

Frågor till Microsoft 2025-04-10

Funktionalitet och säkerhetsåtgärder

1. Om användaren ställer frågor till Copilot som inte är relaterade till webbsidan kan ni då garantera att Copilot inte indexerar *eller* får tillgång till informationen på webbsidan?

1.1 Om ja, vilka tekniska säkerhetsåtgärder har ni vidtagit för att säkerställa det?

2. Om användaren ställer frågor till Copilot som är relaterade till webbsidan användaren befinner sig på kan ni då garantera att Copilot inte indexerar *eller* får tillgång till informationen på webbsidor som är öppna i andra flikar?

2.1 Om ja, vilka tekniska säkerhetsåtgärder har ni vidtagit för att säkerställa det?

Microsofts kommentar:

Detta avser Microsoft 365 Copilot Chat och kontextuellgrundning genom Edge:

*Detta är förmågan att grunda en chattkonversation i den **aktuella webbsidans** kontext. Det gäller uppmaningar som "Sammanfatta det här dokumentet" eller "Vad säger den här sidan om..." med **hänvisning till fliken som för närvarande visas av användaren i huvudfönstret i Edge**. Kontextuell grundning gäller endast för instanser av chatt när du använder Copilot i Edge-sidofältet, eftersom skrivbords-/helskärmsinstanser inte tillåter samtidig webbkontext.*

Fråga 1, är sedan en tid tillbaka eskalerad till produktägaren ytterligare kommentarer och förtydliganden men vi har trots påstötning inte erhållit några än. Vi hänvisas till nedan länkar tills vidare.

Ni kan läsa mer här:

[Microsoft 365 Copilot Chat in Edge | Microsoft Learn](#)

[Copilot in Edge webpage summarization behavior | Microsoft Learn](#)

3. Har Microsoft vidtagit några tekniska skyddsåtgärder för att personuppgifter ej ska finnas med i den information (de sökord) som skickas över till Bing vid användning av Copilot Chat?

3.1 Om ja, vilka tekniska skyddsåtgärder har vidtagits?

3.2 Hur säkerställer Microsoft att personuppgifter som förekommer i dokument eller bilder som laddas upp i Copilot Chat inte överförs till Bing vid användning av Copilot Chat?

Microsofts kommentar:

Som vi tidigare informerat så är Microsoft 365 Copilot chat med Företagsskydd (Enterprise Data Protection) utformad för att minimera att känslig information hanteras utanför er egen miljö (M365 Tenant) och att skickas till Bing Söktjänsten.

All data som hanteras av Microsoft 365 Copilot Chat är krypterad både vid vila och under överföring och följer GDPR och andra relevanta dataskyddsregler.

För er som har er miljö (M365 Tenant) och användare i Sverige/EU så säkerställs genom EU Data gräns (EU Data boundary) att er data stannar inom EU:s datagränser.

En viktigt utformning, är att den genererade sökfrågan skiljer sig från användarens ursprungliga prompt, Den generade sökfrågan som ev. skickas till Bing består av några få ord genererade utifrån användarens prompt.

Vidare så ingår **inte** följande information i den genererade sökfrågan som skickas till Bing-söktjänsten:

- Användarens hela prompt, såvida inte prompten är mycket kort (till exempel "lokalt väder")
- Hela Microsoft 365-filer (till exempel e-postmeddelanden eller dokument) eller filer som laddats upp till Copilot
- Hela webbsidor eller PDF-filer som sammanfattas av Copilot i Microsoft Edge (endast för Microsoft 365 Copilot Chat)
- Identifierande information baserat på användarens Microsoft Entra ID (till exempel användarnamn, domän eller klientorganisations-ID)

Utöver det så har avtalsmässiga åtaganden om de genererade sökfrågorna som skickas till Bing-söktjänsten gjorts enligt nedan:

- Microsoft har inga andra rättigheter än vad som krävs för att tillhandahålla tjänsten.
- De används inte för att förbättra Bing.
- De används inte för att skapa annonseringsprofiler eller för att spåra användarbeteende.
- De delas inte med annonsörer.
- De används inte för att träna generativa AI-grundmodeller.
- De behandlas som konfidentiell kundinformation och skyddas av lämpliga tekniska och organisatoriska åtgärder.

Ni kan läsa mer om Säkerhet och efterlevnad för Microsoft 365 Copilot Chat här:

[Service Trust Portal -M365 - Security and Compliance with Microsoft 365 Copilot Chat \(March 2025\)](#)

[Data, sekretess och säkerhet för webbsökning i Microsoft 365 Copilot och Microsoft 365 Copilot Chat | Microsoft Learn](#)

[Efterlevnad av EU:s AI-förordning | Microsoft Säkerhetscenter](#)

Promptar och svar:

- Dataskydd för företag (Enterprise Data Protection-EDP), [Dataskyddstillägg för Microsofts produkter och tjänster \(Data Protection Addendum-DPA\)](#) och [Produktvillkor](#) gäller.
- Microsoft fungerar som personuppgiftsbiträde.

Webbsökningsfrågor som genereras av Copilot

- Omfattas av [Microsoft-tjänsteavtal](#) mellan varje användare och Microsoft, tillsammans med [Microsofts sekretesspolicy](#).
- Dessutom lägger produktvillkoren till ytterligare åtaganden för Microsoft som personuppgiftsansvarig när det gäller hantering av webbfrågedata.
- I händelse av konflikt har [Produktvillkoren](#) företräde framför [Microsoft-tjänsteavtal](#) och [Microsofts sekretesspolicy](#).
- Microsoft fungerar som en oberoende personuppgiftsansvarig som ansvarar för att följa alla tillämpliga lagar och personuppgiftsansvarigas skyldigheter.
- Dataskyddstillägget för Microsofts produkter och tjänster (DPA) gäller inte för användningen av Bing.

EU-Datagräns (EU Data boundary)

[Översikt över Microsofts EU-datagräns | Microsoft Säkerhetscenter](#)

Notera: Att det som står på våra uppdaterade sidor och officiella dokument är det som gäller utifall att det råder någon informationskonflikt med ev. sammanfattningar här.

Läs därför igenom bifogade länkar.

4. Kan "agenter" aktiveras i Microsoft Copilot Chat utav Microsoft själva utan en aktiv handling eller godkännande från Staden?

Microsofts kommentar:

Möjligheten till att använda agenter hanteras centralt av Staden och vi föreslår en genomgång med vår Tekniska specialist för att säkerställa att ni har rätt förståelse för hur ni bäst kan hantera detta.

Läs mer här:

[Agents for Microsoft 365 Copilot Chat | Microsoft Learn](#)

[Manage agents for Microsoft 365 Copilot in Integrated Apps - Microsoft 365 admin | Microsoft Learn](#)

5. Kan Copilot Chat enbart få tillgång till uppgifter/handlingar inom Stadens M365-miljö OM Staden centralt aktiverar den funktionen eller kan användaren själv välja vad Copilot Chat ska kunna få tillgång till?

Microsofts kommentar:

Microsoft 365 Copilot Chat kan inte anropa organisationsinnehåll på egen hand, men användarna har två alternativ för att komma åt innehåll från sin organisation som Copilot Chat kan använda.

Alternativ 1 – Tillhandahåll organisationsinnehåll som en del av sin prompt:

Användare kan aktivt tillhandahålla organisationsinnehåll som en del av sin prompt för Copilot Chat att använda. De kan tillhandahålla organisationsinnehåll som en del av sin prompt på tre sätt:

1. Användare skriver eller klistrar in den här informationen direkt i chatten.
2. Användare laddar upp en fil genom att välja knappen "(+) Lägg till innehåll" i chattrutan. De kan också dra och släppa en fil i chattrutan.
Uppladdade filer **lagras i användarens OneDrive för företag som en del av företagets dataskydd.**
3. Användare skriver en prompt i Copilot Chat i Edge efter att ha aktiverat inställningen "Tillåt åtkomst till alla webbsidor eller PDF", och en intranätsida öppnas i webbläsaren. I det här scenariot kan Copilot eventuellt använda det innehållet för att besvara frågor.

Alternativ 2 – Använd en agent som har åtkomst till organisationsinnehåll:

Användare kan också komma åt organisationsinnehåll via agenter som har grundats i delade klientdata, till exempel SharePoint- eller Graph Connector-innehåll. När sådan agent används kan användare fråga Copilot Chat om de data eller det innehåll som agenten har åtkomst till.

Se kommentar på fråga fyra kring aktivering av agenter.

Notera att: För båda alternativen använder Copilot Chat inte dina data för att träna grundmodeller och **företagsdataskydd (EDP) gäller så att ingen data skickas vidare till Bing utan hanteras inom ramen för er M365 miljö.** Se även kommentarer på fråga 3.

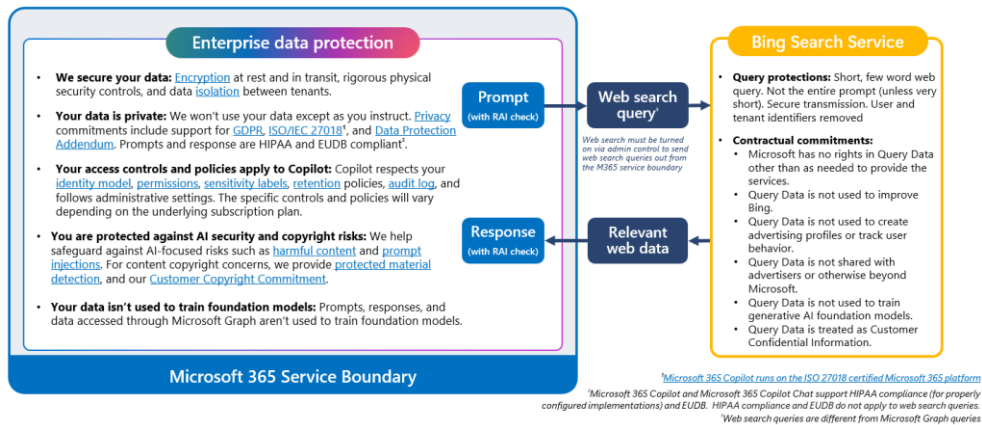
Ni kan läsa mer här:

[Microsoft 365 Copilot Chat Privacy and Protections - Organizational data | Microsoft Learn](#)

Illustrationer som vi tidigare delat med er för förtydligande:

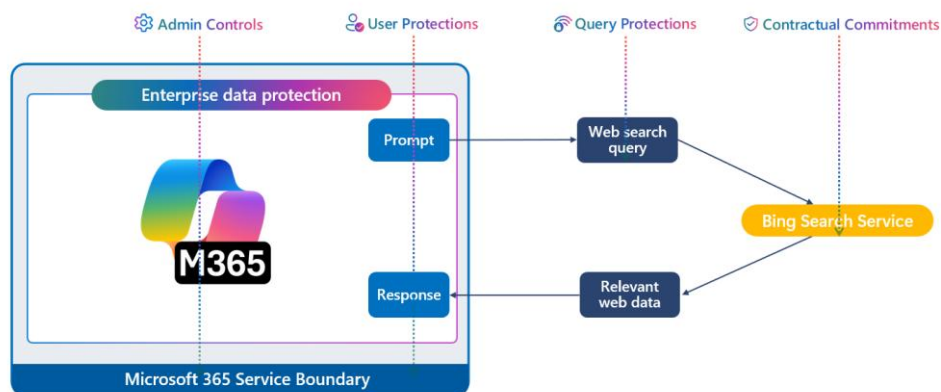
Prompts and responses vs web search queries

Use of M365 Copilot and M365 Copilot Chat involves prompts (entered by users) and responses (content generated by Copilot). In both M365 Copilot and M365 Copilot Chat prompts and responses are protected by EDP.



Protection in practice

Web queries are protected throughout the grounding process.



Web queries have multiple layers of protections and controls

