstår det som olämpligt att avkräva samtycke för personuppgiftsbehandling från enskilda anställda för att de ska få tillgång till önskvärd funktionalitet i Webbaserat kontorsstöd.

Behandlingen av den anställdes personuppgifter bör vila på någon annan rättslig grund som enligt dataskyddsförordningen är användbar för myndigheter, t.ex. fullgörande av avtal (anställningsavtalet). Det bör vidare noteras att den anställde inte kan samtycka å

andras vägnar för personuppgiftsbehandling, som när text med personuppgifter om andra än den anställde bearbetas av leverantören. Myndigheter kan inte heller använda sig av den rättsliga grunden intresseavvägning vid fullgörande av sina uppgifter.

Den personuppgiftsansvarige bär ansvar för att behandlingen sker enligt en giltig rättslig grund. Det är viktigt att säkerställa att myndigheter, i sin egenskap av personuppgiftsansvariga, har kontroll över vilka behandlingar som blivande ramavtalsleverantörer och deras underleverantörer utför i Webbaserat kontorsstöd avseende personuppgifter som myndigheten ansvarar för.

4.3 Underbiträden

En leverantör är personuppgiftsbiträde i den utsträckning leverantören behandlar personuppgifter för den personuppgiftsansvariges (myndighetens) räkning. Ett personuppgiftsbiträde kan i sin tur under vissa förutsättningar anlita s.k. underbiträden för att utföra personuppgiftsbehandling. Underbiträden är också personuppgiftsbiträden men benämns underbiträden, då de anlitas på initiativ av det personuppgiftsbiträde som den personuppgiftsansvarige har sin huvudsakliga avtalsrelation med. I Statens inköpscentrals utkast till personuppgiftsbiträdesavtal, som är en del av de nya ramavtalen inom Programvaror och tjänster, är detta reglerat enligt ett av personuppgiftsansvariges valda alternativ:

1) Personuppgiftsbiträdet har inte rätt att anlita underbiträden. Att helt stänga denna möjlighet kräver stöd i en laglighetsprövning eller risk- och sårbarhetsanalys.
2) Personuppgiftsbiträdet måste inhämta ett skriftligt förhandstillstånd inför anlitandet av varje tänkt underbiträde.
3) Personuppgiftsbiträdet måste underrätta den personuppgiftsansvarige om planerna på att anlita ett underbiträde, men behöver inget aktivt förhandstillstånd. Istället ges den personuppgiftsansvarige en möjlighet att inom skälig tid invända mot det tilltänkta underbiträdet innan det utför någon personuppgiftsbehandling.

Ett särskilt anpassat personuppgiftsbiträdesavtal kommer behöva tas fram avseende Webbaserat kontorsstöd. En modell enligt alternativ 3 ovan framstår då som lämplig. Anlitande av underbiträden innebär inte på något sätt att kraven mildras gällande bundenhet till instruktioner för personuppgiftsbehandling, krav på säkerhetsåtgärder och rättsliga krav i övrigt. Förhållningssättet till personuppgiftsbehandling som utförs av ett underbiträde bör således vara detsamma som till personuppgiftsbehandling som utförs av det huvudsakliga personuppgiftsbiträdet. Det vore fördelaktigt både för leverantörer och myndigheter om antalet biträden kan hållas på en så överskådlig nivå som möjligt. Det bör även övervägas i vilken utsträckning leverantörer ska förse Statens inköpscentral och myndigheter med ytterligare information om ett planerat underbiträde i samband med att en leverantör avser att addera underbiträdet. Ett underbiträdes agerande kan ha effekter som påverkar leverantörens tillhandahållande av Webbaserat kontorsstöd i stort.

4.4 En stabil och tydlig avtalsstruktur

För att säkerställa en laglig behandling av personuppgifter och tillgodose enskilda individers rättigheter är det viktigt att den personuppgiftsansvarige kan förstå den avtalsrättsliga strukturen och praktiskt kan ta till sig avtalsinnehållet. De vanligt förekommande molntjänsterna på marknaden har inte sällan komplexa avtalsstrukturer med ett omfattande antal dokument, hänvisningar och dynamiskt innehåll. Det är heller inte ovanligt att molntjänstleverantören ensam bestämmer över förändringar i molntjänsten, vilket delvis kan vara både nödvändigt och önskvärt men likväl medför en risk att den molntjänst myndigheten anskaffat förändras över tid till nackdel för myndigheten. Vid flitiga ändringar av avtalsvillkoren kan det dessutom vara svårt att hålla sig uppdaterad om vilka delar som ändrats och på vilket sätt.

I stora komplexa molntjänster där flera olika leverantörer i olika led är inblandade, såsom mängder av underbiträden, tillkommer risken att myndigheten ofta inte får se alla avtal mellan de olika leverantörerna. Det är viktigt att säkerställa en konstruktion som är stabil och tydlig även i denna situation.

En eventuellt kommande ramavtalsupphandling bör innehålla en tydlig avtalsstruktur som säkerställer att både leverantören men även dennes underleverantörer förstår ramavtalet och dess innehåll redan på förhand. Även för myndigheterna är detta givetvis en fördel. I ett sådant läge är det dock viktigt att tidigt säkerställa att kraven kommer att uppfyllas. Kraven bör ges erforderlig uppmärksamhet i upphandlingsskedet för att underlätta för anbudsgivarna att förstå vad som behöver efterlevas och vilka åtgärder som behöver vidtas.

4.5 Granskning av personuppgiftsbiträden

Kontraktsuppföljning är centralt eftersom den personuppgiftsansvarige ytterst ansvarar för hanteringen av personuppgifter. Revisionsklausuler kan vara känsliga för leverantörer, dels av affärsmässiga skäl men även när leverantörer har ett stort antal kunder och det kan vara svårt säkerställa att revisionen inte får del av en annan kunds information. Detta fråntar dock inte den personuppgiftsansvariges ansvar från att kontrollera personuppgiftsbiträdet. Datainspektionen har i tillsynsärendet 574-2011 avseende personuppgiftslagen (1998:204) uttalat att tredjepartsrevision kan vara ett sätt att kontrollera en tjänsts säkerhets- och kvalitetskrav men att detta inte fråntar den personuppgiftsansvariges ansvar att kontrollera att personuppgiftsbiträdet verkligen vidtar de säkerhetsåtgärder som krävs. Det framstår inte som alldeles tydligt vilken omfattning en revision måste ha och vilken eventuell kompletterande insyn som krävs för att leva upp till kraven i dataskyddsförordningen. En bedömning måste göras i det enskilda fallet för att uppnå tillräcklig kontroll.

Med tanke på förstudiens omfattning torde den granskning som kommer att behöva ske under ramavtalsperioden vara relativt komplex, vilket innebär att ramavtalsupphandlingen måste säkerställa att kvalificerade leverantörer är införstådda med detta. I den mån det skulle vara möjligt, vilket i så fall måste utredas vidare, kan det vara önskvärt för alla parter att Statens inköpscentral genomför delar av revisionen för att underlätta för både leverantörerna och myndigheterna. Om tillsynsmyndigheten dessutom har möjlighet

att bidra med kompetens skulle det sannolikt vara ytterligare resursbesparande för både myndigheterna, leverantörerna och tillsynsmyndigheten, den största fördelen är dock den förhöjda kvaliteten och en ökad rättslig trygghet.

4.6 Överföring till tredjeland

Dataskyddsförordningen syftar till att säkerställa rätten till privatlivet, en mänsklig rättighet. Genom att länderna i EU och EES är bundna av förordningen och därmed tillämpar ett enhetligt regelverk, främjas det fria flödet av personuppgifter mellan dessa länder. Ett land som inte är bundet av dataskyddsförordningen är ett så kallat tredjeland. Trots att ett tredjeland inte är bundet av just dataskyddsförordningen kan det under vissa omständigheter ändå vara möjligt att överföra personuppgifter dit. Kapitel fem i dataskyddsförordningen (artikel 44 – 50) reglerar vad som krävs för att en tredjelandsöverföring ska vara möjlig. För det första anges i artikel 44 att ”Alla bestämmelser i detta kapitel ska tillämpas för att säkerställa att den nivå på skyddet av fysiska personer som säkerställs genom denna förordning inte undergrävs.” Det är alltså enskilda individer som ska skyddas. Ett säkerställande pekar på att det inte bör vara möjligt att godta tveksamma fall eller situationer där tillräcklig kunskap saknas. En grundläggande del av dataskyddsförordningen som utgör exempel på det skydd som måste upprätthållas, gäller individers tillgång till effektiva rättsmedel för att hävda sina rättigheter och friheter. Detta framgår av mål C-362/14 (Maximillian Schrems mot Data Protection Commissioner), där EU-domstolen anger:

> *En lagstiftning i vilken det inte föreskrivs någon möjlighet för enskilda att använda rättsmedel för att erhålla tillgång till, rätta eller radera uppgifter som rör dem, respekterar inte det väsentliga innehållet i den grundläggande rätten till effektivt domstolsskydd, vilken är stadfäst i artikel 47 i stadgan [EU-stadgan om de grundläggande rättigheterna]. I artikel 47 första stycket i stadgan föreskrivs nämligen att var och en vars unionsrättsligt garanterade fri- och rättigheter har kränkts har rätt till ett effektivt rättsmedel inför en domstol, med beaktande av de villkor som föreskrivs i den artikeln. Möjligheten till en effektiv domstolsprövning i syfte att säkerställa iakttagandet av unionsrätten är härvidlag i sig en grundförutsättning för en rättsstat.*

Artikel 47 i EU-stadgan om de grundläggande rättigheterna lyder i sin helhet:

> ***Rätt till ett effektivt rättsmedel och till en opartisk domstol***
> *Var och en vars unionsrättsligt garanterade fri- och rättigheter har kränkts har rätt till ett effektivt rättsmedel inför en domstol, med beaktande av de villkor som föreskrivs i denna artikel.*
>
> *Var och en har rätt att inom skälig tid få sin sak prövad i en rättvis och offentlig rättegång och inför en oavhängig och opartisk domstol som har inrättats enligt lag. Var och en ska ha möjlighet att erhålla rådgivning, låta sig försvaras och företrädas.*

Rättshjälp ska ges till personer som inte har tillräckliga medel, om denna hjälp är nödvändig för att ge dem en effektiv möjlighet att få sin sak prövad inför domstol.

EU-kommissionen kan efter att ha granskat lagstiftning, internationella åtaganden och en rad andra aspekter i ett tredjeland fatta beslut om att ett tredjeland redan som det är säkerställer en adekvat skyddsnivå i förhållande till dataskyddsförordningen. Mot bakgrund av EU-domstolens praxis gällande dataskyddsdirektivet ”ska begreppet ’adekvat skyddsnivå’ förstås som att det krävs att detta tredjeland, genom sin interna lagstiftning eller på grund av de internationella förpliktelser som åligger landet, de facto säkerställer en nivå för skyddet av grundläggande fri- och rättigheter som är väsentligen likvärdig med den skyddsnivå som garanteras inom unionen”. I enlighet med artikel 45 i dataskyddsförordningen har EU-kommissionen fattat flera beslut om adekvat skyddsnivå för tredjeländer i sin helhet och det tillhandahålls en lista över dessa godkända tredjeländer. Detta underlättar betydligt för den som har personuppgifter som kan komma att överföras till något av dessa tredjeländer. EU-kommissionen ska fortlöpande övervaka att besluten om dessa tredjeländer alltjämt är korrekta och kan ändra eller upphäva besluten.

Har EU-kommissionen inte fattat beslut om att godkänna ett visst tredjeland, kan det under vissa förutsättningar som anges i artikel 46 ändå vara möjligt att överföra personuppgifter till tredjelandet. Ett av villkoren som uttryckligen anges är att det finns tillgång till lagstadgade rättigheter och effektiva rättsmedel för de individer vars personuppgifter behandlas. Utöver denna förutsättning måste den som överför personuppgifterna dessutom först ”ha vidtagit lämpliga skyddsåtgärder”. Enligt artikel 46 kan sådana lämpliga skyddsåtgärder uppnås genom att använda av EU-kommissionen godkända ”standardiserade dataskyddsbestämmelser”, även kallat standardavtalsklausuler. Dessa klausuler är mycket vanligt förekommande vid tredjelandsöverföring och ingås då mellan den personuppgiftsansvarige och personuppgiftsbiträdet. I artikel 46 – 47 finns även andra alternativ för att vidta lämpliga skyddsåtgärder, utöver de vägar som EU-kommissionen kan godkänna. Exempel på sådana vägar inbegriper utfästelser eller avtal, såsom uppförandekoder eller bindande företagsbestämmelser.

Det bör understrykas att tredjelands myndigheter inte är part i eller på något sätt bundna av villkoren i standardavtalsklausuler, uppförandekoder eller bindande företagsbestämmelser varför användning av dessa verktyg inte i sig möjliggör överföring till tredjeland. För att överföring med dessa verktyg ska vara godtagbart måste det dessutom finnas tillgång till lagstadgade rättigheter och effektiva rättsmedel för de individer vars personuppgifter behandlas. Det går utöver vad enskilda avtalsparter, som en svensk myndighet och en molntjänstleverantör, råder över och kan avtala om. En bedömning av lagstadgade rättigheter och effektiva rättsmedel måste göras från land till land. I sammanhanget kan noteras det omfattande antal aspekter som EU-kommissionen har att beakta enligt artikel 45.2 innan EU-kommissionen kan fatta beslut om adekvat skyddsnivå i ett tredjeland.

Som nämnts har EU-kommissionen beslutat att vissa länder säkerställer en adekvat skyddsnivå i sin helhet. Dessa är för närvarande Andorra, Argentina, Bailiwick of Guernsey, Färöarna, Israel, Isle of Man, Jersey, Nya Zeeland, Schweiz och Uruguay. Därtill

har EU-kommissionen fattat beslut om adekvat skyddsnivå gällande organisationer i Kanada när kanadensisk lagstiftning för skydd av personuppgifter i privat sektor är tillämplig på mottagarens personuppgiftsbehandling, samt gällande överföringar till USA om mottagaren anslutit sig till Privacy Shield.

Privacy Shield är en överenskommelse som ingicks 2016 mellan EU-kommissionen och USA om överföring av personuppgifter från EU till vissa organisationer i USA. Privacy Shield innefattar dels ett antal principer för hur personuppgifter som överförs från EU till USA kan hanteras, dels en mekanism för företag att ansluta sig till principerna samt viss tillsyn för att se till att företagen verkligen följer principerna. Även om skyddet vid behandling av personuppgifter i USA normalt sett inte är väsentligen likvärdigt skyddet inom EU, är tanken att personuppgiftsbehandling inom just Privacy Shield-ramverket sker med säkerställande av en adekvat skyddsnivå. Privacy Shield ger således ingen generell möjlighet att överföra personuppgifter till USA utan förutsätter att den som behandlar personuppgifterna i USA lovat att underkasta sig principerna och regelverket i Privacy Shield. Dessutom måste företaget först ha godkänts av amerikanska myndigheter innan en överföring under Privacy Shield kan bli möjlig.

Företag i USA kan anmäla till det amerikanska handelsministeriet att de vill ansluta sig till Privacy Shield och handelsministeriet tillhandahåller en lista över godkända organisationer. När ett företag har tagits upp på handelsministeriets lista anser EU-kommissionen att överföring till företaget uppnår en adekvat skyddsnivå. Precis som med de tredjeländer som EU-kommissionen godkänt i sin helhet, genomför EU-kommissionen regelbundet översyn för att se till att överföringar inom Privacy Shield-ramverket fortsatt säkerställer en adekvat skyddsnivå. Finns brister kan EU-kommissionen ändra eller upphäva beslutet om att Privacy Shield säkerställer en adekvat skyddsnivå. Ytterst kan ett beslut om adekvat skyddsnivå även bli föremål för domstolsprövning och upphävas.

4.7 Tredjelands rättsordning

Myndigheter i tredjeland är bundna till att följa och verkställa tredjelandets rättsordning. Som tidigare nämnts är ett tredjelands myndigheter inte part i eller bundna av villkoren i standardavtalsklausuler, uppförandekoder eller bindande företagsbestämmelser varför användning av dessa verktyg i sig inte möjliggör överföring till tredjeland. Om överföring med hänvisning till något av dessa verktyg ska vara godtagbart måste det även finnas tillgång till lagstadgade rättigheter och effektiva rättsmedel för de individer vars personuppgifter behandlas.

Komplexiteten i olika tredjeländers regelverk för personuppgiftsbehandling kan skilja sig åt men varje personuppgiftsansvarig har alltid ett ansvar för att en tredjelandsöverföring är rättsligt korrekt. Även vid överföring till ett tredjeland som EU-kommissionen beslutat säkerställer en adekvat skyddsnivå, bör påminnas om att EU-kommissionens beslut kan komma att upphävas i domstol. Frågan är särskilt relevant när det gäller USA, där EU-kommissionens tidigare beslut om adekvat skyddsnivå vid överföringar till USA, inom Safe Harbour-ramverket, upphävdes av EU-domstolen.

Som tidigare nämnts genomför EU-kommissionen regelbundet översyn av Privacy Shield, och det publiceras en årlig granskningsrapport. I EU-kommissionens andra årliga rapport från december 2018 framkom att vissa framsteg gjorts sedan den förra översynen. Det framkom också att USA fortfarande inte utnämnt en permanent tillsatt ombudsman i enlighet med ramverket och att det i synnerhet efterfrågas att USA bekräftar sitt politiska engagemang för ombudsmannamekanismen. En oberoende ombudsman ska enligt Privacy Shield-ramverket inrättas som en tillsynsmekanism ”för ingrepp som hör samman med nationell säkerhet” och återspegla ett åtagande från USA att ”ta itu med och åtgärda klagomål från enskilda i EU”. Det kan nämnas att överföringar enligt standardavtalsklausuler och bindande företagsbestämmelser också omfattas av ombudsmannamekanismen. EU-kommissionen noterade i sin rapport att det endast fanns en tillförordnad ombudsman, att avsaknaden av en permanent tillsatt ombudsman var ”mycket otillfredsställande” samt att EU-kommissionen övervägde att vidta lämpliga åtgärder enligt dataskyddsförordningen om ingen valts ut för posten senast den 28 februari 2019. Vid förstudierapportens publicering har presidentämbetet namngivit en tilltänkt ombudsman, men denne har ännu inte genomgått den process som krävs för att tillträda.

Ombudsmannens uppgift analyserades av den irländska domstolen High Court i ett mål om personuppgiftsbehandling och överföring till tredjeland. High Court angav att det synes finnas ett välgrundat argument för att ombudsmannamekanismen inte respekterar det väsentliga innehållet i den grundläggande rätten till effektivt domstolsskydd, som är stadfäst i artikel 47 i EU-stadgan om de grundläggande rättigheterna. High Court noterade flera problematiska aspekter, bl.a. att ombudsmannen inte ger EU-medborgare rättsligt skydd, att den inte är en domare och att den inte tycks vara självständig från den verkställande makten i USA. High Court lade särskild vikt vid att ombudsmannens beslut inte är föremål för domstolsprövning. High Court noterade att om en EU-medborgares personuppgifter olagligen behandlats, har den vars rätt trätts förnär uppenbarligen inte möjlighet att få vare sig skadestånd, ett beslut som förhindrar ytterligare överträdelser eller ens en utfästelse med den innebörden. Detta beror på att ombudsmannen varken bekräftar eller förnekar huruvida en individ varit föremål för elektronisk övervakning. Det kan noteras att High Courts anmärkningar kvarstår oavsett om ombudsmannen är tillförordnad eller permanent tillsatt.

I EU-kommissionens översyn deltar även representanter från den Europeiska Dataskyddsstyrelsen (European Data Protection Board, EDPB), som publicerar en egen rapport från den årliga granskningen. Bildandet av EDPB slås fast i dataskyddsförordningen. Det är en oberoende EU-organisation med representanter från EU-ländernas tillsynsmyndigheter för personuppgiftsbehandling. Organisationen har som syfte att främja en enhetlig tillämpning av dataskyddsförordningen. Gällande ombudsmannamekanismen anger EDPB i sin rapport att ombudsmannen saknar tillräckliga befogenheter och att den för närvarande inte kan leva upp till kraven på ett effektivt rättsmedel inför en domstol enligt artikel 47 i EU:s stadga om de grundläggande rättigheterna.

I det irländska målet angav High Court att Privacy Shield-ramverket består av tre skyddskomponenter: “In essence, [the safeguards set out in the Privacy Shield Decision] are threefold: the protections based upon the privacy shield principles (which are essentially private law remedies), the provisions of US law and the Privacy Shield Ombudsperson

mechanism." Privacy Shield-principerna är väsentligen privaträttsliga åtgärder, dvs. inte sådana garantier av lagstadgat slag som EU-rätten kräver. Ombudsmannamekanismen har redan behandlats. Därmed återstår att beröra vilket skydd amerikansk rätt ger.

EU-kommissionen ansåg i sin andra årliga rapport om Privacy Shield att den lagstiftning som var viktigast i förhållande till myndigheters åtkomst till personuppgifter gällde sektion 702 av Foreign Intelligence Surveillance Act, FISA. FISA sektion 702 möjliggör för amerikanska underrättelsemyndigheter att samla på information om icke-amerikanska medborgare som rimligen kan antas ("reasonably believed") befinna sig utanför USA. Den domstol som handlägger dessa ärenden är Foreign Intelligence Surveillance Court, FISC. Enligt den irländska domstolen High Court är alla förhandlingar i FISC som utgångspunkt hemliga, dock finns en möjlighet till beslut om offentliggörande. High Court angav vidare att amerikanska myndigheter enligt FISA kan inhämta och spara en EU-medborgares personuppgifter utan att bevisa sannolika skäl ("probable cause") till FISC relaterade till motiven till inhämtningen om EU-medborgaren. High Court angav att när FISC fattar hemliga beslut om övervakning innebärande att även företag som ska verkställa besluten måste hemlighålla sin delaktighet, saknas juridiska eller administrativa vägar för individer vars personuppgifter inhämtas att få kännedom om inhämtningen. Det saknas därmed också möjlighet för individer att få tillgång till, korrigera eller radera personuppgifter, likaså saknas en rätt till administrativ eller rättslig prövning.

Hemlighållandet kan få betydande konsekvenser. High Court noterade som ett exempel att FISC fattat beslut om att godkänna ett visst övervakningsprogram vid 41 tillfällen. Endast efter att övervakningsprogrammet olagligen avslöjades av en visselblåsare, fick enskilda individer kännedom om det och kunde därmed utmana dess rättsliga giltighet. Övervakningsprogrammet berörde miljontals människor, främst amerikanare, och förklarades slutligen olagligt. High Court bedömde att om motsvarande fall drabbat EU-medborgare hade dessa haft svårare att framföra ett rättsligt anspråk eftersom EU-medborgare utan anknytning till USA inte får åberopa samma regler till stöd för sin talan.

High Court berörde också Executive Order 12333, EO 12333, utfärdad av presidentämbetet i USA. Det är inte en lag utan en exekutiv order som presidenten när som helst kan återkalla eller ändra. Enligt High Court är det huvudsakligen från EO 12333 som den amerikanska signalspaningsmyndigheten NSA hämtar sitt mandat för underrättelse-inhämtning från utlandet. High Court uppger vidare att NSA inte behöver inhämta förhandstillstånd för övervakning enligt EO 12333, att NSA:s agerande enligt EO 12333 inte regleras genom lagstiftning, inte är föremål för rättslig tillsyn och inte kan bli föremål för domstolsprövning. Enligt EO 12333 måste underrättelseinhämtningen vara "for foreign intelligence" enligt definitionen i EO 12333. High Court uppger:

> *"This is an extremely broad definition, wider than the definition in FISA:*
>
> > *'**Information relating** to the capabilities, **intentions and activities of foreign** powers, organisations or **persons**, but not including counterintelligence except for information on international terrorist activity.' (emphasis added)"*

High Court noterar att det finns vissa begränsningar i EO 12333 gällande inhämtning om personer med viss anknytning till USA, men att motsvarande begränsningar saknas för exempelvis EU-medborgare. Det finns dock ett presidentdirektiv, PPD-28, som innebär vissa begränsningar i hur inhämtning enligt EO 12333 får genomföras. High Court redogör för att amerikanska myndigheter uppger att det inte sker massövervakning, dock att det förekommer inhämtning av uppgifter genom signalspaning i större omfattning (”in bulk”), samt att det händer att uppgifter inhämtas om personer som inte är av intresse ur underrättelsesynpunkt.

High Court noterade också de svårigheter som finns för individer, i synnerhet individer utan anknytning till USA, att få talerätt i amerikansk domstol avseende överträdelser relaterade till personuppgiftsbehandling. Detta torde gälla de flesta EU-medborgare. En individ måste med framgång göra gällande att den har talerätt för att över huvud taget kunna inleda en rättsprocess och det noterades att detta är en mycket komplex fråga när det gäller hemlig myndighetsövervakning. High Court angav att på grundval av alla bevis som granskats är just frågan om talerätt ett extraordinärt svårt hinder för en individ att övervinna i fall som gäller amerikanska myndigheters hemliga övervakning.

High Court granskade även andra aspekter av amerikansk rättsordning och kom fram till slutsatsen att det finns invändningar gällande vilka rättigheter som egentligen tillförsäkras enskilda med hänsyn till artikel 47 i EU-stadgan om de grundläggande rättigheterna. Målet i High Court gällde överföring av personuppgifter till USA med stöd av standardavtalsklausulerna, där principerna i Privacy Shield inte tillämpas, och därför aktualiserades frågan om vad ombudsmannamekanismen respektive amerikansk rätt ger för skydd till EU-medborgare. High Court ansåg det finnas välgrundade skäl att tro att de beslut EU-kommissionens fattat om att anta standardavtalsklausuler, är ogiltiga. Därmed beslutades att hänskjuta frågan om standardavtalsklausulernas giltighet till EU-domstolen, vars prövning ännu inte slutförts.

Även i granskningsrapporten som EDPB publicerade gällande Privacy Shield, noteras att FISA sektion 702 och EO 12333 fortfarande är viktiga frågor för EDPB, särskilt när det gäller frågor om massiv och urskillningslös tillgång till EU-medborgares personuppgifter.

En fråga som uppstår är hur ett tredjelands begäran praktiskt ska bemötas, särskilt när tredjelandet anser att dess rättsordning är tillämpligt på den part begäran riktas till. Artikel 48 i dataskyddsförordningen reglerar just denna typ av fall, där utländsk rättsordning måste hanteras i förhållande till dataskyddsförordningen. Artikel 48 lyder i sin helhet:

> ***Överföringar och utlämnanden som inte är tillåtna enligt unionsrätten***
> *Domstolsbeslut eller beslut från myndigheter i tredjeland där det krävs att en personuppgiftsansvarig eller ett personuppgiftsbiträde överför eller lämnar ut personuppgifter får erkännas eller genomföras på något som helst sätt endast om det grundar sig på en internationell överenskommelse, såsom ett avtal om ömsesidig rättslig hjälp, som gäller mellan det begärande tredjelandet och unionen eller en medlemsstat, utan att detta påverkar andra grunder för överföring enligt detta kapitel.*

Här kan beaktas ett mål i amerikanska högsta domstolen gällande om amerikanska myndigheter kunde kräva av ett amerikanskt bolag att få tillgång till personuppgifter i ett e-postkonto som det amerikanska bolaget lagrade i EU. I målet bistod EU-kommissionen den amerikanska högsta domstolen med en skrivelse om hur dataskyddsförordningens krav vid denna typ av begäran ska tolkas. EU-kommissionen skrev att EU:s uppfattning, utifrån internationell rätt, är att när tredjelands myndighet begär information av ett företag med hemvist i samma jurisdiktion som tredjelandets myndighet, men där informationen finns i annan jurisdiktion, ska vissa principer i internationell rätt tillämpas. EU-kommissionen skrev vidare att artikel 48 i dataskyddsförordningen är tydlig med att myndighets- eller domstolsbeslut från ett land som inte är bundet av dataskyddsförordningen, och som gäller överföring av personuppgifter till det landet, endast kan erkännas och verkställas om det sker i enlighet med reglerna för internationell rättshjälp, såvida inte någon annan grund för överföring är möjlig enligt kapitel 5 i dataskyddsförordningen. Eftersom EU-kommissionen inte bedömde det troligt att metoderna i artikel 45 – 47 var framkomliga, återstod endast två undantagsbestämmelser i artikel 49. I den ena bestämmelsen är en förutsättning som EU-kommissionen berörde, huruvida överföringen är ”nödvändig för ändamål som rör den personuppgiftsansvariges tvingande berättigade intressen och den registrerades intressen eller rättigheter och friheter inte väger tyngre”. Då ska den personuppgiftsansvarige dessutom bl.a. informera tillsynsmyndigheten och den registrerade om överföringen. Den andra undantagsbestämmelsen som EU-kommissionen berörde gäller om ”överföringen är nödvändig av viktiga skäl som rör allmänintresset”. Ett sådant allmänintresse måste finnas erkänt i EU-rätten eller en medlemsstats nationella rätt.

Utifrån vad som tidigare redogjorts, kan här påminnas om de rättigheter som ska säkerställas EU-medborgare enligt artikel 47 i EU-stadgan om de grundläggande rättigheterna, samt att det alltjämt finns ett krav enligt artikel 44 i dataskydds-förordningen att den nivå på skyddet av fysiska personer som säkerställs genom data-skyddsförordningen inte undergrävs. Detta måste beaktas i förhållande till tredjelands lagstiftning som utgör hinder för tillgång till effektiva rättsmedel samt som i alltför vaga ordalag möjliggör myndigheters åtkomst till personuppgifter. Eftersom bestämmelserna i artikel 49 i dataskyddsförordningen utgör undantagsregler ska de dessutom tolkas restriktivt, vilket bör föranleda viss försiktighet i tolkningen samt säkerställande att undantagen verkligen är tillämpbara. Det synes därmed inte finnas något utrymme för tillämpning av artikel 49 i tveksamma fall.

Mot bakgrund av de rättsliga synpunkter som gjorts gällande bör betonas att överföring till tredjeland ändå inte är omöjlig, tvärt om framgår en tydlig väg i artikel 48 i form av internationella överenskommelser. Den möjlighet som synes återstå är således att den utländska begäran om personuppgifter framställs enligt reglerna för internationell rätts-hjälp. För svensk del innebär det att tredjelands myndighet eller domstol framställer sin begäran till svenska rättsvårdande myndigheter, som i sin tur gör en självständig prövning av begäran och fattar beslut om huruvida begäran ska verkställas. Det är också denna väg som EU-kommissionen särskilt lyfte fram i sin skrivelse till den amerikanska högsta domstolen.

Medan målet i den amerikanska högsta domstolen pågick stod det klart att en ny amerikansk lagstiftning, CLOUD Act, skulle underlätta för amerikanska myndigheter att få ut uppgifter som amerikanska bolag förfogar över utanför USA. CLOUD Act (Clarifying Lawful Overseas Use of Data) trädde i kraft i mars 2018. Lagen innebär att amerikanska företag som tillhandahåller it-tjänster kan tvingas lämna ut sina kunders information till amerikanska myndigheter oavsett var informationen fysiskt är lagrad. Det som avgör om CLOUD Act gäller är alltså att leverantörens nationella hemvist är USA och inte var informationen geografiskt sett är lagrad eller på annat sätt behandlas. I och med att CLOUD Act trädde i kraft avskrev den amerikanska högsta domstolen målet.

Inledningen till CLOUD Act lyder ”Timely access to electronic data held by communications-service providers is an essential component of government efforts to protect public safety and combat serious crime, including terrorism.” Lagen tar alltså sikte på bekämpning av allvarliga brott, terrorism samt att skydda den amerikanska allmänheten. Exakt hur långt formuleringen ”protect public safety” sträcker sig får i dagsläget anses oklart, och kan förmodas variera över tid. CLOUD Act tar upp ett antal områden som en amerikansk domstol ska ta ställning till, däribland amerikanska nationella säkerhetsintressen. Ur ett EU-perspektiv kan noteras att EU-lagstiftning som dataskyddsförordningen främst tar sikte på att skydda EU-medborgare. Amerikanska domstolar kan således enligt CLOUD Act ha andra prioriteringar att ta hänsyn till. En begäran om uppgifter enligt CLOUD Act kan riktas till det bolag som har åtkomst till uppgifterna istället för att gå genom systemet för internationell rättshjälp. Med begäran kan dessutom följa ett yppandeförbud som innebär att bolaget inte får informera sin kund om begäran.

När EU-domstolen fann att föregångaren till Privacy Shield, Safe Harbour, var ogiltigt, var det av flera skäl, bl.a. att amerikanska myndigheter hade rätt att kringgå skyddet för personuppgifter samt att det inte fanns någon möjlighet för en individ att blir ”glömd” eller ändra felaktiga uppgifter. I sin dom rörande Safe Harbour resonerade EU-domstolen inte i första hand utifrån vad som kunde bevisas ha skett i enskilda fall i termer av åtkomst till personuppgifter, utan utifrån vad amerikansk lag faktiskt möjliggör. Safe Harbour kunde inte säkerställa någon adekvat skyddsnivå och upphävdes därför. Som tidigare noterats består den nya överenskommelsen Privacy Shield av flera delar som enligt EU-kommissionen säkerställer en adekvat skyddsnivå för enskilda EU-medborgare när deras personuppgifter överförs. Som redovisats har det gjorts gällande flera allvarliga brister avseende det skydd som Privacy Shield påstås kunna erbjuda. Även Privacy Shield är nu föremål för giltighetsprövning i EU-domstolen.

Mot bakgrund av de krav som dataskyddsförordningen ställer upp, får det anses att FISA sektion 702, EO 12333 och CLOUD Act var för sig är högst problematiska ur dataskydds-förordningens perspektiv. Lagstiftning och regler med motsvarande problematiska innebörd finns i flera andra länder, t.ex. Indien, Kina och Ryssland. En svensk myndighet som låter företag som lyder under ett sådant regelverk behandla personuppgifter, synes därmed ge det utländska regelverket företräde framför EU:s dataskyddsförordning, villkoren i personuppgiftsbiträdesavtalet mellan myndigheten och leverantören samt reglerna för internationell rättshjälp.

4.8 Brottsbekämpande verksamhet

Dataskyddsförordningen är en generell lagstiftning för personuppgiftsbehandling, men finns det speciallagstiftning inom ett visst område har den företräde framför dataskyddsförordningen. Brottsdatalagen, BDL, är en sådan särskild lag som gäller i myndigheters brottsbekämpande verksamhet. Med det menas allt arbete som sker för att förebygga, förhindra, utreda, avslöja eller lagföra brott. Många brottsbekämpande myndigheter har även andra uppgifter, till exempel gränskontroll eller tullkontroll, som inte direkt innebär brottsbekämpning. För personuppgiftsbehandling i sådan verksamhet gäller inte BDL. Då gäller i stället dataskyddsförordningen.

BDL gäller för personuppgiftsbehandling i brottsbekämpande verksamhet hos myndigheter som Polismyndigheten, Ekobrottsmyndigheten, Tullverket, Skatteverket, Kustbevakningen och Åklagarmyndigheten. BDL gäller även i verksamhet för att verkställa straffrättsliga påföljder. Sådan verksamhet bedrivs till exempel av:

- Kriminalvården, om någon döms till fängelse
- Kronofogdemyndigheten, om någon döms till böter
- Kommunernas socialnämnder, om ungdomar döms till vård inom socialtjänsten
- Sjukhus, om någon döms till rättspsykiatrisk tvångsvård

Användning av Webbaserat kontorsstöd i dessa verksamheter, som finns i såväl staten som regioner och kommuner, måste alltså ske i enlighet med BDL.

Både dataskyddsförordningen och BDL utgår från samma principer, till exempel att personuppgifter bara får behandlas för särskilda, uttryckligt angivna och berättigade ändamål. Tredjelandsöverföring regleras i BDL på ett likartat sätt som i dataskyddsförordningen. I 8 kap. 1 § BDL anges förutsättningarna för när ”En behörig myndighet får överföra personuppgifter till ett tredjeland” och ett av rekvisiten är att överföringen ska riktas till ”en behörig myndighet i ett tredjeland”. Den som överför uppgifterna ska enligt BDL särskilt beakta risken att enskilda får ett försämrat skydd för sina personuppgifter. Utländsk myndighet lyder inte under BDL. Redan ordalydelsen i BDL tyder på att ingen annan än en svensk behörig myndighet får överföra uppgifterna till ett tredjeland. Det gäller då oavsett om det i övrigt hade varit möjligt att använda ett beslut om adekvat skyddsnivå, tillräckliga skyddsåtgärder eller någon undantagssituation.

Det får konstateras att FISA sektion 702, EO 12333, CLOUD Act och liknande regelverk synes hindra tredjelandsöverföring även enligt BDL.

4.9 Aggregering av personuppgifter

I dataskyddsförordningens beaktandesats 75 noteras särskilt att risker kan uppkomma vid personuppgiftsbehandling som inbegriper ett stort antal personuppgifter och gäller ett stort antal personer. Detta tydliggörs vidare i beaktandesats 91 som beskriver att en konsekvensbedömning behövs vid storskalig uppgiftsbehandling, som gäller ett stort antal registrerade och sannolikt innebär en hög risk när teknik används storskaligt. Slutligen framgår av beaktandesats 92 fördelarna med att en konsekvensbedömning avseende

dataskydd inriktar sig på ett vidare område än en enskild myndighets införande. Så är fallet när myndigheter avser att skapa en gemensam plattform eller när flera personuppgiftsansvariga planerar att införa en gemensam miljö.

Kommuner, regioner och de största statliga myndigheterna har tusentals anställda var för sig och kan därför behöva bedöma de ovan angivna beaktandesatserna i förhållande till artikel 19 i dataskyddsförordningen gällande konsekvensbedömningar och risk- och sårbarhetsanalyser innan det kan avgöras om en viss molntjänst kan tas i bruk.

4.10 Personuppgifter i e-post

Angående riskerna med e-post uppger Datainspektionen på sin webbplats bland annat:

> *När man hanterar e-post finns det alltid en risk för att andra än den avsedda mottagaren kan ta del av meddelandet. I många fall är det omöjligt att säkerställa identiteten hos en mottagare enbart utifrån en uppgiven e-postadress. Det finns dessutom säkerhetsbrister i de kommunikationsprotokoll som ligger till grund för e-postsystem. När ett e-postmeddelande skickas mellan e-postservrar över Internet passerar det ofta andra servrar på vägen. Om informationen i e-postmeddelandet är oskyddad finns det inget som hindrar att kopior av informationen sparas undan vid var och en av dessa servrar. Det blir därmed svårt att se till att inte obehöriga tar del av den kopierade informationen. Detta gäller särskilt då e-posten är åtkomlig via öppet nät eller är synkroniserad med mobila enheter som till exempel bärbara datorer, pekplattor och mobiltelefoner.*
>
> *Dagens e-postprogram innehåller också en del funktioner som ökar riskerna för att e-postmeddelanden skickas fel. Det kan vara namn och e-postadresser som fylls i automatiskt eller upprättade e-postlistor som gör att e-posten oavsiktligt riskerar att skickas till fel mottagare eller till betydligt fler mottagare än avsändaren avsett.*
>
> ***Det finns risker även med ”intern” e-post***
> *Den senaste tidens teknikutveckling har gjort att det blivit allt svårare att tala om intern hantering av e-post. Uppfattningen om att e-post som skickas inom en organisation inte går över öppna nät är i de flesta fall felaktig. Om det exempelvis finns funktioner för webbmejl innebär de så gott som alltid att e-post görs tillgängligt via ett öppet nät. Det gäller också när e-post, utan att gå över ett virtuellt privat nätverk, kan hämtas till e-postklienter utifrån via till exempel POP eller IMAP. Detsamma gäller om vissa tjänster, till exempel antivirusfunktioner eller spamtvätt, tillhandahålls av en extern leverantör. Om hela eller delar av drift, administration eller underhåll av e-postsystemet läggs ut på en extern part, ett personuppgiftsbiträde, tillkommer frågor kring hur denne går till väga för att logga in till e-postsystemet. Funktioner för distans-administration används ofta över öppet nät.*

Den ökade användningen av och synkroniseringen med mobila enheter gör också att det blir svårare att tala om intern hantering av e-post eftersom sådana ofta används utanför den egna organisationens lokaler och nätverk.

Behandling av känsliga personuppgifter och integritetskänsliga personuppgifter kräver ett starkare skydd enligt dataskyddsförordningen. Detta då behandling av sådana uppgifter kan innebära betydande risker för de grundläggande rättigheterna och friheterna som varje medborgare har.

Generellt gäller att denna typ av uppgifter ska skyddas på ett sådant sätt att obehöriga inte kan ta del av uppgifterna, vilket i praktiken kan innebära att känsliga och/eller särskilt integritetskänsliga uppgifter måste krypteringsskyddas på ett sådant sätt att endast den avsedda mottagaren kan ta del av dem. Vissa e-postsystem har funktioner för att kryptera meddelanden mellan användare inom samma e-postdomän, men vanligtvis behövs särskilda krypteringsnycklar eller programvaror för att kryptera e-post.

Inledningsvis noteras att en myndighet inte råder över vilka uppgifter som skickas till myndighetens e-postlösning. Webbaserat kontorsstöd bör således kunna hantera inkommande e-post med känsliga personuppgifter utan att Webbaserat kontorsstöd orsakar olämpliga personuppgiftsbehandlingar. Kraven på säkerhet för känsliga personuppgifter är relevanta även i andra sammanhang än e-post, exempelvis i handlingar och chattmeddelanden. Webbaserat kontorsstöd kan exponeras för risker vid överföring av känsliga eller integritetskänsliga personuppgifter över öppna nät, synkronisering till mobila klienter, distansadministration, antivirusfunktioner och spamfilter. Mot bakgrund av avsnitt 4.9 ska dessutom stora ansamlingar av personuppgifter i sig beaktas vid utformandet av skyddet för personuppgifterna. Det vore därför mycket fördelaktigt om Webbaserat kontorsstöd kan utformas med en hög skyddsnivå som möjliggör och underlättar användning även med stora ansamlingar känsliga och integritetskänsliga personuppgifter.

4.11 Sammanfattning

Eftersom personuppgiftsbehandling är en ofrånkomlig del av Webbaserat kontorsstöd och personuppgiftsbehandling många gånger är komplicerad att avtala om på ett korrekt sätt krävs att dessa delar är väl täckta av ett eventuellt ramavtal samt att det blir så enkelt som möjligt för myndigheterna. De risker som lyfts fram och som är förknippade med tredjelands rättsordning måste beaktas. Det är väsentligt att säkerställa att myndigheters användning av Webbaserat kontorsstöd är rättsligt hållbar över tid.

Statens inköpscentral kan inte vara personuppgiftsansvarig eller personuppgiftsbiträde för den personuppgiftsbehandling som en annan myndighet ansvarar för. Därför måste myndigheter alltid göra sina egna risk- och sårbarhetsanalyser och ange syftet med personuppgiftsbehandlingen i det personuppgiftsbiträdesavtal som ingås. Ramavtalet kan dock inkludera mallar och instruktioner för att på så sätt ensa och förenkla processen.

5 Offentlighet och sekretess

5.1 Allmänna handlingar och sekretess

Webbaserat kontorsstöd omfattar en hel kontorsarbetsplats med funktioner för fillagring och dokumenthantering som stödjer ett modernt arbetssätt där tjänstemän enkelt och säkert skapar och delar information. Mängder av information kommer då att placeras i Webbaserat kontorsstöd, där sekretess kan gälla för såväl allmänna handlingar som andra uppgifter vilka skapas och hanteras i myndigheternas dagliga arbete. Det kan handla om alltifrån arbetsutkast till uppgifter i chattkonversationer mellan tjänstemän. Både allmänna handlingar och andra slags uppgifter kan således vara sekretessbelagda och därmed omfattas av röjandeförbud. Förbud till följd av sekretess och tystnadsplikt gäller oavsett om röjandet sker muntligen, genom utlämnande av allmän handling eller på något annat sätt.

Tryckfrihetsförordningen, TF, beskriver rätten att ta del av allmänna handlingar ”till främjande av ett fritt meningsutbyte, en fri och allsidig upplysning och ett fritt konstnärligt skapande”. Myndigheter ska enligt offentlighets- och sekretesslagen, OSL, särskilt se till att rätten att ta del av allmänna handlingar enligt TF säkerställs samtidigt som sekretesskyddet upprätthålls. OSL anger vilka skäl som föranleder sekretess för en uppgift. Sekretess gäller exempelvis om det är påkallat med hänsyn till det allmännas ekonomiska intresse samt skyddet för enskildas personliga eller ekonomiska förhållanden. Sekretess enligt OSL omfattar därmed ett långt bredare omfång av uppgifter än det som berör Sveriges säkerhet. En myndighet som använder ett så generellt verktyg som Webbaserat kontorsstöd kommer oavsett verksamhet att hantera sekretessreglerade uppgifter i Webbaserat kontorsstöd.

En sekretessreglerad uppgift definieras i OSL som en uppgift för vilken det finns en bestämmelse om sekretess. En sekretessbestämmelse består i regel av tre delar som anger sekretessens föremål, dess räckvidd och dess styrka. Sekretessbestämmelsens *föremål* beskriver den typ av information som kan hemlighållas, exempelvis kan en sekretessbestämmelse gälla ”uppgift om enskilds personliga förhållanden”. En sekretessbestämmelses *räckvidd* kan avgränsas så att sekretessen bara gäller i en viss typ av ärenden, i en viss typ av verksamhet eller hos en viss myndighet. Några få sekretessbestämmelser gäller utan att räckvidden är begränsad. Uppgiften ska då inte lämnas ut oavsett i vilket ärende, i vilken verksamhet eller hos vilken myndighet uppgiften förekommer.

Sekretessbestämmelsens *styrka* bestäms i regel med hjälp av en skadeprövning. Här skiljs mellan ett rakt eller omvänt skaderekvisit som avgör utgångspunkten i bedömningen om en uppgift är offentlig eller kan lämnas ut. Gäller ett rakt skaderekvisit för en uppgift är utgångspunkten att uppgiften är offentlig. Endast om det finns anledning att anta att en viss skada uppstår om uppgiften lämnas ut, gäller sekretess. Vid omvänt skaderekvisit gäller motsatsen, dvs. som utgångspunkt kan uppgiften inte lämnas ut. Uppgiften får då

endast göras offentlig om det står klart att uppgiften kan röjas utan att viss skada uppstår. Står detta inte klart, exempelvis i avsaknad av ett tillräckligt robust beslutsunderlag, får uppgiften inte lämnas ut. Sekretessen kan även vara absolut och gäller då utan att någon skadeprövning görs. Ett exempel på detta är s.k. upphandlingssekretess som gäller för anbud i sin helhet innan tilldelningsbeslut fattats i en offentlig upphandling.

En uppgift kan omfattas av sekretess när vissa omständigheter föreligger, för att sedan kunna lämnas ut när omständigheterna förändrats. Sekretess för uppgifter enligt OSL kan i vissa fall gälla – eller inte gälla – beroende på hur uppgifterna kommer att användas. Prövning om utlämnande av uppgifter behöver därför ske från fall till fall. Enligt OSL ska frågan om utlämnande prövas av den myndighet som förvarar handlingen, om inget annat är föreskrivet. Några uppgifter är till sin natur av så enkelt slag att uppgifterna i praktiken offentliggörs tillsvidare – typexemplet är information på en myndighets publika webbplats. De allra flesta uppgifter i en myndighets dagliga arbete kan dock inte offentliggöras på detta sätt eftersom omständigheterna som föranleder sekretess är föränderliga.

Den grundlagsskyddade rätten att ta del av allmänna handlingar gäller även i en krissituation. Vissa leverantörer bär ett särskilt lagstadgat ansvar för att säkerställa upprätthållandet av digitala tjänster, vilket utvecklas i kapitel 6. Ytterst är det dock myndigheterna som alltjämt måste säkerställa tillgängligheten till sina uppgifter och de it-funktioner som krävs för att komma åt dem. Det gäller dels för att en myndighet ska fungera i sig självt och kunna samverka med andra myndigheter, dels så att uppgifter fortsatt kan lämnas ut enligt TF. Rätten att ta del av allmänna handlingar förutsätter myndigheternas tillgänglighet till dessa handlingar.

När OSL begränsar grundlagsskyddet i TF är det av tungt vägande skäl som måste hanteras på ett varsamt och ansvarsfullt sätt. Sekretessen värnar intressen i vitt skilda sammanhang: värdefulla företagshemligheter, fakta med bäring på Sveriges civila och militära försvar, integritetskänslig dokumentation om enskilda i sjukvården, skolan och socialtjänsten är alla exempel på uppgifter som ska skyddas. Det framstår som angeläget att myndigheter agerar trovärdigt och aktsamt med denna information som anförtrotts det offentliga. Uppstår tvivel kring förmågan att trygga sekretessen på ett generellt plan, riskerar det att rubba breda gruppers förtroende och agerande gentemot myndigheter i stort.

5.2 JO-ärenden

Justitieombudsmannen, JO, granskade i JO-ärendet 3032-2011 två offentliga vårdgivare som ingått avtal med ett företag om journalföring av patientuppgifter. Enligt avtalen skulle läkarsekreterare anställda hos företaget på distans lyssna av inlästa diktat och skriva in uppgifterna i patientjournaler. Hanteringen var elektronisk och uppgifter skulle aldrig lagras utanför vårdgivarnas it-system. Varken det faktum att läkarsekreterarna haft en avtalsreglerad tystnadsplikt i förhållande till sin arbetsgivare (företaget), eller att annan tvingande lagstiftning rörande personuppgifter kunde hindra röjande, ansågs tillräckligt för att godta upplägget. JO lade vid bedömningen vikt vid att vårdgivarnas egen personal kan dömas för brott mot tystnadsplikt om en sekretessbelagd uppgift röjs, till skillnad från

företagets läkarsekreterare. Det fanns inte heller någon alternativ grund för utlämnande. Avtalen mellan vårdgivarna och företaget innebar därmed att företagets anställda skulle ta del av sekretessbelagda uppgifter i strid med OSL. JO gav vårdgivarna allvarlig kritik och ansåg det anmärkningsvärt att vårdgivarna inte ägnat sekretessaspekterna större uppmärksamhet i samband med att avtalen ingicks.

I JO-ärendet 6466-2015 hade en kommuns barn- och utbildningsförvaltning e-postat en elevs läkarintyg mellan e-postservrar över internet till vårdnadshavarna och till flera befattningshavare. Med hänvisning till Datainspektionens råd konstaterade JO att det borde ha vidtagits särskilda säkerhetsåtgärder för att säkerställa att rätt person fick åtkomst till uppgifterna och att de överfördes på ett säkert sätt, t.ex. genom kryptering. Eftersom det inte gjordes fanns det risk att obehöriga, dvs. andra än de avsedda mottagarna, kunde ta del av de känsliga personuppgifterna. JO kritiserade förvaltningen för hanteringen.

De risker med e-post som Datainspektionen beskriver har tidigare nämnts i avsnitt 4.10. Datainspektionens vägledande material är skrivet utifrån tillämpningen av regelverket kring behandling av personuppgifter. Stort fokus ligger dock på riskerna för uppgifters konfidentialitet vilket är högst relevant vid hantering av sekretessreglerade uppgifter. Även Webbaserat kontorsstöd kan exponeras för risker vid överföring av uppgifter över öppna nät, synkronisering till mobila klienter, distansadministration, antivirusfunktioner och spamfilter.

5.3 Yttranden från eSamverkansprogrammet

Den juridiska expertgruppen inom eSamverkansprogrammet, som består av 23 statliga myndigheter samt Sveriges Kommuner och Landsting, gjorde den 17 december 2015 ett rättsligt uttalande om när sekretessreglerade uppgifter anses röjda till tjänsteleverantörer.

> *Om uppgifter görs tekniskt tillgängliga för en tjänsteleverantör som enligt avtalet inte får ta del av eller vidarebefordra uppgifterna och omständigheterna i övrigt medför att det är osannolikt att detta ändå sker, ska uppgifterna enligt expertgruppens bedömning inte anses som röjda i offentlighets- och sekretesslagens mening.*

För att inte bryta mot OSL krävs enligt uttalandet dels att avtalet förhindrar tjänsteleverantören från att ta del av och vidarebefordra uppgifterna, dels att det i praktiken och alldeles oavsett avtalet, är osannolikt att så ändå sker. Redan mot bakgrund av eSamverkansprogrammets första uttalande om röjandebegreppet bör noteras att molntjänstleverantörers avtal inte kan hindra molntjänstleverantören från att vidarebefordra uppgifter till rättsvårdande myndigheter. Tvärtom är molntjänstleverantörer givetvis skyldiga att följa tillämpliga lagar och myndighetsbeslut.

Den 12 november 2018 gjorde eSamverkansprogrammets juridiska expertgrupp ytterligare ett rättsligt uttalande, nu om sekretessreglerade uppgifter och utländskt ägda molntjänster, där slutsatsen i det tidigare uttalandet utvecklas vidare.

> *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. Anledningen är att det inte längre är osannolikt att uppgifterna kan komma att lämnas till utomstående. Detsamma får anses gälla om redan ägarförhållanden eller geografisk placering av en tjänsteleverantörs tekniska hjälpmedel ger anledning att befara att mänskliga rättigheter (till exempel skyddet för privatlivet) eller det allmännas intressen (t.ex. rikets säkerhet) inte skulle säkerställas om svenska myndigheters data hade tillgängliggjorts.*

Projektgruppen konstaterar att uttalandet tar sikte på situationen där en molntjänst som omfattas av utländsk rättsordning kommer i konflikt med reglerna för internationell rättshjälp samt svensk rätt i övrigt.

5.4 Analys av Pensionsmyndigheten

I Pensionsmyndighetens rapport ”Molntjänster i staten – En ny generation av outsourcing” konstateras att en myndighet kan lämna ut sin information till en molntjänstleverantör, under förutsättning att informationen inte är sekretessreglerad och att det inte är olämpligt av andra skäl att lämna ut informationen till leverantören i fråga.

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

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

5.5 Sekretess i relation till utländska regelverk

Som tidigare noterats innebär CLOUD Act att amerikanska myndigheter i hemlighet kan begära uppgifter av ett amerikanskt bolag som lagrar uppgifter utanför USA, istället för att gå genom systemet för internationell rättshjälp. Vidare synes FISA sektion 702 och EO 12333 möjliggöra för amerikanska underrättelsemyndigheter att inhämta information om icke-amerikanska medborgare, utan rättsliga garantier för de som drabbas att få information om inhämtningen eller möjlighet att opponera sig i domstol utifrån vad EU-reglerna kräver. För en mer utförlig redogörelse av dessa regelverk, se avsnitt 4.7. Regler med motsvarande innebörd som de amerikanska finns även i andra länder.

Samtidigt som ett utländskt företag kan omfattas av vissa utländska regelverk, kan den information som begärs ut eller samlas in vara sekretessbelagd enligt de svenska sekretess-reglerna i OSL. Som tidigare nämnts är mängder av uppgifter sekretessreglerade enligt OSL, inte bara sådana uppgifter som berör Sveriges säkerhet.

8 kap. 3 § OSL reglerar specifikt utlämnande av sekretessbelagda uppgifter till utländska myndigheter:

> ***Sekretess mot utländska myndigheter eller mellanfolkliga organisationer***
> *En uppgift för vilken sekretess gäller enligt denna lag får inte röjas för en utländsk myndighet eller en mellanfolklig organisation, om inte*
> *1. utlämnande sker i enlighet med särskild föreskrift i lag eller förordning, eller*
> *2. 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 till den utländska myndigheten eller den mellanfolkliga organisationen.*

Det finns ingen särskild föreskrift i lag eller förordning som medger ett utlämnande enligt FISA sektion 702, EO 12333 eller CLOUD Act varför punkt 1 ovan inte synes kunna tillämpas. Ett utlämnande till utländsk myndighet enligt punkt 2 ovan kräver att två förutsättningar uppfylls.

För det första måste den svenska myndighet som ansvarar för den sekretessbelagda uppgiften i motsvarande fall få lämna ut uppgiften till en annan svensk myndighet, exempelvis en svensk brottsbekämpande myndighet. Uppgifter som överförs eller inhämtas med stöd av FISA sektion 702, EO 12333 eller CLOUD Act tillgodoser amerikanska myndigheters behov och intressen. Det synes inte finnas några garantier för att en amerikansk myndighets bedömning måste överensstämma med en svensk myndighets bedömning.

För det andra måste den svenska myndighet som ansvarar för den sekretessbelagda uppgiften göra en prövning och konstatera att det står klart att det är förenligt med svenska intressen att uppgiften lämnas ut till den amerikanska myndigheten.

Eftersom en amerikansk myndighets begäran eller inhämtning kan vara hemlig, saknas möjlighet för en svensk myndighet att göra de prövningar som krävs. Det synes därför

varken vara möjligt att säkerställa att en uppgift i motsvarande fall skulle få lämnas ut till en svensk myndighet och inte heller stå klart att svenska intressen tillgodoses.

Lagstiftaren har i 8 kap. 3 § OSL uttryckligen reglerat förutsättningarna för utlämnande av uppgifter till utländska myndigheter varför t.ex. FISA sektion 702, EO 12333 och CLOUD Act var för sig framstår som problematiska ur ett OSL-perspektiv. Lagstiftning och regler med motsvarande problematiska innebörd finns i flera andra länder, t.ex. Indien, Kina och Ryssland. En svensk myndighet som låter företag som lyder under ett sådant regelverk hantera sekretessreglerade uppgifter, synes därmed ge det utländska regelverket företräde framför svensk lagstiftning. I förhållande till detta bör särskilt beaktas kraven i TF och OSL om att myndigheter ska se till att sekretesskyddet upprätthålls.

5.6 Sekretess och leverantör av Webbaserat kontorsstöd

I vissa molntjänster kan en leverantörs personal komma i kontakt med en kunds uppgifter som överförts till leverantörens molntjänst. Det kan exempelvis vara när tekniska fel i molntjänsten måste rättas. En särskild fråga gäller möjligheten att en myndighet i avtal tydligt anger att leverantörens personal inte får ta del av innehållet i lagrade uppgifter utan myndighetens förhandstillstånd. Myndigheten kan då göra en sekretessprövning i det enskilda fallet. Digitaliseringsrättsutredningen (SOU 2018:25) konstaterar att det bland myndigheter råder osäkerhet kring vad som är tillåtet gällande sekretessreglerade uppgifter och molntjänster. Utredningen föreslår en komplettering i OSL som under vissa angivna förutsättningar skulle möjliggöra ett utlämnande (röjande) som en sekretessbrytande grund.

I 2 kap. 12 § TF talas om tillhandahållande av allmän handling utan att det närmare preciseras vad som utgör ett ”tillhandahållande”. Där anges att ”Kan handling ej tillhandahållas utan att sådan del därav som icke får lämnas ut röjes, skall den i övriga delar göras tillgänglig för sökanden i avskrift eller kopia.” Detta kan tyda på att det föreligger ett utlämnande eller ett röjande så fort handlingen eller dess innehåll gjorts ”tillgänglig”.

En myndighet som använder Webbaserat kontorsstöd bör ha en möjlighet att verifiera att sekretesskyddet verkligen upprätthålls. Olika avtalsmässiga och tekniska verktyg kan övervägas för att uppnå en sådan effektiv kontroll. Till att börja med bör det underlätta om endast ett begränsat antal juridiska personer och en begränsad mängd personal kan komma i kontakt med sekretessreglerade uppgifter. Upprätthållande av avtalsvillkoren kan knytas till viten. Möjligheten kan övervägas att Webbaserat kontorsstöd till sin funktion byggs så att myndigheter ges en betydande kontroll över en leverantörs behörigheter och faktiska agerande i tjänsten. Ett led i detta skulle kunna vara att samtliga väsentliga delar av de programvarukomponenter som utgör Webbaserat kontorsstöd kan granskas för att säkerställa avtalat funktionssätt. Det kan även övervägas att bygga in verktyg för självständig kontroll, exempelvis genom loggar med oavvislighetsmekanism. Det skulle innebära att en myndighet på ett fristående och tillförlitligt sätt kan kontrollera vad leverantörens personal gjort i tjänsten och därmed verifiera att sekretessen upprätthålls. En annan typ av åtgärd är att myndigheter kan ge förhandsgodkännande innan leverantörens personal får bereda sig tillgång till uppgifter, så att myndigheten kan

säkerställa att uppgifterna i det konkreta fallet inte omfattas av sekretess enligt OSL. Även i det fallet skulle en teknisk lösning kunna verifiera att en sådan överenskommen mekanism följs i praktiken, då myndighetens kontrollmöjlighet är fristående från leverantören. Myndigheterna är då inte beroende av att leverantören själv granskar och rapporterar om sitt eget agerande med övervakningsverktyg som till fullo står under leverantörens kontroll.

Även om myndigheter som använder Webbaserat kontorsstöd har betydande insyn i en leverantörs agerande synes det också angeläget att myndigheterna har möjlighet att snabbt återta sin information. Ett återtagande kan beroende på situation innebära en migrering till en lösning som driftas av myndigheten själv, eller till en annan leverantör som också tillhandahåller Webbaserat kontorsstöd.

5.7 Kryptering eller andra åtgärder med samma verkan

Det andra uttalandet från eSamverkansprogrammet, se avsnitt 5.3, vidrör möjligheten att kryptering eller andra åtgärder med samma verkan kan innebära att sekretessreglerade uppgifter får hanteras av en tjänsteleverantör. Det kan exempelvis ske genom att all e-post är krypterad och alla dokument är krypterade. För att det ska fungera fullt ut krävs det dock att myndigheten:

- Använder ett, i förhållande till skyddsvärdet, lämpligt krypto
- Att endast myndigheten har tillgång till krypteringsnycklarna och inte leverantören
- Att informationen krypteras innan den blir tillgänglig i molntjänsten
- Att myndigheten kan säkerställa krypteringens säkerhet i alla led

Om kryptering ska tillämpas på uppgifter i Webbaserat kontorsstöd skulle det t.ex. krävas att myndigheten endast hanterar krypterad e-post samt aldrig skapar handlingar i ordbehandlaren. Ett dokument som skapas i en webbaserad ordbehandlare, och därmed direkt lagras i Webbaserat kontorsstöd, kan därför inte krypteras utanför ordbehandlarens ramar förrän efter att det laddats ner okrypterat från Webbaserat kontorsstöd.

Att en myndighet skulle kunna säkerställa att all inkommande e-post är krypterad ter sig osannolikt, och om det inte går att upprätta handlingar i ordbehandlaren faller halva syftet med Webbaserat kontorsstöd.

En möjlig lösning skulle kunna vara att endast kryptera det som är sekretessreglerat med den eventuella risken att information som är sekretessreglerad blir mer identifierbar just genom krypteringen.

5.8 Ständig sekretessprövning av enskilda tjänstemän

Sekretessreglerade uppgifter kan såväl skapas, lagras och inkomma till Webbaserat kontorsstöd. Ett förhållningssätt till hur det undviks att sekretessreglerade handlingar skapas eller lagras i Webbaserat kontorsstöd är att förlita sig på att tjänstemän alltid gör

korrekta sekretessprövningar samt att en handling aldrig inleds som öppen men under handläggningens gång blir sekretessreglerad. Tjänstemän har att följa OSL under straffansvar (20 kap. 3 § brottsbalken). I praktiken innebär dock ett sådant förhållningssätt betydande problem för den myndighet som vill undvika sekretessreglerade uppgifter i Webbaserat kontorsstöd. Det gäller särskilt i krissituationer när det kan antas vara vanligare att fel och slarv begås. Inte ens den myndighet som konsekvent undviker sekretessreglerade uppgifter i Webbaserat kontorsstöd utifrån egna tjänstemäns agerande, kan dock hindra inkommande e-post med sekretessreglerade uppgifter.

Användarvänlighet är centralt i en it-lösning där mängder av sekretessreglerade uppgifter hanteras, både för att Webbaserat kontorsstöd och reglerna om sekretess ska vinna legitimitet och acceptans. Webbaserat kontorsstöd som underlättar för tjänstemäns sekretessprövningar är därför klart mer fördelaktigare än alternativen.

5.9 Sammanfattning

Webbaserat kontorsstöd kan kräva betydande investeringar, dels från de leverantörer som står för tillhandahållandet, dels från myndigheterna i form av resurser för migrering och införande. Det är därför angeläget att ett Webbaserat kontorsstöd som erbjuds på ett kommande ramavtal är en lösning som är hållbar över tid. Flera frågor gällande sekretess måste hanteras i Webbaserat kontorsstöd.

Regelverket kring OSL och TF är komplext samtidigt som det krävs att regelverket följs. Det framstår som angeläget att myndigheter agerar trovärdigt och aktsamt med den information som anförtrotts det offentliga. Såväl myndigheters möjlighet att tillhandahålla offentliga allmänna handlingar, som upprätthållandet av sekretessen, måste säkerställas.

Utifrån eSamverkansprogrammets rättsliga uttalande instämmer projektgruppen i att sekretessreglerade och säkerhetskänsliga uppgifter som finns tillgängliga i en utländsk molntjänst, på det sätt som eSamverkansprogrammet uttalat, är att anse som röjda.

Baserat på vad som anförts tidigare föreligger konflikter mellan utländsk rättsordning och svensk sekretesslagstiftning. Det är dessutom en föränderlig värld där nya regler kan påverka de it-lösningar som svenska myndigheter använder varför upprätthållandet av svenska sekretessregler ständigt måste säkerställas.

För att upprätthålla sekretesskyddet i Webbaserat kontorsstöd kan krävas att myndigheter ges särskild insyn i uppbyggnaden av tjänsten, vilken personal som arbetar i tjänsten samt att det finns verktyg som möjliggör övervakning och kontroll som är självständig från leverantören. Kryptering av uppgifter är att betrakta som en teoretisk lösning, i praktiken bedömer dock projektgruppen att den sannolikt innebär alltför stor påverkan för att vara ett alternativ utifrån perspektiven funktion, prestanda och användarvänlighet.

Splittrad lagring av information på olika digitala platser förutsätter ständiga interna sekretessprövningar. En handling eller ett projekt kan i olika skeden omfatta såväl sekretessbelagd som offentlig information. Utöver bristerna ur perspektivet användarvänlighet och arbetsbelastning, kan konstateras att regelverket om sekretess är komplext.

Webbaserat kontorsstöd måste därför så långt som möjligt kunna användas så att enskilda tjänstemän i det dagliga arbetet kan hantera uppgifter, oavsett sekretessnivå, på ett säkert sätt.

6 Samhällsviktiga och digitala tjänster

6.1 Lag om informationssäkerhet för samhällsviktiga och digitala tjänster

Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster med tillhörande förordning (2018:1175) samt MSB:s föreskrifter MSBFS 2018:7, 2018:8, 2018:9, 2018:10 och 2018:11 utgör hittills det svenska genomförandet av EU:s direktiv om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem, ”NIS-direktivet” (EU 2016/1148). Ytterligare föreskrifter är att vänta från de myndigheter som regleringen utpekar har föreskriftsansvar. Föreskrifterna ska hantera hur leverantörerna av samhällsviktiga tjänster i respektive sektor ska arbeta med riskanalyser och säkerhetsåtgärder.

Syftet med NIS-direktivet är att uppnå en hög gemensam nivå på säkerhet i nätverk och informationssystem inom EU för att upprätthålla samhällelig eller ekonomisk verksamhet. Direktivet anger att säkerhetsincidenter är ett allvarligt hot mot systemens funktion, kan undergräva användarnas förtroende och medföra allvarliga ekonomiska konsekvenser.

Lagen tar sikte på flera tjänster som myndigheter använder, erbjuder medborgare, äger och/eller ansvarar för inom sektorerna energi, transport, hälso- och sjukvård, leverans och distribution av dricksvatten och digital infrastruktur samt digitala tjänster. En digital tjänst är, om vissa kriterier uppnås, internetbaserade marknadsplatser, internetbaserade sökmotorer och molntjänster.

Lagen om informationssäkerhet gäller för leverantörer av samhällsviktiga tjänster som tillhandahåller en tjänst som bedöms viktig för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet, tillhandahållandet av tjänsten är beroende av nätverk och informationssystem och en incident skulle medföra en betydande störning vid tillhandahållandet av tjänsten. För att vara leverantör av digitala tjänster behöver leverantören ha sitt huvudkontor i Sverige, ha en årsomsättning som överstiger 10 miljoner euro och ha 50 eller fler anställda.

6.2 Skyldigheter för leverantörer

Leverantörer av samhällsviktiga tjänster ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete avseende nätverk och informationssystem som de använder för att tillhandahålla samhällsviktiga tjänster. Leverantörer ska också göra en riskanalys med en åtgärdsplan. Riskanalysen ska dokumenteras och uppdateras årligen. Vidare ska leverantörer vidta ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverk och informationssystem som de använder för att tillhandahålla samhällsviktiga tjänster.

Även leverantörer av digitala tjänster ska bedriva ett systematiskt informationssäkerhetsarbete, hantera risker relaterade till tjänsterna och rapportera incidenter. Leverantörer av digitala tjänster ska arbeta med att hantera risker och införa säkerhetsåtgärder enligt EU-kommissionens genomförandeförordning (EU) 2018/151 och rapportera incidenter enligt MSBFS 2016:11.

Webbaserat kontorsstöd kan vara en digital tjänst om den uppfyller de krav för t.ex. molntjänster som ställs i lagen om informationssäkerhet.

6.3 Sammanfattning

Lagen om informationssäkerhet för samhällsviktiga och digitala tjänster ställer krav som kanske måste hanteras i en kommande ramavtalsupphandling av Webbaserat kontorsstöd om den levereras som molntjänst samt uppnår kriterierna för att vara en digital tjänst. Det ställs krav på myndigheter som bedriver samhällsviktiga tjänster samt statliga myndigheter att bedriva ett systematiskt informationssäkerhetsarbete. Det innebär bl.a. att innan information hanteras av extern aktör ska informationen klassas, risker bedömas och säkerhetskrav identifieras. Utkontraktering kan endast ske om leverantören uppfyller ställda krav. Leverantörens förmåga att under avtalets tid upprätthålla ställda säkerhetskrav ska kontrolleras.

7 Säkerhetskänslig verksamhet

7.1 Inledning

En mängd faktorer kan påverka de varor och tjänster som en myndighet använder eller kan komma att använda. En myndighets konsekvensanalys kan inte endast göras baserat på de lagar, förordningar och avtal som påverkar den molntjänst som ska användas. Exempelvis måste risker för obehörig avlyssning, modifiering av hårdvara och programvara samt hemliga tvångsmedel tas med i beräkningen.

7.2 Säkerhetsskyddslagen

Den nya säkerhetsskyddslagen (2018:585) gäller från den 1 april 2019. Lagen medför flera väsentliga förändringar jämfört med den lagstiftning som gällt från 1996. I det följande redogörs för några av förändringarna som skulle kunna påverka Webbaserat kontorsstöd.

I 1 kap. 1 – 2 §§ framgår att den nya lagen gäller för den som till någon del bedriver verksamhet av betydelse för Sveriges säkerhet och att säkerhetsskyddsklassificerade uppgifter är uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt OSL, eller som skulle ha omfattats av sekretess enligt den lagen om den hade varit tillämplig. Detta innebär att även privata aktörer omfattas av lagstiftningen, dessa ansvarar därigenom självständigt för att enskilda säkerhetsskyddsklassificerade uppgifter samt aggregerade uppgifter som tillsammans blir säkerhetsskyddsklassificerade, hanteras säkert.

I 2 kap. 5 § anges att säkerhetsskyddsklassificerade uppgifter ska delas in i säkerhetsskyddsklasser utifrån den skada som ett röjande av uppgiften kan medföra för Sveriges säkerhet. Indelningen i säkerhetsskyddsklasser görs enligt följande:

1. kvalificerat hemlig vid en synnerligen allvarlig skada
2. hemlig vid en allvarlig skada
3. konfidentiell vid en inte obetydlig skada
4. begränsat hemlig vid endast ringa skada

I 2 kap. 6 § anges att statliga myndigheter, kommuner och regioner som avser att genomföra en upphandling och ingå ett avtal om varor eller tjänster ska se till att det i ett säkerhetsskyddsavtal anges hur kraven på säkerhetsskydd enligt 1 § ska tillgodoses av leverantören om:

1. det i upphandlingen förekommer säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre, eller
2. upphandlingen i övrigt avser eller ger leverantören tillgång till säkerhetskänslig verksamhet av motsvarande betydelse för Sveriges säkerhet.

Det finns ett samband mellan totalförsvarsverksamheten och säkerhetsskyddslagen, men säkerhetsskyddslagen tar endast sikte på uppgifter och verksamhet som är av betydelse för Sveriges säkerhet. Det räcker alltså inte att en verksamhet är samhällsviktig för att den ska anses vara av betydelse för Sveriges säkerhet. Avgörande för om samhällsviktig verksamhet också kan anses röra Sveriges säkerhet, och därmed omfattas av säkerhetsskyddslagens tillämpningsområde, är i stället att en antagonistisk handling mot verksamheten skulle kunna medföra skadekonsekvenser på nationell nivå. Emellertid kompliceras bilden av att begreppet Sveriges säkerhet inte ska tolkas kategoriskt. Skyddsvärda verksamheter på regional eller till och med lokal nivå skulle ändå kunna få nationell betydelse.

Som framgår av propositionen (2017/18:89) till den nya säkerhetsskyddslagen utgår säkerhetsskyddslagen idag från att behov av säkerhetsskydd främst gäller skydd av hemliga uppgifter. Kopplingen till OSL kan ge intryck av att säkerhetsskydd främst är en

angelägenhet för myndigheter och andra offentliga organ för vilka den lagen är tillämplig. Därutöver handlar det om ett säkerhetsskydd med inriktning att skydda mot terrorism för flygplatser och byggnader, anläggningar m.m. som enligt skyddslagen är skyddsobjekt. I propositionen anges vidare att avgränsningarna i lagen blivit för snäva och medför eller riskerar att medföra att t.ex. verksamheter som är av betydelse för att upprätthålla grundläggande samhällsfunktioner faller utanför tillämpningsområdet. Ett första steg är en ändrad systematik som bl.a. tydligare innefattar säkerhetskänslig verksamhet som bedrivs hos enskilda, dvs. även företag. Det anges också att det skyddsvärda området inte bör avgränsas genom regleringen om skyddsobjekt, utan ska utformas så att det även kan innefatta annan säkerhetskänslig verksamhet, t.ex. hantering av informationssystem eller sammanställningar av uppgifter som är av central betydelse för ett fungerande samhälle eller verksamhet som behöver skyddas på den grunden att den kan utnyttjas för att skada nationen.

Vid en analys av säkerhetsskyddslagen i förhållande till Webbaserat kontorsstöd uppstår frågan om en myndighet som anskaffar Webbaserat kontorsstöd sannolikt kommer att hantera säkerhetsskyddsklassificerade uppgifter och/eller ger tillgång till säkerhetskänslig verksamhet av betydelse för Sveriges säkerhet. Vad som är säkerhetsskyddsklassificerade uppgifter har en väsentligt vidare definition i den nya säkerhetsskyddslagen. Det kan inte uteslutas att myndigheter kan komma att befatta sig med sådan information eftersom Webbaserat kontorsstöd omfattar funktioner för ordbehandling, fillagring och e-post. I Säkerhetspolisens vägledning för säkerhetsanalys framkommer dessutom att bedömningen av säkerhetsskyddsnivån för ett it-system måste omfatta såväl de enskilda uppgifterna som den totala informationsmängden som it-systemet är tänkt att hantera. Information om hur säkerhetsskyddsklassificerade uppgifter skyddas, t.ex. driftdokumentation, processer, rutiner, arkitektur och design är känsliga och därför måste även dessa skyddas.

Nästa fråga blir om det spelar någon roll för myndighetens prövning av den första frågan om leverantören redan har ett större antal svenska myndigheter som kunder. Propositionen till nya säkerhetsskyddslagen anger bl.a. att ”hantering av informationssystem eller sammanställningar av uppgifter som är av central betydelse för ett fungerande samhälle” i sig ska anses omfattas av säkerhetsskydd. Det kan därför vara nödvändigt att ta reda på hur många andra myndigheter som finns hos en leverantör för att kunna avgöra om leverantören kan komma i fråga. Då uppstår frågan hur en sådan utredning skulle kunna genomföras, därtill kan en sådan utredning inte baseras på statisk information. Säkerhetsbedömningen måste hållas uppdaterad samtidigt som omständigheterna hos en leverantör och vilka kunder denne har kommer att förändras.

7.3 Utkontraktering

I ett digitaliserat samhälle och en globaliserad omvärld är elektroniska angrepp ett av de allvarligare hoten. Det innebär samtidigt att bristande informationssäkerhet är en av de allvarligare sårbarheterna, vilket ger upphov till stora konsekvenser för säkerhetsskyddet. Offentlig it-infrastruktur utsätts för elektroniska angrepp och underrättelseverksamhet. Idag ansvarar varje myndighet för sin egen it-verksamhet samtidigt som investeringar i it-säkerhet kan upplevas som kostsamma. Inför stora investeringar ställs myndigheter ofta inför frågan om arbetsuppgifter bör utföras inom den egna organisationen eller

utkontrakteras. Utkontraktering kan innebära att myndigheter visserligen effektiviserar men att de samtidigt då kan förlora kontrollen över vem som har åtkomst till skyddsvärd information. Även åtkomst till den egna informationen kan försvåras.

En utgångspunkt i allt säkerhetsskyddsarbete är att säkerhetskänsliga uppgifter ska ha samma nivå av skydd oavsett i vilken verksamhet de förekommer. För att bibehålla ett högt säkerhetsskydd vid utkontraktering av säkerhetskänslig verksamhet krävs därför en förberedande säkerhetsskyddsanalys. Det krävs också insikt om den egna verksamhetens nationella betydelse och beroendeförhållanden. I varje enskilt fall finns det dessutom anledning att bedöma om det över huvud taget är lämpligt att utkontraktera verksamheten. I ”Granskning av Transportstyrelsens upphandling av it-drift” talas om myndigheters förmåga att göra en analys av vilka delar av verksamheten som bör utkontrakteras, särskilt i relation till utbudet av globala, avancerade it-tjänster:

> *Det säger sig självt att om vissa centrala delar av de tekniska system som får en svensk myndighet att överhuvudtaget fungera styrs och underhålls från företag i länder långt borta så innebär det vissa risker. Även system som ska vara öppna och tillgängliga och som inte i sig innehåller någon känslig information kan vara av sådan samhällsbetydelse att det inte är lämpligt att kontrollen över dessa ligger någon annanstans än i Sverige.*

Stora konsekvenser kan uppstå när it-drift läggs ut hos privata företag. Utkontraktering kan innebära att flera kunders system och information samlas i samma lagringsmedium eller lagringsmiljö, vilket innebär en ökad exponering. I den nationella säkerhetsstrategin understryks att digitaliseringen har påverkan på Sveriges säkerhet. I säkerhetsstrategin nämns att digitaliseringen medför risker och hot som är förknippade med några av de mest komplexa säkerhetsutmaningarna. Som exempel anges antagonistiska hot som informationsoperationer och elektroniska angrepp mot skyddsvärda informations- och kommunikationssystem, t.ex. i form av dataintrång, sabotage eller spionage.

Av Säkerhetspolisens ”10 tips för säkrare outsourcing” kan utläsas att användande av utländska leverantörer med långa leverantörskedjor minskar möjligheterna till insyn ytterligare när leverantören utför arbetet utanför Sveriges gränser. Myndigheter bör därför ställa krav på att få godkänna vilka underleverantörer som huvudleverantören använder. Vid användande av molntjänster behöver en noggrann analys göras då det inte alltid är lämpligt att använda en viss molntjänstleverantör eller molntjänst. Särskild försiktighet bör iakttas då den information som molntjänstleverantören ska hantera innehåller allmänna handlingar, sekretessbelagda uppgifter eller personuppgifter. Information som är klassificerad som känslig och som kan medföra stora risker bör myndigheten avstå från att ha i molntjänster. Information som rör Sveriges säkerhet får inte hanteras i molntjänster om inte tillfredsställande säkerhetsskydd kan garanteras. Även om information får lämnas ut enligt OSL kan det som tidigare konstaterats finnas omständigheter som ändå gör det olämpligt att anlita en molntjänstleverantör. Omständigheter att beakta kan vara vem som i praktiken har kontroll över molntjänsten, vilket lands rättsordning som blir tillämplig på informationen som hanteras, om molntjänstleverantören regelbundet byter ut sina underleverantörer och vem som ansvarar för informationsförlust m.m. Information som upprättats i molntjänster kan också vara svåra att gallra och radera, särskilt på ett sätt

där myndigheten kan säkerställa att det verkligen har skett. Att ta bort information via molntjänstens gränssnitt är inte att jämställa med sådan radering där informationen inte går att återskapa.

Av Säkerhetspolisens ”Säkerhetsskyddad upphandling - en vägledning” framgår det att när myndigheter använder utländska molntjänster innebär det att svenska staten riskerar sämre kontroll över samhällsviktiga system eftersom möjligheterna att säkerhetspröva personal och utnyttja svenska kontrollinstrument är begränsade i utlandet. Det är dessutom svårare för svenska myndigheter att bedöma hotbilden i de länder till vilka verksamhet har utkontrakterats. Om det internationella säkerhetsläget förändras, vilket kan gå snabbt, saknas i värsta fall såväl kompetens som kapacitet och tid för att kunna flytta hem verksamheten till Sverige. Vidare blandas i molntjänster ofta flera kunders information i samma hårdvara och programvara. Detta medför en ökad risk då en störning för en kund kan orsaka störningar även för andra kunder. Att ha tillräcklig kontroll över molntjänstleverantörens driftspersonal är också svårt.

7.4 Ackumulering och aggregering

En ytterligare problemställning är hur situationen bör hanteras när utkontraktering av it-drift involverar en stor mängd uppgifter som sedda var för sig är klassificerade som begränsat hemliga, eller som inte är säkerhetsskyddsklassificerade alls, men som sammantagna kan vara betydligt känsligare i förhållande till Sveriges säkerhet. Det kan t.ex. handla om situationer där uppgifter som sammanställts har bearbetats eller kan bearbetas så att det av sammanställningen kan utvinnas annan och mer känslig information än av uppgifterna var för sig. En annan situation kan vara att den sammanställda informationen visar på exempelvis beroenden mellan olika verksamheter, förmåga, sårbarheter eller andra förhållanden som kan leda till en inte obetydlig skada för Sveriges säkerhet om den röjs. Det kan av förarbetena till säkerhetsskyddslagen utläsas att sammanställningar av uppgifter från olika källor kan göra att den sammanställda informationen kan anses utgöra säkerhetsskyddsklassificerade uppgifter även om informationen härrör från öppna källor. Uppgifterna i en sammanställning kan alltså vara säkerhetsskyddsklassificerade, fastän de i ett annat sammanhang inte är det var och en för sig. Det framgår vidare av förarbetena att myndigheter, vid sin klassificering av uppgifter, måste bedöma om en samling av uppgifter i en viss säkerhetsskyddsklass medför att en högre säkerhetsskyddsklass ska tillämpas. Dock bör onödiga administrativa kostnader undvikas och ingrepp i enskildas integritet m.m. bör inte utöka klassificeringen i större utsträckning eller med placering i högre klass än vad som är nödvändigt. Förarbets-uttalandena kan tolkas så att myndigheterna i sitt arbete med säkerhetsskydds-klassificering är skyldiga att beakta mängden uppgifter och konsekvenserna av att de sammanställs. Rättsläget kan alltså uppfattas på det sättet att en mängd uppgifter som, sedda var för sig, är att bedöma som begränsat hemliga bör klassificeras som konfidentiella om de finns i en samling och skadan vid röjande inte skulle bli obetydlig.

Av Transportstyrelsens utredning ”Kartlägga hanteringen av vissa uppgifter” framgår att myndigheten hanterar en enorm mängd uppgifter men att endast en begränsad del av informationsmängden handlar om hemliga uppgifter, en större del rör uppgifter som är sekretessbelagda, men den absolut största mängden uppgifter rör sig om information som

är offentlig. Trots att de flesta uppgifterna är öppen information blir den totala informationsmängden som Transportstyrelsen i vissa fall har sammanställt i sina register i sig en skyddsvärd tillgång. Det beror bl.a. på att det högupplösta grunddatat med sin detaljrikedom ger en allt för heltäckande bild av informationsinnehållet sett till olika säkerhetsperspektiv. Någon som har tillgång till helheten kan genom att analysera olika uppgifter upptäcka avvikelser och på detta sätt genom slutledning få fram hemlig information. Med en oinskränkt tillgång till stora informationsmängder följer i regel risker för åtgärder och analyser som av säkerhetsskäl inte bör få förekomma. Även avsaknad av information som borde ha funnits kan utgöra en risk.

I Säkerhetspolisens föreskrifter och allmänna råd om säkerhetsskydd samt vägledning för säkerhetsskydd beskrivs att en risk- och sårbarhetsanalys ska resultera i en sammanställning över de åtgärder som ska genomföras för att säkerhetsskyddet ska vara godtagbart. I analysen är myndigheten även skyldig att göra en bedömning av säkerhetsskyddsnivån av såväl de enskilda uppgifterna som den totala informationsmängden som systemet är tänkt att hantera. Detta gäller även om en myndighet upplåter ett it-system till en annan myndighet.

En molntjänstleverantör kommer till sin natur att ha omfattande nyttoinformation, driftinformation samt säkerhetsrelaterad information i form av loggar och liknande. Negativa konsekvenser kan därmed uppkomma genom att molntjänstleverantören kan skapa nya sammanställningar av känslig art. Om flera myndigheter använder samma molntjänst uppstår ännu fler möjligheter att sammanställa information. En större aggregerad mängd information om svenska myndigheter ökar givetvis intresset från antagonister att försöka komma åt denna information från just denna molntjänst, och med ökat intresse kommer mer resursstarka ansträngningar. Ytterligare konsekvenser uppstår över tid eftersom mängden information hela tiden ökar. En antagonist kan således göra mer avancerade analyser av svensk offentlig sektor ju längre tid som förlöpt.

7.5 Sammanfattning

Det finns en mängd parametrar som styr om bruket av Webbaserat kontorsstöd faller inom säkerhetsskyddslagen eller inte. Om Webbaserat kontorsstöd skulle falla inom säkerhetsskyddslagen behöver detta beaktas vid ramavtalsupphandlingen och av de myndigheter som avropar Webbaserat kontorsstöd.

En möjlig väg skulle kunna vara att Webbaserat kontorsstöd skapas på ett sådant sätt att t.ex. sekretessbelagd information och känsliga personuppgifter, även i stor skala, får hanteras men inte säkerhetsklassificerad information. Det skulle innebära att de flesta myndigheter skulle kunna hantera all sin information i Webbaserat kontorsstöd utan att den blir för komplicerad att skapa och underhålla samt att kostnaden hålls på en rimlig nivå. Leverantören kan vid någon punkt behöva, som enskild, göra en egen bedömning av hur säkerhetskänslig deras Webbaserat kontorsstöd är och därefter behöva vidta nödvändiga åtgärder.

Utöver bedömningar utifrån säkerhetsskyddslagen kan en myndighet behöva göra en konsekvensanalys där risker för obehörig avlyssning, modifiering av hårdvara och programvara samt hemliga tvångsmedel tas med i beräkningen.

8 Övrig analys

8.1 Inledning

Detta kapitel omfattar flera skilda frågeställningar som också kan påverka Webbaserat kontorsstöd, men som i sammanhanget har bedömts ha något mindre inverkan på Webbaserat kontorsstöd än frågeställningarna i kapitel 4 – 7.

8.2 Informationsklassning

En myndighet bör klassificera all sin information och hantera den därefter. Det är dock inte alltid enkelt för enskilda tjänstemän att bedöma vilken informationsklass en handling har, något som dessutom kan ändras över tid. Som exempel kan ett dokument inledningsvis endast innehålla okänslig information för att i ett senare skede innehålla säkerhetskänslig information. Likaså kan ett kalkylark med personuppgifter vid en punkt ha blivit en så stor aggregering av personuppgifter att kalkylarket måste klassificeras om.

Det finns verktyg som kan analysera uppgifter och automatiskt föreslå klassificering. Ett sådant verktyg kan vara till stor hjälp för den enskilde tjänstemannen, men är inte heltäckande. Webbaserat kontorsstöd bör därför ha sådana egenskaper att tjänstemän kan vara trygga med att t.ex. sekretessreglerad information och känsliga personuppgifter får hanteras i molntjänsten.

8.3 Informationssäkerhet för myndigheter

Den ökade användningen av it-system i offentlig sektor har gjort att frågor om informationssäkerhet blivit viktigare än någonsin. Att brister i sådan säkerhet kan få allvarliga konsekvenser är väl känt, vilket exempelvis framgår i ”Granskning av Transportstyrelsens upphandling av it-drift” (DS 2018:6).

Korrekt informationssäkerhet är mycket viktigt vid användandet av Webbaserat kontorsstöd. MSB är den myndighet som har i uppgift att samordna arbetet med hela samhällets informationssäkerhet samt har föreskriftsrätt på informationssäkerhets-området. Alla statliga myndigheter ska bedriva ett systematiskt informationssäkerhets-arbete med stöd av standarderna SS-EN ISO/IEC 27001:2017 och SS-EN ISO/IEC 27002:2017 om ledningssystem för informationssäkerhet samt rapportera allvarliga it-

incidenter som inträffar eller kunde ha resulterat i allvarliga konsekvenser för myndigheternas informationshantering. Kraven i sin nuvarande utformning har funnits sedan 2016 men liknande krav har funnits i över tio år. Ett kommande ramavtal måste ha tydliga kravställningar dels för att uppfylla MSB:s föreskrifter, dels för att underlätta myndigheternas informationssäkerhetsarbete.

8.4 Bevarande och gallring av handlingar

Arkivlagen (1990:782), arkivförordningen (1991:446) samt Riksarkivets föreskrifter och allmänna råd reglerar hur offentligas handlingar ska arkiveras och gallras. Lagring av allmänna handlingar i molntjänster ställer krav på tillförlitlighet och autenticitet. En myndighet som är skyldig att bevara allmänna handlingar måste kunna garantera handlingarnas autenticitet över tid och måste därför säkerställa att molntjänsten är tillförlitlig och att det finns förutsättningar för myndigheten, och i förlängningen även för enskilda, att få tillgång till de oförvanskade allmänna handlingarna. På motsvarande sätt måste myndigheten kontrollera att det finns förutsättningar att oåterkalleligt gallra allmänna handlingar.

Arkivförfattningarnas krav måste genomlysas innan en myndighet anlitar en molntjänst-leverantör för hantering av allmänna handlingar. En myndighet bör inte enbart förvissa sig om att det finns garantier för att bevara eller gallra allmänna handlingar. Myndigheten bör också överväga vilka generella risker som finns med att lagra sina allmänna handlingar i en molntjänst. Problem kan uppstå om molntjänstleverantören försätts i konkurs, blir uppköpt eller på annat sätt avvecklar sin verksamhet. För att så långt som möjligt undvika risken att allmänna handlingar går förlorade, sprids till obehöriga, förstörs etc. måste myndigheten säkerställa att det i avtalet med molntjänstleverantören finns villkor som ger myndigheten garantier för att arkivförfattningarnas regler kan uppfyllas.

Om molntjänstleverantören har underleverantörer måste myndigheten även säkerställa att handlingar varken förvanskas eller förstörs samt att även underleverantörer gallrar de handlingar som myndigheten beslutat gallra. Ju fler underleverantörer och komplexare molntjänst desto svårare för en myndighet att säkerställa arkivförfattningarnas krav.

Webbaserat kontorsstöd bör säkerställa att gallring kan ske korrekt, att leverantören kan garantera utplåning av gallrade handlingar, att handlingars autenticitet upprätthålls samt att alla handlingar verkligen förstörs när en myndighet avslutar Webbaserat kontorsstöd hos leverantören.

8.5 Patientsekretess

Vid behandling av patientuppgifter i hälso- och sjukvården gäller särskilda författnings-krav på säkerhetsåtgärder enligt patientdatalagen (2008:355) och patientsäkerhetslagen (2010:659) tillsammans med Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter i hälso- och sjukvården.

Eftersom patientuppgifter, dvs. uppgift om patients hälsa och personliga förhållanden, är av mycket integritetskänslig karaktär ställs stora krav på hanteringen t.ex. behörighetstilldelning, behörighetsstyrning, åtkomstkontroll, loggkontroll, loggars utformning, loggars livslängd, stark autentisering, kryptering, spärrade uppgifter, samtycke, aktiva val samt spårbarhet.

Av Socialstyrelsens föreskrifter och allmänna råd framgår det att vårdgivaren ska ansvara för att det finns loggar över bl.a. vilka åtgärder som har vidtagits med uppgifter om en patient, att det framgår vid vilken vårdenhet eller vårdprocess åtgärderna vidtagits samt patientens identitet. Dessa loggar ska sparas i minst fem år.

Gällande patientuppgifter i e-post är det oklart om detta alls är tillåtet, eventuellt kan kryptering möjliggöra det men rättsläget är oklart. Med e-post kan avsändare, mottagare, ärendemening och namn på bilagor inte krypteras vilket därför ställer krav på att den enskilde tjänstemannen aldrig anger något som rör en patient där.

Sekretessbelagda patientuppgifter kan sannolikt inte alls hanteras i en chatt eller i en videokonferens. Att hantera patientuppgifter i ett kalkylark eller dokument i Webbaserat kontorsstöd ställer speciella krav på t.ex. molntjänstens uppbyggnad, loggning och arkivering men det är högst oklart om lagkraven tekniskt alls kan tillgodoses i en molntjänst. Datainspektionen har i tillsynsärendet 1947-2016 angett att vårdgivaren är personuppgiftsansvarig enligt patientdatalagen och därför ska se till att personuppgifter behandlas bara om det är lagligt och i enlighet med vårdgivarens instruktioner till personer som arbetar under vårdgivarens ledning. Vidare anges att enligt patientdatalagen är vårdgivaren skyldig att dokumentera all elektronisk åtkomst för att ge vårdgivaren möjlighet att kontrollera åtkomst i efterhand.

8.6 Inlåsningseffekter

Inlåsningseffekter är ett mångfacetterat område. Vissa effekter är av teknisk natur, t.ex. filformat, API:er och kompatibilitet. Andra rör mera mjuka värden som kompetens, utbildning, tradition och vana.

Både Konkurrensverket och EU-kommissionen har gjort studier över inlåsningseffekter i it-system. Slutsatserna från dessa studier är att både proprietära programvaror och molntjänster för med sig betydande inlåsningseffekter. Många myndigheter är inlåsta i it-system eftersom detaljerad kunskap om hur systemet fungerar endast är tillgängligt för leverantören, och att när de behöver köpa ny funktionalitet eller nya licenser är det endast den befintliga leverantören som kan leverera. Bättre utnyttjande av öppna standarder gör det möjligt för konkurrenter att erbjuda alternativa lösningar vilket minskar inlåsningen och ger ökad konkurrens, vilket i sin tur sänker priserna och höjer kvaliteten. Dessutom kan beroendet till en enda leverantör av ett it-system och dess framtida utveckling leda till problem med kontinuitet eftersom det finns en risk att leverantören väljer att sluta stöda it-systemet eller viss funktionalitet i it-systemet. För att en myndighets information ska kunna vara åtkomlig på lång sikt och för alla brukare krävs det att informationen inte är lagrad på ett sådant sätt att endast det it-system som skapade informationen till fullo kan tillgodogöra sig informationen.

En myndighet bör alltid beakta vilka långsiktiga effekter som kan uppstå för den information som upprättas i ett it-system. Detta är viktigt eftersom informationen många gånger måste kunna förvaltas långt efter att det it-system som ursprungligen anskaffades tagits ur drift. Dessa långsiktiga effekter inkluderar även aspekter som rör inter-operabilitet mellan olika it-system och förvaltning av information inom och utanför den egna organisationen, exempelvis de processer som är nödvändiga för att organisationen ska kunna överlämna information till Riksarkivet för långtidslagring. En myndighet kan inte förutsätta att ett filformat, så som det implementerats i det ursprungliga it-systemet, har tillgänglig dokumentation i tillräcklig utsträckning. Detta kan leda till stora problem om det i princip är omöjligt att utveckla en teknisk lösning för att migrera och arkivera sin egen information.

Webbaserat kontorsstöd bör motverka inlåsningseffekter genom att använda sig av öppna standarder, t.ex. för filformat, kommunikationsprotokoll och API:er. Dessutom bör Webbaserat kontorsstöd skapas med programvara som är långsiktigt förvaltningsbar för att säkerställa att information är användbar på lång sikt. Om inlåsningseffekter minimeras blir det väsentligt enklare och mer juridiskt hållbart för en myndighet att byta leverantör av Webbaserat kontorsstöd utan informationsförluster.

8.7 Cybersecurity Act

Under 2019 kommer sannolikt EU:s nya förordning ”Cybersecurity Act” att träda i kraft. Cybersecurity Act är en kompletterande lagstiftning till dataskyddsförordningen och NIS-direktivet. Syftet är att främja it-säkerheten inom EU genom att EU:s byrå för nät- och informationssäkerhet, ENISA, får utökat mandat och befogenheter.

Cybersecurity Act kommer innebära att leverantörer kan låta ENISA certifiera sina produkter och tjänster, bl.a. molntjänster. Certifieringen kommer t.ex. innebära att vissa standarder ska uppfyllas, vissa tekniska krav samt att vissa kravställda processer ska finnas på plats. En produkt eller tjänst som är certifierad av en medlemsstat kommer automatiskt vara erkänd som certifierad i hela EU vilket är tänkt att förenkla för alla parter och sänka tröskeln för handeln mellan medlemsstaterna.

Cybersecurity Act ger också ENISA ett utökat mandat att stödja medlemsländerna och EU-institutionerna i it-säkerhetsfrågor, ENISA kommer därför att få utökade resurser.

När Cybersecurity Act trätt i kraft bör det utredas närmare om en certifiering ska vara ett krav på varje leverantör som tillhandahåller Webbaserat kontorsstöd.

8.8 Hållbarhet

Statens inköpscentrals målsättning är att inom ramen för verksamhetens uppdrag, offentlig sektors behov och lagstiftningens möjligheter, på ett ansvarsfullt sätt beakta miljö och sociala hänsyn vid upphandling och förvaltning av de statliga ramavtalen. De statliga ramavtalen ska bidra till att offentlig sektor kan möta de mål som satts i den nationella upphandlingsstrategin, Agenda 2030 och de nationella miljömålen.

Hållbarhetshänsyn kan tas i alla delar av en upphandling, dvs. som kvalificeringskrav (t.ex. krav på miljöledningssystem), som tekniska krav (t.ex. krav på viss märkning eller certifiering), eller som kontraktsvillkor (t.ex. arbetsrättsliga villkor).

De datacenter där driften av Webbaserat kontorsstöd sker har en väsentlig miljöpåverkan i form av datorer, klimatanläggningar och elförbrukning. En kommande ramavtals-upphandling bör därför ställa krav på att dessa datacenter är energieffektiva och att ägarna av datacentren aktivt arbetar med att minska sin miljöpåverkan.

17 kap. 2 § LOU reglerar skyldigheten för upphandlande myndighet att alltid ställa vissa arbetsrättsliga villkor, när det är behövligt. Bedömningen av behövligheten ska vara en helhetsbedömning vid vilken myndigheten kan beakta såväl egna erfarenheter som uppgifter från branschorganisationer, arbetsmarknadens parter eller från andra aktörer. Behovet ska avse risken för oskäliga arbetsvillkor i Sverige.

Statens inköpscentral har lång erfarenhet av ramavtal för programvaror, molntjänster och datacenter samt har haft dialog med ett stort antal myndigheter, leverantörer och branschorganisationer under åren. Baserat på det har det inte framkommit missförhållanden gällande arbetsrätt, facklig tillhörighet eller diskriminering. Statens inköpscentral anser därför att varken branschen som sådan medför risk för oskäliga arbetsvillkor eller andra omständigheter medför att det är behövligt att ställa arbetsrättsliga villkor.

9 Omvärldsbevakning

9.1 Australien

Australien adderade i december 2018 lagstiftning till sina telekommunikationslagar genom Telecommunications and Other Legislation Amendment (Assistance and Access) Act. Tilläggen innebär t.ex. att molntjänstleverantörer blir skyldiga att bygga in funktioner för att australiensiska rättsvårdande myndigheter ska kunna få tillgång till krypterad information. Kryptering är en komplex fråga, dels ska den personliga integriteten och myndigheters information skyddas, dels behöver rättsvårdande myndigheter ha möjlighet att förhindra och beivra brott.

Lagen innebär att rättsvårdande myndigheter i Australien kan tvinga t.ex. molntjänstleverantörer att bistå med hjälp gällande krypterad information på tre olika sätt:

1. En begäran om att ”frivilligt” hjälpa rättsvårdande myndigheter.

2. En begäran om att molntjänstleverantören ska dekryptera information om molntjänstleverantören redan innehar möjlighet att dekryptera.
3. Ett krav på molntjänstleverantörer att bygga in möjligheten för rättsvårdande myndigheter att få ut dekrypterad information.

De två första punkterna påminner om flera länders lagstiftning, men den tredje punkten är, vad projektgruppen känner till, Australien först ut i västvärlden med.

Det finns tre motiveringar i lagen som möjliggör för rättsvårdande myndigheter i Australien att kräva hjälp av en leverantör:

1. Rättshjälp vid allvarliga brott mot australiensisk rättsordning.
2. Rättshjälp vid synnerligen allvarliga brott enligt andra länders rättsordning.
3. Skydda den nationella säkerheten.

Den australiensiska lagstiftningen belyser svårigheterna med stora it-projekt där myndighetens införandekalkyl bygger på ett långvarigt nyttjande, samtidigt som rättsliga förutsättningar utanför myndighetens kontroll snabbt kan påverka möjligheten att använda tjänsten. Projektgruppen gör bedömningen att liknande lagstiftning kan komma att dyka upp i fler länder varför denna risk måste tas i beaktande.

9.2 Nederländerna

Den nederländska staten gav ut en rapport, i form av en ”Data Protection Impact Assessment” under dataskyddsförordningen, i november 2018 gällande hur programvaran ”Office” samt molntjänsterna ”Sharepoint online” och ”Onedrive online” från Microsoft förhåller sig till dataskyddsförordningen.

Rapporten sammanfattar åtta risker med programvaran och molntjänsterna:

1. Enskilda organisationer kan inte överblicka de specifika risker som kan påverka dem eftersom leverantören inte tillhandahåller några verktyg eller dokumentation över datainsamlingen.
2. Ingen möjlighet för kunden att påverka eller avsluta datainsamlingen.
3. Olaglig lagring av känslig och hemlig information, både metadata och innehåll skapat av kunden.
4. En felaktig bedömning från leverantörens sida att denne endast är personuppgiftsbiträde när den i själva verket är delad personuppgiftsansvarig tillsammans med kunden, så som anges i artikel 26 i dataskyddsförordningen.
5. Inte tillräcklig kontroll över underbiträden och vilken personuppgiftsbehandling som faktisk sker.
6. Brist på ändamålsbegränsning av personuppgiftsbehandlingen både vad gäller behandling av insamlad diagnostisk data samt möjligheten att addera nya behandlingar av dessa data.
7. Överföring av all sorts diagnostisk data utanför EU/EES med hjälp av Privacy Shield, vars giltighet är föremål för rättsprövning av EU-domstolen.

8. Ingen bortre tidsgräns för hur länge leverantören får spara diagnostisk data och inget verktyg med vilket kund kan radera insamlad diagnostisk data.

En slutsats de drar är att myndigheter som använder programvaran och/eller molntjänsterna därför behöver säkerställa hur dessa risker ska kunna hanteras. Detta kan delvis göras genom att olika funktioner i programvaran stängs av men också genom att undvika molntjänsterna helt och hållet, inklusive molntjänsten ”Office 365” som innehåller ”Sharepoint” och ”Onedrive”. Om leverantören i framtiden anser sig ha hanterat alla riskerna på ett adekvat sätt behöver myndigheterna göra en förnyad granskning.

Projektgruppen vill framhålla att även om rapporten specifikt analyserar en programvara och två molntjänster från en specifik leverantör är det inte orimligt att anta att andra proprietära programvaror och molntjänster skulle bedömas på ett likartat sätt vid en likartad granskning.

9.3 Tyskland

Tyskland har en strikt reglering om att sekretessbelagd information inte får lagras eller bearbetas utanför Tyskland. Detta har skapat utrymme för nytänkande hos leverantörerna och den tyska staten. Ett exempel är att Deutsche Telekom, under 2015 – 2016, byggde två nya datacenter i Tyskland där de skapade en helt tysk version av bl.a. ”Office 365”. Molntjänsten blev inte tillräcklig framgångsrik av flera anledningar och är i princip helt avvecklad idag.

Tyska federala myndigheter har genom deras myndighet för Shared Services, Informationstechnikzentrum Bund, skapat en statlig molntjänst ”Bundescloud” där federala myndigheter idag kan ansluta sig för fillagring och dokumenthantering. Molntjänsten är baserad på programvaran ”Nextcloud”. Enligt företrädare för Informationstechnikzentrum Bund kommer tjänsten att under 2019 utökas med kollaborativa verktyg för ordbehandling, kalkylark och presentationsverktyg för att senare utökas med chatt och videokonferens. Tjänsten är säkerställd både enligt dataskydds-förordningen och tyska sekretesslagar samt granskad av den tyska myndigheten för it-säkerhet, Bundesamt für Sicherheit in der Informationstechnik.

9.4 USA

2018 förnyade USA på nytt FISA sektion 702. I och med detta är sektion 702 giltig till slutet av 2023, men kan förlängas ytterligare. Sektion 702 ger amerikanska underrättelse-myndigheter rätt att samla på information om icke-amerikanska medborgare där det finns ett tydligt motiv för insamling. Det är för en svensk civil myndighet svårt att bedöma om någon hotbild finns eller om signalspaning pågår gentemot myndigheten. Oavsett hur det ligger till finns det ingen mekanism där en svensk myndighet kan få insyn i detta varför även denna lagstiftning bör tas med i risk- och sårbarhetsanalysen.

9.5 Sammanfattning

Det sker stora förändringar i världen som påverkar molntjänster varav endast en delmängd är möjlig för en myndighet att konkret bedöma. Webbaserat kontorsstöd som används av myndigheter i stor skala skulle kunna vara av intresse för andra länder att kunna avlyssna, påverka och/eller slå ut.

10 Leverantörsperspektiv

10.1 Inledning

För att kartlägga leverantörernas utbud inom Webbaserat kontorsstöd och fånga in synpunkter på hur ett kommande ramavtal skulle kunna konstrueras har det i förstudien genomförts möten med olika typer av leverantörer. Samtliga leverantörer återges i avsnitt 14.2. Detta kapitel berör den information projektgruppen inhämtat från leverantörerna.

10.2 Möten med leverantörer

Projektgruppen träffade leverantörerna enskilt för att säkerställa en öppen dialog. Mötena har inte protokollförts.

Generellt sett var leverantörerna eniga om att rättsläget har förändrats och att det numera behöver göras fler rättsliga bedömningar i förhållande till molntjänster. Leverantörerna beskrev nuvarande marknad för Webbaserat kontorsstöd i Sverige som en oligopolmarknad där det i princip bara är två leverantörer som förekommer, Microsoft och Google.

Enligt flera leverantörer säljer vissa amerikanska molntjänstleverantörer speciella versioner av sina molntjänster anpassade för myndigheter. Dessa är i dagsläget, enligt uppgift från leverantörerna, endast tillgängliga för amerikanska myndigheter. Bakgrunden ska vara att amerikanska myndigheter ställer högre säkerhetskrav på molntjänsterna varför dessa måste tillhandahållas i separata miljöer med högre säkerhet.

Vad projektgruppen uppfattat finns det ingen tjänst på den svenska marknaden idag, utöver tjänsterna från Google och Microsoft, som har hela den funktionalitet som förstudien omfattar. En följd av det blir att de rättsliga analyserna i kapitel 4 – 8 som rör utländska molntjänster i allmänhet och amerikanska molntjänster i synnerhet måste beaktas fullt ut.

Flera leverantörer som projektgruppen träffade är principiellt positiva till att medverka till att ta fram alternativ till de former av Webbaserade kontorsstöd som finns på marknaden idag. De flesta är medvetna om att ingen har en sådan molntjänst idag och att flera leverantörer kommer behöva samarbeta för att kunna skapa ett komplett erbjudande. Av

de systemintegratörer som projektgruppen träffade ansåg samtliga att det skulle vara möjligt att utveckla och underhålla ett Webbaserat kontorsstöd.

Marknaden idag präglas av att systemintegratörerna bedriver en typisk återförsäljarverksamhet av molntjänsterna från Microsoft och Google samt adderar konsulttjänster för t.ex. migrering, integration och utbildning. Det förekommer också att systemintegratörerna sätter ihop en kundspecifik lösning där de sammanfogar olika molntjänster.

Kunskapsnivån hos de olika leverantörerna gällande de olika juridiska regelverk som en myndighet som använder Webbaserat kontorsstöd behöver beakta var mycket varierad. En tolkning av detta är dels att det saknas tydliga och allmänt tillgängliga instruktioner eller regler att förhålla sig till, dels att kompetensen rörande t.ex. sekretessregler, Sveriges säkerhet och inlåsningseffekter generellt behöver höjas.

10.3 Sammanfattning

Möten med leverantörer har visat att marknaden domineras av ett fåtal amerikanska molntjänstleverantörer samt att det inte upplevs finnas några realistiska alternativ till dessa i dagsläget. Givet frågeställningen som förstudien tydliggör och alternativet att upphandla ett ramavtal finns ett klart intresse från flera leverantörer att vilja vara med och utveckla Webbaserat kontorsstöd som kan omhänderta svensk offentlig sektors behov och de regleringar som styr dessa verksamheter.

11 Marknadsanalys

11.1 Inledning

För att kartlägga marknadens utbud har projektgruppen, utöver leverantörsmöten, undersökt marknaden för både programvaror och molntjänster som helt eller delvis erbjuder förstudiens funktionella avgränsning.

11.2 Nuvarande marknadsutbud

De leverantörer som projektgruppen identifierat som är marknadsledande för ett komplett Webbaserat kontorsstöd är Microsoft med sin tjänst ”Office 365” och Google med sin tjänst ”G Suite”. Utöver dessa har IBM sin tjänst ”Connections”.

Vad projektgruppen har funnit är att dessa tre tjänster är välutvecklade, stabila och med god funktionalitet. Sättet de fungerar på och mängden funktionalitet skiljer sig åt en del men alla verkar uppfylla de grundläggande funktionalitetskrav som förstudien omfattar.

Det finns en mängd leverantörer som säljer t.ex. lagring, e-post, videokonferens, fildelning eller ordbehandling som molntjänst. Projektgruppen har dock inte funnit någon utöver de tre nyss angivna leverantörerna som i dagsläget säljer detta som en helhet.

11.3 Komponenter

Om en leverantör vill skapa en egen tjänst finns det en mängd olika komponenter att använda. Vissa är licensierade med en proprietär licens, andra är licensierade med en öppen källkodslicens. Många av programvarorna har färdiga integrationer med vissa av programvarorna medan andra är mer isolerade. Nedan angivna programvaror, i bokstavsordning, är endast ett axplock för att påvisa olika sorters programvaror och ska inte ses som en uttömmande lista.

För fillagring och dokumenthantering finns t.ex. Alfresco, Nextcloud, Owncloud, Pydio, Seafile, Sharepoint och Storegate. Dessa är inte direkt jämförbara då deras funktionalitet skiljer sig en hel del åt, likaså pris, licensmodell och funktioner utöver fillagring och dokumenthantering.

Chatt och videokonferens är oftast molntjänster men t.ex. Jitsi och Skype for business finns som programvara.

Exempel på programvaror för kollaborativ ordbehandling, kalkylark och presentation inkluderar bl.a. Libreoffice Online, Onlyoffice och Sharepoint med Office Online Server.

Programvaror som finns för e-post, kalender och kontakter är t.ex. Egroupware, Exchange, Open-Xchange, Securemailbox och Zimbra. Till detta går att addera programvara för mötesbokning, t.ex. Framadate.

Utöver dessa programvaror som löser delar av funktionaliteten finns plattformar som innehåller flera av funktionerna t.ex. Nextcloud, Sandstorm, Sharepoint och Zimbra.

11.4 Tekniska överväganden

Tillhandahållande av Webbaserat kontorsstöd kommer sannolikt behövas över lång tid, minst 10 år men 20 år är sannolikt en rimlig målbild. Den tekniska livslängden behöver därför tas med i beräkningen när det gäller hur Webbaserat kontorsstöd skapas för att säkerställa långsiktig hållbarhet.

Det skulle vara fördelaktigt om leverantörerna erbjuder tekniskt diversifierade lösningar för att minska samhällets sårbarhet samt ge leverantörerna större möjlighet att erbjuda olika värdeadderande tjänster. Mot detta står att det blir mer komplicerat för myndigheter som vill byta från en leverantör till en annan samt att leverantörerna eventuellt skulle kunna minska sina risker vid uppbyggnaden genom att dela på kompetens rörande grundläggande komponenter. I det fall många av leverantörerna använder samma programvara som hämtas från samma källa uppstår en ny risk för hela offentlig sektor om programvaran är komprometterad. Det kommer sannolikt krävas betydande insatser för

att säkerställa att all programvara verkligen är säker att använda i Webbaserat kontorsstöd.

Om internet är den enda informationsbäraren mellan myndigheten och leverantören måste risken för att internet i Sverige slås ut tas med i beräkningen. Det bör därför övervägas vilka krav på anslutningar en leverantör av Webbaserat kontorsstöd ska erbjuda utöver internet.

Oavsett hur Webbaserat kontorsstöd skapas måste ett grundläggande krav vara att öppna standarder används, särskilt gällande filformat och kommunikationsprotokoll.

11.5 Sammanfattning

Den svenska marknaden för Webbaserat kontorsstöd idag är i princip uppdelad mellan två leverantörer. Det finns dock en mängd tillgängliga programvaror som tillsammans kan användas som grund för Webbaserat kontorsstöd om marknaden är beredd att skapa alternativ.

Kraven på säkerhet i Webbaserat kontorsstöd blir självklart höga. För att inte myndigheter eller leverantörer ska råka urholka säkerheten bör en eventuell ramavtalsupphandling även ta sikte på hur olika leverantörers Webbaserat kontorsstöd kommunicerar med varandra samt hur myndigheterna kommunicerar med Webbaserat kontorsstöd.

12 Slutsatser

12.1 Inledning

Projektgruppen har genom samtal med it-branschen, myndigheter och experter, samt inläsning av en stor mängd rapporter, beslut och juridisk doktrin försökt att skaffa sig en bred bild av de problem och möjligheter som finns rörande Webbaserat kontorsstöd.

Projektgruppen har noterat att det råder konsensus om att dagens marknad domineras av två amerikanska molntjänstleverantörer. Samtidigt har det framkommit ett flertal juridiska frågeställningar kring användningen av t.ex. amerikanska molntjänster.

Projektgruppen har därför haft att ta ställning till hur ett eventuellt kommande ramavtal skulle kunna upphandlas, och med vilken kravställning, för att offentlig sektor ska få tillgång till ändamålsenligt Webbaserat kontorsstöd som samtidigt uppfyller gällande lagar.

Projektgruppen har även övervägt några olika alternativ för hur Webbaserat kontorsstöd skulle kunna upphandlas. Dessa alternativ är endast utkast som påvisar några möjliga vägar framåt. Alternativen framgår i avsnitt 12.4 – 12.6.

12.2 Säkerhet

En grundförutsättning, och som inte får vara något som adderas på i efterhand, för Webbaserat kontorsstöd är att säkerheten är tillräcklig för att myndigheter tryggt ska kunna lagra och bearbeta uppgifter som åtminstone är sekretessbelagda samt känsliga personuppgifter, oavsett uppgiftsmängd.

En leverantör av Webbaserat kontorsstöd kan i framtiden komma att omfattas av säkerhetsskyddslagen, exempelvis genom att leverantören bedömer att den aggregerade mängden uppgifter i Webbaserat kontorsstöd innebär att ny information uppstår som då blir säkerhetsskyddsklassificerad. Leverantören behöver då på egen hand vidta de åtgärder som krävs för att uppfylla säkerhetsskyddslagen.

Behovet av att Sverige som land har kontroll över sin information och konsekvenserna av att inte ha tillgång till informationen kan beaktas utifrån ett totalförsvarsperspektiv. I en internationell kris eller konflikt, kan övervägas viljan och förmågan från andra länder att bereda sig tillgång till, manipulera eller neka åtkomst till information som en leverantör hanterar. Risken är att avtalsinnehåll vid sådana tillfällen kan frångås och att informationen då inte skyddas mot obehörig åtkomst.

Programvara som används bör, av säkerhetsskäl, i första hand vara öppen källkod, i andra hand källkodsgranskad, i tredje hand programvara där det gjorts utförliga tester på programvarans beteende för att säkerställa dess tillförlitlighet.

Underliggande hårdvara bör, av säkerhetsskäl, endast användas för leverantörens tillhandahållande av Webbaserat kontorsstöd. Endast myndigheter som avropat från det kommande ramavtalet får vara kunder i samma driftsmiljö. Hårdvara bör dessutom vara så öppen som möjligt för granskning, t.ex. från Open Compute Project. Webbaserat kontorsstöd bör kunna dela datacenter med andra tjänster som leverantören tillhandahåller inklusive exempelvis el, reservkraft, kyla, brandskydd och bevakning. Alla lagringsmedia ska vara krypterade.

Webbaserat kontorsstöd bör loggas i ett loggsystem med oavvislighetsmekanismer.

Varje leverantör av Webbaserat kontorsstöd bör, för att upprätthålla hög tillgänglighet, dels ha en egen anslutning till internet specifikt för Webbaserat kontorsstöd, dels mot dubbla internetleverantörer. Utöver anslutning till internet skulle det också vara positivt om varje leverantör av Webbaserat kontorsstöd har en egen förbindelse, som inte är en del av internet, till varje annan leverantör av Webbaserat kontorsstöd. Dessa anslutningar bör då vara hårdvarukrypterade på länklagret. Med dessa åtgärder kommer Webbaserat kontorsstöd dels inte vara lika sårbart för överbelastningsattacker från internet, dels möjliggöra informationsutbyte mellan myndigheter som i alla led är krypterad och skild från internet.

12.3 Rättsliga krav

En leverantör av Webbaserat kontorsstöd får inte behandla personuppgifter för egna syften eftersom det inte finns rättsligt stöd för det. Leverantören behöver ta detta i beaktande vid skapande av Webbaserat kontorsstöd. Webbaserat kontorsstöd ska dessutom vara skapad så att all slags personuppgiftsbehandling som en myndighet har rätt att göra i sin myndighetsutövning är legal att utföra i Webbaserat kontorsstöd. Detta inkluderar behandling av känsliga personuppgifter.

En leverantör av Webbaserat kontorsstöd får inte ta del av eller röja uppgifter utan att en myndighet så begärt, t.ex. vid felavhjälpning. En teknisk lösning med oavvislighetsloggar bör övervägas, som ger myndigheten en självständig kontrollmöjlighet genom att loggar fortlöpande kopieras till myndigheten. På detta sätt torde sekretessreglerade uppgifter kunna lagras och bearbetas av myndigheten i Webbaserat kontorsstöd.

Vid en eventuell ramavtalsupphandling bör Statens inköpscentral, utifrån samtliga rättsliga aspekter, ställa långtgående krav för att förenkla så mycket som möjlighet för myndigheternas avrop.

En kommande upphandling måste ta hänsyn till olika förändringar på marknaden och hos leverantörerna som kan uppkomma under tiden ramavtalet är i kraft. Ett exempel på förändring är om en leverantör hamnar på obestånd. Myndigheters data som finns hos den leverantören måste då kunna flyttas till någon annan tjänst med ganska kort varsel. I detta läge aktualiseras dels frågan om format på informationen, dels konkursförvaltarens intressen i förhållande till ramavtalet. Ett annat exempel är om en leverantör köps upp av en utländsk leverantör och där lagstiftning i köparens hemvist kan tvinga leverantören att lämna ut kundinformation. I det läget torde leverantören inte längre kunna vara leverantör på ramavtalet. Frågan om format på informationen aktualiseras även här. Det bör också övervägas avtalsvillkor som ger framförhållning i situationer där leverantörers obestånd, uppköp och liknande förhållanden kan bli aktuella.

12.4 Alternativ 1 - Stegvis uppbyggnad

Det förefaller sannolikt att flera leverantörer, som vill delta i en kommande ramavtals-upphandling, i dagsläget inte tillhandahåller Webbaserat kontorsstöd. Ett alternativ är då att ramavtalsupphandlingen möjliggör för leverantörerna att stegvis bygga upp Webbaserat kontorsstöd.

Ett förslag på hur denna stegvisa uppbyggnad skulle kunna gå till är följande:

Steg 1 – Fillagring och dokumenthantering. En myndighet kan i detta steg lagra alla typer av uppgifter utom säkerhetsskyddsklassificerade uppgifter i Webbaserat kontorsstöd. Webbaserat kontorsstöd bör vara konstruerat på så sätt att information säkert kan delas mellan alla myndigheter som har Webbaserat kontorsstöd. Efter att steg 1 är i drift är minst fysisk uppbyggnad, inloggning, loggning och säkerhet genomfört. Steg 1 torde vara relativt lätt för en myndighet att migrera till, dock beroende på kraven på metadata. Leverantören kan i detta läge börja ta betalt för Webbaserat kontorsstöd.

Steg 2 – Addera chatt, videokonferens och kontakter. En myndighet kan nu konferera säkert via text och video både internt och med andra myndigheter som också har Webbaserat kontorsstöd. Även videokonferens med parter som inte har Webbaserat kontorsstöd bör kunna bjudas in, dock med lägre säkerhet.

Steg 3 – Addera ordbehandling, kalkylark och presentation. En myndighet kan nu upprätta nya handlingar samt arbeta kollaborativt i samma dokument, även tillsammans med andra myndigheter som också har Webbaserat kontorsstöd.

Steg 4 – Addera e-post och kalender. En myndighet kan nu hantera e-post säkert inom myndigheten, mellan myndigheter som också har Webbaserat kontorsstöd samt, dock med lägre säkerhet, omvärlden.

Varje steg innebär utökad funktionalitet ovanpå redan tidigare byggda steg. I slutändan är tjänsten komplett och fullt integrerad. Genom detta stegvisa förfarande kan en leverantör ta en begränsad risk, börja ta betalt relativt tidigt och myndigheterna får för varje steg en bättre tjänst där redan det första steget innebär något som marknaden inte erbjuder idag.

12.5 Alternativ 2 – Komplett lösning

Alternativ 2 innebär att ramavtalsupphandlingen utgår från att leverantörerna skapar helt separata Webbaserat kontorsstöd med komplett funktionalitet, men med lång leveranstid. Varje leverantör ansvarar för sin egen Webbaserat kontorsstöd och inga krav ställs på att leverantörernas Webbaserat kontorsstöd ska kopplas samman.

Detta alternativ innebär att leverantören behöver investera mer i sitt Webbaserat kontorsstöd innan det går att ansluta myndigheter men de slipper kostnader för att bygga ihop sitt Webbaserat kontorsstöd med andra leverantörers. Webbaserat kontorsstöd blir på detta sätt funktionellt mer jämförbart med dagens erbjudanden än alternativ 1.

12.6 Alternativ 3 – Endast programvaror

Alternativ 3 innebär att leverantören säljer en programvara, eller svit av programvaror, med tillhörande underhållsavtal och konsulttjänster. Myndigheten får då sköta drift av Webbaserat kontorsstöd på egen hand.

Detta alternativ är på flera sätt enklast ur ett rättsligt perspektiv, men ställer högst krav på myndighetens egen it-drift och it-säkerhet.

13 Rekommendation

Förstudierapporten visar att myndigheterna har ett behov av ett juridiskt hållbart Webbaserat kontorsstöd som ger stöd för fillagring, dokumenthantering, samarbetsverktyg, ordbehandling, e-post och andra funktioner. Avrop av Webbaserat kontorsstöd från ramavtalen inom Programvaror och tjänster bedöms i dagsläget som orealistiskt eftersom projektgruppen inte har identifierat någon leverantör som för närvarande tillhandahåller Webbaserat kontorsstöd med full funktionalitet och där uppfyllande av samtliga identifierade regelverk kan säkerställas. Förstudierapporten visar också att det framstår som tekniskt möjligt och hanterbart att upphandla Webbaserat kontorsstöd som både är tekniskt och rättsligt godtagbart. Det förutsätter dock att offentlig sektor tillsammans med marknaden först har tagit tillräckliga initiativ för att påvisa ett konkret behov och investeringsvilja. Exempel på offentliga aktörer med kompetens och resurser att driva frågan framåt kan vara samverkansorganisationer, regioner och de stora statliga myndigheterna, antingen var för sig eller gemensamt. Statens inköpscentral ser positivt på att bidra till sådana initiativ med sin kompetens och erfarenhet.

För att upprätthålla kontinuitet i frågan och behålla tempo föreslås att Statens inköpscentral tillsvidare, och innan andra initiativ är etablerade, genomför en fördjupad dialog med offentlig sektor samt företrädare från it-branschen som på egen hand har förmåga att leverera hela eller stora delar av Webbaserat kontorsstöd. Projektgruppen rekommenderar att Statens inköpscentral, när en marknad har etablerats, genomför en ramavtalsupphandling av Webbaserat kontorsstöd som kan användas av hela offentlig sektor.

14 Källförteckning

14.1 Referensgrupp

Följande myndigheter, regioner, kommuner och övriga deltog i referensgruppen.

Barnombudsmannen
Borlänge kommun
eSamverkansprogrammet
Falköpings kommun
Falu kommun
Försäkringskassan
Inera

Kammarkollegiet
Konjunkturinstitutet
Kungliga tekniska högskolan
Lantmäteriet
Länsstyrelsen
Migrationsverket
Pensionsmyndigheten
Region Skåne
Region Stockholm
Region Värmland
SMHI
Tandvårds- och läkemedelsförmånsverket
Tillväxtverket
Trafikverket

14.2 Möten med leverantörer

Följande företag deltog i leverantörsmöten.

Atea Sverige AB
Blue Safespring AB
Bouvet Public Skills AB
CAG Group AB
City Network Hosting AB
Crayon AB
DGC One AB
Digitalist Sverige AB
Dustin Sverige AB
Google Sweden AB
Microsoft AB
Online Partner AB
Proact IT Group AB
RedBridge AB
Redpill Linpro AB
Saab AB
SecureAppbox AB
Storegate AB

14.3 Expertstöd

Följande bidrog med expertstöd.

Advokatfirman Conny Larsson
Försvarets materielverk
Hannes Snellman Advokatbyrå
Myndigheten för samhällsskydd och beredskap

Romab
Säkerhetspolisen

14.4 Referenslitteratur och andra källor

1991
NJA 1991 s. 103

2010
Säkerhetsskyddad upphandling - En vägledning, januari 2010, Säkerhetspolisen
Säkerhetsskydd - En vägledning, juli 2010, Säkerhetspolisen

2011
IT inom statsförvaltningen - har myndigheterna på ett rimligt sätt prövat frågan om outsourcing bidrar till ökad effektivitet? RiR 2011:4, januari 2011, Riksrevisionen
Beslut 574-2011, september 2011, Datainspektionen

2012
A Global Reality - Governmental Access to Data in the Cloud, maj 2012, Hogan Lovells

2013
Against lock-in: building open ICT systems by making better use of standards in public procurement, juni 2013, EU-kommissionen

2014
Beslut 3032-2011, september 2014, Justitieombudsmannen
Informationssäkerheten i den civila statsförvaltningen RiR 2014:23, november 2014, Riksrevisionen

2015
Säkerhetspolisens föreskrifter och allmänna råd om säkerhetsskydd PMFS 2015:3, mars 2015, Säkerhetspolisen
Deutsche Telekom to act as Data Custodian for Microsoft Cloud in Germany, november 2015, T-Systems
Röjandebegreppet enligt offentlighets- och sekretesslagen, december 2015, eSamverkansprogrammet
Molntjänster i staten – en ny generation av outsourcing, december 2015, Pensionsmyndigheten

2016
Outsourcing – en vägledning om sekretess och persondataskydd, februari 2016, eSamverkansprogrammet
Bedömning avseende vilka avtalsvillkor som gäller för Microsofts it-tjänst Office 365 Plan E3 jämte vissa därtill hörande avtalsfrågor, februari 2016, Tillväxtverket
Informationssäkerhetsarbete på nio myndigheter - En andra granskning av informationssäkerhet i staten RiR 2016:8, maj 2016, Riksrevisionen

IT-standarder, inlåsning och konkurrens, Uppdragsforskningsrapport 2016:2, oktober 2016, Konkurrensverket

2017
En gemensam statlig molntjänst för myndigheternas it-drift, februari 2017, Statens servicecenter
10 tips för säkrare outsourcing, april 2017, Säkerhetspolisen
The Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems, oktober 2017, Irish High Court
Beslut 6466-2015, november 2017, Justitieombudsmannen
No. 17-2 – Brief of the European Commission on behalf of the European Union as Amicus Curiae in support of neither party – Supreme Court of the United States, december 2017, EU-kommissionen
Beslut 1947-2016, december 2017, Datainspektionen

2018
Kartlägga hanteringen av vissa uppgifter, januari 2018, Transportstyrelsen
Ett modernt och stärkt skydd för Sveriges säkerhet – ny säkerhetsskyddslag, februari 2018, Regeringens proposition 2017/18:89
Granskning av Transportstyrelsens upphandling av it-drift Ds 2018:6, februari 2018, Näringsdepartementet
Microsoft and Deutsche Telekom's 'German cloud' wafts away, mars 2018, Handelsblatt
Rättsutredning - Frågor om röjande vid användning av molntjänster, mars 2018, SKL
Juridik som stöd för förvaltningens digitalisering, mars 2018, SOU 2018:25
eHälsa och IT i landstingen, maj 2018, SLIT-gruppen
Bedömning av Customer Lockbox, maj 2018, Göteborgs stad
Att tänka på i och med införandet av GDPR och CLOUD Act, juni 2018, Safespring
Annual Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act, juni 2018, Microsoft Corp
Myndigheten för samhällsskydd och beredskaps föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster MSBFS 2018:7, oktober 2018, MSB
Digital Government Review of Sweden, oktober 2018, OECD
Bedömning av Microsofts grundsäkerhetsnivå gällande Office 365, oktober 2018, Göteborgs stad
Rättsligt uttalande om röjande och molntjänster, oktober 2018, eSamverkansprogrammet
Molntjänster – SKL kommenterar eSams rättsliga utlåtande, november 2018, SKL
Myndigheter i USA kan få del av hemliga uppgifter i molnet, november 2018, ST Publikt
DPIA Diagnostic data in Microsoft Office Proplus, november 2018, Dutch Ministry of Justice and Security
Kompletteringar till den nya säkerhetsskyddslagen, november 2018, SOU 2018:82
Upphandla informationssäkert - en vägledning, november 2018, MSB
Report from the Commission to the European Parliament and the Council on the second annual review of the functioning of the EU-U.S. Privacy Shield, december 2018, EU-kommissionen
Molntjänster och säkerhet, december 2018, Microsoft
Annual Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act, december 2018, Alphabet Inc

Offentlighet i det digitala samhället: Vidareutnyttjande, sekretess och dataskydd, 2018, Ledendal, Larsson & Wernberg

2019
Molntjänster tillhandahållna av utländska leverantörer – Presentation för Regeringskansliet, januari 2019, Advokatfirman Kahn Pedersen
EU - U.S. Privacy Shield - Second Annual Joint Review, januari 2019, European Data Protection Board
It-juristen: Stor risk för lagbrott, februari 2019, Dagens samhälle
Säkerhet för personuppgifter i e-post, 2019, Datainspektionen