

2025-05-17

Rekommendation från dataskyddsombudet

Dataskyddsombudet ska enligt artikel 39 GDPR informera och ge råd till den personuppgiftsansvarige eller personuppgiftsbiträdet och de anställda som behandlar om deras skyldigheter enligt GDPR och andra av unionens eller medlemsstaternas dataskyddsbestämmelser.

Förvaltningen för Intraservice har ombett dataskyddsombudet att göra en bedömning av riskanalysen för Microsoft Copilot Chat¹ samt Microsofts EU Data Boundary. När det gäller Microsofts EU Data Boundary och övriga avtal hänvisar dataskyddsombudet till den juridiska bedömning avseende rättsliga ramar och avtalsrisker för Microsofts företagsskydd som genomförts av förvaltningens jurister.² Denna redogör på ett tydligt och detaljerat sätt för de rättsliga samt säkerhetsrelaterade risker som föreligger vid användning av Copilot Chat. De risker som lyfts utifrån ett integritetsperspektiv är samma som dataskyddsombudet tidigare identifierat. Dataskyddsombudet delar de bedömningar som görs i underlaget, och stödjer den rekommendation som lämnas.

Tidigare lämnade rekommendationer

Dataskyddsombudet lämnade 2025-01-23 en rekommendation till förvaltningen gällande hanteringen av Copilot i Edge. Förvaltningen rekommenderas då;

1. att inaktivera funktionen Copilot i Edge.
2. att ta ansvar för att identifiera och dokumentera vilka av de stadengemensamma systemen som använder webbläsaren för behandling av extra skyddsvärda och känsliga personuppgifter samt för uppgifter som är sekretessbelagda.
3. att när system med webbdelar identifierats genomföra tester (i en säker testmiljö) för att se om det går att använda Copilot i dessa webbdelar. Om tester visar att Copilot kan få tillgång till information i webbdelar, trots att möjligheten att sammanställa sidinnehåll är avstängd, behöver det vidtas ytterligare åtgärder för att Copilot inte ska kunna användas i dessa webbdelar.
4. att informera förvaltningar och bolag om risken för att Copilot i Edge kan användas i webbdelar inom både stadengemensamma och verksamhetsspecifika verksamhetssystem. Och i samband med att information tillhandahålls redogöra för de möjligheter som finns för att hantera denna risk på kort respektive lång sikt.

Intraservice har sedan rekommendationen lämnades stängt av möjligheten att använda Copilot i Edge för samtliga av Stadens verksamheter.

Om Copilot Chat

Det som tidigare hette Copilot i Edge heter nu Copilot Chat och finns i två utföranden.

¹ Riskanalys för informationssäkerhet, Copilot Chat 2025-04-11

² Juridisk bedömning – Bedömning av rättsliga ramar och avtalsrisker för Microsoft företagsskydd (2025-05-13)

1. Copilot Chat i Edge – där assistenten använder information från den aktuella fliken i det öppna webbfönstret genom ett sidofönster.
2. Copilot Chat för webb – 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.

Bedömning av risk- och sårbarhetsanalys för Copilot Chat

Bakgrund

Risikanalysen avser Microsofts Copilot Chat och har tagits fram av Intraservice som underlag för att kunna fatta beslut om att åter aktivera tjänsten i stadens O365-miljö. Den är tänkt att ge stöd i att bedöma vilka skyddsåtgärder och begränsningar som krävs för att möjliggöra ett säkert införande i verksamheten.

Avgränsningar

Risikanalysen anges gälla teknisk och logisk informationssäkerhet, och omfattar inte verksamhetsspecifika dataskyddsrisker eller andra juridiska hot som inte kan hanteras genom tekniska åtgärder.

Tidigare identifierade risker

I risikanalysen framgår även att denna ska adressera de dataskyddsrisker som dataskyddsbudet tidigare lyft. Dessa risker innefattar bland annat att tjänsten kan få åtkomst till mejl, filer och mappar via webben och skicka information vidare till externa tjänster som Bing, där Microsoft är personuppgiftsansvarig, utan att detta omfattas av stadens befintliga avtal.

En ofullständig riskbild

Risikanalysen visar att det inte bedöms finnas några *mycket höga risker* med användningen av Copilot Chat. De risker som bedöms vara höga är användarrelaterade och handlar om oavsiktligt (#5) eller avsiktligt (#6) röjande av information. När det gäller dataskyddsriskerna (#15-17) så har dessa bedömts vara medelhöga och anges kunna risk reduceras med hjälp av föreslagna åtgärder.

Efter att ha gått igenom risikanalysen, och specifikt identifierade s.k. dataskyddsrisker, är dataskyddsbudets uppfattning att förvaltningen ej omhändertagit dataskyddsbudets tidigare rekommendation och de risker som i denna lyfts föreligga med användningen av Copilot Chat.

Exempelvis när det gäller risk #15 ”Microsoft får tillgång till känslig information i aktuellt webbfönster” så beskrivs risken enbart handla om att ”Användare ber Copilot om att sammanfatta innehållet av fliken i Edge, och Copilot läser öppen flik som innehåller känslig info”, vilket dataskyddsbudet inte håller med om eftersom risken även är att Copilot läser av webbsidan även om frågan som ställs inte direkt gäller innehållet på den. Att begränsa risken till att enbart omfatta felaktig användning av Copilot blir missvisande, eftersom den kvarstående risken inte kan åtgärdas genom utbildning eller anvisningar.

Det hade varit mer lämpligt att förvaltningen adresserat denna risk enskilt och i det kartlagt vilka webbdelar som kan innehålla känslig/sekretessbelagd information och utifrån det vidtagit tekniska skyddsåtgärder för att förhindra/förbjuda användning av

Copilot på dessa sidor. Varför förvaltningen ej omhändertagit dataskyddsbudets tidigare lämnade rekommendation gällande detta framgår ej av underlaget.

Dataskyddsbudet saknar även risker kopplat till att Microsoft anger sig vara personuppgiftsansvarig för den data som skickas till Bing. Detta adresserar förvaltningen inte i underlaget, i stället ligger fokus på olämplig lagring (#16) och behandling av data utanför EU (#17) där problemet beskrivs vara att information som delas kan innehålla skyddsvärd information och olämplig data. När det gäller Bing har dataskyddsbudet även noterat att användningen av den funktionen bedöms kunna utgöra en åtgärd för att hantera en av de tekniska riskerna, dock helt utan resonemang kring de risker aktiveringen av funktionen för med sig.

När det gäller risk #17 hade dataskyddsbudet förväntat sig att förvaltningen skulle lyfta att Microsoft kan överföra information till exempelvis USA (men även andra delar av världen) för oklara säkerhetsändamål och problematiken med tredjelandsoverföringar och användningen av underbiträden i länder utan adekvat skyddsnivå. Inget av detta nämns i rapporten.

Dataskyddsbudet vill även särskilt påpeka att det saknas motiveringar till riskbedömningarna och hur åtgärderna bedöms kunna minska riskerna till en nivå som möjliggör återaktiveringen av Copilot Chat. Dataskyddsbudets bedömning är att de åtgärder som är angivna inte är tillräckliga och att förvaltningen behöver ta ett större ansvar för att implementera tekniska åtgärder, i stället för att lägga allt på slutanvändaren.

Utelämnade risker

Dataskyddsbudet redogör nedan för de risker, från den tidigare lämnade rekommendationen, som ej adresserats i riskanalysen.

1. Överföring av data till Microsoft utan rättslig grund

Copilot Chat för webb innebär att sökningar kan göras via Bing. För de uppgifter som skickas till Bing anger sig Microsoft vara personuppgiftsansvarig. Det finns inga säkerhetsåtgärder som förhindrar att personuppgifter skickas till Bing. Om personuppgifter skickas till Bing innebär det en delning av personuppgifter som avviker från övriga M365-hanteringen, eftersom Microsoft i detta fall tar över personuppgiftsansvaret. Om Microsoft blir personuppgiftsansvarig för uppgifterna krävs en rättslig grund för överföringen. I det fall det inte går att fastställa en giltig rättslig grund för överföringen innebär det att behandlingen är olaglig.

2. Att Copilot Chat i webbläsaren kan användas i vissa av M365-apparna

Dataskyddsbudet har tidigare kunnat konstatera att Copilot kunnat användas i Outlook när denna öppnats via webbläsaren.

3. Röjande av information från webbaserade verksamhetssystem till Microsoft genom användning av Copilot Chat i webbläsaren

Det bedöms vara en risk att Copilot i Edge är möjligt att använda i webbapplikationer som hanterar extra skyddsvärda och känsliga personuppgifter samt uppgifter som omfattas av sekretess. Det finns en risk för att Copilot indexerar/läser av webbsidans innehåll när man använder Copilot med en webbsida uppe även när frågan (prompten) som ställs inte är kopplad till sidinnehållet (förutsatt att användaren har tillåtelse tillgång till att använda sidinnehållet, dvs. har accepterat villkoren en gång).

För att bedöma denna risk har dataskyddsombudet frågat Microsoft ifall dem kan garantera att Copilot inte indexerar *eller* får tillgång till informationen på webbsidan i det fall användaren ställer frågor till Copilot som inte är relaterade till webbsidan, samt i så fall hur (vilka säkerhetsåtgärder) som vidtagits för att säkerställa det.

Microsoft har ej kunnat svara på frågan, vilket får bedömas medföra att risken föreligger.

4. Osäkerhet och bristande kontroll över underbiträden och tredjelsöverföringar

Microsoft har, trots att det specifikt efterfrågats, inte kunnat lämna en lista över de underbiträden som används för att tillhandahålla Stadens O365-miljö, inkluderat Copilot Chat. I stället hänvisar man till listan över samtliga möjliga underbiträden som är tillgänglig via Microsofts hemsida. Utifrån att Microsoft själva inte kan redogöra för vilka underbiträden som används får dataskyddsombudet utgå från att samtliga angivna kan aktualiseras, vilket innebär möjliga tredjelsöverföringar till flera länder utan adekvat skyddsnivå.

Sammantagen bedömning och rekommendation

Dataskyddsombudet ställer sig starkt kritisk till riskanalysens slutsats att Copilot Chat kan återaktiveras om föreslagna åtgärder implementeras. Utifrån riskanalysens kraftigt begränsade omfattning, avsaknaden av motiveringar/resonemang och då ansvariga helt utelämnat flera av de risker som dataskyddsombudet tidigare lyft delar dataskyddsombudet ej denna bedömning. De frågeställningar som behöver adresseras när det gäller Copilot Chat är betydligt mer komplexa än vad som redogörs för i underlaget. Detta visas även genom den separata juridiska bedömning som förvaltningens jurister genomfört, med bland annat riskanalysen som utgångspunkt.

Rekommendation för Copilot Chat

Sammantaget bedömer dataskyddsombudet att det i nuläget saknas rättsliga förutsättningar för att använda Copilot Chat, och förvaltningen avråds därför från att aktivera Copilot Chat för organisationer inom Staden.

Rekommendation för O365-plattformen

Då risken gällande osäkerhet och bristande kontroll över underbiträden och tredjelsöverföringar inte är unik för Copilot Chat, utan gäller O365-plattformen som helhet, rekommenderas förvaltningen omgående att vidta tekniska och organisatoriska skyddsåtgärder för att säkerställa att användningen av plattformen är förenlig med de krav på dataskydd som gäller enligt GDPR.

Utifrån ett dataskyddsperspektiv vore en lämplig hantering att identifiera de/n personuppgiftsbehandlingar där O365 används som en informationsbärare och genomföra konsekvensbedömningar för de/n behandlingarna.

Dataskyddsenheten

GÖTEBORGS STAD