Uppdrag tillämpningsregler molntjänst Office 365

Beslutad 2021-03-23—24 § 38, av: Regionstyrelsen

REGION JÄMTLAND HÄRJEDALEN

Sammanfattning

Ett uppdrag har givits till informationssäkerhetsgruppen om att ta fram beslutsunderlag för tillämpningsregler för hur regionen ska använda tjänsterna i Microsoft Office 365-plattformen (nedan kallad ”O365”). Uppdragsgivare är regionstabschef. En förutsättning i uppdraget var att utgå från den utredning som genomförts av Danderyds kommun. Informationssäkerhetsgruppens bedömning är att, även om Danderyds kommuns utredning kan finnas som en grund, behöver Region Jämtland Härjedalen, som personuppgiftsansvarig och informationsägare, göra ett ställningstagande och fatta beslut utifrån egna underlag och bedömningar. I arbetet har därför aspekter såsom juridiska förutsättningar samt säkerhetsmässiga krav belysts. Grundprinciperna i dataskyddsförordningen och något av de rättsliga grunderna ska vara uppfyllda för att regionen ska kunna hantera personuppgifter. De lagliga grunderna är rättslig förpliktelse, allmänt intresse och avtal. Regionen har därmed laglig grund för behandling av personuppgifter. Att behandla personuppgifter i O365 som är en molntjänst innebär ett utlämnande av personuppgifter och strider därmed mot nuvarande lagstiftning. Microsoft som leverantör kan komma åt och begära ut dessa uppgifter (enligt Cloudact).

Med utgångspunkt att Region Jämtland Härjedalen redan använder O365, och utifrån de alternativa kontorsstödssystem som finns till hands, lämnar informationssäkerhetsgruppen rekommendationen att O365 kan fortsätta användas för öppen och intern information i klass 0-1 inklusive ”personuppgifter bas”. Informationsklass 2 ska som utgångspunkt inte hanteras i O365, men kan i vissa fall göra det efter särskild risk- och konsekvensanalys samt komplettering med tekniskt skydd (MIP). Sekretessuppgifter som rör Sveriges säkerhet (så kallad säkerhetsskyddsklassificerad information), hälso- och sjukvårdsuppgifter, och övriga information i klass 3 ska inte hanteras i O365.

O365 ska inte ersätta de verksamhetssystem som regionen normalt har för hantering av uppgifter inom kärnverksamheten. De systemen ska även i fortsättningen användas framför O365. O365 ska aldrig användas för långtidslagring av sekretessreglerade och sekretessbelagda uppgifter samt personuppgifter efter att bearbetningen är klar. Regionstyrelsen (som personuppgiftsansvariga) bör fatta beslut om detta.

I uppdraget har riskreducerande åtgärder identifierats som rekommenderas vidtas för regionens fortsatta informationshantering i O365. Informationsklassning samt hanteringsregler utifrån klassning behöver utarbetas och tillämpas i O365, vilket bedöms som den högst prioriterade åtgärden att införa. Kopplat till klassning föreslås det tekniska skyddet MIP tillämpas i O365 genom regelstyrning och kryptering. Regionens dokumenthanteringsplan ska tillämpas även i O365 och behöver förtydligas i nuvarande riktlinjer för informationshantering i O365.

Förslag ges också om att förbättringar som bör genomföras avseende backuphantering som kompletterar O365-tjänsternas inbyggda lagringsfunktioner, releasehantering av applikationer i tjänsteplattformen, loggning och logguppföljning, gallring samt möjlighet att upptäcka om känsliga personuppgifter hanteras i O365

INNEHÅLL

1 Bakgrund

Microsoft Office 365 (nedan förkortat ”O365”) är i drift i Region Jämtland Härjedalen sedan 2018. Plattformen är helt molnbaserad och omfattar flera tjänster som redan är inarbetade och nödvändiga verktyg i daglig drift för samtliga verksamheter.

De fördelar som ofta anförs med O365 är sänkta kostnader (till följd av att färre resurser behövs för drift och att on-premise-licenser blir allt dyrare), högre säkerhet (eftersom det är svårt att matcha ledande molntjänstföretag gällande uppnådd säkerhet i tjänsterna) och ökad effektivitet genom bättre funktioner för samarbete (till exempel genom att flera medarbetare kan redigera ett dokument samtidigt). Dessa fördelar kommer genom att Microsoft erbjuder O365 som en molntjänst.

O365 som molntjänst innebär också att all data som regionen lägger upp i tjänsten behandlas i Microsofts datacenter som finns utanför regionens lokaler (och istället i datacenter inom EU och i tredje land). Detta innebär att Microsoft som tjänsteleverantör, liksom andra tjänsteleverantörer av molntjänster, kan komma åt regionens data, som till exempel e-post, chattkonversationer och filer som lagras på olika delningsytor.

Det faktum att plattformen är helt molnbaserad och dessutom ägs av amerikansk leverantör leder till utmaningar inom juridik, informationssäkerhet och dataskydd (person-uppgiftshantering).

1.1 Uppdraget och syfte

Informationssäkerhetsgruppen tilldelades i november 2020 ett uppdrag att utarbeta ett beslutsunderlag på tillämpningsregler för O365. Dessa ska enligt uppdragsgivaren baseras på en utredning som genomförts i Danderyds kommun, vilken legat till grund för deras ställningstagande i frågan. En annan utgångspunkt som angavs i uppdraget var att Region Jämtland Härjedalen inte själva kan ha bättre säkerhet än leverantören. Vidare angavs i uppdraget att Cloud Act inte ska anses som hindrande utifrån att Cloud Act tillkom som en möjlighet att förhindra terrorism samt att det finns en mängd instanser att passera om en sådan begäran skulle ankomma regionen.

I uppdraget ska också klargöras vilken beslutsnivå i regionen som ska fatta beslut om tillämpningsreglerna. Underlaget och beslutet ska inte omfatta molntjänster generellt utan avser specifikt O365.

Uppdraget har genomförts av dataskyddsombud, dataskyddshandläggare, informations-säkerhetssamordnare, IT-säkerhetsansvarig, och beredskapschef. Uppdragsgivare är Regionstabschef och uppdraget ska återrapporteras till Regiondirektör.

Underlaget syftar till att belysa vilka tillämpningsregler som krävs för en säker informationshantering i O365 för regionens verksamheter samt att ge svar på följande frågeställningar:

- Vilka är de primära riskerna med att använda O365 och vilka skyddsåtgärder ska tillämpas för att få en acceptabel risknivå?

- Vilken typ av information får hanteras respektive inte hanteras i O365-tjänsteplattformen?

- Hur kan regionen säkerställa att endast kartlagda/kända/godkända tjänster används i O365-tjänsteplattformen?

- Hur säkras och dokumenteras att regionens användning av O365 sker enligt gällande lagar och regelverk?

En förutsättning i uppdraget var att utgå från den utredning som Danderyds kommun genomförde 2019, se Referens 1, avseende laglighet i användningen av O365 inom deras kommun. Sammanfattningsvis verkar utredningen från Danderyds kommun ge stöd för att det inte utgör ett röjande av sekretessbelagda uppgifter att hantera dessa i en molntjänst. Deras utredning konstaterar att eSam och E-delegationen menar att utlämnandet till O365 och Microsoft inte utgör ett röjande om det antingen finns ett tydligt förbud för leverantören att ta del av informationen, eller det är osannolikt att så sker.

Även om Danderyds kommuns utredning kan finnas som en grund, behöver Region Jämtland Härjedalen, som personuppgiftsansvarig och informationsägare, göra ett ställningstagande och fatta beslut utifrån egna underlag och bedömningar. En kommentar till Danderyds kommuns slutsats kring att utlämnandet till O365 och Microsoft inte utgör ett röjande, är att personalen hos Microsoft t.ex. i samband med support har möjlighet att ta del av kommunens data, Microsoft har alltid administrativa behörigheter som kommer åt data. Det kan tala för att de sekretessreglerade och sekretessbelagda uppgifterna i O365 ändå skulle kunna anses vara röjda.

Det som också tillkommit efter att Danderyds kommun genomförde sin utredning är att ”Privacy Shield” har upphävts och ogiltighetsförklarats av EU-domstolen (det s.k. SchremsII-målet).

Därav har en genomgång av de legala förutsättningarna ändå gjorts och sammanfattats inom ramen för detta arbete. Som grund till de hanteringsregler och skyddsåtgärder som föreslås har en enklare risksammanställning gjorts, se Bilaga 1.

2 Juridiska aspekter

I många fall upptäcks de juridiska aspekterna när ett beslut, om att migrera till en molntjänst som t.ex. O365, redan har fattats eller, ännu senare, när tjänsten har implementerats i verksamheten. Nedan följer dessa juridiska aspekter vid införande av en molntjänst.

2.1 Röjande-begreppet, Offentlighet- och sekretesslagen (2009:400)

När Region Jämtland Härjedalen hanterar uppgifter i O365 innebär det att regionen röjer uppgifterna eftersom de tillgängliggörs till tjänsteleverantören (Microsoft). Detta gäller oavsett om omständigheterna när uppgifterna tillgängliggjordes tjänsteleverantören var sådana att man – t.ex. pga. kryptering eller annan teknisk säkerhetsåtgärd – inte måste ha räknat med att tjänsteleverantören eller någon annan utomstående skulle

komma att ta del av uppgifterna. Uppgifterna är röjda enligt offentlighets- och sekretesslagen (2009:400) eftersom ett utlämnande är en form av röjande.

2.2 Dataskyddsförordningen

Eftersom data som hanteras i O365 omfattar personuppgifter gäller dataskydds-förordningen ("GDPR") med omfattande krav på åtgärder och risk för höga sanktionsavgifter vid regelbrott. Utöver Dataskyddsförordningen finns ett flertal speciallagar som kan bli tillämpliga beroende på typ av verksamhet och typ av data som hanteras i tjänsten. I grunden finns Offentlighets- och sekretesslagen ("OSL") som styr hur offentliga verksamheter ska hantera sekretessbelagda uppgifter. Då Regionens utgångspunkt är att sekretessbelagd information enligt OSL inte ska hanteras i O365, har tyngdpunkten i denna översyn lagt på personuppgiftsbehandling.

Dataskyddsförordningen föreskriver att överföring av personuppgifter till ett tredjeland bara får ske under förutsättning att det aktuella tredjelandet säkerställer en adekvat skyddsnivå för dessa uppgifter. I avsaknad av ett sådant beslut om adekvat skyddsnivå får en sådan överföring endast äga rum om den personuppgiftsansvarige har vidtagit lämpliga skyddsåtgärder. Dessa åtgärder kan bland annat kan utgöras av standardiserade dataskyddsbestämmelser som antas av EU-kommissionen, och under förutsättning att det finns lagstadgade rättigheter och effektiva rättsmedel för de registrerade. Ett sådant rättsmedel i tredjelandet USA har tidigare varit ramverket ”Privacy Shield” (en mekanism för självcertifiering kopplad till amerikanska leverantörer av molntjänster).

En särskild risk som aktualiseras med användning av O365 är överföring av personuppgifter till USA. Denna risk har ökat avsevärt efter EU-domstolens dom i mål C-311/18 ("SchremsII-målet") som säger att personuppgifter inte längre lagligen kan överföras till USA (eller behandlas med åtkomst från USA) med stöd av Privacy Shield-ramverket.

En vanlig missuppfattning är att användning av O365 inte innebär en behandling av personuppgifter varför det därför inte skulle kunna förekomma några tredjelands-överföringar när tjänsten används. Mot bakgrund av den vida definition som finns av begreppet personuppgift är det dock omöjligt att använda tjänsten utan att behandla personuppgifter då även IP-adresser, logguppgifter och information i Active Directory utgör personuppgifter.

En annan vanlig missuppfattning är att personuppgifter måste lagras i ett tredjeland för att det ska räknas som överföring. Som tredjelandsöverföring räknas dock även när en person som befinner sig i ett tredjeland får åtkomst till personuppgifter som lagras inom EU/EES. När Microsofts personal kommer åt personuppgifter som lagras inom EU/EES innebär detta alltså en tredjelandsöverföring enligt reglerna i GDPR.

Den del av verksamheten som ansvarar för ett IT-system eller digital tjänst (lösning) ska kunna påvisa korrekt och laglig behandling av personuppgifter (lagefterlevnad, compliance) enligt Dataskyddsförordningen (för tillsynsmyndighet, de registrerade samt PuA, dvs. nämnd-/bolag) men med fördel även internt (för interna controllers, internrevisor m.fl.).

Sammantaget uppfyller Region Jämtland Härjedalen kraven för personuppgiftshantering enligt Dataskyddsförordningen.

Rättsakten som regionstyrelsen har med Microsoft är skriven av Microsoft själva, vilket möjligen utgör ett problem då Microsoft ensidigt kan ändra villkoren (dock, enligt Microsofts

egna uppgifter, inte utan att meddela regionen) och regionens personuppgiftsansvariga på så sätt lämnar ifrån sig kontrollen över personuppgiftshanteringen till personuppgiftsbiträdet.

När en personuppgiftsansvarig eller ett personuppgiftsbiträde behandlar personuppgifter genom användning av utrustning som finns i tredjeland utgör det en överföring av personuppgifter till tredjeland. Det saknar betydelse hur lång eller kort tid som utrustningen används, och om uppgifterna är krypterade eller pseudonymiserade. Det är ändå fråga om personuppgifter och en överföring av sådana uppgifter.

2.2 Cloud Act

Cloud Act (Clarifying Overseas Use of Data) är en amerikansk lag som innebär att amerikanska myndigheter ska ges tillgång även till data som lagras utomlands och att amerikanska leverantörer av det skälet inte kan vägra lämna ut sådana data. Lagen trädde i kraft 23 mars 2018. Cloud Act ger amerikanska myndigheter rätt att få ut information, som har anknytning till amerikanska myndigheters brottsutredningar, direkt från molntjänst-leverantörer i amerikansk ägo.

Cloud Act innebär att amerikanska staten nu får möjlighet att kräva ut större mängder data som också sannolikt innebär tillgång, läsning och utlämning av europeiska medborgares data.

Microsoft, som levererar O365, är ett amerikanskt bolag. Det medför att uppgifter som lagras i O365-tjänsterna kan begäras ut med stöd i Cloud Act och andra liknande regelverk, utan att regionen först ges möjlighet att göra en sekretessprövning eller få kännedom om att ett utlämnande kommer att ske eller redan har skett.

Region Jämtland Härjedalen kan därmed alltså inte själva pröva ett utlämnande av information från O365. Ett utlämnande kan ske inom ramen för Cloud Act via leverantören till amerikanska myndigheter vilket ligger utanför Regionens kontroll. Risken för att detta skulle ske bedöms försiktigt som låg.

2.3 Privacy Shield

Privacy Shield är en amerikansk mekanism för självcertifiering av molntjänstleverantörer. Den 16 juli 2020 meddelade EU-domstolen dom i det så kallade Schrems II-målet. Domstolen slår fast att Privacy Shield-avtalet mellan EU och USA inte ger ett tillräckligt skydd för personuppgifter när dessa förs över till USA. Giltigheten för Privacy Shield mellan EU-kommissionen och USA upphävdes därmed med omedelbar verkan eftersom avtalet stred mot GDPR och tre artiklar i EU-stadgan.

Ogiltigförklarandet av Privacy Shield innebär att det inte längre är tillåtet för personuppgifts-ansvariga i EU att med Privacy Shield som grund överföra personuppgifter till amerikanska molntjänstleverantörer.

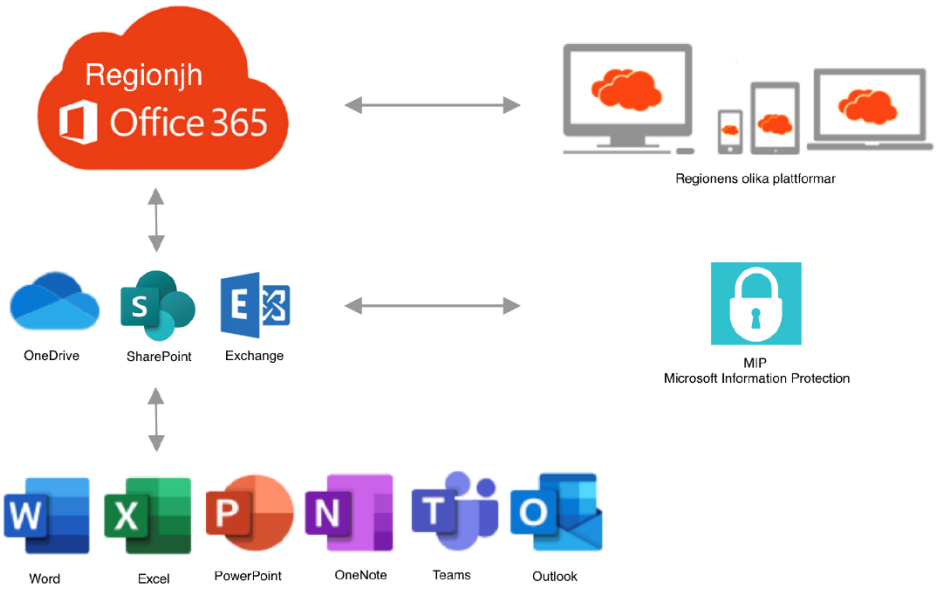
Kontentan är att om en svensk myndighet överför personuppgifter med stöd av Privacy Shield, är detta sedan 16:e juli 2020 en olaglig överföring. Med nuvarande lagstiftning begår regionen regelbrott och riskerar därmed att Integritetsskyddsmyndigheten utdömer viten och sanktionsavgifter.

2.4 Övriga juridiska aspekter

Ytterligare en juridisk aspekt är att användningen av en molntjänst som O365, medför att handlingar riskerar att bli allmänna vid en tidigare tidpunkt än de är avsedda att bli eller annars hade blivit. När en användare exempelvis använder delade dokument i tjänstens olika plattformar finns en risk att handlingen anses expedierad (och upprättad) av den myndighet som lagt upp dokumentet och inkommen hos den andra myndigheten utan att så är avsikten.

Regionen ska också ta hänsyn till reglerna i arkivlagen om bevarande av handlingar. Det ska finnas tydliga regler om vem som fattar beslut om gallring av dokument i O365. Om enskilda medarbetare raderar eller lagrar dokument som ska bevaras i enlighet med arkivlagen bör regionen säkerställa att dokumenten finns tillgängliga för medborgarna i enlighet med Tryckfrihetsförordningen.

3 Tjänster som ingår i O365



Region Jämtland Härjedalen använder O365 sedan 2018 och systemskissen ovan visar de applikationer och lagringsytor som ingår i basutbudet av O365. Det finns många fler flera applikationer i O365, men i detta uppdrag har bedömning utgått från basutbudet.

Det är komplicerat att följa alla flöden i O365. En grund är därför att välja ut de delar som lagrar information. Lagringsytorna i O365 är OneDrive (för personlig lagring), SharePoint är en yta för att lagra och dela dokument med andra och Exchange online är mailservern där mailboxar för varje konto lagras och används av Outlook-klienten.

Microsoft information protektion, MIP. Är ett skydd som går ut på att lägga på kryptering alternativt regelstyrning på en viss typ av data i O365. Detta förklaras vidare under punkt 6.3.

3.1 Microsoft molndesign för offentlig sektor

Microsoft släppte i december 2020 ett koncept med en samling förhållningssätt som benämns ”Microsoft molndesign för offentlig sektor” i syfte att offentlig sektor att kunna använda O365 på ett ”säkert” sätt.

I korthet innebär detta koncept en ”paketering” av redan tillgängliga skyddsfunktioner i O365. Denna paketering består av verktyg, mallar, regler/policys, rapporter och utbildningar som ska tydliggöra hur molntjänsterna ska konfigureras och användas för att uppfylla regleringar och lagkrav för offentlig sektor i Sverige. Exempel på regleringar/lagar som omfattas är dataskyddsförordningen/GDPR och Offentlighets- och sekretesslagen (OSL).

Sammanfattningsvis kan sägas att inga nya tjänster har lanserats i samband med konceptet. Microsoft molndesign för offentlig sektor förändrar eller underlättar heller ingenting inom de legala förutsättningarna, däremot förtydligas ansvarsförhållanden mellan leverantör och kund. Det påtalas till exempel att kunden är informationsägare och att de som leverantör ansvarar för t ex teknisk säkerhet.

4 Lagringsytor

O365 är inte avsett för att vara lagringsplats för handlingar som ska diarieföras eller arkiveras. Sådana handlingar ska dokumenteras i Region Jämtland Härjedalens godkända ärende och dokumenthanteringssystem. O365 ska betraktas som arbetsverktyg där dokument får skapas och lagras under den tiden som de utgör ett arbetsmaterial. De medger också lagring av övriga dokument och handlingar som kan anses vara av ringa värde, tex dubbletter av handlingar där myndigheten redan har ett arkivexemplar eller en tillfällig lista i Excel.

Det är den enskilde medarbetarens ansvar att känna till eller ta reda på värdet av de uppgifter som medarbetaren behandlar dvs, om det är offentligt eller är sekretesskyddat information, om informationen innehåller extra skyddsvärda uppgifter eller känsliga personuppgifter. Behovet av att använda O365:s lagringstjänster regleras av medarbetarens uppdrag.

Det finns redan regionövergripande dokumentstyrningsregler (RS/1060/2018) som är styrande för Region Jämtland Härjedalen. Där hänvisas till dokumenthanteringsplaner som finns för olika områden/kategorier. För administrativa dokument anges att godkända lagringsytor är Platina och Centuri. Det finns också en fastställd ”riktlinje för informationshantering i Teams och OneDrive” dok nr 51826 (https://centuri/regno/51826). Där anges att:

”*OneDrive och Teams ska betraktas som arbetsverktyg där dokument sparas under den tid som de utgör ett arbetsmaterial. De medger också lagring av övriga dokument och handlingar som kan anses vara av ringa värde, t.ex. dubbletter av handlingar där myndigheten redan har ett arkivexemplar eller en tillfällig lista i Excel.*

Varken OneDrive eller Teams är avsedda att vara lagringsplats för handlingar som ska diarieföras eller arkiveras. Sådana handlingar och dokument ska hanteras i Region Jämtland Härjedalens godkända ärende och dokumenthanteringssystem.”

Således finns redan gällande dokumenthanteringsplaner och även en riktlinje för informationshantering i O365, de senare behöver kompletteras enligt förslag under 6.5.

Medarbetare i Regionen har alltså möjlighet att både spara dokument lokalt och i molnet, det kan vara en utmaning att förstå och hantera lagring rätt samt känna till gällande regler och riktlinjer. Tydligare anvisningar kan underlätta detta.

5 Säkerhet

En utgångspunkt i uppdraget var att Region Jämtland Härjedalen inte själva kan ha bättre säkerhet i en lokal driftlösning än vad leverantören har i O365 molntjänster.

Informationssäkerhetsgruppen delar slutsatserna i utredningen från Danderyd om att de skalfördelar det innebär med Microsofts stordrift i Office 365 medger en nivå på säkerhet i form av både teknik och personella resurser som är svår att uppnå som enskild organisation, både kompetensmässigt och ekonomiskt. Därmed får Microsofts grundsäkerhetsnivå ses som tillräcklig för att skydda informationen som regionen lagras i Office 365, förutsatt att Region Jämtland Härjedalen nyttjar och tillämpar relevanta säkerhetslösningar. Molntjänstens säkerhetsfunktioner och kvalitén i dessa är en av flera förutsättningar för att bedriva ett effektivt säkerhetsarbete, sett till skydd mot kvalificerade hot.

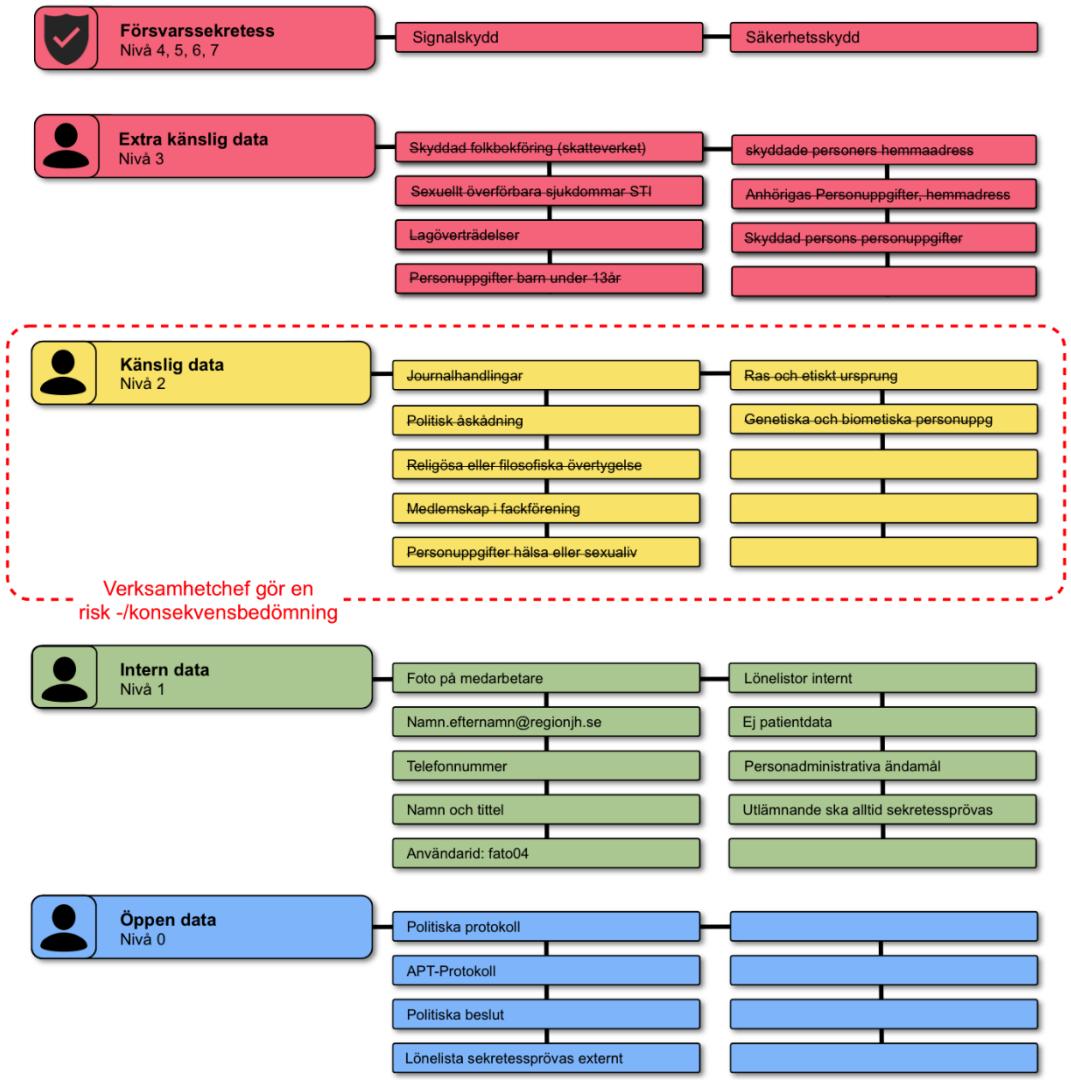
Utredningen gör också bedömningen att risken för att obehöriga genom angrepp kommer åt information är en större risk, än ett utlämnande via Cloud Act, varför det är fortsatt viktigt att arbeta och stärka IT- cybersäkerhetsarbetet i Regionen.

Förutom den tekniska aspekten av säkerhet och yttre cyberhot, så finns det också interna säkerhetsaspekter att beakta såsom risker i användarbeteenden och i hur informationen hanteras i O365 av Regionens medarbetare. Det finns till exempel, som nämns på andra ställen, risk att sekretessklassad information hanteras, lagras och även delas till externa användare som bjuds in i olika samarbetsytor i O365.

6 Förslag på åtgärder

6.1 Regler för informationsklassning

För att fastställa skyddsvärdet behöver informationsklassning genomföras av den data som hanteras i O365 och hanteringsregler tas fram. När det gäller personuppgifter så föreslås att följande struktur används:



I nuvarande informationsklassningsmodell som tillämpas i Regionen, används klasser 1–4, utifrån de olika aspekterna riktighet, konfidentialitet, tillgänglighet och spårbarhet. För att anpassa modellen mot nya nationella rekommendationer från Myndigheten för samhällsskydd och beredskap (MSB) kommer nivåerna 0–7 istället att införas. Klassindelning för personuppgifter ska också integreras i den modellen.

Modellen ovan visar det nya förslaget på samtliga klassningsnivåer utifrån aspekten konfidentialitet från öppna data till Försvarssekretess. I det här uppdraget kommer bara nivåerna 0 och 1 att tydliggöras. Nivån 2 behöver ytterligare utredas och riskvärderas särskilt

för att avgöra om information på denna nivå kan lämpa sig för att lagra i en molntjänst som O365. Nivå 3 är av sådan art att det i dagsläget inte är möjligt att lägga information med denna klassningsnivå i en molntjänst som O365.

Nivå 0-2 är alltså de nivåer som regionen ser som tänkbara i O365, det finns dock några juridiska hinder. För att hantera känsliga data, nivå 2 ska det alltid föregås av en risk- och konsekvensanalys av en verksamhetschef.

Informationssäkerhetsgruppen föreslår att klassning med dessa informationsklasser börjar tillämpas både när dokument skapas och när e-mail skickas. Nedan beskrivs ett tekniskt skydd som kallas Microsoft Information Protection (MIP). Detta skydd möjliggör att dessa informationsklasser kan tillämpas genom att för ett dokument eller ett e-postmeddelande sätta en etikett (”label”) som anger klassningen på innehållet. Användare måste då alltid i O365 göra ett aktivt val vilken klass dokumentet eller mailet är. Förslaget är också att den förvalda klassen alltid är ”intern data”. Om informationen sedan ska delas externt så väljs etikett/klass ”öppen”.

Modellen ovan med klassning av personuppgifter behöver integreras i Regionens övergripande informationsklassningsmodell. Detta arbete har hög prioritet inom funktionen för informationssäkerhet och dataskydd under 2021. Regler för informationsklassning kan fastställas av Regionstabschef.

6.2 Hantering av personuppgifter i O365

Regionen har, som nämnts, enligt dataskyddsförordningen laglig grund för behandling av personuppgifter. Den lagliga grunden är rättslig förpliktelse, avtal och allmänt intresse.

En åtgärd är att regionen behöver vara tydlig med kraven för att hantera information i O365. Krav för att få använda O365 vid utförandet av sina arbetsuppgifter är att man endast hanterar information som är informationsklassad som nivå 0–1. Medarbetare som hanterar känslig information (informationsklassningsnivå 2–3) måste säkerställa att informationen lagras av Region Jämtland Härjedalen godkända lagringsytor.

I informationsklass 1 ingår personuppgifter ”bas” d.v.s. foto på medarbetare, namn, telefonnummer, titel, användarid. Exempel på personuppgifter kan t. ex. vara olika namnlistor på medarbetare och semesterlistor. För övrig nivå av behandling av personuppgifter utöver ovanstående som ligger i en högre informationsklass (nivå 2), ska alltid föregås av en riskanalys och konsekvensbedömning enligt Regionens gällande regelverk. Ansvarig för att genomföra riskanalysen är informationsägare (ofta verksamhetschef) och samråd ska alltid ske med Dataskyddsombudet.

Genom att Regionen som personuppgiftsansvarig beslutar om att hantera personuppgifter i O365 finns en risk att Regionen bryter mot lagstiftning och att Integritetsskyddsmyndigheten utdömer vite. Regionstyrelsen rekommenderas ändå att ta beslut att personuppgifter i klass 0 och 1 får hanteras i O365. För nivå 2 ska alltid riskanalys utföras och om beslut om hantering i O365 tas ska kryptering användas. Separat beslut ska skrivas kring detta.

6.3 Införande av tekniska skydd av information - MIP

Microsoft Information Protection (MIP) är ett skydd som regionen redan i liten skala har börjat testa som en säkerhetshöjande åtgärd för att skydda data i O365. Det är ett skydd som går ut på att lägga kryptering alternativt regelstyrning på en viss typ av etikett (motsvarande en viss informationsklass). I praktiken läggs då behörigheter på utifrån Microsoft Information Protection (MIP), som är ett krypteringsskydd och en option från Microsoft. Ett sådant arbete är redan påbörjat i form av ett pilotprojekt inom HR avdelningen.

Utifrån MIP har regionen möjlighet att värdera den information som skapas och sätta på en etikett som talar om hur informationen får hanteras. Idag finns tre etiketter (klassningsnivåer för konfidentialitet) framtagna för Regionen: öppen, intern och känslig.

Öppen data är den etikett regionen sätter för att kunna dela information internt eller externt. Här används inget extra skydd/kryptering.

Intern data denna etikett föreslås vara förvald i O365 och alla dokument och mail som regionen skapas ska ha den etiketten från grunden. Detta gör att alla regionanställda måste göra ett aktivt val och en bedömning om informationen ska delas med extern part eller inte. Har vi gäster i ett Teams kommer inte alla dokument att vara tillgängliga förens man aktivt ändrar dokumentet till Öppen data. E-post kommer inte att kunna skickas till extern part innan man gjort bedömning och ändrat etiketten på e-posten till Öppen data. Etikett intern data är reglerstyrd och inte krypterad.

Känslig data är den etikett regionen sätter när det är ett dokument eller mejl som bara några få ska ta del av, här kopplas en eller flera användare till etiketten för att kunna behörighets styra de som få ta del av informationen internt som externt. Behörigheten går att återkalla av den som skapat etiketten, oavsett om det är en intern eller extern som tagit del av informationen. Etiketten känslig data är krypterad.

Det finns även möjligheter att skapa fasta ”MIP grupper” inom regionen med egen etikett. Då skapas en etikett som heter ”Ekonomi” som exempel, vilket gör att bara medlemmar i gruppen bara kan ta del av den krypterade informationen.

Rekommendationen är att riktlinjen för informationshantering i O365 kompletteras med skydd av information inklusive personuppgifter enligt ovan. Utifrån Regionstyrelsens beslut kan implementering och tillämpning av MIP beslutas av Regionstabschef.

6.4 Upptäcka läckage av känsliga personuppgifter

Känsliga uppgifter, vare sig det gäller känsliga/extra skyddsvärda personuppgifter eller andra typer av känsliga uppgifter, behöver ett särskilt skydd. För att kunna upptäcka om sådana känsliga uppgifter ”läcker” till en ej godkänd lagringsyta eller skickas oskyddat per e-post behövs en funktion för att upptäcka och eventuellt blockera sådant läckage. Detta kan göras med inbyggda funktioner för Data Leakage Protection (DLP) i O365. Ett regelverk behöver skapas av O365 förvaltning. Beslut om tillämpning av sådant regelverk kan fattas av Regionstabschef.

6.5 Lagring och gallring

För att säkerställa att uppgifter såsom personuppgifter inte sparas längre än de behövs krävs att Regionens dokumenthanteringsplan tillämpas även i Office, vilket med fördel kan förtydligas i riktlinjerna för informationshantering i O365. Det behövs också ett förtydligande kring lagringsytorna i O365 som är OneDrive och SharePoint.

Dessutom föreslås att regionen använder sig av de automatiska ”retention labels” (Microsofts benämning), alltså automatiska gallringsregler som finns i O365-plattformen. Det innebär att automatisk gallring kan skapas i O365 genom att sätta upp regler med etiketter på dokument för att styra lagringstid (alltså när de automatiskt ska raderas/gallras). Det behöver säkerställas att detta harmonierar med Regionens dokumenthanteringsplaner. Denna uppgift behöver tilldelas förvaltningen av O365 och informationsförvaltningsrådet. Beslut kan fattas av Regionstabschef.

För tjänster som lagrar information i O365 (Outlook, SharePoint, OneDrive) kan det vara av värde att fortsatt utreda om det i framtiden också bör finnas lokalt alternativ till lagring av redundansskäl.

6.6 Krav på backuptagning

Bland de inbyggda standardfunktionerna i O365 saknas backupfunktioner för informationen som lagras i tjänsterna. Detta innebär att om information raderas är det inte säkert att den kan återskapas/återställas. Följande standardtider gäller i O365 för informationens lagring (kan inte påverkas av regionen som kund).

- Exchange e-post och kalender, kontakter: **14 dagar efter borttag** av användaren raderas informationen permanent

- SharePoint/OneDrive/Teams: **93 dagar efter borttag** av användaren raderas informationen permanent

Exempel på vad som inte går att göra utan backupfunktioner är att återskapa/återställa information som den såg ut vid en viss tidpunkt. Att återställa information från ett inaktiverat konto är inte heller möjligt på ett enkelt sätt.

En rekommendation är att Regionen framåt utarbetar en backupstrategi för O365 enligt ”best practice”. Beslut kan fattas av Regionstabschef.

6.7 Behov av loggning – logguppföljning

Dataskyddsförordningen ställer krav på att det går att spåra och följa upp vilka som haft åtkomst till specifika personuppgifter. Detta kräver tillgång till funktioner för loggning av åtkomst till dessa uppgifter.

Loggning införs lämpligast genom att använda de inbyggda loggfunktionerna i O365-tjänsten. Tillsvidare bedöms dessa funktioner vara tillräckliga för att tillgodose kraven på spårbarhet för lagrade personuppgifter i O365. Något externt loggverktyg bör inte krävas för ändamålet. Förutom att använda loggverktyg behöver rutiner tas fram med beskrivning av vem som ska ges åtkomst till loggar samt vilken loggranskning som kan bli aktuell att utföra. Arbetet

behöver utvecklas i samråd mellan O365 förvaltningen samt funktionen för dataskydd. Beslut kan fattas av Regionstabschef.

6.8 Hantering av löpande tillägg/ändringar i O365-tjänsterna

Innehållet/funktioner i O365-tjänsterna ändras löpande av leverantören (Microsoft) vilket innebär att regionen som kund inte kommer att kunna ha full kontroll över vilka funktioner som finns att tillgå vid varje tidpunkt. Regionen behöver förhålla sig till att O365-tjänsterna kontinuerligt ändras över tid med nya och ändrade funktioner.

Dessa förutsättningar innebär i sig utmaningar med att kunna styra hur användarna får använda tjänsterna. Det kan också finnas också avtalsmässiga aspekter som behöver beaktas.

För att få en ökad kontroll över vilka tjänster och funktioner som är tillgängliga för regionens användare föreslås att följande införs:

- En tydlig ”releasehantering” för de tjänster som ska vara tillgängliga i O365. Detta innebär att innan en tjänst införs ska det föregås av ett releaseförfarande där tjänsten godkänns för användning med säkerställande av att det finns nödvändigt användarstöd att tillgå för att kunna använda tjänsten på rätt sätt.

- Inför en typ av godkännandeförfarande för att analysera nya O365-tjänster som eventuellt ska införas för användning inom regionen. Vissa tjänster ska inte vara tillgängliga för alla utan enbart för vissa grupper av användare.

Ovanstående punkter bör ges som uppdrag till O365-förvaltningen vilket kan beslutas av Regionstabschef.

7 Bedömning och rekommendationer

Grundprinciperna i dataskyddsförordningen och något av de rättsliga grunderna ska vara uppfyllda för att regionen ska kunna hantera personuppgifter. De lagliga grunderna är rättslig förpliktelse, allmänt intresse och avtal. Regionen har därmed laglig grund för behandling av personuppgifter. Att behandla personuppgifter i O365 som är en molntjänst innebär ett utlämnande av personuppgifter och strider därmed mot nuvarande lagstiftning. Microsoft som leverantör kan komma åt och begära ut dessa uppgifter (enligt Cloud Act).

Problematiken med utlämnande av personuppgifter uppstår även vid egen serverdrift (som i princip alltid kräver extern support) utan att en molntjänst används, och det är i vart fall nödvändigt för regionen att välja något av de kontorsstödssystem som finns till hands. Det finns också många fördelar med O365 som arbetsredskap. Personuppgifter behöver ges det skydd som lagstiftningen kräver, oavsett vilket system som används.

Med utgångspunkt att Region Jämtland Härjedalen redan använder Office 365, och utifrån de alternativa kontorsstödssystem som finns till hands, lämnar informationssäkerhets gruppen rekommendationen att Office 365 kan fortsätta användas för öppen och intern information i klass 0–1 inklusive personuppgifter bas. Det är av största vikt att sekretessuppgifter som rör Sveriges säkerhet (så kallad säkerhetsskyddsklassificerad information), hälso- och sjukvårdsuppgifter, och övrig information i nivå 3 inte hanteras i

O365. Informationsklass 2 ska som utgångspunkt inte heller hanteras i O365, men kan i vissa fall göra det efter särskild risk- och konsekvensanalys samt komplettering med tekniskt skydd (MIP).

O365 ska inte ersätta de verksamhetssystem som regionen normalt har för hantering av uppgifter inom kärnverksamheten. De systemen ska även i fortsättningen användas framför Office 365. Office 365 ska aldrig användas för långtidslagring av sekretessreglerade och sekretessbelagda uppgifter samt personuppgifter efter att bearbetningen är klar. Regionstyrelsen (som personuppgiftsansvariga) bör fatta beslut om detta.

Sekretessbelagda uppgifter ska som grund överhuvudtaget inte behandlas i O365, däremot behandlas personuppgifter i hög utsträckning i det dagliga arbetet. Cloud Act och liknande regelverk kan medföra att utlämnandet utgör risk för att obehöriga kan få åtkomst till personuppgifter och risk för ett röjande av sekretessbelagda uppgifter (om sådana finns), om Microsoft får åtkomst till uppgifterna och/eller att de lämnas ut av Microsoft till tredje part. Sannolikheten att uppgifterna lämnas ut av Microsoft till tredje part bedöms i dagsläget med viss försiktighet som låg. Detta medför att risken för att Regionen, utifrån Cloud Act och liknande regelverk, röjer sekretessbelagda uppgifter bedöms som låg. Om uppgifter lämnas ut av Microsoft, kan det utgöra ett brott mot tystnadsplikten.

Tillräcklig säkerhet för regionens information är en förutsättning för att verksamheten ska kunna fullgöras. Informationssäkerhetsgruppen delar slutsatserna i utredningen från Danderyd om att de skalfördelar det innebär med Microsofts stordrift i Office 365 medger en nivå på säkerhet i form av både teknik och personella resurser som är svår att uppnå som enskild organisation, både kompetensmässigt och ekonomiskt. Region Jämtland Härjedalen behöver däremot säkerställa att relevanta säkerhetslösningar nyttjas och tillämpas. Förutom den tekniska aspekten av säkerhet finns andra risker i användarbeteenden och i hur informationen hanteras i O365 av Regionens medarbetare. Detta måste fortsatt beaktas och flera av de åtgärder som föreslås grundas i denna säkerhetsaspekt. Det är av största vikt att medarbetare i så stor utsträckning som möjligt får förutsättningar att ”göra rätt”.

I uppdraget har riskreducerande åtgärder identifierats som rekommenderas vidtas för regionens fortsatta informationshantering i Office 365. Informationsklassning samt hanteringsregler utifrån klassning behöver utarbetas och tillämpas i O365, vilket bedöms som den högst prioriterade åtgärden att införa. Kopplat till klassning föreslås det tekniska skyddet MIP tillämpas i O365 genom regelstyrning och kryptering.

Regionens dokumenthanteringsplan ska tillämpas även i Office, vilket föreslås förtydligas i nuvarande riktlinjer för informationshantering i O365. Det behövs också ett förtydligande kring lagringsytorna i dessa riktlinjer (som i O365 som är Onedrive och Sharepoint). Det är som medarbetare inte helt lätt att göra rätt i informationshanteringen och det krävs en tydligare styrning som underlättar.

För att kunna upptäcka om känsliga personuppgifter ”läcker” till en ej godkänd lagringsyta eller i e-post bör inbyggda funktioner för Data Leakage Protection (DLP) i O365 användas. Dessutom föreslås att regionen använder sig av de av automatiska gallringsregler som finns i O365-plattformen (s.k. retention labels).

Bland de inbyggda standardfunktionerna i O365 saknas backupfunktioner för informationen som lagras i tjänsterna. En rekommendation är att Regionen framåt utarbetar en backupstrategi för O365 enligt ”best practice”.

För att leva upp till kraven i Dataskyddsförordningen rekommenderas att loggning införs i O365. Det här är dock ett arbete som kräver mycket mer än en ”teknisk åtgärd” och som behöver analyseras och utredas mer, innan åtgärden kan införas.

Regionen behöver förhålla sig till att O365-tjänsterna kontinuerligt ändras över tid med nya och ändrade funktioner. För att få en ökad kontroll över vilka tjänster och funktioner som är tillgängliga för regionens användare föreslås att en tydlig releasehantering och godkännandeförfarande införs.

7.1 Framtidsspaning

Pågående arbete inom EU rörande säkerhet i molntjänster kan komma att påverka synen på och användningen av molntjänster inom de närmaste åren. Det handlar framför allt om EU Cloud Code of Conduct som är ett regelverk/ramverk som leverantörer av molntjänster kan använda sig av för att kunna påvisa att de uppfyller dataskyddslagstiftningen/GDPR. Ramverket kopplas till GDPR samt till GDPR samt till ISO 27001 och ISO 27018 (standarder för informationssäkerhet resp. säkerhet i molntjänster). Ännu så länge är Cloud Code of Conduct ett frivilligt regelverk som molnleverantörer kan använda sig av i syfte att uppvisa att man efterföljer lagkrav och standarder. Code of Conduct ska både kunna användas för leverantörens självevaluering samt för 3:e-partscertifiering via ett certifieringsorgan.

Målet med certifieringen är att den ska garantera regelefterlevnad och att s.k. ”Privacy-by-design” (inbyggt dataskydd) samt ”Privacy-by-default” (förvald säkerhetsnivå) blir inbyggt per automatik i molntjänsten. Certifieringen kommer att erbjudas i tre olika nivåer (*Basic*, *Substantial* respektive *High* som motsvarar olika ”motståndsnivåer” för skydd mot cyberangrepp/säkerhetshot). Certifieringen kommer, åtminstone initialt, att vara frivillig för företag inom och utanför EU. Cyber Security Act är aktuellt för både leverantörer av molntjänster och kunder, och kan komma att bli en viktig del i kravställningar inom upphandling och inköp.

Hur en sådan certifiering för regionens O365-tjänster skulle kunna påverka ställningstagande om användning av tjänsterna är ännu för tidigt att bedöma. Orsaken är att tillräcklig information ännu saknas om vad de tre olika certifieringsnivåerna ”Basic”, ”Substantial” och ”High” innebär i praktiken. Det är också ännu oklart om Microsoft kommer att ansluta sig till och genomgå CSP-certifieringen via ”CSP Cert”.

Den Europeiska Dataskyddsmyndigheten (EDPB) publicerade, med anledning av SchremsII-domen, nyligen två nya vägledningar avseende överföring av personuppgifter utanför EU/EES. I korthet innebär dom att personuppgiftsansvarig behöver göra en riskanalys för varje land som personuppgifter ska överföras till och därefter, om nödvändigt, implementera ytterligare skyddsåtgärder utöver exempelvis standardklausulerna. Om man tror att vidtagna åtgärder inte uppnår en tillräcklig säkerhetsnivå, ska överföringen bedömas som olaglig. EDPBs vägledning innehåller sex steg att följa för att riskanalysera och bedöma personuppgiftshanteringen och den ska dokumenteras. Regionen behöver under 2021 uppdatera riktlinjer för personuppgiftshantering enligt denna nya vägledning vilket funktionen för dataskydd ansvarar för. Kravet om riskanalys gäller för personuppgifter i nivå två.

I ett delbetänkande, SOU 2021:1, Säker och kostnadseffektiv it-drift, fokuserar utredaren på förutsättningarna för statliga myndigheter, kommuner och regioner att utkontraktera sin IT-

drift. Utredaren bedömer att en utkontraktering av sin IT-drift innebär ett ”röjande” och lämnar därför ett förslag på ett tillägg i Offentlighet- och sekretesslagen (2009:400) (10 kap. 2 a §). Tillägget tar sikte på fall då uppgifter lämnas ut till företag eller en annan enskild (tjänsteleverantör) eller till en annan myndighet som har i uppdrag att utföra endast teknisk bearbetning eller teknisk lagring av de uppgifter som lämnas ut för den utlämnande myndighetens räkning. Ett utlämnande ska – enligt den föreslagna bestämmelsen – inte ske om övervägande skäl talar för att det intresse som sekretessen ska skydda har företräde framför intresset av utkontraktering.

Utredningen ska slutredovisas senast 15:e oktober 2021 och det är i dagsläget inte klart huruvida utredarens författningsförslag kommer att antas.

8 Referenser

Referens 1: Office 365 i Danderyds kommun, Danderyds kommun KS 2019/0296, 2019-07-04

9 Bilaga 1: Risker – användning av Office 365-tjänsterna

Nedan redovisas en sammanställning av identifierade risker med användning av O365. Riskerna är inte kvantifierade utan ska ses som en översikt över typer av risker som förekommer och hur de kan hanteras genom riskreducerande åtgärder. Sammanställningen ska kunna utgöra underlag till kommande, mer riktade riskanalyser som behöver genomföras för specifika O365-tjänster/användningsområden.

Riskområde	Riskhändelse	Kommentar	Konsekvens	Förslag på riskreducerande åtgärder
Hantering av personuppgifter	Risk för regelbrott mot GDPR – överföring av personuppgifter till USA (ej godkänd tredjelands-överföring)	Privacy Shield skyddar inte längre och kan inte åberopas vid lagring i amerikanska molntjänster	GDPR/dataskydds-lagstiftningen kan inte efterlevas	Säkerställ att riskbedömning görs innan lagring av känsliga uppgifter görs till O365. Säkerställ att informationsskydd (såsom MIP) används för känslig information om den ska tillåtas lagras i O365 (baserat på riskanalys).
	Personuppgifter bas sprids obefogat utan informationsskydd i O365		GDPR/dataskydds-lagstiftningen kan inte efterlevas – medelhög konsekvens	Säkerställ att MIP-skyddet med minst nivån/etiketten ”Intern” används för dessa uppgifter.
	Känsliga personuppgifter hanteras/delas i O365	Allmänt hantering av känsliga person-uppgifter	GDPR/dataskydds-lagstiftningen kan inte efterlevas – allvarlig konsekvens	Separat riskanalys behöver genomföras på aktuella informationsmängder innan lagring av känsliga personuppgifter eventuellt kan tillåtas i O365.
		Försök till extern delning	Otillåten lagring av känsliga personuppgifter i O365 kan medföra att dessa uppgifter läcker till obehöriga.	Aktivera Data Leakage Protection (DLP) i O365 (upptäckt och blockering av otillåten lagring av känsliga person- uppgifter).
			Känsliga personuppgifter delas obehörigt med externa användare	Säkerställ att MIP-skyddet med minst nivån/etiketten ”Intern” används för dessa uppgifter.

Riskområde	Riskhändelse	Kommentar	Konsekvens	Förslag på riskreducerande åtgärder
			(via t ex Teams)	
	Amerikanska myndigheter begär ut känsliga personuppgifter via leverantören, regionen kan själva inte pröva utlämnande (Cloud Act)		GDPR/dataskydds-lagstiftningen kan inte efterlevas – allvarlig konsekvens	Det saknas idag åtgärd som kan ge acceptabel risknivå för denna riskhändelse. Vad som är tillräckligt informationsskydd via t ex MIP (med ”egen nyckel-hantering”, DKE) behöver bedömas.
	Det går inte att se vilka som tagit del av känsliga personuppgifter som lagras i O365		Överträdelse av dataskydds-lagstiftningen	Säkerställ loggning och möjlighet till uppföljning över vem som har givits åtkomst till personuppgifter.
	Känsliga person-uppgifter delas obehörigt via videotjänst i O365		GDPR/dataskydds-lagstiftningen kan inte efterlevas – allvarlig konsekvens	Säkerställ att godkänd videotjänst används för känsliga uppgifter baserat på syften med videomöte samt genomförd riskbedömning.
Informations-förlust	Informationsförlust relaterat till att regionen inte har egen backup/ redundans		Informationsförlust - överträdelse av lagkrav (förvaltningslagen, arkivlagen, tryckfrihets-förordningen för hantering av allmänna handlingar)	Identifiera vilka information/tjänster som ska omfattas av lokal backup. Inför lokal backuptagning av denna information/tjänster.
Verifiering av uppfyllnad regulatoriska krav i tjänsterna	Regionen kan inte kontrollera och redovisa hur regulatoriska krav uppfylls vid användande av O365-tjänsterna		Bristande kontroll av efterlevnad av regulatoriska krav samt bristande möjligheter att kunna redovisa denna efterlevnad för tillsyns-myndigheter.	Övervaka kravefterlevnad/ regulatorisk status för regionens aktuella O365-tjänster (via ”compliance-portal”/ motsvarande.
Obehörig spridning av konfidentiell information (ej specifikt personuppgifter)	Sekretessbelagd information används i O365 och läcker till obehöriga	Generell risk, oavsett hur läckage sker (oavsiktligt läckage)	Sekretessbelagd information i O365 läcker till obehöriga.	Separat riskanalys behöver genomföras på aktuella informationsmängder innan lagring av konfidentiell information eventuellt kan tillåtas i O365.
				Skapa en lokal lagring av information som inte kan/får lagras i O365 molntjänst.
	Intrång från obehörig sker (cyberhot) och konfidentiell	Specifik risk som avser antagonistiskt hot/angrepp (intrång, attack)		Säkerställ att cyberhot (intrång, angrepp) mot informationen i O365 kan identifieras och avvärjas.

Riskområde	Riskhändelse	Kommentar	Konsekvens	Förslag på riskreducerande åtgärder
	information stjäls/ läcker			
Oreglerad användning av information (hantering av ej klassad information)	Information som inte har informations-klassats lagras i O365		Information som inte är tillåten att hantera i O365 hanteras i tjänsten vilket kan göra att konfidentiell information läcker till obehöriga.	Tillämpa informationsklassning för den information som ska lagras i O365 molntjänster. Säkerställ att endast information med godkända klassnings-nivåer lagras i O365. Tydliggör hanteringsregler för information och tillämpa dessa genom anvisningar till regionens användare gällande vad som får hanteras i O365-tjänsterna.
Oreglerad användning av ej godkända tjänster/ plattformar	Nya applikationer och tjänster i O365 bedöms och godkänns inte innan de införs	Information hanteras i av regionen ej godkända tjänster – oreglerad användning med eventuella lagöverträdelser som följd	Medarbetare börjar använda tjänster i O365 utan att veta om/ hur de får användas. Risk för överträdelse av flera lagkrav.	Inför ett godkännande-förfarande för samtliga tjänster i O365 innan de kan godkännas för användning.
	Användning av applikationer och tjänster i O365 har inte reglerats och beskrivits (lathundar mm)		Medarbetare börjar använda tjänster i O365 utan att veta hur de får användas. Risk för överträdelse av flera lagkrav.	Ta fram/komplettera rutiner för hur O365-tjänster får användas.
	Användare förstår inte var information hamnar och lagras (SharePoint, OneDrive)	Handhavande, användare oklar över var information sparas/delas	Felaktig användning/ hantering av information (i strid med regelverk). Risk för överträdelse av flera lagkrav.	Inför MIP-skyddet som grundskydd för att minska konsekvenser av att information lagras/ delas på ”fel” plats. Säkerställ att användare känner till gällande regelverk var information ska lagras/delas.
	Användare lagrar information i O365 som inte ska lagras i molntjänst (som ska diarieföras och arkiveras)			
	Det saknas kontroll över vilken typ av information som lagras i O365	Generell risk (efterlevnads-kontroll)		Inför ett scannings-verktyg som kan identifiera information och ge underlag till vidare hantering av denna information
Hantering av allmänna handlingar	Handling blir allmänna (publikt tillgängliga) tidigare än de är avsedda att bli	Avser att moln-leverantören av O365 (Microsoft) kan ta del av uppgifter	Överträdelse av tryckfrihets-förordningen, förvaltningslagen.	Avtalsreglering hur leverantören får hantera uppgifter.

Riskområde	Riskhändelse	Kommentar	Konsekvens	Förslag på riskreducerande åtgärder
	Regler om gallring och lagring följs inte		Överträdelse av tryckfrihets-förordningen, arkivlagen.	Säkerställ att gallringsstöd införs i O365, exempelvis via ”retention labels” och retention policies. Överväg införande av scanningsverkyg som stöd för automatisk/ halvautomatisk gallring.
Avtalsrisker - ansvarsroller	Otydlig ansvars-fördelning mellan leverantör (Microsoft) och kund (Region Jämtland Härjedalen)		Överträdelse av dataskydds-lagstiftningen, tryckfrihets-förordningen, förvaltningslagen, arkivlagen.	Säkerställ att det upprättas personuppgifts-biträdesavtal med leverantören inkl. reglering av underleverantörer. Regionen behöver kunna påverka vilka underleverantörer som hanterar sin data alternativt få garantier för att dessa underleverantörer har adekvat skyddsnivå. Huvudleverantören ska ha tecknat avtal avseende person-uppgiftsbiträde med sina under-leverantörer.