MSMD AIR

Microsoft Molndesign Analys av Införande och Risk

knowit

Innehållet i denna rapport är endast avsett som allmän information och utgör inte, och skall heller inte användas som, professionell rådgivning. Det kan förekomma att innehållet inte är uttömmande eller helt uppdaterat. Inga åtgärder eller beslut bör baseras på information tillgänglig i denna rapport som ersättning för juridisk rådgivning. Vid behov av juridisk rådgivning är ni välkomna att kontakta någon av våra jurister. Direkt eller indirekt användning av innehållet i rapporten sker på egen risk.

Författare, år 2021

Richard Oehme
Senior managementkonsult med fokus på samhällssäkerhet och cybersäkerhetsfrågor samt ordförande för Säkerhets- och försvarsföretagens cyberförsvarsgrupp. Han har tidigare arbetet med underrättelsefrågor på FRA i olika positioner, som sakkunnig på Försvarsdepartementet i underrättelsestyrning, som chef för Regeringskansliets säkerhetssektion och vid Statsrådsberedning som chef för en analyssektion. Efter åren i Regeringskansliet var han chef för Verksamheten för cybersäkerhet och skydd av samhällsviktig verksamhet vid MSB innan han blev konsult. Han är också aktiv som reservofficer.

Lisa Lundin
Konsultchef och director för juridik på Knowit. Hon har arbetat med dataskydd och e-förvaltning i mer än femton års tid i olika juristroller vid Polisen, Säkerhets- och integritetsskyddsnämnden och Säkerhetspolisen samt i uppdrag som senior juristkonsult för flera olika myndigheter. Lisa har varit med och utformat regelverk, hjälpt verksamheten att förstå och tillämpa dem samt arbetat med tillsyn.

Henrik Aldermo
Senior molnarkitekt Azure & Microsoft 365. Efter drygt 30 år i branschen i bland annat konsult- och chefsroller har Henrik stor erfarenhet av såväl traditionell IT-infrastruktur som moderna molntjänster. Han har länge haft fokus på Microsofts produkter och även arbetat med informationssäkerhet och kvalitetsledning samt verksamhetsutveckling. Henrik är även utbildad internrevisor och certifierad Azure Solutions Architect.

Ranja Bunni
Senior dataskyddsjurist som bistår olika typer av verksamheter med deras digitaliseringsarbete. Hon har lång erfarenhet från Integritetsskyddsmyndigheten (IMY), flera andra myndigheter samt från förvaltningsdomstol. Ranja har under åren bland annat arbetat med juridisk rådgivning, tillsyn, process i domstol, utbildning, projektledning, remisshantering och samverkan mellan myndigheter.

Magnus Sjölund
Senior säkerhetskonsult som arbetar med informations- och cybersäkerhetsfrågor samt med säkerhetsskydd. Han har bred erfarenhet från strategisk nivå ner till detaljerade tekniska områden och har även arbetat mycket med utbildning, ledning och ledarskap. Han tjänstgjorde länge inom Försvarsmakten som officer på ett flertal olika befattningar både inom landet och internationellt och har även civil utbildning som säkerhetschef.

Författare, revision år 2024

Lisa Lundin
Konsultchef och director för juridik på Knowit. Hon har arbetat med dataskydd och e-förvaltning i mer än femton års tid i olika juristroller vid Polisen, Säkerhets- och integritetsskyddsnämnden och Säkerhetspolisen samt i uppdrag som senior juristkonsult för flera olika myndigheter. Lisa har varit med och utformat regelverk, hjälpt verksamheten att förstå och tillämpa dem samt arbetat med tillsyn.

Magnus Sjölund
Senior säkerhetskonsult som arbetar med informations- och cybersäkerhetsfrågor samt med säkerhetsskydd. Han har bred erfarenhet från strategisk nivå ner till detaljerade tekniska områden och har även arbetat mycket med utbildning, ledning och ledarskap. Han tjänstgjorde länge inom Försvarsmakten som officer på ett flertal olika befattningar både inom landet och internationellt och har även civil utbildning som säkerhetschef.

Désirée Veschetti
Senior förvaltningsjurist med lång erfarenhet av myndighetsstyrning, informationshantering och informationssäkerhetsarbete inom offentlig förvaltning. Under sina yrkesverksamma år har hon utvecklat förmågan att på ett strukturerat sätt arbeta med förändring och verksamhetsutveckling på olika nivåer inom statlig förvaltning. Ett av de områden som Désirée arbetat längst med är e-förvaltning.

Johanna Grundberg
Jurist och projektledare med fokus på dataskydd och e-förvaltning. Hon har erfarenhet från både offentlig och privat sektor, där hon bland annat arbetat med Privacy by Design, som Privacy Officer och juridisk rådgivning. Hon har certifierat sig inom dataskydd (CIPP/E) och har utbildat sig inom informationssäkerhet med godkänd tentamen av certifieringen CISM (utfärdad av ISACA).

Civan Öztürk
Jurist med fokus på IT-rätt och verksamhetsfrågor. Han har arbetat med uppdrag inom offentlig och privat sektor med regelefterlevnad på dataskyddsområdet bland annat som dataskyddsombud (DPO), Privacy Officer och juridisk rådgivare. Civan är certifierad inom dataskydd (CIPP/E) och har utbildat sig inom informationssäkerhet med godkänd tentamen av certifieringen CISM (utfärdad av ISACA).

Versionshistorik

Version	Huvudsakliga ändringar	Utgivningsdatum
1.0	Första utgåvan av vägledningen	2021-11-30
1.1	Uppdateringar i vägledningens huvuddokument, Appendix A, Appendix B, Appendix D, Bilaga 2 och Bilaga 4. Uppdateringarna syftar till att spegla ett förändrat rättsläge sedan v. 1.0 kom år 2021 och gäller i första hand juridiska resonemang i vägledningen. Viss information om Microsofts erbjudanden, utfästelser och statistik har också uppdaterats i anslutning till de juridiska resonemangen. Länkar i hela vägledningen har kontrollerats och vid behov uppdaterats.	2024-01-31

Knowit AB (publ)
info@knowit.se
knowit.se

Omslagsbild
Maxger/Shutterstock.com

Innehållsförteckning

1 Inledning

1.1 Om vägledningen

Utgångspunkten för vägledningen, benämnd Microsoft Molndesign Analys av Införande och Risk (MSMD AIR), är de krav som ställs på informationshantering utifrån framför allt Dataskyddsförordningen (EU 2016/679, GDPR) och Offentlighets- och sekretesslagen (2009:400, OSL) vid ett införande av hela eller delar av Microsoft 365.

Vägledningen syftar till att stödja offentliga verksamheter, primärt kommuner, vid införandet av hela eller delar av Microsoft 365. Vägledningen tillhandahåller en metod för riskanalys och olika underlag för bedömningar verksamheten kan behöva göra inför ett införande. En central del av metoden är ett juridiskt resonemang kring olika avvägningar utifrån ovanstående författningar. Här beskrivs också tekniska och administrativa åtgärder som en aktör kan överväga vid ett införande för att uppnå tillräcklig säkerhet i relation till ställda regulatoriska krav.

Vägledningen har tagits fram av Knowit AB i ett samarbete mellan dotterbolagen Knowit Cloud och Knowit Cybersecurity & Law (hädanefter Knowit). Arbetet med att ta fram vägledningen har skett på uppdrag av Microsoft Sverige AB.

Den första versionen av vägledningen färdigställdes den 30 november 2021 och publicerades den 14 december 2021. Under år 2023 skedde sedan två viktiga förändringar av de juridiska förutsättningarna för användandet av molntjänster; dels fattade EU-kommissionen ett så kallat adekvansbeslut avseende organisationer som är anslutna till Data Privacy Framework i USA, dels infördes en ny sekretessbrytande bestämmelse i OSL. Med anledning av detta valde Knowit att uppdatera vägledningens juridiska delar och publicera en ny version av vägledningen som färdigställdes i januari 2024.

I uppdraget har Knowit haft full frihet att formulera vägledningen utifrån våra utgångspunkter, observationer och slutsatser.

1.2 Målgrupp

Fokus för denna vägledning är att stödja framför allt kommunala aktörer i sin riskanalys vid ett införande av Microsoft 365. Även andra offentliga och privata aktörer kan ha nytta av vägledningen.

Vägledningen ska kunna utgöra ett stöd till de olika ansvariga i en kommun som är delaktiga vid beslut om ett införande av en molntjänst som Microsoft 365. Dessa aktörer är primärt it-chefer, it-strateger, säkerhetschefer, informationssäkerhetsansvariga, digitaliseringsansvariga, dataskyddsombud och jurister.

Även en ansvarig förvaltningschef, kommunstyrelse eller motsvarande ska kunna läsa hela eller delar av vägledningen för att få förståelse för de utmaningar som finns vid ett införande av en molntjänst som denna och vilka åtgärder som kan vidtas för att minimera riskerna eller hantera andra aspekter vid ett införande.

1.3 Omfattning och avgränsning

Vägledningen tar sin utgångspunkt i de olika överväganden en verksamhet kan behöva göra avseende Microsoft 365 som helhet och olika delar av miljön så som Azure AD, klientapplikationer i Microsoft 365, lagring i SharePoint, Exchange och OneDrive samt behandling av data genom exempelvis transkribering eller diktering. Därtill beskrivs vissa andra grundvärden till exempel Microsofts verktyg och processer för att skydda kundens data och Microsofts kategorier av data samt hur dessa relaterar till olika delar i Microsoft 365.

Vägledningen beskriver nuvarande lagstiftning och vad de juridiska kraven i praktiken innebär för olika delar inom Microsoft 365. De primära regelverk som ligger till grund för arbetet är GDPR och lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning med tillhörande svensk förordning (2018:219). Även tillämpliga delar av OSL omfattas, med undantag för bestämmelser om sekretess till skydd för Sveriges säkerhet (säkerhetsskydd).

Sedan vägledningen först kom ut år 2021 har Microsoft börjat erbjuda Copilot för Microsoft 365. Inom ramen för den uppdatering som skett av vägledningen år 2024 har Knowit inte utrett vilka möjligheter och risker som specifikt användningen av Copilot för Microsoft 365 medför.

1.4 Läsanvisning

Vägledningen är som beskrivs ovan uppbyggd för att kunna möta olika yrkeskategoriers skiftande behov av kunskap kring hur Microsoft 365 är uppbyggd och hur olika delar i en risk- och sårbarhetsanalys kan genomföras.

Efter det inledande kapitel 1, som sätter ramarna för vägledningen, kommer en kort beskrivning av de för denna vägledning två centrala subjekten, *Övergripande om molntjänster och regelverk* i kapitel 2. I detta kapitel beskrivs övergripande Microsoft 365 och de olika regelverk som primärt är relevanta vid en användning av molntjänster. Därefter beskrivs i kapitel 3 den metod som ligger till grund för denna vägledning. I kapitel 4 beskrivs sedan framtida utveckling inom området utifrån två perspektiv, dels den utveckling som sker inom Microsoft, dels några av de rättsliga utredningar som kan komma att påverka denna fråga.

Efter kapitel 1–4, som sätter ramarna för vägledningen, kommer fyra (4) appendix. Appendixen är analytiska, resonerande och förklarande i syfte att stödja olika yrkeskategorier såsom riskanalytiker, jurister, it- och informationssäkerhetsspecialister, säkerhetschefer, it-chefer med flera i sin analys inför ett införande av Microsoft 365.

Det fyra appendixen till stöd för riskanalysen är:

Appendix A	**Modell för risk- och sårbarhetsanalys av ett införande av Microsoft 365** Modellen för risk- och sårbarhetsanalys som presenteras i denna vägledning fokuserar på ett införande av Microsoft 365. Modellen utgår från kända metoder som kompletterats med utvecklade delar för att omhänderta de utmaningar och möjligheter som finns med ett införande av Microsoft 365.
Appendix B	**Rättsliga överväganden med analytisk modell** Här sker utförliga rättsliga analyser framför allt avseende GDPR med kompletterande regelverk och OSL i relation till Microsoft 365. I detta appendix sker i tillämpliga fall också beskrivningar av administrativa och tekniska mitigerande åtgärder som kan vidtas.

Appendix C	**Administrativa och tekniska åtgärder** I detta appendix presenteras ett resonemang med exemplifieringar av administrativa och tekniska åtgärder som kan vidtas för att mitigera identifierade risker eller hantera andra aspekter vid en implementering av Microsoft 365.
Appendix D	**Scenario baserat på ett införande av Microsoft Teams** Syftet med scenariot är att det ska utgöra ett stöd med exempel på olika aspekter som behöver beaktas/hanteras i en risk- och sårbarhetsanalys samt konsekvensbedömning inom ramen för ett införande av Microsoft 365. Utifrån ett tänkt verksamhetsbehov har ett införande av Teams valts som scenario då det berör ett stort antal av de kritiska noder och frågeställningar som en organisation behöver tänka på vid ett införande. I detta ingår juridik, teknik och administrativa åtgärder och hur dessa kan beaktas samlat och i relation till den funktionalitet som verksamheten vill nyttja i Microsoft 365.

Utöver ovanstående appendix finns det fem bilagor i denna vägledning. Bilagorna har som målsättning att vara deskriptiva och förklarande i syfte att tydliggöra fakta och reda ut osäkerheter. Detta dels i syfte att bringa ordning i och tydliggöra vissa centrala frågor och aspekter som uppstår vid ett införande och nyttjande av molntjänster, dels för att kunna hänvisa till dessa frågor och aspekter i denna inledning och i de olika appendixen.

I bilagorna finns en mall för en riskanalys med fokus på införandet av en molntjänst, mer information om Microsoft 365 och annan information som kan vara värdefull vid riskanalysen. Avslutningsvis finns en bilaga med begrepp och förkortningar som används i vägledningen.

De olika delarna av vägledningen – metodbeskrivningen, visualiseringen av Microsoft 365, appendix och bilagor – korsrefererar till varandra i stor utsträckning. Målet är att det ska underlätta för läsaren att förstå hur de olika komponenterna i riskanalysen är sammanflätade och påverkar varandra.

I vägledningen finns också textstycken som omgärdas av linjer. Det är dels gråtonade rutor med en heldragen linje runt texten, dels rutor med en streckad linje runt texten. Gråtonade rutor med heldragen linje markerar text som utgör en bedömning av Knowit. Rutor med streckad linje markerar ett citat av en text från Microsoft.

I vägledningen beskrivs Microsoft 365 generellt på en övergripande nivå i syfte att ge läsaren en tillräcklig förståelse av tjänsten. För den som behöver fördjupa sig i detaljer finns det en stor mängd referenser till Microsofts dokumentation där fördjupningar kan ske.

1.5 Nomenklatur, språkbruk och begrepp

I vägledningen används nomenklatur och begrepp som nyttjas i aktuella författningarna eller som annars är vanligt förekommande i offentlig sektor. Microsofts nomenklatur och begrepp används också, i första hand för att beskriva Microsoft 365, möjliga tekniska och administrativa åtgärder samt de datatyper som de olika åtgärderna är anpassade till.

Några centrala begrepp att ha med sig i läsandet av vägledningen är:

Administrativa åtgärder/ organisatoriska åtgärder
I denna vägledning används begreppen organisatoriska åtgärder respektive administrativa åtgärder. Organisatoriska åtgärder är ett begrepp som används i flera bestämmelser i GDPR och även i de riktlinjer som den europeiska dataskyddsstyrelsen (EDPB) har gett gällande tredjelandsöverföringar. Administrativa åtgärder är ett vidare begrepp än organisatoriska åtgärder och tar inte enbart sikte på det som omfattas av GDPR.

Dataskyddsregelverk
Dataskyddsregelverk avser samtliga regelverk som syftar till att skydda personuppgifter – såväl kraven i GDPR som de krav som framgår av nationell lagstiftning som kompletterar implementeringen av GDPR eller sektorspecifika regelverk som finns på dataskyddsområdet.

Integritetsrisk
Integritetsrisk avser risken för intrång i den personliga integriteten – närmare bestämt ett brott mot rätten till skydd av personuppgifter som föreskrivs i bland annat EUF-föredraget och som GDPR reglerar.[1]

Informationssäkerhetsrisk
Informationssäkerhetsrisk avser möjligheten att ett givet hot utnyttjar en sårbarhet hos en informationstillgång eller en grupp av informationstillgångar och därigenom orsakar organisationen skada.[2]

Kritisk nod
I Microsoft 365 finns ett antal ”noder” som är särskilt viktiga att beakta i en risk- och sårbarhetsanalys utifrån juridiska bedömningar och tekniska samt organisatoriska mitigerande åtgärder. Dessa noder är också ofta av den karaktären att de är representativa så till vida att de beskriver många av de utmaningar en organisation behöver beakta på flera andra ställen i Microsoft 365 vid ett införande. Dessa noder har vi valt att kalla ”kritiska noder”.

Mitigerande åtgärder
Mitigerande åtgärder avser åtgärder för att hantera en risk. Dessa kan vara juridiska (avtalsrättsliga), tekniska eller organisatoriska.

Molntjänst
En molntjänst är en tjänst som möjliggör tillgång till en skalbar och elastisk pool av delbara dataresurser.[3] Molntjänster möjliggör nätverksåtkomst till en gemensam pool av konfigurerbara datorresurser (till exempel nätverk, servrar, lagring, applikationer och tjänster) som på begäran snabbt kan tillhandahållas med minimal hantering eller interaktion med tjänsteleverantören.[4]

[1] Jfr. SOU 2016:41 s. 148.
[2] Se till exempel SVENSK STANDARD SS-EN ISO/IEC 27000:2020 s. 9 (anm. 6).
[3] Definition från NIS-direktivet, Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster, 2 §.
[4] NIST:s definition av “Cloud computing”: https://csrc.nist.gov/publications/detail/sp/800-145/final , 2023-12-18

Metod och modell I vägledningen använder vi begreppen metod och modell. Med metod så avses det övergripande ramverk som beskrivs i denna vägledning och som omfattar såväl de inledande kapitlen 1–4, men framför allt de olika appendixen A-D och hur de interagerar och förstärker varandra. Med modell avses olika komponenter i detta ramverk såsom den modell för risk- och sårbarhetsanalys vid ett införande av Microsoft 365 som beskrivs i Appendix A eller de modeller för GDPR och OSL analys som beskrivs i Appendix A och B.
Personuppgift Varje upplysning som avser en identifierad eller identifierbar fysisk person. En identifierbar fysisk person är en person som direkt eller indirekt kan identifieras genom en identifierare såsom ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.[5]
Risk Med risk avses här en oönskad händelse eller effekt.
Risknivå Begreppet risknivå används för att beskriva den specifika risk som är en kombination av en händelses konsekvenser (inklusive ändrade omständigheter) och tillhörande sannolikhet för händelsens förekomst, i enlighet med definitionen i ISO27000[6].
Risktyper eller riskkategorier Det finns flera olika typer av risker. I denna vägledning behandlas bland annat integritetsrisk och informationssäkerhetsrisk.
Tredjelandsöverföring En tredjelandsöverföring sker när personuppgifter överförs till eller görs tillgängliga för en mottagare i ett land utanför EU/EES (ett så kallat tredjeland).

I Bilaga 5 finns en mer utförlig begrepps- och förkortningslista.

[5] Artikel 4 i GDPR.
[6] SVENSK STANDARD SS-EN ISO/IEC 27000:2020.

2 Metod

2.1 Övergripande beskrivning av metoden

Utgångspunkten för denna vägledning är en metod till stöd för primärt en kommunal aktör för att kunna genomföra en riskanalys vid införandet av hela eller delar av Microsoft 365. Nedan beskrivs de olika delarna i metoden och vad syftet är med de olika delarna samt hur dessa förhåller sig till varandra.

De olika delarna i metoden är:

- Riskanalys med fokus på Microsoft 365.
- Rättsliga överväganden med analytisk modell.
- Administrativa och tekniska mitigerande åtgärder för Office 365.
- Scenariobeskrivning med visualisering (kartbild) av Microsoft 365.

I all informationshantering är informationskartläggning och informationsklassning några av de centrala och grundläggande åtgärderna för en organisation att genomföra. Vikten av att genomföra dessa framgår tydligt i standarden för informations- och cybersäkerhet ISO 27000-serien och styrande regelverk från ansvariga myndigheter och organisationer. Utan klassning av informationen blir det i princip omöjligt att på ett strukturerat sätt hantera och skydda den på rätt sätt. Detta förhållande gäller även i en situation då en aktör väljer att lägga hela eller delar av sin information i en molntjänst. Den utgångspunkten gäller även för denna vägledning.

Här nedan beskrivs de olika delarna i metoden övergripande och avslutningsvis sker en beskrivning hur man kan arbeta med den i sin helhet.

2.2 Riskanalys med fokus på Microsoft 365

Modellen för risk- och sårbarhetsanalys i denna vägledning utgår från den övergripande analys som verksamhetsutövaren behöver genomföra innan ett införande av en molntjänst. Modellen är avsedd att komplettera verksamhetsutövarens analys främst med de särskilda aspekter som tillkommer vid användning av Microsoft 365 under GDPR och OSL.

I den övergripande analysen bör samtliga risker eller andra aspekter som identifieras i samband med införande och användning av tjänsten beskrivas. Inom vissa regelverk finns också särskilda krav på genomförande av riskanalys och vad den ska innehålla. Dessa särskilda krav bör omhändertas i den övergripande analysen genom att även uppta dessa risker och hanteringen av dem.

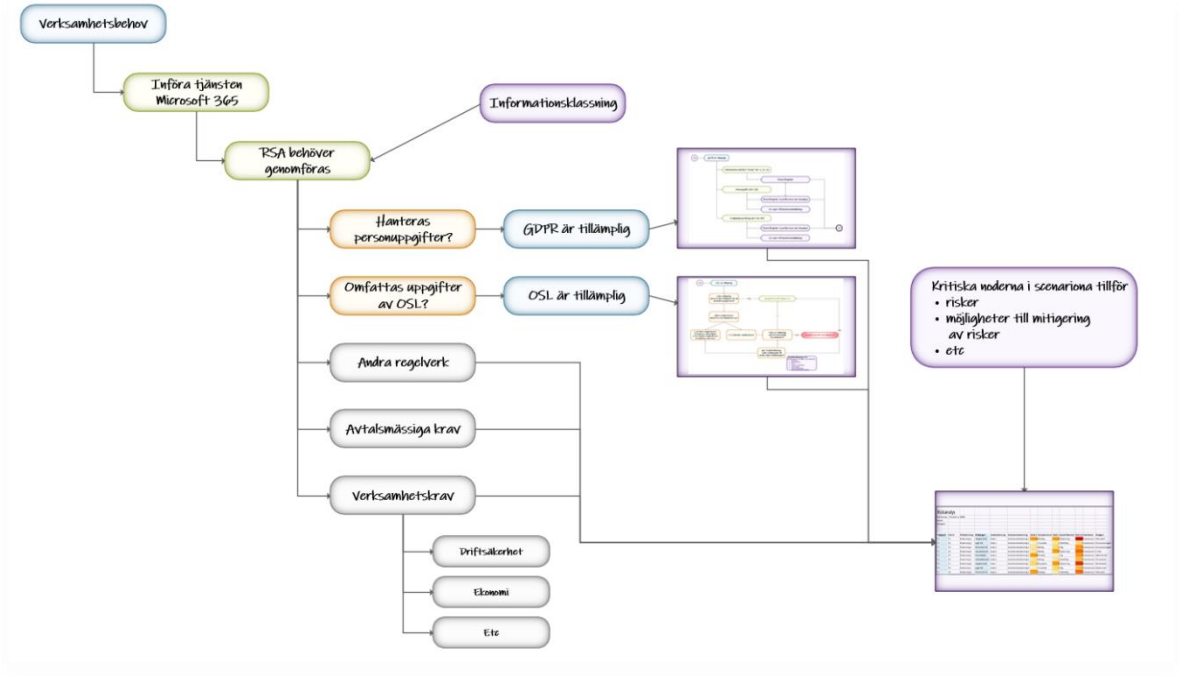
Modellen för riskanalys är tydligt strukturerad i steg och utgår från de krav som ställs inom respektive regelverk och från verksamheten själv. Bedömningarna inom respektive del är i vissa fall mycket omfattande. Resultaten av dessa återförs i modellen till risk- och sårbarhetsanalysen och kan bedömas och jämföras med övriga aspekter och bedömningar. Modellen samlar därmed kravställningarna, bedömningarna av dem och hur de är tillämpliga i verksamheten, åtgärder som vidtas för att hantera dem liksom bedömningar av eventuella kvarvarande risker eller andra aspekter på en och samma plats. Detta möjliggör ett komplett underlag som stöd för införandebeslutet liksom dokumentation av de bedömningar som ligger till grund för beslutet.

I detta sammanhang bör särskild vikt läggas vid beskrivningen av respektive risk och bedömningen som görs av hur den hanteras. Ett tydligt syfte med utförliga beskrivningar i analysen är att den också ska kunna ligga till grund för samverkan med externa aktörer, exempelvis vid ett samråd med Integritetsskyddsmyndigheten avseende dataskydd.

Analysen bör använda verksamhetens ordinarie modell för risk- och sårbarhetsanalyser, vilken kompletteras med de specifika delar som behövs för denna analys. För de offentliga verksamheter som ännu inte infört en egen modell eller behöver uppdatera den hänvisas i första hand till MSB:s metodstöd[7].

I Appendix A beskrivs samtliga delar och aspekter som bedöms behöva tillföras till den övergripande risk- och sårbarhetsanalysen. Dessa är utformade för att kunna läggas till vid användning av MSB:s verktyg för risk- och sårbarhetsanalys[8] och är kompatibla med ISO27000- och ISO31000-serierna.

Bilden nedan visar övergripande modellen för risk- och sårbarhetsanalys. För en närmare nedbrytning se Appendix A och 3.5.2 *Hur kan jag arbeta med vägledningen (metoden)?* Nedan.



Ett konkret exempel för referens på hur en mall för dokumentation av analysen kan utformas som är kompletterad med dessa delar för Microsoft 365 finns i Bilaga 1. Den bygger på MSB:s mall för risk- och sårbarhetsanalys och omfattar de generella kraven i ISO27000- och ISO31000-serierna.

[7] https://www.informationssakerhet.se/metodstodet, 2023-12-18
[8] https://www.informationssakerhet.se/siteassets/metodstod-for-lis/2.-identifiera-och-analysera/verktygslada/verktyg-analys-risk.xlsx, 2023-12-18

2.3 Rättsliga överväganden med analytisk modell

Den analytiska modellen är tänkt att ge underlag och struktur för bedömningen av de centrala juridiska frågorna i GDPR och OSL som verksamheten har att ta ställning till vid ett införande av Microsoft 365. Slutsatserna från de rättsliga övervägandena kan sedan till exempel användas vid den övergripande risk- och sårbarhetsanalysen (se Appendix A), som ett underlag för en konsekvensbedömning avseende dataskydd i relevanta delar eller som ett underlag för beslut om vilka tekniska och administrativa åtgärder som bör väljas vid implementeringen av Microsoft 365 (se Appendix C). Den analytiska modellen belyser flera juridiska bedömningar och ställningstaganden som kan behöva dokumenteras som ett led i införandet av Microsoft 365.

Modellen består av fyra avsnitt; tre om GDPR och ett om OSL. Avsnitten är fristående, och vilket eller vilka avsnitt en verksamhet bör använda sig av beror på hur det är tänkt att Microsoft 365 ska implementeras och vilken typ av information som verksamheten tänkt behandla däri. Med andra ord kan det bli aktuellt att använda den analytiska modellen i samtliga avsnitt eller bara några av dem. Visualiseringarna och scenariobeskrivningarna i Appendix D kan bland annat vara ett stöd i bedömningen av vilka avsnitt i den analytiska modellen som blir aktuella vid olika typer av implementering av Microsoft 365.

Alla fyra avsnitt i Appendix B innehåller

- en beskrivning av den juridiska kontexten,
- en modell för hur den övergripande juridiska frågan kan besvaras, där den är uppdelad i delfrågor som följer på varandra i en systematisk ordning, samt
- information om omständigheter som kan vara relevanta för bedömningen, inklusive om funktionalitet och valmöjligheter i Microsoft 365.

Avsnitten om GDPR blir aktuella att använda om det är tänkt att personuppgifter ska behandlas vid användningen av Microsoft 365. Som visualiseringen och scenariobeskrivningarna i Appendix D illustrerar, kommer användningen av Microsoft 365 i princip alltid innebära att åtminstone personuppgifter om den som använder Microsoft 365 behandlas inom ramen för Azure AD, exempelvis i form av ett användarnamn. Därtill kan det förekomma personuppgifter i den data som användarna för in eller skapar när de arbetar i Microsoft 365. Den analytiska modellen i avsnitten om GDPR hjälper alltså verksamheten att ta ställning till vilka risker eller andra aspekter som kan finnas med att använda Microsoft 365 för att behandla personuppgifter som kan finnas i olika kategorier av data.

Avsnittet om OSL blir aktuellt att använda om det finns regler om sekretess som gäller i verksamheten och om det är tänkt att sådana uppgifter som dessa regler tar sikte på ska hanteras i Microsoft 365. Verksamheter som *inte* har några bestämmelser om sekretess i OSL som gäller för deras uppgifter behöver inte använda denna del av vägledningen eftersom reglerna i OSL i så fall inte kan vara ett hinder för att använda Microsoft 365.

Den analytiska modellen i avsnittet om OSL hjälper alltså den som har bestämmelser om sekretess i OSL som gäller för uppgifter i verksamheten, att ta ställning till om det är tillåtet att använda Microsoft 365 för att behandla dessa uppgifter.

2.4 Administrativa och tekniska mitigerande åtgärder

Microsoft 365 erbjuder en mängd val och inställningar som påverkar hur information behandlas i plattformen. I vägledningen beskrivs många av dessa i samband med scenariobeskrivningens

aktiviteter och detta avsnitt fungerar mer som en sammanfattning och översikt över relevanta administrativa och tekniska mitigerande åtgärder.

Administrativa mitigerande kan vara policys om hur tjänster får användas eller regler hur information ska klassas och hur den, utifrån detta, får hanteras. Tekniska åtgärder kan förstärka de administrativa genom att exempelvis stänga eller styra av funktioner, begränsa om ett dokument får delas externt och så vidare.

Syftet är att med konkreta exempel resonera om när och hur olika åtgärder kan användas för att möta identifierade risker eller andra aspekter och vad de får för effekt på den slutliga analysen. Vägledningen innehåller också exempel på hur funktioner i Microsoft 365 kan hjälpa organisationer att upprätthålla sin informationsklassning med tillhörande skyddsåtgärder.

Läs om administrativa och tekniska mitigerande åtgärder i Appendix C.

2.5 Scenariobeskrivning

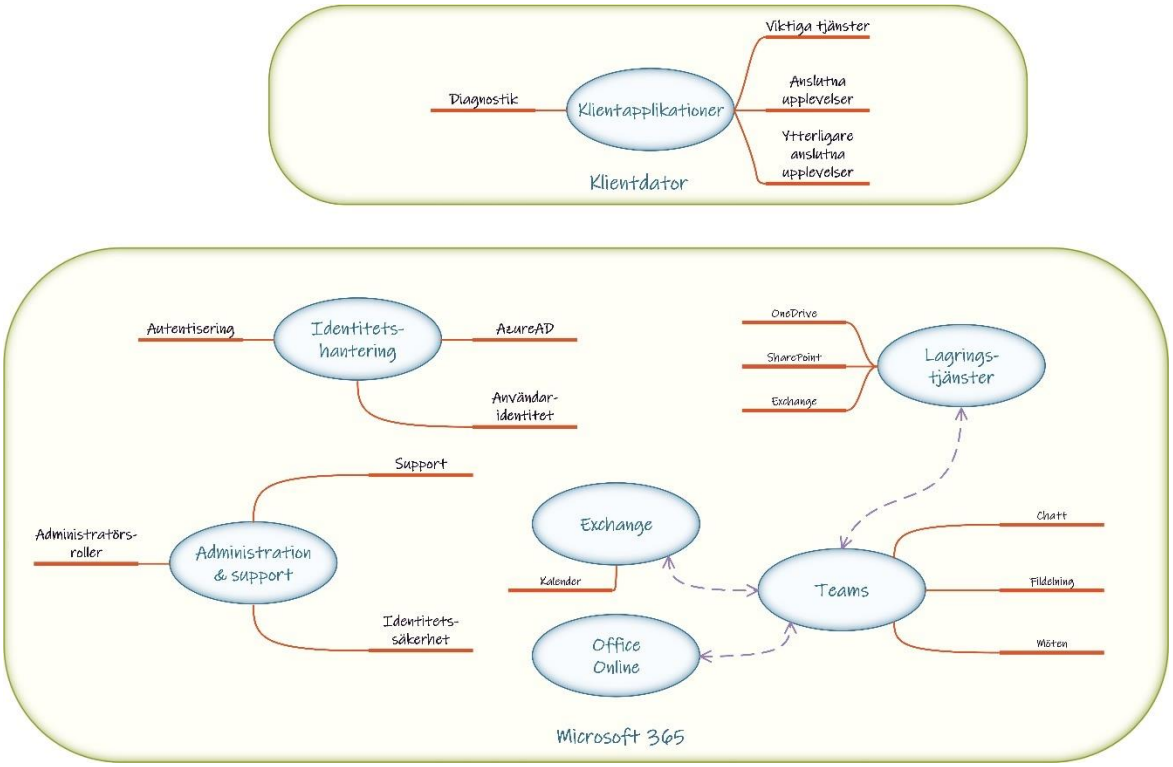
En förutsättning för en framgångsrik riskanalys är att alla inblandande har samsyn i vad analysen omfattar och vilka frågeställningar som är relevanta. Det är också kritiskt att olika kompetenser verkligen förstår varandra och att organisationen använder en väl etablerad och gemensam terminologi. Mot bakgrund av detta innehåller vägledningen ett tänkt scenario som tar sin utgång i typiska verksamhetsbehov av en integrerad plattform för digitalt samarbete såsom Microsoft Teams. I scenariot beskrivs, på ett enkelt och pedagogiskt vis, en handfull aktiviteter som berör exempelvis inloggning, dokumentdelning och möten i Microsoft Teams. För varje aktivitet presenteras ett resonemang kring vilka juridiska, tekniska och administrativa frågeställningar som är relevanta samt vilka åtgärder som är tänkbara.

Syftet med scenariot är att fånga upp huvuddelen av de rättsliga överväganden och mitigerande åtgärder som en offentlig verksamhet såsom en kommun behöver göra vid införande av Microsoft 365. Det ska också fungera som ett stöd för alla typer av intressenter vid diskussioner, workshops, utredningar och dylikt.

Ett scenario baserat på ett fiktivt verksamhetsbehov och Microsoft Teams finns i Appendix D.

2.5.1 Visualisering av Microsoft 365

Som ett komplement till den beskrivande texten i scenariobeskrivningen finns också en visualisering i form av en ”kartbild” av Microsoft 365. Syftet är att ge en övergripande bild av helheten i den önskade implementeringen av Microsoft Teams samt att ytterligare belysa de kritiska noder där en närmare analys behöver ske utifrån juridiska bedömningar, mitigerande administrativa och tekniska åtgärder eller andra aspekter. Vidare belyser visualiseringen samband och beroenden som behöver bedömas i relation till andra centrala komponenter i Microsoft 365.



I ovanstående visualisering beskrivs det vi valt att kalla Kritiska noder. Dessa fokuserar främst på de områden där personuppgifter kan lagras eller behandlas. Några exempel är:

- Identitetshanteringen, som lagrar och behandlar information om alla användare.
- Klientapplikationer, skickar data från om hur de används.
- Tjänster och applikationer som lagrar och behandlar kunddata, det vill säga verksamhetens egen information.

Utan att förringa behovet av att i en risk- och sårbarhetsanalys dyka tillräckligt djupt ner i vissa detaljer, är tanken också att en aktör med denna kartbild i åtanke ska ha möjlighet att bibehålla perspektiv på helheten. Mer om detta beskrivs i Appendix A, Risk- och sårbarhetsanalys och Appendix D, Scenario baserat på ett införande av Microsoft Teams.

Sammanfattningsvis kan denna visualisering, utöver att vara ett stöd i själva risk- och sårbarhetsanalysen, vara till hjälp i många i olika sammanhang som:

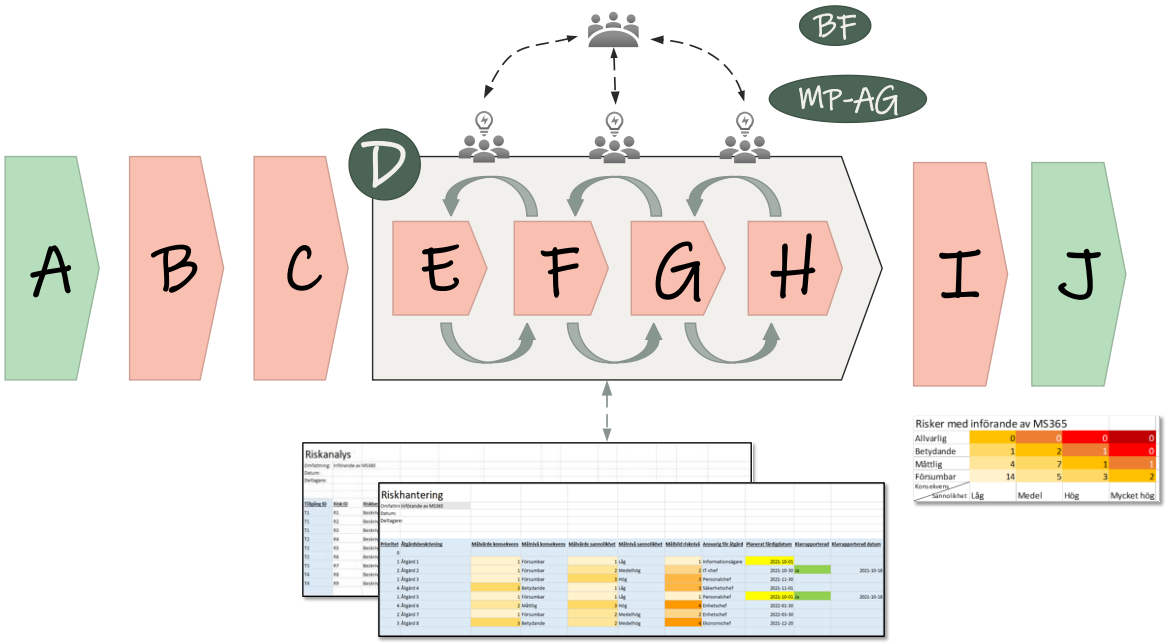
1 Underlag för initial diskussion och etablering av gemensam bild och förståelse utifrån olika perspektiv och kompetenser i en kommun (offentlig sektor) – CIO, CSO, DPO etcetera.
2 Ett sätt att visa för beslutsfattare var olika bedömningarna behöver ske utifrån legala krav och vilka mitigerande administrativa och tekniska åtgärder som kan behöva vidtas vid ett införande av hela eller delar av Microsoft 365.
3 Stöd för olika typer av workshops, utredningsarbete, med mera.
4 Underlag för beskrivning av behandlingen i en konsekvensbedömning (DPIA) avseende dataskydd.

2.6 Hur kan jag arbeta med vägledningen (metoden)?

Utgångpunkten vid skapandet av denna vägledning har varit att den ska kunna vara ett stöd för flera olika professioner i en kommun (eller annan offentlig aktör) vid ett införande av hela eller delar av Microsoft 365. De primära befattningar vi haft i åtanke har varit it-chefer, it-strateger, säkerhetschefer, informationssäkerhetsansvariga, digitaliseringsansvariga, dataskyddsombud och jurister. Även ansvarig förvaltningschef, kommunstyrelse eller motsvarande ska kunna läsa hela eller delar av vägledningen för att skapa sig förståelse för de utmaningar som finns vid ett införande av en molntjänst som denna.

De olika delarna av vägledningen har olika syften och de olika delarna förstärker varandra. Motorn i hela arbetet är den risk- och sårbarhetsanalys som beskrivs i Appendix A: *Modell för risk- och sårbarhetsanalys vid ett införande av Microsoft 365*.

I bilden och tillhörande tabell nedan beskrivs en tänkt process för hur risk- och sårbarhetsanalysen kan ske enligt denna vägledning (modell). Den skiljer sig i princip inte från hur de flesta processer av detta slag bör genomföras förutom att den har ett fokus på ett införande av Microsoft 365. I arbete med en risk- och sårbarhetsanalys av detta slag är det av största vikt att alla de kompetenser som beskrivs ovan aktivt deltar i arbetet och att dessa arbetar integrerat med varandra under hela den tid som analysen genomförs. För att säkerställa att ett integrerat arbete enligt detta kan ske krävs bildandet av det vi valt att kalla för multiprofessionella arbetsgrupper (MP-AG i bilden nedan). Dessa grupper ska sedan med regelbundenhet ha tillgång till beslutsfattare (BF i bilden nedan).

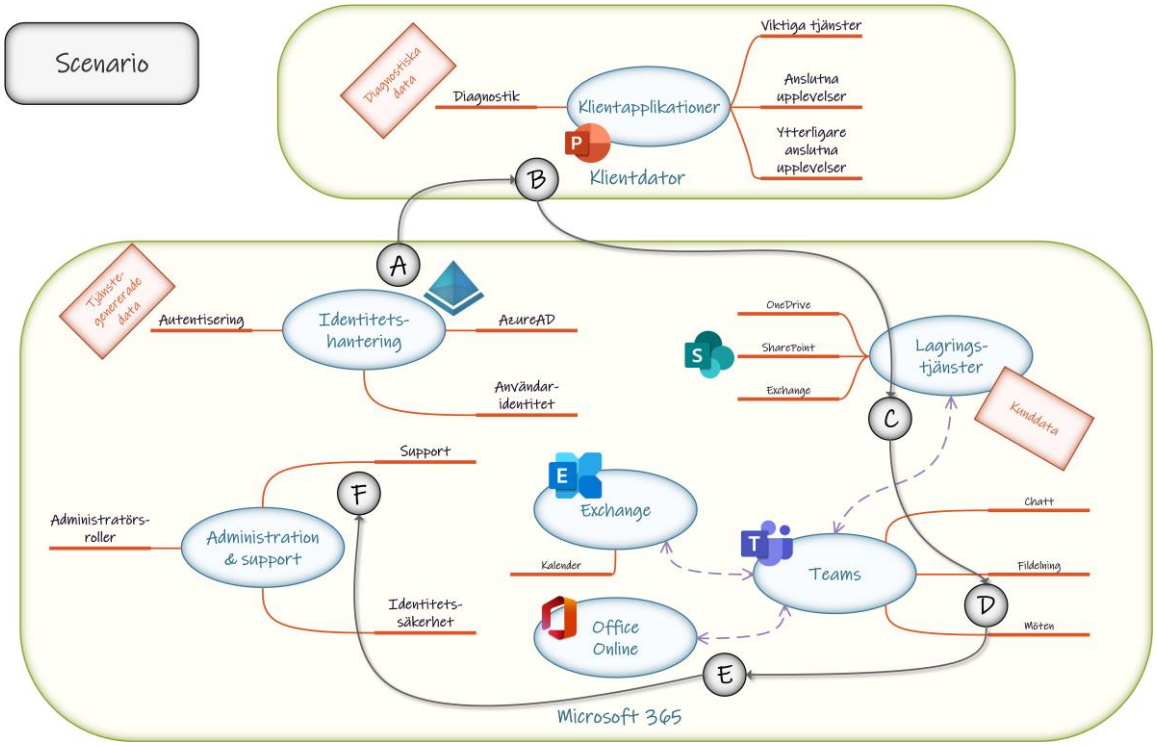


De olika stegen i processen med relevanta frågeställningar

A	**Verksamhetsbehov** ✓ Vilka processer ska systemet stödja? ✓ Vilka är verksamhetens konkreta behov? ✓ Vilka krav ska, respektive bör, systemet uppfylla? ✓ Vilka scenarion finns i just er verksamhet? ✓ Finns det andra alternativ som helt eller delvis skulle kunna användas för att lösa behoven?
B	**Informationskartläggning och -klassning** ✓ Säkerställ att kartläggning och klassning av verksamhetens information är genomförd. Detta är nödvändigt för att kunna genomföra de bedömningar som ingår i analysen och som måste ligga till grund för ett beslut om införande.
C	**Verksamhetens information** ✓ Vilken information kommer att behandlas i tjänsten? ✓ Hur är den informationen klassad? ✓ Omfattas informationen av GDPR? ✓ Omfattas informationen av OSL?
D	**Risk- och sårbarhetsanalys** ✓ Vilka roller och kompetenser ska delta i processen? ✓ Vilka uppdelningar behöver göras i tid eller områden? ✓ Behövs några ytterligare resurser för att kunna genomföra analysen, exempelvis någon mer information?
E	**Juridisk analys** ✓ Utöver GDPR och OSL, vilka andra lagrum och regelverk är relevanta för verksamheten och den information som ska behandlas? ✓ Vilka bedömningar gör ni utifrån vägledningen och analyserna?
F	**Åtgärder** ✓ Vilka åtgärder bidrar till att minska konsekvenserna eller sannolikheterna för riskerna? ✓ Beskriv även åtgärder som bidrar till att hantera konsekvenserna om riskerna trots åtgärder ändå skulle realiseras.
G	**Kvarstående risk** ✓ Finns risker även efter att åtgärderna genomförts? ✓ Kan eventuella kvarstående risker minimeras på andra sätt?
H	**Samlad bedömning** ✓ Är de kvarstående riskerna acceptabla? ✓ Hur bedöms riskerna i de olika alternativen jämfört med varandra?
I	**Beslutsunderlag** ✓ Vilken information och vilka bedömningar ska vara med i beslutsunderlaget? ✓ Sammanställ beslutsunderlaget
J	**Beslut** ✓ Ta beslut. ✓ Dokumentera beslutet. ✓ Dokumentera hur beslutet ska kommuniceras.

Till stöd för detta arbete innehåller vägledningen ett scenario som närmare beskrivs i Appendix D och som övergripande beskrivs under avsnitt 2.5 ovan. Syftet med detta scenario är att stödja aktörer med att beskriva olika aspekter som behöver beaktas vid ett införande av Microsoft 365. Därtill ska scenariot ge exempel på olika aspekter som behöver hanteras i en risk- och sårbarhetsanalys och eventuell konsekvensbedömning. I detta ingår tekniska och administrativa åtgärder och hur dessa kan beaktas samlat och i relation till hela den funktionalitet som verksamheten vill nyttja i Microsoft 365. I scenariot identifieras det vi valt att benämna *kritiska noder*. Dessa noder är valda för att de sammantaget kommer beröra många av de utmaningar en aktör har att ta ställning till vid ett införande.

I bilden nedan syns de olika delarna (kritiska noderna) i det fiktiva scenario som närmare beskrivs i Appendix D. Dessa är utmärkta genom cirklarna i alfabetisk ordning (A-F).



I scenariots olika steg (A-F) berörs följande aspekter:

- Övergripande beskrivning inklusive teknik och arkitektur av den kritiska noden
- Juridik
- Administrativa och tekniska mitigerande åtgärder
- Referenser till Microsofts underlag

För en närmare bild av hur detta kan gestalta sig se Appendix D.

Scenariot ska således kunna användas i flera olika syften, exempelvis för att:

- Hjälpa aktören att se helheten i den önskade implementeringen utan att tappa bort de kritiska noderna.

- Stödja aktören i själva analysen; var finns juridiska och andra utmaningar och vilka mitigerande åtgärder kan vidtas?
- Ge stöd för workshops, utredningsarbete och dokumentation.
- Utgöra underlag för diskussion och etablering av gemensam bild samt förståelse utifrån olika perspektiv och kompetenser i en kommun (offentlig sektor) – CIO, CSO, DPO etcetera.
- Visuellt tydliggöra för beslutsfattare vilka utmaningar som finns vid ett införande av hela eller delar av Microsoft 365 och vilka åtgärder som kan vidtas för att mitigera risker.

Vi som tagit fram denna vägledning har en lång erfarenhet från offentlig sektor och har utgjort ett multiprofessionellt team (MP-AG). Vi är jurister, informationssäkerhets- och molnexperter (Microsoft 365) och tidigare beslutsfattare med lång erfarenhet från arbete med många olika aspekter av dessa frågor. Detta har sammantaget varit en förutsättning för att kunna ta fram denna vägledning (metod). Det har också varit en ”resa” där vi har utmanat, möjliggjort och lärt oss av varandra och på detta sätt hela tiden kunnat tillföra nya aspekter och tankar (analyser) i arbetet. Vår gemensamma bedömning är att detta arbetssätt är en absolut förutsättning för ett framgångsrikt, balanserat och lagligt införande med beaktande av alla de risker och andra aspekter som finns vid ett införande av en tjänst som denna. Med det som utgångspunkt är vår starka rekommendation att kommuner (och andra) skapar denna typ av team (MP-AG) vid ett införande av Microsoft 365 och därtill har med utpekade beslutsfattare (BF) i hela arbetet med införandet. Då denna vägledning är generisk utifrån verksamheter är det centralt att varje aktör som har för avsikt att införa en molntjänst som Microsoft 365 gör detta utifrån sina förutsättningar.

3 Övergripande om Microsoft 365 och relevanta regelverk

3.1 Microsoft 365

Microsoft 365 är i sitt grundutförande en amerikansk global molntjänst som erbjuder applikationer och tjänster för produktivitet och samarbete som exempelvis SharePoint, OneDrive, Exchange och Teams. Plattformen kan användas på flera olika sätt då den innehåller allt från lagring och delning av dokument till intranätfunktioner och digitala möten. I Microsoft 365 ingår även ”Office-programmen”, det vill säga klientapplikationer som exempelvis Word, Excel, PowerPoint och e-postklienten Outlook.

Översikt över Microsoft 365 för företag
Microsoft 365 för företag är en komplett och intelligent lösning som gör att alla kan samarbeta och arbeta tillsammans på ett säkert sätt.

Microsoft 365 för Enterprise, som är utformat för stora organisationer men kan även användas för medelstora och små företag som behöver de mest avancerade funktionerna för säkerhet och produktivitet.

Komponenter
Microsoft 365 för företag består av:

Tjänster	***Beskrivning***
Lokala appar och molnbaserade appar och produktivitetstjänster	*Innehåller både Microsoft 365-appar för företag, de senaste Office-app[arna] för PC-och Mac (till exempel Word, Excel, PowerPoint, Outlook och andra) samt en komplett uppsättning onlinetjänster för e-post, fillagring och samarbete, möten och mycket mer.*
Windows 10 Enterprise	*Uppfyller behovet av både stora och medelstora organisationer. Det är den mest produktiva och säkra versionen av Windows för användare. För IT-tekniker tillhandahåller det även omfattande hantering av installationer, enheter och appar.*
Enhetshantering och avancerade säkerhetstjänster	*Innehåller Microsoft Intune, som är en molnbaserad tjänst för Enterprise Mobility Management som gör det lättare för personalen att arbeta produktivt och skydda din organisationsdata.*

Referens: Översikt över Microsoft 365 för företag - Microsoft 365 Enterprise | Microsoft Docs

3.1.1 Microsofts molndesign

Microsoft Molndesign för offentlig sektor, MSMD, är ett ramverk av råd och verktyg som kan stödja verksamheter i den offentliga sektorn i sin användning av Microsoft 365. Designen är tänkt för organisationer som omfattas av regleringar och lagar som exempelvis GDPR och OSL.

På en övergripande nivå innehåller MSMD följande komponenter:

Microsoft Secure Score & Security Compliance Toolkit, stödjer konfiguration, mätning och uppföljning för att säkerställa skyddsåtgärder i Microsoft 365.
Compliance Manager, kan användas för arbete med regelefterlevnad genom att översätta krav till åtgärder samt mäta graden av efterlevnad.
E-Discovery & Data Subject Request, kan användas för att hantera och svara på förfrågningar om åtkomst, rättelse, radering och export av personuppgifter i Microsoft 365.
Microsoft Information Protection, kan användas för att klassa och kontrollera tillgång till information i Microsoft 365, till exempel enligt principerna för KLASSA från Sveriges Kommuner och Regioner (SKR).
Mall för Data Protection Impact Assessment (DPIA), kan användas för att göra en konsekvensbedömning (DPIA) om behov finns.
Utbildning i MSMD hos Microsofts partner.
Customer Lockbox, som inför ett extra administrativt steg för godkännande innan Microsofts personal får ta del av kunddata eller andra datakategorier. Detta kan exempelvis användas för sekretessprövning vid supportärenden.
Double Key Encryption krypterar tillgång till data för Microsoft med verksamhetens egen krypteringsnyckel.
Microsoft 365 Hybrid med Exchange och SharePoint lokalt installerad (on prem), som kan användas för att lagra vissa data lokalt och annan data i Microsoft 365.

”Microsoft Molndesign: Offentlig Sektor för Azure och Microsoft 365
Genom vår nya molndesign gör vi det nu enklare för offentlig sektor att börja använda molntjänster från Microsoft. Paketet innehåller verktyg, mallar, policyer, rapporter och utbildningar som tillsammans tydliggör hur molntjänster kan användas i enlighet med de regleringar, krav och lagar som gäller för offentlig sektor i Sverige.

Microsoft Molndesign är framtagen för att underlätta för offentlig sektor att använda molntjänster från Microsoft med mycket hög IT-säkerhet och innehåller ett antal verktyg som förenklar uppfyllnad av regleringar och lagar som GDPR och OSL. Microsoft Molndesign innehåller verktyg för både IT-tjänster i molnet via Azure och användande av molnbaserade produktivitetsverktyg som Microsoft 365.”

Referens: Microsoft Molndesign: Offentlig sektor

3.1.2 Microsofts olika datatyper

I en molntjänst skapas och lagras olika typer av data. Dessa kan delas in i kategorier vilket kan underlätta för att vid behov vidta skyddsåtgärder som är anpassade för en specifik kategori. Som exempel går det att dela in riskanalysen i olika delar där en analys endast hanterar personuppgifter i kunddata, och andra analyser hanterar andra kategorier.

Microsoft delar in data i följande kategorier:

Kunddata: Kunddata är alla de data, inklusive text, ljud, video, bildfiler och programvara, som du tillhandahåller till Microsoft eller som tillhandahålls för din räkning genom din användning av Microsofts onlinetjänster för företag, med undantag för Microsoft Professionella tjänster. Det omfattar kunddata, som är de data som du laddar upp för lagring eller bearbetning, och appar som du laddar upp för distribution via en Microsoft-molntjänst för företag. Kundinnehåll omfattar till exempel e-post och bilagor i Exchange Online, Power BI-rapporter, SharePoint Online-webbplatsinnehåll eller chattkonversationer.
Personliga uppgifter: Personliga uppgifter avser all information som rör en identifierad eller identifierbar fysisk person. En identifierbar fysisk person är någon som kan identifieras, direkt eller indirekt, till exempel ett namn, id-nummer, platskoordinater, online-id eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, mentala, ekonomiska, kulturella eller sociala identitet. Microsoft använder samma GDPR-definition för personuppgifter. Det omfattar pseudonymiserade data. Förutom att personliga uppgifter är en delmängd av administratörsdata och betalningsdata är personliga uppgifter också en delmängd av var och en av de datakategorier som anges ovan.
Data från Professionella tjänster: Data från Professionella tjänster avser alla de data, inklusive alla text-, ljud-, video- och bildfiler samt programvara, som tillhandahålls till Microsoft av eller på uppdrag av en kund (eller som kunden tillåter Microsoft att hämta från en produkt) eller som på annat sätt hämtas eller bearbetas av eller på uppdrag av Microsoft genom överenskommelse med Microsoft om att hämta Professionella tjänster.
Administratörsdata: Administratörsdata är information om administratörer som levereras under registrering, inköp eller administration av Microsoft-tjänster, till exempel namn, telefonnummer och e-postadresser. Det omfattar också aggregerad användningsinformation och data som är kopplade till ditt konto, till exempel de kontroller du väljer. Vi använder administratörsdata för att tillhandahålla tjänster, slutföra transaktioner, betjäna kontot och upptäcka och förebygga bedrägerier.
Betalningsdata: Betalningsdata är den information du tillhandahåller när du köper något online hos Microsoft. Det kan innehålla kreditkortsnummer och säkerhetskod, namn, faktureringsadress och annan finansiell information. Vi använder betalningsdata för att slutföra transaktioner och för att upptäcka och förebygga bedrägerier.

Genom att förstå vilka typer av data som finns i Microsoft molntjänster blir det enklare att använda komponenterna i MSMD och tillämpa dem på olika kategorier av data.
Referens: [Microsofts kategorier för onlinetjänster | Säkerhetscenter]

3.1.3 Microsofts ”kontroller” för att begränsa access och tillgång till data

Microsoft beskriver i sitt standardiserade dataskyddstillägg (DPA) vilka säkerhetsåtgärder de vidtagit för leveransen av Microsoft 365.

”Säkerhetsrutiner och säkerhetspolicyer
Microsoft ska implementera och upprätthålla lämpliga tekniska och organisatoriska åtgärder avsedda att skydda kunddata, data i Professionella tjänster och personuppgifter mot oavsiktlig eller olaglig förstöring, förlust, ändring, obehörigt utlämnande av eller åtkomst till personuppgifter som överförs, lagras eller i övrigt behandlas. Dessa åtgärder ska anges i en Microsoft-säkerhetspolicy. Microsoft ska göra den policyn tillgänglig för Kunden, tillsammans med annan information som Kunden skäligen begär angående Microsofts säkerhetsrutiner och säkerhetspolicyer.

Dessa åtgärder ska därutöver uppfylla de krav som anges i ISO 27001, ISO 27002 och ISO 27018. Kunder har tillgång till en beskrivning av säkerhetskontrollerna för dessa krav.”

Gällande DPA kan hittas på http://aka.ms/dpa.

Bilaga A i ”Dataskyddstillägg för Microsofts produkter och tjänster” beskriver de åtgärder Microsoft åtar sig att upprätthålla inom följande områden:

- Organisation av informationssäkerhet
- Tillgångshantering
- HR-säkerhet
- Fysisk säkerhet och miljösäkerhet
- Kommunikations- och verksamhetshantering
- Åtkomstkontroll
- Incidenthantering avseende informationssäkerhet
- Hantering av affärskontinuitet

Bilaga C i samma dokument beskriver ytterligare säkerhetsåtgärder. Mer information från Microsoft finns också här:

- Data locations for the European Union - How Microsoft protects your data | Microsoft Docs

3.1.4 Oberoende granskningar av efterlevnad för Microsoft 365

Microsoft har samlat alla certifikat och rapporter från externa revisioner på i sin ”Service Trust Portal” under avsnittet ”Audit Reports”[9]. Här finns bland annat oberoende granskningar av Microsoft 365 utifrån standarderna ISO 27001, ISO 27017, ISO 27018, ISO 27701 och ISO 22301.

3.2 Relevanta regelverk

Detta avsnitt innehåller en övergripande beskrivning av flera regelverk som är relevanta vid användning av molntjänster. Innehållet i avsnittet kommer i huvudsak att utgå från kommuner och de regelverk som är relevanta för dessa.

[9] Audit Reports (microsoft.com), 2023-12-18

De regelverk och rättsområden som beskrivs i det är avsnittet är:

- GDPR med kompletterande regelverk,
- OSL,
- Lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster,
- MSB:s föreskrifter på området,
- Säkerhetsskyddslagen (2018:585)
- samt vissa frågor om upphovsrätt och immateriella rättigheter.

3.2.1 GDPR med kompletterande regelverk

EU:s dataskyddsförordning 2016/679 (GDPR) är ett EU-rättsligt regelverk som syftar till att harmonisera skyddet för personers rättigheter och friheter vid behandling av personuppgifter och säkerställa det fria flödet av personuppgifter inom EU. GDPR är tillämplig på alla verksamheter som behandlar personuppgifter och det görs ingen skillnad på om verksamheten är i privat eller offentlig sektor. GDPR är ett omfattande regelverk och innebär bland annat att verksamheter måste följa de grundläggande principerna, se till att personuppgiftsbehandlingen har en rättslig grund och informera de registrerade om hur deras personuppgifter hanteras. På dataskyddsområdet finns det förutom GDPR även en mängd annan lagstiftning som kan vara bra att känna till. Det innebär att det kan finnas flera tillämpliga lagar samtidigt och särskilda regler för en viss myndighet eller verksamhet i andra författningar.

GDPR gäller i sin helhet i svensk rätt och det krävs därför inte någon kompletterande svensk lagstiftning. I förordningen ges dock en möjlighet för medlemsstaterna att införa kompletterande nationella bestämmelser. Detta har i svensk rätt gjorts i lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen). Syftet med dataskyddslagen är att begränsa eller förtydliga vissa bestämmelser samt göra dessa begripliga för de personer eller verksamheter som omfattas av GDPR. Utöver dataskyddslagen har även regeringen gett ut en förordning som kompletterar både GDPR och dataskyddslagen. Förordning (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning innehåller vissa specifika förtydligande bestämmelser. Till sist finns det även bestämmelser om dataskydd i olika registerförfattningar som gäller för en viss myndighet, en grupp av myndigheter eller i en viss typ av verksamhet. Registerförfattningarna innehåller särskilda regler som är anpassade efter den aktuella verksamheten.

GDPR kompletteras även med praxis från framförallt Europeiska unionens domstol (EU-domstolen). Bland annat har EU-domstolens dom i det så kallade Schrems II-målet[10] fått stor betydelse för tolkningen av vad som gäller vid överföring av personuppgifter till länder utanför EU/EES. Även nationella domstolars avgöranden och vägledningar från den Europeiska dataskyddsstyrelsen (EDPB) kan vara av intresse vid tolkningen av GDPR.

3.2.2 Offentlighets- och sekretesslagen (OSL)

Enligt 2 kap. TF har var och en rätt att ta del av allmänna handlingar. Denna rätt får endast begränsas om det är nödvändigt med hänsyn till vissa särskilda intressen och begränsningarna ska tydligt anges i en bestämmelse eller lag. I svensk rätt återfinns dessa begränsningar i OSL och den innehåller regler om myndigheters handläggning vid registrering, utelämnande och övrig

[10] Dom av den 16 juli 2020 i mål C-311/18 Data Protection Commissioner mot Facebook Ireland Ltd och Maximilian Schrems.

hantering av allmänna handlingar. Utöver det innehåller lagen även bestämmelser om sekretess och tystnadsplikt. Bestämmelserna i OSL syftar till att reglera både hanteringen av allmänna handlingar och sekretessreglerade handlingar.

Tillämpningsområdet för OSL är allmänna handlingar, vilka definieras i TF:s andra kapitel. Med handling avses enligt 2 kap. 3 § TF ”en framställning i skrift eller bild samt en upptagning som endast med tekniska hjälpmedel kan läsas eller avlyssnas eller uppfattas på annat sätt.” Definitionen på handling är därmed bred och det är mycket som innefattas i begreppet. För att en handling ska ses som allmän krävs att den förvaras hos, inkommer till eller upprättas hos myndigheten. En upptagning, till exempel en elektronisk handling, anses vara förvarad hos myndigheten om den är tillgänglig för myndigheten med ett tekniskt hjälpmedel som gör att handlingen kan läsas, avlyssnas eller uppfattas på annat sätt. En handling anses inkommen till myndigheten när den anlänt till behörig befattningshavare, eller om det gäller en elektronisk handling så när den är tillgänglig med ett tekniskt hjälpmedel. En handling anses upprättad hos myndigheten när den expedierats, eller om den inte gjort det, när det ärende som den tillhör slutbehandlats eller om handlingen på annat sätt färdigställts.

Det finns vissa handlingar som visserligen uppfyller de ovan nämnda kriterierna för att vara *allmänna handlingar*, men som av olika anledningar inte ska vara tillgängliga för var och en. Dessa handlingar skyddas genom sekretess, vilket innebär ett förbud mot att röja en uppgift genom utlämnande av allmän handling.

Ur ett informationssäkerhetsperspektiv kan OSL anses ha två olika syften. Det ena syftet är att se till att allmänna handlingar är tillgängliga, riktiga och spårbara. Med det menas att den information som allmänheten har rätt till ska finnas tillgänglig hos myndigheten. Utöver att den ska vara tillgänglig ska informationen vara uppdaterad och korrekt. Till sist ska informationen vara strukturerad på ett sådant sätt att den går att spåra eller hitta. Det andra syftet är att se till att de handlingar som omfattas av sekretess inte finns tillgängliga för de som inte ska ha tillgång till informationen.

Den 1 juli 2023 genomfördes en förändring av OSL då en ny sekretessbrytande bestämmelse infördes i 10 kap. 2 a §. Förändringen är tänkt att möjliggöra utlämnande av uppgifter som omfattas av sekretess genom användning av en molntjänst när leverantörens uppdrag endast är *teknisk bearbetning* och *teknisk lagring* av uppgifterna.

3.2.3 NIS-direktivet / Lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster och MSB:s föreskrifter

Syftet med NIS-direktivet är att förbättra den inre marknadens funktion genom att ställa krav på säkerhet i nätverks- och informationssystem. I korthet innebär det krav på informationssäkerhet och incidentrapportering för vissa särskilda aktörer. Regleringen är tillämplig på leverantörer av samhällsviktiga tjänster och vissa digitala tjänster. De leverantörer som omfattas av reglerna kan finnas både i offentlig och privat sektor. I direktivet identifieras sju sektorer som tillhandahåller samhällsviktiga tjänster. Dessa är bankverksamhet, digital infrastruktur, energi, finansmarknadsinfrastruktur, hälso- och sjukvård, leverans och distribution av dricksvatten samt transport. Det är verksamheten själv som ansvarar för att identifiera sig som en samhällsviktig tjänst.

I svensk rätt har NIS-direktivet implementerats i lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster samt i förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster. Som ett komplement till de två nämnda regelverken har MSB meddelat ett antal föreskrifter som rör bland annat informationssäkerhet för statliga myndigheter (MSBFS 2020:6) och säkerhetsåtgärder i informationssystem för statliga myndigheter (MSBFS 2020:7). Även om dessa regelverk primärt är för statliga myndigheter är det vanligt att andra aktörer i offentlig sektor använder dem som stöd i sitt systematiska informationssäkerhetsarbete.

För kommuner specifikt gäller vissa särskilda föreskrifter från MSB. Den första är MSB:s föreskrift om anmälan och identifiering av leverantörer av samhällsviktiga tjänster (MSBFS 2018:7), vilken är särskilt tillämplig på kommunala verksamheter som bedriver samhällsviktig verksamhet. Den andra är MSB:s föreskrift och allmänna råd om kommuners risk- och sårbarhetsanalyser (MSBFS 2015:5), där krav på informationssäkerhet finns med som en indikator för bedömning av kommunens generella krisberedskap.

Den 14 december 2022 fattade EU beslut om ett nytt direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå inom hela unionen (NIS 2-direktivet). NIS 2-direktivet ska börja tillämpas den 18 oktober 2024 och ska dessförinnan genomföras i svensk rätt. Jämfört med det första NIS-direktivet kommer NIS 2-direktivet ha ett större tillämpningsområde och omfatta flera nya sektorer av samhällsviktiga tjänster. NIS 2-direktivet innehåller även högt ställda och mer konkreta krav på säkerhetsåtgärder för de verksamheter som omfattas. Vidare innehåller NIS 2-direktivet mer kännbara sanktioner och ett utpekat ansvar för ledningen i de organisationer som omfattas.

3.2.4 Säkerhetsskyddslagen

Säkerhetsskyddslagen (2018:585) är tillämplig för den som bedriver säkerhetskänslig verksamhet. Med säkerhetskänslig verksamhet menas en verksamhet som är av betydelse för Sveriges säkerhet. Sådana verksamheter kan finnas både i offentlig sektor och i privat verksamhet. Bedömningen av vad som utgör säkerhetskänslig verksamhet får göras i ljuset av samhällsutvecklingen. Tidigare var det framför allt Försvarsmaktens verksamheter som förknippades med Sveriges säkerhet, men idag finns det även andra aktörer som har uppgifter och information som kan vara känsligt för rikets säkerhet. Sådana typer av uppgifter kan bland annat handla om viktig civil infrastruktur som flygplatser eller energianläggningar.

De krav som ställs på de verksamheter som omfattas av lagen är att de ska ha skydd mot spionerі, sabotage, terroristbrott och andra brott som kan hota verksamheten och skydd av säkerhetsskyddsklassificerade uppgifter. Utöver säkerhetsskyddslagen finns även säkerhetsskyddsförordningen (2018:586) som innehåller kompletterande bestämmelser.

I denna vägledning kommer vi inte att fördjupa oss närmare i säkerhetsskyddslagstiftningen.

3.2.5 Krav på säkerhet i andra regelverk

Utöver dessa mer generella regelverk som har nämnts ovan finns det specifika krav i annan lagstiftning som gäller säkerhet för specifika verksamheter eller informationstyper, till exempel inom hälso- och sjukvården. Anledningen till att de specifika regelverken finns är att den verksamhet eller den information som de rör är väldigt skyddsvärd och att brister i *konfidenitalitet, riktighet* eller *tillgänglighet* kan få allvarliga konsekvenser.

3.2.6 Upphovsrätt och immateriella rättigheter

I Microsofts användarvillkor[11] framgår det att användaren av tjänsten vidhåller äganderätten till innehållet på tjänsten och att Microsoft inte gör något anspråk på den äganderätten. Vidare i villkoret stadgas att Microsoft dock förbehåller sig en ”global, royaltyfri immateriell rättighet” att använda användares innehåll. Microsoft menar att en sådan immateriell rättighet krävs för att tillhandahålla och förbättra tjänsten. Med det menas att Microsoft har rätt att använda innehållet utan kostnad, men att det inte är samma sak som att de äger innehållet.

[11] https://www.microsoft.com/sv-se/servicesagreement/ 2023-12-18

4 Framtida utveckling inom området

Microsoft utvecklar kontinuerligt sina molnplattformar och de tjänster som erbjuds. Det innebär att den som använder sig av denna vägledning även bör utforska vilket utbud av tjänster Microsoft har vid det tillfället.

Till exempel pågår fortfarande utvecklingen av Microsoft EU Data Boundary, en europeisk datagräns för Microsofts molntjänster. Det ger utökade möjligheter för kunder att både behandla och lagra alla personuppgifter i EU, Norge eller Schweiz. Mer om detta finns i avsnitt 3.3 i Appendix B.

Inom juridiken sker det också förändringar som kan komma att påverka frågeställningarna och slutsatserna som behandlas i denna vägledning. Även om GDPR funnits sedan år 2018 saknas det i flera delar fortfarande vägledande praxis för hur bestämmelserna ska tolkas (se avsnitt 3 i Appendix B). Detsamma gäller den nya sekretessbrytande regeln i 10 kap. 2 a § OSL, vars praktiska tillämpningsområde ännu till viss del är oklart (se avsnitt 4 i Appendix B). Det är därför viktigt att följa rättsutvecklingen på området.

knowit

Appendix A – Modell för risk- och sårbarhetsanalys vid ett införande av Microsoft 365

1. Inledning

Detta appendix beskriver en modell för den risk- och sårbarhetsanalys som en offentlig verksamhet, exempelvis en kommun, behöver göra inför beslut att använda Microsoft 365. Analysmetoden har ett verksamhetsperspektiv och utgår från att verksamheten (kommunen) gör en avvägd bedömning av alla de aspekter som påverkar verksamheten. Analysen bör därför omfatta både verksamhetens användning av tjänsten Microsoft 365 inklusive vilka behov, möjligheter och begränsningar som föreligger, och de lagar och regelverk som är tillämpliga. Den kan då också utgöra underlag för jämförelse mellan att införa Microsoft 365, någon annan tjänst, eller att helt undvika att införa någon tjänst alls.

En förutsättning för att kunna genomföra en risk- och sårbarhetsanalys och avvägd bedömning av alla de risker och andra aspekter som påverkar ett eventuellt införande av Microsoft 365, likväl som någon annan motsvarande tjänst, är ett strukturerat och kontinuerligt informationssäkerhetsarbete inom verksamheten. Det är också en definitiv förutsättning för att upprätthålla informationssäkerhet över tid, oavsett tjänster. Två av de viktigaste delarna i ett sådant arbete är informationskartläggning och klassning av informationstillgångar.

2. Omfattning

Detta är primärt en kompletterande del, om än betydande, till den analys som verksamhetsutövaren behöver göra inför användning av en molnbaserad tjänst. Vi adresserar främst de aspekter som härrör till Dataskyddsförordningen (GDPR) och tillhörande regelverk, Offentlighets- och sekretesslagen (OSL) och i tillämpliga delar andra regelverk, standarder, generella verksamhetsbehov samt andra aspekter. Det som därutöver behöver ingå i verksamhetsutövarens analys är bland annat specifika verksamhetsbehov samt eventuella ytterligare krav från författningar eller avtal som verksamheten omfattas av.

3. Exempel på risker och andra aspekter att beakta

Följande generaliserade exempel är möjliga risker eller andra aspekter, identifierade med utgångspunkt i de aktuella regelverken, som en verksamhetsutövare kan behöva hantera.

Felaktig hantering av personuppgifter
Att personuppgifter hanteras felaktigt, exempelvis utanför avsedd miljö, eller läcker till extern part kan vara en risk som behöver beaktas oavsett tjänst eller teknisk miljö. Risker med att personuppgifter hanteras felaktigt kan ha flera perspektiv, exempelvis som integritetsrisk, juridisk risk och varumärkesrisk.

Verksamhetsbrister
Att verksamhetsutövaren genom bristande funktion inte uppfyller sina åtaganden gentemot kunder, medlemmar, medborgare eller andra är en aspekt som vi bedömer ofta behöver beaktas i sammanhanget. Detta kan avse ett behov av digitala tjänster för att kunna utföra verksamhetens uppdrag på ett acceptabelt sätt utifrån gällande regelverk.

Generella it-säkerhetsrisker
Generella it-säkerhetsrisker, exempelvis i form av it-attacker, behöver beaktas av alla verksamhetsutövare som använder digitala tjänster eller verktyg. Dessa risker har generellt sett ökat och bedöms under överskådlig framtid fortsätta utgöra konkreta risker för verksamheter inom målgruppen för vägledningen.

Olovlig underrättelseinhämtning
Att extern part genom underrättelseinhämtning olovligen tar del av information ur tjänsten är en risk som kan behöva beaktas, men som har mycket stora skillnader i värdering beroende på verksamhetens art och specifika omständigheter för den aktuella verksamhetsutövaren.

4. Beskrivning av modellen

Modellen för riskanalys som här presenteras är tydligt strukturerad i steg och utgår från de krav som ställs inom respektive regelverk och i förekommande fall från verksamheten själv. Bedömningarna i de olika delarna av analysen är ofta komplexa och omfattande. Detta gäller i allra högsta grad bedömningar avseende GDPR och OSL. Dessa bör därför genomföras som särskilda aktiviteter. Underlag för att genomföra bedömningar inom dessa två områden återfinns i Appendix B, Rättslig analys. De utförliga beskrivningarna av de identifierade riskerna eller andra aspekter så som bedömningar, motiv för bedömningarna och resultaten av dessa bör också dokumenteras separat. Resultaten av bedömningarna i respektive del återförs till risk- och sårbarhetsanalysen och kan där bedömas och jämföras med övriga aspekter och bedömningar. Modellen samlar därmed kravställningarna, bedömningarna av dessa, hur de är tillämpliga i verksamheten, åtgärder som vidtas för att hantera dessa samt bedömningar av eventuella kvarvarande risker eller andra aspekter på en och samma plats. Detta möjliggör ett komplett underlag som stöd för införandebeslutet liksom dokumentation av de bedömningar som ligger till grund för beslutet.

Modellen är kompatibel med MSB:s metodstöd för informationssäkerhet[1], ISO27000[2]- och ISO31000[3]-serierna och bedöms passa väl med den offentliga verksamhetens ordinarie risk- och sårbarhetsanalys. I detta sammanhang framhålls särskilt ISO/IEC 27005:2022 Vägledning om riskhantering inom informationssäkerhet[4] samt för dataskydd ISO/IEC 27701:2019 Tillägg till ISO/IEC 27001 och ISO/IEC 27002 för hantering av personuppgifter – Krav och vägledning[5].

[1] https://www.informationssakerhet.se/metodstodet/, 2023-12-15.
[2] https://www.sis.se/produkter/informationsteknik-kontorsutrustning/allmant/ss-en-isoiec-2700120232/, 2023-12-15.
[3] https://www.sis.se/produkter/foretagsorganisation/foretagsorganisation-och-foretagsledning-ledningssystem/foretagsorganisation/ss-iso-310002018/, 2023-12-15.
[4] https://www.sis.se/produkter/foretagsorganisation/tjanster/ovrigatjanster/ss-isoiec-270052022/, 2023-12-15.
[5] https://www.sis.se/produkter/informationsteknik-kontorsutrustning/itsakerhet/ss-en-isoiec-2770120212/, 2023-12-15.

5. Risk- och sårbarhetsanalysens uppbyggnad

Processen är huvudsakligen uppdelad i tre delar; identifiering av risker eller andra aspekter, hantering av dem i form av åtgärder och uppföljning av åtgärderna. Eftersom delar av analysen kan vara mycket omfattande bör den som nämnt ovan delas upp i flera delområden och tillfällen. Två delområden som behöver analyseras för sig är GDPR och OSL. Dessa beskrivs utförligt i Appendix B, Rättslig analys.

Analysen genomförs i följande steg:

1. Arbetsgrupp med kompetenser som behövs för genomförande av den aktuella analysen sätts samman utifrån verksamhetens behov och möjligheter. Person med mandat att fatta beslut avseende riskanalysen bör leda arbetet. Dokumentation av analysen i mallen bör göras av en utsedd person.

2. Omfattning för aktuell analys fastställs liksom nivåer för konsekvenser och sannolikheter i enlighet med verksamhetens riskhanteringspolicy eller motsvarande. I den föreslagna mallen för dokumentation av analysen ingår även förslag till nivåindelningar. Vilka konsekvenser respektive sannolikheter som medför vilken nivå bör specificeras av verksamheten.

3. Risker och andra aspekter identifieras och beskrivs tydligt. Åtminstone huvuddelen av riskerna bör identifieras innan arbetet fortskrider till att hantera dem.
    a. Kategori för respektive risk bör beskrivas redan här i syfte att tydliggöra och särskilja vilken slags risk som avses.
    b. Orsak till respektive konsekvens av risken beskrivs.
    c. Värden för konsekvens och sannolikhet fastställs.
    d. Riskägare fastställs om det i detta läge är möjligt.

4. Åtgärder eller annan hantering för respektive identifierad risk eller annan aspekt dokumenteras.
    a. Prioritet för respektive risk eller annan aspekt fastställs för att påvisa om, och i så fall med vilken ambition den ska åtgärdas.
    b. En eller flera åtgärder dokumenteras för varje risk med deras respektive bedömda målvärden för konsekvens och sannolikhet. Detta avser kvarstående risknivåer efter att åtgärden är genomförd.
    c. Ansvarig för respektive åtgärd fastställs och bör uttryckas med befattning eller roll.
    d. Tidpunkt för när åtgärden ska vara genomförd bör fastställas och dokumenteras.

Mallen i Bilaga 1 innehåller dessutom fält för uppföljning av åtgärderna med möjlighet att dokumentera när de genomförts. Verksamhetsutövare kan här också fastställa och dokumentera åtgärder för incidenthantering om risker trots vidtagna åtgärder ändå skulle realiseras. Alternativt kan referens till sådan kontinuitetsplanering noteras här.

Nedan visualiseras modellen i tre bilder. Den första bilden (bild A) visar övergripande modellen för risk- och sårbarhetsanalys. Den andra bilden (bild B) visar den del av modellen som beskriver bedömningar avseende GDPR. Detta markeras i bild A med B. Den tredje bilden (C) visar den del av modellen som beskriver bedömningar avseende OSL. Detta markeras i bild A med C. Mallen för den samlade dokumentationen av analysen markeras i bild A med D. Dokumentation av analysen i mallen beskrivs närmare nedan.

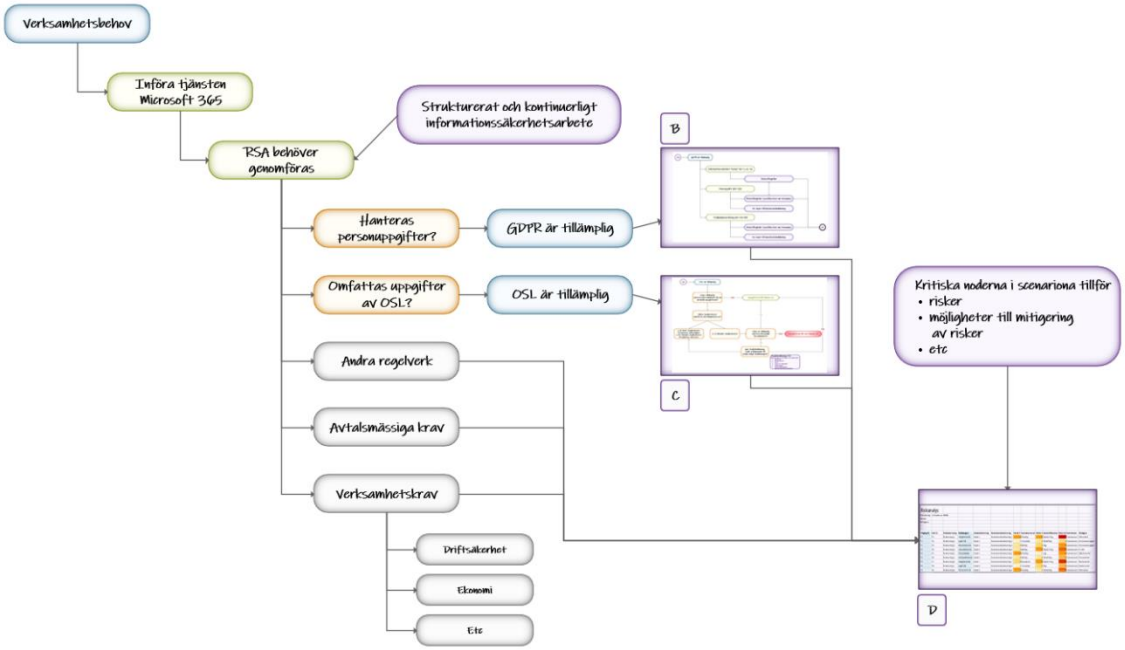


Bild A. Övergripande bild över modellen för risk- och sårbarhetsanalys.

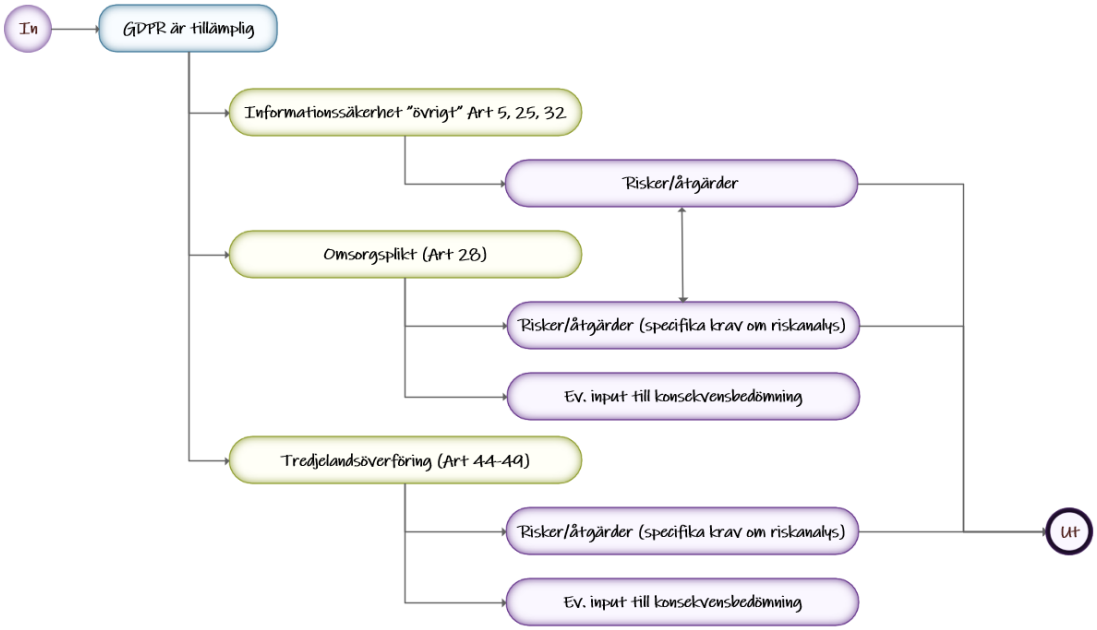


Bild B. Del av modellen som beskriver bedömningar avseende GDPR.

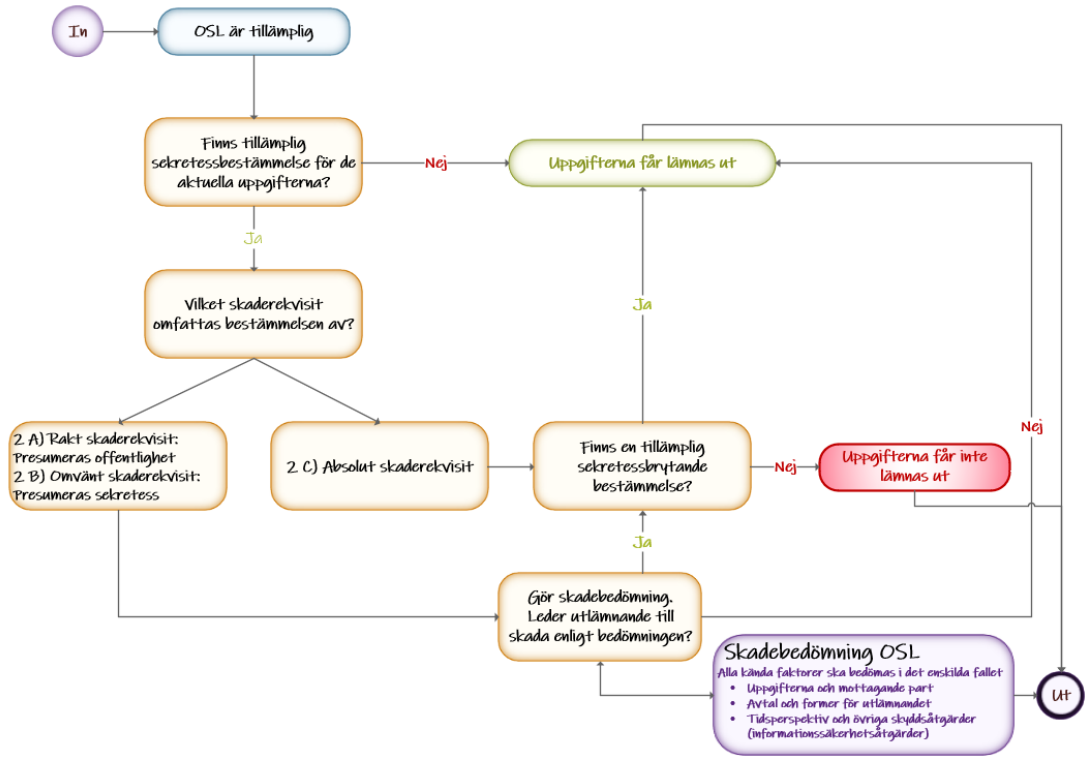


Bild C. Del av modellen som beskriver bedömningar avseende OSL.

6. Dokumentation av analysen i mallen

Mallen är både ett stöd för praktiskt genomförande av analysen och ett underlag för dokumentation av resultaten. Dokumentationen fyller flera syften, varav spårbarhet till bedömningar av risker eller andra aspekter, och värderingar av planerade åtgärder med eventuella kvarstående risker är nödvändiga delar för införandebeslutet. Dokumentation med spårbarhet genom hela analysprocessen behövs också för uppföljning av planerade åtgärder och kommunikation med både interna och externa mottagare.

Bilden nedan (D) visar första steget i mallen för dokumentation av analysen som närmare beskrivs i Bilaga 1.

Riskanalys

Omfattning: Införande av MS365
Datum:
Deltagare:

Tillgång ID	Risk ID	Riskbeskrivning	Riskkategori	Orsaksbeskrivning	Konsekvensbeskrivning	Värde K	Konsekvensnivå	Värde S	Sannolikhetsnivå	Risknivå	Kommentar	Riskägare
T1	R1	Beskrivning 1	Integritetsrisk	Orsak 1	Konsekvensbeskrivning 1	4	Allvarlig	4	Mycket hög		Kommentar 1	Enhetschef
T1	R2	Beskrivning 2	Legal risk	Orsak 2	Konsekvensbeskrivning 2	1	Försumbar	2	Medelhög	2	Kommentar 2	Informationsägare
T1	R3	Beskrivning 3	Ekonomisk risk	Orsak 3	Konsekvensbeskrivning 3	2	Måttlig	3	Hög	4	Kommentar 3	Informationsägare
T2	R4	Beskrivning 4	Varumärkesrisk	Orsak 4	Konsekvensbeskrivning 4	2	Måttlig	4	Mycket hög	5	Kommentar 4	IT-chef
T2	R5	Beskrivning 5	Personskada	Orsak 5	Konsekvensbeskrivning 5	4	Allvarlig	1	Låg	4	Kommentar 5	Säkerhetschef
T2	R6	Beskrivning 5	Verksamhetsrisk	Orsak 6	Konsekvensbeskrivning 6	2	Måttlig	2	Medelhög	3	Kommentar 6	Personalchef
T3	R7	Beskrivning 6	Integritetsrisk	Orsak 7	Konsekvensbeskrivning 7	3	Betydande	4	Mycket hög	6	Kommentar 7	Ekonomichef
T4	R8	Beskrivning 7	Legal risk	Orsak 8	Konsekvensbeskrivning 8	1	Försumbar	3	Hög	3	Kommentar 8	Kvalitetschef
T4	R9	Beskrivning 8	Ekonomisk risk	Orsak 9	Konsekvensbeskrivning 9	4	Allvarlig	2	Medelhög	5	Kommentar 9	Enhetschef

Bild D. Mallens steg 1, Riskidentifiering (fiktiva uppgifter).

Detaljerad beskrivning av de ingående delarna i modellen beskrivs i Bilaga 1.

Observera att det ifyllda underlaget kan vara känsligt och behöver klassas avseende informationssäkerhet och hanteras utifrån klassningen.

7. Resultat och underlag för beslut om införande av Microsoft 365

Resultaten av genomförda risk- och sårbarhetsanalyser är bland annat dokumenterade bilder av kvarstående risker eller andra aspekter efter att beslutade åtgärder är vidtagna. I vår modell är det primärt dessa resultat som bör ligga till grund för införandebeslutet, tillsammans med andra underlag från ekonomiska bedömningar etc. Med jämförelse av de olika alternativen kan ett avvägt beslut fattas utifrån vad de innebär för verksamheten, och vad de kräver i form av åtgärder för att uppfylla verksamhetens behov och tillämpliga regelverk.

Bilderna nedan visar sammanställningar över risker i tre fiktiva fall. Den första visar identifierade risker eller andra aspekter med att inte införa någon tjänst alls. Den andra visar kvarstående risker eller andra aspekter efter införande av Microsoft 365 med vidtagna åtgärder. Den tredje visar kvarstående risker eller andra aspekter efter införande av annan tjänst med vidtagna åtgärder.

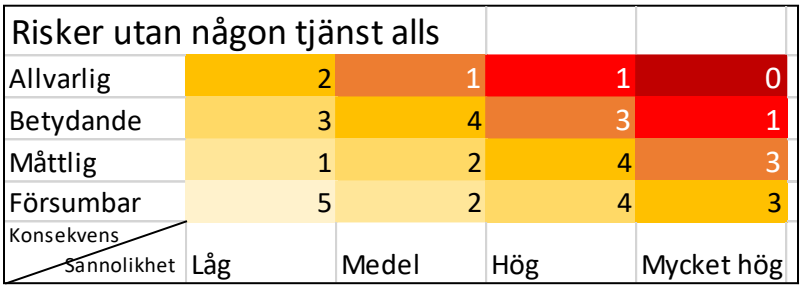


Bild E. Risker från analys av ett fiktivt exempel om att inte införa någon tjänst alls.

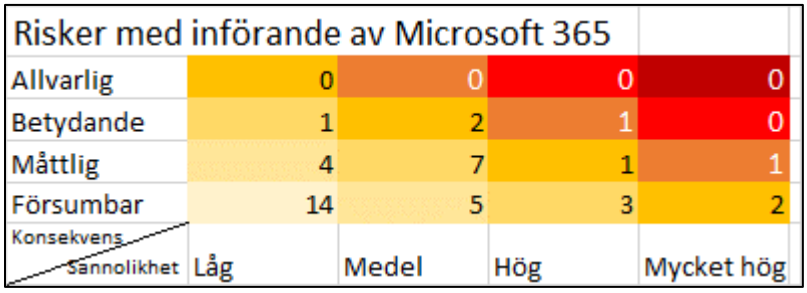


Bild F. Kvarstående risker från analys av ett fiktivt exempel om att införa Microsoft 365.

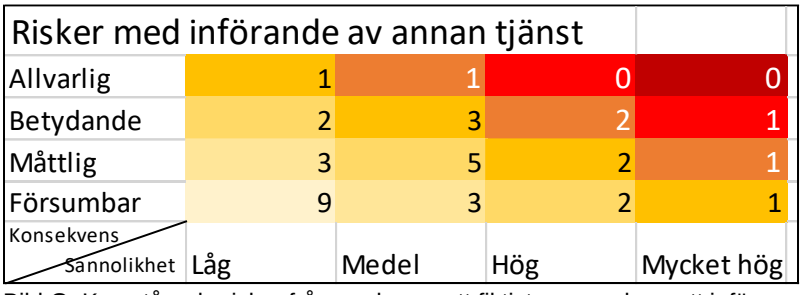


Bild G. Kvarstående risker från analys av ett fiktivt exempel om att införa annan molntjänst.

knowit

Appendix B – Rättsliga överväganden med analytisk modell

Detta appendix belyser de juridiska frågorna, primärt utifrån de rättsregler som styr behandling av personuppgifter (i första hand Dataskyddsförordningen [GDPR]) och hantering av sekretessreglerade uppgifter (Offentlighets- och sekretesslagen [OSL]). Appendixet riktar sig till den som har behov av ett mer ingående juridiskt underlag i dessa frågor. Det syftar till att beskriva gällande rätt och vilka rättsliga bedömningar som kan behöva vidtas samt till att ge stöd och vägledning i dessa. Den analytiska modellen i detta appendix är tänkt att ge underlag och struktur för bedömningen av de centrala juridiska frågorna i GDPR och OSL som verksamheten har att ta ställning till vid ett införande av Microsoft 365.

Slutsatserna från de rättsliga övervägandena kan sedan till exempel användas

- vid den övergripande risk- och sårbarhetsanalysen (se Appendix A),
- som ett underlag för en konsekvensbedömning avseende dataskydd i relevanta delar eller
- som ett underlag för beslut om vilka tekniska och administrativa åtgärder som bör väljas vid implementeringen av Microsoft 365 (se Appendix C).

Den analytiska modellen belyser flera juridiska bedömningar och ställningstaganden som kan behöva dokumenteras som ett led i införandet av Microsoft 365.

Modellen består av fyra avsnitt; tre om GDPR och ett om OSL. Avsnitten är fristående, och vilket eller vilka avsnitt en verksamhet bör använda sig av beror på hur det är tänkt att Microsoft 365 ska implementeras och vilken typ av information som verksamheten tänkt behandla däri. Med andra ord kan det bli aktuellt att använda den analytiska modellen i samtliga avsnitt eller bara i några av dem.

Visualiseringarna och scenariobeskrivningarna i Appendix D kan bland annat vara ett stöd i bedömningen av vilka avsnitt i den analytiska modellen som blir aktuella vid olika typer av implementering av Microsoft 365.

Alla tre avsnitt i Appendix B innehåller

- en beskrivning av den juridiska kontexten,
- en modell för hur den övergripande juridiska frågan kan besvaras, där den är uppdelad i delfrågor som följer på varandra i en systematisk ordning, samt
- information om omständigheter som kan vara relevanta för bedömningen, inklusive om funktionalitet och valmöjligheter i Microsoft 365.

I de olika avsnitten förekommer flera frågeställningar, resonemang och beskrivningar som är snarlika. Ni bör vara uppmärksamma på att det är olika frågor som ska bedömas och att det finns skillnader både i vad de bestämmelser det gäller syftar till och vilken betydelse samma faktiska omständigheter har för utgången av bedömningen av respektive fråga.

Den analytiska modellen i avsnitten om GDPR hjälper verksamheten att ta ställning till vilka risker som kan finnas med att använda Microsoft 365 för att behandla personuppgifter.

Det första avsnittet i GDPR-delen handlar om de krav på lämplig it-/informationssäkerhet som GDPR kräver att verksamheten ställer om en molntjänst så som Microsoft 365 används för att hantera personuppgifter.

I det efterföljande avsnittet om GDPR redogörs för omsorgsplikten när en verksamhet använder sig av ett personuppgiftsbiträde såsom vid användning av Microsoft 365. Därefter ges en metod för hur verksamheterna ska kunna göra sina egna bedömningar om omsorgsplikten. I varje del finns en beskrivning av den juridiska kontexten och information om omständigheter som kan vara relevanta för bedömningen av Microsoft 365. Valda informationssäkerhetsåtgärder och eventuell påverkan av tredjelands lagstiftning är exempel på områden som kan behöva ingå i bedömningen inom ramen för omsorgsplikten och som därför beskrivs i det här avsnittet.

I det tredje avsnittet i detta appendix redogörs för de steg som verksamheterna ska ta vid en tredjelandsöverföring. Avsnittet inleds med en beskrivning av vad en överföring till tredjeland är (avsnitt 3.2). Därefter följer avsnittet i stora drag de rekommendationer som EDPB har gett i området. I varje del finns en beskrivning av den juridiska kontexten och information om omständigheter, inklusive om funktionalitet och valmöjligheter i Microsoft 365, som kan vara relevanta för bedömningen.

Avsnittet om OSL blir aktuellt att använda om det finns regler om sekretess som gäller i verksamheten och om det är tänkt att sådana uppgifter som dessa regler tar sikte på ska användas i Microsoft 365. Verksamheter som inte har några bestämmelser om sekretess i OSL som gäller för deras uppgifter behöver inte använda denna del av vägledningen eftersom reglerna i OSL i så fall inte kan vara ett hinder för att använda Microsoft 365.

Den analytiska modellen i avsnittet om OSL hjälper alltså den som har bestämmelser om sekretess i OSL som gäller för uppgifter i verksamheten att ta ställning till vilka risker som kan finnas med att använda Microsoft 365 för att behandla dessa uppgifter.

Vidare beskriver avsnittet om OSL en förändring av OSL som genomfördes den 1 juli 2023. Förändringen är tänkt att möjliggöra utlämnande av uppgifter som omfattas av sekretess genom användning av en molntjänst när leverantörens uppdrag är teknisk bearbetning och teknisk lagring av uppgifterna.

Dokumentationsplikten
Analysen ni gör i det följande ska dokumenteras, främst för att ni ska kunna uppfylla er ansvarsskyldighet enligt GDPR[1]. Analysen i det följande är inte en konsekvensbedömning avseende dataskydd enligt GDPR[2], även om innehållet i denna analys kan användas som underlag för en sådan.

[1] Artikel 5 GDPR.
[2] Artikel 35 GDPR.

Nedan visualiseras de analytiska modellerna i två bilder. Den första bilden (bild A) visar den del av modellen som beskriver bedömningar avseende GDPR. Den andra bilden (B) visar den del av modellen som beskriver bedömningar avseende OSL.

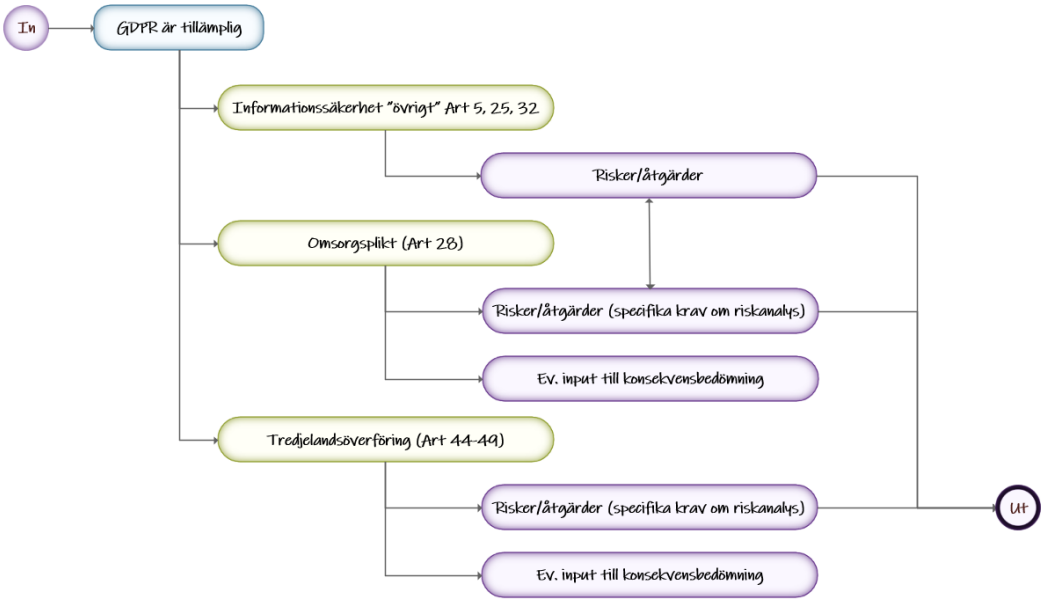


Bild A ovan. Del av modellen som beskriver bedömningar avseende GDPR.

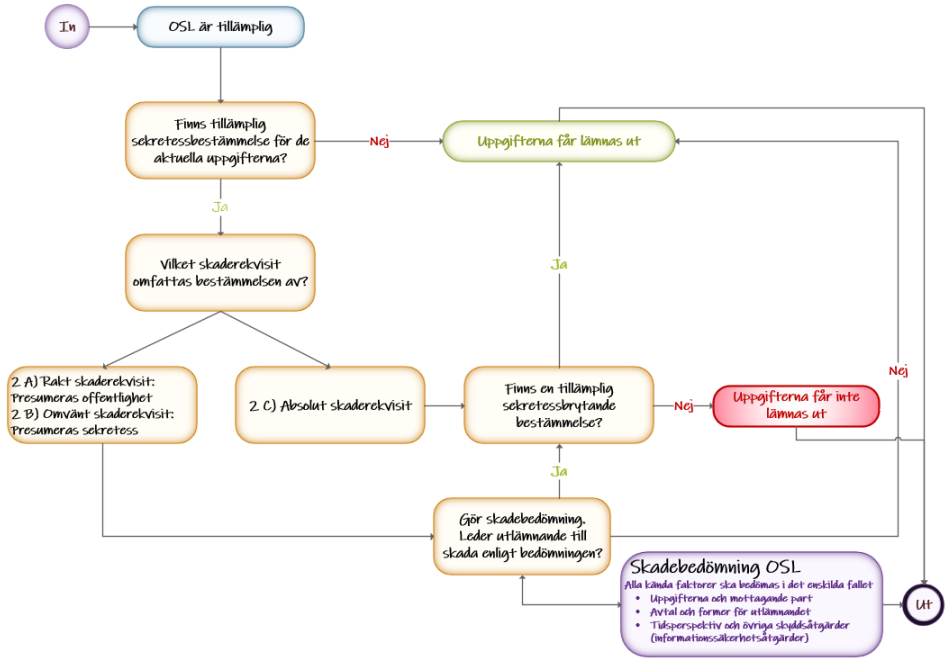


Bild B ovan. Del av modellen som beskriver bedömningar avseende OSL.

1 Informationssäkerhet enligt GDPR

1.1 Vad behandlas i detta avsnitt?

Det här avsnittet av den analytiska modellen hjälper verksamheten att ta ställning till om de krav på lämplig it-/informationssäkerhet som GDPR ställer på verksamheten uppfylls vid användningen av Microsoft 365.

I detta avsnitt ges en kort översikt på de relevanta bestämmelserna i GDPR som berör säkerhet (avsnitt 1.2). Därefter beskrivs en modell för hur verksamheterna ska kunna göra sina egna bedömningar om säkerhetskraven vid anlitandet av Microsoft 365 (avsnitt 1.3). I varje del finns en beskrivning av den juridiska kontexten och information om omständigheter, inklusive om funktionalitet och valmöjligheter i Microsoft 365, som kan vara relevanta för bedömningen av frågan.

1.2 Säkerhet enligt artikel 32 GDPR

Personuppgifter ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder (integritet och konfidentialitet)[3].

Den personuppgiftsansvarige ska därför – med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter – vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken.[4] Detta inbegriper när det är lämpligt,

a) pseudonymisering och kryptering av personuppgifter,

b) förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och -tjänsterna,

c) förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident,

d) ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet[5].

När ni behandlar personuppgifter måste ni därför se till att alla personuppgifter ni behandlar skyddas så att ingen obehörig kommer åt dem och de inte används på ett otillåtet sätt. Ni ska också se till så att personuppgifter inte förloras eller blir förstörda, till exempel genom olyckshändelser. Det innebär att ni måste välja *tekniska och organisatoriska säkerhetsåtgärder* som skyddar uppgifterna på ett lämpligt sätt.

[3] Artikel 51 f GDPR.
[4] Artikel 32 och skäl 74 GDPR.
[5] Artikel 32.1 p. a-d GDPR.

Exempel

Tekniska säkerhetsåtgärder[6]

- autentisering
- behörighetsspärrar
- brandväggar
- kryptering
- pseudonymisering
- säkerhetskopiering
- antivirusskydd

Organisatoriska säkerhetsåtgärder[7]

- tilldelning av åtkomsträttigheter
- interna rutiner
- instruktioner
- riktlinjer

Begreppen *tekniska och organisatoriska åtgärder* förekommer i olika sammanhang i GDPR. Även om det i många fall rör sig om samma åtgärder i praktiken, är det viktigt att göra skillnad på de olika bedömningarna. Vissa tekniska och organisatoriska åtgärder kan nämligen anses vara effektiva och lämpliga utifrån bestämmelserna om informationssäkerhet i artikel 32, utan att de för den skull anses vara lika effektiva som kompletterande skyddsåtgärder för den som till exempel stödjer sig på standardavtalsklausuler vid tredjelandsöverföringar (se avsnitt 3.6.5).

1.3 Bedömning av lämpliga tekniska och organisatoriska åtgärder

1.3.1 Underlag för bedömningen

För att kunna göra en bedömning av vilka tekniska och organiska åtgärder som är lämpliga i förhållande till risken med behandlingen i Microsoft 365 är det viktigt att ni dels vet vilka typer av uppgifter ni ska använda i Microsoft 365, i vilket sammanhang och i vilken omfattning de ska behandlas samt för vilka ändamål; dels att ni har kunskap om vilka åtgärder ni respektive Microsoft kommer att vidta för skydda uppgifterna.

Till att börja med behöver ni fundera på vilka verksamheter som är tänkta att använda Microsoft 365 och vilken typ av uppgifter som kan komma att behandlas i Microsoft 365. Besvara följande frågor och dokumentera svaren.

- Vilka kategorier av uppgifter om vilka kategorier av personer kommer hanteras i Microsoft 365?
- Hur omfattande är behandlingen (antal uppgifter, antal personer, tidsperiod)?
- Vad är syftet med behandlingen?
- I vilken typ av verksamhet sker behandlingen?

Sedan behöver ni fundera på och dokumentera hur ni har tänkt implementera Microsoft 365, det vill säga vilken funktionalitet och vilka säkerhetsåtgärder ni har tänkt använda. I Appendix C finns en utförlig beskrivning av de säkerhetsåtgärder som erbjuds i Microsoft 365. Visualiseringen och

[6] IMY,https://www.imy.se/verksamhet/dataskydd/dataskydd-pa-olika-omraden/arbetsliv/tillaten-behandling--vilka-krav-galler/sakerhet/, 2023-12-15.
[7] IMY,https://www.imy.se/verksamhet/dataskydd/dataskydd-pa-olika-omraden/arbetsliv/tillaten-behandling--vilka-krav-galler/sakerhet/, 2023-12-15.

scenariobeskrivningen i Appendix D kan också ge vägledning när det gäller vilka alternativ som finns.

Besvara följande frågor och dokumentera svaren.

- Vilka säkerhetslösningar i Microsoft 365 har ni tänkt implementera?
- Vilka tekniska och organisatoriska åtgärder har ni tänkt implementera vid sidan av Microsoft 365, till exempel interna rutiner för hur Microsoft 365 ska användas?

1.3.2 Bedömning

Det första steget i att bedöma vilka tekniska och organisatoriska åtgärder som är lämpliga är att bedöma vilken *risk* som är förknippad med behandlingen. Ni behöver därför göra en grundlig riskanalys[8] för att förstå vilka konsekvenser otillräcklig säkerhet för behandlingen skulle kunna få. Besvara följande frågor och dokumentera svaren.

- Vilka konsekvenser skulle det få för de personer vars uppgifter ni kommer att behandla om personuppgifter som ni kommer att behandla
    - mister sin *konfidentialitet?*
    - *ändras eller raderas* oavsiktligen?
    - är *otillgängliga* under en kortare eller längre tid?

Det är konsekvenser för fysiska personers fri- och rättigheter (integritetsrisk) som ska bedömas, inte konsekvenser för verksamheten. Exempel på konsekvenser som kan vara intressanta är fysisk, materiell eller immateriell skada[9] som drabbar den vars personuppgifter det gäller.

I nästa steg ska ni bedöma hur planerade tekniska och organisatoriska säkerhetsåtgärder påverkar sannolikheten för att dessa konsekvenser skulle förverkligas. Besvara följande frågor och dokumentera svaren.

- Hur påverkas sannolikheten för att de tänkbara konsekvenserna realiseras av
    - de säkerhetslösningar i Microsoft 365 som ni tänkt använda?
    - de tekniska och organisatoriska åtgärder som ni tänkt implementera vid sidan av Microsoft 365?
- Är de tilltänkta åtgärderna lämpliga med hänsyn till slutsatsen från riskanalysen?
- Finns det andra åtgärder som är lämpliga att vidta, med hänsyn tagen även till kostnaderna och möjligheterna att genomföra åtgärderna?[10]

[8] IMY, https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/informationssakerhet/, 2023-12-15.
[9] Skäl 83 GDPR.
[10] IMY, https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/informationssakerhet/, 2023-12-15.

Exempel på säkerhetsåtgärder i Microsoft 365

I Appendix C finns en utförlig beskrivning av de säkerhetsåtgärder som erbjuds i Microsoft 365. Visualiseringen och scenariobeskrivningarna i Appendix D kan också ge vägledning när det gäller vilka alternativ som finns. Nedan följer några exempel på säkerhetsåtgärder som erbjuds i Microsoft 365.

- ✓ **Microsoft Secure Score & Security Compliance Toolkit**, stödjer konfiguration, mätning och uppföljning för att säkerställa att det finns tillräckliga skyddsnivåer för personuppgifter i Microsoft 365.
- ✓ **E-Discovery & Data Subject Request**, gör det möjligt att hantera och svara på förfrågningar om åtkomst, rättelse, radering och export av personuppgifter i Microsoft 365.
- ✓ Mall för **Data Protection Impact Assessment (DPIA)**, underlättar arbetet med att göra en DPIA om behov finns.
- ✓ **Utbildning** i MSMD hos Microsofts partner.
- ✓ **Double Key Encryption** (eller motsvarande) som krypterar tillgång till data för Microsoft via organisationens egen krypteringsnyckel.
- ✓ **Microsoft 365 Hybrid** med Exchange och SharePoint lokalt installerad, gör det möjligt att lagra vissa data lokalt och annan data i Microsoft 365.
- ✓ **End-to-end encryption** innebär möjligheten till kryptering mellan slutpunkter.
- ✓ **Customer Lockbox** som innebär en ytterligare möjlighet att begränsa informationsdelning vid supportärenden.

* * *

Om de tekniska och organisatoriska åtgärder som ni planerar att vidta är lämpliga i förhållande till risken, uppfyller ni kraven i artikel 32 GDPR.

Anser ni att de tekniska och organisatoriska åtgärder som ni planerar att vidta *inte* är lämpliga i förhållande till risken enligt artikel 28, bör ni överväga om det finns ytterligare tekniska och organisatoriska åtgärder som skulle vara lämpliga och som skulle kunna implementeras. Om så är fallet, gör om bedömningen ovan.

Ni är nu klara med alla steg i avsnitt 1 i den här modellen. Ni bör dokumentera era bedömningar och använda aktuella slutsatser som en del i den risk- och sårbarhetsanalys som genomförs med stöd av Appendix A. Fortsätt till avsnitt 2.

2 Omsorgsplikten

2.1 Vad behandlas i detta avsnitt?

Det här avsnittet av den analytiska modellen hjälper verksamheten att ta ställning till om den så kallade *omsorgsplikten* är uppfylld vid anlitandet av Microsoft med den tilltänkta implementeringen av Microsoft 365.

Avsnittet inleds med en beskrivning av omsorgsplikten innebär (avsnitt 2.2) och de olika frågor som verksamheten behöver ta ställning till med anledning av den. Därefter beskrivs en modell för hur verksamheterna ska kunna göra sina egna bedömningar om omsorgsplikten är uppfylld vid anlitandet av Microsoft med den tilltänkta implementeringen av Microsoft 365 (avsnitt 2.3–2.4). I varje del finns en beskrivning av den juridiska kontexten och information om omständigheter, inklusive om funktionalitet och valmöjligheter i Microsoft 365, som kan vara relevanta för bedömningen av frågan.

2.2 Omsorgsplikten enligt artikel 28 GDPR

2.2.1 Introduktion

Om en behandling ska genomföras på en personuppgiftsansvarigs vägnar ska den personuppgiftsansvarige endast anlita personuppgiftsbiträden som *ger tillräckliga garantier* om att genomföra *lämpliga tekniska och organisatoriska åtgärder* på ett sådant sätt att behandlingen uppfyller kraven i denna förordning och säkerställer att den registrerades rättigheter skyddas[11].

När den personuppgiftsansvarige anlitar ett personuppgiftsbiträde måste den uppfylla omsorgsplikten[12] oavsett vilket personuppgiftsbiträde den anlitar och oavsett om behandlingen kommer att innebära en tredjelandsöverföring eller inte. Omsorgsplikten innebär att den personuppgiftsansvarige behöver utreda vilka förutsättningar personuppgiftsbiträdet har att efterleva sina skyldigheter enligt dataskyddsregelverket. Den personuppgiftsansvarige ska med andra ord göra en riskbedömning avseende personuppgiftsbiträdets förmåga att efterleva sina skyldigheter vid val av biträde.[13] Ett personuppgiftsbiträdes anslutning till en godkänd uppförandekod får användas för att visa att tillräckliga garantier tillhandahålls.[14]

[11] Artikel 28 GDPR.
[12] Artikel 28 GDPR.
[13] Säker och kostnadseffektiv IT-drift – rättsliga förutsättningar för utkontraktering, även kallad it-driftsutredningen (SOU 2021:1), sida 202.
[14] Artikel 28.5, artikel 40 och 41 GDPR.

Skäl 81 GDPR

För att se till att kraven i denna förordning uppfylls vad gäller behandling som av ett personuppgiftsbiträde ska utföras på en personuppgiftsansvarigs vägnar ska den personuppgiftsansvarige, när denne anförtror behandling åt ett personuppgiftsbiträde, endast använda personuppgiftsbiträden som *ger tillräckliga garantier*, i synnerhet i fråga *om sakkunskap, tillförlitlighet och resurser, för att genomföra tekniska och organisatoriska åtgärder* som uppfyller kraven i denna förordning, bl.a. vad gäller säkerhet i samband med behandlingen av uppgifter. Personuppgifts biträdets anslutning till en godkänd uppförandekod eller en godkänd certifieringsmekanism kan användas som ett sätt att påvisa att den personuppgiftsansvarige fullgör sina skyldigheter. När uppgifter behandlas av ett personuppgiftsbiträde, bör hanteringen regleras genom ett avtal eller en annan rättsakt enligt unionsrätten eller medlemsstaternas nationella rätt mellan personuppgiftsbiträdet och den personuppgiftsansvarige, där föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och kategorier av registrerade anges, med beaktande av personuppgiftsbiträdets specifika arbets- och ansvarsuppgifter inom ramen för den behandling som ska utföras och risken med avseende på den registrerades rättigheter och friheter. […] Efter det att behandlingen på den personuppgiftsansvariges vägnar har avslutats, bör personuppgiftsbiträdet återlämna eller radera personuppgifterna, beroende på vad den personuppgiftsansvarige väljer, såvida inte lagring av personuppgifterna krävs enligt den unionsrätt eller medlemsstaternas nationella rätt som personuppgiftsbiträdet omfattas av.

2.2.2 Vad menas med tillräckliga garantier om lämpliga tekniska och organisatoriska åtgärder?

Begreppet *tillräckliga garantier* i artikel 28 GDPR har inte definierats i förordningen. Det framgår inte heller i övrigt hur garantierna ska lämnas eller vilka garantier som är tillräckliga. Med det sagt framgår det av skäl 81 GDPR att tillräckliga garantier ska i synnerhet ges i fråga *om sakkunskap, tillförlitlighet och resurser*, för att genomföra tekniska och organisatoriska åtgärder.[15] Begreppet *tillräckliga* antyder att det ska göras en helhetsbedömning av risken med de tilltänkta behandlingarna samt vilka garantier som ska ses som tillräckliga med hänsyn till dessa risker.[16]

Begreppet *lämpliga tekniska och organisatoriska åtgärder* saknar även en direkt definition i artikel 28 GDPR, men förekommer i flera andra artiklar i GDPR.[17] Vilka organisatoriska och tekniska åtgärder som ska ses som lämpliga ska avgöras med beaktande av *behandlingens art, omfattning, sammanhang* och *ändamål* samt *riskerna för fysiska personers rättigheter och friheter* enligt artikel 25 GDPR. Även om den sistnämnda bestämmelsen skiljer sig i innehållet från omsorgsplikten i artikel 28, har dessa bestämmelser liknande syften i att vidta åtgärder för att uppfylla förordningen och skydda de registrerades rättigheter. Det ligger i sakens natur att även i artikel 28 beakta *behandlingens art, omfattning, sammanhang* och *ändamål* samt *riskerna för fysiska personers rättigheter och friheter* vid avgörandet av lämpligheten om de tekniska och organisatoriska åtgärder som ska vidtas så att behandlingen uppfyller förordningen. En sådan tolkning är även i linje med skäl 81 som är hänförlig till omsorgsplikten.

[15] Säker och kostnadseffektiv it-drift, SOU 2021:1 s. 202.
[16] EDPB, Riktlinjer 07/2020 angående begreppen personuppgiftsansvarig och personuppgiftsbiträde i GDPR, version 2.0, s. 34.
[17] Artikel 25 och 32 GDPR.

Att åtgärderna ska vara *lämpliga* innebär att de ska vara lämpliga i förhållande behandlingens art, omfattning, sammanhang och ändamål samt riskerna för fysiska personers rättigheter och friheter.[18]

Mot denna bakgrund behöver ni svara på två sammanhängande frågor:

- Vilka tekniska och organisatoriska åtgärder är *lämpliga* i ert fall?
- Lämnar Microsoft *tillräckliga garantier* om att genomföra sådana lämpliga åtgärder?

2.3 Bedömning av lämpliga tekniska och organisatoriska åtgärder

2.3.1 Inför bedömningen

För att kunna göra en bedömning av vilka tekniska och organiska åtgärder som är *lämpliga* för personuppgiftsbiträdet att genomföra i ert fall är det viktigt att ni först vet vilka typer av uppgifter ni ska använda i Microsoft 365, i vilket sammanhang och i vilken omfattning de ska behandlas samt för vilka ändamål. Besvara följande frågor och dokumentera svaren.

2.3.1.1 Kategorier av personuppgifter och behandlingens art

- Vilka kategorier av personer rör uppgifterna som kommer hanteras i Microsoft 365?
    - Är det till exempel endast anställda?

- Vilka typer av uppgifter kommer hanteras i Microsoft 365?
    - Är det harmlösa uppgifter såsom e-postadress eller namn?
    - Förekommer det känsliga personuppgifter?
    - Förekommer det personnummer eller samordningsnummer?

Känsliga personuppgifter är uppgifter om, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i en fackförening, hälsa sexualliv eller sexuell läggning, genetiska uppgifter och biometriska uppgifter som används för att entydigt identifiera en person.[19] I Bilaga 5 finns en närmare beskrivning av detta.

Personnummer och samordningsnummer är inte känsliga personuppgifter enligt definitionen i artikel 9 GDPR, men anses vara extra skyddsvärda och får endast behandlas om det är *klart motiverat* enligt 3 kap.10 § lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

2.3.1.2 Behandlingens omfattning, sammanhang och ändamål

- I vilken typ av verksamhet och i vilket sammanhang sker behandlingen?
- Hur omfattande är behandlingen (antal uppgifter, antal personer, tidsperiod)?
- Om uppgifterna lagras under en längre period, hur lång är denna period?
- Vad är syftet med behandlingen?
    - Är syftet att planera verksamheten genom till exempel digitala möten?
    - Är syftet att dela information om pågående ärenden?
    - Är syftet att arbeta gemensamt med pågående ärenden?

[18] Jämförelse med artikel 25 GDPR.
[19] Artikel 9.1 GDPR.

- Ska behandlingen ske i realtid?[20]
    - Vilka uppgifter behandlas i realtid?

2.3.1.3 Risker för enskildas fri- och rättigheter

För att kunna göra en bedömning av vilka tekniska och organiska åtgärder som är *lämpliga* för personuppgiftsbiträdet att genomföra i ert fall behöver ni också överväga och dokumentera vilken risk för enskildas fri- och rättigheter (integritetsrisk) som är förknippad med behandlingen.

Det handlar till exempel om risker som är förknippade med *nivån av säkerhet* hos personuppgiftsbiträdet, det vill säga vilka åtgärder som vidtas för att förhindra oavsiktlig eller olaglig förstöring, ändring eller obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.[21] Underlag och slutsatser från bedömningen i avsnitt 1.3.2 kan med fördel beaktas här. Det kan också handla om andra risker förknippade med personuppgiftsbiträdets förmåga att leva upp till krav i GDPR eller i personuppgiftsbiträdesavtalet.

Om personuppgiftsbiträdet direkt eller indirekt lyder under tredjelands lagstiftning är det också en risk som bör övervägas inom ramen för omsorgsplikten eftersom det potentiellt kan påverka personuppgiftsbiträdets möjligheter att leva upp till kraven i GDPR och i personuppgifts-biträdesavtalet. I avsnitt 2.4 i detta appendix finns mer information om hur det kan vägas in i den bedömning som ni bör göra inom ramen för omsorgsplikten.

Dokumentera vilka risker för fysiska personers rättigheter och friheter som ni anser att behandlingen i Microsoft 365 skulle kunna leda till.

- Vilka risker anser ni finns?
- Hur stor är sannolikheten att dessa risker realiseras med er tilltänkta implementering av Microsoft 365?

2.3.2 Bedömning av lämpliga tekniska och organisatoriska åtgärder

Nästa steg i bedömningen är att ta ställning om de åtgärder som ni har tänkt vidta är *lämpliga* med hänsyn till vad som framkommit i analysen så här långt. Att åtgärderna ska vara *lämpliga* innebär att de ska vara lämpliga i förhållande behandlingens art, omfattning, sammanhang och ändamål samt riskerna för fysiska personers rättigheter och friheter.[22]

Ni behöver fundera på och dokumentera hur ni har tänkt implementera Microsoft 365, det vill säga vilken funktionalitet och vilka säkerhetsåtgärder ni har tänkt använda. I Appendix C finns en utförlig beskrivning av de säkerhetsåtgärder som erbjuds i Microsoft 365. Visualiseringen och scenario-beskrivningen i Appendix D kan också ge vägledning när det gäller vilka alternativ som finns.

Besvara följande frågor och dokumentera svaren.

- Vilka säkerhetslösningar i Microsoft 365 har ni tänkt implementera?
- Vilka tekniska och organisatoriska åtgärder har ni tänkt implementera vid sidan av Microsoft 365?
- Är åtgärderna sammantaget *lämpliga* i förhållande behandlingens art, omfattning, sammanhang och ändamål samt riskerna för fysiska personers rättigheter och friheter?

[20] Se scenariobeskrivningarna i Appendix D.
[21] Artikel 32.2 GDPR.
[22] Jämförelse med artikel 25 GDPR.

- Vilka åtgärder kan ni vidta för att minska riskerna ytterligare?

2.3.3 Bedömning av om garantierna är tillräckliga

Slutligen behöver ni ta ställning till om de garantier, om att vidta tekniska och organisatoriska åtgärder, som ges i Microsoft 365 är *tillräckliga* på ett sådant sätt att behandlingen uppfyller kraven i GDPR[23].

Exempel på åtgärder som Microsoft erbjuder är bland annat följande:

- Endast behandla personuppgifter på dokumenterade instruktioner från Kunden (personuppgiftsansvarige), inbegripet när det gäller överföringar av personuppgifter till ett tredjeland eller en internationell organisation, såvida inte denna behandling krävs enligt unionsrätten eller enligt en medlemsstats nationella rätt som Microsoft omfattas av, och i så fall ska Microsoft informera Kunden om det rättsliga kravet innan uppgifterna behandlas, såvida sådan information inte är förbjuden med hänvisning till ett viktigt allmänintresse enligt denna rätt.
- Säkerställa att personer med behörighet att behandla personuppgifterna har åtagit sig att iaktta konfidentialitet eller omfattas av en lämplig lagstadgad sekretess.
- Vidta alla åtgärder som krävs enligt artikel 32 GDPR.
- Under beaktande av behandlingens art hjälpa den personuppgiftsansvarige genom lämpliga tekniska och organisatoriska åtgärder, i den mån detta är möjligt, så att den personuppgiftsansvarige kan fullgöra sin skyldighet att svara på begäran om utövande av den registrerades rättigheter enligt kapitel III GDPR.
- Bistå den personuppgiftsansvarige med att se till att skyldigheterna enligt artiklarna 32–36 GDPR fullgörs, med beaktande av typen av behandling och den information som Microsoft har att tillgå.
- Efter den personuppgiftsansvarige val radera eller returnera alla personuppgifter till den personuppgiftsansvarige efter det att tillhandahållandet av behandlingstjänster har avslutats, och radera befintliga kopior såvida inte lagring av personuppgifterna krävs enligt unionsrätten eller medlemsstats nationella rätt.
- Ge den personuppgiftsansvarige tillgång till all information som krävs för att visa efterlevnad av de skyldigheter som fastställs i artikel 28 GDPR och för att främja och bidra till granskningar, inbegripet inspektioner, som genomförs av den personuppgiftsansvarige eller av annan granskare på uppdrag av den personuppgiftsansvarige[24].
- Microsoft erbjuder flera krypteringslösningar[25] .

[23] Artikel 28 GDPR.
[24] Microsoft senaste mall för personbiträdesavtal, se följande länk: https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=32&year=2023, 2023-12-05.
[25] De krypteringslösningar Microsoft erbjuder beskrivs i detalj i dessa separata vitböcker:
För Office 365:https://aka.ms/mscloudCMkryptering, 2023-12-13.

Mer detaljer om de tekniska och organisatoriska åtgärder som Microsoft erbjuder se avsnitt 3.6.5 i detta appendix samt Appendix C och D.

Uppförandekod

Ett personuppgiftsbiträdes anslutning till en godkänd uppförandekod får används för att visa att tillräckliga garantier tillhandahålls.[26] Tanken är att uppförandekoden ska ge dataskyddsprinciperna och andra bestämmelser i GDPR en mer praktisk innebörd och därigenom underlätta för dem som ska tillämpa reglerna. Innan en uppförandekod kan börja tillämpas behöver den godkännas av en tillsynsmyndighet. En förutsättning för att en kod ska godkännas är att tillsynsmyndigheten bedömer att den bidrar till en korrekt och effektiv tillämpning av GDPR.

Att en personuppgiftsansvarig eller ett personuppgiftsbiträde har tillämpat en godkänd uppförandekod ska dessutom beaktas vid beslut om en eventuell sanktionsavgift och storleken på sanktionsavgiften. Om tillsynsmyndigheten till exempel anser att de åtgärder som kodens övervakningsorgan vidtar mot den som brustit i efterlevnaden är tillräckligt effektiva, proportionerliga eller avskräckande kan myndigheten avstå från sanktioner.[27]

Observera att ett personuppgiftsbiträdes anslutning till en godkänd uppförandekod inte per automatik innebär att biträdet lämnar *tillräckliga garantier* enligt omsorgsplikten.

Microsoft Azure är godkänd för EU Cloud of Conduct[28], en uppförandekod för molntjänster under GDPR. Information om detta finner ni på följande länk: https://learn.microsoft.com/en-us/azure/compliance/offerings/offering-eu-cloud-coc, 2023-11-27.

* * *

Om ni bedömer att personuppgiftsbiträdet ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder är kraven i artikel 28 GDPR uppfyllda.

Anser ni att personuppgiftsbiträdet *inte* ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder enligt artikel 28 GDPR, bör ni överväga om det finns ytterligare tekniska och organisatoriska åtgärder som skulle vara lämpliga och som skulle kunna implementeras. Om så är fallet, gör om bedömningen ovan.

Ni är nu klara med alla steg i avsnitt 2 i den här modellen. Ni bör dokumentera era bedömningar och använda aktuella slutsatser som en del i den risk- och sårbarhetsanalys som genomförs med stöd av Appendix A.

Observera att ni som en del av riskbedömningen i avsnitt 2.3.1.3 ovan bör ha tagit del av informationen i avsnitt 2.4 nedan.

Om er tilltänkta implementering av Microsoft 365 kommer att innebära att personuppgifter överförs till ett land utanför EU/EES ska ni gå vidare till avsnitt 3.

[26] Artikel 28.5 GDPR.
[27] IMY: https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/uppforandekoder-och-certifieringar/ 2023-12-05 och EDPB:s riktlinjer 1/2019 om uppförandekoder och övervakningsorgan enligt förordning (EU) 2016/679, version 2.0 från den 4 juni 2019, se följande länk: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_sv.pdf , 2023-12-19.
[28] EU Cloud Code of Confuct, lista över certifierade enligt uppförandekoden finns på websidan, https://eucoc.cloud/en/public-register/list-of-adherent-services, 2023-11-27.

Om så inte är fallet, men ni har bestämmelser om sekretess i OSL som gäller för uppgifter i verksamheten, ska ni gå till avsnitt 4 i denna modell.

I annat fall är ni klara med alla steg i denna modell.

2.4 Mer om risken för att enskildas fri- och rättigheter kränks på grund av tredjelands lagstiftning

2.4.1 När uppstår en sådan risk?

Överföring av personuppgifter till en mottagare i tredjeland får enligt GDPR endast ske under vissa särskilda förutsättningar (se avsnitt 2.4.3 för en närmare förklaring av vad en överföring till tredjeland är samt avsnitt 3 för en närmare beskrivning av reglerna för det). Anledningen till att det finns en sådan begränsning i GDPR är att det vid en överföring av personuppgifter till en organisation utanför EU/EES finns en risk att de fri- och rättigheter som enskilda åtnjuter inom EU/EES åsidosätts om motsvarande fri- och rättigheter saknas i det mottagande landet. Enkelt utryckt kan det innebära att enskilda utsätts för *risken* att deras fri- och rättigheter kränks på ett sätt som inte hade varit tillåtet inom EU/EES. En överföring av personuppgifter till tredjeland får därför inte ske om nivån av skydd för uppgifterna i tredjelandet inte motsvarar den som finns inom EU/EES.

En tredjelandsöverföring sker först i samband med att uppgifterna faktiskt överförs till myndigheter eller annan mottagare i tredjeland.[29] Med det sagt är det inte bara när personuppgifter överförs till ett tredjeland som en sådan *risk* kan uppstå. I flera länder förekommer lagstiftning som innehåller skyldigheter för organisationer som lyder under landets lagstiftning att tillgängliggöra personuppgifter för myndigheter för exempelvis brottsbekämpande syften, oavsett var dessa uppgifter befinner sig geografiskt.

Det innebär att personuppgiftsbiträden som direkt eller indirekt, till exempel på grund av sin koncernstruktur, lyder under sådan tredjelandslagstiftning potentiellt skulle kunna hamna i en situation då det tvingas välja mellan att bryta mot bestämmelserna i GDPR och i avtalet med den personuppgiftsansvarige eller att bryta mot lagstiftningen i tredjeland.[30]

När Microsoft 365 används kan tredjelands lagstiftning bli gällande beroende på vilka tjänster som används och vilken organisation som använder dem. För det första kan tredjelands lagstiftning bli tillämplig på grund av att *er organisation träffas av den*. I det fallet är det inte avgörande om och hur Microsoft 365 används, utan det beror på helt andra faktorer. Den frågan kommer inte att behandlas vidare här men den kan vara relevant i er risk- och sårbarhetsanalys.

För den andra kan *de tjänster och funktioner ni väljer att använda* i Microsoft 365 ha en påverkan på hur och var personuppgifterna behandlas av Microsoft, vilket innebär att personuppgifter kan komma att omfattas av tredjelands lagstiftning med anledning av att de överförs dit (se avsnitt 2.4.3 för mer information om vad en tredjelandsöverföring är).

[29] EDPB, Riktlinjer 05/2021 om samspelet mellan tillämpningen av artikel 3 och bestämmelserna om internationella överföringar enligt kapitel V i dataskyddsförordningen, version 2.0, s. 14.
[30] Säker och kostnadseffektiv IT-drift – rättsliga förutsättningar för utkontraktering, även kallad it-driftsutredningen (SOU 2021:1), s. 203.

För det tredje omfattas Microsoft som koncern av lagstiftning i USA; bland annat sådan lagstiftning som innebär att det finns skyldighet att på begäran lämna ut uppgifter till brottsbekämpande myndigheter och underrättelsemyndigheter. En översikt över sådan lagstiftning finns i Bilaga 2.

Omsorgsplikten innebär som ovan nämnts att den personuppgiftsansvarige vid valet av ett personuppgiftsbiträde behöver utreda vilka förutsättningar biträdet har att efterleva sina skyldigheter enligt GDPR och personuppgiftsbiträdesavtalet, bland annat i ljuset av lagstiftning i tredjeland.

Om er planerade behandling i Microsoft 365 *uteslutande* kommer att ske inom EU och inte kommer att innebära en överföring av personuppgifter till tredjeland, gör ni denna bedömning som en integrerad del i bedömningen av omsorgsplikten, i det steg som beskrivs i avsnitt 2.3.1.3. I följande avsnitt finns information som kan vara en del av underlaget för den bedömningen.

Om den behandlingen i Microsoft 365 ni planerar *kommer att innebära en överföring av personuppgifter till tredjeland* bör ni även följa stegen i avsnitt 3 i detta appendix.

2.4.2 Hur kan den risken bedömas?

Som ovan nämnts bör ni inom ramen för omsorgsplikten bedöma vilka förutsättningar biträdet har att efterleva sina skyldigheter enligt GDPR och personuppgiftsbiträdesavtalet, bland annat i ljuset av lagstiftning i tredjeland. Det är många faktorer som skulle kunna påverka detta, bland annat sannolikheten att det Microsoftbolag som ni har avtal med skulle tvingas föra över personuppgifter till tredjeland på grund av en förfrågan från en myndighet, hur Microsoft i så fall åtar sig att agera samt hur det skulle kunna påverka enskildas fri- och rättigheter om en överföring skulle ske.

När det gäller bedömningen av *sannolikheten* för att det Microsoftbolag ni har avtal med för över uppgifter till ett tredjeland på grund av en tvingande förfrågan från en myndighet finns det statistik från Microsoft och andra källor som beskriver hur ofta sådana förfrågningar förekommer. Statistiken från Microsoft visar att Microsoft får förfrågningar från myndigheter i USA (och andra länder), men att det handlar om ett mindre antal jämfört med antalet kunder som använder Microsofts tjänster. Mer information om den här statistiken finns i Bilaga 2.

Ett exempel från Microsoft[31]

Jag håller på att göra en risk och sårbarhetsanalys – kan jag beräkna sannolikheten att data lämnas ut till amerikanska rättssystemet i en brottsutredning?

Under andra halvåret 2022 lämnade Microsoft ut personuppgifter rörande icke-amerikanska företagskunder (globalt) till amerikanska myndigheter i fyra fall. Denna siffra kan ställas i relation till att Microsoft 365 har närmare 350 miljoner användare globalt.[32]

Microsoft kan tillhandahålla mer information till sina kunder gällande den praktiska tillämpningen av amerikansk lagstiftning. Den finns att tillgå i följande länk:

https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWXwSh?culture=en-us&country=us (2024-01-09).

När det frågan om hur Microsoft *åtar sig att agera* om en sådan förfrågan skulle komma, finns det information om det i det personuppgiftsbiträdesavtal som Microsoft ingår med samtliga kunder. I

[31]Microsoft, https://news.microsoft.com/sv-se/2021/02/11/microsofts-molntjanster-och-sakerhet/, 2023-12-05.
[32] Microsoft, https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report, 2024-01-12.

personuppgiftsbiträdesavtalet anger Microsoft att de bland annat åtar sig att bestrida samtliga sådana förfrågningar de får samt att Microsoft, i de fall de inte når framgång med sitt bestridande och behöver lämna ut personuppgifter, begränsar utlämnandet av personuppgifter till endast det som måste lämnas ut enligt lag. Detta innebär att Microsoft vidtar åtgärder för att minska mängden personuppgifter som delas med utländska myndigheter.

I det biträdesavtal som Microsoft tillhandahåller åtar de sig att vidta följande åtgärder för att bestrida en order.

Bestridande av order

I händelse av att Microsoft får en order från tredje man om tvingat utlämnande av personuppgifter som behandlas enligt detta DPA ska Microsoft:

a. göra alla rimliga ansträngningar för att hänvisa tredje man direkt till Kunden med sin begäran om data.
b. omgående meddela Kunden, såvida det inte är förbjudet enligt lag som är tillämplig på begärande tredje man, och, om det är förbjudet att meddela Kunden, använda alla lagliga medel för att erhålla rätten att undanröja förbudet för att kunna lämna så mycket information som möjligt till Kunden så snart som möjligt
c. använda alla lagliga medel för att bestrida ordern om utlämnande baserat på rättsliga brister enligt den begärande partens lagar eller eventuella relevanta lagkonflikter med tillämplig lag i EU eller tillämplig medlemsstat.

Om efter att ha vidtagit stegen a. till c. ovan, Microsoft eller något av deras koncernbolag fortfarande tvingas lämna ut personuppgifter ska Microsoft endast lämna ut den minsta mängd av dessa data som är nödvändig för att uppfylla ordern om tvingat utlämnande.[33]

När det gäller vilken *risk för enskildas fri- och rättigheter* de utlämnanden som kan ske innebär bör ni beakta vilken nivå av skydd för enskildas fri- och rättigheter som erbjuds i USA. I den bedömningen kan EU-kommissionens beslut om adekvat skyddsnivå för amerikanska organisationer som omfattas av Data Privacy Framework (”DPF”)[34] vägas in, även om beslutet i sig rör möjligheten att föra över personuppgifter till USA med stöd av artikel 45 GDPR. Innan EU-kommissionen kan meddela ett adekvansbeslut är den nämligen skyldig att göra en grundlig utredning av om det land, de sektorer eller de organisationer som beslutet avser tillgodoser enskildas fri- och rättigheter inom dataskyddens område.[35] Det sker i syfte att bedöma om personuppgifter har ett motsvarande skydd hos mottagaren som de skulle ha inom EU/EES. Denna utredning redovisas som en del av skälen i ett adekvansbeslut.

EU-kommissionen har gjort bedömningen att det skydd för enskildas fri-och rättigheter som DPF ger är *väsentligen likvärdigt* med den skyddsnivå som garanteras inom EU/EES enligt GDPR, jämfört med EU:s stadga om de grundläggande rättigheterna.[36] Med andra ord menar EU-kommissionen att enskilda inte utsätts för en högre risk för kränkning av sina fri- och rättigheter när

[33] Microsoft, https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=32&year=2023, 2023-11-27.
[34] EDPB, Information note on data transfers under the GDPR to the United States after the adoption of the adequacy decision on 10 July 2023.
[35] Artikel 45.2 GDPR.
[36] EU-komissionen, Comission implementing decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework.

personuppgifter förs över till DPF-anslutna organisationer i USA än när personuppgifter behandlas inom EU/EES. I bedömningen har EU-kommissionen dels vägt in de åtaganden som DPF innebär för de organisationer som väljer att ansluta sig till den, dels de möjligheter myndigheter i USA har att begära eller bereda sig tillgång till personuppgifter som till exempel finns hos amerikanska molntjänstleverantörer.

Det bör noteras att även andra tredjeländer har lagstiftning liknande den amerikanska där personuppgifter kan samlas in av myndigheter för brottsbekämpande syften eller underrättelsesyften. Sådan lagstiftning finns även inom EU/EES.

2.4.3 Vad är en tredjelandsöverföring?

GDPR innehåller ingen definition av begreppet överföring till tredjeland. Med det sagt har EDPB tagit fram en vägledning i denna fråga. EDBP ställer upp tre kriterier som måste vara uppfyllda för att en behandling ska kvalificeras som en tredjelandsöverföring.[37]

- En personuppgiftsansvarig eller ett personuppgiftsbiträde (uppgiftsutförare) omfattas av GDPR för behandlingen i fråga.
- Uppgiftsutföraren lämnar ut personuppgifter som omfattas av behandlingen genom översändande eller på annat sätt gör dem tillgängliga för en annan personuppgiftsansvarig, en gemensamt personuppgiftsansvarig eller ett personuppgiftsbiträde (uppgiftsinförare).
- Uppgiftsinföraren är i tredjeland, oavsett om uppgiftsinföraren omfattas av GDPR för behandlingen i fråga i enlighet med artikel 3 GDPR, eller är en internationell organisation.

Den första punkten tar sikte på att personuppgiftsansvarig och/eller personuppgiftsbiträdet omfattas av GDPR för behandlingen i fråga. EDPB har även tagit fram riktlinjer för att avgöra om tillämpligheten av GDPR, som kan vara ett stöd i den bedömningen.[38]

Den andra och tredje punkten anger att personuppgifterna måste *överföras* eller på *annat sätt göras tillgängliga* av en personuppgiftsansvarig eller ett personuppgiftsbiträde för en personuppgiftsansvarig eller personuppgiftsbiträde som geografiskt befinner sig i ett tredjeland eller internationell organisation. Det innebär att överföringen eller tillgängliggörandet av personuppgifter måste ske mellan två olika organisationer. Exempelvis innebär inte en privatpersons överföring av personuppgifter till en organisation i ett tredjeland en tredjelandsöverföring i GDPR:s mening. Notera att den sista punkten gäller avsett om uppgiftsinföraren omfattas av GDPR eller inte.[39]

[37] EDPB, Riktlinjer 05/2021 om samspelet mellan tillämpningen av artikel 3 och bestämmelserna om internationella överföringar enligt kapitel V i dataskyddsförordningen, version 2.0, s. 7.
[38] EDPB, Riktlinjer 3/2018 om den allmänna dataskyddsförordningens territoriella tillämpningsområde (artikel 3), version 2.1, s. 5 ff.
[39] EDPB, Riktlinjer 05/2021 om samspelet mellan tillämpningen av artikel 3 och bestämmelserna om internationella överföringar enligt kapitel V i dataskyddsförordningen, version 2.0, s. 7–8.

Exempel på överföring av personuppgifter till tredjeland:

- När ni anlitar ett personuppgiftbiträde i ett land utanför EU/EES.
- När ni ger någon utanför EU/EES tillgång, exempelvis läsbehörighet, till personuppgifter som finns lagrade inom EU/EES.
- När ni lagrar personuppgifter i en molntjänst som är baserad utanför EU/EES.
- När ni lagrar personuppgifter, till exempel på en server, i ett land utanför EU/EES
- När ni skickar dokument som innehåller personuppgifter per e-post till någon i ett land utanför EU/EES.[40]

EDPB har vidare bedömt att det *inte* är fråga om en tredjelandsöverföring när personuppgifter behandlas uteslutande inom EU, även om den personuppgiftsansvarige eller personuppgifts-biträdet som behandlar personuppgifterna är bunden av tredjelandslagstiftning som innebär att denne kan åläggas att lämna ut uppgifter direkt till ett tredjelands myndigheter. Tredjelands-överföringen sker först i samband med att uppgifterna överförs till myndigheter eller annan mottagare i tredjeland.[41]

Om Microsoft 365 och lagring i EU

Microsoft lanserade den 1 januari 2023 EU Data Boundary för kunder i EU- och EFTA-länderna[42]. Det nya initiativet gör det möjligt för kunder att både behandla och lagra alla personuppgifter[43] EU, Norge eller Schweiz. Detta åtagande gäller för Microsofts huvudsakliga molntjänster Azure, Microsoft 365, Dynamics 365 och Power Platform.[44]

[40] Integritetsskyddsmyndigheten, https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/overforing-till-tredje-land/, 2023-12-13.
[41] EDPB, Riktlinjer 05/2021 om samspelet mellan tillämpningen av artikel 3 och bestämmelserna om internationella överföringar enligt kapitel V i dataskyddsförordningen, version 2.0, s. 14.
[42] EFTA-länderna inbegriper, förutom EES-länderna, även Schweiz.

[43] Microsoft, https://blogs.microsoft.com/eupolicy/2024/01/11/microsoft-cloud-european-data-boundary, 2024-01-16.
[44] Microsoft, https://techcommunity.microsoft.com/t5/partner-updates-denmark-iceland/update-eu-data-boundary-for-the-microsot-cloud/ba-p/3808127, 2023-11-24.

3 Tredjelandsöverföringar

3.1 Vad behandlas i detta avsnitt?

Det här avsnittet av den analytiska modellen hjälper verksamheten att ta ställning till om de *överföringar av personuppgifter till ett tredjeland* som kan bli aktuella med den tilltänkta implementeringen av Microsoft 365 är förenliga med GDPR.

Avsnittet inleds med en beskrivning av vad en överföring till tredjeland är (avsnitt 3.2). Därefter följer de olika frågor som verksamheten behöver ta ställning till om personuppgifter överförs till tredjeland (avsnitt 3.3–3.6). Systematiken i avsnittet följer EDPB:s rekommendation[45] på området. I varje del finns en beskrivning av den juridiska kontexten och information om omständigheter, inklusive om funktionalitet och valmöjligheter i Microsoft 365, som kan vara relevanta för bedömningen.

3.2 Vad är en tredjelandsöverföring?

De nedanstående avsnitten blir endast aktuella om den implementation av Microsoft 365 som ni har tänkt er *innebär att personuppgifter kan överföras till tredjeland*. GDPR innehåller ingen definition av begreppet överföring till tredjeland. I avsnitt 2.4.3 finns en mer ingående beskrivning av de tolkningar av begreppet som förekommer vad en *överföring till tredjeland*. Som framgår däri är EDPB av den åsikten att det inte är fråga om en tredjelandsöverföring när personuppgifter behandlas uteslutande inom EU, även om den personuppgiftsansvariga eller personuppgifts-biträdet som behandlar personuppgifterna är bunden av tredjelands lagstiftning som innebär att denna kan åläggas att lämna ut uppgifter direkt till ett tredjelands myndigheter.[46]

Exempel på överföring av personuppgifter till tredjeland:

- När ni skickar dokument som innehåller personuppgifter per e-post till någon i ett land utanför EU/EES.
- När ni anlitar ett personuppgiftbiträde i ett land utanför EU/EES.
- När ni ger någon utanför EU/EES tillgång, exempelvis läsbehörighet, till personuppgifter som finns lagrade inom EU/EES.
- När ni lagrar personuppgifter i en molntjänst som är baserad utanför EU/EES.
- När ni lagrar personuppgifter, till exempel på en server, i ett land utanför EU/EES.

3.3 Till vilket land överförs personuppgifter?

Första steget i modellen är att kartlägga till vilket eller vilka länder överföringen sker till. I Appendix C och D finns en beskrivning av olika funktionaliteter i Microsoft 365 och även information om behandlingar som kan medföra tredjelandsöverföringar. Observera att informationen i Appendix C och D inte är en uttömmande beskrivning av Microsoft 365, utan utgör ett hjälpmedel för bedömningen.

[45] Rekommendation från EDPB om kompletterande säkerhetsåtgärder vid överföring av personuppgifter till länder utanför EU/EES.
[46] EDPB, Riktlinjer 05/2021 om samspelet mellan tillämpningen av artikel 3 och bestämmelserna om internationella överföringar enligt kapitel V i dataskyddsförordningen, version 2.0, s.14.

Ni behöver utreda frågan utförligt och dokumentera era slutsatser.

Om Microsoft EU Data Boundary

Microsoft erbjuder sina kunder inom EU och EFTA möjlighet att begränsa delningen av personuppgifter utanför EU och EFTA genom att lagra och behandla ”Kunddata”[47] och personuppgifter[48] i datacenter inom EU och EFTA. Erbjudandet gäller tjänsterna Microsoft 365, Azure, Dynamics 365 och Power Platform. På Microsofts webbsida finns det information om i vilka länder informationen lagras samt att det i vissa fall även går att välja ett specifikt datacenter.[49]

Om ni väljer att utnyttja Microsofts erbjudande EU Data Boundary bör ni vara uppmärksamma på att EU Data Boundary fortfarande utvecklas och att förändringar kan komma att ske. Det innebär att det kan förekomma att personuppgifter ändå överförs till tredjeland om vissa funktioner eller inställningar används. För att försäkra er om att personuppgifter inte överförs utanför EU/EES är det viktigt att läsa ”Product Terms” för varje tjänst. Vidare skriver Microsoft översiktligt på sin webbsida om vilka tjänster som kommer att omfattas och inte.[50]

3.4 Finns det ett adekvansbeslut enligt artikel 45?

EU-kommissionen har fattat beslut om att skyddsnivån i vissa länder är adekvat, det vill säga tillräckligt hög för att personuppgifter ska få föras över dit med stöd av artikel 45 GDPR.

En uppräkning av de länder som har en adekvat skyddsnivå finns på följande länk:

https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en, 2023-11-24.

Storbritannien och Sydkorea utgör exempel på tredjeländer som EU-kommissionen beslutat om adekvat skyddsnivå för.[51] EU-kommissionen har den 10 juli 2023 även fattat beslut om adekvat skyddsnivå för organisationer i USA som har anslutit sig till DPF.[52] Det innebär att personuppgifter kan överföras till organisationer som genom sin DPF-certifiering omfattas av beslutet, utan att ytterligare skyddsåtgärder enligt kap 5 GDPR behöver vidtas.

Microsoft omfattas av DPF[53] vilket innebär att en överföring av personuppgifter till de Microsoft-bolag som är certifierade i USA kan ske med stöd av artikel 45.1 GDPR.

[47] Se definition i avsnitt 3.1.2 i Vägledningen eller i bilaga 5 i begrepp och förkortningslista.
[48] Microsoft, https://blogs.microsoft.com/eupolicy/2024/01/11/microsoft-cloud-european-data-boundary/, 2024-01-12.
[49] Microsoft, https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-learn, 2023-11-24.
[50] Microsoft, https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-learn, 2023-11-24.
[51] På EU-kommissionens hemsida anges vilka länder som omfattas av beslut om adekvat skyddsnivå, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en, 2023-11-27.
[52] EU-kommissionen, Commission implementing decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023D1795, 2023-11-24.
[53] https://www.dataprivacyframework.gov/s/participant-search/participant-detail?id=a2zt0000000KzNaAAK&status=Active, 2023-12-06.

Ett beslut om adekvat skyddsnivå är bindande för samtliga medlemsländer och deras tillsynsmyndigheter och innebär att en överföring av personuppgifter kan ske utan att godkännande inhämtas eller att kompletterande skyddsåtgärder implementeras.[54]

* * *

Om EU -kommissionen har fattat beslut om att det land, den region eller sektor som ni överför uppgifterna till har en adekvat skyddsnivå[55] är överföringen förenlig med GDPR. I de fall en tredjelandsöverföring aktualiseras vid användandet av Microsoft 365 är mottagarlandet oftast USA, vilket innebär att överföringen kan grunda sig på artikel 45.1 GDPR och beslutet om adekvat skyddsnivå för DPF. Med det sagt bör ni bevaka att beslutet om adekvansskyddsnivå förblir giltigt.

Ni är då klara med alla steg i avsnitt 3 i den här modellen. Ni bör dokumentera era bedömningar och använda aktuella slutsatser som en del i den risk- och sårbarhetsanalys som genomförs med stöd av Appendix A.

Om ni har bestämmelser om sekretess i OSL som gäller för uppgifter i verksamheten, ska ni gå till avsnitt 4 i denna modell. I annat fall är ni klara med alla steg i denna modell.

Om överföringen sker till ett land som inte omfattas av DPF eller annat ett adekvansbeslut ska ni fortsätta till nästa avsnitt.

3.5 Är det en undantagssituation då uppgifter får överföras till ett land utanför EU/EES enligt artikel 49?

I undantagsfall kan det vara tillåtet att föra över personuppgifter till ett land utanför EU/EES även om landet saknar en adekvat skyddsnivå (se avsnitt 3.4) och trots att lämpliga skyddsåtgärder inte har vidtagits (se avsnitt 3.6 nedan).

Personuppgifter får till exempel överföras till ett land utanför EU/EES om den registrerade uttryckligen har samtyckt till det, efter att ha fått information om riskerna med den överföring som sker även om det saknas beslut om adekvat skyddsnivå eller lämpliga skyddsåtgärder.

Europeiska dataskyddsstyrelsen har tagit fram närmare riktlinjer om vad som gäller enligt artikel 49, se följande länk:
https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_sv.pdf

* * *

Om överföringen av personuppgifter till tredjeland är en sådan undantagssituation som beskrivs i artikel 49 GDPR och ni uppfyller kraven däri, är överföringen förenlig med GDPR. Observera att ni i vissa fall ska informera både IMY och de registrerade om överföringen och era bedömningar.

---

[54] EU-kommissionen, Commission implementing decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023D1795, s 60, 2023-11-24.

[55] Artikel 45 GDPR.

Ni är då klara med alla steg i avsnitt 3 i den här modellen. Ni bör dokumentera era bedömningar och använda aktuella slutsatser som en del i den risk- och sårbarhetsanalys som genomförs med stöd av Appendix A.

Om ni har bestämmelser om sekretess i OSL som gäller för uppgifter i verksamheten, ska ni gå till avsnitt 4 i denna modell. I annat fall är ni klara med alla steg i denna modell.

Om överföringen *inte* är en sådan undantagssituation som beskrivs i artikel 49 GDPR eller ni inte uppfyller kraven däri, ska ni fortsätta till nästa steg i modellen.

3.6 Kan ni vidta *lämpliga skyddsåtgärder* enligt artikel. 46?

3.6.1 Vilka lämpliga skyddsåtgärder finns enligt artikel 46?

Personuppgifter får överföras till ett land utanför EU/EES om ni vidtar så kallade lämpliga skyddsåtgärder så som:

- bindande företagsbestämmelser,
- standardavtalsklausuler som EU-kommissionen har beslutat om (Standard Contractual Clauses, SCC),
- godkända uppförandekoder eller certifieringsmekanismer,
- rättsligt bindande instrument mellan myndigheter.[56]

3.6.2 Standardavtalsklausuler

Den 4 juni 2021 antog EU-kommissionen två nya uppsättningar standardavtalsklausuler. Den ena uppsättningen används vid överföring av personuppgifter mellan EU/EES och ett tredje land. Den andra uppsättningen används mellan en personuppgiftsansvarig och ett personuppgiftsbiträde och är därmed avsedd att kunna användas som ett personuppgiftsbiträdesavtal.

EU kommissionens senaste standardavtalsklausuler finns här: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en, 2023-11-24.

Observera att standardavtalsklausulerna inte får ändras. Om det är nödvändigt kan ni lägga till klausuler om affärsrelaterade frågor, men sådana får då inte strida mot någon standardavtalsklausul.

Enligt standardavtalsklausulerna ska dataexportören, om denne har anledning att tro att dataimportören inte längre kan fullgöra sina skyldigheter enligt dessa klausuler, omedelbart identifiera lämpliga åtgärder (till exempel tekniska eller organisatoriska åtgärder för att säkerställa säkerhet och konfidentialitet). Dataexportören ska avbryta dataöverföringen om denne anser att det inte kan säkerställas att det finns några lämpliga skyddsåtgärder för sådan överföring.[57]

[56] Artikel 46 GDPR.
[57] EU- komissionen, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en, 2023-12-18.

Microsoft och standardavtalsklausulerna

Microsoft implementerade de nya standardavtalsklausulerna den 15 september 2021.[58] I personuppgiftsbiträdesavtalet som Microsoft erbjuder anges att all överföring av kunddata, data i professionella tjänster och personuppgifter ut ur Europeiska unionen, Europeiska Ekonomiska Samarbetsområdet, Storbritannien och Schweiz som görs för att tillhandahålla produkterna och tjänsterna regleras av 2021 års standardavtalsklausuler implementerade av Microsoft. Dessutom ska överföringar från Storbritannien och Schweiz regleras av 2010 års standardavtalsklausuler[59].

Microsoft använder sig av Processor-to-Processor-klausulerna (eller P2P SCC). P2P SCC ingås mellan Microsoft Ireland Operations Limited (MIOL) (personuppgiftsbiträdet inom EU/dataexportör) och Microsoft Corporation, (personuppgiftsbiträdet utanför EU/dataimportör). P2P SCC publicerades i Service Trust Portal. Genom Microsoft-bolag signerar P2P SCC som både dataimportör och -exportör, har Microsoft ett stort ansvar för att dataöverföringarna sker i enlighet med villkoren och GDPR.[60]

3.6.3 Finns det lagstiftning i det landet överföringen sker till som påverkar skyddet?

Nästa steg är att bedöma om det finns bestämmelser i tredjelandets lagstiftning och/eller praxis som kan påverka effektiviteten av de överföringsverktyg ni använder er av.[61]

Bedömningen bör fokuseras först och främst på lagstiftning som är relevant för den kontext överföringen görs i samt artikel 46 GDPR. Som underlag för bedömningen kan ni även inhämta information om lagstiftning och praxis i det tredjelandet från ett flertal källor, exempelvis

- rättspraxis från Europeiska unionens domstol (EU-domstolen) och Europeiska domstolen för de mänskliga rättigheterna (Europadomstolen/ECHR),
- kommissionens underlag för adekvansbeslut för destinationslandet även om den aktuella överföringen inte omfattas av det aktuella beslutet,[62]
- resolutioner och rapporter från mellanstatliga organisationer, andra regionala organ och FN: s organ,
- nationell rättspraxis eller beslut som fattas av oberoende rättsliga eller administrativa myndigheter behöriga inom dataskydd och dataskydd i tredjeländer, och
- rapporter och analyser från behöriga regleringsnätverk, till exempel Global Privacy Assembly (GPA).

Fler exempel på källor som kan användas för att utreda tredjelands lagstiftning och/eller praxis återfinns i Bilaga 3 i EDPB:s rekommendationer, se följande länk:

[58] Microsoft, https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=1&year=2023 2023-11-24.
[59] Microsoft, https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=32&year=2023 2023-11-24.
[60] Microsoft, https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=1&year=2023 2023-11-24.
[61] European Data Protection Board (EDPB), Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU lever of protection of personal data, version 2.0, slutligt antagna efter publik konsultation.
[62] EDPB Information note on data transfers under the GDPR to the United States after the adoption of the adequacy decision on 10 July 2023, https://edpb.europa.eu/our-work-tools/our-documents/other-guidance/information-note-data-transfers-under-gdpr-united-0_en, s.2, 2023-12-18.

https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf

Ni bör göra en bedömning om lagstiftningen i tredjeland ger en väsentligen likvärdig nivå av skydd i som inom EU/EES. Ni kan till exempel beakta följande.

- Personuppgifter bör endast få behandlas utifrån tydliga, precisa och tillgängliga bestämmelser.
- Nödvändighet och proportionalitet ska säkerställas för legitima mål.
- En oberoende tillsynsmekanism bör finnas.
- Enskilda personer ska ha tillgång till effektiva rättsmedel.[63]

Innan EU-kommissionen kan meddela ett adekvansbeslut är den skyldig att göra en grundlig utredning av om det land, de sektorer eller de organisationer som beslutet avser tillgodoser fri- och rättigheter inom dataskyddens område.[64] Det sker i syfte att bedöma om personuppgifter har ett motsvarande skydd hos mottagaren som de skulle ha inom EU/EES och denna utredning redovisas som en del av skälen i adekvansbeslutet. EU-kommissionens utredning kan vara ett underlag i bedömningen av rättsläget i det aktuella tredjelandet även om beslutet i sig inte gäller för den aktuella överföringen. Det innebär exempelvis att skälen för adekvansbeslutet för DPF utgöra underlag för bedömningen av skyddet för personuppgifter i USA även vid en överföring av personuppgifter till en mottagare i USA som inte omfattas av DPF.

3.6.4 Är den aktuella lagstiftningen tillämplig på era behandlingar?

Om ni har konstaterat att det finns bestämmelser i tredjelandets lagstiftning som kan påverka effektiviteten av de överföringsverktyg ni använder er av, är nästa steg att ta reda på om den lagstiftningen är tillämplig på era överföringar av personuppgifter och vilken risk det *i praktiken* innebär för enskildas fri- och rättigheter. Om ni har anledning att tro att den aktuella lagstiftningen *i* praktiken inte kommer att tillämpas på de personuppgifter ni tänkt överföra behöver sådan lagstiftning nämligen inte vara ett hinder.

Ni bör undersöka egenskaperna för var och en av era överföringar och avgöra om nationell lagstiftning och/eller praxis som gäller i det land till vilket överföringen sker påverkar dessa överföringar.[65]

Vilka lagar och metoder som gäller kan bero på

- ändamålen med behandlingen och överföringen (till exempel syften relaterade till marknadsföring, HR, lagring, tekniskt stöd, kliniska studier)
- typ av aktörer som är involverade i behandlingen (offentliga eller privata aktörer)
- sektor där överföringen sker (till exempel adtech, telekommunikation, ekonomi, hälsa, journalistik och så vidare.)

[63] EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0 Adopted on 18 June 2021 https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf, 2023-11-28.
[64] Artikel 45.2 GDPR.
[65] EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0 Adopted on 18 June 2021 https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf, 2023-11-28.

- kategorier av personuppgifter (till exempel kan tredje land ha särskilda lagar som rör minderåriga)
- om uppgifterna kommer att lagras i tredjelandet eller om det finns fjärråtkomst till data lagras inom EU/EES
- format för personuppgifter som ska överföras (dvs. i ren text/ pseudonymiserad eller krypterad).[66]

Exempel: I vissa länder finns det begränsningar för myndigheternas rätt att kräva information från media, advokater eller vårdpersonal. Med andra ord kan syftet, typen av aktörer, sektorn, samt kategorierna av personuppgifter vara avgörande för om tredjelands lagstiftning tillämpas på den aktuella överföringen.

EU-standarder, såsom artiklarna 47 och 52 i EU:s stadga om de grundläggande rättigheterna, bör kunna användas som referens, särskilt för att bedöma om offentliga myndigheter i tredjelands möjligheter att begära eller bereda sig tillgång till uppgifter är begränsad till vad som är nödvändigt och proportionerligt i ett demokratiskt samhälle.

Lagar och praxis som ger offentliga myndigheter sådana möjligheter kan innebära ett intrång i integriteten, oavsett om uppgifterna är känsliga eller om personerna i fråga faktiskt har påverkats negativt av intrånget. Med det sagt är det inte alla intrång som utgör en kränkning. Det är först när lagar och praxis går utöver vad som är nödvändigt och proportionellt som de utgör en kränkning.[67]

Det kan finnas situationer där lagstiftningen i tredjelandet är problematisk, men där det inte finns någon anledning att tro att den problematiska lagstiftningen kommer att tillämpas på överföringen i praktiken. I så fall behöver ni inte vidta några ytterligare åtgärder. Ni bör dokumentera skälen för bedömningen att lagen inte tolkas eller tillämpas i praktiken så att den täcker överföringen, även med hänsyn till erfarenheter från liknande aktörer inom samma bransch och/eller relaterade till liknande överföringar, som samt annan relevant information.

Exempel: Ett inslag i bedömningen om ett ingrepp är proportionellt kan vara om personuppgifterna i fråga redan är offentligt tillgängliga. Myndigheternas insamling av offentligt tillgängliga personuppgifter kan lättare utgöra ett proportionellt ingripande än insamling av information som inte är tillgänglig för allmänheten. Det måste betraktas konkret från fall till fall.

[66] EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0 Adopted on 18 June 2021 https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf, 2023-11-28.
[67] Datatillsynet, https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/overforing-av-personopplysninger-ut-av-eos/ , 2023-12-15.

Att kringgå reglerna genom att publicera personuppgifter i det enda syftet att överföra dem till ett tredjeland kan i alla fall vara i strid mot både artikel 6 och kapitel V GDPR[68].

Microsofts uppgifter om den praktiska tillämpningen av amerikansk lagstiftning

Microsoft kan tillhandahålla mer information till sina kunder gällande den praktiska tillämpningen av amerikansk lagstiftning. Den finns att tillgå i följande länk:

https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWXwSh?culture=en-us&country=us (2024-01-09).

* * *

Om ni efter bedömningen ovan anser att det inte finns någon anledning att tro att relevant och problematisk lagstiftning kommer att tillämpas i praktiken för de personuppgifter ni kommer att föra över till tredjeland – och därför inte heller påverkar det skydd som SCC:erna är tänkta att ge – behöver ni inte införa ytterligare kompletterande skyddsåtgärder. Ni är då klara med alla steg i avsnitt 3 i den här modellen. Ni bör dokumentera era bedömningar och använda aktuella slutsatser som en del i den risk- och sårbarhetsanalys som genomförs med stöd av Appendix A.

Om ni har bestämmelser om sekretess i OSL som gäller för uppgifter i verksamheten, ska ni gå till avsnitt 4 i denna modell. I annat fall är ni klara med alla steg i denna modell.

Om ni har anledning att tro att relevant och problematisk lagstiftning kommer att tillämpas i praktiken för de personuppgifter ni kommer att föra över till tredjeland, ska ni fortsätta till nästa steg i modellen.

3.6.5 Kompletterande åtgärder

I de fall mottagarlandet inte uppnår en i allt väsentligt likvärdig skyddsnivå för uppgifterna som inom EU eller EES, kan de lämpliga skyddsåtgärderna, såsom EU-kommissionens standardavtalsklausuler, behöva kompletteras med ytterligare skyddsåtgärder.

Detta steg är bara nödvändigt om er bedömning visar att tredjelands lagstiftning och/eller praxis påverkar effektiviteten av överföringsverktyget som ni använder er av vid överföringen. Kompletterande åtgärder kan vara effektiva i vissa länder, men inte nödvändigtvis i andra. Det är en helhetsbedömning som behöver göras i varje enskilt fall.

[68] Datatillsynet, https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/overforing-av-personopplysninger-ut-av-eos/ , 2023-11-28.

Myndigheter i tredjeländer kan ha möjlighet att få tillgång till överförda personuppgifter på följande sätt:

a) **Under transport** genom åtkomst till de kommunikationslinjer som används för att överföra personuppgifter till mottagaren. Denna åtkomst kan vara passiv i vilket fall innehållet i kommunikationen, möjligen efter en urvalsprocess, kopieras. Åtkomsten kan också vara aktiv i den meningen att innehållet i kommunikationen ändras eller raderas.

b) **I förvar hos en avsedd mottagare av uppgifterna** genom åtkomst till de anläggningar där uppgifter behandlas, eller genom att begära att en mottagare av uppgifterna lokaliserar och extraherar data av intresse och överlämnar det till myndigheterna.[69]

Microsofts uppgifter i frågan:

Enligt Microsofts uppgifter ger Microsoft ingen myndighet direkt eller obehindrad åtkomst till kunddata (inklusive personuppgifter) och lämnar endast ut uppgifter om det krävs enligt lag. Observera att Microsoft tillhandahåller information om de förfrågningar som de har fått från den amerikanska regeringen i enlighet med nationella säkerhetslagar i sin rapport om nationella säkerhetsorder i USA, som finns vid denna länk: https://www.microsoft.com/en-us/corporate-responsibility/us-national-security-orders-report?activetab=pivot_1:primaryr2, 2023-11-28.

I listan nedan ges exempel på vissa effektiva skyddsåtgärder.[70] Ni kan utforska andra kompletterande åtgärder. Framtidens tekniska, juridiska eller organisatoriska utveckling kan leda till uppkomsten av nya kompletterande åtgärder för er att överväga. Ni bör från fall till fall identifiera vilka kompletterande åtgärder som kan vara effektiva för en uppsättning av överföringar till ett specifikt tredjeland när ni använder ett specifikt överföringsverktyg i artikel 46 GDPR. Ni behöver inte upprepa bedömningen varje gång ni utför samma överföring av en specifik typ av personuppgifter till samma tredjeland.

Ni kan vid behov se på följande (icke uttömmande) lista över omständigheter som är relevanta för att veta vilka kompletterande åtgärder som skulle vara mest effektiva vid överföringen av personuppgifter.[71]

- Formatet för de personuppgifter som ska överföras (dvs. i klartext/pseudonymiserat eller krypterat).
- Uppgifternas art (kategorier av uppgifter som omfattas av artiklarna 9 och 10 GDPR).
- Längd och komplexitet i databehandlingsflödet, såsom antal aktörer som är involverade i en behandling och förhållandet mellan dem (till exempel innebär överföringarna flera personuppgiftsansvariga eller både personuppgiftsansvariga och biträden).

[69] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, version 2.0 (Adopted on 18 June 2021).
[70] Bilaga 2 i EDPB:s rekommendationer innehåller en icke uttömmande lista med exempel på sådana ytterligare skyddsåtgärder.
[71] EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0 Adopted on 18 June 2021 https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf, 2023-11-28.

- Möjlighet att uppgifterna kan bli föremål för vidare överföringar inom samma tredjeland eller även till andra tredjeländer (till exempel inblandning av underbiträden).

Några av de personuppgifter som planeras att överföras till tredjeländer kan kräva kompletterande åtgärder medan andra personuppgifter kanske inte kräver det med tanke på formella och/eller praktiska tillämpning av lagstiftningen i tredjeland.[72]

3.6.5.1 Tekniska åtgärder

Kryptering

Användning av kryptering kan vara en effektiv åtgärd när personuppgifter överförs till vissa tredjeländer där lagstiftningen påverkar effektiviteten av överföringsverktyget.

Exempel på effektiva tekniska åtgärder vid tredjelandsöverföringar

En dataexportör använder en molntjänstleverantör i ett tredjeland för att lagra personuppgifter, till exempel för säkerhetskopiering. Följande tekniska åtgärder är effektiva om:

1. personuppgifterna behandlas med stark kryptering före överföring, och identiteten av importören är verifierad,

2. krypteringsalgoritmen (till exempel nyckellängd, driftsläge, om överensstämmer med den senaste tekniken och kan anses vara robust mot kryptoanalys utförs av de offentliga myndigheterna i mottagarlandet med hänsyn till resurserna och tekniska möjligheter (till exempel datorkraft för brutala kraftattacker) tillgängliga för dem,

3. krypteringens styrka och nyckellängden tar hänsyn till den specifika tidsperioden under som sekretess för de krypterade personuppgifterna måste bevaras,

4. krypteringsalgoritmen implementeras korrekt och med korrekt underhållen programvara utan kända sårbarheter vars överensstämmelse med specifikationen av algoritmen valt har verifierats, till exempel genom certifiering,

5. nycklarna hanteras på ett tillförlitligt sätt (genereras, administreras, lagras, länkas till en avsedd mottagares identitet och återkallad), och

6. nycklarna behålls enbart under kontroll av dataexportören eller av en enhet som man litar på inom EES eller under en jurisdiktion som erbjuder en väsentligen likvärdig nivå av skydd som garanteras inom EES.

[72] EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0 Adopted on 18 June 2021 https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf, 2023-11-28.

Mer information om vilka tekniska skyddsåtgärder som kan vidtas vid en överföring av personuppgifter till ett land utanför EU finns i EDPB:s vägledning, se följande länk:https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf

De krypteringsåtgärder som Microsoft erbjuder

Microsoft hanterar nycklarna till den starka standardkrypteringen som finns i miljön, men kunderna kan också använda sin egen kryptering. Ur ett avtalsmässigt perspektiv, kommer Microsoft "(...) inte att tillhandahålla någon tredje part: (a) direkt, indirekt, heltäckande eller obegränsad åtkomst till bearbetade data; (b) plattformskrypteringsnycklar som används för att säkra bearbetade data eller möjligheten att bryta sådan kryptering (...)".

Microsoft erbjuder flera krypteringslösningar (inklusive BYOK) som beskrivs i detalj i dessa separata vitböcker: Kundhanterad kryptering Microsoft 365: https://aka.ms/mscloudCMkryptering.

Kompletterande information finns även i bilaga 5 till denna vägledning.

Microsoft erbjuder också så kallad "Double Key Encryption" (https://aka.ms/dke) där Microsoft lagrar en nyckel i Microsoft Azure, och kunden håller den andra nyckeln. Kunden har full kontroll över en av kundnycklarna med hjälp av Double Key Encryption -tjänsten.

Microsoft har även end-to-end-kryptering i Teams, se följande länk: https://support.microsoft.com/en-us/office/use-end-to-end-encryption-for-microsoft-teams-calls-1274b4d2-b5c5-4b24-a376-606fa6728a90

3.6.5.2 Avtalsrättsliga åtgärder

I vissa situationer kan avtalsrättsliga åtgärder komplettera och förstärka skyddsåtgärderna för överföringsverktyget. Eftersom avtalsåtgärder i allmänhet inte kan binda myndigheterna i det tredje landet när de inte är part i avtalet, behöver dessa åtgärder ofta kombineras med andra tekniska och organisatoriska åtgärder för att tillhandahålla den nivå av dataskydd som krävs.

Detaljerad information om vilka avtalsrättsliga skyddsåtgärder som kan vidtas vid en överföring av personuppgifter till ett land utanför EU finns i EDPB:s vägledning, se följande länk: https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf

Exempel på avtalsrättsliga åtgärder:

- Exportören kan lägga bilagor till kontraktet med information som importören kommer att tillhandahålla innan avtalet ingås, baserat på dess bästa ansträngningar, om tillgång till data av offentliga myndigheter, inklusive inom underrättelseområdet. Detta kan hjälpa data exportören att uppfylla sin skyldighet att dokumentera sin bedömning av skyddsnivån i tredjeland. Det kan också understryka importörens skyldighet att bistå exportören i dess bedöma och engagera sitt ansvar för att ge den objektiv, tillförlitlig information relevant, verifierbar och offentligt tillgänglig eller på annat sätt tillgänglig information.
- Exportören kan också lägga till klausuler enligt vilka importören intygar att

  (1) det inte har avsiktligt skapat bakdörrar eller liknande programmering som kan användas för att komma åt systemet och/eller personuppgifter,

(2) den har inte avsiktligt skapat eller ändrat sina affärsprocesser på ett sätt som underlättar tillgång till personuppgifter eller system, och

(3) den nationella lagstiftningen eller regeringens policy kräver inte att importören skapar eller underhåller bakdörrar eller för att underlätta tillgång till personliga data eller system eller för att importören ska vara i besittning eller överlämna krypteringsnyckeln.

- Kontraktet kan tvinga importören och/eller exportören att omedelbart meddela den registrerade om begäran från tredjelandets offentliga myndigheter eller från importörens oförmåga att följa de avtalsenliga åtagandena, så att den registrerade kan söka information och en effektiv rättelse (till exempel genom att lämna in ett krav hos hans/hennes behöriga tillsynsmyndighet myndighet och/eller rättslig myndighet och visa sin ställning vid domstolarna i det tredjelandet), inklusive kompensation från dataimportören för material och icke-material skada som uppkommit på grund av avslöjandet av hens personuppgifter som överförts under det valda överföringsverktyget i strid med åtagandena som det innehåller.
- Importören kan åta sig att granska lagligheten av varje föreläggande om att lämna ut uppgifter. När den bestrider en order, bör dataimportören även söka interimistiska åtgärder för att fördröja verkställigheten tills domstolen har beslutat i frågan. Importören kan också förbinda sig att tillhandahålla den minsta mängd information som är tillåten när denne ska svara på ordern, baserat på en rimlig tolkning av ordern.

I det biträdesavtal som Microsoft tillhandahåller åtar de sig att vidta följande åtgärder för att bestrida en order.

Bestridande av order

I händelse av att Microsoft får en order från tredje man om tvingat utlämnande av personuppgifter som behandlas enligt detta DPA ska Microsoft:

d. göra alla rimliga ansträngningar för att hänvisa tredje man direkt till Kunden med sin begäran om data.
e. omgående meddela Kunden, såvida det inte är förbjudet enligt lag som är tillämplig på begärande tredje man, och, om det är förbjudet att meddela Kunden, använda alla lagliga medel för att erhålla rätten att undanröja förbudet för att kunna lämna så mycket information som möjligt till Kunden så snart som möjligt
f. använda alla lagliga medel för att bestrida ordern om utlämnande baserat på rättsliga brister enligt den begärande partens lagar eller eventuella relevanta lagkonflikter med tillämplig lag i EU eller tillämplig medlemsstat.

Om efter att ha vidtagit stegen a. till c. ovan, Microsoft eller något av deras koncernbolag fortfarande tvingas lämna ut personuppgifter ska Microsoft endast lämna ut den minsta mängd av dessa data som är nödvändig för att uppfylla ordern om tvingat utlämnande.[73]

[73] Microsoft, https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=32&year=2023, 2023-11-27.

Exempel på andra avtalsrättsliga åtgärder som Microsoft erbjuder:

- Endast behandla personuppgifter på dokumenterade instruktioner från Kunden (personuppgiftsansvarige), inbegripet när det gäller överföringar av personuppgifter till ett tredjeland eller en internationell organisation, såvida inte denna behandling krävs enligt unionsrätten eller enligt en medlemsstats nationella rätt som Microsoft omfattas av, och i så fall ska Microsoft informera Kunden om det rättsliga kravet innan uppgifterna behandlas, såvida sådan information inte är förbjuden med hänvisning till ett viktigt allmänintresse enligt denna rätt.
- Säkerställa att personer med behörighet att behandla personuppgifterna har åtagit sig att iaktta konfidentialitet eller omfattas av en lämplig lagstadgad sekretess.
- Vidta alla åtgärder som krävs enligt artikel 32 GDPR.
- Under beaktande av behandlingens art hjälpa den personuppgiftsansvarige genom lämpliga tekniska och organisatoriska åtgärder, i den mån detta är möjligt, så att den personuppgiftsansvarige kan fullgöra sin skyldighet att svara på begäran om utövande av den registrerades rättigheter enligt kapitel III GDPR.
- Bistå den personuppgiftsansvarige med att se till att skyldigheterna enligt artiklarna 32–36 GDPR fullgörs, med beaktande av typen av behandling och den information som Microsoft har att tillgå.
- Efter den personuppgiftsansvarige val radera eller returnera alla personuppgifter till den personuppgiftsansvarige efter det att tillhandahållandet av behandlingstjänster har avslutats, och radera befintliga kopior såvida inte lagring av personuppgifterna krävs enligt unionsrätten eller medlemsstats nationella rätt.
- Ge den personuppgiftsansvarige tillgång till all information som krävs för att visa efterlevnad av de skyldigheter som fastställs i artikel 28 GDPR och för att främja och bidra till granskningar, inbegripet inspektioner, som genomförs av den personuppgiftsansvarige eller av annan granskare på uppdrag av den personuppgiftsansvarige.[74]

[74] Microsoft, https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=32&year=2023, 2023-11-27.

3.6.5.3 Organisatoriska åtgärder

Organisatoriska åtgärder kan bestå av interna policys och organisatoriska metoder som personuppgiftsansvariga och biträden skulle kunna tillämpa själva och ålägga importörerna av data i tredjeländer. Till exempel bör verksamheten vara organiserad så att den är väl rustad för att hantera utlämningsförfrågningar, den ska ha bra rapporteringslinjer. Det är viktigt att dokumentera väl vid eventuella utlämningsbegäranden. God utbildning och strikt åtkomsthantering är viktiga organisatoriska åtgärder.

I denna vägledning används begreppet *organisatoriska åtgärder* i detta appendix. I de övriga delarna används begreppet *Administrativa åtgärder.* Administrativa åtgärder är ett vidare begrepp än organisatoriska åtgärder och tar inte enbart sikte på det som omfattas av GDPR. Organisatoriska åtgärder är ett begrepp som används i flera bestämmelser i GDPR och även i de riktlinjer som EDPB har gett ut gällande tredjelandsöverföringar.

Ni behöver vara observanta på för vilket syfte de organisatoriska åtgärderna ska användas. Om organisatoriska åtgärderna ska användas som komplement vid tredjelandsöverföringar, ska dessa åtgärder vara sådana att de minskar risken vid en tredjelandsöverföring.

Att välja och genomföra en eller flera organisatoriska åtgärder kommer inte nödvändigtvis att systematiskt säkerställa att er överföring uppfyller kraven. Beroende på de specifika omständigheterna vid överföringen och den bedömning som är utförd på lagstiftningen i tredjelandet, kan organisatoriska åtgärder behövas för att komplettera avtalsmässiga och/eller tekniska åtgärder, för att säkerställa att överföringen uppfyller kraven enligt GDPR.

Detaljerad information om vilka organisatoriska skyddsåtgärder som kan vidtas vid en överföring av personuppgifter till ett land utanför EU finns i EDPB:s vägledning, se följande länk:https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf

Vissa organisatoriska åtgärder hos Microsoft

Customer Lockbox

Nästan all felsökning i Microsoft 365 är automatiserad och kräver inte tillgång till kunddata. Skulle det ändå behövas tillgång till kunddata, exempelvis vid ett supportärende, måste personal på Microsoft följa en gedigen process för att få godkännande till åtkomst. Med Customer Lockbox för Office 365 får organisationen möjlighet att granska och godkänna, eller avvisa, en begäran från Microsoft om tillgång till kunddata (det vill säga organisationens data). Processen används i situationer där en Microsoft-tekniker behöver åtkomst till kunddata för att kunna lösa en supportförfrågan.

Customer Lockbox kan användas som ett steg där en extra bedömning görs av huruvida information som kan komma att delas vid en supportförfrågan är känslig och om informationen i så fall kan delas eller inte.

Policys

Policys kan användas till exempel för att styra tillgängliga applikationer i Teamsklienten eller bestämma om det ska vara möjligt att spela in digitala möten, om detta strider mot verksamhetens beslutade regler för användning.

Tilldelning av licens

Genom att inte tilldela användare licens för en tjänst, exempelvis Microsoft Sway, förhindras användare att använda delar av Microsoft 365 där verksamheten identifierat risker som exempelvis tredjelandsöverföring.

Mer information om organisatoriska åtgärder som Microsoft tillämpar, såsom behörighetstilldelning, policys med mera finner ni på följande länk: https://servicetrust.microsoft.com/

* * *

Om ni bedömer att de kompletterande skyddsåtgärder som ni har vidtagit är tillräckliga kan tredjelandsöverföringen ske med stöd av artikel 46 GDPR. Ni är då klara med alla steg i avsnitt 3 i den här modellen. Ni bör dokumentera era bedömningar och använda aktuella slutsatser som en del i den risk- och sårbarhetsanalys som genomförs med stöd av Appendix A.

Om ni har bestämmelser om sekretess i OSL som gäller för uppgifter i verksamheten, ska ni gå till avsnitt 4 i denna modell. I annat fall är ni klara med alla steg i denna modell.

Om ni inte bedömer att de kompletterande skyddsåtgärder ni har vidtagit är tillräckliga ska ni fortsätta till nästa steg i modellen.

3.6.6 Om de kompletterande åtgärderna inte är tillräckliga, finns det möjlighet att stänga av funktionalitet eller välja bort behandlingen?

Om ni bedömer att de kompletterande skyddsåtgärderna ni kan vidta inte är tillräckliga vid en överföring till tredjeland, bör ni se över den tilltänkta implementeringen av Microsoft 365 för att se om det är möjligt att välja bort vissa funktionaliteter och därigenom undvika en överföring till tredjeland. Visualiseringen och scenariobeskrivningen i Appendix D kan ge vägledning när det gäller vilka alternativ som finns.

Om ni väljer att göra förändringar i den tänkta implementeringen av Microsoft 365, genom att till exempel välja bort viss funktionalitet som innebär tredjelandsöverföringar, bör ni göra om bedömningen ovan i relevanta delar.

Ni bör dokumentera era bedömningar och använda aktuella slutsatser som en del i den risk- och sårbarhetsanalys som genomförs med stöd av Appendix A.

* * *

Ni är nu klara med alla steg i avsnitt 3 i den här modellen.

Om ni har bestämmelser om sekretess i OSL som gäller för uppgifter i verksamheten, ska ni gå till avsnitt 4 i denna modell. I annat fall är ni klara med alla steg i denna modell.

4 Sekretessreglerade uppgifter

4.1 Vad behandlas i detta avsnitt?

Det här avsnittet av den analytiska modellen blir aktuellt att använda om det finns regler om sekretess som gäller i verksamheten, och om det är tänkt att sådana uppgifter som dessa regler tar sikte på ska användas i Microsoft 365. Verksamheter som inte har några bestämmelser om sekretess i OSL som gäller för deras uppgifter behöver inte använda denna del av vägledningen eftersom reglerna i OSL i så fall inte kan vara ett hinder för att använda Microsoft 365.

Den analytiska modellen i avsnittet om OSL hjälper alltså den som har bestämmelser om sekretess i OSL som gäller för uppgifter i verksamheten att ta ställning till om det är tillåtet att använda Microsoft 365 för att behandla dessa uppgifter.

Liksom i övriga avsnitt behandlas här de delfrågor som behöver besvaras i tur och ordning (avsnitt 4.2–4.7). För varje delfråga finns en beskrivning av den juridiska kontexten och information om omständigheter, inklusive om funktionalitet och valmöjligheter i Microsoft 365, som kan vara relevanta för bedömningen av delfrågan.

4.2 Vad är sekretess?

I Tryckfrihetsförordningen (TF) stadgas offentlighetsprincipen, vilken innebär en rätt för var och en att ta del av handlingar från det allmänna, såsom kommuner och myndigheter. Syftet med offentlighetsprincipen är att ge samhället insyn i det allmännas olika verksamheter. Det finns emellertid uppgifter som var och en inte ska kunna ta del av och rätten till insyn är begränsad till allmänna handlingar, under förutsättning att de inte omfattas av sekretess.

Sekretess utgör därmed en begränsning av offentlighetsprincipen och ska endast användas när det är nödvändigt. Reglerna om sekretess finns i OSL och innehåller bland annat bestämmelser om vilka uppgifter som ska omfattas av sekretess och mot vem sekretessen riktar sig. I 2 kap. 1 § OSL stadgas att lagens tillämpningsområde omfattar ett förbud att röja *uppgifter*. Uppgifter i OSL:s mening är inte detsamma som allmänna handlingar i TF:s mening. Tillämpningsområdet för vilka typer av uppgifter som omfattas av bestämmelserna i OSL är således bredare än allmänna handlingar i TF:s mening.

Enligt den systematik som finns i OSL ska en sekretessbedömning göras varje gång någon begär ut en handling från en kommun eller myndighet. Bedömningen görs med andra ord i varje enskilt fall. Med det sagt behöver även användning av molntjänster – om uppgifter lämnas ut till företaget som äger molntjänsten – bedömas utifrån de regler som finns i OSL om skydd för uppgifter som omfattas av sekretess.

Frågan om offentlighet och sekretess vid användning av molntjänster har diskuterats i flera år. E-samverkan (eSam) har bland annat utkommit med olika rättsliga utlåtanden och vägledningar för användning av molntjänster och en vägledning vid myndigheters utkontraktering.[75] Det senaste bidraget i rättsutvecklingen är en ny sekretessbrytande regel för teknisk bearbetning eller teknisk lagring av uppgifter (10 kap. 2 a § OSL). Den nya regeln kan beaktas när en myndighet utkontrakterar IT-drift till en tjänsteleverantör som exempelvis tillhandahåller en teknisk

[75] eSam, Molnfrågan, https://www.esamverka.se/vad-vi-gor/molnfragan.html, 2023-12-13.

infrastruktur eller teknisk plattform för it-drift. Den kan också beaktas när tjänsteleverantören tillhandahåller applikationer och andra IT-baserade tjänster.[76] Regeln kommer att diskuteras i den avslutande delen av detta avsnitt.

4.3 Röjs uppgifterna genom användning av Microsoft 365?

Sekretess definieras i 3 kap. 1 § OSL som ett ”förbud mot att röja en uppgift, vare sig det sker muntligen, genom utlämnande av en allmän handling eller på något annat sätt” och innebär således *ett förbud mot att röja uppgifter*.

För att bedöma om användningen av Microsoft 365 innebär att uppgifter röjs enligt OSL är det därför av avgörande betydelse hur begreppet *utlämnande* tolkas. Bestämmelserna i OSL tar sikte på innehållet i handlingen – uppgifterna – och inte själva handlingen i sig. Uppgifter som omfattas av sekretess och som görs tillgängliga för en tjänsteleverantör anses utlämnade eller röjda.[77]

Om ni lämnar ut en handling i vilken det finns uppgifter som mottagaren inte kan ta del av därför att de är oläsliga för mottagaren, till exempel om de finns i en helt maskad pappershandling eller är krypterade, blir frågan om de oläsliga *uppgifterna* ändå ska anses röjda.

Om uppgifterna är skyddad av kryptering ska inte uppgifterna anses vara röjda om båda förutsättningarna nedan är uppfyllda.

- Mottagaren hindras att ta del av uppgifternas informationsbärande innehåll genom kryptering.
- Mottagaren saknar teknisk kapacitet att forcera krypteringen.[78]

I Bilaga 3 finns mer information om de möjligheter till kryptering som finns i Microsoft 365.

Oavsett om kryptering kan förhindra ett röjande eller inte, så betyder det inte att kryptering är irrelevant för huruvida uppgifter får lämnas ut. Även om kryptering inte skulle bedömas hindra ett röjande, kan kryptering påverka bedömningen av vilken skada eller vilket men ett utlämnande innebär (se avsnitt 4.6.4) samt lämplighetsbedömningen av utkontrakteringen (se avsnitt 4.7.4).

Att uppgifter lämnas ut och röjs är däremot inte alltid ett problem. Det beror på att ett röjande kan vara både tillåtet och otillåtet enligt OSL. Det är bara otillåtet när uppgifterna omfattas av sekretess och det saknas sekretessbrytande regler som gör röjandet tillåtet.

Resonemanget i det följande utgår ifrån att användandet av Microsoft 365 bedöms innebära att uppgifter röjs för Microsoft i OSL:s mening.

* * *

Om ni gör bedömningen att den implementering av Microsoft 365 (vald krypteringslösning med mera) som ni valt innebär att (1) Microsoft inte kan ta del av uppgifternas informationsbärande innehåll och (2) Microsoft inte heller kan forcera krypteringen kan uppgifterna behandlas i Microsoft 365 utan hinder av sekretess. Ni är i så fall klara med alla steg i denna modell. Ni bör dokumentera era bedömningar och använda aktuella slutsatser som en del i den risk- och sårbarhetsanalys som genomförs med stöd av Appendix A.

[76] Prop. 2023/22:97 s. 7.
[77] Prop. 2023/22:97 s. 7.
[78] Prop. 2023/22:97 s. 7.

Om ni gör bedömningen att den implementering av Microsoft 365 (vald krypteringslösning med mera) som ni valt innebär att det är antingen möjligt för Microsoft att ta del av uppgifternas informationsbärande innehåll eller att krypteringen kan forceras av Microsoft, bör ni fortsätta till nästa steg i modellen och bedöma om uppgifterna omfattas av sekretess.

4.4 Finns det en tillämplig sekretessbestämmelse?

Som nämnt ovan innebär sekretess ett förbud att röja uppgifter. Bestämmelser om vilka uppgifter som ska omfattas av sekretess finns i OSL.

Ett första steg i bedömningen av om en uppgift omfattas av sekretess är att avgöra om det finns en sekretessbestämmelse som gäller för de aktuella uppgifterna.

Sekretessbestämmelserna i OSL är utformade så att de antingen gäller i utpekade *verksamheter* eller för vissa *typer av uppgifter*. Exempel på en sekretessbestämmelse som gäller i en utpekad verksamhet är 26 kap. 1 § OSL där ”sekretess gäller *inom socialtjänsten* för uppgift om en enskilds personliga förhållanden”. Exempel på en sekretessbestämmelse som gäller för särskild uppgift är 21 kap. 1 § OSL där ”sekretess gäller för uppgift som rör en enskilds hälsa eller sexualliv…”.

Sekretessbestämmelserna syftar till att skydda ett bestämt intresse som anses vara särskilt skyddsvärt. Sådana intressen kan vara skydd för enskilda, verksamheter eller Sveriges säkerhet.

* * *

Om det saknas en tillämplig sekretessbestämmelse omfattas uppgifterna inte av sekretess. Det innebär att det enligt definitionen av sekretess i 3 kap. 1 § OSL inte finns något förbud mot att röja dem; tvärtom är presumtionen att åtminstone allmänna handlingar i så fall är offentliga och ska lämnas ut. Det innebär att det är tillåtet att lämna ut uppgifterna genom att använda Microsoft 365. Ni är i så fall klara med alla steg i denna modell. Ni bör dokumentera era bedömningar och använda aktuella slutsatser som en del i den risk- och sårbarhetsanalys som genomförs med stöd av Appendix A.

Om det finns en tillämplig sekretessbestämmelse behöver det i sig inte innebära ett förbud mot att lämna ut uppgifterna. Däremot behöver ni fortsätta till nästa steg i modellen och göra en bedömning av vilken skada eller vilket men som kan drabba det intresse som sekretess-bestämmelsen ska skydda om uppgifterna lämnas ut genom att använda Microsoft 365.

4.5 Vad är skada och men?

4.5.1 Allmänt om skada och men

Begreppet skada avser endast ekonomisk skada, till skillnad från men som har en mer vidsträckt innebörd.[79] Men kan utgöras av olika typer av integritetskränkningar, som missaktning eller obehag, men även konsekvenser av ekonomisk art som inte uppfyller kraven för ekonomisk skada.

I skadebedömningen är det viktigt att komma ihåg att det är en ständig intresseavvägning mellan sekretess och offentlighet. Uppgifter som hanteras av det allmänna ska inte skyddas av sekretess om det inte är nödvändigt med hänsyn till enskildas eller annans säkerhet; huvudregeln är istället transparens och öppenhet.

För att underlätta dessa avvägningar har sekretessbestämmelserna i OSL tre olika typer av skaderekvisit: i) absolut, ii) rakt, och iii) omvänt skaderekvisit.

4.5.2 Absolut sekretess

Om en uppgift omfattas av en sekretessbestämmelse med absolut sekretess finns det inte utrymme att göra en bedömning av vilken skada ett utlämnande av uppgifterna skulle kunna innebära. Det absoluta skaderekvisitet känns igen genom att det inte står något om i vilka fall uppgifterna får lämnas ut, utan det står endast att det föreligger sekretess.

Exempel på en bestämmelse med absolut sekretess är 27 kap. 1 § OSL där det stadgas att sekretess gäller ”i verksamhet som avser bestämmande av skatt eller fastställande av underlag för bestämmande av skatt eller som avser fastighetstaxering för uppgift om en enskilds personliga eller ekonomiska förhållanden”.

Om det råder absolut sekretess är det endast tillåtet att lämna ut uppgifterna om det finns en tillämplig sekretessbrytande regel.

För mer information om sekretessbrytande bestämmelser, se avsnitt 4.7.

4.5.3 Rakt skaderekvisit

Om en uppgift omfattas av en sekretessbestämmelse med rakt skaderekvisit presumeras inte skada vid utlämnande av uppgifterna. Det innebär att uppgifterna får lämnas ut så länge som det inte innebär skada. Det raka skaderekvisitet används på uppgifter som typiskt sett är harmlösa ifall det utlämnas. Huvudregeln i dessa fall är med andra ord offentlighet. Skaderekvisiten kan ha olika formuleringar och ibland används ”skada”, ”men” eller liknande, men i andra fall används ”allvarligt men” eller ”allvarlig skada”. I de fallen är det särskild presumtion för offentlighet.[80]

Exempel på rakt skaderekvisit är 22 kap. 4 § OSL där det framgår att sekretess gäller ”i ärende om byte av namn för uppgift om en enskilds personliga förhållanden, om det av särskild anledning kan antas att den enskilde eller någon närstående till denne lider men om uppgifterna röjs”.

4.5.4 Omvänt skaderekvisit

Om en uppgift omfattas av en sekretessbestämmelse med omvänt skaderekvisit presumeras skada vid ett utlämnande av uppgifterna. Det innebär att uppgifterna endast får lämnas ut om det

[79] Zetterström, S, m.fl, Offentlighet, sekretess och dataskydd, s. 74.
[80] Holstad, S, m.fl, Sekretess i allmän verksamhet, s. 30.

kan antas att skada inte kommer föreligga vid ett utlämnande. Huvudregeln i dessa fall är med andra ord sekretess.

Exempel på omvänt skaderekvisit är 25 kap. 1 § OSL där det stadgas att sekretess ”gäller inom hälso- och sjukvården för uppgift om en enskilds hälsotillstånd eller andra personliga förhållanden, om det inte står klart att uppgifterna kan röjas utan att den enskilde eller någon närstående till denne lider men”.

4.6 Innebär användningen av Microsoft 365 skada eller men?

4.6.1 Om bedömningen av skada och men vid utlämnande av en större mängd uppgifter

Systematiken i OSL är uppbyggd på att ett utlämnande av en uppgift sker på begäran av en enskild och en bedömning av huruvida uppgifterna omfattas av sekretess görs i varje enskilt fall. Vid användande av molntjänster är det inte praktiskt möjligt att göra en sekretessbedömning för varje enskild uppgift, utan det är nödvändigt att göra en schablonbedömning för en stor mängd uppgifter.

Vägledning för hur en prövning av ett utlämnande av en större mängd uppgifter ska göras kan hämtas från propositionen till OSL avseende begäran av massuttag.[81] I propositionen framgår att det är möjligt att besluta om en begäran av massuttag under förutsättning att det finns kännedom om mottagaren, syftet med begäran och den *typiska skaderisken*.[82] eSam har intagit en liknande inställning och menar att det vid utlämning av en större mängd uppgifter kan göras enligt en schabloniserad prövningsmodell.[83] eSams prövningsmodell innehåller liknande kriterier som de föreslagna i propositionen, nämligen kunskap om mottagaren, hur denne kommer hantera uppgifterna och spridningsrisken. Dessa kriterier, tillsammans med den typiska skaderisken för uppgifterna, utgör enligt eSam ett tillräckligt bedömningsunderlag för utlämnande.[84]

Vid molntjänstanvändning är det känt vem som är mottagaren av informationen samt syftet med användningen. Syftet framgår av vad som avtalats mellan parterna. Ofta faller det inom ramen för det som i kallas *teknisk bearbetning eller teknisk lagring* (se avsnitt 4.7.3 för diskussion av begreppen), men det är inte uteslutet att det även kan finnas andra syften.

När uppgifter lämnas ut för teknisk bearbetning eller teknisk lagring är det inte meningen att mottagaren ska använda uppgifterna för egna syften så som att sprida informationen vidare; all bearbetning eller lagring ska ske för den utlämnande myndighetens syften.[85] För att minska spridningsrisken ytterligare finns det olika säkerhetsåtgärder som myndigheterna kan vidta, till exempel tystnadsplikt och kryptering eller annan pseudonymisering av uppgifterna.

4.6.2 Om tystnadsplikt

Tystnadsplikt föreligger i två former, antingen straffsanktionerad tystnadsplikt eller civilrättslig tystnadsplikt. Genom lagen (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter omfattas även privata molntjänstleverantörer av straffsanktionerad tystnadsplikt. Av 4 § framgår att den ”som på grund av anställning eller på något annat sätt deltar i eller har deltagit i en tjänsteleverantörs verksamhet att på uppdrag av en myndighet endast

[81] Prop. 1979/80 med förslag till sekretesslag m.m. Del A. s. 81 f.
[82] Prop. 1979/80 med förslag till sekretesslag m.m. Del A. s. 81.
[83] eSam, Outsourcing 2.0 – En vägledning om sekretess och dataskydd, s. 49.
[84] eSam, Outsourcing 2.0 – En vägledning om sekretess och dataskydd, s. 49.
[85] Jämför med resonemanget i SOU 2021:1 Säker och kostnadseffektiv it-drift, s. 296.

tekniskt bearbeta eller tekniskt lagra uppgifter får inte obehörigen röja eller utnyttja dessa uppgifter.” Utkontraktering betyder i sammanhanget anlitande av en extern part för att leverera en tjänst, den externa parten kan bli en uppgiftsmottagare. Ni bör påminna uppgiftsmottagaren att den straffsanktionerade tystnadsplikten gäller för personal placerad i Sverige.

En utmaning med lagen, som togs upp av ett antal remissinstanser, är att den gäller med begränsning till den allmänna domsrätten enligt 2 kap. brottsbalken, vilket bland annat innebär att lagen endast är tillämplig på svenska medborgare eller utlänningar som befinner sig i Sverige.[86] När en tjänsteleverantör har ett bolag i Sverige med anställda här är det inte helt ovanligt att viss bearbetning görs av personal som är placerad utanför Sveriges gränser. I sådana fall är det viktigt att säkerställa att även den personal som är placerad utanför landet omfattas av tystnadsplikt, förslagsvis genom en klausul i avtalet med leverantören.

4.6.3 Om kryptering, annan pseudonymisering eller anonymisering

Ni kan även minska spridningsrisken med utlämnandet genom kryptering eller annan pseudonymisering. Enligt ett JO-utlåtande kan pseudonymiserade uppgifter motverka skada för den enskilde då avidentifierade uppgifter ansågs innebära att den enskilde inte lidit skada vid utlämnande.[87]

Om uppgifterna är krypterade på ett sådant sätt att mottagaren inte kan ta del av dem lider det skyddsvärda intresset typiskt sett ingen skada eller inget men. Detsamma gäller om uppgifterna pseudonymiseras eller anonymiseras på ett sådant sätt att det inte går att avgöra vem eller vad de rör.

Det finns olika alternativ för att kryptera uppgifter i Microsoft 365. De beskrivs utförligt i Bilaga 3. I korthet kan kunden välja mellan lösningar där Microsoft håller krypteringsnyckeln, lösningar där kunden har en egen krypteringsnyckel, eller en kombination av de båda varianterna.

När det gäller annan pseudonymisering och anonymisering är det exempel på tekniska och administrativa åtgärder som myndigheten potentiellt skulle kunna vidta vid den praktiska implementationen av Microsoft 365. Hur det skulle kunna se ut är beroende av omständigheterna i det enskilda fallet.

4.6.4 Bedömning av skada och men

4.6.4.1 Underlag för bedömningen

För att kunna göra en bedömning av om ett användande av Microsoft 365 kan innebära skada eller men är det viktigt att ni dels vet vilka typer av uppgifter ni vill använda i Microsoft 365, dels att ni har kunskap om vilka åtgärder ni respektive Microsoft kommer att vidta för skydda uppgifterna och upprätthålla sekretessen.

Till att börja med behöver ni fundera på vilka verksamheter som är tänkta att använda Microsoft 365 och vilken typ av uppgifter som kan komma att behandlas i Microsoft 365. Besvara följande frågor och dokumentera svaren.

- Vilka kategorier av uppgifter om vilka kategorier av personer kommer hanteras i molntjänsten?

[86] Se prop. 2019/20:201 Tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter, s. 16 f, samt Skatteverkets och Åklagarmyndighetens remissvar till SOU 2018:25 Juridik som stöd för förvaltningens digitalisering.
[87] JO beslut den 4 juni 2019, dnr 6794-2017, Kritik mot Region Halland för att ha lämnat ut personuppgifter till tredje land i strid med gällande lagstiftning m.m. s. 16.

- Vilken typ av verksamhet hör uppgifterna till?
- Finns det en sekretessbestämmelse som gäller för uppgiftstypen eller verksamheten (se avsnitt 4.4)?
- Vilket intresse är det som sekretessbestämmelsen ska skydda (se avsnitt 4.4)
- Vilken typ av skaderekvisit omfattas uppgifterna i så fall av (se avsnitt 4.5)?

I vissa fall kan en utkontraktering innefatta ett utlämnade av flera olika uppgiftstyper med olika grader av sekretess. I de fallen genomförs skadebedömningen med utgångspunkt att alla uppgifter träffas av den högre sekretessgraden.

Sedan behöver ni fundera på och dokumentera hur ni har tänkt implementera Microsoft 365, det vill säga vilken funktionalitet och vilka säkerhetsåtgärder ni har tänkt använda. Besvara följande frågor och dokumentera svaren.

- Kommer lagringen av uppgifterna ske i eller utanför Sverige?
- Kommer ni att använda funktionalitet som innebär att uppgifter överförs till ett annat land än där de lagras?
- Kommer Microsofts personal kunna ta del av uppgifterna? Om ja, i vilken form?
- Var befinner sig personalen geografiskt? Träffas samtliga som tar del av uppgifter av den svenska straffrättsliga tystnadsplikten?
- Om det finns anställda som tar del av uppgifter som inte träffas av den straffrättsliga tystnadsplikten: finns en civilrättslig tystnadsplikt avtalad för dessa anställda?
- Vilka säkerhetsåtgärder
    - i Microsoft 365 har ni tänkt använda?
    - har ni tänkt implementera vid sidan av Microsoft 365?

Exempel på säkerhetsåtgärder i Microsoft 365

I Appendix C finns en utförlig beskrivning av de säkerhetsåtgärder som erbjuds i Microsoft 365. Visualiseringen och scenariobeskrivningarna i Appendix D kan också ge vägledning när det gäller vilka alternativ som finns. Nedan följer några exempel på säkerhetsåtgärder som erbjuds i Microsoft 365.

- ✓ **Microsoft Secure Score & Security Compliance Toolkit**, stödjer konfiguration, mätning och uppföljning för att säkerställa att det finns tillräckliga skyddsnivåer för uppgifter i Microsoft 365.
- ✓ **Utbildning** i MSMD hos Microsofts partner.
- ✓ **Double Key Encryption** (eller motsvarande) som krypterar tillgång till data för Microsoft via organisationens egen krypteringsnyckel.
- ✓ **Microsoft 365 Hybrid** med Exchange och SharePoint lokalt installerad, gör det möjligt att lagra vissa data lokalt och annan data i Microsoft 365.
- ✓ **End-to-end encryption** innebär möjligheten till kryptering mellan slutpunkter.
- ✓ **Customer Lockbox** som innebär en ytterligare möjlighet att begränsa informationsdelning vid supportärenden.

4.6.4.2 Bedömning

Ni behöver nu bedöma vilken typ av skada eller men det skyddsvärda intresset typiskt sett skulle lida om uppgifterna lämnades ut genom användningen av Microsoft 365, med den implementering och de tekniska och administrativa åtgärder ni har valt. Det är utlämningen i denna specifika kontext som ska bedömas, inte vilken skada eller vilket men som skulle kunna uppstå ifall uppgifterna skulle bli tillgängliga för allmänheten.

Ni behöver se till att bedömningen tar hänsyn till varje tillämplig sekretessbestämmelse och varje identifierat skyddsvärt intresse. Besvara följande frågor och dokumentera svaren.

- Vilken skada eller vilket men skulle det skyddsvärda intresset typiskt sett kunna lida om uppgifterna skulle komma Microsoft eller Microsofts personal till del, med hänsyn tagen till de tekniska och administrativa skyddsåtgärder ni kommer att implementera?
- Hur skulle den skadan eller det menet kunna realiseras vid användning av Microsoft 365?
- Vid rakt skaderekvisit (presumtion för offentlighet): Är det något som tyder på att det är sannolikt att skadan eller menet skulle realiseras vid er användning av Microsoft 365?
    - Om ja, finns det ytterligare åtgärder som kan vidtas för att minska risken för skada eller men?
- Vid omvänt skaderekvisit (presumtion för sekretess). Står det klart att skadan eller menet inte skulle realiseras vid er användning av Microsoft 365?
    - Om nej, finns det ytterligare åtgärder som kan vidtas för att minska risken för skada eller men?

* * *

Om ni efter ovan beskrivna bedömning kommer fram till att det *typiskt sett* inte skulle innebära risk för skada eller men att lämna ut uppgifterna genom att använda Microsoft 365, alternativt att de vidtagna åtgärderna motverkar risken för skada eller men, omfattas uppgifterna inte av sekretess och ni kan lämna ut dem genom att använda Microsoft 365. Ni är i så fall klara med alla steg i denna modell. Ni bör dokumentera era bedömningar och använda aktuella slutsatser som en del i den risk- och sårbarhetsanalys som genomförs med stöd av Appendix A.

Om ni efter ovan beskrivna bedömning kommer fram till att det typiskt sett kan innebära risk för skada eller men att lämna ut uppgifterna genom att använda Microsoft 365 omfattas uppgifterna av sekretess gentemot Microsoft. Då får de inte lämnas ut genom att använda Microsoft 365 om det inte finns en tillämplig sekretessbrytande regel. Fortsätt till nästa steg i modellen för att göra denna bedömning.

4.7 Finns det en sekretessbrytande bestämmelse?

4.7.1 Om sekretessbrytande bestämmelser i OSL

Om uppgifterna omfattas av sekretess finns det ändå möjlighet att kunna lämna ut uppgifterna, om de omfattas av någon sekretessbrytande bestämmelse. De sekretessbrytande bestämmelserna finns i 10 kap. OSL. Bestämmelserna är indelade i tre delar: första delen som är till förmån för den enskilda, andra delen som är till förmån till den enskilda och myndigheter och den tredje delen som är till förmån endast för myndigheter. De sekretessbrytande bestämmelserna innebär att sekretess som annars skulle ha skyddat uppgifterna inte längre ska gälla i vissa undantagssituationer.

I 10 kap. 2 a § OSL finns en sekretessbrytande bestämmelse som syftar till att skapa bättre förutsättningar för utkontraktering, det vill säga anlitande av tredje part för att leverera en tjänst, och samordning av IT-drift.[88] Bestämmelsen är tillämplig om samtliga följande kriterier är uppfyllda.

- Utlämnandet sker till en enskild eller annan myndighet (uppgiftsmottagare).
- Uppgiftsmottagaren har för den utlämnande myndighetens räkning i uppdrag att endast tekniskt bearbeta eller tekniskt lagra uppgifterna.
- Det är med hänsyn till omständigheterna inte olämpligt att uppgifterna lämnas ut.

I följande avsnitt beskrivs respektive kriterium.

4.7.2 Sker utlämnandet till enskild?

För att det första kriteriet i 10 kap. 2 a § OSL ska vara tillämpligt ska ett *utlämnande* ske. Se avsnitt 4.3 för bedömning om ett utlämnande skett. Utlämnandet ska dessutom ske till en *enskild*, vilket kan vara en fysisk eller juridisk person.[89]

4.7.3 Har uppgiftsmottagaren i uppdrag att endast tekniskt bearbeta eller tekniskt lagra uppgifterna?

För att det andra kriteriet i 10 kap. 2 a § OSL ska vara uppfyllt ska uppgiftsmottagarens uppdrag vara att *endast tekniskt bearbeta eller tekniskt lagra* uppgifterna. Vad som ingår i uppdraget ska framgå av vad som avtalats mellan parterna. Uppdraget ska endast avse teknisk lagring eller bearbetning och inte avse utkontraktering i annat syfte. Vilka åtgärder som omfattas av uttrycket teknisk bearbetning eller teknisk lagring kan förändras över tid med anledning av den tekniska utvecklingen.[90]

Genom den nya sekretessbrytande bestämmelsen har begreppen teknisk bearbetning och teknisk lagring både förtydligats och till viss del förändrats. Exempel i förarbetena förtydligar vilka åtgärder som omfattas av begreppen. Ett uppdrag för att teknisk bearbeta eller tekniskt lagra uppgifter kan vara att införa, förvalta, utveckla och avveckla en it-driftstjänst. Under dessa olika faser kan olika åtgärder vara nödvändiga för att upprätthålla den tillgänglighet, funktionalitet och prestanda i tjänsten som avtalats mellan parterna. Som exempel på åtgärder som omfattas av teknisk bearbetning och teknisk lagring nämns följande.

- Förändring och tillägg i en befintlig tjänsts funktionalitet.
- Etablering av en tilläggstjänst.
- Integration med andra tjänster.
- Konfiguration, test och utveckling.
- Tillhandahållande av supporttjänster.
- Säkerhetstester och andra säkerhetshöjande åtgärder som uppgradering, uppdatering, säkerhetskopiering, kryptering, anonymisering, pseudonymisering och incidenthantering.
- Vid avveckling av en tjänst kan era uppgifter behöva migreras eller exporteras tillbaka till er eller till en annan uppdragstagare.[91]

[88] Prop. 2022/23:97 s. 10.
[89] Prop. 1979/80:2 Del A s. 329.
[90] Prop. 2022/23 s. 10–11.
[91] Prop. 2023/22:97 s. 16–17.

Den tidigare nämnda förändringen av begreppen gäller uppgiftsmottagarens personals möjlighet att ta del av uppgifterna.[92] Om personalens tillgång till uppgifterna är nödvändig för att utföra arbetsuppgifter som utgör ett led i den tekniska bearbetningen eller tekniska lagringen anses det omfattas av begreppen teknisk bearbetning och teknisk lagring. Exempel på uppgifter som anses vara nödvändiga i detta avseende är drifts- och säkerhetsrelaterad information (uppgifter om användarkonton, loggar, krypteringsnycklar, lösenord och säkerhetsinställningar), men kan även vara andra uppgifter i läsbar form. Lagstiftaren har inte tydliggjort vilka övriga uppgifter som omfattas.[93]

Ni bör undersöka vad som är avtalat mellan er och Microsoft för att bedöma om det avtalade avser endast teknisk bearbetning och teknisk lagring av uppgifterna. Det är endast de uppgifter som utkontrakterats för teknisk bearbetning och teknisk lagring som kan lämnas ut med stöd av bestämmelsen. Om avtalet däremot omfattar andra åtgärder än vad som bedöms vara teknisk bearbetning och lagring kan ni inte stödja utlämnandet på 10 kap. 2 a § i OSL.

4.7.4 Är det med hänsyn till omständigheterna inte olämpligt att uppgifterna lämnas ut?

Ni behöver därefter göra en *lämplighetsbedömning*, eftersom lämplighet är ett villkor för att uppgifterna kan lämnas ut med stöd av 10 2 a § OSL. Inom ramen för lämplighetsbedömningen ska alla omständigheter som är relevanta för det enskilda fallet beaktas, på samma sätt som vid annan skadeprövning vid utlämnande av allmänna handlingar. Som utgångspunkt ska omständigheter som har koppling till er som den utlämnande myndigheten och er uppgiftsmottagare beaktas. Dessutom ska omständigheter som har koppling till uppgifterna som kan bli föremål för utlämnande beaktas.

Följande omständigheter kan exempelvis ha betydelse för bedömningen.[94]

- Om utlämnandet är förenligt med övrig tillämplig lagstiftning i det enskilda fallet.
- Vilken typ av uppgifter det rör samt uppgifternas omfattning.
    - Se avsnitt 2.1 och 2.6 i vägledningen för mer information om informationsklassning.
- Vilka skyddsintressen som sekretessen gäller till förmån för.
    - Se avsnitt 4.4 för bedömning av sekretessbestämmelser.
- Om det finns villkor i avtalet som riskerar att frånta er kontrollen över uppgifterna.
    - I detta sammanhang bör ni granska ert avtal med Microsoft med fokus på de instruktioner ni lämnat till Microsoft för hantering av uppgifterna. Vidare kan granskningen innefatta att undersöka om Microsofts uppdrag endast innebär teknisk bearbetning och teknisk lagring, se avsnitt 4.7.3.
- Om det förekommer underleverantörer som potentiellt kan få tillgång till uppgifterna samt vilka krav som i så fall ställs på dem att förhindra vidare spridning av uppgifterna.
- Om uppgiftsmottagaren omfattas av en lag- eller avtalsreglerad tystnadsplikt.
    - Kontrollera om personalen hos Microsoft och eventuella underleverantörer som potentiellt kan få del av uppgifterna omfattas av tystnadsplikt. Undersök först vilket Microsoftbolag som är part i avtalet. Undersök sedan om dess personal som tar

[92] Jämför Prop. 2023/22:97 s. 16–17 med HFD 2018 ref. 48 där förvaltningsdomstolen tidigare fastslagit att uppgiftsmottagaren både administrativt och tekniskt ska begränsa den egna personalens tillgång till uppgifter så att dessa inte är tillgängliga i läsbart skick. Personalen ansågs tidigare enbart kunna ta del av den drifts- och säkerhetsrelaterade informationen för att teknisk bearbetning eller teknisk lagring av uppgifter skulle föreligga.

[93] Prop. 2023/22:97 s. 17.

[94] Prop. 2023/22:97 s. 17.

del av uppgifterna befinner sig i Sverige och därmed omfattas av den svenska straffrättsliga tystnadsplikten. Undersök till sist om personal som befinner sig utanför Sverige tar del av uppgifter och i så fall omfattas av civilrättslig tystnadsplikt genom avtal med Microsoft, se avsnitt 4.6.2.

- Var uppgifterna kommer att hanteras geografiskt.
    - Ni bör granska avtalet med Microsoft och bedöma om det kan bli aktuellt med annan jurisdiktion än den svenska. Det kan dels påverka tillämpligheten av den lagreglerade tystnadsplikten, dels frågan om risken att utländska myndigheter har möjlighet att begära eller bereda sig tillgång till de uppgifter som omfattas av sekretess. Jämför med resonemanget i avsnitt 3.3 om tredjelandsöverföringar (notera återigen att det avsnittet endast omfattar uppgifter som bedöms vara personuppgifter; sekretessbelagda uppgifter kan omfatta fler eller färre uppgifter än personuppgifter).
- Vilka åtgärder uppgiftsmottagaren vidtar för att skydda uppgifterna.
    - I vissa fall påverkar vidtagna säkerhetsåtgärder samtliga perspektiv, exempelvis påverkar kryptering av uppgifter både er kontroll över uppgifterna och skyddet av de faktiska uppgifterna. Dessutom är det en omständighet som påverkar uppgiftsmottagarens tillgång till uppgifterna. Ni bör undersöka hur uppgifterna skyddas genom att använda insikter från arbetet med risk- och sårbarhetsanalysen, se avsnitt 2.2 i vägledningen samt avsnitt 7 i Appendix A.
- Vilka risker som finns i förhållande till samlokalisering av uppgifter tillhörande olika kunder till uppgiftsmottagaren.
    - Ni bör ta upp riskerna specifikt i risk- och sårbarhetsanalysen. Se även avsnitt 2.2 i vägledningen samt Appendix A.

* * *

Om uppgifterna omfattas av sekretess men det finns en sekretessbrytande bestämmelse, till exempel 10 kap. 2 a § OSL, som kan användas går det bra att lämna ut dessa uppgifter genom att använda Microsoft 365. Ni är då klara med alla steg i den här modellen. Ni bör dokumentera era bedömningar och använda aktuella slutsatser som en del i den risk- och sårbarhetsanalys som genomförs med stöd av Appendix A.

Om ni bedömer att det inte är möjligt att tillämpa 10 kap. 2 a § OSL för utkontraktering på grund av att det är olämpligt att uppgifterna lämnas ut, ska ni fortsätta till nästa steg i modellen.

Om ni av andra skäl bedömer att det saknas en tillämplig sekretessbrytande bestämmelse som kan användas är det inte förenligt med OSL att lämna ut uppgifterna. Ni är då klara med alla steg i den här modellen.

Ni bör dokumentera era bedömningar och använda aktuella slutsatser som en del i den risk- och sårbarhetsanalys som genomförs med stöd av Appendix A.

4.7.5 Är det med hänsyn till omständigheterna inte olämpligt att uppgifterna lämnas ut efter att ha vidtagit vissa åtgärder?

Om ni bedömer att det är olämpligt att uppgifterna lämnas ut, kan ni se över den tilltänkta implementeringen av Microsoft 365 för att undersöka om det är möjligt att vidta åtgärder som gör att utkontrakteringen kan bedömas vara lämplig. Som ovan nämnts ska ni vid lämplighetsbedömningen beakta omständigheter som har koppling till er som den utlämnande myndigheten och till uppgiftsmottagaren. Dessutom ska omständigheter som har koppling till uppgifterna som kan bli föremål för utlämnande beaktas.

Exempelvis kan en åtgärd vara att anpassa er användning av Microsoft 365 så att sekretess-reglerade uppgifter inte behandlas utanför Sverige. En annan åtgärd skulle kunna vara att avtala med Microsoft om åtgärder som tydliggör hur uppgifterna ska behandlas, vad de ska användas till eller som annars underlättar kontrollen av uppgifterna under hela avtalsperioden och förhindrar att de får spridning. Det kan bland annat vara villkor om att

- Microsoft inte får använda uppgifterna för sina egna ändamål.
- Microsoft endast får anlita underleverantörer efter ert skriftliga godkännande.
- Microsofts personal omfattas av civilrättslig tystnadsplikt i de fall de inte omfattas av den straffrättsliga tystnadsplikten, se avsnitt 4.6.2.
- Microsoft ska lämna tillbaka och därefter radera uppgifterna vid avtalets slut.

Om anledningen till att utkontrakteringen bedöms vara olämplig är att vissa uppgifter som skulle omfattas av den har ett väldigt högt skyddsvärde kan kryptering eller anonymisering av dessa uppgifter vara att alternativ, se avsnitt 4.6.3. Ett annat alternativ kan vara att säkerställa att Microsoft 365 inte används för att hantera den typen av uppgifter genom att skapa interna rutiner som tydliggör vilka uppgifter som får hanteras i Microsoft 365.

* * *

Om ni efter att ha vidtagit vissa åtgärder bedömer att det inte är olämpligt att uppgifterna lämnas ut, går det bra att lämna ut dessa uppgifter genom att använda Microsoft 365.

Om ni efter att ha vidtagit vissa åtgärder bedömer att det är olämpligt att uppgifterna lämnas ut, är det inte förenligt med OSL att lämna ut uppgifterna.

Ni är nu klara med alla steg i den här modellen. Ni bör dokumentera era bedömningar och använda aktuella slutsatser som en del i den risk- och sårbarhetsanalys som genomförs med stöd av Appendix A.

Appendix C – Administrativa och tekniska åtgärder

1.1 Inledning

Utgångspunkten för detta appendix är att ge offentliga verksamheter en uppfattning om vilka mitigerande administrativa och tekniska åtgärder som kan vidtas i eller kring Microsoft 365 i syfte att hantera de risker eller andra aspekter som användning av tjänsten kan medföra. Åtgärderna kan i flera fall både användas fristående och i kombination för att förstärka varandra.

Ett systematiskt och kontinuerligt informationssäkerhetsarbete är en förutsättning för att en verksamhet ska kunna hantera de risker och andra aspekter som användning av en molntjänst innebär. Genom ett sådant tillvägagångssätt skapas förutsättningar för en övergripande målbild för informations- och it-säkerhet. Med utgångspunkt i de risker organisationen identifierat i samband med ett införande fastställs sedan relevanta administrativa och tekniska skyddsåtgärder i styrande dokument. Här är också en väl implementerad informationskartläggning och informationsklassning en förutsättning för att skydda information på ett relevant sätt samtidigt som information och system kan användas effektivt. I arbetet med informationssäkerhet och åtgärder finns det flera standarder, regelverk och riktlinjer att utgå ifrån, exempelvis MSB:s förskrifter för statliga myndigheter MSBFS 2020:6 och MSBFS 2020:7 som bygger på ISO 27000[1].

Vid en risk- och sårbarhetsanalys inför ett införande av Microsoft 365 behöver verksamheten gå igenom vilka administrativa och tekniska åtgärder som verksamheten kan införa för att mitigera de risker som identifieras. Ofta finns det olika avvägningar att göras i valet mellan administrativa och tekniska åtgärder. I vissa fall värderas tekniska åtgärder med större vikt än administrativa, exempelvis inom vissa delar av Dataskyddsförordningen (GDPR). I andra fall är administrativa åtgärder de enda som erbjuds för att hantera en identifierad risk, exempelvis ett internt förbud om att inte diskutera säkerhetsskyddsklassificerade uppgifter eller känsliga personuppgifter i videomöten.

1.2 Exempel på åtgärder

Nedanstående exempel på mitigerande åtgärder är inte på något sätt en komplett förteckning över möjligheterna till sådana åtgärder i Microsoft 365, utan syftet med dessa beskrivningar är att ge organisationer stöd i processen att utifrån egna förutsättningar och behov värdera denna typ av åtgärder. I denna vägledning har vi valt att beskriva exemplen på de möjliga mitigerande åtgärderna i följande fyra övergripande områden:

- Användning av Microsoft 365
- Informationsklassning och skyddsåtgärder
- Roller och rättigheter
- Standarder och regelefterlevnad

[1] https://www.sis.se/produkter/informationsteknik-kontorsutrustning/allmant/ss-en-isoiec-2700120232/, 2023-12-15.

2 Användning av Microsoft 365

2.1 Administrativa åtgärder

2.1.1 Interna regelverk och utbildning

En organisation kan genom beslut reglera hur Microsoft 365 får användas i olika sammanhang, antingen generellt eller utifrån vilken information som behandlas. Dessa regler för användning kan kommuniceras till verksamheten genom policys, föreskrifter, instruktioner och utbildning. I dessa regler kan även ingå bestämmelser om hur tekniska åtgärder får, kan eller ska tillämpas.

2.2 Tekniska åtgärder

Nedan beskrivs förslag på tekniska åtgärder.

2.2.1 Tillgängliga tjänster och funktioner

Tjänsterna i Microsoft 365 kan på olika sätt styras eller blockeras för hela eller delar av organisationen. Några exempel:

- Genom att inte tilldela användare licens för en tjänst, exempelvis Microsoft Sway, förhindras användare att använda delar av Microsoft 365 där verksamheten identifierat risker som exempelvis tredjelandsöverföring.
- Med centralt styrda policyer för klientapplikationer kan organisationen blockera anslutna upplevelser som analyserar data, exempelvis diktering, om det bedöms vara en risk att röstdata behandlas av Microsoft.
- Användning av tredjeparts lagringstjänster, som Box och Google Drive, kan stängas av i Teams på organisationsbasis för att förhindra att information lagras utanför Microsoft 365.
- Policyer kan användas för att styra tillgängliga applikationer i Teamsklienten, eller huruvida det ska vara möjligt att spela in digitala möten, om detta strider mot verksamhetens beslutade regler för användning.
- Microsoft 365 kan integreras med Exchange och SharePoint lokalt installerad i en hybridlösning där kunddata lagras i lokal miljö. Se vidare i avsnitt 3.1.1 om Microsoft Molndesign, MSMD.
- Ytterligare en åtgärd som kan vidtas är att lagra information på annan plats än i Microsoft 365.

Beslut om tillgängliga tjänster kan exempelvis baseras på dokumentation om var data lagras och behandlas i Microsoft 365:

Referens: https://learn.microsoft.com/en-us/microsoft-365/enterprise/o365-data-locations?view=o365-worldwide

2.2.2 Villkorlig åtkomst

Funktioner i Azure Active Directory kan användas för att skapa policyer för villkorlig åtkomst. Dessa policyer[2] styr hur användare kan ansluta till tjänsten. Dessa regelverk kan även kombineras med enhetshanteringen i Microsoft Intune[3], som kan användas för att styra vilka enheter som får användas för att ansluta till tjänsten.

Några exempel på hur en organisation kan använda villkorlig åtkomst är:

- Att kräva att flerfaktorsautentisering (MFA) alltid används för konton med administratörsbehörigheter. Detta innebär att inloggning med ett konto som har administratörsbehörigheter alltid måste använda MFA. Vanligt förekommande är annars att konton utan administratörsbehörigheter inte behöver använda MFA vid varje enskild inloggning.
- Blockera åtkomst från klientdatorer som inte är uppdaterade. Detta innebär att anslutning till tjänsten inte kan göras från en klientdator som inte kan verifiera att den har installerat säkerhetsuppdateringar till en viss nivå.
- Tillåt enbart webbåtkomst från publika datorer. Detta innebär att anslutningar från lokalt installerade klientapplikationer blockeras om klientdatorn inte är medlem i organisationens domän.
- Spärra åtkomst om risk upptäcks, till exempel en ”omöjlig resa”. Detta innebär bland annat att en anslutning till tjänsten från en ny plats, dit det är fysiskt omöjligt att en användare kan ha flyttat sig under en viss tid, blockeras.

3 Informationsklassning och skyddsåtgärder

3.1 Administrativa åtgärder

3.1.1 Informationsklassning

Informationsklassning innebär att verksamheten på ett enhetligt sätt värderar organisationens information utifrån vilka konsekvenser ett otillräckligt skydd skulle kunna få. Utifrån en fastställd informationsklassningsmodell grupperas och kategoriseras informationen i olika klasser för vilka verksamheten vidtar olika skyddsåtgärder baserat på de risker som identifierats. Skyddsåtgärder kan exempelvis omfatta regler för hur information får delas eller skickas.

För mer information om informationsklassning hänvisar vi i första hand till SKR:s vägledning och verktyg för klassning på informationssäkerhet.se[4].

[2] https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview, 2023-12-15
[3] https://docs.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune, 2023-12-15.
[4] https://www.informationssakerhet.se/stod--vagledning/saker-hantering-av-information2/skls-verktyg-for-klassning/, 2023-12-15.

3.2 Tekniska åtgärder

De åtgärder som beskrivs här är hämtade ut Microsoft Molndesign för Microsoft 365. Se mer information i avsnitt 2.4.

3.2.1 Microsoft Information Protection

Microsoft Information Protection (MIP) ingår i Microsoft 365 och är ett stöd för att införa och upprätthålla ett klassificeringssystem. Tjänsten bygger på klassificering av information via etiketter, samt skydd och kryptering via Azure Rights Management. Den kan användas som bas för rättighetshantering som styr tillgång och åtkomst till information i Microsoft 365.

Exempel: Information som klassas som intern tillåts inte att delas externt, gäster kan inte bjudas in till den och e-post krypteras.

3.2.2 Microsoft DLP, Cloud App Security och Intune App Protection

Microsoft 365 innehåller funktioner som kan användas för att förhindra dataförlust och bevaka hur känslig information hanteras. Några exempel är Data Loss Prevention (DLP), Microsoft Cloud App Security och Intune App Protection.

Microsoft DLP kan exempelvis användas för att övervaka om det förekommer personnummer i ett dokument och uppmärksamma användaren på att det identifierats. Tjänsten kan också blockera information från att delas utanför organisationen. Verksamheten kan också definiera egna typer av känslig information, till exempel diarienummer eller dokument baserade på en specifik mall, som ska övervakas av funktionen.

Microsoft Cloud App Security kan anslutas till och övervaka andra molntjänster för att förhindra att information delas via dem. Tjänsten kan också användas för att uppmärksamma verksamheten på avvikelser och risker eller automatiskt vidta säkerhetsåtgärder enligt fastställda regler.

Intune App Protection är en del av klienthanteringsplattformen i Microsoft 365 och kan exempelvis användas för att förhindra att information kopieras från företagsapplikationer på mobila enheter.

4 Roller och rättigheter

4.1 Administrativa åtgärder

4.1.1 Interna processer och regler för behörighetsstyrning

I rekommenderade säkerhetsåtgärder ingår bland annat att ha en särskild process för styrning av administratörsrättigheter inom verksamheten och att följa principerna om minsta möjliga åtkomst. I Microsoft 365 finns funktioner som kan användas för att stödja en sådan process.

4.2 Tekniska åtgärder

4.2.1 Hantering av privilegierad åtkomst i Microsoft 365

Privilegierad åtkomst ger möjlighet till detaljerad åtkomstkontroll över administrativa uppgifter i Microsoft 365. Verksamheten kan sätta upp regler för vem som kan begära åtkomst, för vilka

åtgärder och hur länge behörigheten ska gälla. Administratörer kan sedan följa en process där de ansöker om åtkomst för att utföra en viss uppgift och en utsedd granskare behöver godkänna ansökan innan behörighet ges. När ändringen är genomförd tas behörighetstilldelningen bort igen. Hela processen loggas. Det finns också inbyggda rutiner för att periodiskt granska det uppsatta regelverket.

4.2.2 Customer Lockbox

Om det, exempelvis vid ett supportärende, skulle behövas tillgång till kunddata kan Customer Lockbox användas för att organisationen ska ha möjlighet att granska en begäran från Microsoft om tillgång till kunddata (det vill säga organisationens data). Processen är tänkt att användas i situationer där en Microsoft-tekniker behöver åtkomst till kunddata för att kunna lösa en supportförfrågan.

Customer Lockbox kan användas som ett steg där en bedömning behöver göras av huruvida information som kan komma att delas vid en supportförfrågan är känslig och om informationen i så fall kan delas eller inte.

Förfrågningar via Customer Lockbox sparas i en granskningslogg. Det ger möjlighet att spåra tillfällen när denna typ av begäran har gjorts, om de accepterats eller nekats samt vilka åtgärder som sedan utförts. Genom sökverktyget för granskningslogg i Security & Compliance Center kan dessa loggar vid behov granskas.

5 Standarder och regelefterlevnad

5.1 Administrativa och tekniska åtgärder

För organisationer som använder standarder i sitt informationssäkerhetsarbete finns det funktioner i Microsoft 365 som kan vara till stöd. Ett exempel är Compliance Manager, en komponent i MSMD som översätter regelkrav till åtgärder i form av konfiguration av tjänsten.

5.1.1 Compliance Manager

I Compliance Manager finns det löpande uppdaterade bedömningsmallar för bland annat ISO 27001, ISO 27018 och GDPR[5]. Verktyget ger förslag på förbättringsåtgärder med detaljerade steg-för-steg-vägledningar och ur flera olika perspektiv. Verksamheten kan se förslagen med utgångspunkt från komponenterna i Microsoft 365 eller i de standarder som ligger till grund för bedömningen. Det finns även arbetsflödesfunktioner för att bland annat tilldela uppgifter till den som ska utföra åtgärden, registrera ändringar eller dokumentera underlag av genomförda ändringar. Som en summering av de åtgärder som utförts finns riskbaserade efterlevnadspoäng som kan användas för att prioritera och mäta förbättringsarbetet. Det ger ett kvantifierat mått på aktuell status för organisationens efterlevnad.

[5] Vissa mallar kan erbjudas som tillval.

6 Referenser och mer information

Mer information om Microsoft Molndesign finns i avsnitt 3.1.1 i vägledningens huvuddokument.

knowit

Appendix D – Scenario baserat på ett införande av Microsoft Teams

Utgångpunkten för detta appendix är att stödja aktörer utifrån ett Teams-scenario genom att beskriva olika aspekter som behöver beaktas vid ett införande av Microsoft 365. Syftet är att scenariot ska utgöra ett stöd där exempel på olika delar som behöver hanteras i en risk- och sårbarhetsanalys och eventuell konsekvensbedömning beskrivs. I detta ingår juridiska, tekniska och administrativa åtgärder och hur dessa kan beaktas samlat och i relation till hela den funktionalitet som verksamheten vill nyttja i Microsoft 365. I scenariot identifieras det vi valt att benämna *kritiska noder*. Dessa noder är valda för att de sammantaget kommer beröra många av de utmaningar en aktör har att ta ställning till vid ett införande. Därvidlag är tanken att scenariot bland annat ska kunna:

- Hjälpa aktören att se helheten i den önskade implementeringen utan att tappa bort de kritiska noderna.
- Stödja aktören i själva analysen; var finns juridiska och andra utmaningar och vilka mitigerande åtgärder kan vidtas?
- Ge stöd för workshops, utredningsarbete och dokumentation.
- Utgöra underlag för diskussion och etablering av gemensam bild samt förståelse utifrån olika perspektiv och kompetenser i en kommun (offentlig sektor) – CIO, CSO, DPO etcetera.
- Vara ett sätt att tydliggöra för beslutsfattare vilka utmaningar som finns vid ett införande av hela eller delar av Microsoft 365 och vilka åtgärder som kan vidtas för att mitigera risker.

1. Inledning

I en risk- och sårbarhetsanalys är det viktigt att arbeta metodiskt och att få ihop såväl relevanta detaljer som helhetsbedömningen. Som hjälpmedel och metod kan aktören utgå från ett fiktivt eller reellt verksamhetsbehov som sedan omsätts i konkreta aktiviteter baserat på den tjänst som ska analyseras. Syftet är att tydliggöra ingående komponenter på ett sätt som gör det enklare att granska dem individuellt likväl som gemensamt.

Scenariots olika aktiviteter innehåller följande aspekter:

- Övergripande beskrivning inklusive teknik och arkitektur samt visualisering av den kritiska noden
- Juridik
- Administrativa och tekniska mitigerande åtgärder
- Referenser till Microsofts underlag

1.1. Ett fiktivt verksamhetsbehov för detta scenario

Scenariot utgår från att en tänkt verksamhet har behov av en integrerad plattform för digitalt samarbete och att de bland annat vill ha följande funktionalitet:

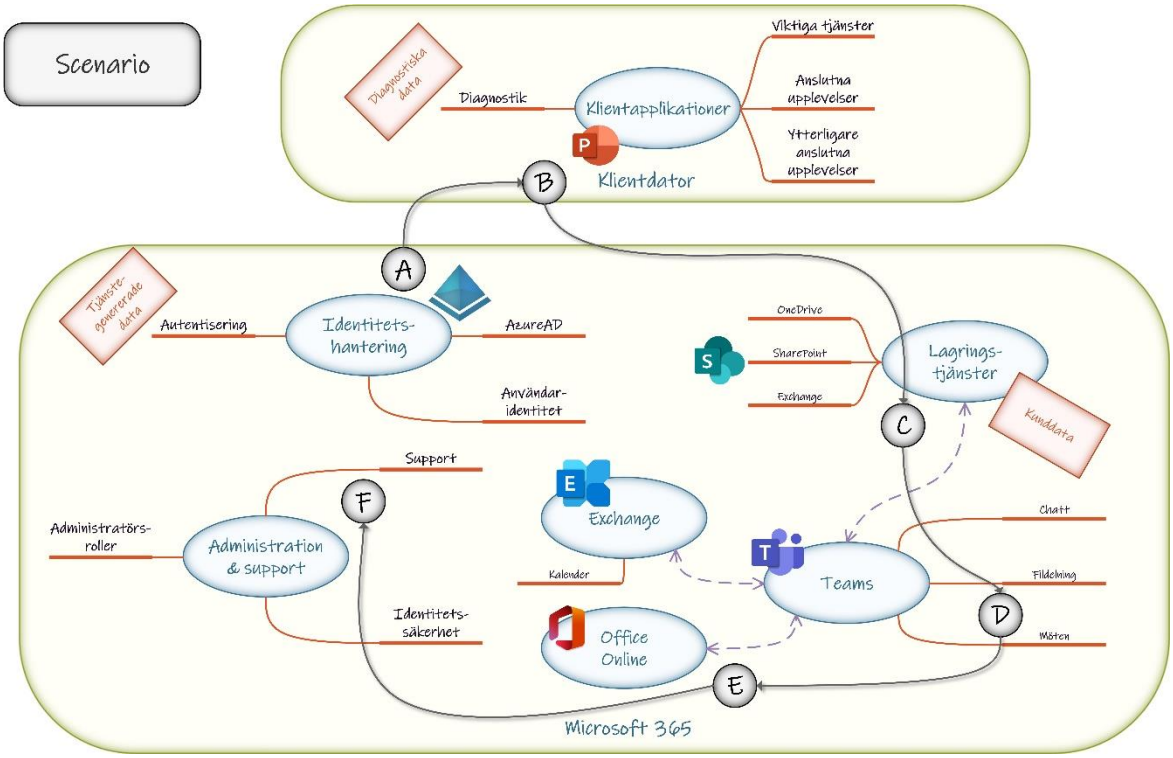
- Möten med ljud och bild.
- Snabbmeddelanden (chatt).
- Möjlighet att lagra och dela dokument.
- Kunna bjuda in externa gäster.
- Tillgänglighetsfunktioner, som exempelvis textning av presentationer och möten.
- Teknisk support från leverantören, vid behov.

2. Scenariobeskrivning

Utifrån ovan givna verksamhetsbehov har vi i Microsoft Teams identifierat följande användaraktiviteter som stöd för våra resonemang

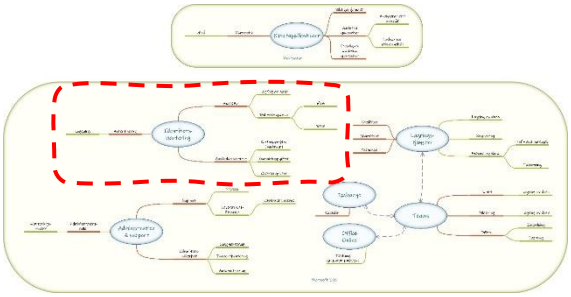
A. Logga in i Microsoft 365 (identitetshantering).
B. Starta PowerPoint och skapa en presentation (klientapplikationer).
C. Spara presentationen till SharePoint och samarbeta i Teams (datalagring och -behandling).
D. Genomför ett digitalt möte i Teams och spela in mötet.
E. Visa presentationen med textning i mötet (anslutna funktioner).
F. Hantera ett supportärende med Microsoft (administration och support).

Grundtanken bakom den här uppdelningen är att nyttja att Microsoft 365 i hög utsträckning använder en modulär arkitektur där samma komponenter används för att leverera flera olika tjänster. Till exempel används Azure Active Directory för all identitetshantering. Likaså hanteras majoriteteten av all dokumentlagring i SharePoint och OneDrive. Andra funktioner, såsom Microsoft 365-klientapplikationer är – även om de är separata program – byggda på ett enhetligt sätt och går att administrera gemensamt. Att studera några få, väl valda exempel, ger sammantaget en bra bild av helheten i plattformen.



A. Logga in i Microsoft 365

Denna aktivitet sker varje gång en användare loggar in i Microsoft 365, exempelvis från en webbläsare eller genom att starta applikationen.



Användaren anger användarnamn, lösenord och bekräftar eventuell tvåfaktorsutmaning.

Övergripande

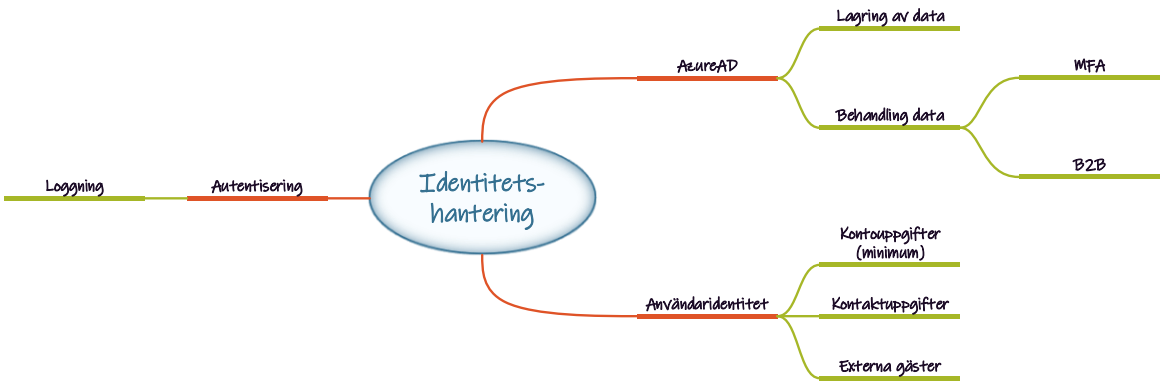
All identitetshantering i Microsoft 365 sker i den gemensamma tjänsten Azure Active Directory (Azure AD). Här skapas användaridentiteter och grupper som kan användas av alla ingående och anslutna tjänster. Även externa gäster som exempelvis bjuds in till en grupp i Microsoft Teams kommer att registreras i Azure AD.

Azure AD kan också användas som autentiseringskälla för tredjepartsystem för inloggning av organisationens medarbetare till andra molntjänster.

- **Vad gör det här till en kritisk nod?**
  Identitetshanteringen är en förutsättning för att över huvud taget kunna använda någon del av tjänsten, även för administration. Här hanteras också många känsliga uppgifter.
- **Hanteras personuppgifter i noden?**
  Ja, i princip all data som hanteras i noden är eller kan innehålla personuppgifter.
- **Valmöjligheter och skyddsåtgärder**
  Användning av identitetshantering är i sig inte valbart. Det finns valmöjligheter gällande vilka uppgifter som används för autentisering samt vilken övrig information om användare som lagras i tjänsten. Det går också att styra flera specifika funktioner, exempelvis hanteringen av externa gäster (B2B) samt hur organisationen använder multifaktorautentisering (MFA).

Teknik och arkitektur

Låt oss nu gå lite djupare in i tekniken bakom identitetshanteringen i Microsoft 365, den data som behandlas i tjänsten samt vilka möjligheter vi har att påverka detta.



Azure Active Directory (Azure AD)
Denna plattformsgemensamma och globala tjänst hanterar all autentisering i Microsoft 365 och Microsoft Azure. Här finns bland annat alla användare registrerade samt externa gäster som bjudits in till organisationen.

För europeiska kunder lagras identitetsdata i Azure AD generellt i datacenter inom EU. Vissa funktioner kan dock, helt eller delvis, tillhandahållas via amerikanska datacenter.

- **Multifaktorautentisering (MFA)**
  Som komplement till användarnamn och lösenord kan en extra autentiseringsmetod vid inloggning användas. Detta kallas multifaktorautentisering (MFA) och de metoder som erbjuds i Azure AD är:
  - Verifiering via mobilapplikationen Microsoft Authenticator. Detta levereras inom EU för de verifieringar som initieras från datacenter inom EU.
  - Engångskod via SMS. Detta levereras via globala tjänsteleverantörer.
  - Verifiering via telefonsamtal. Detta levereras via amerikanska datacenter.

Ovan nämnda metoder kan också användas för verifiering om organisationen tillåter att användare själva återställer sina lösenord genom så kallad ”Self-service Password Reset” eller SSPR.

*“**Microsoft Azure AD Multi-Factor Authentication***
For cloud-based Azure AD Multi-Factor Authentication, authentication is complete[d] in the closest datacenter to the user. Datacenters for Azure AD Multi-Factor Authentication exist in North America, Europe, and Asia Pacific.

- *Multi-factor authentication using phone calls originate from US datacenters and are routed by global providers.*
- *Multi-factor authentication using SMS is routed by global providers.*
- *Multi-factor authentication requests using the Microsoft Authenticator app push notifications that originate from EU datacenters are processed in EU datacenters.*
  - *Device vendor-specific services, such as Apple Push Notifications, may be outside Europe.*
- *Multi-factor authentication requests using OATH codes that originate from EU datacenters are validated in the EU.*

For more information about what user information is collected by Azure Multi-Factor Authentication Server (MFA Server) and cloud-based Azure AD MFA, see Azure Multi-Factor Authentication user data collection.”

Referens: Identity data storage for European customers - Azure AD | Microsoft Docs

- **Externa gäster (Business-to-business, B2B)**
  Inbjudningar till externa gäster skickas via amerikanska datacenter. Här lagras också e-postadresser för mottagare som väljer att frånsäga sig inbjudningar.

> ***"Microsoft Azure Active Directory B2B (Azure AD B2B)***
> *Azure AD B2B stores invitations with redeem link and redirect URL information in US datacenters. In addition, email address of users that unsubscribe from receiving B2B invitations are also stored in U.S. datacenters."*
>
> Referens: Identity data storage for European customers - Azure AD | Microsoft Docs

- **Användaridentiteter**
  För att kunna ge organisationens medarbetare och gäster tillgång till Microsoft 365 krävs användarkonton upplagda i Azure AD. Dessa kan skapas direkt i molntjänsten eller via synkronisering med verksamhetens interna Active Directory-katalog i en så kallad hybridlösning. Det går också att välja en kombination av de båda lösningarna. Oavsett vilket finns det en mängd olika attribut för varje användarkonto, några obligatoriska och andra valfria.

- **Kontouppgifter (minimum för att kunna logga in)**
  De uppgifter som krävs för att skapa ett användarkonto är:
  - Användarnamn, vanligtvis samma som användarens e-postadress.
  - Visningsnamn, ofta *"förnamn efternamn".*

- **Kontaktuppgifter**
  Det finns ytterligare attribut som kan lagras för respektive användarkonto. Denna information kan exempelvis visas i systemets adressbok eller användas för att dela upp användare i grupper baserat på avdelning, ort eller liknande. Några exempel på attribut är:
  - Förnamn och efternamn.
  - Användarens chef.
  - Anställningsnummer.
  - Adress.
  - Telefonnummer.
  - Ålderskategori
  - Medgivande.

- **Externa gäster (B2B)**
  Konton för externa gäster i Azure AD har samma egenskaper som vanliga användarkonton med samma attribut för konto- respektive kontaktuppgifter.

Loggning i Azure AD
Autentisering och annan aktivitet i Azure AD loggas i plattformen och sparas i 30 dagar. Syftet är att organisationer som använder exempelvis Microsoft 365 ska kunna övervaka säkerheten och följa upp eventuella avvikande händelser. Informationen är tillgänglig för administratörer och innehåller bland annat information om användarnamn, applikation, klient, IP-adress, tidpunkt etcetera.

Juridik
Eftersom personuppgiftsbehandlingar sker i denna aktivitet blir Dataskyddsförordningen (GDPR) tillämplig.

Informationssäkerhet enligt GDPR

1. Följ stegen i Appendix B (1) i avsnittet om informationssäkerhet.

Relevant för detta scenario:

- ✓ Inga känsliga personuppgifter behöver behandlas i denna aktivitet
- ✓ Vissa uppgifter kan vara offentliga/harmlösa
- ✓ Stark autentisering
- ✓ Säkerhetsloggar
- ✓ Kryptering
- ✓ Behörighetsstyrning för att reglera vem som får lov att bjuda in gäster och från vilka domäner.

Omsorgsplikten enligt GDPR

2. Följ stegen i Appendix B (2) i avsnittet om omsorgsplikten

Relevant information om omsorgsplikten för detta scenario:

- ✓ Inga känsliga personuppgifter behöver behandlas.
- ✓ De personuppgifter som krävs för att skapa konto är harmlösa uppgifter som kan vara offentliga
- ✓ Behandlingen sker huvudsakligen inom EU med undantag som är möjliga att välja bort

Tredjelandsöverföringar

3. Följ stegen i Appendix (B) i avsnittet om tredjelandsöverföringar om ni i föregående avsnittet gör bedömningar att tredjelandsöverföringar kommer att ske
- ✓ Uppgifter om e-postadress kan överföras till USA om ni väljer telefonsamtal eller SMS för MFA.

Offentlighet och sekretess

4. Följ stegen i Appendix B (4) gällande OSL

Administrativa och tekniska mitigerande åtgärder
Identitetshanteringen i Microsoft 365 är en obligatorisk tjänst och en förutsättning för att använda plattformen. Utifrån identifierade risker eller andra aspekter finns det dock valmöjligheter samt tekniska och administrativa skyddsåtgärder som en organisation kan vidta. Vad som behövs är individuellt för varje verksamhet men här följer några generella exempel:

- **Tillåtna metoder för multifaktorsautentisering (MFA).** För att minska risken att information behandlas i amerikanska datacenter i samband med MFA kan organisationen stänga av

telefonsamtal och SMS som valbara alternativ för MFA.

- **Policy för vilka attribut organisationen lagrar för användarkonton** i Azure AD samt hur organisationen exempelvis hanterar medarbetare med skyddad identitet.

- **Regler för hur organisationen hanterar externa gäster**. Det går exempelvis att styra vem som får lov att bjuda in gäster och från vilka domäner. Det går också att inkludera en länk till organisationens integritetspolicy i inbjudan som skickas.

  Microsoft 365 erbjuder också möjlighet att via Azure Information Protection mer i detalj styra tillåten delning av information beroende på hur den är klassad. Mer information om detta presenteras i bilaga C.

- **Hantering av säkerhetsloggar**. Information om exempelvis misslyckade inloggningsförsök är viktig information i en organisations säkerhetsarbete. Det bör finnas fastställda rutiner för hur dessa loggar granskas. Detta är exempelvis ett av kraven i ”Föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter” (MSBFS 2020:7, §16–17).

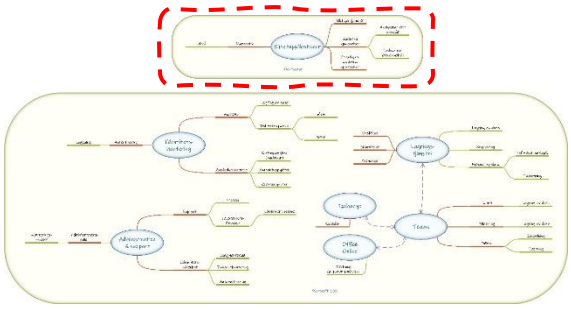
Länkar till Microsofts underlag

Nedan länkar till Microsofts dokumentation kan ge fördjupat underlag för relevanta delar i denna kritiska nod.

- What is Azure Active Directory?
- Identity data storage for European customers - Azure AD
- Azure AD MFA user data collection - Azure Active Directory
- Default user permissions - Azure Active Directory
- Audit logs in Azure Active Directory

B. Starta PowerPoint och skapa en presentation

Klientapplikationerna i Microsoft 365 genererar diagnostiska data när de används. Här använder vi PowerPoint som exempel men samma resonemang gäller för Word, Excel etcetera.



Övergripande

Ett vanligt sätt att använda tjänsterna i Microsoft 365 är via ”Microsoft 365-applikationer för företag” eller Office 365 som de ibland kallas. I paketet ingår Outlook, Word, Excel, PowerPoint, Teams och OneDrive.

- **Vad gör det här till en kritisk nod?**
  Klientapplikationerna genererar diagnostiska data som skickas till Microsoft för behandling. Läs mer om Microsofts definition av diagnostiska data i avsnitt 3.1.2.
- **Hanteras personuppgifter i noden?**
  Ja, pseudonymiserade personuppgifter.
- **Valmöjligheter och skyddsåtgärder**
  Organisationer kan välja vilken nivå av diagnostiska data som skickas samt om detta ska styras centralt eller individuellt.

Teknik och arkitektur

Denna aktivitet analyserar diagnostikinsamlingen i Microsoft 365 klientapplikationer. I en efterföljande aktivitet kommer vi närmare beskriva det som kallas anslutna upplevelser.

Microsoft 365 diagnostikdata

Så här skriver Microsoft om diagnostikdata[1] i Office[2] (vilket för detta vidkommande är detsamma som Microsoft 365):

”Du förväntar dig att Office ska vara säkert och fungera korrekt. För att kunna motsvara förväntningarna samlar vi in diagnostikdata när du använder Office och OneDrive. Detta hjälper oss att identifiera och åtgärda problem, identifiera och minimera hot och ge dig en bättre

[1] Ej att förväxla med Microsoft datakategorier, som beskrivs i avsnitt 3.1.2 i Vägledningen.
[2] https://support.microsoft.com/sv-se/office/diagnostikdata-i-office-f409137d-15d3-4803-a8ae-d26fcbfc91dd 2023-12-18

upplevelse. Dessa data omfattar inte ditt namn eller din e-postadress, innehållet i dina filer eller information om appar som inte är relaterade till Office eller OneDrive."

Diagnostikdata kan innehålla pseudonymiserade personuppgifter.

> ***"Note:** Diagnostic data may contain "personal data" as defined by Article 4 of the European GDPR, but it does not contain your name, your email address, or any content from your files. All diagnostic data Microsoft collects during the use of Office applications and services is pseudonymized, as defined in ISO/IEC 19944:2017, section 8.3.3. "*
>
> Referens: Diagnostic data in Office (microsoft.com)

Viktiga tjänster
Utöver diagnostikdata och oavsett inställningar kommer klientapplikationerna alltid att behöva ansluta till det Microsoft kallar viktiga tjänster ("essential services") i Microsoft 365. Detta krävs bland annat för att installera och uppdatera programvara samt för att verifiera att användaren är licensierad.

Juridiken
Eftersom personuppgiftsbehandlingar sker i denna aktivitet blir GDPR tillämplig.

Informationssäkerhet enligt GDPR

1. Följ stegen i Appendix B (1) i avsnittet om informationssäkerhet.

Relevant för detta scenario:

- ✓ Inga känsliga personuppgifter behöver behandlas i denna aktivitet.
- ✓ Personuppgifter pseudonymiseras.
- ✓ Kryptering.

Omsorgsplikten enligt GDPR

2. Följ stegen i Appendix B (2) i avsnittet om omsorgsplikten

Relevant information om omsorgsplikten för detta scenario.

- ✓ Inga känsliga personuppgifter behöver behandlas.
- ✓ Personuppgifter pseudonymiseras, men kompletterande uppgifter finns hos Microsoft.
- ✓ Möjlighet för en användare att skicka enbart obligatoriska diagnostiskdata.
- ✓ Behandling i datacenter inom EU, men undantag kan förekomma.

Tredjelandsöverföringar

3. Följ stegen i Appendix B (2) i avsnittet om tredjelandsöverföringar om ni bedömer att tredjelandsöverföringar sker.

- ✓ Möjlighet att minska uppgifter som behandlas.
- ✓ Personuppgifter pseudonymiseras, men kompletterande uppgifter finns hos Microsoft.

Offentlighet och sekretess

4. Följ stegen i Appendix B (4) gällande OSL.

Administrativa och tekniska mitigerande åtgärder

Om organisationen väljer att inte göra några anpassningar kan en användare av Microsoft 365 klientapplikationer själv välja att skicka enbart obligatoriska diagnostiskdata eller att även inkludera valfria diagnostikdata

Vill organisationen styra inställningen centralt kan en administratör skapa en policy för alla eller vissa gruppvis utvalda användare. En sådan policy bestämmer om klientapplikationerna ska skicka obligatoriska diagnostiskdata, valfria diagnostikdata eller inga diagnostikdata.

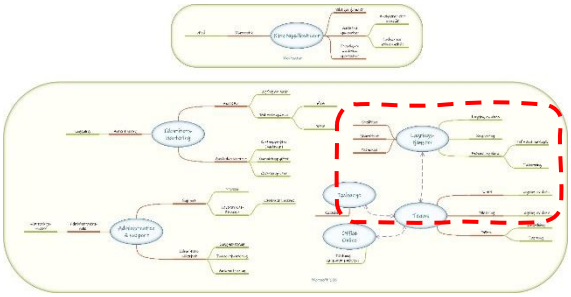
Länkar till Microsofts underlag

Här finns länkar till Microsofts dokumentation för att ge fördjupat underlag för relevanta delar i denna kritiska nod.

- Diagnostikdata i Office (microsoft.com)
- Required diagnostic data for Office - Deploy Office | Microsoft Docs
- Optional diagnostic data for Office - Deploy Office | Microsoft Docs
- Essential services for Office - Deploy Office | Microsoft Docs
- Overview of privacy controls for Microsoft 365 Apps for enterprise - Deploy Office | Microsoft Docs
- Use policy settings to manage privacy controls for Microsoft 365 Apps for enterprise - Deploy Office | Microsoft Docs

C. Spara presentationen till SharePoint och samarbeta i Teams

Kunddata som sparas i Microsoft 365 lagras oftast i SharePoint eller OneDrive. I detta scenario tittar vi främst på lagringstjänsterna i plattformen, där även Microsoft Exchange ingår.



Övergripande

SharePoint och OneDrive är två tjänster i en datalagringplattform som är gemensam för många funktioner i Microsoft 365. Här sparas dokument och filer som skapas eller laddas upp via exempelvis Word, Excel, PowerPoint och Teams. Den lagrade informationen, kunddata, behandlas också av olika funktioner i plattformen, som exempelvis indexering för sökning. Det är också lagringstjänsterna som möjliggör funktioner för delning och samarbete i Microsoft 365.

- **Vad gör det här till en kritisk nod?**
  Den information som lagras i SharePoint, OneDrive och Exchange är av kategorin kunddata[3] vilket inkluderar all data som tillhandahålls Microsoft av kunden, det vill säga av användarna till tjänsten.
- **Hanteras personuppgifter i noden?**
  Ja, om den information som lagras här innehåller personuppgifter.
- **Valmöjligheter och skyddsåtgärder**
  Organisationer behöver själva identifiera och klassificera den egna information som lagras i Microsoft 365 samt fastställa och införa relevanta skyddsåtgärder.

Teknik och arkitektur

Microsoft 365 är en modulär plattform där en uppsättning basfunktioner används av flera olika tjänster. Datalagringen i SharePoint, OneDrive och Exchange är ett tydligt exempel på detta.

SharePoint

Detta är en av de viktigaste och centrala tjänsterna i Microsoft 365. SharePoint kan användas som en komplett samarbetsplattform där organisationer kan skapa intranätfunktioner med innehållshantering och publiceringsfunktioner. Webbplatser baserade på SharePoint kan bland

[3] Se definition av Microsoft datatyper i avsnitt 3.1.2 i Vägledningen.

annat rymma sidor, listor, formulär och dokument. Här finns också funktioner för behörighetsstyrning, godkännandeflöden och versionshantering.

I kombination med klient- och webbapplikationerna för Microsoft 365 kan användare skapa, dela och samarbeta kring dokument och filer lagrade i SharePoint. Tjänsten används också som ”motor” för fildelningsfunktioner och webbplatser i Microsoft Teams. Användare kan söka efter innehåll i SharePoint och organisationer kan lägga till metadata och attribut för att strukturera informationen.

OneDrive
OneDrive är byggt på samma tekniska plattform som SharePoint men mer anpassat för enskilda användare och samarbete mellan enskilda användare (en till en). En lagringsyta för varje användare ingår i de flesta licensformer för Microsoft 365 och tjänsten kan också nyttjas för att automatiskt lagra filer i molntjänsten som sparas ”lokalt” på klientdatorer.

Även OneDrive används av Microsoft Teams för att dela dokument och filer mellan användare samt för att lagra inspelningar av Teams-möten.

Exchange
Microsoft Exchange används primärt för att lagra och hantera e-post. Tjänsten används dock också av Microsoft Teams för direktmeddelanden och kalenderinformation.

Lagring av data
Lagring av kunddata sker enligt avtalet för Microsoft 365 samt tillhörande dataskyddstillägg för europeiska kunder i datacenter inom EU.

Behandling och överföring av data
Behandling av kunddata sker oftast inom EU, men enligt Microsofts dokumentation kan det finnas undantag.

> ***“Where EU data is computed***
> *When you initiate the use of any of the above services, the computations needed to provide the service for your data stored in one of our regional European datacenters (or in your country) will take place within that same geographic boundary unless a temporary data transfer is needed to perform the computation in a Microsoft datacenter located further away.”*
>
> Referens: Data locations for the European Union - Microsoft 365 Enterprise | Microsoft Docs

Möjligheten för Microsoft att överföra data utanför EU i syfte att tillhandahålla överenskomna tjänster finns också beskrivna i avtalen för Microsoft 365.

Kryptering av data
Kryptering av kunddata, både i vila och vid överföring, finns inbyggd i Microsoft 365. Mer information om kryptering finns i bilaga 3.

Juridiken
Eftersom personuppgiftsbehandlingar sker i denna aktivitet blir GDPR tillämplig.

Informationssäkerhet enligt GDPR

1. Följ stegen i Appendix B (1) i avsnittet om informationssäkerhet.

Relevant för denna aktivitet:

- ✓ Känsliga personuppgifter kan behandlas i detta scenario.
- ✓ Säkerhetsloggar.
- ✓ Kryptering.
- ✓ Behörighetsstyrning genom att reglera vem som får lov att bjuda in gäster och från vilka domäner.
- ✓ Publicering av valbara klassificeringsetiketter som skyddar känslig information från obehöriga

Omsorgsplikten enligt GDPR

1. Följ stegen i Appendix B (2) i avsnittet om omsorgsplikten.

Relevant information om omsorgsplikten för detta scenario:

- ✓ Känsliga personuppgifter kan behandlas
- ✓ Behandling i datacenter inom EU, men undantag kan förekomma.
- ✓ Möjlighet att välja en tjänstegenererad krypteringsnyckel eller tillhandahålla egna kundnycklar genom "Double Key Encryption".

Tredjelandsöverföringar

2. Följ stegen i Appendix B (2) i avsnittet om tredjelandsöverföringar om ni bedömer att tredjelandsöverföringar sker.
- ✓ Möjlighet att välja en tjänstegenererad krypteringsnyckel eller tillhandahålla egna kundnycklar genom "Double Key Encryption".

Offentlighet och sekretess

3. Följ stegen i Appendix B (4) gällande OSL.

Administrativa och tekniska mitigerande åtgärder

Lagringsplattformen i Microsoft 365 är en förutsättning för att använda tjänster som exempelvis Microsoft Teams. Den går inte att välja bort. Den generella arkitekturen för lagring och behandling av data går heller inte att påverka förutom att välja region för data i vila, exempelvis ”EU”.

Det finns säkerhetsfunktioner med tillhörande skyddsåtgärder i Microsoft 365. Exempelvis kan valbara klassificeringsetiketter publiceras som kan bidra till att skydda känslig information från obehöriga. Det finns också funktioner för att automatiskt identifiera hantering av personuppgifter i plattformen och utföra åtgärder enligt uppsatta regler, som exempelvis att blockera delning av dokument. Vidare finns det möjlighet att reglera vem som får bjuda in externa gäster och vilken information som kan göras tillgänglig externt.

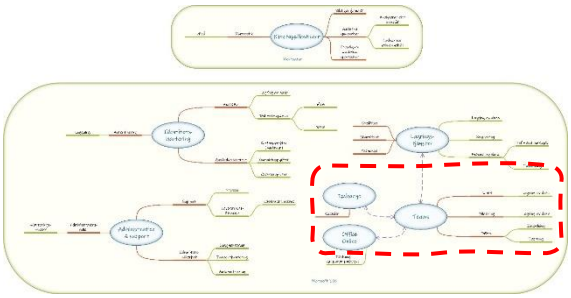
Mer information om informationssäkerhet och skyddsåtgärder finns i Appendix C.

Länkar till Microsofts underlag
Här finns länkar till Microsofts dokumentation för att ge fördjupat underlag för relevanta delar i denna kritiska nod.

- Microsoft 365 Multi-Geo - Microsoft 365 Enterprise | Microsoft Learn
- Microsoft Teams IT architecture and voice solutions posters - Microsoft Teams | Microsoft Docs
- Commercial Licensing Terms (microsoft.com)
- Licensing Documents (microsoft.com)
- Kryptering i Microsoft 365 - Microsoft 365 Compliance | Microsoft Docs
- Krypteringstjänst med kundnyckel - Microsoft 365 Compliance | Microsoft Docs

D. Genomför ett digitalt möte i Teams och spela in mötet.

Den här aktiviteten beskriver att spela in digitala möten för att på så sätt dokumentera det som sägs eller visas.



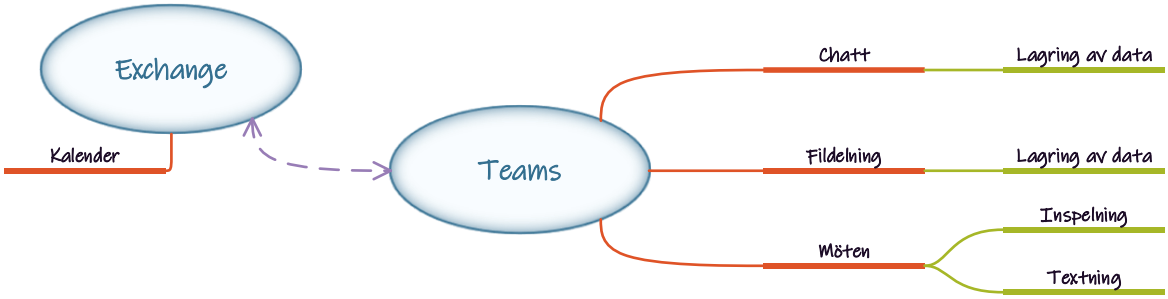
Övergripande

Inspelade möten lagras i SharePoint eller OneDrive och hanteras som andra delade filer. Dock kan det vara viktigt att granska hur organisationen behandlar denna typ av data eftersom det är en upptagning av ljud och bild som kan ha känsligt innehåll.

- **Vad gör det här till en kritisk nod?**
  Den information som behandlas och lagras i Microsoft Teams inkluderar all data[4] som tillhandahålls Microsoft av kunden vid användning av tjänsten, inklusive det som sägs på ett digitalt möte eller skrivs i en chatt.
- **Hanteras personuppgifter i noden?**
  Ja, om den information som lagras här innehåller personuppgifter.
- **Valmöjligheter och skyddsåtgärder**
  Verksamheten behöver själv identifiera och klassificera sin information som lagras i Microsoft 365 samt fastställa och införa relevanta skyddsåtgärder.

Teknik och arkitektur

En av huvudfunktionerna i Microsoft Teams är möjligheten att genomföra digitala möten med ljud, bild, chatt och fildelning. Inspelade möten lagras på och delas via SharePoint eller OneDrive.



Möten, inspelning och textning

Om funktionen att spela in möten tillåts (i konfiguration av tjänsten), kan organisatören av ett digitalt möte i Microsoft Teams spela in detta, inklusive ljud och bild. Tillsammans med inspelningen skapas en fil för undertexter.

Efter avslutat möte kommer inspelningen att vara tillgänglig via OneDrive eller SharePoint för alla som var inbjudna, oavsett om de var med eller inte. Inspelning, textning och delade filer kommer att visas under mötessammanfattning i Microsoft Teams.

[4] Se definition av Microsoft datatyper i avsnitt 3.1.2. i Vägledningen.

Alla funktioner som nämns här är inte fullt utrullade i plattformen ännu, men bör finnas tillgängliga under 2021.

Kryptering av data
Möjlighet till kryptering mellan slutpunkter (”end-to-end encryption”) har nyligen introducerats av Microsoft. Detta kan enbart aktiveras för röstsamtal ett till ett mellan två klientdatorer och fungerar inte i gruppmöten eller liknande.

I övrigt följer kryptering av data i Microsoft Teams samma mönster som för övriga Microsoft 365-tjänster. Se föregående aktivitet för mer information om detta.

Juridiken
Eftersom personuppgiftsbehandlingar sker i denna aktivitet blir GDPR tillämplig.

Informationssäkerhet enligt GDPR

1. Följ stegen i Appendix B (1) i avsnittet om informationssäkerhet.

Relevant för detta scenario:

- ✓ Känsliga personuppgifter kan behandlas i detta scenario.
- ✓ Stark autentisering.
- ✓ Säkerhetsloggar.
- ✓ Kryptering.
- ✓ Behörighetsstyrning.

Omsorgsplikten enligt GDPR

2. Följ stegen i Appendix B (2) i avsnittet om omsorgsplikten.

Relevant information om omsorgsplikten för detta scenario.

- ✓ Möjlighet finns att välja bort inspelning och ha mötet endast i realtid.
- ✓ Känsliga personuppgifter kan behandlas.
- ✓ Behandling sker för kunder i EU i datacenter inom EU, men undantag kan förekomma.
- ✓ Möjligheten till kryptering mellan slutpunkter (”end-to-end encryption”) har nyligen introducerats av Microsoft men inspelning av mötet är då inte möjlig.

Tredjelandsöverföringar

3. Följ stegen i Appendix B (2) i avsnittet om tredjelandsöverföringar om ni bedömer att tredjelandsöverföringar sker.

- ✓ Möjligheten till kryptering mellan slutpunkter (”end-to-end encryption”) har nyligen introducerats av Microsoft men inspelning av mötet är då inte möjlig.

Offentlighet och sekretess

4. Följ stegen i Appendix B (4) gällande OSL.

Administrativa och tekniska mitigerande åtgärder

Det går exempelvis att reglera om det ska gå att spela in möten eller aktivera textning i Microsoft Teams. Detta kan göras per användargrupp.

Om verksamheten tillåter inspelning är det väsentligt att användarna förstår innebörden av och reglerna kring det samt att det finns tydliga riktlinjer för vilken information som får behandlas i mötet.

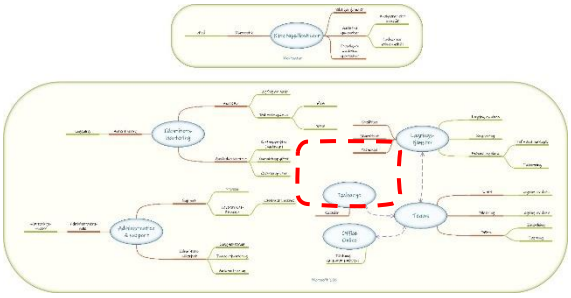
Länkar till Microsofts underlag

Här finns länkar till Microsofts dokumentation för att ge fördjupat underlag för relevanta delar i denna kritiska nod.

- Microsoft Teams IT architecture and voice solutions posters - Microsoft Teams | Microsoft Docs
- Meetings and conferencing in Microsoft Teams - Microsoft Teams | Microsoft Docs
- Manage meeting policies in Microsoft Teams - Microsoft Teams | Microsoft Docs
- Microsoft Teams Privacy - Microsoft Teams | Microsoft Docs

E. Visa presentationen med textning

Av tillgänglighetsskäl eller andra kan det vara önskvärt att använda exempelvis textning.



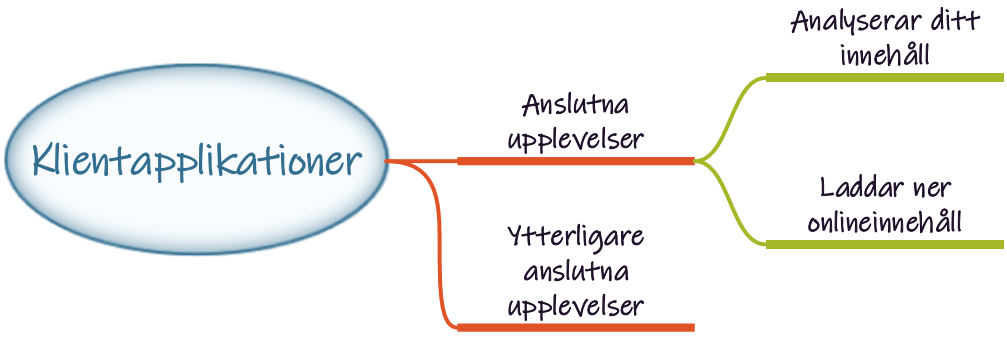
Övergripande

Anslutna upplevelser (Connected experiences), är samlingsnamnet på tilläggsfunktioner som ingår i Microsoft 365. Här finns bland annat textning, diktering och översättning som kan användas av klientapplikationer och andra tjänster i plattformen.

- **Vad gör det här till en kritisk nod?**
  Anslutna upplevelser kan behandla kunddata.
- **Hanteras personuppgifter i noden?**
  Ja, om den information som behandlas här innehåller personuppgifter.
- **Valmöjligheter och skyddsåtgärder**
  Verksamheter behöver själva identifiera och klassificera den egna information som lagras i Microsoft 365 samt fastställa och införa relevanta skyddsåtgärder. Det är också viktigt att användare förstår hur olika funktioner behandlar data.

Teknik och arkitektur

Anslutna funktioner delas in i olika kategorier beroende på hur de behandlar data.



Funktioner som analyserar ditt innehåll
Det här är funktioner som använder ditt innehåll för att ge designrekommendationer, redigeringsförslag, datainsikter och liknande funktioner. PowerPoint Designer, Dictate och Translator är några exempel på dessa typer av funktioner.

Dikteringsfunktionen (Dictate), som ett exempel, lagrar ingen data men det varierar från funktion till funktion. Verksamheten kan behöva undersöka specifikt hur respektive funktion behandlar och/eller lagrar organisationens data om de är aktuella för användning.

Funktioner som laddar ner onlineinnehåll
Med de här är funktionerna kan du söka efter och ladda ned onlineinnehåll som exempelvis mallar,

bilder, 3D-modeller, program-hjälp, videor och referensmaterial. Excels avancerade datatyper och Outlooks väderinformation är exempel på dessa typer av funktioner.

Valfria anslutna upplevelser
Hit räknas funktioner som tillhandahålls av tjänster utanför Microsoft 365, som exempelvis kartor från Bing[5], CV-assistenten från LinkedIn och väderinformation från MSN[6].

Juridiken
Eftersom personuppgiftsbehandlingar sker i denna aktivitet blir GDPR tillämplig.

Informationssäkerhet enligt GDPR

1. Följ stegen i Appendix B (1) i avsnittet om informationssäkerhet.

Relevant för detta scenario:

- ✓ Känsliga personuppgifter kan behandlas i denna aktivitet
- ✓ Stark autentisering
- ✓ Säkerhetsloggar
- ✓ Kryptering
- ✓ Behörighetsstyrning.

Omsorgsplikten enligt GDPR

2. Följ stegen i Appendix B (2) i avsnittet om omsorgsplikten.

Relevant information om omsorgsplikten för detta scenario:

- ✓ Möjlighet finns att välja bort funktioner och personuppgiftsbehandlingar som förekommer.
- ✓ Känsliga personuppgifter kan behandlas.
- ✓ Behandling sker för kunder i EU i datacenter inom EU, men undantag kan förekomma.
- ✓ Möjlighet finns att välja en tjänstegenererad krypteringsnyckel eller tillhandahålla egna kundnycklar, men Microsoft behöver också nycklar för att tjänsterna ska fungera.

Tredjelandsöverföringar

3. Följ stegen i Appendix B (2) i avsnittet om tredjelandsöverföringar om ni bedömer att tredjelandsöverföringar sker.

- ✓ Möjlighet att välja bort funktionaliteter och även tredjelandsöverföringar.

[5] Söktjänst från Microsoft.
[6] En internettjänst från Microsoft.

Offentlighet och sekretess

4. Följ stegen i Appendix B (4) gällande OSL.

Administrativa och tekniska mitigerande åtgärder

Om organisationen väljer att inte göra några anpassningar kan en användare av Microsoft 365 klientapplikationer själv välja vilka typer av anslutna upplevelser som ska vara tillgängliga.

Inställningar kan göras centralt genom att skapa en policy för alla eller gruppvis utvalda användare. En sådan policy bestämmer vilka typer av anslutna upplevelser som ska vara tillgängliga.

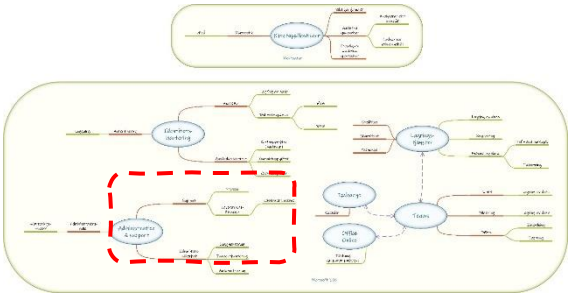
Länkar till Microsofts underlag

Här finns länkar till Microsofts dokumentation för att ge fördjupat underlag för relevanta delar i denna kritiska nod.

- Anslutna upplevelser i Office - Deploy Office | Microsoft Docs
- Översikt över valfria anslutna upplevelser i Office - Deploy Office | Microsoft Docs
- Nödvändiga tjänstdata för Office - Deploy Office | Microsoft Docs
- Teams Optional Connected Experiences - Microsoft Teams | Microsoft Docs
- Overview of privacy controls for Microsoft 365 Apps for enterprise - Deploy Office | Microsoft Docs
- Use policy settings to manage privacy controls for Microsoft 365 Apps for enterprise - Deploy Office | Microsoft Docs

F. Hantera supportärende med Microsoft

Om verksamheten stöter på problem med Microsoft 365 behöver organisationens administratörer ibland involvera Microsoft i felsökningsprocessen.



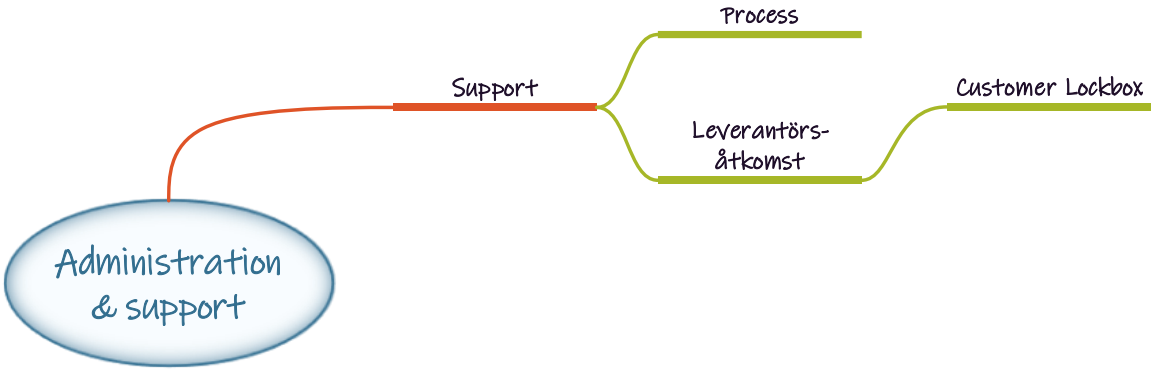
Övergripande

Supportprocessen för Microsoft 365 har ansvarsfördelning och kontrollfunktioner både för kunden och leverantören. Det är dock viktigt att förstå de olika aktiviteterna för att kunna identifiera om och när kunddata eller andra datakategorier behandlas.

- **Vad gör det här till en kritisk nod?**
  I supportprocessen kan kunddata eller andra datakategorier komma att delas med leverantören.
- **Hanteras personuppgifter i noden?**
  Ja, om den information som behandlas i tjänsten innehåller personuppgifter.
- **Valmöjligheter och skyddsåtgärder**
  Verksamheter behöver själva identifiera och klassificera den egna information som lagras i Microsoft 365 och vara uppmärksam på vilken data som behandlas i ett eventuellt supportärende.

Teknik och arkitektur

Här följer en inledande beskrivning av den tekniska arkitekturen för supportprocessen.



Supportbegäran

En användare med relevant behörighet kan skapa och hantera en supportbegäran inne i administratörsportalen för Microsoft 365. Användaren anger då sina kontaktuppgifter samt önskemål om hur kommunikation i ärendet ska ske.

Process
Felsökning i Microsoft 365 är oftast automatiserad och kräver då inte tillgång till kunddata. Skulle ändå Microsoft personal behöva tillgång till kunddata finns en process för att få åtkomst genom en intern så kallad Lockbox-process.

Customer Lockbox
Customer Lockbox är en funktion som lägger till ett administrativt steg i supportprocessen där kunden får möjlighet att granska en begäran från Microsoft om tillgång till kunddata. Processen används i situationer där personal från Microsoft behöver åtkomst till kunddata för att kunna lösa en supportförfrågan.

Juridiken
Eftersom personuppgiftsbehandlingar sker i denna aktivitet blir GDPR tillämplig.

Informationssäkerhet enligt GDPR

1. Följ stegen i Appendix B (1) i avsnittet om informationssäkerhet.

Relevant för denna aktivitet:

- ✓ Möjlighet till behörighetsstyrning. Det finns en process för att personal från Microsoft ska få åtkomst till kunddata genom en intern så kallad Lockbox-process.
- ✓ Felsökning i Microsoft 365 är oftast automatiserad och kräver då inte tillgång till kunddata.

Omsorgsplikten enligt GDPR

2. Följ stegen i Appendix B (2) i avsnittet om omsorgsplikten

Relevant information om omsorgsplikten för denna aktivitet:

- ✓ Felsökning i Microsoft 365 är oftast automatiserad och kräver då inte tillgång till kunddata.
- ✓ Behandling sker för kunder inom EU oftast i datacenter inom EU, men undantag kan förekomma.
- ✓ Användning av tilläggsfunktionen Customer Lockbox minskar risken för en överföring till tredjeland.

Tredjelandsöverföringar

3. Följ stegen i Appendix B (2) i avsnittet om tredjelandsöverföringar om ni bedömer att tredjelandsöverföringar sker.

- ✓ Användning av tilläggsfunktionen Customer Lockbox minskar risken för en överföring till tredjeland.
- ✓ Organisatoriska åtgärder i form av snäv behörighetstilldelning.

Offentlighet och sekretess

4. Följ stegen i Appendix B (4) gällande OSL.

Administrativa och tekniska mitigerande åtgärder

Några exempel på mitigerande åtgärder för hantering av supportärenden är följande:

- ✓ Policy och process för vem som får skapa en supportbegäran.
- ✓ Aktivering av Customer Lockbox med tillhörande rutin och granskning av vilken data som behandlas i samband med supportärende.

Länkar till Microsofts underlag

Här finns länkar till Microsofts dokumentation för att ge fördjupat och mer komplett underlag för relevanta delar i denna kritiska nod.

- ✓ Få support | Microsoft Docs
- ✓ Customer Lockbox-begäranden - Microsoft 365 Compliance | Microsoft Docs
- ✓ Licensing Documents – DPA (microsoft.com)

knowit

Bilagor

Bilaga 1	Detaljerad beskrivning och mall för risk- och sårbarhetsanalys av ett införande av Microsoft 365
Bilaga 2	Om CLOUD Act, FISA, EO 12333 och EO 14086
Bilaga 3	Krypteringsmöjligheter
Bilaga 4	Referenser
Bilaga 5	Begrepp och förkortningslista

knowit

Bilaga 1. Detaljerad beskrivning och mall för risk- och sårbarhetsanalys av ett införande av Microsoft 365

Innehåll i denna bilaga:

1 Inledning

Här redovisas först den detaljerade beskrivningen av de ingående delarna i modellen för risk- och sårbarhetsanalys. Sedan presenteras mallen för dokumentation av risk- och sårbarhetsanalysen. Mallen utgår från modellen i MSB:s Metodstöd för informationssäkerhet[1] och omhändertar även de krav som ställs på dokumentation av riskanalys (riskbedömning) i MSB:s föreskrifter om informationssäkerhet för statliga myndigheter[2]. Den är därmed i linje med hur kommuner redan bör arbeta med riskanalyser och tillför de aspekter som behöver bedömas när Microsoft 365 specifikt står i fokus. Se även kapitel 3. Metod, och Appendix A – Modell för risk och sårbarhetsanalys av ett införande av Microsoft 365.

Genom mallen ska vägledningen och verktyget ge stöd för genomförandet av riskanalysen och underlag för dokumentation av den. Detta bidrar också till att beslutet om användning av Microsoft 365 kan bli genomtänkt och medvetet samt belyst ur alla kritiska aspekter avseende legalitet, nytta etc.

Innehållet i dokumentationen från risk- och sårbarhetsanalysen ska också kunna användas för intern och extern kommunikation av besluten kring användning av Microsoft 365.

[1] https://www.informationssakerhet.se/metodstodet/, 2023-12-15.
[2] Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter, MSBFS 2020:6, https://www.msb.se/siteassets/dokument/regler/forfattningar/msbfs-2020-6-foreskrifter-om-informationssakerhet-for-statliga-myndigheter.pdf, 2023-12-19.

2 Beskrivning av de ingående delarna i modellen

2.1 Översiktlig beskrivning

I modellen beskrivs och bedöms följande aspekter:

Första delen, Riskidentifiering och -värdering:

- Risker kan analyseras utifrån vilken informationstillgång de hör ihop med
- Identifierade risker bör ha unika identiteter (Risk-ID:n)
- Riskbeskrivningarna behöver vara utförliga
- Risker behöver kategoriseras
- Orsaker till respektive risk behöver beskrivas
- Konsekvenser av och sannolikheter för respektive risk behöver beskrivas och värderas i enlighet med verksamhetens fastställda nivåer
- En sammanfattande risknivå behöver sammanställas
- Riskägare behöver utses

Andra delen, Riskhantering och uppföljning:

- Risker behöver prioriteras
- Åtgärderna behöver beskrivas
- Bedömda nivåer avseende konsekvens och sannolikhet efter genomförd åtgärd behöver beskrivas
- En sammanfattande risknivå efter genomförda åtgärder behöver sammanställas
- Ansvarig för åtgärd behöver utses
- Planerat datum för genomförande behöver fastställas
- Klarrapportering

Ovanstående aspekter är också införda i mallens två delar, riskidentifiering och -värdering (bild A) respektive riskhantering och uppföljning (bild B), och utgör strukturen för dokumentation av analysen. Respektive verksamhet kan också införa ytterligare aspekter i den aktuella analysen.

2.2 Detaljerad beskrivning

2.2.1 Första delen: Riskidentifiering och -värdering

Risker kan analyseras utifrån vilken informationstillgång de hör ihop med
Informationskartläggningen kan användas som underlag att utgå från för att identifiera risker eller andra aspekter kopplade till respektive informationstillgång.

Identifierade risker bör ha unika Risk-ID:n
Syftet med unika ID:n på risker genom hela analysen är att säkert kunna hantera dem över tid genom en hel process av identifiering ända till kontroller och långsiktig uppföljning av vidtagna åtgärder.

Riskbeskrivningarna behöver vara utförliga
Identifierade risker behöver beskrivas utförligt både för att kunna särskiljas från andra, likartade risker, och för att kunna förstås även av parter som inte deltagit i analysen.

Risker behöver kategoriseras
Identifierade risker behöver kategoriseras, dels för att vara hanterbara som delmängder, dels för att särskilja dem från andra, likartade risker. Kategoriseringarna kan också underlätta kommunikationen med andra berörda vilken risk som avses. Exempel på kategorier av risker som kan användas är integritetsrisker, legala risker, ekonomiska risker, varumärkesrisker, risk för personskada och verksamhetsrisker.

Orsaker till respektive risk behöver beskrivas
För att möjliggöra mitigering av risker behöver orsaker till dem analyseras och beskrivas tydligt. Identifierade orsaker ligger i stor utsträckning också till grund för värderingar av sannolikhet och konsekvens för respektive risk.

Konsekvenser av respektive risk behöver beskrivas och värderas
För att rätt kunna värdera och utveckla möjliga åtgärder för att hantera respektive risk behöver konsekvenser av dem tydligt beskrivas. Konsekvenserna behöver också kvantifieras till ett värde enligt modellens skala för att bli möjliga att jämföra med andra.

Sannolikheter för respektive risk behöver beskrivas och värderas
För att rätt kunna värdera och utveckla möjliga åtgärder för att hantera respektive risk behöver sannolikheter för dem tydligt beskrivas. Sannolikheterna behöver också kvantifieras till ett värde enligt modellens skala för att bli möjliga att jämföra med andra.

En sammanfattande risknivå behöver sammanställas
För att kunna värdera och bedöma risker, inte minst i jämförelse med andra risker, behöver en sammanfattande risknivå framställas. Den beräknas i vår modell utifrån värdena för sannolikhet och konsekvens genom att addera dem[3].

Riskägare behöver utses
För att möjliggöra genomförande och uppföljning av beslutade åtgärder behöver en ansvarig för åtgärden utses. Vi rekommenderar att det ansvaret ges till en roll eller befattning.

2.3 Andra delen, Riskhantering och uppföljning

Risker behöver prioriteras
För att ange rätt ambition och möjliggöra en effektiv förvaltning behöver åtgärderna prioriteras. Alternativet att avstå från att åtgärda risken markeras i modellen genom att ange prioritet 0.

Åtgärderna behöver beskrivas
För att en åtgärd ska ge förväntad effekt behöver tydligt beskrivas både vad åtgärden består i och vad den bedöms ha för effekt.

Bedömda nivåer avseende konsekvens och sannolikhet efter genomförd åtgärd behöver beskrivas
För att värdera åtgärderna och motivera dem behöver de bedömda målnivåerna avseende konsekvens och sannolikhet beskrivas. Detta är också en viktig del för att ge spårbarhet till bedömningar och beslut, samt för att dokumentera dem och möjliggöra kommunikation kring dem.

[3] Samma beräkningssätt som används i MSB:s mall.

De behöver också kvantifieras enligt modellens skala på samma sätt som bedömning av konsekvensen innan åtgärd genomförts.

En sammanfattande risknivå efter genomförda åtgärder behöver sammanställas
För att kunna värdera och bedöma kvarstående risker, inte minst i jämförelse med andra risker och åtgärder, behöver en sammanfattande risknivå framställas. Den beräknas i vår modell utifrån värdena för sannolikhet och konsekvens genom att addera dem.

Ansvarig för åtgärd behöver utses
För att beslutade åtgärder ska kunna genomföras inom verksamheten behöver ansvarig för respektive åtgärd fastställas, på motsvarande sätt som för riskägare.

Planerat datum för genomförande behöver fastställas
För att komplettera ambitionsnivån för respektive åtgärder och möjliggöra uppföljning behöver planerat slutdatum för genomförande av åtgärder fastställas.

Klarrapportering
För att möjliggöra uppföljning av åtgärder på enskild och sammanfattad nivå innehåller mallen även utrymme för dokumentation av om åtgärden är genomförd och vilket datum detta skedde.

Observera att det ifyllda underlaget kan vara känsligt och behöver klassas avseende informationssäkerhet och hanteras utifrån klassningen.

3 Dokumentation av analysen i mallen

Mallen är både ett stöd för praktiskt genomförande av analysen och ett underlag för dokumentation. Dokumentationen fyller flera syften, varav spårbarhet till bedömningar av risker eller andra aspekter, och värderingar av planerade åtgärder med eventuella kvarstående risker är nödvändiga delar för införandebeslutet. Dokumentation med spårbarhet genom hela analysprocessen behövs också för uppföljning av planerade åtgärder och kommunikation med både interna och externa mottagare.

Bilderna nedan (A och B) visar ett exempel på mallens två delar efter genomförd analys. Uppgifterna är fiktiva.

Bild A. Mallens steg 1, Riskidentifiering och -värdering (fiktiva uppgifter).

Riskidentifiering och -värdering

Omfattning: Införande av Microsoft 365
Datum:
Deltagare:

						Konsekvens		Sannolikhet				
Tillgång ID	**Risk-ID**	**Riskbeskrivning**	**Riskkategori**	**Orsaksbeskrivning**	**Konsekvensbeskrivning**	**Värde K (1-4)**	**Konsekvensnivå**	**Värde S (1-4)**	**Sannolikhetsnivå**	**Risknivå**	**Kommentar**	**Riskägare**
T1	R1	Beskrivning 1	Integritetsrisk	Orsak 1	Konsekvensbeskrivning 1	4	Allvarlig	4	Mycket hög	7	Kommentar 1	Enhetschef
T1	R2	Beskrivning 2	Legal risk	Orsak 2	Konsekvensbeskrivning 2	1	Försumbar	2	Medelhög	2	Kommentar 2	Informationsägare
T1	R3	Beskrivning 3	Ekonomisk risk	Orsak 3	Konsekvensbeskrivning 3	2	Måttlig	3	Hög	4	Kommentar 3	Informationsägare
T2	R4	Beskrivning 4	Varumärkesrisk	Orsak 4	Konsekvensbeskrivning 4	2	Måttlig	4	Mycket hög	5	Kommentar 4	IT-chef
T2	R5	Beskrivning 5	Personskada	Orsak 5	Konsekvensbeskrivning 5	4	Allvarlig	1	Låg	4	Kommentar 5	Säkerhetschef
T2	R6	Beskrivning 5	Verksamhetsrisk	Orsak 6	Konsekvensbeskrivning 6	2	Måttlig	2	Medelhög	3	Kommentar 6	Personalchef
T3	R7	Beskrivning 6	Integritetsrisk	Orsak 7	Konsekvensbeskrivning 7	3	Betydande	4	Mycket hög	6	Kommentar 7	Ekonomichef
T4	R8	Beskrivning 7	Legal risk	Orsak 8	Konsekvensbeskrivning 8	1	Försumbar	3	Hög	3	Kommentar 8	Kvalitetschef
T4	R9	Beskrivning 8	Ekonomisk risk	Orsak 9	Konsekvensbeskrivning 9	4	Allvarlig	2	Medelhög	5	Kommentar 9	Enhetschef

Bild B. Mallens steg 2, Riskhantering och uppföljning (fiktiva uppgifter).

Riskhantering och uppföljning

Omfattning: Införande av Microsoft 365
Datum:
Deltagare:

			Mål för konsekvens		Mål för sannolikhet						
Prioritet (0-4)	**Åtgärdsbeskrivning**	**Åtgärdskategori**	**Målvärde konsekvens (1-4)**	**Målnivå konsekvens**	**Målvärde sannolikhet (1-4)**	**Målnivå sannolikhet**	**Målrisknivå**	**Åtgärdsansvarig**	**Planerat färdigdatum**	**Klarrapporterad**	**Klarrapporterad datum**
0											
1	Åtgärd 1	Administrativ	1	Försumbar	1	Låg	1	Informationsägare	2021-10-01		
2	Åtgärd 2	Administrativ	1	Försumbar	2	Medelhög	2	IT-chef	2021-10-30	Ja	2021-10-18
1	Åtgärd 3	Teknisk	1	Försumbar	3	Hög	3	Personalchef	2021-11-30		
4	Åtgärd 4	Teknisk	3	Betydande	1	Låg	3	Säkerhetschef	2021-11-01		
1	Åtgärd 5	Administrativ	1	Försumbar	1	Låg	1	Personalchef	2021-10-01	Ja	2021-10-18
4	Åtgärd 6	Administrativ	2	Måttlig	3	Hög	4	Enhetschef	2022-01-30		
2	Åtgärd 7	Teknisk	1	Försumbar	2	Medelhög	2	Enhetschef	2022-03-30		
3	Åtgärd 8	Administrativ	3	Betydande	2	Medelhög	4	Ekonomichef	2021-12-20		

Observera att det ifyllda underlaget kan vara känsligt och behöver klassas avseende informationssäkerhet och hanteras utifrån klassningen.

knowit

Bilaga 2. Om CLOUD Act, FISA, EO 12333 och EO 14086

Innehåll i denna bilaga:

Vi vill understryka att detta avsnitt inte gör anspråk på att vara en uttömmande beskrivning av aktuella lagstiftningar.

1 Inledning

Här beskrivs översiktligt tre omtalade rättsliga instrument som ger myndigheter i USA möjlighet att på olika sätt ta del av uppgifter som behandlas av till exempel molntjänstleverantörer: Cloud Act, sektion 702 i FISA och Executive Order 12333. Utöver information om vad respektive instrument gäller, finns det även information om de utlämnanden som skett enligt dessa regelverk, såsom statistik gällande frekvensen av begäran och utlämnanden med mera.

I den så kallade Schrems II-domen[4], som kom år 2020, konstaterade EU-domstolen att skyddet för personuppgifter i USA inte generellt kunde anses vara *väsentligen likvärdigt* med det skydd som garanterades inom EU/EES. Sedan dess har USA infört nya bindande skyddsåtgärder för att bemöta kritiken i domen. USA har uppdaterat sin underrättelse-och övervakningsreglering genom President Bidens Executive Order 14086 (EO 14086).[5] Den nya exekutiva ordern ställer bland annat krav på nödvändighet och proportionalitetsbedömning vid utövandet av övervaknings-verksamhet samt inrättandet av en oberoende och opartisk dataskyddsdomstol (Data Protection Review Court, DPRC). DPRC tar emot och hanterar klagomål från EU-medborgare gällande beslut som rör deras personuppgifter som samlats in för brottsbekämpande syften av amerikanska underrättelsetjänster.

Förändringarna ledde till att EU-kommission bedömde att USA har en nivå av skydd för personuppgifter som är likvärdigt den som finns inom EU/EES. Mot bakgrund av det fattade EU-kommissionen den 10 juli 2023 ett beslut om adekvat skyddsnivå för organisationer i USA som är

[4] Dom av den 16 juli 2020 i mål C-311/18 Data Protection Commissioner mot Facebook Ireland Ltd och Maximilian Schrems.
[5] Executive Order (E.O.")14086 of October 7, 2022, on Enhancing Safeguards for United States Signals Intelligence Activities".

anslutna till EU-US Data Privacy Framework (DPF). I skälen[6] till beslutet har EU-kommissionen också redogjort för relevant lagstiftning i USA samt för de förändringar som bland annat genomförts genom EO 14086.

2 Om CLOUD Act

CLOUD Act står för *Clarifying Lawful Overseas Use of Data Act*. CLOUD Act antogs år 2018 och syftar till att på olika sätt överbrygga hinder för amerikanska brottsbekämpande myndigheter att få tillgång till bevisning som återfinns utanför USA. Bland annat innehåller CLOUD Act tillägg till *Stored Communications Act*[7] som förtydligar att amerikanska brottsbekämpande myndigheter har möjlighet att – under vissa förutsättningar och som huvudregel efter domstolsprövning – begära tillgång till information som innehas av företag som lyder under amerikansk lag, oavsett var informationen finns.[8] I denna del gäller CLOUD Act dels för ”Electronic Communications Services”, dels för "Remote Computing Services”, vilket inbegriper molntjänster som Microsoft 365.

En leverantör av sådana tjänster som omfattas av regelverket och som får en begäran har möjlighet att bestrida den inom 14 dagar om denne kan visa att

- utlämnandet skulle strida mot utländsk rätt (i detta fall svensk rätt),
- kunden är en utländsk organisation, samt
- "rättviseskäl" ger för handen vid en intresseavvägning mellan leverantörens intresse och myndighetens intresse att få tillgång till den aktuella informationen att begäran ska avslås.

3 Om sektion 702 i FISA

Enligt sektion 702 i *Foreign Intelligence Surveillance Act* (FISA) har den allmänna åklagaren i USA och direktören för den nationella underrättelsetjänsten möjlighet att gemensamt godkänna inhämtning avseende (i) icke-amerikanska *personer* (ii) som rimligen antas befinna sig utanför USA (iii) som kan ha så kallad *utländsk underrättelseinformation*. Begreppet *personer*[9] i FISA omfattar inte bara fysiska personer utan även grupper, företag, organisationer och främmande makt omfattas. Begreppet *utländsk underrättelseinformation*[10] innefattar information som har bäring på USA:s förmåga att skydda sig mot en faktisk eller potentiell attack, sabotage eller

[6] EU-kommissionen, Adequacy decision for the EU-US Data Privacy Framework, https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en, 2023-12-18.
[7] United States Code, title 18, chapter 121.
[8] United States Department of Justice: https://www.justice.gov/criminal-oia/page/file/1153466/download, 2023-12-18.
[9] FISA §§ 1801(m), 1881(a).
[10] FISA § 1801(e)(1).

underrättelseverksamhet från främmande makt, internationell terrorism, utvecklingen av massförstörelsevapen och liknande allvarliga hot.[11]

Dessutom kräver avsnitt 702 i FISA att allmänna åklagaren i samråd med direktören för den nationella underrättelsetjänsten antar riktningsförfaranden, minimeringsprocedurer och förfrågningsförfaranden som de intygar uppfyller de lagstadgade kraven i avsnitt 702 och överensstämmer med det fjärde ändringsförslaget.[12]

FISA gäller också för ”Electronic Communications Services”, vilket inbegriper ett flertal olika telefoni-, internet- och andra kommunikationstjänster.[13] Molntjänster som Microsoft 365 omfattas av regelverket.

4 Om EO 12333

Executive Order 12333 (EO 12333) gör det möjligt för National Security Agency (NSA) i USA att få åtkomst till uppgifter som är ”i transit” på väg till USA. NSA har åtkomst till undervattenskablar på Atlantens botten och kan samla in och lagra information som överförs med hjälp av kablarna innan de anländer till USA, där de omfattas av bestämmelserna i FISA. [14]

5 Microsofts statistik om den praktiska tillämpningen av lagstiftningen

Microsoft lämnar var sjätte månad en rapport med information om de förfrågningar de får från *brottsbekämpande myndigheter* i hela världen. Rapporten publiceras på deras webbplats: https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report.

Av rapporten framgår att de allra flesta av Microsofts kommersiella kunder aldrig blivit föremål för en förfrågan från en brottsbekämpande myndighet; de allra flesta förfrågningar som kommit gäller konsumentkonton.

Enligt Microsofts statistik kom det under perioden juli–december år 2022 53 förfrågningar från brottsbekämpande myndigheter i USA som avsåg kunddata från kommersiella kunder utanför USA. I fyra fall ledde begäran till att data lämnades ut.[15] Microsoft 365 har närmare 350 miljoner användare globalt.

[11] Se även Privacy and Civil Liberties Oversight Board, https://irp.fas.org/offdocs/pclob-702.pdf, s. 20-22, 2023-12-18.
[12] Office of the Director of National Intelligence, https://www.intel.gov/assets/documents/702%20Documents/statistical-transparency-report/2020_ASTR_for_CY2019_FINALOCR.pdf, s. 11, 2023-12-18.
[13] FISA § 1881(b)(4).
[14] EU-domstolens dom från den 16 juli 2020 (begäran om förhandsavgörande från High Court (Irland) - Irland) – Data Protection Commissioner mot Facebook Ireland Limited och Maximillian Schrems (C-311/20), p. 63, se följande länk: https://curia.europa.eu/juris/documents.jsf?num=C-311/18, 2023-12-18.
[15] Microsoft, https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report, 2024-01-12.

Microsoft publicerar även en rapport om de förfrågningar från *underrättelsemyndigheter* de får med stöd av bland annat FISA. Rapporten publiceras på deras webbplats: https://www.microsoft.com/en-us/corporate-responsibility/us-national-security-orders-report?activetab=pivot_1:primaryr2.

Microsoft får endast redovisa statistiken i intervaller med hundratal eller tusental. Enligt Microsofts statistik kom det under perioden juli–december år 2022 0-499 FISA-förfrågningar om att få ta del av ”content” och 0–499 FISA-förfrågningar om att ta del av ”non-content”.[16] Microsoft redovisar inte hur många av dessa förfrågningar som föranlett dem att lämna ut data. Däremot skriver Microsoft att de många gånger framgångsrikt har bestridit begäran i domstol.[17]

Enligt Microsoft har ingen myndighet direkt tillgång till kunddata genom så kallade ”bakdörrar” eller på något annat sätt.[18]

I det biträdesavtal som Microsoft tillhandahåller åtar de sig att vidta följande åtgärder för att bestrida en order.

Bestridande av order

I händelse av att Microsoft får en order från tredje man om tvingat utlämnande av personuppgifter som behandlas enligt detta DPA ska Microsoft:

a. göra alla rimliga ansträngningar för att hänvisa tredje man direkt till Kunden med sin begäran om data.
b. omgående meddela Kunden, såvida det inte är förbjudet enligt lag som är tillämplig på begärande tredje man, och, om det är förbjudet att meddela Kunden, använda alla lagliga medel för att erhålla rätten att undanröja förbudet för att kunna lämna så mycket information som möjligt till Kunden så snart som möjligt
c. använda alla lagliga medel för att bestrida ordern om utlämnande baserat på rättsliga brister enligt den begärande partens lagar eller eventuella relevanta lagkonflikter med tillämplig lag i EU eller tillämplig medlemsstat.

Om efter att ha vidtagit stegen a. till c. ovan, Microsoft eller något av deras koncernbolag fortfarande tvingas lämna ut personuppgifter ska Microsoft endast lämna ut den minsta mängd av dessa data som är nödvändig för att uppfylla ordern om tvingat utlämnande.[19]

[16] Sist i detta avsnitt finns en förklaring av begreppen ”content” och ”non-content”.
[17] Microsoft, https://www.microsoft.com/en-us/corporate-responsibility/us-national-security-orders-report?activetab=pivot_1:primaryr2, 2023-12-15.
[18] Microsoft, https://blogs.microsoft.com/datalaw/our-practices/, 2023-12-15.
[19] Microsoft, https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?isToggleToList=True&lang=32&year=2021, 2023-12-15.

Microsoft har även en FAQ där de besvarar vanliga frågor om de förfrågningar de får.[20] Nedan följer några exempel på frågor och svar i FAQ:n.

Q: What is the process for disclosing customer information in response to government legal demands?

A: Microsoft requires an official, signed document issued pursuant to local law and rules. Specifically, we require a subpoena or equivalent before disclosing non-content, and only disclose content to law enforcement in response to a warrant (or its local equivalent). Microsoft's compliance team reviews government demands for customer data to ensure the requests are valid, rejects those that are not valid, and only provides the data specified in the legal order.

Q: How many enterprise cloud customers are impacted by law enforcement requests?

A: In the first half of 2022, Microsoft received 142 requests from law enforcement around the world for accounts associated with enterprise cloud customers. In 95 cases, these requests were rejected, withdrawn, no data, or law enforcement was successfully redirected to the customer. In 47 cases, Microsoft was compelled to provide responsive information: 16 of these cases required the disclosure of some customer content and in 31 of the cases we were compelled to disclose non-content information only. Of the 16 instances that required disclosure of content data, 13 of those requests were associated with U.S. law enforcement.

Q: What services are subject to law enforcement requests?

A: As our law enforcement requests reports have shown, the overwhelming majority of requests seek information related to our free consumer services. By comparison, we have received very few requests for data associated with use of our commercial services used by enterprise customers.

Q: How does Microsoft define a FISA order seeking disclosure of content?

A: This category would include any FISA electronic surveillance orders (50 U.S.C. § 1805), FISA search warrants (50 U.S.C. § 1824), and FISA Amendments Act directives or orders (50 U.S.C. §1881 et seq.) that were received or active during the reporting period.

Q: How does Microsoft define a FISA order requesting disclosure of noncontent?

A: This category would include any FISA business records (50 U.S.C. § 1861), commonly referred to as 215 orders, and FISA pen register and trap and trace orders (50 U.S.C. § 1842) that were received or active during the reporting period.

[20] Microsoft, https://blogs.microsoft.com/datalaw/our-practices/#what-is-process-disclosing-customer-information-legal, 2023-12-15.

Q: Are legal demands subject to secrecy orders included in your reporting?
A: Yes. All government requests for data, including any that were accompanied by non-disclosure orders, also known as secrecy orders, are included in our transparency reports. Microsoft has a long history of successfully challenging unnecessary secret surveillance, both directly in communications with law enforcement and formally in court. Microsoft has also advocated in Congress to reform the U.S. non-disclosure order statute, 18 U.S.C. § 2705, to ensure that such orders are properly narrowed, time-limited, and only approved by judges when truly necessary to protect a criminal investigation.

knowit

Bilaga 3. Krypteringsmöjligheter

I denna bilaga beskrivs de möjligheter till kryptering som erbjuds i Microsoft 365 och kundens möjligheter till nyttjande av egna krypteringsnycklar samt vilka juridiska och tekniska konsekvenser dessa alternativ medför.

Innehåll i denna bilaga:

3.1 Generellt om kryptering

Mycket kortfattat så är kryptering algoritmiska funktioner som omvandlar information från klartext till krypterad chiffertext i syfte att skydda informationen från obehörig åtkomst. För att kunna dekryptera och åter få tillgång till innehållet i klartext krävs åtkomst till den nyckel som användes för att kryptera informationen. Att bibehålla krypteringsnyckeln hemlig för obehöriga blir därför helt avgörande och skyddseffekten av krypteringen blir i stor utsträckning en fråga om vem som har tillgång till nycklarna.

Kryptering kan användas i många olika sammanhang för att exempelvis skydda i innehållet på hårddiskar eller i enskilda filer och dokument mot att obehöriga. Det kan också användas för att säkert föra över information mellan olika system. Begrepp som då brukar användas är att information är krypterad i vila respektive under transport.

3.2 Kryptering inom GDPR

För uppgifter som omfattas av Dataskyddsförordningen (GDPR) och tillhörande regelverk kan kryptering fylla olika funktioner. Det kan exempelvis användas för att komplettera och förstärka en behörighetsstyrning, det kan användas för pseudonymisering eller anonymisering av uppgifter eller vara en del av åtgärder för att förhindra obehörig åtkomst till uppgifterna.

3.3 Kryptering inom OSL

För uppgifter som omfattas av Offentlighets- och sekretesslagen (OSL) kan kryptering vara en åtgärd med flera syften, exempelvis för att skydda uppgifterna mot obehörig åtkomst. Detta kan vara fallet exempelvis då uppgifterna behöver kommuniceras över externa nätverk där informationen i klartext annars inte får hanteras. Kryptering kan också användas i funktioner för att upprätthålla riktighet eller spårbarhet för exempelvis säkerhetsloggar.

3.4 Kryptering i Microsoft 365

I Microsoft 365 finns flera olika möjligheter till kryptering för att skydda information både i vila och under transport. Det finns också flera olika lager av kryptering i tjänsten och flera olika sätt att hantera krypteringsnycklar. Några av dessa beskrivs närmare nedan.

Värt att notera är att många av tjänsterna i plattformen, till exempel indexering och sökning, generellt är beroende av att ha tillgång till och kunna läsa informationen för att fungera. Krypteringsalternativ som hindrar tjänsternas åtkomst till kunddata kan därför medföra begränsningar i vilka funktioner som är tillgängliga.

3.4.1 Tjänstekryptering (Service Encryption)

Förutom kryptering i underliggande infrastruktur använder Exchange Online, Microsoft Teams, SharePoint Online och OneDrive även tjänstekryptering för att skydda kunddata.

Tjänstekrypteringen erbjuder två olika alternativ för hanteringen av krypteringsnycklar:

Nycklar hanterade av Microsoft (Microsoft-managed keys) Microsoft hanterar alla krypteringsnycklar, inklusive rotnycklar.
Kundhanterade nycklar (Customer Key) Kunden generar egna krypteringsnycklar som lagras i ett Azure Key Vault och sedan används som rotnycklar för tjänstekrypteringen. Detta innebär att kunden har kontrollen att exempelvis blockera en rotnyckel om den kommit i orätta händer. Skulle rotnycklarna bli otillgängliga finns det möjlighet för kunden att begära återställning via en av Microsoft hanterad tillgänglighetsnyckel.

Oavsett val av nyckelhantering kan Microsoft 365 servicekryptering hantera kunddata i syfte att leverera plattformens tjänster:

” Service encryption is not meant to prevent Microsoft personnel from accessing your data. Instead, Customer Key helps you meet regulatory or compliance obligations for controlling root keys. You explicitly authorize Microsoft 365 services to use your encryption keys to provide value added cloud services, such as eDiscovery, anti-malware, anti-spam, search indexing, and so on.”

Referens: Service encryption with Customer Key - Microsoft 365 Compliance | Microsoft Docs

3.4.2 Informationsskydd genom datakryptering

Ramverket Microsoft Information Protection (MIP) erbjuder tjänster för att identifiera, klassificera och skydda kunddata i Microsoft 365. Verksamheten kan bland annat definiera etiketter som gör att tjänsten automatiskt märker och krypterar dokument som är markerade på det sättet.

3.4.3 Azure Information Protection

Krypteringen i MIP hanteras av tjänsten Azure Information Protection (AIP) och Azure Rights Management Service (Azure RMS). Här lagras den nyckel som används för att kryptera informationen och kunden kan välja hur denna nyckel, ”tenant root key”, genereras:

Nyckel genererad av Microsoft är standardalternativet. Microsoft ansvarar för alla aspekter av nyckelhanteringen.
Kundgenererad nyckel (Bring Your Own Key, BYOK) där kunden själv utfärdar en nyckel som överförs till ett Azure Key Vault för att sedan användas av tjänsten.

Data krypterat med nyckel genererad av Microsoft eller kundgenererad nyckel kan ändå behandlas av Microsoft i syfte att leverera plattformens tjänster:

“Azure RMS ensures that authorized people and services, such as search and indexing, can continue to read and inspect the protected data.
Ensuring ongoing access for authorized people and services, also known as "reasoning over data", is a crucial element in maintaining control of your organization's data. This capability may not be easily accomplished with other information protection solutions that use peer-to-peer encryption.”

Referens: What is Azure Rights Management? - AIP | Microsoft Docs

3.4.4 Kryptering med dubbla nycklar (Double Key Encryption, DKE)

DKE gör det möjligt att kryptera information med en andra nyckel hanterad helt utanför Microsoft 365. Kunden tillhandahåller och ansvarar själv för den infrastruktur som behövs för att leverera nyckelhanteringen. DKE fungerar ihop med Microsoft 365 klientapplikationer för Windows och skyddar informationen på ett sätt som gör att Microsoft och tjänsterna i Microsoft 365 inte kan läsa innehållet.

3.5 Referenser till Microsofts dokumentation om kryptering:

- Encryption in Microsoft 365 - Microsoft 365 Compliance | Microsoft Docs
- Service Encryption - Microsoft 365 Compliance | Microsoft Docs
- Service encryption with Customer Key - Microsoft 365 Compliance | Microsoft Docs
- Learn about the availability key for Customer Key - Microsoft 365 Compliance | Microsoft Docs
- Microsoft Information Protection in Microsoft 365 - Microsoft 365 Compliance | Microsoft Docs
- Restrict access to content using sensitivity labels to apply encryption - Microsoft 365 Compliance | Microsoft Docs
- What is Azure Rights Management? - AIP | Microsoft Docs
- Your Azure Information Protection tenant key | Microsoft Docs
- Double Key Encryption overview and FAQ - Microsoft 365 Compliance | Microsoft Docs

knowit

Bilaga 4. Referenser

Denna bilaga ger referenser till ett antal olika underlag som kan vara bra att känna till i samband med er risk- och sårbarhetsanalys.

Observera att vissa dokument i listan nedan inte är uppdaterade och kan innehålla information som inte tar hänsyn till ändringar som skett sedan dokumentet publicerades, i synnerhet ändringarna i de juridiska förutsättningarna till följd av EU-kommissionens adekvansbeslut för DPF samt den nya sekretessbrytande bestämmelsen i 10 kap. 2 a § OSL.

Innehåll i denna bilaga:

4.1 Några risk- och sårbarhetsanalyser för molntjänster

Ale kommun har genomfört en risk- och sårbarhetsanalys av användandet av Office 365 för kommunens sektor: utbildning, kultur och fritid:
https://docplayer.se/2850188-Risk-och-sarbarhetsanalys.html

Danderyds kommun lät 2019 genomföra en utredning om användningen av Office 365 i kommunens verksamhet:
https://meetingsplus.danderyd.se/committees/kommunstyrelsen/kommunstyrelsen-2019-09-30#21684

4.2 Rättsliga utlåtanden från Integritetsskyddsmyndigheten (IMY) och andra myndigheter samt övriga reflektioner kring rättsläget

SOU 2021:1 Säker och kostnadseffektiv it-drift – rättsliga förutsättningar för utkontraktering (It-driftsutredningen):
https://www.regeringen.se/rattsliga-dokument/statens-offentliga-utredningar/2021/01/sou-20211/

En samling av de remissyttranden som lämnats in avseende It-driftsutredningen:
https://www.regeringen.se/remisser/2021/02/remiss-sou-20211-it-driftsutredningens-delbetankande-saker-och-kostnadseffektiv-it-drift--rattsliga-forutsattningar-for-utkontraktering/

IMY:s remissyttrande som lämnats in avseende It-driftsutredningen:
https://www.imy.se/globalassets/dokument/remissvar/2021/yttrande-over-saker-och-kostnadseffektiv-it-drift--rattsliga-forutsattningar-for-utkontraktering-sou-2021-1.pdf

Knowits remissyttrande som lämnats in avseende It-driftsutredningen:
https://www.knowit.se/globalassets/newsarticle/remissyttrande.pdf

eSam:s vägledning för utkontraktering:
Vägledning för utkontraktering - nya förutsättningar som påverkar bedömningen - eSamverka

Ett beslut från den franska högsta förvaltningsdomstolen där domstolen anger vikten av en helhetsbedömning vid avgörandet om de garantier som personuppgiftsbiträdet ger är tillräckliga (beslutet är på franska)
https://www.legifrance.gouv.fr/ceta/id/CETATEXT000043261200
Ett examensarbete från Uppsala universitet där frågan om överföring av sekretessreglerade uppgifter till molntjänster utreds:
https://www.diva-portal.org/smash/get/diva2:1435004/FULLTEXT01.pdf

Rekommenderad läsning finns också i IMY:s förhandssamråd, som går att begär ut från IMY. Se exempelvis Region Skånes förhandssamråd om IT-system för patientjournaler eller Stockholms stads förhandssamråd rörande Microsoft Teams och Azure.

4.3 Olika svenska underlag av betydelse för denna vägledning

FOI:s modell för risk- och sårbarhetsanalys (FORSA). FORSA innehåller vägledning som kan underlätta arbetet med en risk- och sårbarhetsanalys:
https://www.foi.se/rapportsammanfattning?reportNo=FOI-R--3288--SE

FOI:s handbok för kommunalt arbete avseende risk- och sårbarhetsanalys:
https://www.foi.se/rapportsammanfattning?reportNo=FOI-R--4656--SE

MSB:s metodstöd i informationssäkerhet (direktlänk till delarna om riskanalys):
https://www.informationssakerhet.se/metodstodet/analysera/#riskanalys

Om riskanalys i MSB:s gamla metodstöd:
https://www.informationssakerhet.se/siteassets/gamla-metodstodet-for-lis/2.-analysera/riskanalys.pdf

MSB:s vägledning för risk- och sårbarhetsanalyser:
https://rib.msb.se/filer/pdf/25893.pdf

MSB:s föreskrifter om kommuners risk- och sårbarhetsanalyser:
https://www.msb.se/contentassets/24ed4fb87fa9462fbc2dd1a12811fbd9/foreskrifter-kommuner-rsa.pdf

MSB:s vägledning om indikatorer för bedömning av kommunens generella krisberedskap:
https://www.msb.se/contentassets/24ed4fb87fa9462fbc2dd1a12811fbd9/indikatorer-kommun.docx

eSam:s webbsida om vad de kallar ”molnfrågan“. Hos eSam finns ett antal underlag som nås genom följande länk
https://www.esamverka.se/vad-vi-gor/molnfragan.html

En redovisning av eSams arbete i ”molnfrågan”. Denna redovisning berör teknik, produkter och säkerhetslösningar i molntjänster:
https://www.esamverka.se/download/18.2592ea441774291f4c756db/1611825241932/PM%20Teknik%20och%20molntjänster%201.0%202021.pdf

Kravspecifikation från eSam vid användande av digital samarbetsplattform i offentlig verksamhet:
https://www.esamverka.se/sokresultat.html?query=Kravspec+digital+samarbetsplattform+f+offentlig+sektor+1.3

Vägledning från eSam om it-avtal. Syftet med vägledningen är att ge en överblick av it-avtalsområdet och en orientering kring de it-avtal som är vanligt förekommande:
https://www.esamverka.se/download/18.1d126bc174ad1e6c39c4e0/1588230902739/Vägledning%20it-avtal%20200414%20.pdf

Vägledning från SKR om molntjänster i den offentliga verksamheten. Vägledningen riktas till kommuner och regioner i deras arbete med att digitalisera verksamheten:
https://skr.se/skr/naringslivarbetedigitalisering/digitalisering/arkitektursakerhet/molntjanster.7559.html

Vägledning från SKR om molntjänster och konfidentialitetsbedömning. Vägledningen riktar sig till kommuner och regioner som vill använda molntjänster, särskilt när det gäller konfidentiell information som bland annat omfattas av sekretess eller utgör känsliga personuppgifter:
https://skr.se/download/18.1d1b45d17f44a93c2fced01/1647965592422/Molntja%CC%88nster-och-konfidentialitetsbedo%CC%88mning.pdf

SKR:s sammanfattning och vägledning till kommuner och regioner rörande CLOUD act och molntjänster:
https://skr.se/download/18.1d1b45d17f44a93c2fced02/1647965592582/Molntja%CC%88nster-va%CC%88gledning-Cloud-Act.pdf

Skatteverket beslut om att inte övergå till att använda Teams i verksamheten:
https://www.skatteverket.se/omoss/varverksamhet/rapporterremissvarochskrivelser/remissvar/2021/remissvar2021/8958696.5.3016b5d91791bf54679d41.html

MSB:s webbsida om risk- och sårbarhetsanalyser
https://www.msb.se/sv/amnesomraden/krisberedskap--civilt-forsvar/risk--och-sarbarhetsanalyser/

MSB:s webbsida om stöd i risk- och sårbarhetsanalys. På denna sida samlas länkar till områden som kan ge stöd för den som ska göra en risk- och sårbarhetsanalys
https://www.msb.se/sv/amnesomraden/krisberedskap--civilt-forsvar/risk--och-sarbarhetsanalyser/stod-i-risk--och-sarbarhetsanalys/

En studie av Örebro universitet som tagits fram på uppdrag av MSB. Studien berör frågor om säkerhet i molnlösningar
https://rib.msb.se/filer/pdf/28496.pdf

Vägledning från IMY om informationssäkerhet:
https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/informationssakerhet/

Vägledning från IMY om säkerhetsåtgärder för att skydda personuppgifter som hanteras inom en organisation:
https://www.imy.se/verksamhet/dataskydd/dataskydd-pa-olika-omraden/arbetsliv/tillaten-behandling--vilka-krav-galler/sakerhet/

Vägledning från IMY om överföring av personuppgifter till ett tredje land, eller med andra ord ett land utanför EU/EES:
https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/overforing-till-tredje-land/

Vägledning från IMY om känsliga personuppgifter enligt artikel 9 GDPR:
https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/introduktion-till-gdpr/personuppgifter/kansliga-personuppgifter/

Vägledning från norska dataskyddsmyndigheten (Datatilsynet) om överföring av personuppgifter utanför EU/EES:
https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/overforing-av-personopplysninger-ut-av-eos

4.4 EU och andra internationella underlag

Rapport om Microsofts efterlevnad av EU Cloud Code of Conduct:
https://eucoc.cloud/fileadmin/cloud-coc/files/reports/202105_ReportVerificationDoA_Microsoft_2021LVL02SCOPE116.pdf

EU Cloud Code of Conduct:
https://eucoc.cloud/en/contact/request-the-eu-cloud-code-of-conduct.html

EU:s standardavtalsklausuler för tredjelandsöverföringar:
https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en

EU:s standardavtalsklausuler för personuppgiftsbiträdesavtal:
https://ec.europa.eu/info/law/law-topic/data-protection/publications/standard-contractual-clauses-controllers-and-processors_en

Rekommendation från EDPB om europeiska nödvändiga garantier för övervakningsåtgärder:
https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_sv.pdf

Rekommendation från EDPB om kompletterande säkerhetsåtgärder vid överföring av personuppgifter till länder utanför EU/EES:
https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf

Rekommendation från EDPB om kompletterande säkerhetsåtgärder vid överföring av personuppgifter till länder utanför EU/EES (på svenska):
https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_sv.pdf

Amerikanska regeringens årliga rapport (”transparensrapport”) med statistik om användandet av FISA, National Security Letters och andra underrättelsebemyndiganden:
https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2023/3688-statistical-transparency-report-regarding-national-security-authorities-calendar-year-2022

4.5 Underlag från Microsoft

Dataskyddstillägg för Microsofts produkter och tjänster:
https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?isToggleToList=True&lang=32&year=2021

Översikt av och vidare läsning om kryptering i Microsofts olika tjänster:
https://docs.microsoft.com/en-us/microsoft-365/compliance/office-365-encryption-in-the-microsoft-cloud-overview?view=o365-worldwide

Microsofts vitbok ”Microsofts molntjänster & svenska krav på integritet och patientdatasäkerhet”:
https://www.regeringen.se/contentassets/a415dda1610244df9e94d58148c012fe/159microsoftbilaga3.pdf

Azure: Microsoft Molndesign Offentlig sektor:
https://pulse.microsoft.com/sv-se/transform-sv-se/na/fa2-microsoft-molndesign/

Microsoft 365: Microsoft Molndesign Offentlig sektor:
https://pulse.microsoft.com/sv-se/transform-sv-se/na/fa2-microsoft-molndesign/Stöddokumentation från Microsoft för genomförande av konsekvensbedömning:
https://www.microsoft.com/en-us/download/details.aspx?id=102395

Lista över Microsofts underbiträden (kräver inloggning):
https://go.microsoft.com/fwlink/p/?linkid=2096306

Rapporter från revisioner (“audit reports”) hos Microsoft (kräver inloggning):
https://servicetrust.microsoft.com/ViewPage/MSComplianceGuideV3

Microsofts blogg om databehandling i EU:
https://blogs.microsoft.com/eupolicy/2021/05/06/eu-data-boundary/

Microsofts blogg om dataskydd och Microsofts kundlöften:
https://blogs.microsoft.com/on-the-issues/2020/11/19/defending-your-data-edpb-gdpr/

Microsofts principer rörande integritet och skydd av data:
https://www.microsoft.com/en-us/trust-center/privacy

Microsofts dokumentation ”Azure for secure worldwide public sector cloud adoption” som belyser tekniska åtgärder inom Azure:
https://docs.microsoft.com/en-us/azure/azure-government/documentation-government-overview-wwps

Pressmeddelande från Microsoft om Azures efterlevnad av EU:s uppförandekod för molntjänster:
https://eucoc.cloud/en/detail/news/press-release-microsoft-azure-adheres-to-the-eu-cloud-code-of-conduct/

Tjänster i Azure filtrerade på vilka regioner de levereras ifrån:
https://azure.microsoft.com/en-us/global-infrastructure/services/?products=all&regions=europe-north,europe-west

Avtal för Microsofts tjänster:
https://www.microsoft.com/sv-se/servicesagreement/

Microsofts rapporter och statistik rörande begäranden om utlämnanden av data från rättsvårdande myndigheter och regeringar:
https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report

Microsofts rapporter och statistik rörande begäranden om utlämnanden av data från amerikanska rättsvårdande myndigheter (FISA och National Security Letters):
https://www.microsoft.com/en-us/corporate-responsibility/us-national-security-orders-report?activetab=pivot_1:primaryr2

Microsoft om var data behandlas och lagras i Teams:
https://docs.microsoft.com/en-us/microsoftteams/location-of-data-in-teams

Microsoft om Teams och dataskydd:
https://docs.microsoft.com/en-us/microsoftteams/teams-privacy

Microsoft om valfria anslutna upplevelser (”optional connected experiences”) i Teams:
https://docs.microsoft.com/en-us/microsoftteams/teams-privacy-oce-overview

Microsoft om diagnostikdata vid desktop-användning av Teams:
https://docs.microsoft.com/en-us/microsoftteams/policy-control-diagnostic-data-desktop

Microsoft om diagnostikdata vid mobilanvändning av Teams:
https://docs.microsoft.com/en-us/microsoftteams/policy-control-diagnostic-data-mobile

Microsoft om inställningar och policies i Teams:
https://docs.microsoft.com/en-us/microsoftteams/policy-control-overview

Microsofts frågor och svar om hur data hanteras, bland annat kopplat till FISA:
https://blogs.microsoft.com/datalaw/our-practices/

Schematisk skiss från Microsoft av riskanalys rörande begäran om data kopplat till brottsutredningar:
https://news.microsoft.com/sv-se/2021/02/11/microsofts-molntjanster-och-sakerhet/

Om kryptering, i form av så kallad double key encryption, i Microsoft 365:
https://docs.microsoft.com/en-us/microsoft-365/compliance/double-key-encryption?view=o365-worldwide

Förklaring om diagnostikdata och hur pseudonymisering fungerar i Office-applikationerna
https://support.microsoft.com/en-us/office/diagnostic-data-in-office-f409137d-15d3-4803-a8ae-d26fcbfc91dd

Microsofts samlingssida med information om dataskydd
https://www.microsoft.com/en-us/corporate-responsibility/privacy

knowit

Bilaga 5. Begrepp och förkortningslista

I detta avsnitt beskrivs och definieras de begrepp och förkortningar som tas upp i metoden (dvs. i vägledningen samt i dess appendix och bilagor) och som aktualiseras när t.ex. en kommun genomför risk- och sårbarhetsanalyser kopplade till implementering av Microsoft 365.

Författningar

CLOUD Act	Clarifying Lawful Overseas Use of Data Act
Dataskyddsförordningen (GDPR)	EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).[21]
Dataskyddslagen	Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning
EO 12333	Executive Order 12333
FISA	Foreign Intelligence Surveillance Act, United States Code, title 50, chapter 36.
NIS-direktivet	Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.[22] I svensk rätt har NIS-direktivet implementerats i lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster samt i förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster.
OSL	Offentlighets- och sekretesslag (2009:400)

[21] https://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=CELEX:32016R0679&qid=1631522014713&from=EN. 2023-12-21.
[22] https://eur-lex.europa.eu/legal-content/SV/ALL/?uri=CELEX:32016L1148. 2023-12-21.

Övriga förkortningar och begrepp

Adekvansbeslut	EU-kommissionens beslut om att ett land har en tillräckligt hög skyddsnivå och att personuppgifter därför får överföras dit utan särskilt tillstånd. Beslutet kan också gälla ett territorium, en internationell organisation eller en eller flera sektorer i ett land.[23]
Administratörsdata	Administratörsdata är information om administratörer som levereras under registrering, inköp eller administration av Microsoft-tjänster, till exempel namn, telefonnummer och e-postadresser. Det omfattar också aggregerad användningsinformation och data som är kopplade till ditt konto, till exempel de kontroller du väljer. Vi använder administratörsdata för att tillhandahålla tjänster, slutföra transaktioner, betjäna kontot och upptäcka och förebygga bedrägerier.
Anonymisering	Personuppgifter som har gjorts anonyma på så sätt att den enskilda personen inte, eller inte längre, kan identifieras anses inte utgöra personuppgifter. För att uppgifter verkligen ska vara anonymiserade, krävs att anonymiseringen är oåterkallelig.[24]
Autentisering	Verifiering av ett påstående. Exempelvis verifiering av att en användare är den hen påstår sig vara. Denna typ av verifiering, utförd av verifierande part, används t.ex. vid inloggning eller vid kommunikation mellan två system eller två användare.[25]
Behandling	En åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.[26]

[23] https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/overforing-till-tredje-land/adekvat-skyddsniva/, 2021-12-21.
[24] https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_sv, 2021-12-21.
[25] SIS-TR 50:2015 Terminologi för informationssäkerhet, s. 32.
[26] https://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=CELEX:32016R0679&qid=1631522014713&from=EN

Behörighet	Tilldelade rättigheter att använda en informationstillgång på ett specificerat sätt.[27] Som exempel kan en användare ha behörighet att läsa en fil.
Betalningsdata	Betalningsdata är den information du tillhandahåller när du köper något online hos Microsoft. Det kan innehålla kreditkortsnummer och säkerhetskod, namn, faktureringsadress och annan finansiell information. Vi använder betalningsdata för att slutföra transaktioner och för att upptäcka och förebygga bedrägerier.
Biometriska personuppgifter	Biometriska uppgifter rör en persons fysiska, fysiologiska eller beteendemässiga egenskaper och gör det möjligt att identifiera människor, till exempel genom fingeravtrycksavläsning eller ögonskanning. Foton på människor är bara biometriska uppgifter när de behandlas med teknik som möjliggör identifiering eller autentisering av en person, till exempel med ansiktsigenkänningsteknik[28].
CIO	Chief Information Officer – IT-direktör.[29]
CISO	Chief Information Security Officer – informationssäkerhetsdirektör.[30]
CSO	Chief Security Officer – säkerhetsdirektör[31]
Data från Professionella tjänster	Data från Professionella tjänster avser alla de data, inklusive alla text-, ljud-, video- och bildfiler samt programvara, som tillhandahålls till Microsoft av eller på uppdrag av en kund (eller som kunden tillåter Microsoft att hämta från en produkt) eller som på annat sätt hämtas eller bearbetas av eller på uppdrag av Microsoft genom överenskommelse med Microsoft om att hämta Professionella tjänster.
Dataskydd	Dataskydd är ett begrepp som används för att ange skyddet för den personliga integriteten i de regelverk som ska tillämpas vid behandling av personuppgifter.[32]

[27] SIS-TR 50:2015 Terminologi för informationssäkerhet, s. 32. 2023-12-21.
[28] https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/introduktion-till-gdpr/personuppgifter/kansliga-personuppgifter/, 2023-12-15.
[29] https://it-ord.idg.se/ord/chefstitlar-pa-c, 2023-12-15.
[30] https://it-ord.idg.se/ord/chefstitlar-pa-c, 2023-12-15.
[31] https://it-ord.idg.se/ord/chefstitlar-pa-c, 2022-12-15.
[32] https://www4.skatteverket.se/rattsligvagledning/edition/2019.8/368071.html, 2023-12-15.

Diagnostikdata	Data som samlas in eller erhålls av Microsoft från programvara som installeras lokalt av kunden i samband med Online-tjänsten och kan även kallas telemetri. Dessa data identifieras vanligen med attribut för den lokalt installerade programvaran eller den maskin som kör den programvaran.[33] Observera att Microsoft har nya datakategorier vilka beskrivs i avsnitt 3.1.2 i Vägledningen.
Data at rest	Data i vila. Data som är lagrade på hårddisk, SSD, USB-minne eller annat icke-flyktigt lagringsmedium. Jämför med data in motion och data in use.[34]
DPA	Data Processing Agreement. Svensk översättning: standardiserat personuppgiftsbiträdesavtal (”PUB”).[35] Se också *personuppgiftsbiträde*.
DPO	Data Protection Officer (Dataskyddsombud).[36]
EFTA	Europeiska frihandelssammanslutningen omfattar Island, Liechstenstein, Norge och Schweiz.
Europeiska dataskydds-styrelsen (EDPB)	Den Europeiska dataskyddsstyrelsen (European Data Protection Board, EDPB) är ett oberoende europeiskt organ som bidrar till en enhetlig tillämpning av dataskyddsreglerna inom hela EU/EES samt främjar samarbetet mellan dataskyddsmyndigheterna.[37]
Fjärrdatortjänster	Tillhandahållare av lagrings- eller behandlingstjänster genom ett elektroniskt kommunikationssystem.[38]
Fjärråtkomst	Möjlighet för en organisations användare att komma åt dess icke publika datorresurser från andra platser än organisationens anläggningar.[39]

[33] https://pulse.microsoft.com/sv-se/transform-sv-se/na/fa2-microsoft-molndesign/
[34] https://it-ord.idg.se/ord/data-at-rest/, 2023-12-15.
[35] https://www.mira.se/terminologi-dataskyddsforordningen-gdpr/, 2023-12-15.
[36] https://www.mira.se/terminologi-dataskyddsforordningen-gdpr/, 2023-12-15.
[37] https://www.imy.se/verksamhet/dataskydd/dataskydd-pa-eu-niva/edbp/, 2023-12-15.
[38] 18 U.S. Code § 2711 - Definitions for chapter, 2 p.
[39] https://csrc.nist.gov/glossary/term/remote_access, 2023-12-15.

Grundläggande principer	GDPR har sju grundläggande principer, vilka ska tas hänsyn till genomgående i behandlingen av personuppgifter. Dessa principer stadgas i artikel 5 GDPR: • Laglighet, korrekthet och öppenhet • Ändamålsbegränsning • Uppgiftsminimering • Korrekthet • Lagringsminimering • Integritet och konfidentialitet • Ansvarsskyldighet.
Harmlösa personuppgifter	Integritetsskyddsmyndigheten använder sig av uttrycket harmlös personuppgift. En befattningshavares namn, tjänstetelefon och e-postadress, som är arbetsrelaterad information, betraktas typiskt som harmlös. Däremot inte digitala bilder på anställda. En bedömning av vad som uppfattas som harmlöst måste göras från fall till fall med utgångspunkt i hur integritetskänsligt det kan vara för den registrerade.[40]
Informationssäkerhet	Bevarande av informationens *konfidentialitet*, *riktighet* och *tillgänglighet*. Ibland läggs också begrepp som autenticitet, ansvarsskyldighet, oavvislighet, tillförlitlighet, spårbarhet och auktorisation till för att beskriva begreppet.[41]
Integritetsskyddsmyndigheten (IMY)	Sveriges dataskyddsmyndighet.
Juridiska (avtalsrättsliga), tekniska och organisatoriska åtgärder	*Juridiska*: avtalsrättsliga åtgärder består i allmänhet av unilaterala, bilaterala eller multilaterala avtalsrättsliga åtaganden.[42] *Tekniska*: tekniska åtgärder som kan komplettera de skyddsåtgärder som ingår i överföringsverktygen i artikel 46 GDPR för att säkerställa efterlevnaden av den skyddsnivå som krävs enligt unionsrätten i samband med överföring av personuppgifter till ett tredjeland.[43]

[40] Magnusson Sjöberg, C, Rättsinformatik, 2 uppl, s. 177.
[41] SVENSK STANDARD SS-EN ISO/IEC 27000:2020 s. 5.
[42] https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_sv.pdf s. 30. 2023-12-21.
[43] https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_sv.pdf s. 23. 2023-12-21.

	Organisatoriska: organisatoriska åtgärder kan bestå av interna regler, organisatoriska metoder och standarder som personuppgiftsansvariga och personuppgiftsbiträden skulle kunna tillämpa på sig själva och ålägga uppgiftsinförare i tredjeländer.[44]
Konfidentialitet (”confidentiality”)	Egenskap som innebär att information inte tillgängliggörs eller avslöjas för obehöriga individer, objekt eller processer.[45]
Kritisk nod	I Microsoft 365 finns ett antal ”noder” som är särskilt viktiga att beakta i en risk- och sårbarhetsanalys utifrån juridiska bedömningar och tekniska samt organisatoriska mitigerande åtgärder. Dessa noder är också ofta av den karaktären att de är representativa så till vida att de beskriver många av de utmaningar en organisation behöver beakta på flera andra ställen i Microsoft 365 vid ett införande. Dessa noder har vi valt att kalla ”kritiska noder”.
Kryptering	Att göra information svårläslig för alla som inte ska kunna läsa den. Genom att använda ett kodsystem eller ett chiffer kastas bokstäver och siffror om och text blir oläslig. För att göra informationen läslig igen krävs avkryptering, som (i bästa fall) bara kan göras av de personer som texten är ämnad för.[46] Kryptering kan förekomma i olika former såsom kryptering av filer eller av trafik.
Kunddata	Kunddata är alla de data, inklusive text, ljud, video, bildfiler och programvara, som du tillhandahåller till Microsoft eller som tillhandahålls för din räkning genom din användning av Microsofts onlinetjänster för företag, med undantag för Microsoft Professionella tjänster. Det omfattar kunddata, som är de data som du laddar upp för lagring eller bearbetning, och appar som du laddar upp för distribution via en Microsoft-molntjänst för företag.

44 https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_sv.pdf s. 37. 2023-12-21.

45 SVENSK STANDARD SS-EN ISO/IEC 27000:2020 s. 2.

46 https://internetstiftelsen.se/guide/digitalt-sjalvforsvar-en-introduktion/kryptering/, 2023-12-15.

	Kundinnehåll omfattar till exempel e-post och bilagor i Exchange Online, Power BI-rapporter, SharePoint Online-webbplatsinnehåll eller chattkonversationer.
Känslig personuppgift	Känsliga personuppgifter är uppgifter om: • etniskt ursprung • politiska åsikter • religiös eller filosofisk övertygelse • medlemskap i en fackförening • hälsa • en persons sexualliv eller sexuella läggning • genetiska uppgifter • biometriska uppgifter som används för att entydigt identifiera en person. I GDPR kallas de här uppgifterna *särskilda kategorier av personuppgifter* och stadgas i artikel 9 GDPR.
Lagring (datalagring)	Lagring av data för framtida användning. Med data menas här allt som kan lagras på hårddisk eller andra digitala medier, det vill säga siffror, text, ljud, foton, video, ritningar och annat. Vanligtvis görs en skillnad mellan lagring och arkivering: lagring görs på hårddiskar eller andra lagringsminnen på ett sådant sätt att lagrade data är tillgängliga utan nämnvärd väntetid. Arkivering görs däremot ofta på billiga men långsamma medier (magnet-band, cd, dvd) och innebär längre väntetid.[47]
Microsofts datatyper	Se *kunddata*, *personliga uppgifter* och *data från Professionella tjänster*, *Administratörsdata* och *Betalningsdata*.
Mitigerande åtgärder	Mitigerande åtgärder avser åtgärder för att hantera en risk. Dessa kan vara juridiska (avtalsrättsliga), tekniska eller organisatoriska.
Molntjänst	En tjänst som möjliggör tillgång till en skalbar och elastisk pool av delbara dataresurser.[48]
Multifaktorautentisering (”MFA")	Kallas också flerfaktor-autentisering. Autentisering baserad på flera oberoende tekniker för autentisering.[49] Se även *autentisering*.

[47] https://it-ord.idg.se/ord/datalagring/, 2023-12-15.
[48] Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster 2 §.
[49] SIS-TR 50:2015 Terminologi för informationssäkerhet, s. 44.

Oavvislighet	Förmåga att bevisa förekomsten av en påstådd händelse eller handling och dess ursprung.[50]
Omsorgsplikt	Omsorgsplikten innebär att den personuppgiftsansvarige behöver utreda vilka förutsättningar personuppgiftsbiträdet har att efterleva sina skyldigheter enligt dataskyddsregelverket. Omsorgsplikten stadgas i artikel 28 GDPR.
(Personlig) integritet	Skyddet av personuppgifter stadgas bland annat i artikel 8 i EU-stadgan om de grundläggande rättigheterna. Där framgår att: 1. Var och en har rätt till skydd av de personuppgifter som rör honom eller henne. 2. Dessa uppgifter ska behandlas lagenligt för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund. Var och en har rätt att få tillgång till insamlade uppgifter som rör honom eller henne och att få rättelse av dem. 3. En oberoende myndighet ska kontrollera att dessa regler efterlevs.
Personuppgift	Varje upplysning som avser en identifierad eller identifierbar fysisk person (också kallad en registrerad), varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.[51] En IP-adress kan utgöra personuppgift – dock inte dynamiska IP-adresser, utan endast fasta. Se även Microsoft datakategori Personliga uppgifter nedan.
Personliga uppgifter (Microsoft datakategori)	"Personliga uppgifter" avser all information som rör en identifierad eller identifierbar fysisk person. En identifierbar fysisk person är någon som kan identifieras, direkt eller indirekt, till exempel ett namn, id-nummer,

[50] SVENSK STANDARD SS-EN ISO/IEC 27000:2020 s. 7.
[51] https://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=CELEX:32016R0679&qid=1631522014713&from=EN, 2023-12-21.

	platskoordinater, online-id eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, mentala, ekonomiska, kulturella eller sociala identitet. Microsoft använder samma GDPR-definition för personuppgifter. Det omfattar pseudonymiserade data. Förutom att personliga uppgifter är en delmängd av administratörsdata och betalningsdata är personliga uppgifter också en delmängd av var och en av de datakategorier som anges ovan.
Personuppgiftsansvarig	En fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter; om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt.[52]
Personuppgiftsbiträde	En fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning.[53]
Policy	Internt styrande dokument som anger organisations avsikter och inriktning, formellt uttalade av dess högsta ledning.[54] En policy kan också vara en centralt beslutad inställning i en tjänst (såsom Teams) som en administratör ställt in för alla, eller delar av, organisationens användare.[55]
Pseudonymisering	Behandling av personuppgifter på ett sätt som innebär att personuppgifterna inte längre kan tillskrivas en specifik registrerad utan att kompletterande uppgifter används, under förutsättning att dessa kompletterande uppgifter förvaras separat och är föremål för tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna inte tillskrivs

[52] Artikel 4 p. 7 GDPR.
[53] Artikel 4 p. 8 GDPR.
[54] SIS-TR 50:2015 Terminologi för informationssäkerhet, s. 14.
[55] https://docs.microsoft.com/en-us/microsoftteams/assign-policies-users-and-groups, 2023-12-15.

	en identifierad eller identifierbar fysisk person.[56]
Registrerad	En identifierad eller identifierbar fysisk person.
Riktighet (”integrity”)	Egenskap som innebär att vara korrekt och fullständig.[57]
Riskanalys	Riskbedömning kallas den övergripande process som innefattar först *riskidentifiering* och *riskanalys*, för att slutligen i en *riskutvärdering* bedöma resultaten för att se om riskens storlek är acceptabel och godtagbar eller om någon annan form av *riskbehandling* behöver appliceras.[58]
Risk- och sårbarhetsanalys	Här avses en process för analys av risker inom en verksamhet som innehåller identifiering av risker och hur dessa ska hanteras.
Röjande	Det följer av lagtexten i OSL att ett utlämnande är en form av röjande. Begreppet är dock omdiskuterat och kan läsas mer om i Appendix B, avsnitt 4.
Sanktionsavgift	Enligt artikel 83 GDPR kan tillsynsmyndigheter, i Sverige Integritetsskyddsmyndigheten, besluta om administrativa sanktionsavgifter vid överträdelser av GDPR. Nästan alla överträdelser av GDPR kan leda till administrativa sanktionsavgifter. Vilka överträdelser det rör sig om anges i GDPR och den kompletterande dataskyddslagen.[59]
Sekretess	Ett förbud att röja en uppgift, vare sig det sker muntligen, genom utlämnande av en allmän handling eller på något annat sätt.[60]
Sekretessreglerad uppgift	En uppgift för vilken det finns en bestämmelse om sekretess.[61]
Sekretessbelagd uppgift	En sekretessreglerad uppgift för vilken sekretess gäller i ett enskilt fall.[62]

[56] https://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=CELEX:32016R0679&qid=1631522014713&from=EN#d1e1469-1-1, 2023-12-21.
[57] SVENSK STANDARD SS-EN ISO/IEC 27000:2020 s. 5.
[58] SVENSK STANDARD SS-EN ISO/IEC 27000:2020 s. 9–11.
[59] https://www.imy.se/om-oss/vart-uppdrag/sa-arbetar-vi-med-tillsyn/vad-kan-tillsynen-leda-till/, 2023-12-15.
[60] 3 kap. 1 § OSL.
[61] 3 kap. 1 § OSL.
[62] 3 kap. 1 § OSL.

Spårbarhet	Entydig härledning av utförda aktiviteter till en identifierad användare.[63]
Standardavtalsklausuler (”standard contractual clauses”, SCC)	Standardiserade avtalsklausuler som EU-kommissionen har antagit för överföringar av personuppgifter mellan personuppgiftsansvariga eller personuppgiftsbiträden inom EES och personuppgiftsansvariga eller personuppgiftsbiträden utanför EES.[64] Standardavtalsklausuler som antagits av EU-kommissionen är överföringsverktyg i enlighet med artikel 46.2 c och 46.5 GDPR.
Supportdata	Data som tillhandahålls Microsoft av eller på uppdrag av kunden för att erhålla teknisk support för onlinetjänster.[65] Observera att Microsoft har nya datakategorier vilka beskrivs i avsnitt 3.1.2 i Vägledningen.
Säkerhetsskydd	Med säkerhetsskydd avses skydd av säkerhetskänslig verksamhet mot spionerі, sabotage, terroristbrott och andra brott som kan hota verksamheten samt skydd i andra fall av säkerhetsskyddsklassificerade uppgifter.[66]
Tillgänglighet (”availability”)	Egenskap att vara åtkomlig och användbar på begäran från ett behörigt objekt.[67]
Tillsynsmyndighet	IMY (Integritetsskyddsmyndigheten) är Sveriges nationella *tillsynsmyndighet* för behandling av personuppgifter.[68]
Tjänstegenererade data	Data som genereras eller härleds av Microsoft genom drift av tjänsten, till exempel användnings- eller prestandadata. De flesta av dessa data innehåller pseudonyma identifierare som genereras av Microsoft.[69] Observera att Microsoft har nya datakategorier vilka beskrivs i avsnitt 3.1.2 i Vägledningen.
Tredjeland	Alla länder som inte är medlemmar i EU/EES.

[63] SIS-TR 50:2015 Terminologi för informationssäkerhet, s. 10.
[64] https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_sv.pdf, 2023-12-21.
[65] https://pulse.microsoft.com/sv-se/transform-sv-se/na/fa2-microsoft-molndesign/
[66] 1 kap. 2 § Säkerhetsskyddslag (2018:585).
[67] SVENSK STANDARD SS-EN ISO/IEC 27000:2020 s. 2.
[68] https://www.imy.se/om-oss/vart-uppdrag/, 2023-12-15.
[69] https://pulse.microsoft.com/sv-se/transform-sv-se/na/fa2-microsoft-molndesign/

Tredjelandsöverföring	En tredjelandsöverföring sker i samband med att personuppgifter överförs till ett tredjeland. Begreppet är dock omdiskuterat och finns att läsa mer om i Appendix B, avsnitt 3.
Underbiträde	Ett företag eller myndighet som behandlar personuppgifter för någon annans räkning är att anse som ett personuppgiftsbiträde. Biträdet kan i sin tur anlita andra biträden, så kallade underbiträden.[70]
Uppförandekod	Riktlinjer som särskilt beskriver hur en viss verksamhet, bransch eller samhällssektor ska behandla personuppgifter i enlighet med GDPR.[71]
Uppgifter om hälsa	Personuppgifter om hälsa är alla uppgifter som ger information om den registrerades tidigare, nuvarande eller framtida fysiska eller psykiska hälsotillstånd. Hälsouppgifter omfattar alltså alla aspekter av din hälsa, till exempel uppgift om • sjukdom • sjukfrånvaro • graviditet • läkarbesök • funktionshinder[72].

[70] https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/personuppgiftsansvariga-och-personuppgiftsbitraden/att-tanka-pa-som-personuppgiftsbitrade/, 2023-12-15.
[71] https://www.imy.se/ordlista/#U, 2023-12-15.
[72] https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/introduktion-till-gdpr/personuppgifter/kansliga-personuppgifter/, 2023-12-15.