

Microsoft 365 Copilot chatt

Utredningsrapport

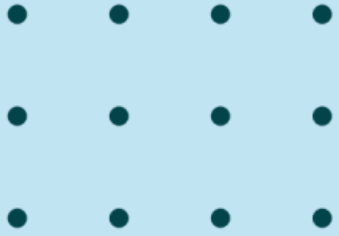
Inraservice nämndmöte - 26 juni 2025

Intraservice bedömning

1. Fortsatt blockering av Microsoft 365 Copilot chatt funktion i Edge-sidofält
2. Möjlighet för förvaltningar/bolag att aktivera Microsoft 365 Copilot chatt efter tröskelanalys
3. Intraservice genomför egen analys för att ta ställning till egen användning

Sammanfattning: Vi föreslår inte ett fritt godkännande – utan en modell där varje organisation själv avgör om, när och hur man vill aktivera Microsoft 365 Copilot chatt, utifrån sin informationshantering och mognadsnivå.



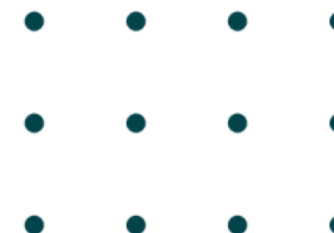


Microsoft 365 Copilot chatt

Sammanfattning av utredningsuppdrag

Den 30 januari 2025 beslutade Intraservice att tillfälligt stänga av AI-chatten Microsoft Copilot i Edge på grund av identifierade säkerhetsrisker och starta en utredning med målet att:

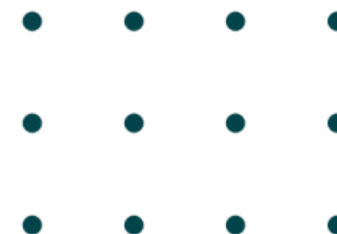
- Övergripande beskriva nyttan och användarpotentialen av Microsoft 365 Copilot chatt
- Identifiera och dokumentera säkerhetsrisker kopplade till användningen av Microsoft 365 Copilot chatt
- Föreslå konkreta tekniska och organisatoriska åtgärder för att minimera riskerna.
- Utfärda en rekommendation och utarbeta en plan i fall Microsoft 365 Copilot chatt -funktionen kan återstartas på ett säkert sätt.
- Säkerställa att verksamheten är förberedd och informerad om förändringarna.



Utredningen innehåller ett brett beslutsunderlag

Viktiga bilagor i utredningen:

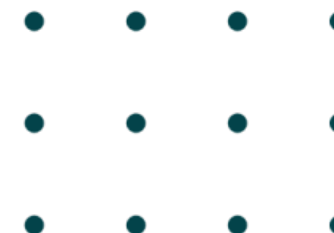
- **Bilaga 1:** Riskanalys – identifierar och bedömer säkerhetsrisker (14 st)
- **Bilaga 2–3:** Microsofts skydd – Enterprise Data Protection & EU Data Boundary
- **Bilaga 4–5:** Frågor och svar från Microsoft – avtal, funktionalitet och säkerhet
- **Bilaga 6:** Lista över förbättringar i Copilot chatt
- **Bilaga 7:** Juridisk bedömning – företagsskyddet ej rättsligt garanterat
- **Bilaga 8:** DSO:s rekommendation – avråder aktivering i nuläget
- **Bilaga 9:** Synpunkter från verksamheter – behov och strategisk potential
- **Bilaga 10:** Stadens AI-riktlinjer – stöd för säker och ansvarsfull användning



Vad är Microsoft 365 Copilot chatt?

(OBS: inte samma som Microsoft 365 Copilot)

- **AI-chattfunktion inom Microsoft 365** - Tänk på detta som ChatGPT. Skillnaden är att denna variant är kopplad till våra licenser och med vissa skyddsåtgärder från Microsoft
- **Kan skriva, sammanfatta, översätta, analysera information** som användaren själv skickar in
- **Används via**
 - Sidopanel i Edge (default browser) – Detta skall förbli stängd!
 - Webben (på samma sett som ChatGPT) – Denna vill vi lämna till förvaltningar/bolag att besluta om
- **Data bearbetas i Microsofts moln**
- **Tillför möjligt nytta till verksamheten**



Riskbild

(Översiktsbeskrivning av riskområdet)

Röjande av känslig information

- Det finns en risk att användare av misstag eller på grund av bristande kunskap förser Microsoft 365 Copilot chatt med känsliga eller sekretessbelagda uppgifter, såsom personuppgifter om anställda, medborgare eller intern information som inte bör spridas

Begränsad kontroll över dataflödet

- När användare i staden använder Microsoft 365 Copilot chatt hanteras en del av data av Microsofts infrastruktur, vilket innebär att man förlitar sig på leverantörens säkerhetsåtgärder.

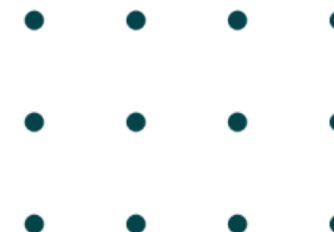
Teknisk utveckling utanför stadens kontroll

- Microsoft 365 Copilot chatt och liknande AI-tjänster är nya och snabbt utvecklande teknologier. Microsoft uppdaterar kontinuerligt Copilots AI-modeller och funktioner för att förbättra tjänsten.

Osäkerheter kring dataöverföring och regelefterlevnad

- Framförallt rör dessa frågor överföring av personuppgifter till tredje land (t.ex. USA)

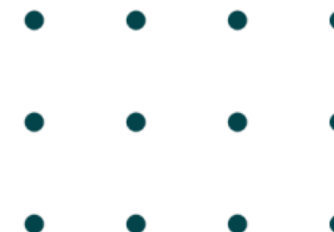
Risk för felaktigt eller vilseledande svar



Risikanalys för informationssäkerhet

(Slutsatser)

- Verksamheter behöver göra egna bedömningar av risker och eventuella samt anpassa sin användning av Microsoft 365 Copilot chatt därefter.
- Vidare behöver genomförbarhet bedömas av de åtgärder som föreslås för att reducera risker. Detta innefattas aspekter av kostnad, tidsåtgång, mognad, mottaglighet, kompetens, komplexitet, teknik, styrdokument, leverantörsavtal, lagar och förordningar samt politisk viljeinriktning.
- Med föreslagna åtgärder kan staden återaktivera Microsoft 365 Copilot chatt för de förvaltningar och bolag som önskar det, med varje enhet ansvarig för sin egen informationshantering.
- Inga risker bedömdes som höga efter att föreslagna åtgärder är införda.

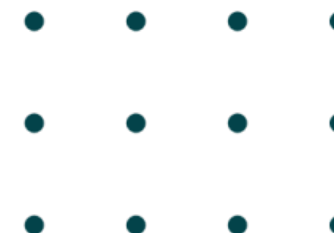


Juridisk bedömning och kontroll

(Rättsliga ramar – vad säger juristerna?)

- Microsoft agerar som personuppgiftsbiträde
- Företagsskyddet bygger på avtal, ej på garantier
- Staden ansvarar fortsatt för korrekt informationshantering
- Juridisk rekommendation: försiktighetsprincip gäller

Sammanfattning: Microsoft erbjuder ett avtalsskydd, men inte rättsligt bindande garantier. Därför föreslås att vi fortsatt agerar med försiktighet, men också använder de verktyg vi har – om riskerna hanteras lokalt.



GDPR

(GDPR och AI – Vad behöver vi tänka på?)

- Fokus på rättsliga förutsättningar och risken för otillbörliga tredjelandsoverföringar
- Betonar behovet av tydliga tekniska skyddsåtgärder framför enskild användares ansvar
- Efterfrågar en bredare granskning av hela Microsoft 365-miljön, inte bara Microsoft 365 Copilot chatt

TU bedömning: Dataskyddsombudets synpunkter har beaktats och den samlade bedömning är att den föreslagna hanteringsmodellen både tar hänsyn till dataskyddsombudets synpunkter och erbjuder en praktiskt genomförbar väg framåt.

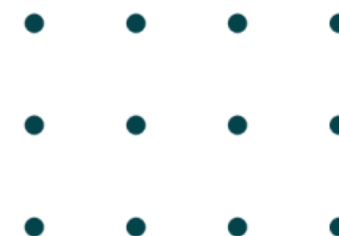


Sociala och strategiska konsekvenser

(Arbetsmiljö, kompetens och varumärke)

- Att stänga Microsoft 365 Copilot chatt bidrar till användning av andra mindre säkrare lösningar som t.ex. ChattGPT
- Ökad digital mognad och minskad stress
- Attraktivitet som arbetsgivare
- Risk för digitala klyftor vid fortsatt avstängning
- **Signalvärde i stadens AI-strategi** – Intraservice roll som möjliggörare eller som hinder till digitalutveckling

Sammanfattning: Att möjliggöra Microsoft 365 Copilot chatt är inte bara ett tekniskt beslut – det handlar om hur vi vill att Göteborgs Stad ska uppfattas som arbetsgivare och organisation.



Sammanfattning:

1. **Fortsätta att tills vidare blockera användningen av Microsoft 365 Copilot chatt i sidofältet i webbläsaren Edge, som är Göteborgs Stads rekommenderade webbläsare.** Blockeringen motiveras av säkerhetsskäl, då denna åtkomstform innebär särskilda risker för oavsiktlig exponering av känslig information.
2. **Erbjuda förvaltningar och bolag möjligheten att, för den egna organisationen, öppna för användning av Microsoft 365 Copilot chatt,** efter att en tröskelanalys (ibland kallad riskacceptansanalys) görs i egna organisationen.
3. **Med utgångspunkt i genomförd riskbedömning rekommenderas Intraservice som förvaltning, att göra en egen tröskelanalys för Intraservice räkning.**



Tack för idag!