Utredningsrapport om hantering av Microsoft 365 Copilot chatt i Göteborgs stad

2025-06-15
Dnr 0244/25

Bakgrund

Användare i staden hade tillgång till Microsoft 365 Copilot chatt under 2024. I början av 2025 framkom risker med att använda Copilot chat i Edge, och ungefär samtidigt tillkom nya funktioner. Intraservice beslutade då att stänga av Microsoft 365 Copilot chatt tillfälligt för att göra en utredning om hur säkerheten i tjänsten kan förbättras.

Utredningens mål:

- Ge en övergripande beskrivning av funktionerna och den potentiella nyttan med Microsoft 365 Copilot chatt, både i appen och i Edge.
- Identifiera och dokumentera säkerhetsrisker kopplade till användningen av Microsoft 365 Copilot chatt i appen och i Edge, samt föreslå konkreta tekniska och organisatoriska åtgärder för att minimera riskerna.
- Ta fram en rekommendation och införandeplan i det fall funktionerna kan erbjudas till förvaltningar och bolag på ett säkert sätt.

Sammanfattning

Den 30 januari 2025, beslutade Intraservice att tillfälligt stänga av den generativa AI-chatten Microsoft 365 Copilot chatt på grund av identifierade säkerhetsrisker och starta en utredning kring användningen av Microsoft 365 Copilot chatt i Göteborgs stad. Beslutet grundades på behovet av en djupare analys av eventuella risker samt en säker och kontrollerad hantering av funktionen innan den kan återinföras.

På uppdrag av verksamhetschef för digital arbetsplats har enheten för informationssäkerhet gjort en hot- och riskanalys tillsammans med medarbetare från tjänsten Office 365 och klientplattform. Parallellt med detta har tjänsten Office 365 fört en dialog med den taktiska referensgruppen för Office 365, som består av kontaktpersoner från ett urval av förvaltningar/bolag i staden, kring identifierade risker och möjliga åtgärder.

Två möten med Microsoft har genomförts, där Microsoft beskrivit hur deras företagsskydd (Enterprise Data Protection) är uppbyggt samt vad som omfattas av EU Data Boundary. I dessa samtal har medarbetare från enheterna samarbetsplattform, klientplattform, och informationssäkerhet deltagit, samt stadens dataskyddsombud,

förvaltningsjurister från Intraservice och även stadens CISO/informationssäkerhetsansvarig.

Utifrån genomförd analys kan Microsoft 365 Copilot chatt, med rätt organisatoriska och tekniska förutsättningar, möjliggöra ökad effektivitet och stärkt digital arbetsmiljö. Risker för verksamheten behöver dock bedömas i en lokal tröskelanalys.

Bedömning ur ett ekonomiskt perspektiv

Ur ett ekonomiskt perspektiv innebär ett beslut att stoppa Microsoft 365 Copilot chatt inom Göteborgs Stad att man avstår från att utnyttja en redan inkluderad del i den licens som samtliga förvaltningar och 14 bolag redan betalar för. Den ekonomiska effekten blir i det fallet ett minskat värde på investeringen. Kostnaden för licenserna kvarstår oavsett om AI-chatten används eller inte, vilket gör att nyttjandegraden av Microsoft 365-licensen sjunker. I praktiken innebär det att Göteborgs Stad betalar för ett verktyg utan att dra nytta av dess kapacitet.

Vidare finns det en potentiell kostnadsbesparing i form av effektivisering av dagliga administrativa arbetsuppgifter. Microsofts 365 Copilot chatt är designad för att, snabba upp informationssökning, sammanfatta dokument, skapa utkast och förbättra beslutsstöd. Om användare inte får tillgång till dessa verktyg kan det leda till att tid och resurser fortsätter att läggas på manuella uppgifter, vilket i sin tur minskar produktiviteten och ökar personalkostnader över tid. Det kan också göra att vissa arbetsuppgifter tar längre tid än nödvändigt, särskilt inom administration, dokumenthantering och informationsbearbetning.

Dessutom finns det en risk att förvaltningar eller individer börjar använda andra leverantörer av generative AI-chattar utanför den Microsoft-reglerade miljön om Copilot chatt inte tillåts. Det kan i förlängningen leda till ökade IT-kostnader för hantering av icke-standardiserade verktyg, behov av ytterligare utbildningsinsatser, samt ökad supportbelastning och osäkerhet kring dataskydd och regelefterlevnad. Sådana alternativa lösningar innebär ofta separata kostnader för licenser eller abonnemang, och ofta utan samma nivå av säkerhetsintegration som Microsoft erbjuder.

Sammanfattningsvis är det ur ett ekonomiskt perspektiv inte gynnsamt att blockera Microsoft 365 Copilot chatt, givet att staden redan investerat i Microsofts plattform. Att inte använda verktyget innebär en förlust av potentiell effektivisering, ökade indirekta kostnader, och risk för teknisk fragmentering mellan förvaltningar. Ur ett ekonomiskt perspektiv framstår det som mer ändamålsenligt att möjliggöra en kontrollerad och behovsstyrd användning av Copilot chatt, snarare än att upprätthålla ett generellt förbud. Detta för att säkerställa att stadens licensinvestering nyttjas fullt ut och att verksamheterna ges möjlighet till effektivisering samt minimera risken för användning av lösningar som inte ingår i stadens portfölj.

Bedömning ur ett socialt perspektiv

Ur ett socialt perspektiv aktualiserar frågan om återaktivering av Microsoft 365 Copilot chatt flera centrala aspekter kopplade till den organisatoriska arbetsmiljön, användarnas digitala förutsättningar och stadens övergripande ambition att vara en modern, inkluderande och effektiv arbetsgivare.

Copilot chatt erbjuder inte enbart teknisk funktionalitet – det är också ett verktyg som kan bidra till att förändra sättet medarbetare arbetar, kommunicerar och utvecklar sin kompetens. En återaktivering av funktionen har därför potential att stärka det sociala samspelet i den digitala arbetsmiljön. Genom att tillhandahålla ett tillgängligt AI-stöd i vardagen kan medarbetare få hjälp med att förstå, formulera, bearbeta och strukturera information, vilket särskilt kan gynna yrkesgrupper med hög kognitiv belastning eller tidsbrist.

Det finns även ett tydligt kompetensfrämjande värde. Användningen av Copilot chatt kan bidra till att öka den digitala mognaden hos personalen, och skapa en lärande kultur där AI betraktas som ett stöd snarare än ett hot. Verktyget kan fungera som en pedagogisk resurs som förstärker individens förmåga att navigera i komplex information, vilket är särskilt betydelsefullt i en kunskapsintensiv offentlig verksamhet.

Samtidigt måste jämlikhet och tillgänglighet beaktas. Ett fortsatt avstängt verktyg riskerar att förstärka digitala klyftor mellan olika verksamheter och yrkesroller. Medarbetare som i sin yrkesutövning skulle ha särskilt stor nytta av AI-stöd – exempelvis i dokumentationstunga funktioner – fråntas möjligheten att arbeta mer resurseffektivt. Detta kan i förlängningen påverka upplevd rättvisa och arbetsbelastning negativt, vilket även är en arbetsmiljöfråga.

En relevant social risk vid ett fortsatt avstängande av Microsoft 365 Copilot chatt är att det kan bidra till ett ökat stresspåslag bland medarbetare som upplever att de halkar efter i den digitala utvecklingen. När andra organisationer eller externa aktörer får tillgång till AI-stöd som effektiviserar och förenklar arbetsuppgifter, kan känslan av otillräcklighet och prestations press förstärkas hos dem som saknar samma verktyg. Detta gäller särskilt i verksamheter med hög arbetsbelastning och krav på snabb informationshantering. Att stå utanför en teknisk utveckling som är på väg att bli norm i moderna arbetsmiljöer kan påverka både självkänsla och arbetsmotivation negativt, vilket i sin tur kan bidra till ökad psykisk belastning och sämre arbetsmiljö över tid.

Samtidigt bör det betonas att stresspåslag relaterat till teknisk utveckling inte är unikt för detta verktyg, utan är en känd och hanterbar utmaning vid införande av nya digitala arbetsstöd. Genom riktade insatser för utbildning, praktisk introduktion och löpande användarstöd kan denna risk mildras betydligt, och i stället bidra till ökad trygghet och självtillit bland medarbetarna i deras digitala arbetsmiljö.

Dessutom påverkar tillgången till moderna arbetsverktyg Göteborgs Stads attraktivitet som arbetsgivare. För att kunna rekrytera och behålla kompetens, särskilt bland yngre och digitalt vana medarbetare, är det av betydelse att erbjuda verktyg som ligger i linje med samtida arbetssätt. Att permanent avstå från AI-stöd riskerar att signalera en avvaktande eller konservativ hållning till innovation, vilket kan påverka hur staden uppfattas av nuvarande och potentiella medarbetare.

Sammantaget innebär en återaktivering av Microsoft 365 Copilot chatt en möjlighet att främja en mer inkluderande, kompetensutvecklande och framtidsinriktad digital arbetsmiljö. Med rätt vägledning, utbildning och etiska ramar kan funktionen integreras på ett sätt som stärker både individens arbetsvardag och organisationens sociala hållbarhet.

Övergripande beskrivning av Microsoft 365 Copilot Chatt

Microsoft 365 Copilot chatt är en generativ AI-chat liknande ChatGPT som användare kan nå på två sätt: som en app via Microsoft 365 på webben och i webbläsaren Edge.

Microsoft 365 Copilot chatt i Edge kan dessutom användas för att sammanfatta en webbsidas innehåll, vilket i sig är potentiell risk om användaren har öppnat en webbapplikation som kan innehålla känslig information, ex Treserva.

Riskerna som har identifierats handlar om att medarbetare kan lägga in känslig information i chatten. All information som läggs in bearbetas i Microsofts molntjänst. Informationen är skyddad genom avtal med Microsoft, men trots detta går det inte att bortse från att bearbetningen i molnet kan innebära en risk för att känslig information exponeras i Microsofts molntjänster.

Funktionsbeskrivning

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

Copilot chatt har inte per automatik, åtkomst till användarens eller stadens samlade dokument eller information lagrad i Microsoft 365 miljö. För att Copilot chatt ska kunna bearbeta innehållet i en specifik fil krävs att användaren aktivt väljer att bifoga filen till chattfunktionen. Det är bara användaren som kan se sina egna frågor och svar och de används inte i några andra sammanhang.

Användarens data skyddas av Microsofts företagsskydd, läs mer under punkt 0. En förutsättning är att användaren är inloggad med sitt arbets- eller skolkonto.

Bifoga filer i Copilot chatt appen
Copilot chatt har en funktion för att bifoga filer. Om användaren bifogar en fil skapas en kopia på användarens Onedrive. I chatfönstret kan användaren välja att bifoga en fil, och därefter ställa frågor mot filens innehåll. Filens innehåll lagras tillfälligt i Copilot chatts minne under den pågående chattsessionen. Filens innehåll raderas i chattsessionens minne när användaren antingen startar om chatsessionen genom knappen ”Ny chatt”, eller genom att stänga webbläsaren. Det räcker inte att enbart stänga webbfliken. Chatsessionens innehåll, det vill säga användarens frågor och svaren man fått, finns kvar men filens innehåll är raderat och användaren kan inte längre ställa frågor mot den.

Microsoft 365 Copilot chatt i Edge
I webbläsaren Microsoft Edge är det möjligt att använda Copilot chatt i webbläsarens sidofönster. Sidofönstret är enkelt att starta och komma åt direkt i webbläsaren genom att

klicka på en ikon för Copilot chatt längst upp till höger i webbläsarfönstret. Om användaren öppnar ett supporterat dokumentformat i webbläsaren, såsom en PDF-fil, syns en ”Fråga Copilot”-ikon för att öppna sidofönstret.

Sammanfatta sidoinnehåll i Edge
Copilot chatt i sidofönstret i Edge har en funktion där användaren kan be Copilot chatt att sammanfatta information på den webbläsarflik som är öppen. Det innebär att Copilot chatt, i det fall användaren ber om det, läser in innehållet på den webbläsarflik som är öppen, och svarar med en sammanfattning. Sammanfattningsfunktionen finns även när man öppnar ett supporterat dokumentformat i webbläsaren.

För att Copilot chatt i Edge ska summera ett sidinnehåll kan man antingen välja snabbknappen ”Skapa en sammanfattning” eller med fritext skriva i verktygets chattfönster att man önskar en sammanfattning av sidan. Copilot chatt har inte tillgång till sidor som användaren inte ber verktyget att behandla.

Första gången en användare använder Copilot chatt i Edge får användaren en dialogruta. I dialogrutan finns en länk, Mer information* som tar användaren till ytterligare information om användning av Microsoft 365 Copilot chatt i Edge.

Genom att godkänna dialogrutan ges Copilot chatt tillåtelse att läsa flikens sidinnehåll i det fall användaren ber verktyget att göra det. Denna fråga ställs en gång per användare och godkännandet gäller endast på den dator som godkännandet genomfördes på. Användaren kan ta tillbaka godkännandet genom att ändra inställningen i webbläsarens inställningar.

När en sida summerats slutar Copilot chatt i Edge att läsa sidans innehåll. Det sidinnehåll som behandlas av Copilot chatt sparas tillfälligt i minnet under den pågående chatsessionen. Detta innehåll raderas automatiskt när användaren avslutar sessionen genom att antingen klicka på ”Uppdatera” eller stänga hela webbläsaren. Observera att det inte räcker att enbart stänga fliken eller sidopanelen – hela webbläsaren måste avslutas för att sessionens innehåll ska rensas helt.

Hot- och riskanalys

Enheten Informationssäkerhet fick i uppdrag av verksamhetschefen för Digital arbetsplats att göra en hot- och riskanalys på Copilot chatt *(se Bilaga 1).*

Bakgrunden till att genomföra en hot- och riskanalys för Copilot chatt grundar sig i behovet av att förstå och reducera potentiella säkerhetsrisker. Det är avgörande att identifiera säkerhetshot och sårbarheter som skulle kunna leda till oönskade händelser.

En hot- och riskanalys ger en inledande systematisk översyn av vilka informationssäkerhetsrisker som finns med användningen av Copilot chatt, inklusive risker för dataläckage eller otillräckligt dataskydd.

Omfattningen och avgränsningen gäller teknisk och logisk informationssäkerhet. Detta innebär en översyn av de säkerhetsåtgärder som innefattas i hot mot stadens information som Copilot chatt skulle kunna medföra.

En avgränsning är att analysen inte hanterar verksamhetsspecifika dataskyddsrisker eller andra juridiska hot som inte kan hanteras genom tekniska åtgärder.

Riskanalysen för Copilot chatt omfattar i nuläget två utföranden:

1. Copilot chatt i Edge, där assistenten på användarens uppmaning kan använda information från den aktuella fliken i det öppna webbfönstret genom ett sidofönster.
2. Copilot chatt – ett webbläge där assistenten använder den information man väljer att skriva in eller dela samt Bing-sökningar för att ge svar baserade på allmän internetinformation.

Målet med riskhanteringen är att belysa de tekniska aspekterna, identifiera de hot som användningen kan innebära, samt utvärdera hur dessa hot kan hanteras direkt i verktyget eller genom åtgärder som verksamhet behöver initiera.

Totalt 14 risker identifierades och togs fram åtgärder för. Vissa risker togs bort då de var dubbletter samt risker där ägandeskap och möjlighet att påverka ligger utanför tjänsten Office 365. Slutsats från hot- och riskanalysen

Analysens slutsats är att denna strukturerade ansats inte bara underlättar förståelsen av utmaningar med hot och risker för informationssäkerhet. Analysen ger också förslag för att behandla identifierade risker vidare.

Verksamheter behöver göra egna bedömningar av risker och eventuella åtgärder samt anpassa sin användning av Copilot chatt därefter.

Vidare behöver genomförbarhet bedömas av de åtgärder som föreslås för att reducera risker. Detta innefattar aspekter av kostnad, tidsåtgång, mognad, mottaglighet, kompetens, komplexitet, teknik, styrdokument, leverantörsavtal, lagar och förordningar samt politisk viljeinriktning.

Med föreslagna åtgärder kan staden återaktivera Copilot chatt för de förvaltningar och bolag som önskar det, där var och en av förvaltningarna och bolag ansvarar för egen informationshantering.

Inga risker bedömdes som höga efter att föreslagna åtgärder är införda. Rapporten i sin helhet finns i Bilaga 1

Hot och riskanalys – taktiska referensgruppen för Office 365[1]

För att uppnå en bred förankring samt säkerställa att relevanta risker identifieras har en kontinuerlig dialog förts med den taktiska referensgruppen för Office 365.

Arbetet inleddes med en gemensam riskidentifiering i samverkan med referensgruppen. Syftet var att identifiera eventuella överlapp mellan gruppens riskbedömning och den riskanalys som tidigare genomförts av Intraservice. Resultatet visade att nio av de risker som Intraservice identifierat även återfanns i referensgruppens bedömning. De risker som värderades som mest kritiska var oavsiktlig felanvändning samt förekomsten av så kallad skugg-AI.

[1] Den taktiska referensgruppen består av ett urval representanter från förvaltningar/bolag som ingår i Utvecklingsorganisationen för Microsoft 365

Referensgruppen gavs därefter möjlighet att ta del av och granska det föreslagna åtgärdspaketet. Gruppen delar Intraservices bedömning att de föreslagna åtgärderna är ändamålsenliga och bidrar till att effektivt minimera de identifierade riskerna.

Det finns en gemensam förståelse för att utbildningsinsatser utgör en avgörande komponent i det förebyggande arbetet. För att säkerställa en korrekt och säker användning av Copilot chatt kan det vara lämpligt att ta fram ett gemensamt material som riktar sig till alla användare, med syfte att beskriva både funktion, ansvarsfördelning och relevanta informationssäkerhetsrisker. Samtidigt betonades att respektive förvaltning och bolag har ett självständigt ansvar för att säkerställa att relevant kunskap sprids och tillämpas internt.

Dialog med Microsoft avseende teknisk och juridisk informationshantering

Parallellt har en strukturerad dialog förts med Microsoft i syfte att skapa klarhet kring hur information tekniskt behandlas inom ramen för Microsoft 365 Copilot, särskilt i chattfunktioner.

Detta arbete har varit avgörande för att säkerställa att de legala och säkerhetsmässiga förutsättningarna uppfyller Göteborgs Stads krav på dataskydd, informationssäkerhet och efterlevnad av tillämplig lagstiftning, inklusive GDPR och offentlighetsprincipen.

Två särskilda möten har genomförts med Microsoft representanter och Intraservice företagsjurister samt staden DSO:er: ett med fokus på **Enterprise Data Protection (EDP)** och ett på **EU Data Boundary (EUDP)**. Efter mötena har Microsoft fortsatt att bistå med svar på fördjupade frågor och kompletterande information, vilket bidragit till ökad tydlighet i hur Copilot hanterar användar- och organisationsdata.

Hantering av organisation- eller företagsdata

Enterprise data protection (EDP)
All data som genereras, samlas in eller används i en kunds Microsoft 365-miljö definieras i detta sammanhang som företagsdata. Göteborgs Stads företagsdata skyddas enligt Microsofts avtal om Enterprise Data Protection (EDP), vilket omfattar hela Microsoft 365-tjänsten – inklusive Microsoft 365 Copilot chatt.

En förutsättning för att skyddet ska gälla är att användaren är inloggad med sitt arbets- eller skolkonto. EDP innebär bland annat följande:

- Användarens chattinnehåll (såsom inmatningar och svar) omfattas av samma avtalsskydd som exempelvis e-post i Exchange eller dokument i SharePoint.
- Vid användning av sökmotorn Bing för att besvara användarinstruktioner skickas endast ett minimalt informationsunderlag. Ingen information om användaren eller organisationen inkluderas.
- Microsoft använder inte chattinnehåll för att profilera användaren.
- Vid filuppladdning till Copilot skickas inte hela filen till externa tjänster, utan endast relevanta nyckelord för att kunna besvara frågan.

- Kryptering tillämpas både vid överföring och lagring av data.
- Innehålls- eller användarinformation används uteslutande för att besvara den aktuella frågan.

Data som hanteras i Copilot används inte för att träna AI-modellens grundarkitektur.

EU Data Boundary (EUDP)
EU-datagränsen är en geografiskt definierad gräns inom vilken Microsoft åtagit sig att lagra och behandla kunddata för större kommersiella onlinetjänster. Detta omfattar all kunddata såsom text, ljud, video, bild och programvara som bearbetas genom användning av Microsofts molntjänster.

EUDP inkluderar även:

- Tjänstegenererade data, skapad vid användning av tjänsten.
- Supportdata, som kan uppstå vid ärendehantering.
- Säkerhetsdata, som används för att upptäcka och mildra cyberhot.

Vissa undantag existerar, särskilt avseende säkerhetsdata, där vissa data fortfarande kan överföras utanför EU för att upprätthålla driftsäkerheten. Denna åtkomst är strikt reglerad och kräver både ett registrerat ärende samt godkännande från behörig chef.

Sammanfattning av juridisk bedömning (Bilaga 7)

Som underlag för beslut om eventuell återaktivering av Microsoft 365 Copilot Chat har en juridisk bedömning genomförts av Intraservices förvaltningsjurister. Syftet har varit att klargöra om det företagsskydd Microsoft erbjuder för tjänsten uppfyller de rättsliga krav som gäller för offentlig verksamhet enligt dataskyddsförordningen (GDPR), offentlighets- och sekretesslagen (OSL), samt principer om rättssäkerhet och myndighetsansvar.

Avtal och företagsskydd – formell grund men ej rättsligt bindande garanti

Bedömningen visar att Microsoft erbjuder ett särskilt företagsskydd för användning av Copilot Chat i företagsmiljö. Detta skydd regleras genom Microsofts produktvillkor (Product Terms), dataskyddsavtal (Data Protection Addendum, DPA) och andra tillhörande dokument. Inom denna avtalsstruktur åtar sig Microsoft bland annat att:

- inte använda kunddata för att träna sina AI-modeller
- agera som personuppgiftsbiträde enligt GDPR
- kryptera data under överföring och vid lagring
- tillämpa tekniska och organisatoriska skyddsåtgärder
- hålla kunddata inom EU genom initiativet EU Data Boundary

Skyddet är dock fullt ut avtalsbaserat och saknar rättslig status i form av externa garantier eller myndighetsprövade säkerhetsstandarder. Microsofts företagsskydd är ensidigt definierat av leverantören och kan därmed ensidigt förändras genom uppdateringar i

villkoren, utan att kunden har möjlighet att påverka innehållet. Detta skapar en osäkerhet kring skyddets långsiktiga stabilitet och rättsliga förutsägbarhet.

Juristbedömningen identifierar ett flertal områden där företagsskyddet inte anses tillräckligt ur ett rättssäkerhets- och dataskyddsperspektiv:

Tredjelandsöverföringar och underbiträden i osäkra jurisdiktioner
En majoritet av Microsofts underleverantörer är lokaliserade i tredje land, inklusive länder utan adekvat skyddsnivå enligt GDPR. Även om Microsoft hänvisar till standardavtalsklausuler (SCC) och andra skyddsmekanismer, konstaterar juristerna att det inte går att verifiera om dessa skydd i praktiken uppfyller kraven. Risken för obehörigt röjande av information kvarstår, särskilt eftersom kundens möjlighet att invända mot underbiträden är starkt begränsad – det enda alternativet är att säga upp tjänsten i sin helhet.

Brister i kontroll över avtalsförändringar
Microsoft har rätt att ensidigt ändra innehållet i produktvillkoren och DPA, vilket innebär att förutsättningarna för företagsskyddet kan ändras utan kommunens godkännande eller möjlighet till prövning i förväg. Detta är särskilt problematiskt för myndigheter som är bundna av krav på rättslig förutsebarhet och kontroll över sina informationsflöden.

Risk för felaktig informationsdelning av användare
Eftersom Copilot Chat bygger på användarens fria inmatning av text (prompts) uppstår en betydande risk att känslig eller sekretessbelagd information delas oavsiktligt. Även med riktlinjer och utbildning kvarstår detta som en inneboende användarrisk. Microsoft påpekar att ansvaret för att inte dela känslig information ligger på kunden, men detta fritar inte myndigheten från det juridiska ansvaret enligt GDPR och OSL.
Mot bakgrund av de rättsliga och säkerhetsmässiga osäkerheter som identifierats rekommenderar förvaltningsjuristerna att försiktighetsprincipen tillämpas.

Sammanfattningsvis av den juridiska bedömningen:

- Microsoft agerar som personuppgiftsbiträde enligt GDPR.
- Skyddet baseras på avtal, inte lagstadgade garantier.
- Kundens möjlighet att påverka är begränsad.
- Staden bär fortsatt ansvar för informationshanteringen.
- Försiktighetsprincipen föreslås som tillämpning

Bemötande av synpunkter på bristande kontroll över avtalsförändringar

Brister i kontroll över avtalsförändringar
I den juridiska bedömningen lyfts det som en betydande brist att Microsoft, i egenskap av leverantör, har möjlighet att ensidigt uppdatera sina produktvillkor och dataskyddsavtal (DPA), utan att kunden ges reell möjlighet att påverka förändringarnas innehåll. Detta bedöms skapa en osäkerhet kring skyddets långsiktiga omfattning och tillämpning, särskilt i en offentlig kontext där rättssäkerhet och förutsebarhet är grundläggande krav.

Tjänsten instämmer i att förutsebarhet och kontroll över villkor för informationshantering är särskilt viktiga inom offentlig sektor. Samtidigt är det av betydelse att sätta denna avtalskonstruktion i sitt sammanhang. Rätten för leverantörer att uppdatera villkor

ensidigt – inom ramen för licensbaserade molntjänster – är idag en etablerad och nödvändig mekanism inom tekniskt komplexa och snabbt föränderliga IT-tjänster.

Bakgrunden till denna modell är att tekniska funktioner, säkerhetsstandarder och regulatoriska krav förändras i hög takt. För att leverantören ska kunna åtgärda sårbarheter, införa förbättrade skyddsåtgärder och anpassa tjänsten till nya lagkrav krävs en flexibel avtalsstruktur. Utan möjlighet till villkorsuppdateringar i takt med den tekniska utvecklingen, skulle avtalet riskera att snabbt bli föråldrat och därmed otillräckligt som skyddsinstrument – inte minst ur ett dataskyddsperspektiv.

Eftersom detta är en viktig synpunkt när det gäller Microsoft 365 Copilot chatt som är i sammanhanget en relativ ny funktion som fortfarande fortsätter utvecklas, har kompletterade frågor ställts till Microsoft. Deras svar om hur Commercial Data Protection (som skyddet för Bing Chat Enterprise hete i september 2023) har utvecklats för att på bättre sätt anpassas i takt med tjänsten, finns att läsa i helhet i Bilaga 6: Lista över förbättringar Microsoft 365 Copilot Chat 250522

Det är även värt att notera att denna avtalsmodell inte är unik för Microsoft, utan återfinns brett i branschen – särskilt bland leverantörer av molnbaserade prenumerationstjänster där funktionalitet uppdateras löpande. I praktiken innebär detta att kunden informeras om väsentliga förändringar i förväg och ges möjlighet att avsluta tjänsten om de inte godtas, vilket utgör ett branschpraxisbaserat balansförhållande mellan leverantörens behov av utveckling och kundens rätt till insyn.

Mot denna bakgrund menar tjänsten att avtalsvillkorens uppdateringsmekanismer inte i sig bör ses som ett avgörande hinder för att använda Microsoft 365 Copilot chatt, utan som ett uttryck för den typ av levande och dynamisk avtalshantering som krävs för moderna IT-tjänster. Däremot bör förändringar av större betydelse följas upp genom intern kontroll och – där så krävs – lokala konsekvensbedömningar i enlighet med den tröskelanalysmodell som nu föreslås.

Risk för felaktig informationsdelning av användare
I sammanhanget är det också viktigt att erinra om den grundläggande principen i GDPR: att risker ska hanteras, inte nödvändigtvis elimineras. Det är varje personuppgiftsansvarigs uppgift att göra en proportionell bedömning av risk i förhållande till nyttan, skyddsåtgärder och informationsklassning.
Förvaltningsteamets bedömning är att de risker som återstår i dagsläget är hanterbara, förutsatt att:

- funktionaliteten används inom ramen för stadens informationsklassningsmodell och gällande säkerhetsrutiner,
- interna riktlinjer begränsar användningen av Copilot Chat för känslig eller sekretessbelagd information, och
- Göteborgs Stad aktivt följer rättsutvecklingen, särskilt kopplat till tredjelandsöverföringar, EU–USA:s Data Privacy Framework och Microsofts avtalsuppfyllelse.

Däremot bör förändringar av större betydelse följas upp genom intern kontroll och – där så krävs – lokala konsekvensbedömningar i enlighet med den tröskelanalysmodell som nu föreslås.

Input från representanter från stadens verksamheter
Företrädare (IT-chefer och utvecklingsledare IT) för Göteborgs Stads förvaltningar och bolag har tagit del av den juridiska bedömningen avseende Microsoft 365 Copilot chatt och dess företagsskydd. De uppskattar det arbete som lagts ned på att analysera de rättsliga ramarna och avtalsriskerna, men anser att rekommendationen behöver vägas noggrant mot stadens övergripande digitaliseringsmål och de verksamhetsmässiga behov som finns i deras respektive organisationer.

Skribenterna påpekar att de avtalsvillkor och risker som lyfts fram för Microsoft 365 Copilot chatt i stort sett är desamma som redan gäller för den Microsoft 365-plattform som staden använder sedan flera år. Vidare uttrycker de en oro för att en alltför restriktiv juridisk bedömning, som inte tillräckligt väger risker mot potentiell nytta, kan leda till att ansvaret för komplexa teknikbeslut skjuts över på enskilda nämnder och bolagsstyrelser. De anser att Intraservice, som stadens IT-expertorgan, bör erbjuda ett balanserat och proaktivt strategiskt underlag, inte bara identifiera risker.

Det har noterats att även om kommentarerna i Bilaga 9, som är författade av företrädare för stadens verksamheter, kanske inte är fullständigt förankrade i respektive förvaltnings- och bolagsledning, så utgör de en viktig synpunkt i det fortsatta arbetet med frågan.

Sammanfattning av DSO:s rapport (Bilaga 8, 2025-05-17)

Dataskyddsombudet (DSO) har, på begäran av Intraservice, granskat riskanalysen för Microsoft 365 Copilot Chat samt Microsofts EU Data Boundary (EUDP). Bedömningen bygger på tidigare rapporter och rekommendationer samt en genomgång av identifierade dataskyddsrisker.

Centrala ståndpunkter från DSO:

- DSO avråder från att aktivera Microsoft 365 Copilot Chat i nuläget med hänvisning till bristande rättsliga förutsättningar.
- Riskanalysen bedöms vara otillräcklig och missvisande – flera tidigare påtalade risker har inte hanterats.
- DSO efterlyser konkreta tekniska skyddsåtgärder, snarare än ett ensidigt fokus på slutanvändarens ansvar.
- Det finns oklarheter kring tredjelandsöverföringar och Microsofts roll som personuppgiftsansvarig, särskilt i samband med Bing-anrop.
- DSO menar att problemen inte är begränsade till Copilot Chat, utan gäller hela O365-miljön, vilket kräver övergripande organisatoriska åtgärder.

Trots den viktiga roll dataskyddsombudet spelar enligt GDPR artikel 39, finns flera skäl att problematisera deras slutsatser:

Övertolkning av riskbilden
DSO tolkar att Microsoft får tillgång till känslig information även utan att användaren aktivt engagerar Copilot, och att detta skulle ske utanför stadens kontroll. Denna tolkning saknar teknisk bevisning. Microsoft har i sin dokumentation tydliggjort att tillgång till

webbsidans innehåll kräver aktivt godkännande från användaren, och dessutom är begränsad till specifika Copilot-lägen (t.ex. Edge Copilot).

Brister i proportion och differentiering
DSO gör ingen tydlig åtskillnad mellan:

- Copilot Chat i Office-appar (t.ex. Word/Outlook), där användardata omfattas av EDP-avtalet och skyddas inom O365-miljön.
- Copilot Chat för webben, där Bing används och där annan juridisk modell gäller.

Alla dessa användningsfall klumpas ihop i en generaliserad riskbedömning. Ett mer nyanserat angreppssätt vore att bedöma olika användningsscenarier separat.

Undervärdering av utbildning och riktlinjer
DSO förkastar utbildning som riskreducerande åtgärd för felaktig användning. Detta är inte i linje med modern säkerhetspraxis, där ”human firewall”-principen erkänns som en grundpelare. Flertalet av de högt klassade riskerna i analysen är direkt kopplade till användarbeteende och är för sig inte begränsade till användningen av Microsoft 365 Copilot chatt.

Bristande koppling till faktisk avtalsgrund
DSO hänvisar till juridisk osäkerhet i tredjelandsöverföringar men erkänner samtidigt att juridiska experter inom förvaltningen har gjort en bedömning av avtalens rättsliga grund. Dessa juridiska slutsatser erkänns men ifrågasätts inte direkt – vilket gör den starka avrådan sårbar som beslutsgrund.

Inkonsekvent hantering av O365-plattformen
DSO lyfter en relevant poäng att vissa grundläggande dataskyddsutmaningar kan vara gemensamma för hela Microsoft 365-plattformen, och speglar en bredare osäkerhet kring hela molnplattformen. Denna utredning är dock avgränsad till de specifika risker och möjligheter som Microsoft 365 Copilot chatt introducerar. En bredare översyn av O365-plattformen hanteras i andra forum.

Förslag till användning av dataskyddsombudets synpunkter
Dataskyddsombudets synpunkter har beaktats i bedömningen och utgör ett viktigt underlag i den fortsatta hanteringen av Microsoft 365 Copilot Chat inom Göteborgs Stad. Förvaltningsteamet instämmer i att de frågeställningar som berörs är komplexa och kräver en välavvägd kombination av tekniska, juridiska och organisatoriska åtgärder.

Den rekommendation som nu lämnas – att fortsatt blockera användning av Copilot Chat i Edge-sidofältet samt att möjliggöra lokal aktivering efter genomförd tröskelanalys – bedöms på ett balanserat sätt hantera huvuddelen av de risker som identifierats av både Intraservice och den taktiska referensgruppen för Office 365. Denna modell skapar förutsättningar för att minimera högriskscenarier centralt, samtidigt som verksamheter med lägre riskprofil ges möjlighet att pröva användningen utifrån egna behov och förutsättningar.

De återstående risker som pekas ut i dataskyddsombudets yttrande – exempelvis relaterade till lokal informationsklassning, tredjelandsöverföring eller felaktig användning – anses vara hanterbara inom ramen för respektive förvaltnings eller bolags lokala tröskelanalys. Genom denna process ges varje organisation möjlighet att göra en egen

bedömning av risknivå och besluta om eventuella kompletterande skyddsåtgärder krävs innan aktivering.

Det är därmed tjänstens samlade bedömning att den föreslagna hanteringsmodellen både tar hänsyn till dataskyddsombudets synpunkter och erbjuder en praktiskt genomförbar väg framåt.

Att använda AI i Göteborgs Stad

Stadsledningskontoret har på Digitala navet publicerat stöddokumentet "Att använda AI i Göteborgs Stad", som syftar till att konkretisera hur medarbetare och chefer i Göteborgs Stad ska arbeta med AI. Målet är att främja en laglig, etisk och ansvarsfull användning av AI-system, oavsett om de är publika eller stadens egna.

Kärnan i dokumentet är nio förhållningsregler som användare måste beakta:

1. **Etiskt och ansvarsfullt användande**: Användare är alltid ansvarig för att AI används etiskt och ansvarsfullt, med människan i kontroll. Detta innefattar respekt för mänsklig autonomi, skadeförebyggande, rättvisa och förklarbarhet.
2. **Säkerhetskrav för information**: Innan ett AI-system används måste användaren säkerställa att det uppfyller säkerhetskraven för den information som ska hanteras. Utgå från att all inmatad information kan sparas och delas av leverantören.
3. **Högriskanvändning och förbjuden AI**: Vissa AI-system är helt förbjudna (t.ex. social poängsättning, kognitiv beteendemanipulation). Användning inom högriskområden (t.ex. kritisk infrastruktur, utbildning, brottsbekämpning) kräver särskilda åtgärder och utredningar av verksamheten.
4. **Sekretess och skyddsvärd information**: Användaren ansvarar för att sekretessbelagda och skyddsvärda uppgifter inte röjs. Man skall inte mata in sekretessbelagda uppgifter om systemet inte riskbedömts som säkert för det. Även sammanställd information kan bli känslig.
5. **Personuppgiftsbehandling**: Personuppgifter får endast behandlas i enlighet med dataskyddslagstiftningen (GDPR). Särskild försiktighet gäller för känsliga personuppgifter.
6. **Ansvar för resultat**: Användaren är alltid ansvarig för resultatet som AI-systemet skapar och hur det används. AI-genererat material ska ses som utkast som kräver noggrann kontroll och faktagranskning. Texter ska vara professionella, sakliga och opartiska.
7. **Transparens och förtroende**: AI-genererat material ska användas ansvarsfullt och transparent för att upprätthålla förtroendet för stadens verksamhet. Ange tydligt om bilder, filmer, ljud eller helt AI-genererad text (som inte bearbetats av människa) är AI-skapad. Använd inte AI olämpligt eller bara för sakens skull.
8. **Allmänna handlingar**: Information som matas in och resultat som erhålls kan utgöra allmänna handlingar. Rättsläget är oklart, men utgå från att både promptar och resultat kan behöva lämnas ut. Verksamheten behöver rutiner för hantering.

9. **Upphovsrätt**: Upphovsrätten måste respekteras. Mata inte in upphovsrättsskyddat material utan tillåtelse. Instruera inte AI att bryta mot upphovsrätten. Var försiktig med att sprida AI-genererat material då det kan inkräkta på andras rättigheter.

AI-riktlinjen "Att använda AI i Göteborgs Stad"[2] fungerar som ett övergripande ramverk som fastställer de generella principerna, ansvarsfördelningen och försiktighetsåtgärderna för all AI-användning inom Göteborgs Stad. Den betonar etik, laglighet, ansvar, informationssäkerhet och dataskydd

Det är tjänsteteamets uppfattning av det inte föreligger någon direkt motsägelse mellan förslaget i detta tjänsteuttalande och stadsledningens regler för AI användning. Dessa två dokument snarare kompletterar och stödjer varandra. AI-riktlinjerna anger att det är verksamhetens ansvar att skapa förutsättningar för korrekt och säker AI-användning samtidigt som den betonar användarens ansvar för att sekretessuppgifter och skyddsvärd information inte röjs, och att sekretessbelagda uppgifter inte får matas in i AI-system om inte systemet riskbedömts som säkert för detta. Risk och konsekvensanalysen som Intraservice genomfört, identifierar riskerna med avsiktlig eller oavsiktlig röjande av skyddsvärd information och rekommenderar framtagning av utbildningsmaterial i hur generativ AI skall användas. Stadsledningskontorets riktlinjer för AI användning utgör en bra utgångspunkt för dessa utbildningar.

Se fullständigt stöddokument i bilaga 10.

Bedömning

Intraservice rekommenderar, efter noggrant övervägande av den juridiska bedömningens försiktighetsprincip och verksamheternas uttryckta behov samt potential för effektivisering, en kontrollerad återaktivering av Microsoft 365 Copilot chatt, där lokala tröskelanalyser fungerar som säkerhetsventil. Denna modell möjliggör effektivisering och innovation samtidigt som juridiska och säkerhetsmässiga risker hanteras på ett proportionerligt och lokalt anpassat sätt.

[2] AI i Göteborgs Stad artikeln finns publicerat på Digitala navet

Bilagor

1. Bilaga 1 Rapport riskanalys för informationssäkerhet - Copilot chatt
2. Bilaga 2 Företagsskydd i Microsoft 365 Copilot chatt_GöteborgsStad 250327
3. Bilaga 3 EU Data Boundary
4. Bilaga 4 Frågor Microsoft 2025-04-10_Del1_Avtal och underbiträden
5. Bilaga 5 Frågor Microsoft 2025-04-10_Del2_Funktionalitet och säkerhetsåtgärder
6. Bilaga 6 Lista över förbättringar Microsoft 365 Copilot chatt_250522
7. Bilaga 7 Microsoft Copilot chatt -_juridisk bedömning_250526
8. Bilaga 8 Bilaga DSO rekommendation för Copilot chatt 2025-05-17.pdf
9. Bilaga 9 Juridisk Bedömning av Microsoft 365 Copilot – Strategiska reflektioner från stadens verksamheter
10. Bilaga 10-Att använda AI i Göteborgs Stad 250524

Ordlista – centrala begrepp

Begrepp	Förklaring
Microsoft 365 Copilot chatt	AI-baserad chattfunktion från Microsoft som kan användas för att skriva, sammanfatta och analysera information.
Generativ AI	Typ av AI som skapar nytt innehåll (text, bild, kod etc.) utifrån användarens instruktioner.
Edge	Microsofts webbläsare.
Tröskelanalys	Riskbedömning som avgör om ett IT-verktyg kan användas inom en viss organisation. Synonym: riskacceptansanalys.
Informationsklassning	Bedömning av hur känslig information är och hur den ska skyddas.
EDP (Enterprise Data Protection)	Microsofts skydd för företagsdata i Microsoft 365-miljön. Reglerar hur data hanteras, krypteras och skyddas.
EUDP (EU Data Boundary)	Microsofts åtagande att lagra och behandla kunddata inom EU/EES. Undantag finns.
DPA (Data Protection Addendum)	Tilläggsavtal till Microsofts huvudavtal som reglerar hantering av personuppgifter enligt GDPR.
SCC (Standard Contractual Clauses)	Standardklausuler från EU-kommissionen för att lagligt överföra personuppgifter till länder utanför EU/EES.
DSO (Dataskyddsombud)	Person som är oberoende expert på dataskydd enligt GDPR och ger råd till organisationen.
Skugg-AI	När medarbetare använder AI-verktyg utanför organisationens godkända IT-miljö, ofta utan kontroll.
Bing	Microsofts sökmotor (motsvarande Google sökmötor). Används för att hämta information från internet.

Referenser

Mer information kring villkor, åtaganden och liknande för Microsofts tjänster:

Dataskyddstillägg för Microsofts produkter och tjänster (DPA)

Microsoft Produktvillkor

Mer information kring hur Microsoft arbetar med säkerhet, sekretess och efterlevnad se Microsoft Säkerhetscenter (Eng. = Trust Center):

Microsoft Säkerhetscenter | Microsoft Säkerhetscenter

Microsoft Säkerhetscenter | Produkter och tjänster Microsoft 365

Lista över Microsofts underordnade personuppgiftsbiträden från 28/2-2025

Microsoft General - Online Services Subprocessors List (02.28.2025)

Mer information om EU Data Boundary:

What is the EU Data Boundary? - Microsoft Privacy | Microsoft Learn