

Artikel 45-vragen van de Partij voor de Dieren over AI en de geüpdatete DPIA Microsoft 365 Copilot

Aanleiding

Op 27 mei 2026 is de tweede update van de overheidsbrede DPIA (Data Protection Impact Assessment) op Microsoft 365 Copilot gepubliceerd. Uit deze beoordeling blijkt dat twee privacyrisico's nog altijd als 'medium' worden gekwalificeerd: onjuiste persoonsgegevens in de door Copilot gegenereerde teksten, en de bewaartermijn voor diagnostische gegevens.¹

Daarnaast introduceerde Microsoft in april 2026 'flex routing' voor Copilot. Hierbij kan de AI-verwerking tijdens piekmomenten buiten de Europese Unie plaatsvinden, wat niet in lijn is met de Europese privacywetgeving. De instelling stond aanvankelijk voor een deel van de organisaties standaard aan en moest actief worden uitgeschakeld; voor sommige organisatietypes was dit een opt-in.²

Verder lijkt sinds het voorjaar van 2026 een bredere verschuiving zichtbaar, waarbij veel aanbieders van generatieve AI hun prijzen verhogen. Microsoft verhoogt per 1 juli 2026 de prijzen van vrijwel alle commerciële Microsoft 365-licenties, mede vanwege toegevoegde AI-functionaliteit.³

Ook introduceerde Microsoft op 2 juni 2026 de tool 'Scout': een AI-tool die continu actief is en meeleest met onder meer de mailbox, chats en bestanden van gebruikers, zoals ambtenaren. Doordat de tool ook handelt zonder dat de gebruiker daar een opdracht toe geeft, is toezicht complexer en is het de vraag of er zicht blijft op welke gegevens naar Microsoft worden gestuurd. Ook kan AI, die 24 uur per dag aan staat, meer energie en water vergen dan traditionele, chat-gebaseerde generatieve AI.⁴

Tot slot verscheen afgelopen maandag een artikel van Nieuwsuur: “Waarschuwing voor personeel dat met AI aan de slag gaat: ‘kans op datalek groot’”. In dit artikel beschrijft Nieuwsuur de casus van gemeente Eindhoven. Daar bleek uit een steekproef dat ambtenaren in een maand tijd meer dan duizend documenten hebben geüpload naar AI-tools zoals ChatGPT. Dit betroffen documenten met privégegevens, zoals BSN-nummers, WMO-gegevens, verslavingsgevoeligheid en financieel gevoelige data. De gemeente heeft dit als datalek moeten melden bij de Autoriteit Persoonsgegevens en ze heeft een verwijderverzoek ingediend, maar het verwijderen van gegevens is niet bevestigd door OpenAI.⁵

¹ <https://open.overheid.nl/details/df789dd8-a669-4893-a455-fb04e0274cda>

² <https://tweakers.net/nieuws/246504/microsoft-wijzigt-copilot-voor-365-dataverwerking-kan-ineens-buiten-eu-gebeuren.html>

³ <https://tweakers.net/nieuws/242268/microsoft-verhoogt-in-2026-wereldwijd-prijzen-van-microsoft-365-voor-ondernemers.html>

⁴ <https://www.microsoft.com/en-us/microsoft-365/blog/2026/06/02/introducing-microsoft-scout-your-always-on-personal-agent/>

⁵ <https://nos.nl/nieuwsuur/artikel/2617591-waarschuwing-voor-personeel-dat-met-ai-aan-de-slag-gaat-kans-op-datalek-groot>

De Partij voor de Dieren maakt zich zorgen over deze ontwikkelingen, en daarom stellen wij de volgende vragen.

Vragen

1. Is het college reeds bekend met de tweede DPIA-update van 27 mei 2026, en is het voornemens de actuele bevindingen te verwerken in het Zwolse AI-beleid?
2. Is het college reeds bekend met de in april 2026 geïntroduceerde flex routing? Kan het college bevestigen dat deze voor de eigen organisatie is uitgeschakeld?
3. Welke concrete maatregelen treft de gemeente tegen de resterende risico's van de geüpdatete DPIA, in het bijzonder het risico van het genereren en gebruiken van onjuiste informatie of adviezen, gegenereerd door AI, over personen?
4. Spelen de stijgende Microsoft-kosten door AI ook voor de gemeente Zwolle? Zo ja, met hoeveel nemen deze kosten naar verwachting toe, en wordt de inzet van generatieve AI hierdoor bijgesteld?
5. Houdt het college zicht op een mogelijke 'vendor lock-in', en wordt er regelmatig geëvalueerd of Europese alternatieven bruikbaar zijn, om te voorkomen dat een latere migratie naar Europese AI-aanbieders onnodig complex en duur wordt?
6. Is het college bekend met de nieuwe tool Scout en met het feit dat deze continu kan meelezen wanneer ambtenaren de tool gebruiken? Houdt het huidige AI-beleid al rekening met dit soort verregaande, mogelijk hoog-risico en niet-duurzame toepassingen van AI?
7. Is het college bekend met het artikel van Nieuwsuur, en wordt er in Zwolle ook gevoelige informatie geüpload naar externe AI-tools? En is het college bereid om in navolging van Eindhoven ook (steekproefsgewijs) onderzoek te doen naar of dit ook in Zwolle gebeurt?

Partij voor de Dieren

Thijmen Fellingier

Debbie Mathijsen