Office 365 i Danderyds kommun

Diarienummer	Senast uppdaterad	Beslutsinstans	Ansvarig processägare
KS 2019/0296	2019-07-04	Kommunstyrelsen	Kommunledningskontoret - Administrativa avdelningen

Dokumentets syfte

Danderyds kommun har sedan år 2017 använt kontorsstödstjänsten Office 365 som tillhandahålls av den globala molntjänstleverantören Microsoft.

Flera myndighetsuttalanden, med olika innebörd, om lämpligheten att använda molntjänster i offentlig verksamhet har publicerats. Myndighetsuttalandena har dock kulminerat, tvärvänt och i viss mån kuvat diskussionen om lämpligheten att använda molntjänster sedan regelverket Cloud Act infördes år 2018.

Sammantaget har det därför funnits skäl att genomföra denna utredning som syftar till att utgöra ett beslutsunderlag för att Danderyds kommun ska kunna ta ställning till om och i så fall hur Office 365 kan och får nyttjas för sekretessreglerad och sekretessbelagd information samt personuppgifter.

Dokumentet gäller för

Alla kommunens verksamheter som arbetar i eller ska arbeta i Office 365.

Utredningen utgör också underlag för vidare arbete med hur Danderyds kommun ska förhålla sig till molntjänster generellt.

Innehållsförteckning

1. Introduktion

Danderyds kommun har sedan år 2017 använt kontorsstödstjänsten Office 365 som tillhandahålls av den globala molntjänstleverantören Microsoft. Microsoft Sverige AB är avtalspart. I praktiken pågår införandet fortfarande och det pågår diskussioner om att utöka hanteringen av kommuns information i plattformen. Tjänsten ger stora möjligheter till effektivisering av arbete med dokument, kalkyler, e-post och med mera. Till exempel kan flera personer samarbeta i olika digitala samarbetsforum och dokument samtidigt. Jämfört med en mer traditionell lösning där funktionaliteten tillhandahålls inom verksamhetens egen hårdvara och arkitektur ger Office 365 stora fördelar avseende effektivitet. Utöver arbetsverktygen och lagring innefattar tjänsten också de säkerhetsfunktioner som Microsofts samlade kapacitet kan erbjuda.

Bakgrunden till att Office 365 infördes var att både öka effektivisering i medarbetarnas arbete genom förbättrad tillgänglighet till arbetsverktyg, men också för att minska kostnader genom att minska kommunens egna hårdvarumiljö (servrar, personal m.m.) med minst bibehållen säkerhet jämfört med tidigare lösning.

Flera myndighetsuttalanden, med olika innebörd, om lämpligheten att använda molntjänster i offentlig verksamhet har publicerats. Myndighetsuttalandena har dock kulminerat, tvärvänt och i viss mån kuvat diskussionen om lämpligheten att använda molntjänster sedan regelverket Cloud Act infördes år 2018. Uttalandena gäller framförallt lämpligheten att använda molntjänstleverantörer som har sitt säte i USA. De juridiska uttalandena därefter har i princip samstämmigt antingen förespråkat att stor försiktighet ska tas vid användning av molntjänster, eller hävdat att det är rent olämpligt att använda molntjänster med global ägare, i vart fall för lagring av känsliga personuppgifter eller sekretessreglerade uppgifter[1].

Det har genomförts flera utredningar av relevanta aktörer på området i Sverige. Uttalandena är många gånger skrivna utifrån enbart en juridisk aspekt, eller ett dataskyddsperspektiv. Uttalandena innehåller ur ett

[1] Med *sekretessreglade* uppgifter menas uppgift för vilken det finns en bestämmelse om sekretess, jfr. 3 kap. 1 § offentlighets- och sekretesslagen. Vad gäller utlämnandet av uppgifter till en molntjänstleverantör, har någon bedömning av om uppgiften är *sekretessbelagd* (vilket egentligen förutsätts enligt offentlighets- och sekretesslagen) inte gjorts. Därför används båda begreppet sekretessreglerad och sekretessbelagd i denna utredning.

säkerhetsmässigt perspektiv ibland tveksamma beskrivningar av hur den tekniska konstruktionen i molntjänsten faktiskt ser ut. Uttalandena saknar många gånger relevanta källhänvisningar. Denna utredning får konstatera att det, i skrivande stund, verkar saknas en sammanvägd bedömning utifrån samtliga nämnda aspekter:

- Juridik
- Dataskydd
- Informationssäkerhet
- IT-säkerhet

Ett vanligt tema i de tidigare utredningarna är att riskerna belyses kring molntjänstleverantörens möjlighet att komma åt kundens information, då detta ger leverantören åtkomst till sekretessreglerad information utan föregående sekretessprövning. Även andra lösningar än molntjänster innebär oftast att den som administrerar systemet har tillgång till den lagrade informationen, då den administrativa behörigheten som krävs för att utföra service och uppgraderingar också ger en teknisk möjlighet att tillskansa sig behörighet till det som lagras i systemet. En sådan jämförelse mellan vad som gäller för molntjänster i förhållande till vad som gäller för andra alternativ saknas nästan alltid.

Denna utredning har därför riktats mot att belysa möjliga alternativ till informationshantering i Office 365 och underkasta dessa samma juridiska, säkerhetsmässiga och dataskyddsmässiga krav som diskussionen kring användningen av molntjänster har aktualiserat. Det är först vid en sådan jämförelse som det är möjligt att avgöra vilken lösning som bäst lever upp till den totala kravbilden.

I de myndighetsuttalanden som gjorts verkar alternativen till lagring i molntjänster – och de juridiska-, säkerhets- och dataskyddsmässiga förutsättningarna för dessa alternativ – inte alltid beaktas. Det framstår som något förenklat att peka ut brister i användandet av globala molntjänster utan att se till bristerna i de alternativa lösningarna som finns. Denna utredning har utgått ifrån att ingen möjligen skulle förespråka att en myndighet skulle använda ett, genom en sammanvägd bedömning utifrån juridiska-, säkerhets- och dataskyddsmässiga skäl, sämre alternativ än det befintliga Office 365.

Utöver att uttalandena oftast inte beaktat de alternativ som finns tillhands saknas också i viss mån en förståelse för vilka konsekvenser dessa olika uttalanden leder till. Konsekvenserna av att till exempel ta hem information

till egen server är inte bara förenade med stora kostnader, utan medför också en hel del säkerhetsrisker.

Sammantaget har det därför funnits skäl att skriva denna utredning som beslutsunderlag för Danderyds kommuns ställningstagande om Office 365 kan och får fortsätta nyttjas när det kommer till sekretessreglerad och sekretessbelagd information och personuppgifter.

1.1 Utredningens syfte

Denna utredning har alltså till syfte att utreda *om* och i så fall hur molntjänsten Office 365 kan och får nyttjas för sekretessreglerad och sekretessbelagd[2] information och personuppgifter. Främst kommer nedanstående frågeställningar avhandlas och besvaras:

1. Finns betänkligheter utifrån offentlighets- och sekretesslagen att lagra information i en molntjänst?
    a. har kommunen stöd för utlämnande av sekretessreglerade uppgifter till Office 365 och Microsoft?
    b. utgör utlämnandet annars ett röjande av sekretessbelagda uppgifter[3]?
    c. utgör Cloud Act och liknande regelverk att utlämnandet utgör ett röjande?
2. Finns betänkligheter utifrån ett dataskyddsperspektiv?
    a. vilka krav ställer lagstiftningen på personuppgiftsbehandling generellt och biträdets hantering specifikt?
    b. finns några hinder för tredjelandsöverföring?
    c. hur påverkar Cloud Act?
3. Är Microsofts grundsäkerhetsnivå tillräcklig för att skydda informationen som ska lagras i molntjänsten?
4. Om svaret på fråga 3 är jakande;
    a. nyttjar Danderyds kommun en relevant uppsättning säkerhetslösningar för detta och
    b. tillämpas säkerhetslösningarna enligt punkt 3?

[2] Med undantag för sådana uppgifter som rör Sveriges säkerhet eller mellanfolkliga förbindelser.

[3] Med s*ekretessbelagd* uppgift menas en *sekretessreglerad* uppgift för vilken sekretessen gäller i enskilt fall, jfr. 3 kap. 1 § offentlighets- och sekretesslagen. Vad gäller utlämnandet av uppgifter till en molntjänstleverantör, har någon bedömning av om uppgiften är sekretessbelagd (vilket egentligen förutsätts enligt offentlighets- och sekretesslagen) inte gjorts. Därför används båda begreppet sekretessreglerad som sekretessbelagd i denna utredning.

Notera att Office 365 inte har bedömts utifrån ett arkivperspektiv då systemet *inte* är avsett för slutlig lagring och arkivering inom Danderyds kommun.

1.2 Informationssäkerhet i Danderyds kommun

I anslutning till arbetet med utredningen om Office 365 pågår ett arbete med att införa informationsklassificeringsrutiner i Danderyds kommun där all information kommunen hanterar delas upp i följande säkerhetsklasser:

- **ÖPPEN** - innehåller information som inte innehåller personuppgifter eller information som är sekretessreglerad och sekretessbelagd. Hit hör också information som efter en sekretess- och menprövning kan lämnas ut utan förbehåll.
- **INTERN** - innehåller information som kan innehålla uppgifter som omfattas av svag sekretess och personuppgifter (inte känsliga personuppgifter). Med svag sekretess menas att uppgiften som huvudregel är offentlig, men att uppgiften endast är sekretessbelagd om den anses kunna leda till skada eller men.
- **KÄNSLIG** – innehåller information som kan innehålla uppgifter som omfattas av stark sekretess, absolut sekretess eller känsliga personuppgifter. Med stark sekretess menas att uppgiften som huvudregel är sekretess och att uppgiften endast kan lämnas ut om det är klart att informationen inte leder till skada eller men. Med absolut sekretess menas att informationen är sekretess oavsett om den leder till men eller skada.
- **HEMLIG** - innehåller uppgifter om Sveriges säkerhet, bland annat sådana uppgifter som regleras i säkerhetsskyddslagen och säkerhetsskyddsförordningen.

Syftet med att införa klassificering är att en starkare säkerhetslösning i Office 365 ska kunna aktiveras för känslig information och som gör det möjligt att klassa dokument beroende på handlingens innehåll, men också att säkerställa att informationsmängdernas konfidentialitet är bedömd redan vid upprättandet. Känslig information ska få ett korrekt skydd från början.

Även om klassificering används för olika handlingstyper (öppen, intern, känslig och hemlig), kan vissa svårigheter uppstå. Till exempel kan en handling som innehåller personuppgifter om facklig tillhörighet vara klassificerad som känslig utifrån ett personuppgiftsperspektiv. Samma uppgift är dock offentlig och saknar helt grund för sekretess enligt offentlighets- och sekretesslagen. Klassificeringen sker också på förhand

trots att handlingens klassificering skulle kunna ändra klass under arbetets gång. Office 365 ger dock möjlighet att ändra klassificering och tillgänglighet i takt med att en informationsmängd skiftar i skyddsvärde.

Denna utredning behandlar, som nämnts, inte hemlig information[4] eftersom sådan information inte är lämplig att bearbeta eller lagra i fleranvändarsystem. Information som klassificeras som hemlig ska inte hanteras i en molntjänst. Däremot kan vissa överväganden komma att ställas i relation till tillämpningen av säkerhetsskyddslagen kring bland annat röjandeproblematik och ”behörighetsbegreppet” där så är relevant i utredningen.

2 Bakgrund

En arbetsgrupp bestående av kommunens dataskyddsombud, säkerhetschef, kommunjurist och en representant för digitaliserings- och utvecklingsenheten har genomfört denna utredning. Representationen i arbetsgruppen har syftat till att utifrån de olika specialistkompetenserna sammantaget belysa de frågor och risker som uppkommer vid användningen av Office 365 främst kopplat till hantering av känsliga personuppgifter, sekretessreglerad och sekretessbelagd information.

> *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 gruppens förtroende och agerande gentemot myndigheter i stort.*[5]

En viktig slutsats som framkommit i det inledande arbetet är att öppen information kan hanteras[6] i Office 365 utifrån alla bedömda perspektiv (legala såväl som säkerhetsmässiga). Utredningen koncentreras därför främst till fortsatt hantering av handlingar som bedöms innehålla personuppgifter, sekretessreglerade och sekretessbelagda uppgifter med tillhörande frågeställningar kring röjandeproblematiken av sekretess, dataskyddslagstiftningen och den adekvata säkerhetsnivån.

Den inledande analysen har identifierat flera komplexa problemområden. Dataskyddslagstiftningen har till syfte att reglera säker och laglig

[4] I detta sammanhang nyttjas begreppet ”hemlig” för samtliga informationsklasser som omfattas av säkerhetsskyddslagen.

[5] Kammarkollegiets Förstudierapport Webbaserat kontorsstöd dnr. 23.2-6283-18, den 22 februari 2019 s. 29.

[6] Med hanteras avses här arbetsmaterial eftersom Office 365 inte är avsett att användas för långsiktig eller permanent lagring (arkivering).

behandling av personuppgifter. Offentlighets- och sekretesslagen innehåller bestämmelser om sekretess och *förbjuder* röjande av sekretessbelagda uppgifter. Lagarna är aktuella när det gäller bedömningen av Office 365. I och med att lagarna har olika syften och ändamål i förhållande till varandra uppstår otydligheter när regelverken i viss mån ska appliceras samtidigt och även delvis ska ställas mot varandra. En hantering som är förenlig med dataskyddslagstiftningen kan t.ex. vara oförenlig med offentlighets- och sekretesslagen och vise versa. Vad gäller Office 365 har också säkerheten i hanteringen av informationen haft en väsentlig roll, vilket kan leda till ytterligare problematik. En hantering av handlingar som ur ett säkerhetsperspektiv är bra kan vara oförenlig med offentlighets- och sekretesslagen eller dataskyddslagstiftningen. Det är olyckligt att myndigheter lämnas att enskilt reda ut hur bestämmelserna ska förhålla sig till varandra.

2.1 Vilken information hanteras i Office 365?

En naturlig fråga kommunen måste ställa sig är vilken information som hanteras i Office 365? Svaret är dock inte helt enkelt. På samma sätt som det är svårt att överblicka vad som ligger på kommunens filservrar är det svårt att överblicka vad som hanteras i Office 365. Dock finns möjligheter att i Office 365 att skapa viss överblick genom att använda det klassificeringsverktyg som tjänsten erbjuder. Allt som hanteras i e-post, Word och Excel t.ex. hanteras i Office 365. Även om kommunen till del kan reglera vad som skrivs i e-post som skickas från eller inom kommunen, har kommunen inga möjligheter att reglera vad allmänheten skickar in med e-post till kommunen.

Då e-posthantering, att skicka och motta e-post, har blivit en förutsättning för att kunna utföra arbetsuppgifter i kommunen oavsett dess slag, hanteras helt säkert sekretessreglerade och sekretessbelagda uppgifter samt personuppgifter i Office 365 i viss mån. Det går dock inte att säga med säkerhet hur stor del av informationsinnehållet i Office 365 som består av sekretessreglerade uppgifter och personuppgifter. Vissa uppgifter kan dessutom under viss tid vara sekretessreglerade för att i ett senare skede inte vara det (till exempel upphandlingsinformation)

Notera att även e-post, Word- och Exceldokument som raderas av användare finns kvar i en tid Office 365, beroende på Microsofts säkerhetskopieringsrutiner.

Genom konstaterandet att känsliga uppgifter (sekretessreglerade, sekretessbelagda och känsliga personuppgifter) förkommer i plattformen bör fokus läggas på att i största möjliga mån skydda kommunens information från obehörig åtkomst.

2.2 Relevanta uttalanden av myndigheter och organisationer

Under genomförandet av denna utredning har olika myndigheter och i sammanhanget relevanta organisationer publicerat uttalanden om globala molntjänster kopplat till både tjänsternas säkerhet och legala aspekter kring dem.

Kammarkollegiet utkom den 22 februari 2019 med en förstudierapport om Webbaserat kontorsstöd. Kammarkollegiet underkände, för statens räkning, marknadens samtliga molntjänsteleverantörer av olika skäl, och anförde följande.

> *[Ett] 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****.*[7]

Sveriges Kommuner och Landsting (SKL) utkom den 12 april 2019 med följande ställningstagande om informationshantering i vissa molntjänster:

> *SKL rekommenderar kommuner och regioner som redan använder denna typ av molntjänster med utländskt ägande, även för information som omfattas av sekretess, att fokusera på* ***säkerhetsåtgärder och riskreducering inom rätt område och i de fall det bedöms nödvändigt återta informationshanteringen.***[8]

Uttalandena skapar en tydlig bild av att myndigheter generellt verkar avrådas från att använda molntjänster. Denna utredning ska titta närmare på flera uttalanden som gjorts. Dessa uttalanden presenteras inledningsvis för att klargöra vikten av att denna utredning, vad gäller Danderyds kommuns molntjänster kommer till stånd. Påståendena kan få påverkan på Danderyds arbete med digitala tjänster, men avgör inte nödvändigtvis frågan om Danderyd har möjlighet eller råd att dra samma slutsatser.

[7] Kammarkollegiets Förstudierapport Webbaserat kontorsstöd dnr. 23.2-6283-18, den 22 februari 2019 s. 57.

[8] Sveriges Kommuner och Landsting, *Ställningstagande om informationshantering i vissa molntjänster*, ärendenr. 19/00087, den 12 april 2019.

2.3 Schabloniserade bedömningar

När en kommuns dokumentproduktion sköts i Office 365 lagras och hanteras ett brett spektrum av olika typer av data i molntjänsten. Både offentlighets- och sekretesslagen samt dataskyddslagstiftningen har avsett att en prövning ska avgöras utifrån en faktisk handling och en faktisk uppgift. Inget av regelverken har avsett att sekretessreglerade uppgifter och personuppgifter ska hanteras genom schabloniserade bedömningar på förhand. Vid användandet av molntjänster blir likväl schabloniserade bedömningar nödvändiga eftersom det rör sig om lagring av stora mängder information. Detta är viktigt att beakta att regelverken i viss mån forceras på detta sätt på dess tillämpning vid lagring i molntjänster.

3 Offentlighets- och sekretesslagen kontra Office 365

Av 3 kap. 1 § offentlighets- och sekretesslagen (2009:400) framgår att sekretess utgör ett förbud att röja en uppgift vare sig det sker muntligen, genom utlämnande av allmän handling eller på något annat sätt.

Dokument i Word och Excel samt e-post som innehåller sekretessreglerade och sekretessbelagda uppgifter sparas kontinuerligt i Office 365 i Danderyds kommun. Office 365 ägs av det amerikanska bolaget Microsoft. Offentlighets- och sekretesslagen gäller bara myndigheter och dess anställda, Microsofts personal omfattas alltså inte av offentlighets- och sekretesslagen.[9]

Även om avsikten inte är att Microsoft ska ta del av handlingarna som sparas i Office 365, lämnas handlingarna ändock ut från kommunen till Office 365 och Microsoft när till exempel ett Word-dokument sparas eller en e-post skickas. Både e-post och Word-dokument kan innehålla sekretessreglerad och sekretessbelagd information, vilket också gäller för övriga tjänster inom Office 365.

Under detta avsnitt kommer utredas om kommunen har stöd för utlämnandet av sekretessreglerade och sekretessbelagda handlingar till Office 365 och Microsoft. Det finns olika uppfattning om i vilken utsträckning Microsoft kommer åt eller tar del av informationen som sparas i Office 365.

[9] Jfr. 2 kap. 1 § offentlighets- och sekretesslagen.

Att kommunens lagring i Office 365 medför att Microsoft kommer åt informationen och därför också utgör ett utlämnande av handlingar baseras framförallt på fyra faktorer enligt följande.

- Microsoft kommer åt kommunens data som lagras i Office 365 och har möjlighet att söka i informationen. Hur stor del av informationen i Office 365 som Microsoft kommer åt eller faktiskt tar del av är ofta uppe för diskussion.
- Microsofts supporttekniker kommer åt kommunens data när de vidtar support. Detta belyses ytterligare under kapitel 4, utifrån vad som gäller om supporten sitter i ett s.k. tredje land och ur ett dataskyddsperspektiv. Detta belyses under avsnitt 5.13 om Customer Lockbox för att begränsa och reglera supportens behörighet till kommunens data.
- Microsofts administrativa behörigheter kommer alltid komma åt innehållet (detta är i princip är en förutsättning för Microsoft för att kunna tillhandahålla en användarduglig tjänst[10]), oavsett om funktioner som Customer Lockbox används.
- Regelverk som Cloud Act *med flera*, medför att kommunens data som lagrats i Office 365 kan komma att utlämnas av Microsoft till utländska myndigheter. Detta kommer diskuteras mer ingående under avsnitt 3.3 och 4.

Danderyds kommun måste ha stöd för utlämnande av sekretessbelagda uppgifter till Office 365 och Microsoft. Det är förenat med straffansvar att röja sekretessbelagda uppgifter. Den som röjer en uppgift som denne är skyldig att hemlighålla kan dömas till *brott mot tystnadsplikten* i enlighet med 20 kap. 3 § brottsbalken (1962:700). Påföljden för gärningen är böter eller fängelse i högst ett år. Personen kan också göra sig skyldig till *tjänstefel* genom att åsidosätta vad som gäller för uppgiften enligt 20 kap. 1 § brottsbalken. Påföljden för detta är böter till fängelse vid grovt brott i högst sex år.

Microsoft är en extern part och lyder inte under offentlighets och sekretesslagen och straffsanktionerade regler om tystnadsplikt, vilket

[10] Microsoft erbjuder ett alternativ till detta som innebär att Microsofts administrativa behörigheter inte kommer åt kommunens data, men användardugligheten i Office 365 begränsas därmed också så kraftigt att Office 365 blir svårt att använda. Denna utredning har gjort bedömningen, på grund av den bristande användardugligheten, att detta alternativ inte är ett tänkbart alternativ för Danderyds kommun.

kommunens personal gör. Detta kan också påverka lämpligheten i att använda molntjänster.

Frågan, om kommunen har stöd för utlämnande av sekretessreglerade och sekretessbelagda uppgifter när kommunen sparar sådana uppgifter i Office 365, kommer att delas upp i tre delar enligt följande.

- Har kommunen stöd för utlämnande av sekretessbelagda uppgifter till Office 365 och Microsoft?
- I annat fall, utgör utlämnandet då ett röjande av sekretessbelagda uppgifter?
- Medför Cloud Act och andra liknande regelverk att utlämnandet utgör ett röjande av sekretessbelagda uppgifter?

För att ta sig an frågeställningarna kommer utredningen att blanda referat ur förarbeten och myndighetsuttalanden (vilka inte sällan är oförenliga med varandra) för att påvisa frågans komplexitet och för att påvisa hur spretigt rättsläget är. Utredningen kommer däremellan redovisa utredningens egna ställningstaganden.

Det finns en hierarki för rättskällor, som det kan vara bra att ha med sig under läsningens gång enligt följande.

1. Tyngst väger lagtexten.
2. Därefter, väger förarbeten och motivuttalanden tyngst.
3. Därefter, väger domstolsavgöranden tyngst.
4. Slutligen, går det att se till doktrinen (litteraturen).

Det medför till exempel att om förarbeten har en ståndpunkt, väger den tyngre än ett rättsfall som har en annan ståndpunkt. Senare daterade uttalanden väger tyngre än tidigare uttalanden inom samma kategori.

Avsnitten avslutas var för sig med en sammanfattning.

3.1 Har kommunen stöd för utlämnande av sekretessbelagda uppgifter till Office 365 och Microsoft?

3.1.1 Sekretessbelagd uppgift får inte röjas (8 kap. 1 §)

När informationen i en handling är sekretessbelagd begränsas enskilda och myndigheters rätt att ta del av handlingen.

Av 8 kap. 1 § offentlighets- och sekretesslagen framgår att en uppgift för vilken sekretess gäller enligt offentlighets- och sekretesslagen inte får röjas

för enskilda eller för andra myndigheter, om inte annat anges i denna lag eller i lag/förordning som denna lag hänvisar till.

Av förarbetena om förslag till sekretesslag framgår följande.

> *Uppgift får inte heller röjas genom att en befattningshavare lämnar information muntligen eller på annat sätt. Innebörden härav är att befattningshavaren inte får* ***låta någon ta del av*** *hemlig uppgift vare sig detta sker genom att allmän handling företes eller att någon får ta del av handling som inte är allmän eller att uppgiften meddelas i brev. Också andra former för röjande av en uppgift kan tänkas, t.ex. att någon förevisar ett hemligt föremål för annan. Bestämmelsen avser alltså varje form av röjande. Det är också utan betydelse om uppgiften före röjandet är dokumenterad eller inte. Inte heller spelar det någon roll om uppgift lämnas ut på begäran av utomstående eller efter initiativ av den som har uppgiften om hand.*[11]

Utredningen gör bedömningen att det utifrån förarbetena framstår som att det är själva tillhandahållandet av uppgiften som är det centrala, och inte huruvida någon faktiskt tillgodogör sig innehållet. Vad gäller molntjänster skulle det medföra att uppgifterna röjs om de sparas i en molntjänst, oavsett om molntjänstleverantören eller någon annan tar del av den.

3.1.2 Lagring för teknisk bearbetning (40 kap. 5 §)

Av 40 kap. 5 § offentlighets- och sekretesslagen framgår att sekretess gäller i verksamhet för enbart teknisk bearbetning eller teknisk lagring för någon annans räkning för uppgift om en enskilds personliga eller ekonomiska förhållanden. Utredningen noterar att bestämmelsen endast gäller för myndigheter och myndighetens personal.[12] Bestämmelsen gäller inte för en extern part som Microsoft. Det går alltså inte att med stöd av 40 kap. 5 § offentlighets- och sekretesslagen finna grund för lagring av sekretessbelagda uppgifter i Office 365.

3.1.3 Kan utlämnandet ske med förbehåll? (10 kap. 14 §)

Det framkommer i 10 kap. 14 § offentlighets- och sekretesslagen att om en myndighet finner att sådan risk för skada, men eller annan olägenhet som enligt en bestämmelse om sekretess hindrar att en uppgift lämnas till en enskild, kan undanröjas genom ett *förbehåll* som inskränker den enskildes rätt att lämna uppgiften vidare eller utnyttja den, ska myndigheten göra ett sådant förbehåll när uppgiften lämnas till den enskilde.

Bestämmelsen väcker frågan, om det går att lämna ut sekretessreglerade och sekretessbelagda uppgifter till Office 365 och Microsoft, genom att utlämna

[11] Prop. 1979/80:2 Del A s. 119-120.

[12] 2 kap. 1 § offentlighets- och sekretesslagen

uppgifterna med förbehåll om att Microsoft inte får lämna uppgiften vidare eller utnyttja uppgifterna?

Justitieombudsmannen har uttalat sig och menat att ett förbehåll inte kan meddelas i förväg utan ska prövas utifrån varje aktuell uppgift, samt att de inte finns utrymme för att meddela generella förbehåll.[13]

Denna utredning kommer fram till att det inte går att genom ett generellt förbehåll, på förväg, lämna ut sekretessbelagda uppgifter till Office 365 och Microsoft.

3.1.4 Är utlämnandet nödvändigt? (10 kap. 2 §)

I 10 kap. 2 § offentlighets- och sekretesslagen finns bestämmelser om sekretessbrytande bestämmelser som medför att en uppgift som är sekretess ändå kan få lämnas ut till enskild, eller till en annan myndighet, om det är *nödvändigt* för att den utlämnande myndigheten *ska kunna fullgöra sin verksamhet*.

Det finns olika uppfattning om vad som krävs för att något ska vara *nödvändigt*, och om ett utlämnande till molntjänstleverantör ens kan vara nödvändigt för en myndighet.

I förarbetena förespråkas en restriktiv hållning och i prop. 1979/80 del A stadgas följande om när det skulle kunna vara nödvändigt för en myndighet att utlämna handlingar.

> *En myndighet kan t.ex. se sig tvungen att ge en annan myndighet del av hemlig information till grund för ett remissyttrande. […] Delgivning med part och annan föreskriven underrättelse till enskild som ett led i behandlingen av ett ärende hör hit. I särskilda fall kan det vidare vara nödvändigt för en tjänsteman att vända sig till en utomstående expert och att därvid upplysa om hemliga omständigheter.*[14]
>
> *Endast i de fall, då det för fullgörandet av ett visst åliggande som en myndighet har är en* ***nödvändig förutsättning att en sekretessbelagd uppgift får lämnas ut, får sekretessen efterges. Blott och bart en bedömning att effektiviteten i myndighetens handlande nedsätts genom en föreskriven sekretess får inte till att sekretessen åsidosätts****.*[15]

Det är alltså inte tillräckligt att effektiviteten i kommunens arbete ökar, för att ett utlämnande ska anses som nödvändigt. Att delgivning till part (vilket

[13] JO 1992/93 s. 197, dnr 145–1990.

[14] Prop. 1979/80:2 del A s. 122.

[15] Prop. 1979/80:2 del A s. 465.

i regel måste ske innan myndigheten kan ta beslut) ges som ett exempel när ett utlämnande får ske, talar för en väldigt restriktiv hållning.

Även Justitieombudsmannen har uttryckt att bestämmelsen ska tolkas restriktivt i ett ärende om läkarsekreterare som kommer hanteras senare i dokumentet. Justitieombudsmannen anförde.

> *Syftet med bestämmelsen är att förhindra att sekretessregleringen gör det omöjligt för en myndighet och dess personal att sköta de uppgifter som myndigheten har ansvar för. Sekretessen får efterges bara i sådana fall då ett utlämnande av sekretessbelagda uppgifter är en nödvändig förutsättning för att myndigheten ska kunna fullgöra ett visst åtagande (se Offentlighets- och sekretesslagen, Zeteo, 1 juli 2013, kommentaren till 10 kap. 2 § OSL, se även Jesper Ekroths och Therése Fridström Montoyas artikel i FT 2008 s. 153). […] Utgångspunkten är alltså att bestämmelsen ska tillämpas restriktivt. I praktiken handlar det om situationer av undantagskaraktär.*[16]

Justitieombudsmannen har i ett annat ärende, funnit att det varit nödvändigt för skattemyndigheterna att lämna ut sekretessbelagda uppgifter (deklaration, kontrolluppgifter och arbetsgivaruppgifter) till ett privat dataföretag för registrering. I ärendet hade skattemyndigheterna och det privata dataföretaget avtalat om tystnadsplikt. Justitieombudsmannen anförde följande.

> *Jag ser för min del inga avgörande invändningar mot den ordning som sålunda kommit till användning […]. Den fråga som jag ställde i inledningen* ***– är det lagligt att lämna sekretessbelagda handlingar till privata servicebyråer för registrering? – är jag alltså beredd att svara ”ja” på under förutsättningen att åtgärden verkligen är nödvändig****.*[17]

eSam, som är en samverkansgrupp mellan 23 myndigheter och Sveriges Kommuner och Landsting för att underlätta och påskynda digitaliseringen av det offentliga Sverige[18], har i sin rapport *Outsourcing - en vägledning i sekretess och persondataskydd*, funnit att det kan vara nödvändigt för en myndighet att lämna ut uppgifter för teknisk bearbetning och lagring enligt följande.

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

[16] JO den 9 september 2014, dnr. 3032–2011, s. 18–19.

[17] JO den 11 mars 1982, dnr. 149–1980 s. 240.

[18] http://esamverka.se/, den 18 mars 2019 kl. 09.38.

> *av rekryteringskonsulter och upphandlingsexperter. Det kan enligt eSams bedömning också finnas flera situationer då det måste anses vara ”nödvändigt” för en myndighet att vända sig till en utomstående aktör för att dra nytta av dennes tekniska utrustning.* ***Framför allt kan detta visa sig vara aktuellt vid åtgärder för teknisk bearbetning och teknisk lagring av myndighetsinformation, såsom storskalig skanning av dokument, tryckeriverksamhet, IT-drift och e-arkivering samt funktioner för t.ex. elektronisk legitimering, elektroniska underskrifter och stöd mot intrång och andra angrepp i myndighetens IT-miljö****.*[19]

Även E-delegationen, som fått i uppdrag av regeringen att samordna myndigheternas IT-baserade utvecklingsprojekt och skapa goda förutsättningar för myndighetsövergripande samordning, har i sitt slutbetänkande *En förvaltning som håller ihop*, öppnat upp för att bestämmelsen skulle kunna användas för ett utlämnande till molntjänstleverantör, enligt följande.

> *Även om bestämmelsen ska tillämpas restriktivt är vår bedömning att avsikten inte har varit att den ska tillämpas endast i situationer av undantagskaraktär. I linje med förarbetenas konkreta exempel på situationer då bestämmelsen kan tillämpas anser vi att ett tillgängliggörande av uppgifter i samband med sådan outsourcing som sker i syfte att dra nytta av utförarens expertkompetens eller tekniska utrustning, i särskilda fall bör anses utgöra ett nödvändigt utlämnande och därmed vara tillåtet.* ***Den sekretessbrytande bestämmelsen om nödvändigt utlämnande bör alltså under vissa omständigheter kunna tillämpas vid outsourcing av teknisk bearbetning eller teknisk lagring,*** *såsom IT-drift eller vissa dokumenthanteringstjänster, samt tekniska hjälptjänster t.ex. avseende it-support.*

Digitaliseringsrättsutredningen som skrivit betänkandet *Juridik som stöd för förvaltningens digitalisering* menar att en sådan tolkning som E-delegationen gjort ovan, är alltför långtgående. Digitaliserings-rättsutredningen anför följande.

> *Det är angeläget att uppgifter som lämnas ut i samband med utkontraktering får samma skydd hos leverantören som hos den utkontrakterande myndigheten.* ***För det fall att uppgifterna lämnas ut till en privat leverantör med stöd av t.ex. bestämmelsen om nödvändigt utlämnande i 10 kap. 2 § offentlighets- och sekretesslagen får uppgifterna i dag inte det skydd hos leverantören som uppgifterna hade fått om personalen omfattats av en straffsanktionerad tystnadsplikt****. Detta medför att det finns en viss risk för bristande sekretesskydd.** *Integritetskänsliga och sekretessreglerade uppgifter som utkontrakteras bör enligt oss utan tvekan ha samma sekretesskydd oavsett om uppgifterna förekommer i uppdragsgivarens verksamhet som omfattas av offentlighets- och sekretesslagen eller i leverantörens verksamhet som inte omfattas av den lagen. På grund av det anförda, och mot bakgrund av den ur bl.a. effektivitetssynpunkt påkallade utkontrakteringen av IT-drift och andra IT-baserade funktioner till privata leverantörer, finns det enligt vår bedömning* ***behov av en författningsreglerad tystnadsplikt för de som är verksamma hos privata leverantörer****. En författningsreglerad tystnadsplikt*

[19] Outsourcing – en vägledning och persondataskydd, eSam, januari 2016, s. 27.

> *kommer enligt utredningens mening att skapa en långsiktigt hållbar rättslig reglering som ger stöd för den offentliga sektorns digitalisering.*[20]
>
> *I våra kontakter med myndigheter med anledning av kartläggningsarbetet framkommer att det finns en* ***betydande tveksamhet inför att lämna ut uppgifter till privata leverantörer*** *med stöd av den aktuella bestämmelsen. Det bör även framhållas att uppgifter som lämnas ut med stöd av bestämmelsen inte heller får samma skydd hos leverantören, eftersom de medarbetare hos leverantörerna som tar del av uppgifterna inte omfattas av en författningsreglerad tystnadsplikt.*[21]

Sammantaget finns utlåtanden från Justitieombudsmannen, eSam och E-delegationen som talar för att det kan vara *nödvändigt* att lämna ut uppgifter till en molntjänstleverantör (det finns då stöd i 10 kap. 2 § offentlighets- och sekretesslagen för att lämna ut sekretessbelagda uppgifter till molntjänstleverantören). Det finns samtidigt förarbeten, vilka backas upp av Digitaliseringsrättsutredningen och Justitieombudsmannen, som talar för att endast effektivisering inte är tillräckligt, utan att det verkligen ska vara *nödvändigt* att uppgiften lämnas ut för att myndigheten ska kunna *fullgöra sin verksamhet*.

Det här innebär att kommunen måste finna att det är nödvändigt att lämna ut uppgifterna till Office 365 och Microsoft – i princip att kommun inte har några andra alternativ än en molntjänstlösning – för att kunna fullgöra sin verksamhet. I annat fall saknar kommunen grund för utlämnande av sekretessbelagda uppgifter till Office 365 och Microsoft.

3.1.5 Sammanfattning

Denna utredning har utrett om kommunen har stöd för utlämnandet av sekretessreglerade och sekretessbelagda uppgifter till Office 365 och Microsoft. Denna utredning har funnit att kommunen måste finna att 10 kap. 2 § offentlighets- och sekretesslagen är tillämplig, och att det är *nödvändigt* för kommunen att lämna ut dessa uppgifter till Office 365 och Microsoft, för att stöd ska finnas för utlämnandet. I förarbetena och av flera instanser förespråkas dock en restriktiv hållning. Utredningen får notera att det föreligger olika uppfattning om det kan anses vara *nödvändigt* att lämna ut uppgifter till en molntjänstleverantör.

Vidare diskussion om detta kommer föras under avsnitt 6.

[20] SOU 2018:25 s. 364-365.

[21] SOU 2018:25 s. 365.

3.2 I annat fall, utgör utlämnandet då ett röjande av sekretessbelagda uppgifter?

3.2.1 Röjande av sekretessbelagda uppgifter

I sådana fall 10 kap. 2 § offentlighets- och sekretesslagen inte är tillämplig, måste frågan ställas om kommunen röjer sekretessbelagda uppgifter på ett otillåtet sätt när uppgifterna sparas i Office 365.

E-delegationen som skrivit slutbetänkandet *En förvaltning som håller ihop* och anför följande.

> *Enligt vår uppfattning bör det i vart **fall inte betraktas som ett röjande i offentlighets och sekretesslagens mening** om en hemlig uppgift har gjorts tillgängliga för en utomstående på ett sådant sätt att det förefaller **osannolikt att mottagaren tar del av uppgifterna**. **Vid outsourcing av exempelvis IT-drift skulle en sådan situation kunna föreligga om tjänsteavtalet har försetts med ett tydligt förbud för leverantören och dennes personal att ta del av den information som hanteras i systemen**. Detta ställer krav på kontrollmekanismer såsom loggning och kännbara civilrättsliga sanktioner vid överträdelser.*[22]

eSam har vidare uttalat följande.

> *Vid utkontraktering av t.ex. IT-drift är avsikten med att uppgifter görs tillgängliga för utföraren inte att denne ska tillgodogöra sig informationsinnehållet. Syftet är istället enbart att utföraren ska **tekniskt bearbeta eller lagra själva informationsmassan**. Enligt expertgruppens bedömning bör det i en sådan situation **inte anses utgöra ett röjande** i offentlighets- och sekretesslagens mening, om tjänsteleverantören och dennes personal inte får ta del av eller vidarebefordra uppgifterna och omständigheterna i övrigt medför att det är **osannolikt** att så sker.*[23]

Sammanfattningsvis verkar uttalandena ge stöd för att det inte utgör ett röjande av sekretessbelagda uppgifter att hantera sekretessbelagda uppgifter i en molntjänst. Utredningen konstaterar att eSam och E-delegationen menar att utlämnandet till Office 365 och Microsoft inte skulle utgöra ett röjande om det antingen finns ett tydligt förbud för leverantören att ta del av informationen, eller det är osannolikt att så sker.

Vad gäller Office 365 har personalen hos Microsoft möjlighet t.ex. i samband med support att ta del av kommunens data. Microsoft har alltid administrativa behörigheter som kommer åt data. Detta kan tala för att de

---

[22] SOU 2015:66, slutbetänkande av E-delegationen, *En förvaltning som håller ihop*, s. 47.

[23] eSams rättsliga uttalande den 17 december 2015, dnr. VER 2015-190. eSam har senare kommit med ett nytt uttalande vad som gäller när molntjänstleverantören kan tvingas följa utländsk lag.

sekretessreglerade och sekretessbelagda uppgifterna i Office 365 ändå skulle kunna anses vara röjda.

Utredningen får notera att uttalandena skett innan Cloud Act och andra liknande regelverk trädde i kraft. eSam har senare kommit med ett nytt reviderat uttalande.

3.2.2 Röjande endast om det går att räkna med att någon obehörig tar del av uppgifterna?

I NJA 1991 s. 103 – som kan vara vägledande[24] vid tillämpning av offentlighets- och sekretesslagen och brott mot tystnadsplikten (20 kap. 3 § offentlighets- och sekretesslagen) – prövades frågan om det straffrättsliga ansvaret för v*årdslöshet med hemlig uppgift* enligt 19 kap. 9 § brottsbalken.

Notera att det finns en viss skillnad för vad som är tillåtet enligt offentlighets- och sekretesslagen, och området där straffansvar inträder.[25]

Notera också att det krävs att någon är *grovt oaktsam* för att kunna dömas för vårdslöshet med hemlig uppgift (vilket rättsfallen nedan avser), men att det endast krävs att någon är *oaktsam*, vilket är ett lägre krav, för att kunna dömas för brott mot tystnadsplikten, 20 kap. 3 § brottsbalken.

Vid ett inbrott hade en gärningsman utan svårigheter kunnat öppna ett säkerhetsskåp innehållande två pärmar med hemliga handlingar om rikets militära försvar. Det var inte utrett om gärningsmannen verkligen läst de hemliga handlingarna. Frågan var om säkerhetscheferna av grov oaktsamhet – genom att förvara reservnycklarna till skåpet i ett enkelt träskåp och inte enligt säkerhetsföreskrifterna – röjt de hemliga handlingarna. Krävdes det att någon obehörig *fått del av* uppgiften för att det skulle utgöra ett *röjande* av sekretessbelagda handlingar? Högsta domstolen anförde följande.

> *Uttrycket "röjer uppgift" i bestämmelsen[26] innebär enligt vanligt språkbruk att en uppgift avslöjas eller uppenbaras. Detta förutsätter att det finns någon person, för vilken uppgiften görs tillgänglig. Det torde dock inte alltid kunna krävas att denne faktiskt har fått kännedom om uppgiften. Det bör sålunda*

[24] Lenberg, Geijer och Tansjö, Zeteo lagkommentaren till 3 kap. 1 § offentlighets- och sekretesslagen, publicerad den 9 januari 2019; samt SOU 2015:66 s. 48 vad gäller att ett liknande resonemang också borde kunna föras vad gäller bestämmelser i offentlighets- och sekretesslagen.

[25] Prop. 1979/80:2 del A s. 85.

[26] Utredningens anmärkning: Uttrycket *röjer någon uppgift* återfinns i brott mot tystnadsplikten, 20 kap. 3 § brottsbalken, och uttrycket *en uppgift för vilken sekretess gäller enligt denna lag får inte röjas* förekommer i 8 kap. 1 och 3 §§ offentlighets- och sekretesslagen.

> *som regel vara tillräckligt att en handling med hemliga uppgifter har kommit i någon obehörigs besittning. Även vissa andra, närliggande situationer bör omfattas. Däremot kan inte varje möjlighet att ta del av en uppgift, som har beretts någon obehörig, medföra att uppgiften ska anses ha röjts; en sådan ordning skulle i realiteten innebära att det oaktsamma handlandet i sig ofta skulle medföra straffansvar. Avgörande för straffansvar bör främst vara om uppgiften har blivit tillgänglig för någon obehörig under sådana omständigheter, att man* ***måste räkna med*** *att den obehörige kommer att ta del av uppgiften.*

Åtalet ogillades.

Det får återigen poängteras att det för vårdslöshet med hemlig uppgift, krävs att någon är *grovt oaktsam*, vilket medför att Högsta domstolen givetvis ställer ett högre krav på den oaktsamma gärningen för att straffansvar ska kunna utgå. Det medför, att även om domen kan vara vägledande för brott mot tystnadsplikten[27], är det inte helt självklart att den är direkt tillämplig för att utreda huruvida ett *oaktsamt* beteende utgör brott mot tystnadsplikten.

Även om det finns en viss skillnad mellan att inte förvara nycklar enligt säkerhetsföreskrifterna i ett enskilt fall, och att kontinuerligt spara sekretessbelagd information i en molntjänst finns visst stöd, i NJA 1991 s. 103, för att sekretessbelagda uppgifter inte per automatik röjs när de hanteras i en molntjänst – i vart fall inte på ett sådant sätt att det bör föranleda *straffansvar vid grov oaktsamhet*. Straffansvar inträder först *när det går att räkna med* att någon obehörig kommer att ta del av uppgiften.

När Arbetsdomstolen avgjorde om det funnits laga grund för avskedandet av den före detta generaldirektören på Transportstyrelsen utreddes om denne gjort sig skyldig till vårdslöshet med hemlig uppgift enligt 19 kap. 9 § brottsbalken. Av flera miljoner körkortsbilder, fanns en liten del sekretessbelagda bilder som hänförde sig till ärenden enligt lagen (2006:939) om kvalificerade skyddsidentiteter. Hade den före detta generaldirektören röjt dessa hemliga uppgifter? Det var utrett att denne hade tagit tre beslut om avsteg från säkerhetsprövning avseende de personer som skulle få åtkomst till hemlig information och att två tjeckiska lagringstekniker tilldelats vissa behörigheter i Transportsstyrelsens IT-system. Arbetsdomstolen, som tog vägledning i det ovan nämnda NJA 1991 s. 103, fann följande.

> *[…]* ***även om det är så att lagringsteknikerna har kunnat ta del av eller se körkortsbilderna*** *finner Arbetsdomstolen därigenom inte visat att de kunnat*

[27] Lenberg, Geijer och Tansjö, Zeteo lagkommentaren till 3 kap. 1 § offentlighets- och sekretesslagen, publicerad den 9 januari 2019.

> *ta del av uppgifter om kvalificerade skyddsidentiteter. Enligt Arbetsdomstolens mening har* ***staten sammantaget inte förmått styrka*** *att uppgifter om kvalificerade skyddsidentiteter blivit tillgängliga för de två lagringsteknikerna under sådana omständigheter* ***att man måste räkna med att de skulle komma att ta del av uppgifterna****. Omständigheterna är inte heller sådana att hemliga uppgifter ändå kan anses ha röjts.*[28]

Sammantaget ansågs det inte styrkt att den före detta generaldirektören röjt hemliga uppgifter enligt 19 kap. 9 § brottsbalken, och laga skäl för avskedande på grund av brott fanns inte.[29]

Vad gäller Office 365 talar även Arbetsdomstolens dom för att det krävs att man måste räkna med att någon ska komma att ta del av uppgifterna för att *straffansvar vid grov oaktsamhet* för brott ska kunna utgå.

Rättsfallen ger möjligen ett visst stöd för att även om en molntjänstleverantör rent tekniskt kan ta del av den sekretessreglerade och sekretessbelagda informationen i molntjänsten, är informationen inte röjd så länge det inte går att *räkna med* att någon obehörig tar del av uppgifterna. I vart fall inte på ett sådant sätt att *straffansvar vid grov oaktsamhet* ska utgå. Notera återigen att det är tillräckligt att någon är *oaktsam* för att straffansvar vid brott mot tystnadsplikten ska aktualiseras.

Vad gäller Microsoft och Office 365 så finns det möjlighet att vid support eller via administrativa behörigheter komma åt kommunens data. Möjligen har kommunen därför skäl *att räkna med* att någon obehörig i vart fall då och då och i mindre omfattning tar del av sekretessreglerade och sekretessbelagda uppgifter, vilket då skulle utgöra ett röjande vid straffansvar vid grov oaktsamhet. IT-avdelningen i Danderyds kommun har de senaste nittio dagarna räknat från den 5 juni 2018, endast vid ett tillfälle begärt Microsofts support angående en oväntat dyr faktura. Mot bakgrund av detta kan slutsatsen dras att Microsoft sällan utför support i kommunens data, vilken kan tala för motsatt tolkning, att kommunen inte har att räkna med att Microsoft tar del av kommunens data. Om så sker är det endast i undantagsfall. Kommunen vet inte hur ofta och om administrativa behörigheter tar del av kommunens data, men sådan möjlighet finns i vart fall. Ingen hänsyn tas i detta skede till Cloud Act, utan detta återkommer den vidare utredningen till under fråga c.

---

[28] Arbetsdomstolens dom nr. 15/19 meddelad i Stockholm den 6 mars 2019 i mål nr A 152/17, s. 75.

[29] Arbetsdomstolens dom nr. 15/19 meddelad i Stockholm den 6 mars 2019 i mål nr A 152/17, s. 75-76.

3.2.3 Går det att avtala om tystnadsplikt?

Under denna rubrik kommer det diskuteras huruvida det går att avtala om tystnadsplikt, och på så sätt antingen undvika att de sekretessbelagda uppgifterna röjs i offentlighets- och sekretesslagens mening, eller säkerställa att molntjänstleverantören beaktar sekretessen.

Detta är intressant utifrån två aspekter enligt följande.

- Om 10 kap. 2 § offentlighets- och sekretesslagen inte är tillämplig (och lagstöd för utlämnandet saknas), kan frågan ställas om ett avtal om tystnadsplikt med leverantören kan läka denna brist?
- Om utlämnandet bedöms vara nödvändigt utifrån 10 kap. 2 § offentlighets- och sekretesslagen (lagstöd för utlämnandet finns), kan frågan ställas om det går att stärka skyddet för de sekretessbelagda uppgifterna i molntjänsten genom att avtala med molntjänstleverantören om ett starkare sekretesskydd?

Notera att ett avtal om tystnadsplikt, aldrig kan innehålla en klausul att personal hos molntjänstleveratören ska falla under tystnadsplikt vid straffansvar, till exempel brott mot tystnadsplikten och tjänstefel (20 kap. 1 och 3 §§ brottsbalken). Personalen hos molntjänstleverantören uppfyller inte de nödvändiga rekvisit som finns i brottsbalkens nämnda bestämmelser, varför ett sådant straffrättsligt ansvar inte kan utgå för molntjänstleverantörens personal.

Även i frågan om det går att avtala med molntjänstleverantören om tystnadsplikt, har flera olika myndigheter uttalat sig.

Förarbetena om förslag på ändringar i den tidigare gällande sekretesslagen ger uttryck för att det går att avtala om tystnadsplikt enligt följande.

> *Sekretesslagen gäller i princip inte den som är anställd hos ett privat rättsobjekt. Om en myndighet har träffat avtal om t.ex. viss experthjälp med ett enskilt företag, kan det emellertid te sig naturligt att arbetstagarna hos företaget får lyda under bestämmelserna i sekretesslagen. Som exempel nämns i förarbetena till sekretesslagen att en arbetstagare har ställts till en myndighets förfogande och deltar i dess verksamhet på samma sätt som om myndigheten hade ingått uppdragsavtal med vederbörande själv. […] Mot bakgrund av det anförda kan konstateras att t.ex. personal från en kontoristförening eller ett bevakningsföretag som regel inte torde vara bundna av sekretesslagen. Jag vill emellertid erinra om att det oftast är möjligt att undvika olägenheter som kan uppkomma till följd härav antingen genom att det enskilda företaget* ***sluter avtal med sina anställda om tystnadsplikt*** *eller genom att en myndighet ställer upp förbehåll om att uppgifter som arbetstagare som inte är offentliga funktionärer får kännedom om i sin verksamhet inte får röjas för utomstående […]. Detta förfarande kan tillämpas t.ex. när en myndighet anlitar en skrivbyrå för utskrift av*

> *handlingar som innehåller sekretessbelagda uppgifter. Enligt min mening finns det inte behov av någon ytterligare lagregel i detta avseende.*[30]

Justitieombudsmannen, har i ärendet då deklarationer lämnades ut av skattemyndigheterna till privata dataföretag för registrering, uttalat sig enligt följande.

> *För den här situationen tror jag dock inte att det är nödvändigt med en i lag inskriven tystnadsplikt. Det bör finnas andra sätt att hantera problemet.*[31]

Pensionsmyndigheten fick av regeringen i uppdrag år 2015 att analysera potentialen för användning av molntjänster i staten, och har redovisat rapporten *Molntjänster i staten – en ny generation av outsourcing* där de anför följande.

> *Under vissa förhållanden kan en avtalsreglerad tystnadsplikt medföra att informationen, utan hinder av sekretess, kan lämnas ut till molntjänstleverantören.*[32]

Justitieombudsmannen har gjort motsatt bedömning i ett ärende om läkarsekreterare. Beslutet gällde en vårdgivare som anlitat ett externt bolag som tillhandahöll läkarsekreterare, vilka på distans journalförde vårdgivarens på diktafon lämnade uppgifter, i patientens journal. Justitieombudsmannen anförde följande.

> *JO konstaterar att läkarsekreterarna hos företaget inte omfattas av den tystnadsplikt enligt OSL som gäller för vårdgivarens egen personal. Frågan om huruvida uppgifterna om patientjournalerna kan göras tillgängliga för läkarsekreterarna är därför i första hand beroende av om ett utlämnande kan ske utan att det innebär med (dvs. skada) för den som skyddas av sekretessen.*
>
> *Läkarsekreterarna har en avtalsreglerad tystnadsplikt i förhållande till arbetsgivaren (dvs. företaget). Vidare följer av regelverket om behandling av personuppgifter en sorts tystnadsplikt för den som behandlar uppgifterna.* ***Enligt JO är dessa ”alternativa” tystnadsplikter för läkarsekreterarna inte tillräckliga för att anse att ett utlämnande kan ske utan att det innebär men (skada) för den som skyddas av sekretessen****. Vid bedömningen har – mot bakgrund av att de uppgifter som behandlas enligt avtalen är av mycket integritetskänsligt slag –* ***vikt lagts bl.a. vid ett vårdgivarens egen personal kan dömas för brott mot tystnadsplikt om sekretessbelagt uppgift felaktigt röjs, medan så inte är fallet när det gäller läkarsekreterare som är anställda i företaget****. Ett utlämnande har inte heller haft stöd i någon av de sekretessbrytande bestämmelser som finns i 10 kap. OSL eller i en lag eller förordning som OSL hänvisar till.*

[30] Prop. 1981/82:186 s. 41–42.

[31] JO 1982-03-11, dnr. 149–1980 s. 241.

[32] Pensionsmyndighetens utredning, Molntjänster i staten – en ny generation av outsourcing, s. 39.

> *JO:s slutsats är att vårdgivarna inte haft rättsligt stöd för att på det sätt som skett lämna ut sekretessbelagda uppgifter om patienter för journalföring av företagets läkarsekreterare. Enligt JO är det anmärkningsvärt att vårdgivarna inte har ägnat sekretessaspekterna större uppmärksamhet i samband med att avtalen ingicks. Vårdgivarna får allvarlig kritik för att de har ingått avtal som innebär att landstinget/regionen lämnar ut patientuppgifter för journalföring av anställda vid ett företag, trots att detta inte är förenligt med regelverket om sekretess.*[33]

Justitieombudsmannens beslut får förstås som att det utgör ett röjande av sekretessbelagda uppgifter att lämna ut uppgifter till extern leverantör – trots att ett avtal om tystnadsplikt ingåtts. Justitieombudsmannen förtydligar att ett avtal om tystnadsplikt aldrig kan medföra ett straffrättsligt ansvar enligt 20 kap. 3 § brottsbalken på det sätt offentlighets- och sekretesslagen förutsätter, varför ett avtal om tystnadsplikt inte är tillräckligt för att kunna lämna ut sekretessreglerade och sekretessbelagda uppgifter.

Justitieombudsmannens beslut om läkarsekreterare, ger uttryck för att det inte är tillräckligt att avtala om tystnadsplikt med molntjänstleverantörer, för att kunna lagra sekretessbelagda uppgifter i molntjänster. Stöd för utlämnande saknades i detta fall, enligt 10 kap. 2 § offentlighets- och sekretesslagen. Personal hos molntjänstleverantören kommer ändå inte underkastas det straffrättsliga ansvaret enligt 20 kap. 3 § brottsbalken.

Denna utredning vill dock poängtera att det är en betydlig skillnad vad gäller uppgifter som lagras och hanteras i molntjänster (vilka inte är avsedda för molntjänstleverantören att ta del av) i jämförelse med läkarsekreterarna som (genom att lyssna av diktafonen och skriva in uppgifterna i patientens journal) verkligen tog del av samtliga patientuppgifter.

Även i betänkandet av Digitaliseringsrättsutredningen, *Juridik som stöd för förvaltningens digitalisering*, anförs funderingar kring om det är tillräckligt att avtala om tystnadsplikt, enligt följande.

> *Enligt vår bedömning kan det i allt ökande grad nu ifrågasättas om det är tillräckligt att den privata leverantörens personal omfattas av en avtalsreglerad tystnadsplikt.*[34]
>
> *Det kan också diskuteras om det är tillräckligt med en avtalsreglerad tystnadsplikt för att mindre integritetskänsliga uppgifter som skyddas av en sekretessbestämmelse försedd med ett rakt skaderekvisit ska kunna lämnas ut till en privat aktör. Det är enligt vår mening inte uteslutet att det vid skadeprövningen i vissa fall skulle kunna anses föreligga skada även i de situationerna. En författningsreglerad tystnadsplikt skulle därför under alla*

[33] JO den 9 september 2014, dnr. 3032–2011.

[34] SOU 2018:25 s. 362.

> *förhållanden väsentligen bidra till att undanröja den osäkerhet kring rättsläget som finns hos myndigheter och andra aktörer.*[35]
>
> *För att skapa en långsiktigt hållbar rättslig reglering som ger stöd för den offentliga sektorns digitalisering,* ***finns det behov av en i lag reglerad tystnadsplikt för de som är verksamma hos en privat leverantör*** *för uppgifter som omfattas av sekretess och som lämnas ut till leverantören i samband med utkontraktering av IT-drift eller andra it-baserade funktioner. Regleringen medför att uppgifter som lämnas ut i samband med sådan utkontraktering får samma sekretesskydd hos leverantören som hos den utkontrakterande myndigheten.*[36]

Denna utredning får notera, att Digitaliseringsrättsutredningens förslag om lagstadgad tystnadsplikt för molntjänstleverantörer, innebär att Digitaliseringsrättsutredningen menar att det *inte* är tillräckligt att avtala om tystnadsplikt.

Sammantaget får utredningen konstatera att det i förarbeten[37] och betänkanden samt av Justitieombudsmannen görs, med varandra, oförenliga tolkningar huruvida det går att lämna ut sekretessbelagda uppgifter genom att avtala om tystnadsplikt med en extern part och på så sätt undvika att uppgiften röjs i offentlighets- och sekretesslagens mening.

Även om det finns visst stöd i förarbeten för att det skulle kunna gå att ingå avtal om tystnadsplikt rör diskussionen där huvudsakligen externa anställda i myndighetens verksamhet. Denna utredning ställer sig tveksam till att en avtalad tystnadsplikt skulle kunna läka att stöd för utlämnande enligt 10 kap. 2 § offentlighets- och sekretesslagen saknas, eftersom en avtalad tystnadsplikt inte medför det straffansvar enligt brottsbalken, som offentlighets- och sekretesslagen förutsätter.

Om stöd för utlämnandet finns i 10 kap. 2 § offentlighets- och sekretesslagen, gör denna utredning bedömningen att det går att stärka skyddet för att de sekretessreglerade och sekretessbelagda uppgifterna i molntjänsten, genom att ingå ett avtal om tystnadsplikt med molntjänstleverantören. Det är bättre att ingå ett sådant avtal, än att inte göra det, även om ett straffansvar inte kan följa med ett sådant avtal.

---

[35] SOU 2018:25 s. 364.

[36] SOU 2018:25 s. 361.

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

3.2.4 Avtal om tystnadsplikt för uppgifter om rikets säkerhet

I diskussionen om det är möjlighet att avtala med molntjänstleverantören om tystnadsplikt, är det intressant att göra en jämförelse med hur uppgifter om Sveriges säkerhet hanteras.

Den 1 april 2019 trädde en ny säkerhetsskyddslag i kraft som gäller den som bedriver verksamhet som är betydelse för Sveriges säkerhet eller som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd, enligt 1 kap. 1 § säkerhetsskyddslagen (2018:585). Till skillnad från den föregående lagen gäller denna lag även för enskilda aktörer.

I 2 kap. 6 § säkerhetsskyddslagen stadgas i huvudsak att myndigheter som avser att genomföra en upphandling eller ingå ett avtal om varor, tjänster eller byggentreprenader ska se till att det i ett *säkerhetsskyddsavtal* anges hur säkerhetsskyddet ska tillgodoses hos leverantören. Detta gäller om det i upphandlingen framkommer säkerhetsskyddsklassificerade uppgifter i klassen konfidentiell eller högre (vilket utgör sekretessbelagda uppgifter[38]), eller om upphandlingen i övrigt ger leverantören tillgång till säkerhetskänslig verksamhet av motsvarande betydelse för Sveriges säkerhet.

Av förarbetena till säkerhetsskyddslagen framgår det i en upphandling som berör uppgifter som klassificeras i den lägsta säkerhetskyddsklassen, eller om den avser säkerhetskänslig verksamhet av motsvarande betydelse för Sveriges säkerhet, torde det finnas *ett mindre behov* av att ingå säkerhetsskyddsavtal med leverantören.[39]

Leverantören, som får ta del av säkerhetskänslig information och som ett säkerhetsskyddsavtal ingås med, kan vara ett bolag med svenska ägarförhållanden, men kan lika gärna vara ett utländskt bolag. Utgångspunkten är att samma förutsättningar gäller vid utländska leverantörer som för svenska. Kan ett ändamålsenligt säkerhetsskydd åstadkommas, utifrån bland annat leverantörens infrastruktur och förutsättningar för informationssäkerhet samt det aktuella landets hotbild, finns det inget som hindrar att en leverantör med säte i utlandet anlitas. Det finns ett antal mekanismer för att anlita en utländsk leverantör. I Sveriges internationella säkerhetsöverenskommelser framgår oftast att parterna ska

[38] Jfr. 1 kap. 2 § säkerhetsskyddslagen

[39] Prop. 2017/18:89 s. 107.

följa den säkerhetsbedömning avseende leverantörer som den andra partens behöriga myndigheter har gjort. Viss anpassning av säkerhetskyddsavtalet kan göras om leverantören har sitt säte utanför Sverige.[40]

Denna utredning gör några försiktiga reflektioner utifrån 2 kap. 6 § säkerhetsskyddslagen enligt följande.

- Att den svenska eller utländska leverantören ingår ett säkerhetsskyddsavtal verkar utgöra en tillräcklig garanti för att den upphandlande myndigheten ska kunna lämna säkerhetsskyddsklassificerade uppgifter till potentiella, även utländska, leverantörer.
- Det förefaller som att det går skräddarsy olika avtalslösningar beroende på uppgiftens känslighet, även för uppgifter inom samma klassificering.

Även vad gäller ett utlämnande av sekretessbelagda uppgifter till en utländsk myndighet anförs det i betänkandet till ny säkerhetsskyddslag enligt följande.

> *[…] ett generellt* ***säkerhetsskyddsavtal [är] den enda möjligheten att med bindande verkan reglera*** *att uppgifter som i Sverige omfattas av sekretess och rör rikets säkerhet* ***hanteras på ett säkert sätt*** *av ett annat land eller en mellanfolklig organisation när sådana uppgifter överlämnas.*[41]

Vad gäller uppgifter om rikets säkerhet som lämnas ut vid upphandlingar, utgår denna utredning ifrån att grund för utlämnande förmodligen finns, i vart fall enligt 10 kap. 2 § offentlighets- och sekretesslagen, eftersom det kan vara nödvändigt att lämna ut viss information för att kunna genomföra en upphandling av varor eller tjänster. Notera likväl att säkerhetsskyddslagen även gäller för privata aktörer, som inte lyder under offentlighets- och sekretesslagen.[42]

Denna utredning har i föregående avsnitt funnit att ett avtal om tystnadsplikt inte kan läka om stöd för utlämnande saknas, men bör ingås med molntjänstleverantören, om stöd för utlämnande finns, för att stärka skyddet för de sekretessreglerade och sekretessbelagda uppgifterna.

Denna utredning får konstatera att uppgifter om rikets säkerhet lämnas ut efter att säkerhetsskyddsavtal ingåtts, även med externa parter som inte

[40] Jfr. SOU 2015:25 s. 433-434.

[41] SOU 2015:25 s. 170, om 8 kap. 3 § offentlighets- och sekretesslagen.

[42] Jfr. 2 kap. 1 § offentlighets- och sekretesslagen.

träffas av offentlighets- och sekretesslagen och straffansvaret i brottsbalken. Notera att grund för utlämnande då torde finnas. Även detta talar för att det går att avtala om hantering av sekretessreglerade och sekretessbelagda uppgifter i en molntjänst, även om det inte kan läka om grund för utlämnande saknas.

3.2.5 Sammanfattningsvis

Denna utredning har utrett om utlämnandet annars, i så fall 10 kap. 2 § offentlighets- och sekretesslagen inte bedöms tillämplig, utgör ett röjande av sekretessbelagda uppgifter?

Utredningen har funnit att det med stöd i rättsfall om straffansvar vid grov oaktsamhet, finns visst stöd för att även om en molntjänstleverantör rent tekniskt skulle kunna ta del av den sekretessreglerade och sekretessbelagda informationen i molntjänsten, är informationen inte röjd så länge det inte går att *räkna med* att någon obehörig tar del av uppgifterna. I vart fall inte på ett sådant sätt att *straffansvar vid grov oaktsamhet* skulle utgå. För brott mot tystnadsplikten räcker det dock att någon är oaktsam. Möjligen talar rättsfallen för att kommunen har att räkna med att Microsoft kommer ta del av uppgifterna i samband med support och via administrativa behörigheter, samtidigt är det sällan support sker i kommunens data. Det går inte att säga om och hur ofta administrativa behörigheter tar del av kommunens data, men sådan möjlighet finns.

Vidare har utredningen funnit att ett avtal om tystnadsplikt med molntjänstleverantören inte kan läka om en grund för utlämnande saknas. Finns dock en grund för utlämnande till molntjänstleverantören, är det bättre att ingå ett avtal om tystnadsplikt, än att inte göra det (även om ett sådant avtal inte kan innebära tystnadsplikt vid straffansvar enligt brottsbalken).

3.3 Utgör Cloud Act och liknande regelverk att utlämnandet utgör ett röjande av sekretessbelagda uppgifter?

3.3.1 Cloud Act och liknande regelverk

I mars 2018 införde amerikanska myndigheter Clarifying Overseas Use of Data, fortsättningsvis *Cloud Act*.

Syftet med Cloud Act var bland annat att förenkla för det amerikanska rättsväsendet att komma åt information som är lagrad utanför landets gränser.[43] Cloud Act ger amerikanska myndigheter rätt att få ut information, som har anknytning till amerikanska myndigheters brottsutredningar, direkt

[43] 18 U.S. Code ingress.

från molntjänstleverantörer i amerikansk ägo. Detta gäller oavsett om informationen är lagrad i USA eller någon annanstans. Även andra utländska regeringar kan framställa anspråk på att få ut information med stöd i Cloud Act.[44] Eftersom Cloud Act medför att amerikanska myndigheter kan få ut information direkt av den globala molntjänstleverantören kringgås bestämmelserna om internationell rättshjälp. Det finns möjligheter att belägga molntjänstleverantören med yppandeförbud, vilket förhindrar molntjänstleverantören att informera kunden (kommunen i denna utredning) om att utlämnande kommer ske eller har skett.[45] Det får till följd att kommunen fråntas möjligheten att göra en sekretessprövning, vilket kommunen är skyldig att göra enligt offentlighets- och sekretesslagen.

Även *Foreign Intelligence Surveillance Act (FISA)* sektion 702 möjliggör för amerikanska underrättelsemyndigheter att samla in information om icke-amerikanska medborgare som antas befinna sig utanför USA. Den, vars personuppgifter behandlas, får inte kännedom om behandlingen och har inte heller någon möjlighet att korrigera eller radera personuppgifter. Vidare har amerikanska presidentämbetet utfärdat en Excutive Order EO12333 som ger den amerikanska signalspaningsmyndigheten stöd för underrättelseinhämtning från utlandet. Hanteringen är inte reglerad i lag, den är inte föremål för rättslig tillsyn och kan inte bli föremål för domstolsprövning. Även Kina, Indien och Ryssland har infört liknande lagstiftning.[46]

Microsoft, som tillhandahåller Office 365, är ett amerikanskt bolag. Det medför att uppgifter som lagras i Office 365 *kan* begäras ut med stöd i Cloud Act och andra liknande regelverk, utan att kommunen får göra en sekretessprövning eller får kännedom om att ett utlämnande kommer ske eller har skett.

Införandet av Cloud Act och andra liknande regelverk, har generellt påverkat synen på lämpligheten att använda globala molntjänster som Office 365.

[44] Jfr. 18 U.S. Code § 2523.

[45] 18 U.S. Code § 2703 (b) (1).

[46] Jfr. Kammarkollegiets Förstudierapport Webbaserat kontorsstöd dnr. 23.2-6283-18, den 22 februari 2019 s. 21–25.

3.3.2 Sekretessbelagd information får inte röjas för en utländsk myndighet (8 kap. 3 §)

Av 8 kap. 3 § offentlighets- och sekretesslagen framgår i huvudsak att en sekretessbelagd uppgift inte får röjas för en *utländsk myndighet* eller en mellanfolklig organisation, om

1. inte utlämnande sker i enlighet med särskild föreskrift i lag eller förordning,
2. eller 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.

Bestämmelsen ska inte förstås som någon förpliktelse att lämna ut en sekretessbelagd uppgift till en utländsk myndighet, utan bestämmelsen reglerar endast när sekretessbelagda uppgifter *får* lämnas till en utländsk myndighet.[47] Avsikten med 8 kap. 3 § offentlighets- och sekretesslagen är inte heller att de sekretessbelagda uppgifterna ska röjas, utan att sekretessen ska bestå med stöd av det mottagande landets nationella lagstiftning, vilken motsvarar offentlighets- och sekretesslagen.[48]

Vad gäller hantering av sekretessreglerade och sekretessbelagda uppgifter i Office 365, utgör inte Microsoft någon utländsk myndighet, utan ett externt globalt bolag. Denna utredning gör därför bedömningen att 8 kap. 3 § offentlighets- och sekretesslagen endast kan appliceras analogt på frågan om lämpligheten av lagring av sekretessbelagd information i molntjänster. 8 kap. 3 § offentlighets- och sekretesslagen torde inte bli direkt tillämplig. Inte heller om amerikanska myndigheter med stöd i Cloud Act begär ut information från Microsoft synes bestämmelsen bli tillämplig, eftersom Microsoft inte lyder under offentlighets- och sekretesslagen.

Det får noteras att Kammarkollegiet antingen gjort en annan bedömning om 8 kap. 3 § offentlighets- och sekretesslagen är tillämplig än vad denna utredning gjort, eller prövat huruvida den svenska myndigheten kan lämna ut uppgifter direkt till det amerikanska rättsväsendet (utan att beakta att informationen är lagrad i en molntjänst, hämtas från en molntjänst och

[47] Lagrådets betänkande 1982/83: KU12 s. 36.

[48] SOU 2015:25 s. 170.

lämnas ut av molntjänstleverantören utan den svenska myndighetens medgivande). Kammarkollegiet anför följande.

> *Det finns ingen särskild föreskrift i lag eller förordning som medger ett utlämnande enligt FISA sektion 702, EO 12333 eller CLOUD Act varför [8 kap. 3 §] punkt 1 [offentlighets- och sekretesslagen] 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.*[49]

Denna utredning har funnit ett utlämnande till Office 365 och Microsoft måste ske med stöd i 10 kap. 2 § offentlighets- och sekretesslagen för att grund för utlämnandet ska finnas. Utredningen noterar därför endast att – oavsett om 8 kap. 3 § offentlighets- och sekretesslagen är tillämplig eller inte – finns det inte något utrymme för att lämna ut sekretessbelagda uppgifter till en global molntjänstleverantör, med stöd i den bestämmelsen.

3.3.3 Uttalanden med hänsyn till Cloud Act och andra liknande regelverk

Redan i förarbetena till sekretesslagen åskådliggjordes röjande av sekretessbelagda uppgifter till ett annat land enligt följande.

[49] Kammarkollegiets Förstudierapport Webbaserat kontorsstöd dnr. 23.2-6283-18, den 22 februari 2019 s. 32–33.

> *Tjänsteman som har tystnadsplikt kan inte sällan i tjänsten vidarebefordra uppgift till annat land utan att han därigenom gör sig skyldig till "obehörigt röjande".*[50]

eSam har 2018 uttalat sig särskilt om globala molntjänster, efter att Cloud Act infördes, enligt följande.

> *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 anlitas eller annan lagligt 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.***[51] *Detsamma får gälla om redan ägarförhållanden eller geografisk placering av en tjänsteleverantörs tekniska hjälpmedel ger anledning att befara att mänskliga rättigheter (till exempel skyddet för privatlivet) och det allmännas intressen (t.ex. rikets säkerhet) inte skulle säkerställas om svenska myndigheters data hade tillgängliggjorts.*[52]

Kammarkollegiet har i sin förstudie om webbaserat kontorsstöd anfört följande.

> *En svensk myndighet som låter företag som lyder under ett sådant regelverk [Cloud Act m.fl.] 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****.*[53]

Säkerhetspolisen vilka listat tio tips om säkrare outsourcing, anför följande.

> *Även om informationen får lämnas ut enligt offentlighets- och sekretesslagen kan det finnas omständigheter som ändå gör det olämpligt att anlita en molntjänstleverantör. Omständigheter att beakta kan t.ex. vara vilket lands rättsordning som blir tillämplig på lagrad information […].*[54]

Advokatbyrån Setterwalls, som på uppdrag av SKL har utrett frågan om röjande av sekretessbelagd uppgift vid användningen av molntjänster, kommer bland annat fram till följande.

> *Det är komplicerat att bedöma om ändamålsenliga kombinationer av fysiska, juridiska, tekniska och administrativa åtgärder inte bara utlovas utan också upprätthålls över tid i en global molntjänst.* ***Det kommer inte att kunna***

---

[50] Prop. 1979/80:2 Del A s. 122.

[51] *Ett röjande kan även ske vid användningen av molntjänster där leverantören enligt avtalet t.ex. tillhandahåller support- och utvecklingstjänster som förutsätter att leverantören får tillgång till informationen som gjorts tillgänglig i tjänsten.*

[52] eSams rättsliga uttalande den 23 oktober 2018, dnr. VER 2018:57.

[53] Kammarkollegiets Förstudierapport Webbaserat kontorsstöd dnr. 23.2-6283-18, den 22 februari 2019 s. 33.

[54] Säkerhetspolisen, *10 tips för säkrare outsourcing*, p. 8

> ***kontrolleras om myndighetens uppgifter röjs till följd av t.ex. hemliga tvångsmedel eller underrättelseverksamhet***.[55]

SKL har den 12 april 2019 tagit följande ställningstagande om informationshantering i vissa molntjänster och bemött eSams uttalande år 2018 enligt följande.

> *SKL gör bedömningen att en rättslig analys av röjandefrågan behöver göras i en bredare kontext där även verksamhetens* ***reella möjligheter till alternativ, riskbedömning och åtgärder för riskreducering*** *till exempel genom begränsningar i tjänsteavtal eller kryptering behöver tas in i bedömningen.*
>
> *SKL rekommenderar kommuner och regioner som ännu inte hanterar sekretessreglerade eller känsliga uppgifter i molntjänster att noga överväga risken för röjande som expertgruppens uttalanden[56] pekar på och när så är möjligt välja annan informationshantering eller genom skyddande säkerhetsåtgärder minimera riskerna.*
>
> ***SKL rekommenderar kommuner och regioner som redan använder denna typ av molntjänster med utländskt ägande, även för information som omfattas av sekretess, att fokusera på säkerhetsåtgärder och riskreducering inom rätt område och i de fall det bedöms nödvändigt återta informationshanteringen***.[57]

Det får noteras att flera instanser menar att sekretessbelagd information röjs om den laddas upp i en molntjänst som lyder under Cloud Act och andra liknande regelverk. Det får också noteras att Cloud Act och liknande regelverk har medfört en generellt ändrad inställning till lämpligheten av molntjänster. Ett tydligt exempel på detta är att eSam år 2015 bedömde att utkontraktering av IT-drift inte ansågs utgöra ett röjande, och år 2018 bedömde att uppgifterna får anses vara röjda om det lagras i en molntjänst som till följd av ägarförhållanden kan bli bunden av regler i annat land.

Denna utredning får notera att offentlighets- och sekretesslagen inte ger något stöd för ett utlämnande på det sätt som Cloud Act och liknande regelverk föreskriver. Utländska myndigheters inhämtande av information på detta sätt är inte förenligt med offentlighets- och sekretesslagen. Cloud Act och liknande regelverk innebär att utländska myndigheter har möjlighet att ta del av kommunens sekretessreglerade och sekretessbelagda uppgifter utan att detta kommer till kommunens kännedom och utan att kommunen får göra en sekretessprövning. Har kommunen inte stöd i lagen för att lämna

---

[55] Axelsson, Furberg, Ljunggren, Setterwalls advokatbyrå, *Rättsutredning – Frågor om röjande vid användning av molntjänster*, den 23 mars 2018, s. 26.

[56] Med expertgruppens uttalanden menas eSams uttalande år 2018 som det får förstås.

[57] Sveriges kommuner och landsting, *Ställningstagande om informationshantering i vissa molntjänster*, ärendenr. 19/00087, den 12 april 2019.

ut sekretessbelagda uppgifter, men om så ändå sker, bedöms myndigheten röja den sekretessbelagda informationen på ett olagligt sätt. Ett sådant röjande kan aktualisera straffansvar jämlikt tjänstefel (20 kap. 1 § brottsbalken) och brott mot tystnadsplikten (20 kap. 3 § brottsbalken).

Kommunen har vetskap om att Microsoft, med stöd i Cloud Act kan komma att lämna ut sekretessreglerade och sekretessbelagda uppgifter till amerikanska eller utländska myndigheter. Utifrån detta får frågan ställas om kommunens utlämnande av sekretessbelagda uppgifter till Office 365 och Microsoft under sådana premisser utgör ett röjande av sekretessbelagda uppgifter?

Denna utredning gör bedömningen att Cloud Act och liknande regelverk kan utgöra ett röjande av sekretessbelagda uppgifter *om* uppgifterna lämnas ut.

Microsoft har i sin egen statistik över mottagna begäran för det senare halvåret 2018 listat att de fått in 4 369 stycken begäran från amerikanska brottsbekämpande myndigheter om att de ska lämna ut uppgifter, varav 103 begäranden rörde data som lagrades utanför USA. Under samma tid mottog Microsoft 36 begäranden från amerikanska brottsbekämpande myndigheter avseende företagskunder vilka köpt mer än 50 konton (jfr. *50 seats*). Av dessa resulterade en begäran i utlämnande av data som lagrades utanför USA.[58] Enligt Microsofts villkor lagras kommunens uppgifter inom EU, men bearbetning och eventuellt support kan ske utanför EU.

Microsoft anför vidare följande.

> *Under det första halvåret 2018 mottogs strax över 23 000 förfrågningar av vilka endast 50 rörde icke-konsumentkonton. Av dessa avvisades eller omdirigerades 32 ärenden av Microsoft och av de kvarvarande gällde 10 ärenden innehåll. Enbart ett av de amerikanska ärendena gällde också data utanför landets gränser. Inga gällde Sverige.*[59]

Av 23 000 begäranden som inkom globalt synes endast 50 begäranden globalt har rört företagskonton såsom Danderyds kommuns konto (jfr. icke-konsumentkonton).

Av statistiken framgår förvisso inte om det finns ytterligare begäranden som inte redovisas i underlaget, i anledning av yppandeförbudet.

---

[58] https://www.microsoft.com/en-us/corporate-responsibility/lerr/

[59] https://news.microsoft.com/sv-se/2018/12/13/molntjanster-och-sakerhet/

Möjligtvis finns här möjlighet att göra en bedömning om sannolikheten av ett utlämnande till amerikanska och utländska myndigheter är hög eller låg.[60] eSam har ansett att uppgifter som görs tillgängliga för en global molntjänst får anses vara röjda, eftersom det inte längre är osannolikt att uppgifterna kan komma att lämnas till utomstående.[61] Påståendet saknar någon källhänvisning.

Denna utredning har övervägt om det pågår underrättelsearbete av andra lands rättsordningar i molntjänsterna, med eller utan molntjänstleverantörens kännedom. Är det möjligen detta eSam syftar på när de menar att det inte är osannolikt att uppgifterna lämnas ut till utomstående?[62] Någon fakta om att det skulle pågå underrättelsearbete i molntjänster finns inte tillgänglig att ta del av för denna utredning. Om det skulle finnas bevis för att underrättelsearbete i molntjänster sker måste det bedömas som väldigt olyckligt att myndigheter – vilka i princip lämnas att självständigt fatta beslut om lämpligheten i att använda molntjänster – inte får del av relevant och konkret information. Med detta sagt, menar denna utredningen att underrättelseverksamhet är möjlig till exempel när kommunikation passerar genom länder, exempelvis genom växelpunkter för internettrafik. Utredningen får därför notera att informationen i Microsoft är krypterad och säkrad genom säkerhetsteknik på ett sätt som denna utredning finner ger ett fullgott skydd, även mot underrättelseverksamhet, läs vidare om detta under avsnitten om säkerhet.

Sett till Microsofts egen statistik om hur många begäranden de fått om utlämnande enligt Cloud Act och hur få av begäranden som rör företagskonton, får sannolikheten att uppgifter lämnas ut med försiktighet bedömas som låg. Notera att kommunen inte alltid skulle få kännedom om ett utlämnade sker eller har skett på grund av yppandeförbudet. Det medför att risken för att kommunen röjer sekretessbelagda uppgifter för amerikanska och utländska myndigheter, när sådana uppgifter sparas i Office 365 och Microsoft, i dagsläget med viss försiktighet får bedömas som låg.

3.3.4 Sammanfattningsvis

Denna utredning har utrett om Cloud Act och liknande regelverk medför att utlämnandet utgör ett röjande av sekretessbelagda uppgifter?

---

[60] Jfr. eSams uttalande år 2015 och 2018 om begreppet *sannolikhet.*

[61] eSams rättsliga uttalande den 23 oktober 2018, dnr. VER 2018:57.

[62] Jfr. eSams rättsliga uttalande den 23 oktober 2018, dnr. VER 2018:57.

Denna utredning har funnit att Cloud Act och andra liknande regelverk kan utgöra ett röjande av sekretessbelagda uppgifter, *om* uppgifterna lämnas ut. Sannolikheten att uppgifterna lämnas ut av Microsoft till amerikanska eller utländska myndigheter bedöms i dagsläget med viss försiktighet som låg. Sannolikheten för att kommunen röjer sekretessbelagda uppgifter bedöms därför också med viss försiktighet som låg. Om så sker, kan det dock utgöra ett brott mot tystnadsplikten. Notera likväl att eSam med flera haft en annan uppfattning än denna utredning.

4 Dataskydd – om personuppgiftsbehandling

Dataskyddslagstiftningen reglerar hur *behandling av personuppgifter* får gå till inom EU/EES och hos aktörer som har verksamhet inom EU/EES. En personuppgift är alla uppgifter som kan användas för att direkt eller indirekt identifiera en fysisk, levande person. Med behandling avses allt som görs med personuppgifterna, t.ex. läsning, bearbetning, lagring, utlämnande, kopiering m.m. Vissa personuppgifter kan klassas som känsliga[63] och skyddsvärda, vilket ställer högre krav på den som behandlar dem.

I ett IT-system kan det förekomma flera olika behandlingar och en mängd varierande personuppgifter. Gemensamt är att all behandling måste ha en rättslig grund och följa förordningens grundläggande principer. Den som bestämmer ändamålen och medlen med behandlingen är personuppgiftsansvarig. I Danderyds kommun är varje nämnd personuppgiftsansvarig för sina personuppgiftsbehandlingar.

4.1 Förordningens grundläggande principer

Förordningen ställer krav på att personuppgifter endast får behandlas utifrån följande grundläggande principer.[64]

- Laglighet, korrekthet och öppenhet,
- Ändamålsbegränsning,
- Uppgiftsminimering,
- Riktighet,
- Lagringsminimering,
- Integritet och konfidentialitet,

[63] Särskilda kategorier av personuppgifter är den korrekta benämningen.

[64] Dataskyddsförordningen, artikel 5.

- Ansvarsskyldighet.

Det är inte tillåtet att behandla personuppgifter utan att följa dataskyddslagstiftningen. Undantaget är behandling av icke levande personers personuppgifter, behandling för privat bruk och vid utövande av sina yttrande- och informationsfriheter.

4.2 Förordningens rättsliga grunder

En behandling av personuppgifter skulle teoretiskt kunna ha flera rättsliga grunder. Varje behandling måste dock ha minst en rättslig grund för att vara laglig.

De rättsliga grunderna är[65]:

- **Samtycke**: den registrerade har uttryckligen sagt ja till att personuppgiften behandlas.
- **Avtal**: behandlingen krävs för att uppfylla ett avtal mellan de registrerade och personuppgiftsansvarig.
- **Intresseavvägning**: den personuppgiftsansvariges intressen med behandlingen väger tyngre än den registrerades integritetsintresse.
- **Rättslig förpliktelse**: det finns lagar eller regler som gör att den personuppgiftsansvarige måste behandla personuppgifter.
- **Myndighetsutövning och uppgift av allmänt intresse**: den personuppgiftsansvarige måste utföra behandlingen inom ramen för sin myndighetsutövning eller för att utföra en uppgift av allmänt intresse.
- **Grundläggande intresse**: den personuppgiftsansvarige måste behandla personuppgifter när en registrerad är oförmögen att samtycka, t.ex. om denne är medvetslös.

4.3 Överföring till tredjeland

All överföring av personuppgifter till tredjeland är otillåten om inte dataskyddslagstiftningen följs. Med tredjeland avses alla länder utanför EU/EES.

EU-kommissionen kan besluta om att tredjeländer omfattas av s.k. adekvat skyddsnivå[66], alltså att landet genom intern lagstiftning säkerställer

[65] Dataskyddsförordningen, artikel 6.

[66] Följande länder har enligt EU-kommissionen adekvat skyddsnivå: Andorra, Argentina, Bailiwick of Guernsey, Färöarna, Isle of Man, Israel, Japan, Jersey, Nya Zeeland, Schweiz,

enskildas fri- och rättigheter på ett sätt som är likvärdig skyddsnivån inom unionen. Det innebär att överföring av personuppgifter till sådana länder inte kräver något särskilt tillstånd.

Det finns utöver adekvat skyddsnivå undantag som gör det möjligt att överföra personuppgifter till tredjeland. Undantagen villkoras dock mot att enskilda ska ha tillgång till lagstadgade rättigheter och effektiva rättsmedel samt att den som gör överföringen vidtar lämpliga skyddsåtgärder. Uppfylls dessa villkor är undantagen att någon av EU-kommissionens standardavtalsklausuler[67] har antagits eller att en företagskoncern har antagit bindande företagsbestämmelser, BCR.[68]

4.4 Privacy Shield

Microsoft är ett amerikanskt bolag. En överföring till USA kan bli laglig om mottagaren har anslutit sig till Privacy Shield. Det är en överenskommelse som ingicks mellan USA och EU-kommissionen 2016. I korthet innebär det att de mottagare som ansöker om att ansluta sig till Privacy Shield och godtas omfattas av adekvat skyddsnivå enligt EU-kommissionen. Observera dock att det inte innebär någon generell möjlighet att överföra personuppgifter till USA i stort utan endast till den Privacy Shield-anslutna mottagaren.

4.5 Om personuppgiftsbiträden

Ett personuppgiftsbiträde är någon utanför den personuppgiftsansvariges organisation som behandlar personuppgifter på uppdrag åt den personuppgiftsansvarige. Då Office 365 är en molntjänst som driftas utanför kommunen blir Microsoft nämndernas personuppgiftsbiträde.

För att säkerställa att detta görs i enlighet med dataskyddsförordningen måste personuppgiftsansvarig reglera biträdets hantering. Det kan göras genom ett personuppgiftsbiträdesavtal (fortsättningsvis PUB-avtal) eller annan rättsakt.

Uruguay. Kanada, om deras lagstiftning för skydd av personuppgifter i privat sektor är tillämplig på mottagarens personuppgiftsbehandling. USA, om mottagaren har anslutit sig till så kallade Privacy Shield.

[67] EU-kommissionen har godkänt vissa standardavtalsklausuler som handlar om dataskydd (Standard Contractual Clauses, SCC). Att ingå någon av dem gör en tredjelandsöverföring laglig.

[68] BCR är regler om personuppgiftsbehandling som en koncern med bolag i flera länder kan ta fram. De måste godkännas av Datainspektionen eller annan tillsynsmyndighet i EU.

Ett personuppgiftsbiträde kan ha underbiträden som inte utgör en direkt avtalspart med personuppgiftsansvarig. Det är biträdets ansvar att teckna erforderliga avtal med sina underbiträden, dock bör personuppgiftsansvarig genom t.ex. PUB-avtal instruera biträdet om hur anlitande av underbiträden får gå till.

4.6 Om sanktioner och skadestånd

Enligt dataskyddslagstiftningen kan brott mot lagstiftningen, oavsett om brottet begås av personuppgiftsansvarig eller biträdet, innebära att tillsynsmyndighet utdömer sanktionsavgifter. Avgiften för myndigheter för mindre överträdelser är maximalt 5 miljoner kronor och för allvarligare överträdelser är det maximalt 10 miljoner kronor. För privat sektor uppgår mindre överträdelser till maximalt 10 miljoner euro eller 2 procent av den globala årsomsättningen. För allvarligare överträdelserna uppgår sanktionsavgiften till maximalt 20 miljoner euro eller 4 procent av den globala årsomsättningen. Att bryta mot förordningens grundläggande principer teoretiseras vara ett sådant brott som motiverar högre sanktionsavgifter.

De registrerade vars personuppgifter har hanterats felaktigt kan begära skadestånd direkt av personuppgiftsansvarig. Det finns inget tak på skadeståndsyrkan vilken torde hanteras i enlighet med sedvanlig rättsprocess. Detta medför att kommunens nämnder kan tilldelas sanktionsavgift eller bli skadeståndsansvarig om kommunens verksamheter behandlar personuppgifter på ett felaktigt sätt.

4.7 Om konsekvensbedömning enligt artikel 35

Innan en behandling av personuppgifter påbörjas ska en konsekvensbedömning göras om behandlingen sannolikt leder till en hög risk[69] för registrerades fri- och rättigheter.

En regelrätt konsekvensbedömning enligt dataskyddsförordningens artikel 35 kan föregås av en riskanalys där säkerhetsåtgärder som behöver vidtas finns med. Denna utredning kan sägas utgöra en sådan riskanalys. Efter genomförd riskanalys beslutas om en konsekvensbedömning är nödvändig.

[69] Artikel 29-gruppen, nuvarande dataskyddsstyrelsen, definierar risk som följer: ”En ’risk’ är ett scenario som beskriver en händelse och dess uppskattade konsekvenser vad gäller allvar och sannolikhet.” i *Riktlinjer om konsekvensbedömning avseende dataskydd och fastställande av huruvida behandlingen ”sannolikt leder till en hög risk” i den mening som avses i förordning 2016/679*, s. 7.

Datainspektionen har tagit fram en förteckning över sådana situationer där en konsekvensbedömning är obligatorisk.[70]

Dataskyddsförordningen beskriver konsekvensbedömningens innehåll enligt följande.

> *Bedömningen ska innehålla åtminstone*
>
> *a) en systematisk beskrivning av den planerade behandlingen och behandlingens syften, inbegripet, när det är lämpligt, den personuppgiftsansvariges berättigade intresse,*
>
> *b) en bedömning av behovet av och proportionaliteten hos behandlingen i förhållande till syftena,*
>
> *c) en bedömning av de risker för de registrerades rättigheter och friheter som avses i punkt 1, och*
>
> *d) de åtgärder som planeras för att hantera riskerna, inbegripet skyddsåtgärder, säkerhetsåtgärder och rutiner för att säkerställa skyddet av personuppgifterna och för att visa att denna förordning efterlevs, med hänsyn till de registrerades och andra berörda personers rättigheter och berättigade intressen.*[71]

4.8 Analys

4.8.1 Vilka krav ställer lagstiftningen på personuppgiftsbehandling generellt och biträdets hantering specifikt?

Det första som behöver beaktas är vilka behandlingar som genomförs i molntjänsten, i detta fall Office 365. Kammarkollegiet beskriver möjlig behandling av personuppgifter i vad de kallar ”Webbaserat kontorsstöd” enligt nedan. Det är inte otänkbart att Danderyds kommun använder Office 365 enligt beskrivningen.

> *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*

[70] https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/konsekvensbedomningar-och-forhandssamrad/forteckning-konsekvensbedomning/, läst 2019-06-25.

[71] Dataskyddsförordningen, artikel 35.7.

> *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.*[72]

Behandlingarna utförs framförallt av verksamheter under kommunens personuppgiftsansvariga nämnder, men behandlingar såsom lagring, kopiering och även överföring är kan också utföras av personuppgiftsbiträdet Microsoft. En närmare analys av tjänstevillkoren kan potentiellt svara på frågan om vilka behandlingar som genomförs av Microsoft. Ett alternativ är en tydlig instruktion från kommunens nämnder medelst t.ex. PUB-avtal där det framgår vilka behandlingar som Microsoft de facto *får* genomföra.

Vidare måste varje behandling ha ett beskrivet och tydligt ändamål samt en rättslig grund. Utöver det måste förordningens grundläggande principer i övrigt följas. Det är möjligt att flera behandlingar omfattas av samma ändamål och rättsliga grund. För den här utredningen har det inte varit möjligt att analysera alla ändamål och rättsliga grunder som åberopas för personuppgiftsbehandlingarna i Office 365 utan det åligger personuppgiftsansvariga (nämnderna) att dokumentera detta i sina förteckningar. Det för med sig att det i nuläget inte går att med säkerhet säga hur Danderyds kommun hanterar personuppgifter i Office 365, eller om den hanteringen är förenlig med lagstiftningens grundläggande principer och krav på rättslig grund.

Vilka personuppgifter som förekommer i Office 365 behöver också beaktas. Då tjänsten inkluderar såväl e-post som dokumentbearbetning kan utredningen utgå ifrån att Office 365 innehåller alla slags personuppgifter, inklusive känsliga och skyddsvärda.

Kommunens nämnder är personuppgiftsansvariga i avtalsrelationen och Microsoft är personuppgiftsbiträde. För närvarande är det dock endast kommunstyrelsen som genom kommunledningskontoret har accepterat Microsofts villkor, vilket betyder att övriga nämnder saknar PUB-avtal eller annan rättsakt med Microsoft.

Det är dock möjligt att utse endast en personuppgiftsansvarig part i avtalsrelationen med Microsoft, exempelvis kommunstyrelsen. Ett sådant beslut behöver dock föregås av en utredning. Utredningen behöver ta reda

[72] Kammarkollegiets Förstudierapport Webbaserat kontorsstöd dnr. 23.2-6283-18, den 22 februari 2019, s.13–14.

på vilka behandlingar som förekommer inom ramen för avtalsrelationen med Microsoft, vilka nämnder som i nuläget är personuppgiftsansvariga för dessa samt om det är möjligt att peka ut kommunstyrelsen som ensamt personuppgiftsansvarig för all behandling i Microsofts tjänster. Alternativt om det är möjligt att utse nämnderna som gemensamt personuppgifts-ansvariga med kommunstyrelsen som huvudsakligt personuppgiftsansvarig.

Kommunens nämnder har inte tecknat kommunens PUB-avtal med Microsoft utan kommunledningskontoret har accepterat Microsofts standardiserade licensvillkor, vilket i sin tur utgör själva instruktionen till hur Microsoft får hantera kundens personuppgifter. Som jämförelse kan sägas att i kommunens PUB-avtal är det kommunens personuppgifts-ansvariga som skriver instruktionen till biträdet, inte tvärtom som blir fallet med att acceptera Microsofts villkor.

I personuppgiftsansvaret ingår att kontrollera/granska sina personuppgiftsbiträden. I Microsofts villkor framgår att de granskar sig själva enligt beskrivningen i villkoren och att kunden samtycker till det genom att acceptera nämnda villkor. Granskningsrapporterna kan tillhandahållas kunden på dennes begäran.[73]

Det är Microsoft som personuppgiftsbiträde som stiftar villkoren och inte kommunens nämnder som är personuppgiftsansvariga. Det finns en risk att notera om sådana här villkor ändras ensidigt då det gör att kommunens personuppgiftsansvariga tappar kontrollen över hanteringen, och ställer också höga krav på att personuppgiftsansvariga kontinuerligt kontrollerar villkoren. Villkoren med Microsoft ändras inte ensidigt under avtalsperioden.

Vad gäller underbiträden så anlitar Microsoft sådana och informerar om vilka det är på sin webbplats. Det framstår som kundens ansvar att kontrollera eventuella förändringar på webbplatsen.[74] På webbplatsen framgår företagets namn, vilket land det är lokaliserat i och inom vilken tjänstekategori som de kan komma att anlitas.

Licensvillkoren utgör kundens medgivande till att Microsoft får anlita underbiträden som de har behov av. I villkoren framgår att Microsoft

[73] Microsoft Online Services Terms (OST) (March 2019), s.11.

[74] https://www.microsoft.com/en-us/trustcenter/privacy/data-management/data-access, läst 2019-05-02.

meddelar kunden genom att ”uppdatera webbplatsen och förse kunden med en metod för att ta emot meddelande om uppdateringen”.[75] Mottagaren i detta fall torde vara någon eller några på kommunens IT-enhet, vilket ställer krav på att det internt finns rutiner eller styrdokument som beskriver hur sådana här ändringar ska meddelas personuppgiftsansvariga och i övrigt hanteras.

Som en jämförelse framgår det i Danderyds kommuns PUB-avtal:

> *12.2 Personuppgiftsbiträdet äger rätt att anlita ett nytt underbiträde. När Personuppgiftsbiträdet avser att anlita ett nytt underbiträde ska Personuppgiftsbiträdet säkerställa underbiträdets kapacitet och förmåga att uppfylla sina skyldigheter enligt Dataskyddslagstiftningen.*
> ***Personuppgiftsbiträdet ska skriftligen meddela den Personuppgiftsansvarige om***
>
> *1. underbiträdets namn, organisationsnummer och säte (adress och land),*
>
> *2. vilken typ av uppgifter och kategorier av Registrerade som behandlas, och*
>
> *3. var Personuppgifterna ska behandlas.*

Skillnaden mellan kommunens PUB-avtal och Microsofts villkor ligger i hur personuppgiftsbiträdet informerar om att underbiträden anlitas. Nuvarande villkor försvårar för kommunens personuppgiftsansvariga att kontrollera och eventuellt invända mot underbiträdena som Microsoft anlitar.

Det är också oklart om kommunen överhuvudtaget kan invända mot att Microsoft anlitar ett visst underbiträde, då det enda alternativet verkar vara att kommunen får säga upp den berörda tjänsten.[76]

Notera att en stor mängd underbiträden ökar risken för förlorad kontroll och därmed ökar även risken för de registrerades fri- och rättigheter, vilket kan medföra att personuppgifter hanteras på ett sätt som kommunen inte avsett.

4.8.2 Finns det några hinder för tredjelandsöverföring?

Adekvat skyddsnivå, nämnt tidigare i utredningen, kan uppnås av bolag i USA om mottagaren av personuppgifterna är ansluten till Privacy Shield, vilket Microsoft är.[77] Det betyder att så länge Microsoft håller kunddata inom sin koncern så är eventuell tredjelandsöverföring inte olaglig.

---

[75] Microsoft Online Services Terms (OST) (March 2019), s.13.

[76] IBID, s.13.

[77] https://www.privacyshield.gov/participant?id=a2zt0000000KzNaAAK&status=Active, läst 2019-03-25.

Det är dock inte utrett om all support eller hantering utförd av underbiträden till Microsoft alltid sker inom EU/EES. Om t.ex. Microsofts support får åtkomst till kunddata från ett tredjeland så är det en tredjelandsöverföring, även om kunddata geografiskt fortfarande är lokaliserad inom EU/EES.

För att undvika tredjelandsöverföringsproblematik helt bör det garanteras i avtalet med Microsoft att all support och hantering utförd av underbiträden alltid sker inom EU/EES. Det bör också undersökas närmare hur standardavtalsklausulerna påverkar frågan.

4.8.3 Hur påverkar Cloud Act?

Om Microsoft tvingas lämna ut kommunens data till tredje part[78], exempelvis brottsbekämpande utländska myndigheter, enligt utländsk lag såsom amerikanska Cloud Act, är det felaktigt utifrån dataskyddslagstiftningen. Då USA inte är ett sådant land som enligt EU-kommissionen har adekvat skyddsnivå i sin helhet innebär det att personuppgifter som överförs utanför Microsofts förvar inte längre hanteras i enlighet med dataskyddslagstiftningen.

Enligt Microsofts licensvillkor kan utlämnande av kunddata, inklusive personuppgifter, till tredje part förekomma. I villkoren framgår att Microsoft ska hänvisa till kunden i första hand, men det ges ingen garanti för att så alltid sker. Likväl framgår i villkoren att om Microsoft är förlagda med yppandeförbud enligt lag så kommer inte Microsoft särskilt att meddela kunden att ett utlämnande av kunddata har skett.[79]

Som en jämförelse framgår det i Danderyds kommuns PUB-avtal:

> *13.1 Personuppgiftsbiträdet ska säkerställa att Personuppgifterna **hanteras och lagras inom EU/EES** av en fysisk eller juridisk person som är etablerad inom EU/EES, om inte PUB-avtalets parter kommer överens om något annat.*
>
> *13.2 Personuppgiftsbiträdet äger endast rätt att överföra Personuppgifter till Tredje land för Behandling (t.ex. service, support, underhåll, utveckling, drift eller liknande hantering) **om den Personuppgiftsansvarige på förhand skriftligen godkänt sådan överföring och utfärdat Instruktioner för detta ändamål.***
>
> *13.3 Överföring till Tredje land för Behandling enligt PUB-avtalet, punkt 13.2, får endast ske om den är förenlig med Dataskyddslagstiftningen och uppfyller de krav på Behandlingen vilka ställs i PUB-avtalet och Instruktioner.*

[78] Tredje part är någon som står helt utanför avtalsrelationen mellan personuppgiftsansvarig och personuppgiftsbiträdet.

[79] Microsoft Online Services Terms (OST) (March 2019), s.9.

Kommunens PUB-avtal gör gällande att biträdet inte får hantera kommunens personuppgifter på något sätt som strider mot dataskyddslagstiftningen och instruktionerna. Danderyds kommuns personuppgiftsansvariga har dock inte tecknat kommunens PUB-avtal med Microsoft. Detta får till följd att nämnderna inte har något avtalat skydd, om Microsoft överför personuppgifter till tredje part.

I beaktandesats 115 i dataskyddsförordningen behandlas andra länders rättsordning. Beaktandesatser, eller skäl som de också kallas, är kommentarer och förtydliganden till förordningens artiklar. Beaktandesatserna gäller för såväl personuppgiftsansvarig, som för personuppgiftsbiträden. Det beaktandesats 115 gör gällande är att en lag i tredjeland enkom inte utgör sådan rättslig grund som gör överföringen av personuppgifter laglig enligt dataskyddslagstiftningen; utan överföringen måste i övrigt alltid följa gällande bestämmelser om tredjelandsöverföring.[80]

Det skulle innebära att om Microsoft lämnar ut personuppgifter till tredje part, t.ex. en utländsk rättsvårdande myndighet, så kan det möjligen tolkas som ett brott mot dataskyddslagstiftningen - oaktat vad som framgår i Microsofts villkor eller kommunens PUB-avtal. Har ett yppandeförbud meddelats, så kommer kommunen dock inte få veta att ett utlämnande till tredje land skett, varför det kan vara svårt för kommunen att agera inom ramen för sitt personuppgiftsansvar.

Det är kommunens nämnder som personuppgiftsansvariga som ansvarar för att all personuppgiftsbehandling sker i enlighet med dataskydds-lagstiftningen, inkluderat att säkerställa att anlitade personuppgiftsbiträden och underbiträden har en god efterlevnad.

5 Säkerhet - IT-säkerhet och informationssäkerhet

5.1 Författningskrav på kommunens säkerhetsarbete

Det finns en mängd författningskrav i lagar, förordningar och föreskrifter som reglerar kommunens säkerhetsarbete. Förutom krav som innebär att kommunen ska vidta säkerhetsåtgärder så förekommer också krav som alla

[80] https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/dataskyddsforordningens-beaktandesatser/, läst 2019-04-10.

handlingars offentlighet med mera som begränsar kommunens möjligheter att ta till alltför långtgående säkerhetsåtgärder.

5.2 Kommunens behov av säkerhet

Säkerheten syftar till att skydda kommunens verksamhet och ytterst till att skydda den samhällsviktiga och säkerhetskänsliga verksamhet som är kritisk för medborgare och organisationer samt, i förlängningen, för Sverige. Kommunens behov av säkerhet styrs utifrån författningskraven, men även utifrån en bredare kontext.

Även de krav som föreligger på kommunens säkerhetsarbete (exempelvis inom ramen för säkerhetsskyddslagstiftningen) baseras på att kommunen ska ha det skydd som krävs utifrån den egna verksamheten.

Därför är det viktigt att poängtera att kommunens säkerhetsarbete ska dimensioneras utifrån de skyddsvärda tillgångar som kommunen är beroende av för att kunna bedriva sin verksamhet samt föreliggande hotbild mot dessa skyddsvärda tillgångar. I slutändan är det konsekvenserna för verksamheten, om en skyddsvärd tillgång görs otillgänglig för verksamheten, som styr vilka säkerhetsåtgärder som ska vidtas.[81] Ju större skada det skulle medföra att en skyddsvärd tillgång är otillgänglig, desto starkare säkerhetsåtgärder måste vidtas för att skydda åtgärden.

5.3 Kommunens skyddsvärda tillgångar

De skyddsvärda tillgångar som finns i kommunens verksamhet definieras nedan.

5.3.1 Personer

De personer i form av medarbetare, förtroendevalda, leverantörer, besökare m.fl. som på något sätt deltar i kommunens verksamhet utgör en skyddsvärd tillgång och den kunskap och erfarenhet som dessa personer besitter är avgörande för att kommunens verksamhet ska kunna fortgå.

5.3.2 Förtroende

Att upprätthålla förtroendet för kommunens verksamhet är en skyddsvärd tillgång då mycket av kommunens verksamhet är beroende av ett förtroende från medborgare, förtroendevalda och andra myndigheter för att kunna fortgå. Detta gäller särskilt då kommunen är beroende av ett stort antal

[81] Konsekvensstyrt säkerhetsarbete. När en konsekvens inte kan accepteras ska säkerhetsåtgärder sättas in för att begränsa konsekvenserna eller sannolikheten för att den oönskade händelsen ska inträffa.

samarbeten med andra aktörer för at kunna upprätthålla olika samhällsviktiga funktioner.

5.3.3 Information

Den information som förekommer inom kommunens verksamhet utgör en skyddsvärd tillgång. Kommunens verksamhet är i mycket hög grad är beroende av tillgång till information. Att informationen är korrekt och tillgänglig när den behövs, samtidigt som den skyddas mot obehörig åtkomst, är avgörande för kommunens verksamhet. Felaktig hantering av information skulle kunna skada såväl kommunen som enskilda individer och organisationer och kunna leda till att förtroendet för kommunen skadas allvarligt. Det gör att det är viktigt att göra korrekta avvägningar kring vilka system som ska användas såväl som att användarna utbildas och att korrekta säkerhetsåtgärder nyttjas.

5.3.4 Egendom och utrustning

Kommunens egendom och utrustning i form av exempelvis fastigheter, fordon och teknisk infrastruktur samt IT-utrustning utgör en skyddsvärd tillgång. Tillgång till egendom och utrustning kan dels vara avgörande för att bedriva verksamhet till vardags, dels för att förebygga eller hantera inträffade krissituationer.

5.3.5 Ekonomiska och kulturhistoriska värden

Kommunen ansvarar även för en mängd skyddsvärden som inte är av operativ betydelse för verksamheten, men som utgör betydande ekonomiska eller kulturhistoriska värden. Det gäller exempelvis konst och kulturhistoriskt viktiga dokument i arkiv m.m. men även de tilldelade ekonomiska medel som kommunen förfogar över. Även dessa ekonomiska och kulturhistoriska värden utgör skyddsvärda tillgångar för kommunen.

5.4 Kommunens förutsättningar att bedriva säkerhetsarbete

Säkerhetsarbetet inom kommunen ska säkerställa att kommunen uppfyller gällande författningskrav och i övrigt stödja de övergripande verksamhetsmålen.

Arbetet ska bedrivas kostnadseffektivt och säkerhetsrelaterade frågor ska så långt som möjligt, hanteras i linjeorganisationen och inarbetas i ordinarie huvudprocesser, riktlinjer och rutiner.

5.5 Hotbild

Generellt har hotbilden mot Sverige i allmänhet och mot information och IT-system i synnerhet ökat de senaste åren. Detta gäller även kommuner.

Säkerhetspolisen, Försvarets radioanstalt och Försvarsmakten har i sina respektive årsrapporter vittnat om detta och även pekat ut specifika aktörer.[82]

Utredningen konstaterar att statslett cyberspionage finns överst på Säkerhetspolisens lista över hot mot Sverige kommande år.[83] Sådant spionage riktar inte endast in sig på försvarsmyndigheter utan även på kommuner och regioner, teknisk infrastruktur och mycket annat. Ett väl utvecklat informationssäkerhetsarbete är nödvändigt tillsammans med en kapacitet att tekniskt hålla den egna informationen säker mot externa angrepp från aktörer med mycket hög kapacitet.

Säkerhetspolisen pekar också på risken för cyberangrepp. Om cyberspionage syftar till att obemärkt bereda sig åtkomst till annans information så kan cyberangrepp sägas vara motsatsen där syftet snarare är att förstöra information och göra system otillgängliga. Även här bedöms aktörerna ha en mycket hög förmåga och en intention att agera och bereda sig tillträde över många år. När det gäller både angrepp och spionage så finns också en bred flora av antagonister som inte nödvändigtvis är utländskt statsstödda, men som har både kunnande och kapacitet (förmåga) att bedriva kvalificerade angrepp mot kommuner och landsting för t. ex. ekonomisk vinning. Här ska också nämnas organiserad brottslighet och politiskt- eller religiöst motiverad extremism som i olika sammanhang har intentionen att både angripa och stjäla information för många olika syften.

Vidare pekar säkerhetspolisen på manipulation av information och påverkansoperationer, även här från utländskt statsledda aktörer. Svensk förmåga att säkerställa riktigheten och tillgängligheten i sin egen information är av stor vikt när det gäller att motverka sådana påverkansförsök.

Sammantaget sker inhämtning av information och angrepp mot system genom flera, ofta samverkande, olika metoder. Det sker allt från direkt inhämtning från de källor som kommunens personal utgör, genom fysisk stöld och genom tekniska angrepp på system. Kommunens säkerhetsarbete

---

82 https://www.sakerhetspolisen.se/download/18.6af3d1c916687131f1fae5/1552543607309/Arsbok-2018.pdf och https://www.forsvarsmakten.se/siteassets/4-om-myndigheten/dokumentfiler/rapporter/must-arsoversikt-2018f.pdf

83 https://www.svt.se/nyheter/inrikes/sapo-listar-sju-hot-mot-sverige-kommande-ar

behöver beakta och möta samtliga hot och metoder för angrepp. Detta gör säkerhetsarbetet mångfacetterat och avvägningar samt bedömningar av vilken säkerhet som är mest kostnadseffektiv behöver genomföras kontinuerligt.

Sett till vilka aktörerna är[84] och vilken förmåga de har till att effektuera angrepp mot kommunens informationstillgångar och system är det viktigt och många gånger nödvändigt att samarbeta med leverantörer som har reell kapacitet att motverka hoten i fråga över tid och också följa den tekniska utvecklingen.

Det är också viktigt att poängtera att det inte är möjligt att över tid skydda sig mot alla hot fullt ut ens för landets största myndigheter, än mindre små kommuner som Danderyd.

Avvägning kan behöva göras huruvida det är mer kostnadseffektivt att i viss mån exponera viss information för hotet från amerikanska rättsvårdande myndigheter eller om samma informationsmängder ska riskera att exponeras mot organiserad kriminalitet, andra landsaktörer eller extremistiska miljöer.

Utan att i denna utredning gå in på detaljerade beskrivningar om de angrepp som kommunen utsatts för de senaste två åren så kan det konstateras att angrepp har skett och sker kontinuerligt. Där angreppen varit nära att lyckas har det hängt samman med brister i mänsklig faktor kopplat till systemhantering där säkerhetsfunktioner inte varit påslagna eller inte uppdaterade och felhantering av information. Fel som kunnat motverkas av en mer automatiserad säkerhetsfunktionalitet som erbjuds inom ramen för Office 365.

5.6 Inriktning och avgränsningar

I bedömningen av hur säker tjänsten Office 365 bedöms vara och hur tjänsten samspelar med kommunens behov av en säker informationshantering har denna utredning granskat fyra övergripande perspektiv inklusive beaktande av hotbilden mot kommunens verksamhet och information.

Det första perspektivet omfattar hur Microsoft som bolag globalt, regionalt och lokalt arbetar med att säkerställa att bolagets interna processer och

[84] Här avses de aktörer som direkt eller indirekt pekas ut som de mest aktiva hoten av svenska underrättelse- och säkerhetsmyndigheter.

rutiner borgar för att obehörig åtkomst till kundernas data inte sker inom ramen för de aktuella tjänsterna.

Det andra perspektivet har varit att granska hur tekniska åtgärder understödjer processer och rutiner för att även på detta plan minska risken för att obehörig medvetet eller omedvetet erhåller tillgång till kundernas information. Bedömning av sannolikhet att Microsofts egen personal missbrukar sina behörigheter i kombination med teknisk djupkunskap för att tillskansa sig åtkomst till stadens information görs alltså till del; dvs skydd mot kvalificerade insiderattacker.

Det tredje perspektivet har varit att granska vilka tekniska skyddsåtgärder som finns och hur väl de fungerar för att minska risken för att obehöriga hos leverantörerna och *kunderna* erhåller tillgång till information de inte ska ha tillgång till, eller medvetet eller av misstag röjer information till obehörig utanför kundernas organisationer.

Dessa åtgärder och tekniska lösningar sammanfaller också många gånger med det fjärde perspektivet, det vill säga skydd mot extern obehörig åtkomst (intrång).

Eventuell konfiguration och specifik implementation omfattas inte i detta dokument utan granskas och godkänns i särskild ordning. Med detta menas exakt hur kommunen konfigurerat sin implementation av tjänsten; vilket inte kommer att beskrivas eftersom detta ändras över tid och då konfigurering av säkerhetslösningarna är en sekretessbelagd uppgift.

5.6.1 Metod

Bedömningen har gjorts i huvudsak utifrån granskning av material som Microsoft tillhandahållit. Då Microsoft är en tjänsteleverantör som agerar på en internationell marknad och har många kunder som ställer höga krav anlitar de externa revisionsföretag för att såväl granska som certifiera sitt tjänsteutbud. Dessa tredjepartsgranskningar och certifieringar har kommit kommunen tillhanda samt varit föremål för granskning för att granskningen ska kunna göras så oberoende som möjligt. Göteborgs stad har genomfört en motsvarande granskning. Där så varit relevant har frågor och svar mellan Göteborgs stad och den svenska representationen för Microsoft nyttjats även i denna granskning.

5.7 Informationssäkerhet i Office 365

Informationssäkerhet är en viktig faktor för tilliten till molntjänster. På grund av den dominerande ställning Microsoft Windows och Microsoft

Office har på marknaden är det vanligt att angripare särskilt inriktar sig på att penetrera dessa system.

Office 365 är därför byggt från grunden för att säkerställa plattformens funktion och tillgänglighet, samt att skydda den information som lagras i plattformen mot olika typer av hot och angrepp.

Microsoft bedriver sedan många år ett omfattande säkerhetsprogram som kontinuerligt identifierar nya hot och motverkar angrepp. De senaste årens fokus på utveckling av Office 365 har även inneburit ökad transparens kring säkerhetsarbetet, samt nya funktioner som underlättar för att bygga ett säkert system som underhålls och uppdateras kontinuerligt. Samtliga kunder oavsett storlek får tillgång till plattformens grundläggande säkerhetsfunktioner.

Följande stycken ger en överblick av de säkerhetsfunktioner som finns i Office 365 och beskriver hur Danderyds kommun genom att använda dessa funktioner bedöms uppnå en högre grad av informationssäkerhet genom att nyttja plattformen jämfört med den traditionella lokala IT-driften.

5.8 Certifieringar och regelverksefterlevnad

Microsoft arbetar aktivt med certifiering av säkerheten i Office 365 och de administrativa rutiner som används i driften av plattformen.

Den är den generella säkerheten i plattformen, Microsofts administrativa rutiner och allmänna informationssäkerhetsarbete som ligger till grund för de informationssäkerhetscertifieringar Office 365 erhållit.

Verifiering av certifieringskrav samt regelverksefterlevnad gentemot några viktiga regelverk säkerställs av en oberoende part och publiceras löpande i Office 365 Service Trust Portal.[85]

Certifieringarna och verifieringarna av dessa påvisar att Microsoft hanterar information i nivå som överstiger vad Danderyds kommuns styrdokument anger för kommunen i övrigt.[86] Med hantering i detta perspektiv avses främst behörighetstilldelning i ett logiskt och tekniskt perspektiv samt skydd för det motsatta; otillbörlig åtkomst.

Sammanfattningsvis bedöms i denna utredning med den kunskap kommunen förfogar över att de certifieringar och regelverk som Office 365

[85] https://servicetrust.microsoft.com/

[86] Se Danderyds kommuns riktlinje för informationssäkerhet.

följer vara tillräckliga för att Danderyds kommun ska kunna anse att plattformen som sådan är byggd med tillräcklig säkerhet. Detta för att hantera de flesta typer av uppgifter, inklusive information som av olika anledningar är att betrakta som känslig.

5.8.1 ISO/IEC 27001

ISO/IEC 27001 är den internationella standard för informationssäkerhet som oftast används som riktmärke vid bedömning av informationssäkerhetsarbete. En certifiering ställer krav på organisation och administrativa rutiner kring informationssäkerhetsarbetet och efterlevnaden måste verifieras regelbundet för bibehållen certifiering.

Danderyds kommun saknar nödvändiga resurser för att certifiera den egna IT-verksamheten enligt ISO/IEC 27001, varför det får ses som ett bidrag till säkerhetsarbetet att Microsoft Office 365 innehar denna certifiering.

Det faktum att Microsofts hantering av Office 365 är certifierad enligt ISO/IEC 27001 innebär dock inte att samma grad av informationssäkerhet automatiskt överförs till Danderyds kommuns användning av plattformen. Danderyds kommun bär huvudansvaret för den information som hanteras i plattformen, samt att nödvändiga rutiner finns på plats för att säkerställa att hanteringen sker i linje med Danderyds säkerhetskrav. Här avses främst behörighetstilldelningen av Danderyds kommuns information till kommunens medarbetare som hanteras av kommunens IT-enhet, men där respektive förvaltning bär ansvaret för att inte tilldela behörigheter i strid mot gällande lagar och interna föreskrifter och riktlinjer.

Stickprov har genomförts av extern granskning av Microsofts efterlevnad av ISO /IEC 27001:2013 på global nivå.[87] Granskningen sammanfattas med att Microsoft i allt väsentligt kan påvisa efterlevnad i enlighet med certifieringen.

5.8.2 Övriga certifieringar och regelverk

Office 365 uppfyller också de säkerhetskrav som ställs i ett antal andra certifieringar och regelverk. Dessa är inte nödvändigtvis direkt tillämpliga på svenska kommuner, men påverkar säkerhetskraven på plattformen så att

87 https://servicetrust.microsoft.com/ViewPage/MSComplianceGuide?command=Download&downloadType=Document&downloadId=7e71ff67-7609-43e6-9d68-4ceea0b41b50&docTab=4ce99610-c9c0-11e7-8c2c-f908a777fa4d_ISO_Reports

olika typer av kundorganisationer skall kunna använda den om de är bundna av att följa dessa regelverk.

Exempelvis uppfyller plattformen kraven i FISMA, en amerikansk lagstiftning som definierar hur amerikanska myndigheter skall arbeta med informationssäkerhet. Termen ”informationssäkerhet” definieras i lagtexten som följer:

> *Skydd av information och informationssystem från obehörig åtkomst, användning, röjande, avbrott, modifikation eller destruktion för att uppnå integritet, konfidentialitet och tillgänglighet.* [88]

Definitionen är allmänt vedertagen för informationssäkerhetsarbete och beskriver Danderyds målsättning för informationssäkerhet.

Svensk lagstiftning specificerar inte lika tydliga krav på myndigheter och deras befattningshavare som FISMA, men det faktum att Office 365 uppfyller kraven visar på att plattformen är tillförlitlig och kan utgöra en pusselbit i säkerhetsarbetet snarare än en säkerhetsrisk.

Office 365 uppfyller också kraven i branschregelverk som HIPAA (amerikansk lagstiftning om hantering av hälsouppgifter) och PCI DSS (kreditkortsindustrins säkerhetsstandard för hantering av kreditkortsuppgifter).

Precis som med ISO 27001 utförs regelbundna revisioner av regelverksefterlevnaden som publiceras på Service Trust Portal för att erbjuda transparens i säkerhetsarbetet kring plattformen.

5.9 Informationslagring i Office 365

Microsoft Office 365 är en av världens mest använda publika molntjänster för kontorsstöd, det vill säga de funktioner som används dagligen olika organisationer för att hantera information digitalt. Förutom traditionella funktioner som e-posthantering och ordbehandling innehåller plattformen ett stort antal nya arbetsverktyg, främst inriktade på att underlätta samarbete kring informationshanteringen.

Gemensamt för alla verktygen är att de är byggda för att möta en ny typ av informationssäkerhetsutmaning, nämligen det faktum att den information som ska skyddas inte längre lagras i kundorganisationens egna datahallar

[88] https://www.govinfo.gov/content/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf, sida 49 (översatt från engelska)

utan istället hanteras av externa tjänsteleverantörer i stora datacenter spridda över hela världen.

När många organisationer delar utrymme inte bara i samma datahall utan även på samma hårdvara ställs mycket höga krav på säkerheten i alla nivåer från fysisk säkerhet till bakgrundskontroller av personal, val av serverhårdvara, krypteringslösningar och åtkomstkontroll.

Huvuduppgiften för de tekniska åtgärderna är att säkerställa att den information som kundorganisationerna lagrar i plattformen inte är åtkomlig för obehöriga. Misslyckas detta äventyras förtroendet för hela plattformen, vilket i praktiken innebär risk för att den blir oanvändbar.

Denna del av utredningen kommer att bedöma huruvida den tekniska säkerheten i Microsoft Office 365 är tillräcklig för att Danderyds kommun kan ha fullt förtroende för att den information kommunen lagrar i plattformen inte görs åtkomlig för obehöriga och att lagringen i övrigt sker på ett säkert sätt. En sådan bedömning bör dock inte göras utan hänsyn till vilka alternativa lösningar Danderyds kommun kan använda för informationslagring och hur säkerhetsnivån för dessa ser ut. Utredningen kommer därför även att analysera kommunens möjligheter att uppnå samma säkerhetsnivå som erbjuds i Office 365 om kommunen skulle välja att lämna plattformen till förmån för ett annat alternativ.

5.9.1 Vilka tjänster för informationshantering nyttjas i Office 365?

Danderyds kommun utnyttjar flera av tjänsterna i Office 365 för att hantera, bearbeta och lagra olika typer av information. Huvudsyftet med tjänsten är att den skall användas för den dagliga informationsbearbetningen i kommunen, där de dokument och meddelanden som hanteras lagras och bearbetas i exempelvis Exchange Online, SharePoint Online och OneDrive for Business.

Förutom dessa tjänster nyttjar kommunen också i allt större utsträckning samarbetsplattformen Teams. Teams använder en kombination av ovan nämnda tjänster för att lagra och bearbeta information.

5.9.2 Var lagras informationen?

Danderyds tenant[89] i Office 365 är knuten till den geografiska placeringen Europa, vilket innebär att den information som lagras i kärntjänsterna Exchange, SharePoint och OneDrive lagras inom EU. Informationen kan

[89] Ungefär Danderyds IT-miljö

komma att bearbetas av system utanför EU, men sådan bearbetning ska inte ändra informationens geografiska hemvist.

I det fall information lagras i OneDrive upprättas även en lokal kopia av informationen på respektive användares dator. Av detta skäl är lagringsenheterna (hårddiskarna) på användarnas datorer krypterade för att minimera risken för obehörig åtkomst om datorn hamnar utanför användarens kontroll.

Många anställda använder också e-post i sina mobiltelefoner, varför en begränsad kopia av sådan information finns lagrad i respektive mobiltelefon. Telefonerna är därför också skyddade.

5.9.3 Leverantörens hantering av Danderyds information

Eftersom Office 365 är en tjänst som tillhandahålls av en extern leverantör uppstår frågeställningar kring i vilken utsträckning leverantören bereds tillgång till Danderyds information. Villkoren för sådan informationsåtkomst regleras i kommunens licensavtal med Microsoft.

Licensavtalet samlar licensköp för alla mjukvarulicenser från Microsoft och använder olika bilagor för att reglera villkor för specifika produkter och tjänster. Avtalsvillkoren för Office 365 finns i bilagan Online Services Terms[90].

Genom villkoren i Online Services Terms förbinder sig Microsoft att hantera Danderyds information i enlighet med avtalsvillkoren.

5.9.4 Informationsägarskap

I Online Services Terms anges uttryckligen att det är Danderyd som äger all information som Danderyd lagrar i tjänsten. Microsoft gör inga anspråk på den lagrade informationen och förbinder sig att endast hantera den i sådan utsträckning som krävs för att leverera den avtalade tjänsten.

Denna deklaration kring informationsägarskapet är nödvändig för att Danderyds kommun skall kunna acceptera förhållandet att Microsoft genom Office 365 hanterar stora mängder konfidentiell information.

Det finns också juridiska anledningar för Microsoft att hålla behörigt avstånd till kundernas information då molntjänstleverantörer i allt större utsträckning utsätts för påtryckningar från olika intressentorganisationer att

[90] Senaste utgåvan av Microsofts villkorsbilagor finns på https://www.microsoft.com/en-us/licensing/product-licensing/products.

ta ansvar för den information som lagras eller presenteras genom tjänsten. Genom att inta positionen att tjänsten endast utgör en lagringsyta där Microsoft saknar insyn kan Microsoft skjuta över ansvarsfrågor kring den lagrade informationen till Danderyds kommun. Exempelvis är det Danderyds kommun som ansvarar för att informationslagring i tjänsten inte bryter mot upphovsrätten.

5.9.5 Förfrågningar från rättsvårdande myndigheter

Vid förfrågningar från rättsvårdande myndigheter om tillgång till kundens information förbinder sig Microsoft i Online Services Terms att hänvisa den efterfrågande myndigheten att vända sig direkt till kunden med sin begäran. Om Microsoft ändå på grund av lag tvingas lämna ut information till rättsvårdande myndigheter förbinder sig Microsoft att meddela kunden att så har skett, förutsatt att inte även meddelandet i sig är förbjudet enligt lag (yppandeförbud).

En majoritet av dessa förfrågningar rör information i Microsofts konsumenttjänster. Under första halvåret 2018 inkom inga förfrågningar efter information tillhörande svenska organisationer.[91]

Microsoft har aktivt och konsekvent drivit frågan om informationsägarskap och molnleverantörens roll i förhållande till rättsvårdande myndigheter i ett antal amerikanska rättsfall[92], då frågan är central för att bibehålla förtroendet för plattformen. Det ska dock noteras att det kan ha förekommit förfrågningar och utlämningar som inte är kända för Microsofts kunder.

5.9.6 Administrativ åtkomst till Danderyds information

I enlighet vad som avtalas i Online Services Terms ansvarar Microsoft för att åtgärda eventuella problem som uppstår i den tekniska funktionen i Office 365.

Detta ansvar innebär att Microsofts supporttekniker kan komma att behöva administrativ åtkomst till Danderyds information för att lösa tekniska problem där informationen orsakar problemet, exempelvis vid datakorruption.

---

[91] Molntjänster och säkerhet: https://news.microsoft.com/sv-se/2018/12/13/molntjanster-och-sakerhet/

[92] Microsoft beskriver detta arbete i följande bloggpost: https://blogs.microsoft.com/on-the-issues/2018/04/03/the-cloud-act-is-an-important-step-forward-but-now-more-steps-need-to-follow/

Det är mycket ovanligt att denna typ av problem uppstår i Office 365. Danderyds kommun har inte upplevt någon incident där detta behov har uppstått under den tid Office 365 använts i kommunen.

5.10 Skydd mot obehörig åtkomst

Office 365 innehåller flera olika mekanismer som samverkar för att säkerställa att obehöriga inte kan komma åt den information som lagras i systemet. Följande stycken avhandlar de viktigaste områdena och jämför dessa mot traditionell hantering, vilket är det alternativ som finns till Office 365.

5.11 Identitetshantering och behörighetskontroll

Grunden i allt skydd mot obehörig åtkomst är att kunna skilja de som är *behöriga* från de som är *obehöriga*. I den digitala världen sker detta genom att de fysiska personer som arbetar med informationen tilldelas digitala identitetshandlingar som används för att få tillgång till information i systemet.

På grund av bredden i den kommunala verksamheten behöver kommuner hantera digitala identiteter som representerarar många olika kategorier av användare. En vanlig indelning är att hanteringen av identiteter för kommunens anställda och elever i skolan sköts olika, men även externa utförare av kommunal verksamhet kan behöva tillgång till kommunens system.

Det finns många fördelar med att centralisera hanteringen av digitala identiteter så att det finns en huvudsaklig identitetskälla. Alla system där behörighetskontroll krävs kan då använda det centrala identitetssystemet för att verifiera användarnas identitet innan de får åtkomst till systemet. För att detta ska fungera är det viktigt att det centrala systemet är åtkomligt från de anslutna systemen, samt att systemet stöder standardprotokoll för användarautentisering (användaridentifiering). Det gör att användare endast behöver logga in en gång för åtkomst till flera system till exempel.

Danderyds digitaliseringsenhet har beslutat att använda Microsofts Azure Active Directory som centralt identitetshanteringssystem, men sköter än så länge skapandet av identiteter i kommunens lokala Active Directory. De digitala identiteterna skapas lokalt hos Danderyds kommuns digitaliseringsenhet och synkroniseras sedan till Microsofts Azure Active Directory, varefter de används för att styra åtkomst till exempelvis Office 365. Azure Active Directory används också för att styra åtkomst till de interna system som publiceras genom funktionen Azure Application Proxy,

som erbjuder anställda och externa utförare säker åtkomst till systemen utan att man behöver vara ansluten till Danderyds interna nätverk. Genom att använda inbyggda funktioner i Azure och Office 365 sparar kommunen resurser som annars hade gått åt till att licensiera, administrera och underhålla lokalt hanterade system.

5.11.1 Multi-faktorautentisering

Azure Active Directory har även möjlighet att avkräva användarna ytterligare uppgifter än lösenord vid autentisering, så kallad multi-faktorautentisering. Denna funktion utgör idag ett nödvändigt skydd för att förhindra att angripare tillskansar sig åtkomst till kommunens system genom att tillskansa sig lösenordet till någon av kommunens identiteter. Det är möjligt, men inte i sammanhanget kostnadseffektivt, att implementera en liknande funktion i lokal drift.

5.11.2 Övervakning, intrångsskydd och villkorsstyrd åtkomst

Azure Active Directory innehåller ett antal övervakningsfunktioner som aktivt bidrar till att höja säkerheten i användarautentiseringen. Bland annat spårar systemet alla inloggningar och upptäcker automatiskt misstänkt aktivitet, exempelvis om en användare är inloggad från olika geografiska platser samtidigt. Systemet kan då automatiskt blockera användarens åtkomst.

Genom att samla inloggningar från många olika kunder i molntjänsten får också Microsoft betydligt bättre möjligheter än en lokal IT-avdelning att tidigt upptäcka angrepp på systemet och hantera dem automatiskt. Då förmågan att upptäcka misstänkta inloggningsmönster är starkt beroende av den totala mängden inloggningar som hanteras är det inte möjligt att uppnå samma resultat i lokal drift då inloggningsvolymerna är avsevärt lägre.

Med hjälp av villkorsstyrd åtkomst kan säkerheten i plattformen anpassas granulärt efter skyddsbehovet i de anslutna systemen. Funktionen gör det möjligt att endast tillåta åtkomst vid vissa tider, från vissa platser, enheter och många andra alternativ som krävs för att erbjuda medarbetarna god tillgänglighet *och* säkerhet.

5.11.3 Säkerhetskrav och jämförelse med lokal drift

Flera av dessa funktioner är så tekniskt avancerade att de inte går att implementera i lokal drift med mindre än att kommunen själv utvecklar sådan funktionalitet. I vissa fall finns färdiga tredjepartsprodukter att tillgå, men bedömningen är att det inte går att motivera kostnaden för att licensiera dessa i jämförelse med den inbyggda funktionaliteten i Azure Active

Directory. Övervakningen av en sådan lösning skulle också behöva skötas av egen personal, dygnet runt, för att motsvara vad som erbjuds i Azure. Kommunen saknar för närvarande intern kompetens och resurser för att hantera detta.

Användning av Azure Active Directory är därmed viktigt för att erbjuda fullgod säkerhet vid inloggning och åtkomstkontroll enligt de behov kommunen identifierat.

5.12 Hantering av administrativa behörigheter

Ett inbyggt informationssäkerhetsdilemma som gäller för alla digitala system är att *minst* en fysisk person behöver tilldelas fullständiga behörigheter för att hantera skötseln av systemet och dela ut de mer begränsade behörigheter som tilldelas de vanliga användarna och begränsade administratörer. I normalfallet hanteras behovet genom att ett så kallat administratörskonto skapas då systemet sätts upp, som sedan används för att skapa ytterligare digitala identiteter som i sin tur kan tilldelas behörigheter efter behov. För att förhindra att all åtkomst styrs av en enskild person är det vanligt att minst två personer har tillgång till administratörskonton med fulla behörigheter i systemet.

Eftersom de personer som har fullständiga behörigheter styr behörighetstilldelningen kan de alltid bereda sig själva tillgång till all information som lagras i systemet. Ur ett strikt åtkomstperspektiv är det därmed omöjligt att helt förhindra varje teknisk möjlighet för de som är administratörer att komma åt informationen. Det är därför av yttersta vikt att administrativa behörigheter begränsas i så stor utsträckning som möjligt, samt att de fysiska personer som har tillgång till administratörskonton är pålitliga. Användningen av administrativa behörigheter bör också följas upp genom tydlig loggning som i efterhand kan granskas.

Vid användning av tjänster från externa leverantörer uppstår frågeställningar kring leverantörens administrativa behörigheter i systemet. Eftersom det är oundvikligt att leverantören har någon form av administrativ behörighet för att kunna underhålla och uppdatera systemet är det viktigt att det på avtalsnivå regleras hur leverantören får utnyttja dessa behörigheter för åtkomst till kundens information och övriga data. Danderyds kommun använder andra system utöver Office 365 där tredje part har administrativ åtkomst av nödvändighet. Problemet är dock inte begränsat till externa leverantörer. Även den interna IT-avdelningens administratörer har möjlighet att komma åt information som de inte är behöriga att se, vilket är

relevant kopplat till kraven på att myndigheter inte får röja sekretessbelagd information till obehöriga även om den egna IT-personalen omfattas av anställningens tystnadsplikt. I praktiken arbetar alla myndigheter med egna rutiner för att säkerställa att de egna administratörerna inte överskrider sina befogenheter när de hanterar sekretessreglerad information. Det är dock, i praktiken, inte säkert att dessa rutiner alltid är formaliserade på samma nivå som ett leveransavtal med en extern tjänsteleverantör kan vara.

5.12.1 Administrativa behörigheter i Office 365

Microsoft sköter driften av Office 365 och har därmed administrativa behörigheter i systemet. Dessa begränsas dock automatiskt för att i största möjliga grad undvika att dessa administratörer får tillgång till kunddata.

Kunden får själv tillgång till ett administratörskonto med behörigheter i den egna miljön och kan därefter skapa ytterligare identiteter i systemet för att därefter styra åtkomsten till kunddata enligt egna önskemål.

Detta innebär att de tillfällen då Microsoft uppgett att de utnyttjar sina administrativa behörigheter begränsas till underhåll och uppdateringar, samt i undantagsfall vid supportförfrågningar från kunden.

5.12.2 Administrativ åtkomst till kunddata vid supportförfrågningar

Om ett problem uppstår i systemet och orsaken bedöms bero på fel (exempelvis korruption) i kunddata kan Microsofts tekniker behöva åtkomst till aktuell data för att åtgärda problemet.

Administrativ åtkomst till kommunens information i Office 365 för Microsofts supporttekniker hanteras då genom ett behörighetssystem kallat ”Lockbox”. Syftet med systemet är att begränsa Microsofts tillgång till kommunens data i samband med support och automatisera hanteringen av de behörigheter som krävs för att lösa problemet. I korthet innebär ”Lockbox” att:

- Ingen fysisk person har stående administrativa behörigheter till kunddata. Administrativa behörigheter skapas istället vid behov.
- En tidsbegränsad administrativ identitet som tilldelas exakt de behörigheter som krävs för att lösa det problem som kunden har rapporterat genereras om behov uppstår.
- All åtkomst i systemet loggas och görs tillgänglig för kommunen så att hanteringen kan spåras i efterhand.

Processen för tilldelning av administrativ åtkomst genom Lockbox ut som följer:

1. Kunden kontaktar Microsoft Support för att begära hjälp med ett problem.
2. Om Microsofts supporttekniker bedömer att administrativ åtkomst till kunddata krävs för att avhjälpa problemet skickar teknikern en begäran om åtkomst till kunddata till Lockbox-funktionen. Begäran inkluderar en tidsgräns för åtkomsten på maximalt fyra timmar.
3. Via Lockbox inspekterar en supportchef hos Microsoft teknikerns begäran om åtkomst för att säkerställa att teknikern inte begärt högre åtkomst än nödvändigt. Supportchefen godkänner teknikerns begäran om den bedöms vara korrekt. Om begäran inte godkänns tilldelas teknikern ingen behörighet och kunden informeras om beslutet.
    a. Om funktionen ”Customer Lockbox” används skickas en begäran om godkännande även till kommunen. Kommunen kan på detta vis även inkludera egen personal i godkännandeförfarandet.
4. Efter godkänd begäran genererar Lockbox en temporär administrativ identitet till teknikern, som tilldelas de specifika behörigheter som godkänts i begäran.
5. Teknikern loggar in i systemet från en för ändamålet dedikerad administrationsdator för att åtgärda problemet. Teknikerns arbete loggas för att säkerställa full spårbarhet i arbetet. Arbetsloggen är tillgänglig för granskning av kunden.
6. Den temporära administrativa identiteten tas bort automatiskt när tidsgränsen för godkännandet går ut. Detta innebär att tekniker som mest kan ha åtkomst till kundens data i totalt fyra timmar. Om problemet inte är löst efter denna tid måste teknikern skicka en ny begäran om åtkomst för att kunna fortsätta arbetet.

Microsoft har fokuserat på att bygga förtroende för de säkerhetsrutiner som skyddar kundens data vid utformningen av Lockboxfunktionen. En viktig grundprincip för Office 365 är att Microsoft inte ska ha kännedom om vilken information kunden hanterar i plattformen[93], varför det blir extra viktigt att all hantering där Microsoft behöver beröra kunddata sker på ett så säkert och begränsat sätt som möjligt.

[93] Framgår på Microsofts hemsida

5.12.3 Alternativet ”Customer Lockbox”

Kunden kan välja att licensiera och aktivera en extra funktion som utöka Lockboxfunktionen genom att introducera ett extra godkännandesteg där en representant för kommunen också måste godkänna teknikerns begäran om åtkomst innan den administrativa identiteten skapas.

Begäran om godkännande från kommunen skickas till en av kommunen specificerad e-postadress.

Customer Lockbox[94] ger därmed en möjlighet för kunden att särskilt godkänna åtkomst till kunddata om ett sådant behov uppstår. Om ett godkännande inte har givits inom 12 timmar avslås begäran automatiskt.

Det extra godkännandesteg som introduceras genom Customer Lockbox ger kunden inblick och beslutsmandat vid behov av åtkomst till kundens information i det aktuella supportärendet. I de fall där ett befintligt internt eller externt regelverk kräver en sådan hantering är funktionen nödvändig för regelefterlevnad.

I praktiken är det dock ovanligt med krav på denna typ av strikt åtkomstkontroll, eftersom den kräver utökade administrativa resurser hos kunden och introducerar hinder för att snabbt kunna avhjälpa eventuella problem.

Den e-postadress som begäran om åtkomst skickas till måste övervakas kontinuerligt då ett supportärende har skickats till Microsoft. Om den person som förväntas godkänna åtkomstbegäran inte är insatt i ärendet krävs också att det är möjligt att snabbt och enkelt utreda frågan internt hos kunden för att ett eventuellt godkännande inte ska bli godtyckligt.

Eftersom Microsoft inte kan hjälpa till att lösa inrapporterade problem om åtkomstbegäran avslås är det svårt att tänka sig något scenario där ett avslag är aktuellt i praktiken. Oavsett vem som slutligen godkänner åtkomsten till kunddata är kommunen ändå tvungen att granska och analysera de loggar som visar vad supportteknikern gjort i systemet för att säkerställa att allt gått rätt till.

Danderyds kommun har aktiverat Customer Lockbox i den nuvarande konfigurationen av systemet. Under den tid som funktionen varit aktiv har inga supportärenden skickats till Microsoft som krävt åtkomst till kunddata.

---

[94] Funktionen Customer Lockbox beskrivs ingående på https://docs.microsoft.com/en-us/Office365/admin/manage/customer-lockbox-requests

Då systemet har varit i drift under ett par år konstaterar denna utredning att det är mycket ovanligt att Microsoft behöver komma åt kunddata i supportärenden.

5.12.4 Administrativa behörigheter i den egna supportorganisationen

I de allra flesta fall där användare behöver support hanteras problemet av kommunens egen supportorganisation. Det är då någon av kommunens It-tekniker som behöver administrativa behörigheter för att kunna lösa problemet, vilket även gäller för de system som sköts lokalt.

I den lokala miljön saknas dock ofta möjligheten att automatiskt tilldela rätt behörighet temporärt, vilket innebär en risk att teknikerna istället tilldelas höga behörigheter permanent. Samma dilemma gäller då externa leverantörer av system i lokal drift behöver åtkomst för att underhålla sina respektive system.

Det är resurskrävande att utveckla en lösning motsvarande Lockbox i den lokala miljön, varför detta inte har prioriteras. Microsofts hantering av administrativa behörigheter vid support och underhåll framstår därför som säkrare än vad kommunen själv har möjlighet att åstadkomma.

5.13 Kryptering av information

En viktig komponent för att skydda information mot obehörig åtkomst är att den krypteras så att endast de som har tillgång till kryptonycklarna har möjlighet att tolka informationen även om den hamnar i orätta händer.

Alla krypteringsfunktioner som används i Office 365 är godkända enligt den amerikanska federala krypteringsstandarden FIPS 140–2, vilket är ett krav för att amerikanska myndigheter skall kunna använda tjänsten. De faktiska kryptografiska funktionerna som inkluderas i standarden överensstämmer med de funktioner MSB rekommenderar för svenska myndigheter[95]. Office 365 har alltså erkänd kryptering.

Kryptering av information inom Office 365 appliceras på flera olika nivåer, vilka presenteras i separata stycken nedan.

[95] Myndigheten för Samhällsskydd och Beredskap, ”Vägledning för grundläggande kryptering”, utgåva 0.94, januari 2019, sid 52

5.13.1 Kryptering vid informationsöverföring

För att den som arbetar med information ska kunna komma åt den, behöver informationen överföras från den plats där den lagras till den enhet där användaren vill arbeta med den. Överföringen sker oftast utan att en användare noterar det, till exempel när en fil hämtas från en lokal filserver, eller när användaren nyttjar en webbläsare för att arbeta i ett webbaserat informationssystem. I Office 365 kommunicerar också olika servrar med varandra för att skapa det innehåll användaren ser.

Den som vill komma över Danderyds information kan alltså försöka avlyssna eller omdirigera informationen när den överförs mellan användaren och Office 365 eller mellan olika servrar i plattformen. För att motverka sådana attacker förses betrodda servrar med certifikat som används för att verifiera att servern verkligen är den enhet kommunikationen är avsedd för.

All kommunikation mellan de servrar som Office 365 nyttjar sker krypterat genom standardprotokollen IPsec och TLS. Kommunikation mellan servrar och användare sker också krypterat med TLS[96].

Microsoft underhåller serversidan av tjänsten så att servrarna stöder den senaste och mest säkra versionen av TLS.

5.13.2 Certifikatinfrastruktur för verifiering av serveridentiteter

Office 365 använder en egen certifikatinfrastruktur som administreras genom verktyget ”SSL Admin”. Certifikaten använder 2048-bitars nyckellängd och kan endast ges ut till publika IP-adresser som ägs av Microsoft. Säkert utgivna certifikat är en förutsättning för att säkerställa att kommunikation inom och till Office 365 endast sker till de servrar som Microsoft har identifierat som tillhörande tjänsten.

Certifikatinfrastrukturen som används i Office 365 uppdateras i takt med nya tekniska krav och förändringar i hotbilden och bedöms vara tekniskt säker. Motsvarande system finns även i lokal drift, dock med lägre grad av automatisering.

5.13.3 Kryptering av lagrad information

De lagringsytor där information finns sparad bör vara krypterade för säkerställa att obehöriga inte kan läsa informationen om själva lagringsmediet blir stulet. Förutom ren hårddiskkryptering går det att

[96] Övergripande information om krypteringen i Office 365 finns på: https://docs.microsoft.com/en-us/Office365/securitycompliance/encryption

kryptera själva filerna för att höja säkerheten ytterligare. Danderyds kommun nyttjar sådan kryptering i form av krypteringstjänsten ”Bitlocker”.

SharePoint Online, som är den centrala informationslagringstjänsten i Office 365, är byggt för att kryptera all information i flera nivåer. SharePoint Online sköter lagringen för flera andra tjänster, som Teams och OneDrive.

All serverhårdvara som används i Office 365 krypteras med Microsofts krypteringsfunktion Bitlocker. Detta säkerställer att all information som sparas på hårddisk i lösningen är krypterad. Förutom Bitlocker krypteras också alla filer som lagras i SharePoint Online individuellt med 256-bitars AES nycklar. Filerna delas upp i olika segment som lagras på olika slumpmässigt valda platser i Azure storage[97]. För att hålla reda på hur en given fil ska sättas ihop sparas data om vilken bit som lagrats var i en separat databas kallad Content Database. Databasen är i sin tur också krypterad med funktionen Transparent Data Encryption (TDE), som skyddar både databasen och dess transaktionsloggar från obehörig åtkomst.

Krypteringsnycklarna som använts för krypteringen sparas separat i en så kallad ”Key Store”.

För att dekryptera informationen krävs samverkan mellan Azure storage, Content Database och Key Store. En angripare måste alltså lyckas ta kontroll över alla tre komponenterna för att komma över den skyddade informationen[98].

I jämförelse med de skyddsmekanismer som vanligen omgärdar filer på exempelvis en traditionell filserver där Danderyds kommun själv sköter driften bedöms skyddet i Office 365 vara väsentligt högre. Om kommunen önskar, går det att använda egna krypteringsnycklar för filkrypteringen även i Office 365, men det kräver att kommunen har en organisation och kompetens för att underhålla nyckelhanteringen på ett säkert sätt. Detta innebär också en försämring av funktionalitet i tjänsterna.

[97] Azure storage är den underliggande lagringstjänst som används av SharePoint Online för att lagra filer

[98] Informationsskyddet i SharePoint Online och OneDrive beskrivs ingående i Microsofts systemdokumentation. https://docs.microsoft.com/en-us/Office365/securitycompliance/data-encryption-in-odb-and-spo

5.14 Azure Rights Management

Azure Rights Management används för att kontrollera vad den som öppnar ett dokument kan och får göra med innehållet. Exempelvis kan utvalda användare få behörighet att läsa innehållet i en fil, men inte kopiera eller vidarebefordra det. Skyddet appliceras på filnivå genom kryptering, vilket innebär att det följer med filen var den än lagras. Funktionen är en viktig del i att göra Danderyds kommuns informationsklassificeringsmodell enkel att applicera för kommunens medarbetare.

Då funktionen också har inbyggt stöd i Officeprogrammen är den mycket svår att ersätta med något annat alternativ.

5.15 E-postkryptering

Genom Office 365 Message Encryption (OME) kan e-postmeddelanden krypteras så att de inte kan läsas av obehöriga. Funktionen kan antingen aktiveras manuellt av den som skickar ett e-postmeddelande och önskar skydda det, eller automatiskt om innehållet i meddelandet är klassificerat som känsligt. Om ett skyddat e-postmeddelande är adresserat till en mottagare utanför Office 365 skickas det inte heller via det traditionella protokollet SMTP. Mottagaren får istället ett e-postmeddelande med en säker länk som leder till Office 365. På detta vis behöver meddelandet aldrig skickas i klartext över internet för att nå mottagaren utan finns kvar i Office 365.

OME är en mer lätthanterad lösning för e-postkryptering än traditionell S/MIME teknik, som också stöds i Office 365. S/MIME kräver relativt omfattande nyckelhantering och rekommenderas därför endast i de fall där avsändare och mottagare av e-post kräver ömsesidig verifiering av varandras identitet.

5.15.1 Krypteringsmöjligheter i lokal drift

Danderyds kommun har begränsade möjligheter att erbjuda motsvarande kryptering som Office 365 i den lokala driften. Detta beror till största delen på att många av de komponenter som ingår i Office 365 är byggda med modernare teknik, exempelvis datalagringen i SharePoint Online eller möjligheten att enkelt kryptera e-postmeddelanden.

Precis som med identitetshanteringen finns i vissa fall tredjepartslösningar som kan bidra till att skapa liknande funktionalitet, men dessa behöver i så fall licensieras, implementeras och underhållas för att erhålla önskad funktionalitet. Till detta saknas kompetens och resurser, varför denna utredning bedömer att det är nödvändigt för Danderyds kommun att utnyttja

Office 365 för att uppnå ett fullgott kryptografiskt skydd för kommunens information.

5.16 Automatiserad systemhantering och driftsäkerhet

En stor del av effektiviteten i publika molntjänster ligger i den höga grad av automatisering som är möjlig att uppnå med standardiserade tjänster. Den automatiska systemhanteringen är en förutsättning för att tjänsterna ska fungera förutsägbart och driftsäkert. En bieffekt av automatiseringen är också att informationssäkerheten höjs, då det är färre människor som behöver administrativa behörigheter för att sköta systemen. Automatiserade funktioner minimerar också risken för handhavandefel i administrationen och att människor oavsiktligt tar del av information de inte är behöriga till.

5.16.1 Automatisering i Office 365

I Office 365 sköts hela den initiala konfigurationen av kundens miljö (även kallad *tenant*) automatiskt. Det administratörskonto som skapas för att kunden ska kunna administrera sin miljö tilldelas ett automatiskt genererat lösenord som endast kunden känner till. Det finns därmed ingen fysisk person hos Microsoft som har tillgång till administratörskontot.

De flesta systemunderhållsåtgärder som utförs i Office 365 är också helt automatiserade. Syftet med automatiseringen är att höja säkerheten och så långt som möjligt eliminera situationer där Microsofts personal behöver hantera kunddata.

5.16.2 Driftsäkerhet

Automatiseringen av Office 365 är också en starkt bidragande orsak till systemets höga tillgänglighet och driftsäkerhet. Microsofts servicenivåavtal för Office 365-tjänster garanterar en tillgänglighet över 99,9% för samtliga tjänster. Brister i tillgängligheten mäts normalt i antal användarminuter som tjänsten inte är tillgänglig under en faktureringsperiod.

I jämförelse med de servicenivåer Danderyds kommun har kapacitet att uppnå i den lokala driften bör Office 365 ses som ett mycket driftsäkert system. Office 365 övervakas exempelvis dygnet runt årets alla dagar, vilket skulle medföra mycket stora personalkostnader att motsvara i den lokala driften. Det innebär även vissa utmaningar att mäta driftsäkerheten i en lokal organisation där det saknas specialiserade system för detta ändamål.

Många IT-organisationer arbetar aktivt med att automatisera den lokala driften i så stor utsträckning som möjligt. Automatiseringen ger stora

fördelar, men kräver också initialt stora resurser när den ska sättas på plats och underhållas.

Danderyds IT-organisation saknar idag de resurser som krävs för en effektiv automatisering av den lokala IT-miljön. Att bygga upp en lämplig organisation internt bedöms kräva ytterligare 1–2 heltidsanställda samt återkommande extern experthjälp till stöd för förvaltningen.

Då IT-organisationen tvingas prioritera bland många nödvändiga insatser förefaller det strategiska valet att satsa på att utnyttja den färdigpaketerade automatiseringen i Office 365 för att höja driftsäkerheten vara effektivt ur ett säkerhetsperspektiv. Kostnadsmässigt kan det konstateras att den automatisering som erbjuds i Office 365 till stor del inkluderas i det ordinarie licenspriset för hela plattformen, vilket ska vägas mot alternativet att bygga upp en egen organisation internt med de utmaningar och kostnader detta skulle innebära.

5.17 Analys och bedömning

Utifrån ett informationssäkerhetsperspektiv kan man ställa sig följande frågor:

- Vem är behörig att ta del av en myndighetsinformation?
- När och hur sker åtkomsten och för vilken information?

För att svara på dessa frågor behöver det klarläggas vilken information myndigheten faktiskt hanterar och hur rutinerna kring informationshanteringen fungerar.

De flesta myndigheter avsätter en betydande del av sina resurser till att upprätthålla den tydlighet kring dokumentation av beslut och processer som följer av offentlighetsprincipen inom svensk förvaltning.

Förtroendet för myndighetens verksamhet är beroende av att myndighetens informationshantering uppfyller de traditionella informationssäkerhetskraven på *riktighet*, *tillgänglighet*, *konfidentialitet* och *spårbarhet*. För att lyckas fullt ut med informationssäkerheten krävs goda rutiner kring säkerhetsarbetet som är väl etablerade i verksamheten (tekniskt såväl som logiskt).

Säkerhetsarbete innebär ofta en ambition att begränsa tillgängligheten till information. En utmaning för myndigheter kopplat till konfidentialitet är dock att eventuella säkerhetsåtgärder inte skall stå i vägen för offentlighetsprincipens krav på öppenhet och insyn. Korrekt hanterat utgör

säkerhetsarbetet eller snarare de mekanismer som skyddar information intill dess att det är klarlagt genom sekretessprövning om den kan lämnas ut eller publiceras, alternativt att det finns grund för att begränsa tillgången till den genom sekretessbeläggning. Detta enligt principen att en handling eller informationsmängd kan anses vara öppen först när den inte bedöms innefatta något som är sekretessreglerade eller sekretessbelagt.

Till skillnad från privata organisationer kan myndigheter heller inte frånsäga sig ansvaret för att hantera viss information, trots att hanteringen kan innebära betydande utmaningar i det vardagliga arbetet. Detta blir särskilt tydligt i det fall informationen är sekretessbelagt, vilket ligger till grund för den diskussion kring ”röjandeproblematiken” vid användning av molntjänster som genomlyses tidigare i utredningen.

Det bör påpekas att risk att obehöriga tar del av information gäller generellt för all informationshantering i myndigheter. Genom att ensidigt beakta riskerna kopplade till informationshantering i molntjänster utan hänsyn till alternativen riskerar det övergripande säkerhetsarbetet att bli lidande. Detta särskilt då informationssäkerhetsarbetet med att skydda information även måste ta hänsyn till kvalificerade hotbilder som inkluderar aktörer med avsevärd kapacitet att tillförskansa sig information de inte har rätt till.

Hotbilden mot svenska myndigheters information har också förändrats i takt med att moderna och automatiserade verktyg för angrepp har blivit tillgängliga även för icke statsdrivna aktörer.

Det är därför av vikt att det är den samlade säkerhetsbedömningen som ligger till grund för de beslut som fattas kring en myndighets informationssäkerhetsrutiner för att myndigheten ska kunna uppfylla de krav som författningar *och* hotbilden ställer. Då det är vanligt att konflikt uppstår mellan två eller flera säkerhetsintressen behöver myndigheten ofta göra en bedömning av vilket intresse som väger tyngst innan beslut om lämplig hantering kan fattas.

Det är sådana överväganden som ligger till grund för att säkerhetsarbetet i Danderyds kommun har resulterat i valet att hittills frångå den traditionella, lokala hanteringen till förmån för molntjänsten Office 365 som huvudsaklig bearbetningsplattform för kontorstjänster. Detta dock med svagheten att valet av tjänst endast beaktat det säkerhetsmässiga perspektivet.

Den funktionalitet för effektiv digitalisering som systemet erbjuder i kombination med de säkerhetslösningar som medföljer bedöms

sammantaget vara dem som ger mest kvalificerat *skydd* mot de flesta förekommande hoten både i dag och i nära framtid då Microsoft kontinuerligt utvecklar sin tjänst och framförallt säkerhet förekommande och bedömda framtida hot. Säkerhetslösningarna bedöms ligga på en nivå som kommunen inte har kapacitet att uppnå vare sig med avseende kompetens eller resurser i form av investeringsbudget.

- Danderyds kommun bör dock säkerställa att alternativ finns för de informationsmängder som bedöms vara särskilt utsatta kopplat till amerikansk lagstiftning av typen Cloud Act.
- Danderyds kommun bör säkerställa att man har egen backup på information i kommunens konton för att säkerställa tillgång till information.
- Kommunen bör etablera rutiner för övervakning av säkerhetsfunktioner och loggar.

Då den normala informationsproduktionen i de flesta verksamheter innebär att det kan vara svårt att särskilja vilka dokument som innehåller sekretessreglerade och sekretessbelagda uppgifter bör utgångspunkten i informationssäkerhetsarbetet alltid vara att skydda samtliga uppgifter mot obehörig åtkomst *som om* de vore sekretessreglerade. Detta blir också tydligt när vissa informationsmängder inledningsvis kan innefatta sekretess under en viss tid för att därefter klassas som offentliga och ej sekretessreglerade.

Ur ett säkerhetsperspektiv bedöms Office 365 kunna rekommenderas för hantering av Danderyds kommuns samtliga informationssäkerhetsklasser utom det som omfattas av säkerhetsskyddslagstiftningen. Rekommendationen gäller intill dess att staten[99] utrett innebörden av hantering i av sekretessreglerad, sekretessbelagd eller på annat sätt känslig information i en molntjänst i allmänhet och i en amerikansk molntjänst i synnerhet. Ytterligare en faktor som kan påverka bedömningen är om Microsoft kan erbjuda sina kunder egen hantering av krypteringsnycklar på sikt, men med bibehållen funktionalitet i tjänsten.

Att nyttja ett kontorsstödssystem som endast kan nyttjas för öppen information är inte rimligt då alternativ som innefattar motsvarande säkerhet inte enkelt kan tillhandahållas för de tillkommande alternativ som då skulle behövas.

[99] Genom tillsynsmyndighet eller på annat sätt.

Sammantaget gör denna utredning bedömningen att Office 365, med de säkerhetsfunktioner som finns tillgängliga för kommunen och hur dessa kontinuerligt hålls uppdaterade mot hotbilderna, är det *säkerhetsmässigt* mest kostnadseffektiva kontorsstödssystemet som finns tillgängligt för Danderyds kommun.

6 Utredarnas analys och rekommendationer

Denna utredning har klarlagt om det finns betänkligheter utifrån offentlighets- och sekretesslagen att lagra Danderyds kommuns information i en molntjänst. Denna utredning har utrett om kommunen har stöd för utlämnandet av sekretessbelagda uppgifter till Office 365 och Microsoft och funnit att kommunen måste göra bedömningen att 10 kap. 2 § offentlighets- och sekretesslagen är tillämplig, och att det är *nödvändigt* för kommunen att lämna ut dessa uppgifter, för att stöd ska finnas för ett utlämnande till Office 365 och Microsoft. I förarbetena och av flera instanser förespråkas en restriktiv hållning och att det är tveksamt om en molntjänstlösning verkligen kan vara nödvändig.

Utredningen har vidare undersökt om utlämnandet annars, om 10 kap. 2 § offentlighets- och sekretesslagen inte bedöms tillämplig, utgör ett röjande av sekretessbelagda uppgifter. Utredningen har funnit att det med stöd i rättsfall om straffansvar vid grov oaktsamhet, finns visst stöd för att även om en molntjänstleverantör rent tekniskt skulle kunna ta del av den sekretessreglerade och sekretessbelagda informationen i molntjänsten, är informationen inte röjd så länge det inte går att *räkna med* att någon obehörig tar del av uppgifterna. I vart fall inte på ett sådant sätt att *straffansvar vid grov oaktsamhet* skulle utgå. För brott mot tystnadsplikten räcker det dock att någon är oaktsam. Möjligen talar rättsfallen för att kommunen har att räkna med att Microsoft kommer ta del av uppgifterna i samband med support och via administrativa behörigheter. Samtidigt är det ovanligt att support sker i kommunens data vilket kan tala för att kommunen inte har att räkna med att Microsoft tar del av uppgifterna. Det går inte att säga om och hur ofta administrativa behörigheter tar del av kommunens data, men sådan möjlighet finns. Vidare har utredningen funnit att ett avtal om tystnadsplikt med molntjänstleverantören inte kan läka om en grund för utlämnande saknas. Finns dock en grund för utlämnande till molntjänstleverantören, är det bättre att ingå ett avtal om tystnadsplikt, än att inte göra det (även om ett sådant avtal inte kan innebära tystnadsplikt vid straffansvar).

I jämförelse med en alternativ lösning med till exempel egen server då en extern tekniker servar systemet, eller en svensk molntjänstlösning då leverantören har administrativa behörigheter och vidtar support, så uppstår samma röjandeproblematik som vid globala molntjänster (ännu beaktas inte Cloud Act). Även med ett alternativ som innebär att kommunen använder egen server med intern tekniker (intern drift) finns en problematik då systemet i princip alltid kan kräva extern support. I samtliga fall krävs då en grund för utlämnande av sekretessbelagda uppgifter, med ett liknande resonemang. Den externa parten omfattas inte av offentlighets- och sekretesslagen, precis som i fallet med Microsoft. Problematiken är alltså inte unik för molntjänstlösningar, utan uppstår i princip mer eller mindre oavsett vilket alternativ för kontorsstödsystem som används. Utifrån detta är det nödvändigt för kommunen att i vart fall göra någon form av utlämnande enligt 10 kap. 2 § offentlighets- och sekretesslagen, utifrån de förutsättningar kommunen har och de alternativ för kontorsstödssystem kommunen har till hands.

Denna utredning har funnit att säkerheten i många fall är bättre i Office 365, än i andra alternativ. Tillräcklig säkerhet för kommunens information är en förutsättning för att verksamheten ska kunna fullgöras. I anledning av detta har utredningen även övervägt om det, utifrån en säkerhetsaspekt, inte är nödvändigt att lämna ut informationen för att kommunen ska kunna fullgöra sin verksamhet, jfr. 10 kap. 2 § offentlighets- och sekretesslagen? Det är märkligt att säkerhetsaspekten inte belysts tydligare i andra uttalanden, särskilt i diskussionen kring 10 kap. 2 § offentlighets- och sekretesslagen, om ett utlämnande kan vara nödvändigt för att myndigheten ska kunna fullgöra sin verksamhet.

Utredningen har vidare utrett om Cloud Act och liknande regelverk kan medföra att utlämnandet också utgör ett röjande av sekretessbelagda uppgifter. Denna utredningen har funnit att Cloud Act och andra liknande regelverk kan utgöra ett röjande av sekretessbelagda uppgifter, *om* uppgifterna lämnas ut. Sannolikheten att uppgifterna lämnas ut av Microsoft till amerikanska eller andra utländska myndigheter bedöms i dagsläget med viss försiktighet som låg. Detta innebär att risken för att kommunen röjer sekretessbelagda uppgifter med viss försiktighet får bedömas som låg. Om så sker, kan det utgöra ett brott mot tystnadsplikten. Notera likväl att eSam

menat att uppgifterna får anses vara röjda då det inte är osannolikt att uppgifterna kan lämnas till utomstående.[100]

Sammantaget finns, utifrån offentlighets- och sekretesslagen, främst två betänkligheter att hantera information i en global molntjänst enligt följande.

- Finns grund för utlämnande av sekretessbelagda uppgifter till Microsoft? Denna betänklighet uppstår även i vid alternativa lösningar för kontorsstödssystem i mer eller mindre utsträckning. Utifrån detta, och utifrån att säkerheten är fundamental för kommunens informationshantering har denna utredning övervägt om det ändå inte är nödvändigt att lämna ut informationen med stöd i kap 10 kap. 2 § offentlighets- och sekretesslagen, utifrån de förutsättningar som kommunen har.
- Finns risk för utlämnande enligt Cloud Act och andra regelverk? Ja, risken finns men bedöms med viss försiktighet som låg. Lämnas sekretessbelagda uppgifter ut kan det utgöra ett brott mot tystnadsplikten.

Denna utredning har utrett vidare om det finns betänkligheter med att behandla personuppgifter i en molntjänst utifrån ett dataskyddsperspektiv. Generellt så finns inga problem med molntjänster så länge dataskyddslagstiftningen efterlevs. Molntjänstleverantörer utgör nästan alltid personuppgiftsbiträden till personuppgiftsansvariga. Det är därför viktigt att biträdets hantering av personuppgifter regleras medelst PUB-avtal eller annan rättsakt. Det är också viktigt att säkerheten är anpassad efter personuppgifternas art.

I det specifika fallet för den här utredningen, Office 365 och Microsoft, framkommer att Microsoft är ansluten till Privacy Shield. Det betyder i korthet att Microsoft omfattas av adekvat skyddsnivå enligt EU-kommissionens regelverk och därmed utgör behandling av personuppgifter i Microsofts tjänster inte en olaglig tredjelandsöverföring. Problematik uppstår dock om Microsoft lämnar ut personuppgifter till rättsvårdande myndighet i tredjeland på grund av t.ex. Cloud Act och därmed möjligen inte följer dataskyddslagstiftningen. Det är vidare osäkert om de underbiträden som Microsoft anlitar i tredjeland omfattas av samma adekvata skyddsnivå som Microsoft själva. Om de inte omfattas av samma skydd skulle det innebära en olaglig tredjelandsöverföring när Microsoft

[100] eSams rättsliga uttalande den 23 oktober 2018, dnr. VER 2018:57.

anlitar sådana underbiträden, vilket i förlängningen kan leda till personuppgiftsincidenter.

Danderyds kommun består av flera personuppgiftsansvariga (varje nämnd är personuppgiftsansvarig). I dagsläget är det dock bara kommunstyrelsen som har någon form av rättsakt med Microsoft (klausuler och bilagor i licensvillkoren kan sägas utgöra sådan rättsakt som är tillämplig istället för PUB-avtal). Övriga nämnder saknar motsvarande reglering. Rättsakten är skriven av Microsoft själva, vilket möjligen utgör ett problem då de ensidigt kan ändra villkoren och kommunens personuppgiftsansvariga därmed lämnar ifrån sig kontrollen över personuppgiftshanteringen till biträdet.

Utredningen gör bedömningen att Microsoft möjligen inte följer dataskyddslagstiftningen om de lämnar ut personuppgifter till tredje part enligt utländsk lag, oberoende av vad som framgår i Microsofts villkor. Personuppgiftsansvariga bör känna till detta. Den eventuella konflikten mellan dataskyddslagstiftningen och Cloud Act eller liknande regelverk är inte rättsligt prövad, såvitt utredningen känner till. Det kan noteras att samtliga myndigheter som använder globala molntjänster där leverantören träffas av Cloud Act eller liknande regelverk, ställs inför samma svårigheter, även om endast en liten del av molntjänsten nyttjas såsom t.ex. e-post.

Om Danderyds kommun ämnar fortsätta använda Office 365 i den utsträckning som görs idag måste följande uppfyllas.

- Det måste upprättas avtal/instruktioner från kommunens personuppgiftsansvariga (nämnderna) till Microsoft som reglerar att Microsoft inte får anlita underbiträden i tredjeland och att de inte får lämna ut personuppgifter till tredje part.
    - T.ex. genom att använda kommunens PUB-avtal med bilagor.

Skulle avtal/instruktioner enligt ovan inte vara möjligt bör kommunen överväga att kontakta Datainspektionen för samråd utifrån frågeställningen huruvida Microsoft följer dataskyddslagstiftningen om de lämnar ut uppgifter till tredje part enligt utländsk lag, och vad det i förlängningen innebär för personuppgiftsansvariga i Danderyds kommun.

Ett alternativ skulle kunna vara att kommunen slutar behandla personuppgifter i Office 365. Detta skulle eliminera alla risker inom dataskydd som denna utredning har lyft. En sådan hantering skulle likväl medföra en rad svårigheter och skulle inte vara praktiskt möjlig att efterleva.

Omfattande administrativa och potentiellt kostsamma åtgärder behövs då vidtas internt. Sammantaget, mot bakgrund av ovan, är det varken rimligt eller önskvärt med en sådan hantering.

På sikt behöver kommunen, om Office 365 fortsätter att användas i samma utsträckning som idag, se över följande.

- Utreda vilken nämnd som är personuppgiftsansvarig för vilka behandlingar i Office 365.
- Inventera personuppgiftsbehandlingar som görs i Office 365 och dokumentera dem i nämndernas förteckningar.
- Genomföra en konsekvensbedömning utifrån artikel 35 dataskyddsförordningen om nödvändiga åtgärder enligt ovan inte genomförs.

Denna utredning har avslutningsvis utrett om Microsofts grundsäkerhetsnivå är tillräcklig för att skydda informationen i molntjänsten och om Danderyd nyttjar och tillämpar relevanta säkerhetslösningar. Utredningen har kommit fram till att molntjänstens säkerhetsfunktioner och kvalitén i dessa är en av flera förutsättningar för att bedriva ett effektivt säkerhetsarbete sett till skydd mot kvalificerade antagonistiska hot. Sett till att konsekvensen för att information röjs, kapas, ändras eller görs otillgänglig genom ett angrepp ställs behovet av att kunna nyttja Microsofts hela uppsättning av säkerhetslösningar mot risken att utländsk lagstiftning under vissa förutsättningar ger andra rättsvårdande myndigheter tillgång till begränsad omfattning av Danderyds data (utlämnandeproblematiken).

Med detta utrett, finner utredning att nedan redovisade riskreducerande åtgärder, måste vidtas för höja kraven på Office 365 och Microsoft:

- Kommunen bör ingå tydliga avtal med molntjänstleverantören om att inga obehöriga ska få tillgång till myndighetens data. Kommunen bör rimligen få möjlighet att påverka vilka underleverantörer som hanterar kommunens data eller få garantier för att dessa underleverantörer har adekvat skyddsnivå (t.ex. är anslutna till Privacy Shield).

Därutöver får nedan redovisade åtgärder anses utgöra minimikrav.

- Utreda möjligheten att implementera säkerhetsfunktioner som möjliggör loggning och kontroll över vem som har givits åtkomst till personuppgifter i Office 365, såväl internt som externt.

- De loggningsfunktioner som finns tillgängliga i tjänsten ska nyttjas.
- Rutiner för intern granskning av loggningsfunktionen ska dokumenteras.
- Säkerhetsfunktioner införs som reglerar leverantörens möjligheter att ta del av kommunens information.
- Handlingar måste klassificeras och att en anpassad säkerhetslösning och hantering utifrån handlingens klassificering finns.
- Säkerställa att huvudleverantören har tecknat avtal avseende personuppgiftsbiträde med sina underleverantörer.
- Besluta om gallrings- och rensningsrutiner samt hur dessa ska verkställas (t.ex. manuellt eller automatiskt).
- Förberedelser ska göras för att kunna ta hem informationen om behov uppstår eller om ett bättre alternativ än Office 365 identifieras.
- Backuplösning ska säkerställas, som garanterar kommunens tillgång till sin information.
- Bevaka möjligheter att implementera säkerhetsåtgärder såsom kryptering där Danderyds kommun äger krypteringsnyckeln för att än säkra upp att obehöriga inte kan komma åt känsliga personuppgifter.
- Ta fram instruktioner, rutiner och andra stöddokument som underlättar för anställda att göra rätt.
- Ta fram styr- och stöddokument som reglerar hur personuppgiftsansvarig ska kontrollera att personuppgiftsbiträdet hanterar personuppgifter i enlighet med dataskyddslagstiftningen.

Cloud Act och liknande regelverk har främst intresse av att få ut uppgifter om enskilda individer (för amerikanska brottsutredningar). Denna typ av uppgifter ska, i övervägande fall, hanteras i andra verksamhetssystem än Office 365.

Utredningen har övervägt vad som skulle hända om uppgifterna skulle lyftas hem till egen server och funnit att det kommer vara svårt för kommunen att upprätthålla samma säkerhetsnivå, som finns i Office 365, utan att pådra sig omfattande kostnader. T.ex. skulle personal behöva anställas och säkerhetssystem anskaffas. Som denna utredning redogjort för har Microsoft god säkerhet.

Denna utredning noterar också att kommunen har utsatts för försök till intrång av kvalificerade aktörer som velat komma åt uppgifter i kommunens system ofta, vilket framkommer bland annat genom loggar, men även via

information från Microsoft. Ett skydd mot dessa angrepp är en förutsättning för en fungerande verksamhet. En lösning som innebär sämre säkerhet rekommenderas inte.

Utredningen gör bedömningen att risken för att obehöriga genom angrepp kommer åt information är en större risk än ett utlämnande via Cloud Act. Med en sämre säkerhet skulle risken för intrång och angrepp från statsaktörer, organiserad brottslighet eller motsvarande utgöra ett större hot mot den skyddsvärda informationen.

Röjandeproblematiken bör ställas i relation till säkerhetsvinsterna, att sekretessbelagd information inte röjs till obehörig vid angrepp eller oaktsamhet.

6.1 Rekommendation

Denna utredning har utrett lämpligheten i att använda Office 365 som kontorsstödssystem utifrån ett juridik-, dataskydds- och säkerhetsperspektiv. Danderyds kommun använder sen år 2017 Office 365. Därför blir utgångspunkten för den fortsätta rekommendationen vilka alternativ som kommunen nu har till hands och vad det skulle innebära att frångå Office 365. Denna utredning har funnit att även andra lösningar med egen server, svensk molntjänstlösning med mera, mer eller mindre, är förenade med vissa brister ur ett röjande- och säkerhetsperspektiv. Andra alternativ innebär sannolikt ökade kostnader.

Med ovan som utgångspunkt lämnar utredningen rekommendation att kommunen kan fortsätta använda Office 365 för sin informationshantering, exklusive för sekretess som rör Sveriges säkerhet, och i övrigt i enlighet med gällande säkerhetsriktlinjer.

För att det ska vara möjligt att fortsätta använda Office 365 på det sätt som det används idag krävs att minst, men inte begränsat till, att tidigare redovisade riskreducerande åtgärder vidtas. Vidare ska kommunen säkerställa att följande åtgärder kontinuerligt vidtas:

- Fortsatt omvärldsbevakning av uttalanden eller ställningstaganden av relevanta myndigheter.
- Fortsätt riskbedömning mot beaktande av framtida uttalanden, ställningstaganden och förändrad hotbild.
- Bevaka att Microsofts lösningar står i paritet med gällande lagstiftning, hotbild med mera.

- Genomförande av tidigare angivna riskreducerande åtgärder i utredningen för att höja kraven på Office 365 och Microsoft.
- Aktivt söka möjligheter i andra alternativa lösningar som borgar för hög säkerhet och som möjliggör legal efterlevnad.

Notera att Office 365 med försiktighet kan användas för bearbetning av känsliga personuppgifter och sekretess, men det ersätter inte de verksamhetssystem som kommunen normalt har för hantering av dessa uppgifter inom kärnverksamheten. De systemen ska även i fortsättningen användas framför Office 365. Office 365 ska aldrig användas för långtidslagring av personuppgifter och sekretess efter att bearbetningen är klar.