2025-05-26

Juridisk bedömning – Bedömning av rättsliga ramar och avtalsrisker för Microsoft företagsskydd

1. Inledning och bakgrund

Intraservice planerar att fatta beslut om att åter aktivera tjänsten Microsoft 365 Copilot Chatt. Microsoft 365 Copilot chatt är en fristående applikation inom ramen för Microsoft 365. Tjänsten har tidigare varit pausad med anledning av osäkerheter kring informationssäkerhet, integritet samt avsaknad av tydliga riskbedömningar. För att möjliggöra ett välgrundat beslut har vi ombetts att genomföra en juridisk bedömning av huruvida det företagsskydd som Microsoft presenterat är tillräckligt för att möjliggöra användning av Microsoft 365 Copilot Chatt i Enterprise-miljö.

Som en del av detta arbete har vi nu genomfört en genomgång av de dokument som vi bedömer vara relevanta för att kunna göra en sådan bedömning. Dessa inkluderar bland annat:

- Microsoft Product Terms, version maj 2025, utgiven av Microsoft Licensing
- Microsoft Products and Services Data Protection Addendum (DPA), version april 2025
- Microsoft Privacy Statement, uppdaterad mars 2024, utgiven av Microsoft Corporation.
- Microsoft Commercial Support Subprocessors, version 10 mars 2025, utgiven av Microsoft Licensing.
- Intern riskanalys genomförd av Intraservice, våren 2025

Om Microsoft 365 Copilot chatt

Microsoft 365 Copilot chatt är en generativ AI-chatt liknande ChatGPT. Med generativ AI menas den typ av artificiell intelligens som skapar nytt innehåll från användarens instruktioner.

Det finns två huvudsakliga gränssnitt för att nå chatten; som en app via Microsoft 365 på webben och i sidofönstret i webbläsaren Edge.

Microsoft 365 Copilot chatt kan exempelvis skriva texter och generera bilder utifrån den information som användaren matar in, eller sammanfatta och översätta text. Microsoft 365 Copilot chatt kan också svara på användarens frågor genom att söka på webben med hjälp av sökmotorn Bing.

Microsoft 365 Copilot chatt i sidofönstret i webbläsaren Edge har en funktion för att läsa in den aktuella webbläsarflikens sidinnehåll. Inläsning görs i det fall användaren efterfrågar en sammanfattning av sidan eller ställer frågor om sidans innehåll.

Avgränsningar

Microsoft erbjuder även en mer omfattande AI-assistent, Microsoft 365 Copilot, genom köp av extra licens. Microsoft 365 Copilot är integrerad med applikationer såsom Word och Excel, och har tillgång till användarens information och dokument inom Microsoft 365-miljön. Den här

bedömningen är avgränsad till att inte omfatta Microsoft 365 Copilot då den hanteras i en separat utredning.

Den här bedömningen är inte heller tänkt som en bedömning av hela Microsoft 365-tjänsten.

2. Företagsskyddets innehåll och rättsliga status

2.1 Vad är företagsskyddet och vad omfattas av det för Microsoft 365 Copilot chat

Vi har tagit del av tillgänglig dokumentation från Microsoft samt haft möjlighet att föra en direkt dialog med representanter från Microsoft Sverige för att förtydliga vissa aspekter av det skydd som erbjuds i samband med användning av Microsoft 365 Copilot Chatt.

Microsoft har infört ett särskilt företagsskydd (Enterprise Data Protection) för användning av Microsoft 365 Copilot chatt.

Nedan redogörs för de centrala komponenterna för företagsskyddet:

1. **AI säkerhets- och upphovsrättsrisker**
   Microsoft förbinder sig att försvara sina kommersiella kunder vid eventuella krav på upphovsrättsintrång kopplat till innehåll som genererats av Microsoft 365 Copilot Chat, förutsatt att tjänsten använts i enlighet med avtalet. Detta åtagande syftar till att minska risken för rättsliga tvister gällande AI-genererat material.

2. **Dataskyddsavtal (DPA)**
   Microsoft åtar sig att inte använda kunddata, såsom användarens chattinmatningar, dokumentinnehåll och e-post, för att träna AI-modeller. Data används endast enligt instruktioner från kunden och hålls inom dennes kontrollerade miljö. Detta är särskilt relevant i förhållande till efterlevnad av GDPR och andra dataskyddsregelverk.

3. **Avtalsmässigt skydd enligt dataskyddsavtal och Produktvillkoren**
   Microsoft agerar som personuppgiftsbiträde enligt villkoren i sitt dataskyddsavtal (DPA) och sina produktvillkor. Det innebär att även Microsoft 365 Copilot Chatt omfattas av samma dataskyddsregler som andra Microsoft 365-tjänster, t.ex. SharePoint. Vad produktvillkoren innefattar framgår av avsnitt 2.2.

4. **Säkerhetsåtgärder**
   Data som behandlas i Microsoft 365 Copilot Chatt krypteras både under överföring och i vila. Microsoft implementerar tekniska och organisatoriska säkerhetsåtgärder samt säkerställer logisk separering av data mellan olika kunder, i enlighet med vedertagna säkerhetsstandarder.

5. **EU Data Boundary**
   För kunder inom EU omfattas Microsoft 365 Copilot Chat av Microsofts initiativ EU Data Boundary, vilket innebär att kunddata behandlas och lagras inom EU:s geografiska område. Detta är centralt för organisationer med krav på geografiskt begränsad datalagring.

Sammanfattning

Det företagsskydd som Microsoft erbjuder i samband med användning av Microsoft 365 Copilot Chatt bygger i huvudsak på Microsofts egna avtalsvillkor och åtaganden, snarare än på rättsligt bindande garantier enligt oberoende lagstiftning eller myndighetsprövning. Detta innebär att om skyddets omfattning eller tillämpning skulle bli föremål för rättslig prövning, exempelvis i domstol eller tillsynsärende, är det i praktiken Microsoft som har definierat ramarna för vad som skyddas, hur data hanteras och vilket ansvar som företaget tar.

2.2 Skyddets grund i Microsofts Produktvillkor

Microsofts produktvillkor utgör den avtalsrättsliga grunden för företagets molntjänster och är direkt avgörande för hur företagsskyddet för Microsoft 365 Copilot Chatt ska förstås och tillämpas. Produktvillkoren är ett standardiserat avtalsdokument som reglerar användningsvillkor, licensbestämmelser och databehandlingsprinciper för Microsofts tjänster. Vilka tjänster som omfattas, hur data får användas och i vilken utsträckning AI-genererat innehåll får spridas eller återanvändas regleras uttryckligen i produktvillkoren. Dessa villkor är därför centrala för att fastställa företagsskyddets faktiska räckvidd och innehåll.

Företagsskyddet för Microsoft 365 Copilot Chatt, är inte ett separat rättsligt avtal utan bygger på, och är villkorat av, de åtaganden som anges i produktvillkoren och det tillhörande dataskyddsavtalet (DPA). Det innebär att skyddet är avtalsbaserat och saknar den rättsliga status som följer av lagstadgade garantier eller bindande myndighetsbeslut. I praktiken utgör det ett ensidigt åtagande från Microsoft baserat på de avtalsvillkor som kunden genom användning av tjänsten har accepterat. Detta innebär att företagsskyddets omfattning och förutsättningar kan ändras över tid.

Sammanfattning

Företagsskyddet för Microsoft 365 Copilot Chatt vilar på Microsofts standardiserade produktvillkor och dataskyddsavtal (DPA). Det utgör inte ett självständigt rättsligt avtal utan är ett avtalsbaserat och ensidigt definierat åtagande från Microsoft. Produktvillkoren reglerar centrala aspekter som licens, dataanvändning och hantering av AI-genererat innehåll får återanvändas, delas eller lagras. Villkoren är dynamiska och uppdateras löpande av Microsoft, vilket innebär att företagsskyddets omfattning och tillämpning kan förändras över tid utan förhandlingsmöjlighet för kunden. Det finns ingen garanti för långsiktig oförändrad tillämpning eller rättsligt bindande kontinuitet, eftersom det är Microsoft som ensidigt fastställer innehållet i villkoren. Skyddet saknar således den rättsliga status som följer av lag eller myndighetsbeslut och dess omfattning kan ändras av Microsoft över tid.

Det ingår inte i vårt uppdrag att bedöma andra typer av avtal. Vi vill dock påpeka att sådana typer av upplägg inte är unik för Microsoft utan vanligt förekommande för licensavtal med prenumeration av molntjänster

2.3 Bing

Bing är Microsofts sökmotor och kan användas i Microsoft 365 Copilot Chatt för att möjliggöra extern informationsinhämtning från internet. Denna funktion aktiveras i huvudsak när en fråga inte kan besvaras med data från användarens instruktion i chatten, eller när realtidsinformation

efterfrågas, exempelvis nyheter, allmänna fakta eller webbaserat innehåll. I dessa fall använder Microsoft 365 Copilot Chatt Bing Search API för att hämta externa svar.

Enligt Microsofts dokumentation inkluderas en del av användarens fråga eller instruktion i webbsökningen när sökmotorn Bing används för att hitta svar. Sökningen görs i Microsofts namn, och ingen information om användaren eller organisationen skickas med i sökningen.

När man jämför en vanlig sökning i Bing eller annan sökmotor på webben, med en konversation i Microsoft 365 Copilot chatt finns det tydliga skillnader i hur personuppgifter behandlas och loggas. Dessa skillnader är särskilt viktiga ur ett dataskydds- och sekretessperspektiv.

Egenskap	Bing-sökning	Copilot chatt (företag)
Annonspersonalisering	Ja	Nej
Datainsamling	IP, plats, sökord, enhet	Begränsad till organisationens miljö
Modellträning	Möjligt	Aldrig
Loggning	Ja, kopplat till konto	Kontrolleras av organisationen

Microsoft har i sin dokumentation tydliggjort att viss databehandling som sker inom ramen för Bing inte omfattas av det dataskyddsavtal (DPA) som gäller för övriga Microsoft 365-tjänster. Detta gäller särskilt när Bing används för Microsofts egna syften, såsom för att förbättra sin söktjänsts funktionalitet, generering av användningsstatistik men också felsökning och teknisk optimering.

I dessa situationer agerar Microsoft som självständig personuppgiftsansvarig, inte som personuppgiftsbiträde. Det innebär att den information som skickas till Bing, frågeinnehåll och teknisk metadata, behandlas enligt Microsofts egna villkor och potentiellt för ändamål som ligger utanför den aktuella myndighetens kontroll eller instruktion.

Sammanfattning

När Microsoft 365 Copilot Chatt använder Bing för att hämta information från internet behandlas delar av användarens fråga eller instruktion utanför Microsoft 365:s ordinarie skyddsrutiner. I dessa fall omfattas inte databehandlingen av det dataskyddsavtal (DPA) som annars gäller för Microsofts molntjänster. Istället agerar Microsoft som självständig personuppgiftsansvarig, vilket innebär att information som skickas till Bing, såsom frågeinnehåll behandlas enligt Microsofts egna villkor.

Microsoft har i sin dokumentation angett att de tillämpar principer om dataminimering och att information om användarkonto och organisation anonymiseras, för att minska integritetsrisken. Enligt Microsofts uppdaterade beskrivning (maj 2025) skickas inte hela användarens prompt till

Bing, utan endast en maskinellt genererad sökfråga. Ingen användaridentifierande information, inga dokument eller uppladdade filer skickas, och det som skickas behandlas som konfidentiell kunddata. Bing-resultat märks tydligt och används inte för annonsering, modellträning eller profilering.

Dessa förbättringar utgör ett steg mot stärkt informationssäkerhet och lagefterlevnad, särskilt för reglerade verksamheter. Detta förändrar dock inte det grundläggande ansvaret eftersom informationen behandlas utanför DPA, och därmed utan instruktion från den personuppgiftsansvarige. Detta innebär att behandlingen sker utanför Intraservice kontroll vilket medför en kvarstående juridisk risk ur ett GDPR- och ansvarsperspektiv.

3. Identifierade risker

3.1 Risk för delning av känslig eller sekretessbelagd information

Även om Microsoft tillhandahåller företagsdataskydd för Microsoft 365 Copilot Chatt, kvarstår det risker för att känslig information oavsiktligt delas med Microsoft, om användare inkluderar sådan information i sina prompts eller uppladdade filer. Microsoft betonar ett ansvar hos användaren att inte dela känslig information i sina inmatningar eller bifogade filer. Vidare uppger Microsoft i sin dokumentation att sådana användardata hanteras inom ramen för företagets dataskydd och inte används för att träna de bakomliggande språkmodellerna. Trots detta är det i dagsläget inte helt klarlagt i vilken utsträckning Microsoft tekniskt kan separera eller utesluta skyddsvärd information från vidare behandling. Det är viktigt att understryka att organisatoriska åtgärder såsom utbildning, interna riktlinjer och rutiner spelar en avgörande roll för att minska risken för oavsiktlig delning av känslig information. Samtidigt kvarstår ett rättsligt ansvar för personuppgiftsansvarig, Intraservice, att säkerställa att skyddet inte enbart vilar på enskilda användares agerande, utan också stöds av tekniska och strukturella kontroller.

Microsoft har i sin dokumentation tydliggjort att ansvaret för korrekt åtkomstkontroll åligger kunden. Det innebär att den personuppgiftsansvarige behöver säkerställa att tjänsten endast används av behöriga och att åtkomstkontroller, loggning och sekretessnivåer är korrekt konfigurerade innan tjänsten tas i bruk. Att ansvaret är utlagt på kunden minskar inte det rättsliga kravet på att faktisk kontroll måste kunna visas upp i efterhand.

Samma risk gäller för data som behandlas inom hela Microsoft 365-tjänsten, inklusive i applikationer som Microsoft 365 Copilot chatt. Information av informationsklass 3 bör därför inte hanteras i tjänsten.

3.2 Risk för utlämnande av data till utländska myndigheter

Microsofts dataskyddsavtal (DPA) och relaterade dokument anger att Microsoft, som ett amerikanskt företag, kan bli skyldiga att lämna ut kunddata till amerikanska myndigheter enligt lagar som CLOUD Act och FISA, även om datan är lagrad inom EU. Detta innebär att det finns en konkret risk att uppgifter som omfattas av svensk sekretesslagstiftning kan lämnas ut till utländska myndigheter utan att svenska myndigheter har någon kontroll eller insyn i utlämnandet.

Microsoft åtar sig att underrätta kunder vid tredjepartsbegäran om utlämnande av data, men detta är inte alltid möjligt. Om en begäran åtföljs av en tystnadsplikt enligt amerikansk

lagstiftning, kan Microsoft vara förbjudna att informera kunden om att data har lämnats ut. Samma situation kan uppstå i andra länder där Microsoft behandlar data, genom egna eller anlitade underleverantörer. Detta innebär att det finns en konkret risk att uppgifter som omfattas av svensk sekretesslagstiftning lämnas ut till utländska myndigheter, utan att svenska myndigheter haft någon kontroll eller insyn i utlämnandet.

3.3 Risk för införande av nya avtalsvillkor

Microsoft förbehåller sig rätten att ensidigt uppdatera produktvillkor och dataskyddstillägget i samband med införande av nya funktioner, tillägg eller relaterad programvara. Även om Microsoft enligt dataskyddsavtalet (DPA) ska meddela väsentliga ändringar, har kunden i praktiken begränsad möjlighet att påverka förändringarnas innehåll eller förhindra att de träder i kraft.

För Microsoft Copilot chat innebär detta att centrala delar av tjänstens funktionalitet, såsom användning av Bing, kan komma att ändras utan föregående prövning eller samråd med kunden. Eftersom företagsskyddet vilar på dessa villkor påverkas även skyddets räckvidd och tillämplighet av sådana ändringar.

Till detta kommer att det finns en inlåsningseffekt av att använda många av Microsofts produkter och tjänster i omfattade grad, ofta integrerade med varandra och tjänster från andra leverantörer. Detta gör det svårt att frånträda tjänsten utan betydande påverkan på den övergripande IT-miljön.

Detta kan aktualisera risken för att Microsoft genomför ändringar av syfte och/eller omfattning av behandling av personuppgifter eller förändringar i tjänstens funktion utan att myndigheten i förväg kan göra en rättslig eller säkerhetsmässig bedömning. För kommunal förvaltning innebär detta en potentiellt allvarlig begräsning i möjligheten att säkerställa informationshanteringen och därmed en rättslig osäkerhet.)

3.4 Risk för åtgärder utan rättsligt stöd

Enligt legalitetsprincipen (5 § Förvaltningslagen) får en myndighet endast vidta åtgärder som har stöd i rättsordningen. När centrala IT-tjänster eller molnplattformar som tillhandahålls av Microsoft integreras uppstår en reell risk att känslig eller sekretessreglerad information bearbetas eller delas utan att Intraservice ges möjlighet att utöva kontroll eller genomföra en egen sekretessprövning. Detta kan leda till att rättsliga krav kring sekretessprövning, dokumenthantering och intern åtkomststyrning inte uppfylls. Det uppstår också en risk för att kravet (i 9 § Förvaltningslagen) på att myndigheters handläggning av ärenden ska ske på ett rättssäkert sätt inte uppfylls. Detta innebär att myndigheten i praktiken överlåter ett konstitutionellt och lagreglerat ansvar till en extern leverantör, vilket strider mot grundläggande principer i svensk förvaltningsrätt.

Den tidigare genomförda riskbedömningen visar att Microsoft 365 Copilot Chatt kan användas på sätt som leder till behandling eller spridning av känsliga uppgifter utan tillräcklig kontroll. Exempel på sådana risker är:

- sammanfattning av innehåll i webbläsarflikar (risk 15)
- användarens inmatning av skyddsvärd information av användare (risk 6)
- otillräcklig utbildning eller otydliga riktlinjer (risk 5)

- otillämplig lagring i molntjänsten (risk 16), och
- att information behandlas i länder utanför EU (risk 17).

De åtgärder som föreslås i riskanalysen, främst användarutbildning och informationsinsatser, kan endast minska en del av riskerna. Eftersom tjänsten bygger på användarens direkta interaktion uppstår en betydande kvarstående risk att felaktig eller otillbörlig informationsdelning sker, även utan uppsåt.

Vidare innebär det en rättslig osäkerhet att risken för att EU-domstolen eller EU-kommissionen i framtiden underkänner USA:s skyddsnivå (risk 18), risken har flyttats bort från verksamhetsnivån trots att den direkt påverkar användningen av Microsoft 365 Copilot Chatt. Denna risk bör kvarstå i bedömningen eftersom den är direkt kopplad till möjligheten att uppfylla dataskydds- och sekretesskrav.

I dessa situationer kan uppgifter göras tillgängliga för Microsoft, vilket ur ett juridiskt perspektiv kan utgöra ett otillåtet röjande enligt Offentlighet- och sekretesslagen, även om det sker oavsiktligt. Därtill kommer risken att uppgifter kan lämnas ut till utländska myndigheter enligt amerikansk lagstiftning, med stöd av amerikansk CLOUD Act, utan att Intraservice underrättas. I dessa fall förlorar myndigheten faktisk kontroll över informationshanteringen, vilket står i direkt strid med offentlighets- och sekretesslagens krav på sekretess och rättssäker behandling.

Det föreligger en icke försumbar risk att åtgärder vidtas utan tillräckligt rättsligt stöd vid användning av Microsoft 365 Copilot Chatt, särskilt i frånvaro av tydliga rutiner, sekretessprövning och tekniska begränsningar.

3.5 Risker vid överföring av personuppgifter till tredje land

Microsoft reglerar sin rätt att föra över kunders personuppgifter till tredje land främst i sitt dataskyddsavtal (DPA). Med vissa undantag som anges i produktvillkoren (se 2.2 och 2.3 ovan) gäller dataskyddsavtalet för dataskydd kopplat till deras produkter och tjänster.

I sitt dataskyddsavtal (DPA) fastställer Microsoft att man tar ansvar för att uppfylla väsentliga delar av GDPR kopplat till tredjelandsöverföring. Microsoft är certifierat för EU: s–USA: s dataskyddsramverk. Vidare regleras all överföring av kunddata, data i professionella tjänster och personuppgifter från EU, EES som görs för att tillhandahålla produkterna och tjänsterna av villkoren från 2021 års standardavtalsklausuler, (SCC) som implementerats av Microsoft. Därmed menar Microsoft att det alternativa kravet i GDPR på att vidta lämpliga skyddsåtgärder vid överföring av personuppgifter till tredje land är uppfyllt.

Microsoft har vid förfrågan presenterat exempel på avtal med standardavtalsklausuler, (SCC) som man använder mot underbiträden vid tredjelandsöverföring kopplat till sina tjänster. Intraservice har även efterfrågat exempel på leveransavtal som Microsoft ingått med underordnade personuppgiftsbiträden i olika tredje länder avseende vilka personuppgifter som överförs, hur den hanteras och i vilka syften. Sådana leveransavtal har inte presenterats. Utifrån befintligt underlag vi inte fullt ut kunnat verifiera hur Microsoft anser att kraven på tredjelandsöverföring säkerställs.

Underordnade personuppgiftsbiträden

Microsoft förbehåller sig rätten att anlita underordnade personuppgiftsbiträden för att tillhandahålla vissa begränsade eller relaterade tjänster för sin räkning. I dataskyddsavtalet

(DPA) anges att kunden samtycker till detta anlitande och till Microsofts koncernbolag/dotterbolag som underordnade personuppgiftsbiträden. Sådant godkännande utgör Kundens föregående skriftliga medgivande till att Microsoft lägger ut behandling av kunddata, data i Professionella tjänster och personuppgifter på underentreprenad, även när sådan behandling innebär överföring av data till tredje land och kundens medgivande krävs enligt standardavtalsklausuler (SCC) eller andra krav i GDPR.

Standardavtalsklausuler, (SCC) innehåller skrivningar som i vissa fall, till exempel när inhemsk lagstiftning tvingar biträdet att lämna ut personuppgifter, innebär att personuppgifter röjs och lämnas ut. Det kan också uppstå situationer när inhemsk lagstiftning tvingar underbiträdet att lämna ut uppgifterna och samtidigt binder underleverantören vid sekretess att meddela att ett utlämnande ägt rum. Det saknas underlag som klargör om Microsoft har gjort en självständig bedömning av om lagstiftning i respektive land där underbiträden har sin verksamhet innebär risker för att kundens uppgifter kan lämnas ut och röjas, med eller utan kundens vetskap. Microsoft kan därmed komma att behandla kundens uppgifter på ett sätt som riskerar att strida mot såväl EU-lagstiftning som svensk lagstiftning.

I sitt dataskyddsavtal (DPA) ger Microsoft kunden mycket begränsade alternativ för det fall kunden inte godkänner ett nytt underordnat personuppgiftsbiträde. Kunden får då enbart rätt att säga upp onlinetjänst, programvaruprodukt, programvarutjänst eller licens. Om den berörda produkten ingår i en svit (eller liknande enskilt köp av tjänster) är uppsägningen tillämplig på hela sviten.

Genomgång av anlitade underordnade personuppgiftsbiträden

För att bättre kunna bedöma omfattningen och lokalisering av Microsofts användning av underordnade personuppgiftsbiträden har vi gjort en genomgång av dokumenten *Microsoft Online Services Subprocessors*, daterat 2025-02-28, och *Microsoft Commercial Support Subprocessors*, daterat 2025-03-10.

En övervägande del av de redovisade biträdena finns i tredje länder, varav större delen saknar adekvat skyddsnivå enligt GDPR. Nedan följer en genomgång av hur utkontrakteringen är fördelad utifrån länder.

Microsoft Online Services Subprocessors

Microsofts användande av underordnade personuppgiftsbiträden för behandling av kunddata och (pseudonymiserad) personliga data i Microsoft Online Services regleras i dataskyddsavtalet (DPA).

Underleverantörerna kategoriseras enligt följande funktionella områden:

1. *Driftar integrerad molnteknologi*

Totalt 7 underleverantörer lokaliserade i:

- Irland: 1
- Nederländerna: 1
- USA: 5

2. *Tillhandahåller anknutna tjänster*

Totalt 6 underleverantörer lokaliserade i:

- Irland: 1
- USA: 5

3 Tillhandahåller kontraktsanställd personal

Totalt 34 underleverantörer lokaliserade i:

- Irland: 2
- Israel: 1
- Indien: 3
- Kina: 1
- Cypern: 1
- USA: 26

4. *Infrastruktur (Data center)*

Totalt 35 underleverantörer, uppdelade i förhållande till GDPR:

- Inom EU/EES: 15
- USA: 1
- Länder med EU-kommissionens beslut om adekvat skyddsnivå: 6
- Övriga tredjeland utan adekvat skyddsnivå: 13

Microsoft Commercial Support Subprocessors

Microsofts organisation för Commercial Support (inklusive dotterbolag) arbetar med Microsoft Services Support offerings, vilket inkluderar Premier support och Microsoft Unified support. Commercial Support använder subprocessors för vad som av Microsoft beskrivs som vissa begränsade funktioner.

Uppdelning och fördelning av länder:

1. *Outsourced to provide contact/call center services:*

- Huvudkontor med 7 dotterbolag i USA
- Dotterbolag i 4 länder med adekvat skyddsnivå
- Dotterbolag i 4 övriga tredjeländer
- Dotterbolag i 3 EU-länder

(Totalt: 18)

2. *Additional staffing:*

- Huvudkontor med 29 dotterbolag i USA
- Dotterbolag i 4 länder med adekvat skyddsnivå
- Dotterbolag i 8 övriga tredjeländer
- Dotterbolag i 36 EU-länder

(Totalt: 77).

3. *Subsidiary Affiliates (dotterbolag):*

- Huvudkontor och dotterbolag i USA (1)
- Dotterbolag i 27 EU-länder
- Dotterbolag i 9 länder med adekvat skyddsnivå
- Dotterbolag i 67 övriga tredje länder

(Totalt: 104).

Sammanfattning

Microsoft har reglerat överföring av personuppgifter till tredjelandsöverföring på olika sätt, huvudsakligen genom Microsoft certifiering för EU: s–USA: s dataskyddsramverk, leverantörsavtal och EU: standardavtalsklausuler (SCC).

Microsoft låter egna dotterbolag och andra underordnade personuppgiftsbiträden behandla kunders personuppgifter. En övervägande del av dessa finns i tredje länder, varav större delen saknar adekvat skyddsnivå. Underordnade biträden omfattas visserligen av standardavtalsklausuler (SCC), men sådana tar inte bort risken för att vidareutnyttjande och röjande av personuppgifter inte ske. Microsoft har inte presenterat någon utredning av vilka risker som finns för röjande av kundens uppgifter till följd av lagstiftning i de länder där respektive biträde har sin verksamhet.

5. Bedömning

5.1 Bedömning av företagsskyddet

Microsofts företagsskydd innebär en förbättrad hantering av stadens data utifrån informationssäkerhet och dataskydd. Det bidrar även till en förbättrad hantering av efterlevnad av dataskyddsregelverk, bland annat genom att tydliggöra ansvarsgränserna i Microsofts dataskyddsavtal (DPA). Inom ramen för Microsoft 365 Copilot Chat innebär detta bland annat att Microsoft åtar sig att inte använda kunddata för att träna sina AI-modeller, samt att agera som personuppgiftsbiträde enligt villkoren i sitt dataskyddsavtal (DPA). Kombinationen av DPA och Microsofts produktvillkor skapar ett strukturerat men standardiserat ramverk för dataskydd.

För de delar av Microsoft 365 Copilot chatt som inte är kopplade till externa tjänster, såsom Bing, bedöms att det finns ett visst avtalsmässigt skydd som kan bidra till rättssäker behandling, under förutsättning att behandlingen sker helt inom Microsoft 365-miljön och på kundens instruktion.

Trots detta är vår samlade bedömning att företagsskyddet i sin nuvarande utformning inte är tillräckligt för att lösa ut de risker som kvarstår, särskilt vid användning av Microsoft 365 Copilot chatt. Tjänsten är fristående men den kan interagera och interagerar med information som användaren aktivt tillför i sina kommandon, exempelvis via öppnade dokument, webbsidor eller teams-konversationer. Det innebär att Microsoft i vissa fall får åtkomst till innehåll som kan vara skyddsvärt enligt offentlighets- och sekretesslagen eller GDPR. Detta aktualiserar särskilda risker kopplade till ändamålsbegränsning, bristande insyn i den tekniska databehandlingen samt behovet av faktisk rättslig kontroll över hur information hanteras.

Därtill förbehåller sig Microsoft rätten att ensidigt ändra innehållet i sina produktvillkor, vilket innebär att de avtalsvillkor som företagsskyddet vilar på kan komma att justeras utan att på förhand godkännas av kunden. Detta innebär att skyddets innehåll och räckvidd kan förändras utan att kunden får möjlighet att påverka detta. För en myndighet, som Intraservice, med högt ställda krav på rättslig förutsägbarhet, avtalsmässig stabilitet och långsiktig efterlevnad av interna regelverk utgör detta en väsentlig osäkerhetsfaktor.

Vidare framgår det att när Microsoft 365 Copilot chatt använder Bing för extern informationshämtning agerar Microsoft som självständig personuppgiftsansvarig. Det innebär att frågeinnehåll och viss teknisk metadata kan komma att behandlas utanför Intraservices kontroll, utan att myndigheten att möjlighet att begränsa ändamålet eller omfattningen av behandlingen. Eftersom någon föregående sekretessprövning inte sker saknas också förutsättningar för att säkerställa en rättssäker informationshantering. Sådan behandling kan även medföra överföring av data till tredje land utan att detta är tydligt reglerat. Sammantaget innebär detta en väsentligt förhöjd risk för att information behandlas i strid mot Offentlighet- och sekretesslagen när det gäller uppgifter som omfattas av sekretess.

En ytterligare risk utgörs av att användare, genom fri textinmatning i Microsoft 365 Copilot chatt, oavsiktligt lämnar ut känslig eller sekretessbelagd information. Eftersom Microsoft 365 Copilot chatt bygger på användarens egna formuleringar, frågor och kommandon, finns det en inneboende risk att information som inte är avsedd att delas behandlas av tjänsten.

Det är därför av avgörande betydelse att användare har tydliga riktlinjer och förståelse för vilken typ av information som är lämplig att mata in i tjänsten. Denna risk kräver att Microsoft 365 Copilot chatt endast används inom definierade ramar, med stöd av utbildning, interna rutiner och tekniska begränsningar där så är möjligt.

Intraservice har genomfört en strukturerad och dokumenterad riskanalys av tjänsten. Av den genomförda riskbedömningen framgår att nödvändiga organisatoriska säkerhetsåtgärder ännu inte har implementerats. Detta medför en ökad osäkerhet ur ett GDPR- och offentlighetsperspektiv, särskilt vad gäller behandlingsändamål, lagringsperioder och vidareanvändning av data. Eftersom Microsoft 365 Copilot chatt baseras på fri textinmatning från användaren och kan involvera funktioner som faller utanför det avtalsreglerade företagsskyddet, exempelvis sökningar via Bing, finns en risk att data behandlas i syften eller sammanhang som inte styrs av användarens instruktioner eller av tillämpliga dataskyddsregler. Detta innebär att vissa behandlingar kan ske utanför Intraservice kontroll, vilket försvårar möjligheten att säkerställa rättssäker informationshantering.

Vidare konstateras att en övervägande del av Microsofts underleverantörer är lokaliserade i tredje land, länder som saknar adekvat skyddsnivå enligt GDPR eller tillräckligt skydd enligt annan relevant lagstiftning. Även om Microsoft anger att man har säkerställt tillräckliga skyddsmekanismer för kundens personuppgifter är det vår bedömning att en väsentlig del av risken för röjande och vidare utnyttjande av uppgifter kvarstår. I det underlag vi har gått igenom framgår det ingenstans huruvida Microsoft har utrett om rättsordningen i de respektive länder där underleverantörer har sitt hemvist kan leda till risk för röjande av kundens data.

En särskild problematisk aspekt är att Microsofts förbehåller sig rätten att anlita underordnade personuppgiftsbiträden som är lokaliserade i tredje land, utan att kunden har någon reell möjlighet att invända. Det enda alternativet som erbjuds är att säga upp den aktuella tjänsten eller hela produktsviten. Med hänsyn till den inlåsning som ofta föreligger kan ett upphörande av användande blir svårt att genomföra. Som en följd av detta kan bedömning och åtgärder av risker påverkas eftersom det saknas alternativa sätt att behandla data. Denna praktiska oförmåga att välja bort en viss leverantör innebär att Intraservice kan tvingas acceptera risknivåer som annars inte skulle godtas, vilket påverkar möjligheten att fatta välgrundade beslut om riskhantering och behandling av personuppgifter.

Mot bakgrund av ovan finns det även anledning att uppmärksamma den rättsliga osäkerhet som uppstår när centrala avtalsvillkor kan ändras ensidigt av leverantören. Myndigheter är enligt bl.a. regeringsformen och GDPR bundna av krav på rättslig förutsebarhet, ansvarsfördelning och kontroll över personuppgiftsbehandlingen. Därtill kan det påverka myndighetens möjlighet att upprätta rättssäkra rutiner. Även svårighet att frånträda avtal av praktiska skäl kan innebära risk för användning av produkter utan eller med begränsat stöd i lag.

Det står klart att risken för att känslig eller sekretessreglerad information bearbetas eller delas utan att Intraservice ges möjlighet att utöva kontroll eller genomföra en egen sekretessprövning är återkommande i förvaltningens bedömningar av centrala IT tjänster eller molnplattformar som tillhandahålls av Microsoft. Särskilt i de delar av tjänsten där behandling sker utanför dataskyddsavtalet, exempelvis genom integration med Bing, försvåras möjligheten att säkerställa rättssäker informationshantering enligt krav i GDPR och offentlighets- och sekretesslagen.

Utöver de osäkerheter som identifierats kring interaktionen i Microsoft 365 Copilot chatt, visar riskanalysen även att Intraservice ännu inte har genomfört de planerade organisatoriska åtgärder som krävs för att hantera de strukturella risker som följer av Microsofts användning av tredjelandsbaserade underleverantörer. Det gäller bland annat utbildningsinsatser och rutiner som rör informationsklassning och hantering av känsliga uppgifter.

En särskilt kvarstående risk är att Intraservice, till följd av Microsofts rätt att låta underleverantörer i tredje land behandla personuppgifter, förlorar faktisk och rättslig kontroll över viss databehandling. En majoritet av dessa leverantörer är lokaliserade i länder som saknar adekvat skyddsnivå enligt GDPR. Trots att Microsoft hänvisar till standardavtalsklausuler och andra skyddsmekanismer, bedömer vi att det fortfarande föreligger en väsentlig risk för att personuppgifter kan röjas eller utnyttjas vidare i strid med EU-rätten och svensk lagstiftning.

5.3 Rekommendation

Mot bakgrund av de rättsliga och säkerhetsrelaterade risker som identifierats i den genomförda analysen är det vår bedömning att det i nuläget finns skäl att tillämpa försiktighetsprincipen i frågan om huruvida Microsoft 365 Copilot Chatt bör göras tillgänglig inom organisationen.

Tjänsten är förknippad med flera osäkerhetsmoment som inte kan anses förenliga med de krav på rättssäkerhet, insyn, ansvarsfördelning och dataskydd som gäller för en offentlig aktör enligt GDPR och offentlighets- och sekretesslagen. Särskilt allvarliga är den bristande kontrollen över tredjelandsöverföringar, risken för att sekretessreglerad information behandlas utan föregående prövning, samt Microsofts möjlighet att ensidigt ändra avtalsvillkor utan kundens medgivande.

Microsofts företagsskydd erbjuder i sin nuvarande utformning inte tillräckliga avtalsrättsliga eller tekniska garantier för att uppfylla kraven på rättslig kontroll och informationssäkerhet. Så länge dessa brister kvarstår bör tjänsten endast övervägas med stor försiktighet och inte tas i bruk utan att ytterligare skyddsåtgärder vidtagits.

Vid ett framtida övervägande om införande behöver Intraservice säkerställa att samtliga relevanta tekniska och organisatoriska skyddsåtgärder är fullt implementerade. Ett införande bör dessutom föregås av en uppdaterad och fördjupad risk- och konsekvensanalys.

Återstående bedömningar

Vi har i vår bedömning inte vägt risker i form av brister i uppfyllande av juridiska krav mot funktion, nytta, kostnader eller effektivitet kopplat till om Microsoft 365 Copilot Chatt ska tas i bruk. Den här bedömningen kan dock bidra med en del av underlaget för en sådan bedömning.

Hala Zeidan, förvaltningsjurist

Henrik Hoffmeister, förvaltningsjurist