IBD Notitie m.b.t. DPIA MS Copilot

Deze notitie, geschreven door de Informatiebeveiligingsdienst voor PO's, FG's en (C)ISO's van gemeentelijke organisaties, biedt een korte samenvatting van de belangrijkste bevindingen uit de DPIA Microsoft Copilot Daarnaast belicht de notitie de (mogelijke) gevolgen voor gemeentelijke organisaties die Copilot gebruiken en geeft ze aanbevelingen voor het beperken van risico's. Deze notitie is bedoeld als hulpmiddel voor gemeentelijke organisaties en bevat geen officieel (VNG) standpunt met betrekking tot het wel of niet mogen gebruiken van Microsoft Copilot.

DPIA en vervolgacties

De DPIA, uitgevoerd in opdracht van SLM Rijk, heeft diverse risico's geïdentificeerd. Op basis van deze bevindingen gaan SLM Rijk en Microsoft in overleg om te onderzoeken hoe deze risico's beperkt kunnen worden. Tot er meer duidelijk is over de uitkomsten van dit overleg, kunnen gemeentelijke organisaties alvast zelf maatregelen nemen om de in de DPIA vastgestelde risico's te beperken. Deze technische en organisatorische maatregelen worden in deze notitie besproken.

Samenvatting DPIA

Microsoft Copilot draait binnen de Microsoft data-omgeving van een organisatie en verzamelt gegevens om slimme oplossingen te genereren. Uit de DPIA blijkt echter dat het onduidelijk is in hoeverre die gegevensverwerking voldoet aan de AVG. Sommige risico's zijn technisch van aard en hangen samen met de koppeling met Microsoft Graph.

Microsoft Graph is een systeem dat toegang biedt tot de inhoud en interacties van gebruikers in een specifieke M365-tenant van de organisatie. Het biedt toegang tot vier hoofdinformatiebronnen:

- kernapplicaties (zoals SharePoint, Outlook, Teams),
- bedrijfsbeveiligingsdiensten,
- Windows,
- Dynamics.

Microsoft Copilot maakt gebruik van deze gegevens via de Graph API om inhoud te analyseren en te doorzoeken. Deze Graph API gebruikt ook metadata over gebruikersgedrag.

Een belangrijk risico komt voort uit het feit dat organisaties de toegang tot hun gegevens niet altijd adequaat beperken. Dit geldt vooral voor documenten in SharePoint, die bij onvoldoende beperking gewoon toegankelijk zijn voor Copilot, zelfs als de gebruiker zelf niet de benodigde toegang heeft. Ook interacties met Copilot worden opgeslagen, inclusief prompts (een korte tekst of opdracht die je gebruikt om in de AI-tool een reactie te genereren) en reacties van Copilot. Gemeentelijke organisaties moeten maatregelen nemen om onnodige opslag van gegevens te beperken, zeker omdat niet duidelijk is hoe lang Microsoft deze gegevens opslaat.

IBD Notitie m.b.t. DPIA MS Copilot

Zolang organisaties gevoelige gegevens niet als zodanig hebben gelabeld en toegangsrechten mogelijk ook niet waterdicht zijn ingericht, kan en zal Copilot geen rekening houden met de aard van deze data. Microsoft biedt tools zoals Purview om documenten te labelen en toegang te beheren. De implementatie hiervan vergt echter veel tijd en inspanning en wordt in de meeste gemeentelijke organisaties niet toegepast. Omdat veel gemeentelijke organisaties verouderde informatie opslaan, brengt de verwerking van onjuiste gegevens door Copilot volgens de DPIA aanzienlijke risico's met zich mee.

Microsoft 365 Copilot verzamelt gegevens via *Required Service Data*, ongeacht de privacy-instellingen die gebruikers kiezen voor diagnostische gegevens. Deze instellingen hebben geen invloed op welke gegevens naar Microsoft worden gestuurd. Door de beperkte transparantie over de verwerking van gegevens door Microsoft, kunnen organisaties hun verplichtingen om medewerkers adequaat te informeren over de doeleinden van de gegevensverwerking niet volledig nakomen. Het gebrek aan controle over de verwerkte gegevens bemoeilijkt het inschatten van risico's en het voorkomen dat persoonlijke gegevens door Microsoft voor commerciële doeleinden worden verwerkt.

Hoge risico's en de daarbij beoogde maatregelen:

De DPIA identificeert vier hoge risico's. Deze risico's en de beoogde mitigerende maatregelen staan in de tabel hieronder. Voor een overzicht van alle gedetecteerde risico's verwijzen we naar de volledige DPIA.

Risico (HOOG)	Maatregelen zoals in DPIA opgenomen
Belemmeringen bij het uitoefenen van inzagerechten door gebruikers. Microsoft geeft incomplete en onbegrijpelijke resultaten terug als het gaat over de gegevens over het gebruik van de Microsoft 365 Copilot dienst. Organisaties moeten een dure licentie kopen om makkelijk toegang te krijgen tot de inhoudelijke en diagnostische gegevens, als een gebruiker daarom vraagt.	Maak geen gebruik van Microsoft 365 Copilot [IBD: voor het verwerken van persoonsgegevens[1]] totdat Microsoft toegang/inzicht verschaft tot/in de diagnostische gegevens die zij van de gebruiker verwerken.

[1] De IBD voegt bij deze maatregelen, afkomstig uit de DPIA, 'voor het gebruiken van persoonsgegevens' toe. We vinden het belangrijk om deze specificering aan te brengen, omdat er ook voorbeelden zijn van het gebruik van Microsoft 365 Copilot waarin risico's laag of nihil zijn. Denk bijvoorbeeld aan het inzetten van Copilot voor het generen van een stukje tekst over een evenement voor inwoners, waar geen persoonsgegevens aan te pas komen. De IBD raadt het gebruik van Microsoft 365 Copilot volledig af m.b.t. het verwerken van bijzondere persoonsgegevens, en roept op terughoudend te zijn met het verwerken van persoonsgegevens, totdat Microsoft de genoemde maatregelen heeft getroffen.

IBD Notitie m.b.t. DPIA MS Copilot

Risico (HOOG)	Maatregelen zoals in DPIA opgenomen
Verlies aan controle en sociaaleconomisch nadeel voor betrokkenen als Microsoft 365 Copilot onjuiste en/of incomplete persoonsgegevens over hen genereert. Dit risico bestaat uit veel deelrisico's. Hoewel Microsoft onderaan elk antwoord de mededeling zet dat gegenereerde antwoorden onbetrouwbaar kunnen zijn, is de kans te groot dat gebruikers niet merken dat persoonsgegevens niet kloppen. 'Overreliance on AI' – een te groot vertrouwen in dat wat de computer zegt, ook klopt - is een bekend probleem bij generatieve AI. De DPIA beschrijft dat de vormgeving van de dienst als chatbot bijdraagt aan een misplaatst geloof in de betrouwbaarheid. Microsoft voegt te weinig frictie toe om mensen continu bewust te laten blijven dat generatieve AI een statistische woordvoorspellingsmachine is, geen zoekmachine. Microsoft claimt dat de antwoorden steeds betrouwbaarder worden, maar geeft organisaties geen inzicht in de resultaten van metingen die Microsoft uitvoert. Microsoft is ook niet transparant genoeg over hoe de Responsible AI filtering rekening houdt met Europese mensenrechten en of er geen overfiltering plaatsvindt op onderwerpen die mogelijk elders in de wereld controversieel zijn.	Maak geen gebruik van Microsoft 365 Copilot [IBD: voor het verwerken van persoonsgegevens] totdat Microsoft mitigerende maatregelen heeft getroffen rondom de transparantie over de toepassing van het zogenaamde RAI filter. Zorg voor intern beleid rondom het gebruik van generatieve AI. Informeer medewerkers over de risico's die ontstaan bij het gebruik van generatieve AI [IBD: en met name als er ook persoonsgegevens verwerkt worden], zeker als niet volledig duidelijk is hoe en vanuit welke bronnen bepaalde informatie tot stand is gekomen en wanneer de koppeling met Bing is uitgeschakeld. Waarschuw ervoor dat informatie mogelijk onjuist is en dat er altijd een check moet plaatsvinden op de door AI gegenereerde respons. Beperk de toewijzing van Copilot licenties aan accounts die geen toegang hebben tot gevoelige gegevens zoals HR-gegevens (anders gezegd: accounts van medewerkers die met gevoelige persoonsgegevens werken mogen niet aan Copilot gekoppeld worden). Zorg voor audit logs en een check op de opvolging van het interne generatieve AI beleid door gebruikers. Controleer daarbij ook de *samples of dialogues* en de diagnostische gegevens.
Gebrek aan transparantie over de persoonsgegevens die Microsoft verwerkt over het gebruik van Microsoft 365 Copilot. Microsoft publiceert geen documentatie over de precieze soorten persoonsgegevens die ze verzamelt. Omdat Microsoft 365 een clouddienst is, moeten gebruikers opdrachten sturen via internet aan de computers van Microsoft. Het is niet duidelijk of Microsoft (stukjes van die) opdrachten bewaart, en welke gegevens over het gebruik Microsoft verzamelt en gebruikt. Microsoft noemt alle diagnostische gegevens over het gebruik van haar online diensten 'Required Service Data'. Dat is inclusief de telemetriestroom als een gebruiker Microsoft 365 Copilot met een browser gebruikt, en inclusief de gegevensstroom naar de Connected Experiences (waarvoor Microsoft verwerker is)	Maak geen gebruik van Microsoft 365 Copilot [IBD: voor het verwerken van persoonsgegevens] totdat Microsoft de vereiste servicegegevens openbaar en adequaat heeft gedocumenteerd, inclusief de telemetriegebeurtenissen van webapp-clients. Zorg ervoor dat het telemetrieniveau in Windows en Office 365 wordt ingesteld op het minst invasieve beveiligingsniveau.

IBD Notitie m.b.t. DPIA MS Copilot

Risico (HOOG)	Maatregelen zoals in DPIA opgenomen
Een risico op heridentificatie van pseudonieme persoonsgegevens door de potentieel hele lange bewaartermijn van de Required Service Data. Als Microsoft de gegevens over het gebruik van de online diensten alleen functioneel zou verwerken, dus onmiddellijk zou weggooien na het uitvoeren van de gevraagde taak, zou die gegevensstroom buiten de scope van de DPIA kunnen blijven. Maar nu is onduidelijk welke persoonsgegevens Microsoft bewaart, en hoe lang. Formeel kan Microsoft alle persoonsgegevens zo lang bewaren als dat een gebruiker klant blijft, plus 180 dagen. Dat kan in de praktijk oplopen tot meer dan 10 jaar, als een medewerker bij een gemeentelijke organisatie blijft werken.	Maak geen gebruik van Microsoft 365 Copilot [IBD: voor het verwerken van persoonsgegevens] totdat Microsoft de bewaartermijnen van de verschillende soorten identificeerbare en gepseudonimiseerde gegevens heeft gespecificeerd.

Aanbevelingen voor gemeenten

Voor gemeenten die Copilot actief gebruiken voor bijvoorbeeld samenvattingen, teksten en gesprekken binnen Microsoft-applicaties (zoals Word, Excel, PowerPoint, Outlook en Teams) zijn er maatregelen om een aantal van bovengenoemde risico's te beperken.

Algemeen

- Gebruik Copilot nooit in combinatie met bijzondere persoonsgegevens (zoals medische gegevens of strafrechtelijke gegevens).
- Wees uitermate terughoudend met het verwerken van persoonsgegevens in Copilot, totdat Microsoft mitigerende maatregelen heeft getroffen op de genoemde risico's.

Op technisch niveau

- Microsoft heeft standaard toegang ingesteld tot zijn datacontrollerservice Bing, wat leidt tot onverenigbare verwerking van content- en diagnostische gegevens voor commerciële doeleinden van Microsoft. Beheerders kunnen deze toegang centraal uitschakelen via het nieuwe 'Bing'-beleid.
  Let op: uitschakelen van Bing heeft direct gevolgen voor de kwaliteit van de informatie die Copilot genereert (minder nauwkeurige antwoorden op basis van verouderde informatie)!

- Microsoft biedt ook toegang tot consumentenversies van Copilot in M365-apps en Windows Enterprise, zelfs als een organisatie Copilot heeft geblokkeerd via EDP. Dit leidt tot onverenigbare verwerking van contentgegevens voor commerciële doeleinden van Microsoft. Beheerders kunnen deze toegang centraal uitschakelen.

IBD Notitie m.b.t. DPIA MS Copilot

- Toegang tot het openbare feedbackforum van Microsoft (Copilot Chat bijvoorbeeld) resulteert eveneens in onverenigbare verwerking van contentgegevens voor commerciële doeleinden. Beheerders kunnen deze toegang uitschakelen. Er kan worden gekozen om medewerkers te het gebruik van feedbackmogelijkheden van Microsoft te verbieden.

Op organisatorisch niveau

- Zorg voor AI-geletterdheid onder medewerkers.[2] Met andere woorden: stimuleer een hoge mate van bewustwording rondom AI. Leg uit hoe generatieve AI werkt en welke risico's het gebruik met zich meebrengt. Wees kritisch op door generatieve AI gegenereerde informatie, zeker als de koppeling met Bing is uitgeschakeld, en leer gebruikers vragen te stellen over hoe die informatie tot stand is gekomen. In het document Aan de slag met AI-geletterdheid van de Autoriteit Persoonsgegevens vinden organisaties verschillende voorbeelden om aan de slag te gaan met AI-bewustwording in de organisatie.

- Wees als organisatie heel duidelijk over wat wel, en wat niet mag bij het gebruik van tools als Microsoft Copilot. Denk daarbij aan: welke functies van Copilot mogen wel gebruikt worden, en welke niet? Zijn er medewerkers die veel gevoelige informatie verwerken die, ter bescherming van die gegevens, geen gebruik mogen maken van Copilot? Welke gegevens mogen wel, en welke nooit in combinatie met Copilot worden gebruikt?
  Maak duidelijke afspraken en zorg dat die breed binnen de organisatie worden gedeeld. Dat is niet een kwestie van één keer een document op intranet publiceren, maar heeft tijd en aandacht nodig. Herhaal de boodschap regelmatig, controleer of de afspraken worden nageleefd en blijf hierover actief in gesprek.

- Gebruik van AI-tools zonder gemeentelijk AI-beleid, is vragen om moeilijkheden. Zeker als, zoals hierboven genoemd, bepaalde ge- en verboden worden gecommuniceerd, moet daar eerst een bovenliggend beleid aan voorafgaan. Verschillende gemeenten hebben al een AI-beleid ontwikkeld en gepubliceerd (online te vinden). Gebruik deze stukken vooral ter inspiratie en als startpunt voor een eigen beleid. De handreiking AI en Algoritmen van de IBD kan hierbij ook ondersteuning bieden.

[2] Dit is eveneens een verplichting die voortvloeit uit de AI Act die sinds 2 februari 2025 van kracht is.