

Bijlage: Microsoft 365 Copilot DPIA, december 2024

De hoge gegevensbeschermingsrisico's in de Microsoft 365 Copilot DPIA zijn:

- 1. 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. Instellingen moeten een dure A5 licentie kopen om makkelijk toegang te krijgen tot de inhoudelijke gegevens, de historische dialoog, als een gebruiker daarom vraagt.
- 2. Verlies aan controle en sociaal-economisch 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, en de dienst 'Copilot' heeft genoemd, niet 'Autopilot', 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 woord voorspellingsmachine is, geen zoekmachine. Microsoft claimt dat de antwoorden steeds betrouwbaarder worden, maar geeft de instellingen 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.
- 3. 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).
- 4. 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 hogeschool of universiteit blijft werken.