

DPIA Microsoft 365 Copilot for Education

Gegevensbeschermingseffectbeoordeling inzake de
verwerking van persoonsgegevens met Microsoft 365 Copilot
for Education

In opdracht van SURF

Bijgewerkte openbare versie – 27 mei 2026

*Dit is een vrijblijvende vertaling. Bij tegenstrijdigheden tussen deze vertaling
en het originele document is het originele document leidend.*



Colofon

DPIA door SURF

www.surf.nl

Contact Vendorcompliance@surf.nl

Projectnaam DPIA-rapport over Microsoft 365 Copilot for Education

Auteurs Privacy Company

Sjoera Nas

Floor Terra

Senior adviseurs

www.privacycompany.eu

Samenvatting

Dit is de tweede update DPIA (Data Protection Impact Assessment) over het gebruik van Microsoft 365 Copilot for Education (te bestellen als M365 Copilot Edu Sub Add-on), hierna: Microsoft 365 Copilot. Deze DPIA is opgesteld voor de Nederlandse onderzoeks- en onderwijsinstellingen, soms afgekort tot 'Nederlandse onderwijssector' of 'onderwijsinstellingen'. De oorspronkelijke DPIA werd gepubliceerd op 13 december 2024 en de eerste update DPIA op 11 september 2025.

Reikwijdte van de DPIA: betaalde versie van Microsoft 365 Copilot

Microsoft 365 Copilot is de naam die Microsoft gebruikt voor alle Copilot generatieve AI mogelijkheden en aanbiedingen. Copilot is een generatieve AI-dienst die gebruikers helpt bij het genereren van samenvattingen, teksten, gesprekken en berekeningen in de kernapplicaties van Microsoft, zoals Word, Excel, PowerPoint, Outlook en Teams. Microsoft biedt verschillende generatieve AI-diensten aan onder de naam Microsoft 365 Copilot, hierna Copilot genoemd. Dit rapport richt zich op de betaalde Educatie licentie. Microsoft stelt deze betaalde dienst (nog) niet beschikbaar aan gebruikers jonger dan 18 jaar. Daarom bevat deze DPIA geen risicobeoordeling met betrekking tot gebruik door kinderen.

Microsoft 365 Copilot is in het voorjaar van 2024 getest met de vier meest gebruikte Office-toepassingen (Word, Excel, PowerPoint, Outlook) op Windows en op macOS, en in de browser via Microsoft 365 Copilot Chat. Testresultaten met betrekking tot *intelligente samenvattingen* in Teams zijn uit dit rapport verwijderd, omdat deze intelligente functies op het moment van de tests door Privacy Company geen specifieke functies van Microsoft 365 Copilot waren. Toen de tests werden uitgevoerd, waren het genereren van afbeeldingen en spraakassistentie nog niet beschikbaar, evenmin als het Nederlands als taal. In juni 2025 werd een kleine hertest uitgevoerd in Word als app en in de browser met Copilot, en Microsoft verleende toegang tot de ruwe gegevens om de nieuwe conceptdocumentatie van Microsoft over de telemetriegegevens en vereiste servicegegevens te verifiëren.

Microsoft heeft de naam van zijn Copilot diensten meerdere keren gewijzigd. Aanvankelijk gebruikte Microsoft de naam 'Copilot with Enterprise Data Protection' voor de gratis toegang (zonder licentie) tot Copilot voor Education gebruikers. Microsoft gebruikt momenteel de naam 'Copilot Chat' voor deze zelfde onbetaalde Copilot dienst. Deze (2^e update) DPIA vermeldt kort enkele risico's met betrekking tot het gebruik van de gratis (consumenten) Copilot diensten, zowel met als zonder een Microsoft werkaccount, maar bevat geen volledige analyse. Deze DPIA heeft ook geen betrekking op het gebruik van een zelfgebouwd generatief AI-model op een afzonderlijke (privé)instantie van het OpenAI LLM, gehost op het cloudplatform Azure van Microsoft.

Over Microsoft 365 Copilot

Het belangrijkste verschil met de gratis Copilot Chat is dat de betaalde Microsoft 365 Copilot toegang heeft tot de *Graph* informatie, de informatie waartoe medewerkers toegang hebben in de M365 clouddiensten SharePoint, OneDrive en Exchange Online. Zowel de gratis als de betaalde versies van

Copilot genereren antwoorden op basis van de informatie in het Large Language Model (LLM) van OpenAI.

Zowel de gratis als de betaalde versie van Copilot hebben standaard toegang tot het internet via de op Bing gebaseerde webchat.

Om feitelijke informatie te verzamelen over de werking van Microsoft 365 Copilot heeft Privacy Company gescripte tests met prompts uitgevoerd en de antwoorden geanalyseerd. Er zijn 15 testscenario's ontwikkeld in samenwerking met de Data School en SURF Rijk, en technisch beoordeeld door Microsoft. SURF heeft 5 extra testscenario's toegevoegd die specifiek zijn afgestemd op de onderwijsomgeving.

Van 4 hoge risico's naar 2 medium risico's

In reactie op de eerste versie van deze DPIA, waarin vier hoge en zeven lage gegevensbeschermingsrisico's werden geïdentificeerd, heeft Microsoft maatregelen genomen of aangekondigd om de vier hoge risico's te beperken. Microsoft heeft geen beperkende maatregelen aangekondigd voor de oorspronkelijke zeven lage (na de eerste update negen) risico's.

In de eerste update van de DPIA werd geconcludeerd dat de maatregelen van Microsoft hebben bijgedragen aan het beperken van 2 van de geïdentificeerde hoge risico's. De maatregelen voor de overige twee hoge risico's hebben de impact en waarschijnlijkheid gedeeltelijk verminderd tot 2 medium risico's. Deze twee resterende medium risico's hebben betrekking op de verwerking van mogelijk onnauwkeurige en onvolledige persoonsgegevens in de gegenereerde antwoorden, en op de te ruwe bewaartermijn van 18 maanden voor de gepseudonimiseerde vereiste servicegegevens en telemetriegegevens.

SURF heeft tussen september 2025 en maart 2026 een dialoog gevoerd met Microsoft en Microsoft om aanvullende risicobeperkende maatregelen gevraagd, maar Microsoft heeft geen relevante nieuwe informatie over de twee medium risico's verstrekt.

Door Microsoft genomen risicobeperkende maatregelen

Sinds 2025 heeft Microsoft de volgende risicobeperkende maatregelen genomen.

- DSAR: Microsoft heeft uitgelegd waarom sommige velden in de diagnostische gegevens in het antwoord op het verzoek om inzage (DSAR) leeg waren: omdat Microsoft voor dat veld geen gegevens verzamelt en naar Microsoft verzendt.
- DSAR: Microsoft heeft toegezegd om in reactie op een DSAR toegang te verlenen tot zowel de telemetriegegevens als de vereiste servicegegevens. Microsoft zal alleen toegang verlenen tot de belangrijkste gebeurtenissen, en niet tot alle gebeurtenissen, om te voorkomen dat bij elke vervolggebeurtenis dezelfde persoonsgegevens worden verzonden.
- Transparantie: Microsoft heeft veel nieuwe artikelen gepubliceerd waarin wordt uitgelegd wat vereiste servicegegevens zijn (alle gegevens die naar Microsoft worden verzonden en door Microsoft worden verwerkt om gebruikers online functionaliteit te bieden, waaronder Copilot), en wat de gegevensstructuren zijn.

- Nauwkeurigheid: Microsoft heeft twee van de drie overeengekomen mitigerende maatregelen in de gebruikersinterface met betrekking tot nauwkeurigheid doorgevoerd, om overmatig vertrouwen op AI te helpen voorkomen. Eén maatregel (diepgaande bronvermeldingen) zal naar verwachting vanaf juni 2026 beschikbaar zijn.
- Nauwkeurigheid: Microsoft heeft toegezegd om tijdens een jaarlijkse bijeenkomst met SURF te overleggen over overkoepelende functionele verbeteringen aan Copilot die betrekking hebben op het verbeteren van de nauwkeurigheid van het systeem (op mondiaal niveau).
- Nauwkeurigheid: Microsoft heeft toegezegd om specifieke escalaties die door onderwijsinstellingen aan SURF zijn gemeld te bespreken, evenals de wijze waarop deze escalaties zijn aangepakt of opgelost. Microsoft kan bij OpenAI hertraining, filtering, verfijning en/of escalatie toepassen om ondersteuningsverzoeken over onnauwkeurige persoonsgegevens effectief op te lossen, en zal de gekozen methoden aan SURF toelichten, met enkele niet nader omschreven uitzonderingen. SURF heeft nog geen dergelijke verzoeken van onderwijsinstellingen ontvangen.
- Nauwkeurigheid: Microsoft heeft twee zinnen gepubliceerd over het doel van het nieuwe Workplace Harms-filter. Microsoft heeft geweigerd meer documentatie over Workplace Harms te verstrekken met voorbeelden die hetzelfde detailniveau bieden als het Harmful Content filter.
- Nauwkeurigheid: Microsoft heeft het voor Education-klanten mogelijk gemaakt om het Harmful Content filter uit te schakelen, mits zij een A5-licentie hebben. In de A3-licentie bestaat een dergelijke optie niet. Microsoft biedt geen enkele optie om het Workplace Harms filter uit te schakelen.
- Gegevensbewaring: Microsoft heeft bekendgemaakt dat het mogelijk de vereiste servicegegevens en telemetriegegevens gedurende de bewaartermijn van 18 maanden moet verwerken voor de drie overeengekomen verwerkingsdoeleinden. Klanten kunnen (in theorie) deze periode verkorten door een gebruikersaccount te verwijderen of hun gebruik van Microsoft 365 te beëindigen. Microsoft heeft geweigerd regels of richtlijnen te verstrekken over hoe het de bewaartermijnen verkort voor gegevens die niet gedurende de volledige 18 maanden nodig zijn. Microsoft vermeldt alleen dat Microsoft het beginsel van gegevensminimalisatie toepast en heeft aangegeven hoe het de gegevens gedurende de 18 maanden beschermt.

Nieuw risico bij gegevensoverdracht: flex routing

In maart 2026 introduceerde Microsoft een potentieel nieuw risico op het gebied van gegevensbescherming: de invoering van 'flex routing' voor het dataverkeer van Microsoft 365 Copilot. Microsoft heeft laten weten dat het voor nieuwe klanten gegevensoverdracht buiten de EU-gegevensgrens mogelijk zou maken, terwijl bestaande klanten hun instellingen moesten controleren. SURF heeft gecontroleerd dat Microsoft de instelling (voor gegevensverwerking uitsluitend binnen de EU) voor bestaande Nederlandse klanten in het onderwijs niet had gewijzigd. Omdat nieuwe Microsoft-klanten deze gegevensoverdracht kunnen uitschakelen, is dit punt toegevoegd als een nieuw 10^e laag risico.

De rol van Microsoft in het kader van de AVG, doeleinden en verenigbaarheid van verdere verwerking

Op basis van het framework met SURF verwerkt Microsoft contractueel en feitelijk alle persoonsgegevens uit de Microsoft 365 Education Online Services als gegevensverwerker. Dit omvat ook de gegevensverwerking door de betaalde Microsoft 365 Copilot. Deze DPIA identificeert echter vijf situaties waarin Microsoft heeft besloten gegevensverwerking buiten de instructies van de verwerker om toe te staan. Verwerking in deze situaties is niet verenigbaar met de doeleinden waarvoor Nederlandse onderwijsinstellingen Microsoft (als verwerker) toestaan persoonsgegevens te verzamelen.

Deze vijf situaties zijn:

1. Toegang tot Bing;
2. Toegang tot de consumentenversies van Copilot in Windows en Office 365 als gebruikers niet zijn aangemeld met hun schoolaccount, en toegang tot de gratis Copilot chat als ze wel zijn aangemeld met hun schoolaccount;
3. Het versturen van feedback naar het openbare feedbackforum (website);
4. Het uitnodigen van aangemelde gebruikers via een vooraf aangevinkt formulier om in te stemmen met commerciële mailings;
5. Het inschakelen van het Workplace Harms filter zonder adequate documentatie of opties om de filtering aan te passen of uit te schakelen.

Onderwijsinstellingen kunnen de hieruit voortvloeiende risico's beperken door de toegang tot Copilot Chat en de gratis consumentenversie van Copilot centraal te blokkeren, en door medewerkers te instrueren geen feedback te sturen of in te stemmen met commerciële mailings. Microsoft biedt geen opties om de vooraf ingestelde niveaus van het filter voor schadelijke inhoud uit te schakelen of te wijzigen bij de veelgebruikte A3-licentie, maar alleen bij de A5-licentie.

Resultaat: 2 medium en 10 lage gegevensbeschermingsrisico's

De uitkomst van deze 2^e DPIA-update is 2 medium en 10 lage gegevensbeschermingsrisico's.

Microsoft heeft 2 technische maatregelen genomen om het risico op onjuiste persoonsgegevens te helpen beperken en zal de derde overeengekomen maatregel in juni 2026 invoeren (diepgaande bronvermeldingen). Zolang er echter geen nieuwe maatregelen of nieuwe informatie van Microsoft beschikbaar zijn, worden twee risico's nog steeds als medium aangemerkt, namelijk met betrekking tot (i) de verwerking van mogelijk onjuiste en onvolledige persoonsgegevens en (ii) de te algemene bewaartermijn van 18 maanden voor de gepseudonimiseerde vereiste servicegegevens en telemetriegegevens.

SURF roept onderwijsinstellingen die Microsoft 365 Copilot gaan gebruiken op om alle klachten over onjuiste persoonsgegevens te melden. Deze beoordeling legt een zware verantwoordelijkheid bij de onderwijsinstellingen om te beoordelen voor welke werk- en leertaken zij het gebruik van Copilot kunnen toestaan zonder onaanvaardbare risico's voor de gegevensbescherming te veroorzaken. Zij moeten duidelijk beleid opstellen over het gebruik van generatieve AI, de aanbevelingen voor

privacyvriendelijke instellingen (waaronder het blokkeren van de toegang tot Bing) opvolgen en de kwaliteit van het met Copilot gegenereerde werk nauwlettend controleren.

Microsoft heeft niet gereageerd op de voorgestelde maatregelen voor de 7 oorspronkelijk geïdentificeerde lage gegevensbeschermingsrisico's.

De onderstaande tabel beschrijft specifieke risicobeperkende maatregelen die onderwijsinstellingen kunnen nemen om de 2 medium en 10 lage risico's te beperken, evenals eerder voorgestelde maatregelen die Microsoft zou kunnen nemen.

Nr.	Medium risico	Maatregelen onderwijsinstellingen	Maatregelen genomen door of voorgesteld aan Microsoft
1.	Aanzienlijk economisch of sociaal nadeel door het gebruik van gegenereerde teksten met onjuiste persoonsgegevens.	Overweeg om geen Microsoft 365 Copilot met een A3-licentie te gebruiken totdat Microsoft organisaties in staat stelt om het filter tegen schadelijke inhoud (Harmful Content) uit te zetten, en adequate transparantie geeft over het filter tegen werkplek schade (Workplace Harms). Met A5: Implementeer een beleid waarin wordt vastgelegd door welke eindgebruikers en wanneer de filtering van schadelijke inhoud uitgeschakeld mag worden. Stel een beleid op voor het gebruik van generatieve AI door medewerkers om correct gebruik te definiëren en, indien geactiveerd, DLP regels uit te leggen. Gebruik de nieuwe optie om het lettertype van de nauwkeurigheidswaarschuwing vetgedrukt te maken. Wijs gebruikers op de opties om bronverwijzingen te controleren en gebruik de nieuwe optie om de diepgaande bronvermeldingen voor elke bron waarnaar wordt verwezen te controleren wanneer Microsoft deze beschikbaar stelt. Geef instructies aan gebruikers om problemen met de RAI-filtering (tegen zowel schadelijke inhoud als werkplek schade), en problemen met gefilterde persoonsgegevens te melden aan copilotklacht@surf.nl	Beheerders kunnen een policy opstellen om (groepen) eindgebruikers toe te staan de Harmful Content filtering per chat uit te schakelen. Microsoft heeft Purview Data Loss Prevention (DLP) ingeschakeld voor Copilot prompts in Enterprise-Klanten. Microsoft biedt beheerders de mogelijkheid om het lettertype van de nauwkeurigheidswaarschuwing vetgedrukt te maken (door AI gegenereerde resultaten kunnen onnauwkeurig zijn) en een hyperlink naar het interne AI-beleid toe te voegen. Microsoft heeft duidelijke bronverwijzingen toegevoegd aan een nieuwe zijbalk en zal per juni 2026 diepgaande bronvermeldingen beschikbaar maken binnen de bronnen waarnaar wordt verwezen. Microsoft heeft twee zinnen gepubliceerd over het doel van het nieuwe filter voor schade op de werkplek (Workplace Harms filter). Microsoft heeft geweigerd om bedieningselementen aan te bieden om het Workplace Harmfilter uit te schakelen en om definities van Workplace Harmfilter te documenteren met voorbeelden die even gedetailleerd zijn als die van het Harmful Content filter. Microsoft zal gebruikers niet informeren dat er een filter is toegepast.

	Geef gebruikers de instructie om klachten of feedback over onjuiste persoonsgegevens te melden aan copilotklacht@surf.nl .	Microsoft zal: “de supportaanvraag waar nodig doorsturen naar de betreffende product- en feedbackteams. Indien nodig kunnen klanten ervoor kiezen om de ernstgraad te verhogen. Het supportteam houdt de klant op de hoogte van de voortgang en de uitkomst.” Microsoft heeft uitgelegd dat het supportaanvragen over onjuiste persoonsgegevens effectief kan oplossen door OpenAI opnieuw te trainen, te filteren, te verfijnen of te escaleren.
	Beheerders hebben toegang tot ingediende feedbackverzoeken van eindgebruikers en kunnen deze ook rapporteren aan SURF.	Microsoft zal klachten die naar SURF zijn gestuurd bespreken in een jaarlijkse vergadering, en met welke technologie het verzoek is opgelost, met enkele ongedefinieerde uitzonderingen.
	Instrueer/train gebruikers om de door Copilot gegenereerde persoonsgegevens altijd te controleren aan de hand van een onafhankelijke boordeling (door een collega) en betrouwbare bronnen.	Geen toezegging om statistieken te verstrekken over Microsofts eigen metingen van de kwaliteit en de onderbouwing van de output van Microsoft 365 Copilot, of inzage in tests en beoordelingen door derden om Microsoft's beweringen over voortdurende verbetering te verifiëren, met name in het Nederlands.
	Waarschuw gebruikers dat persoonsgegevens, met name over VIP's en professoren, gebaseerd kunnen zijn op verouderde en onjuiste trainingsgegevens die voor de LLM zijn gebruikt.	
	Voorkom de toewijzing van licenties aan accounts die toegang hebben tot (veel) bijzondere persoonsgegevens, zoals HR-gegevens	
	Schakel de toegang tot Bing uit en informeer gebruikers over de risico's voor betrokkenen als gevolg van de beperkingen van Copilot met betrekking tot de nauwkeurigheid van de gegenereerde gegevens.	Geen toezegging om de gegevensverwerking en doeleinden verder te beperken wanneer Bing is ingeschakeld.
	Schakel auditlogging in en stel regels op voor de controle op de naleving van het interne generatieve AI beleid, onder meer door controle op steekproeven van dialogen en diagnostische gegevens.	
	Houd de door Microsoft aangekondigde verbeteringen aan Copilot bij via meldingen in het Berichtencentrum en de M365-roadmap en lees het jaarlijkse RAI-filtrerapport .	

2.	Heridentificatie van gepseudonimiseerde gegevens door onbekende bewaartermijnen van <i>vereiste servicegegevens</i> (zowel inhoudelijke als diagnostische gegevens).	Geen maatregelen mogelijk, behalve het verwijderen van een account of het beëindigen van het contract voor M365-diensten.	Microsoft heeft bekendgemaakt dat het de diagnostische gebeurtenis gegevens voor Microsoft 365 apps en diensten, waaronder Microsoft 365 Copilot, tot 18 maanden bewaart , zonder voldoende motivering van de noodzaak van deze bewaartermijn, of uitleg over hoe het bepaalt wanneer gegevens voor een kortere periode moeten worden bewaard. Microsoft heeft uitgelegd dat het voor het verzamelen van deze gegevens als verwerker dezelfde evenredigheidseisen hanteert als bij de gecontroleerde, geautoriseerde verdere verwerking voor de legitieme zakelijke doeleinden van Microsoft.
----	--	---	---

Nr.	Laag risico	Maatregelen onderwijsinstellingen	Maatregelen genomen door of voorgesteld aan Microsoft
3.	Verlies van controle door gebrek aan transparantie <i>Vereiste servicegegevens en de telemetrie</i> gebeurtenissen van Webapp gebruikers.	Bestudeer de nieuwe publieke documentatie van Microsoft over de RSD en telemetriegegevens om de betrokkenen goed te kunnen informeren over de gegevensverwerkingen door een betaalde Copilot-licentie.	Microsoft heeft uitgebreide nieuwe documentatie gepubliceerd over het verschil tussen telemetriegegevens en RSD, en heeft uitgelegd dat er verschillende gegevensstromen zijn voor inhoudelijke gegevens in de RSD en diagnostische gegevens in de RSD.
		Stel het telemetrieniveau in Windows en Office 365 in op het minst ingrijpende niveau 'beveiligings'-'vereist'- niveau.	Microsoft bevestigt dat de diagnostische RSD geen inhoudelijke gegevens bevat, met uitzondering van bestandsnamen bij het delen van OneDrive-bestanden.
4.	Onvermogen van betrokkenen om inzagerechten uit te oefenen in hun diagnostische gegevens.	Dien een DSAR in en vergelijk de resultaten met de nieuwe openbare documentatie van Microsoft over de verschillende diagnostische gegevens (telemetriegegevens en RSD).	Microsoft heeft nieuwe documentatie gepubliceerd, waaronder een Readme-bestand, en biedt op een transparante, begrijpelijke en gemakkelijk toegankelijke manier toegang tot de telemetriegegevens en de vereiste servicegegevens over het gebruik van Microsoft 365 Copilot, met beschrijvende namen voor de bestanden en mappen. Microsoft legt ook uit waarom sommige velden leeg zijn.
			Microsoft documenteert alle RSD-name spaces en legt uit waarom het geen inzage geeft in meerdere telemetrieberichten die verwijzen naar dezelfde gebruikersactie.
			Microsoft verbindt zich ertoe een inzageverzoek in te willigen zonder dat de gegevens worden gewist terwijl het verzoek nog in behandeling is.
5.	Openbaarmaking van of toegang tot persoonsgegevens als gevolg van incidentele doorgiften aan ingehuurd personeel in 30 derde landen.	Maak gebruik van de professionele ondersteuningsdiensten, niet van de in-app ondersteuningsopties.	Geef specifiekere en consistente openbare uitleg over de waarschijnlijkheid van gegevensdoorgifte naar de VS voor veiligheidsdoeleinden en verdere doorgifte.
6.	Openbaarmaking van of toegang tot persoonsgegevens buiten de EU als gevolg van Copilot flex routing.	Nieuwe klanten: wijzig de standaardinstelling en schakel flex routing uit.	Schend de EU Data Boundary verbintenis, waarbij alle gegevensverwerking voor Core Services uitsluitend in de EU plaatsvindt, met SURF niet. Met uitzondering van beperkte doorgiften voor veiligheidsdoeleinden.

7.	Reputatieschade: onvermogen om (her)generatie van onjuiste persoonsgegevens in de output te voorkomen nadat een betrokkene een klacht heeft ingediend.	Dien een (Professional Services) ondersteuningsverzoek in om Microsoft te vragen het opnieuw genereren van duidelijk onjuiste persoonsgegevens te voorkomen.	Microsoft zal: <i>“het ondersteuningsverzoek doorsturen naar de betreffende product- en feedbackteams, indien van toepassing. Indien nodig kunnen klanten ervoor kiezen om de urgentie te verhogen. Het supportteam houdt de klant op de hoogte van de voortgang en het resultaat.”</i> Microsoft heeft uitgelegd dat het ondersteuningsverzoeken over onjuiste persoonsgegevens effectief kan oplossen door hertraining, filtering, finetuning of escalatie naar OpenAI toe te passen.
		Geef gebruikers de instructie om onjuiste persoonsgegevens te melden aan copilotklacht@surf.nl	
		Dien alleen feedbackverzoeken in bij meer algemene/minder urgente zaken.	
8.	Verlies van controle / verlies van vertrouwelijkheid als gevolg van verdere verwerking door Microsoft (als gevolg van standaardinstellingen).	Schakel de toegang tot de webchat (Bing) uit in zowel Microsoft 365 Copilot als in Copilot Chat. Raadpleeg de SLM-handleiding met privacy vriendelijke instellingen voor M365 .	Voldoe aan de wettelijke verplichting voor privacy by design en by default: wanneer Microsoft als gegevensverwerker wordt ingeschakeld, moet alle gegevensverwerking in de rol van verwerkingsverantwoordelijke standaard worden uitgeschakeld, inclusief toegang tot Bing via Copilot Chat.
		Schakel de optie uit om feedback te geven aan het openbare (verantwoordelijke) feedbackforum. Als andere soorten (verwerkers)feedbackdiensten niet zijn uitgeschakeld: bekijk de ingediende feedback via de beheerconsole.	
		Schakel de toegang tot de gratis versies van Copilot in Bing, Edge, Windows, Office en alle M365 services uit waar Microsoft toegang mogelijk maakt tot deze ‘Microsoft als verantwoordelijke’-versies van Copilot.	Microsoft heeft de geconstateerde glitch verholpen die optrad wanneer ‘Additional Optional Connected Experiences’ waren uitgeschakeld, en raadt nu aan om een groepsbeleid te gebruiken om de toegang tot Bing uit te schakelen, zowel in de gratis (consumenten)versie als in de betaalde versie.
		Schakel aanvullende optionele verbonden ervaringen in Office 365 uit.	
9.	Verlies van tijd en concentratie: gebruik van accountgegevens om e-mails te versturen.	Gebruik de centrale opt-out-functionaliteit voor alle of sommige gebruikers in de organisatie voor mailings over Microsoft 365 Copilot.	Overweeg opnieuw om e-mails naar gebruikers met een licentie te willen sturen. Deze verwerking is contractueel toegestaan, maar ethisch ongewenst.
		Geef gebruikers de instructie om alert te zijn op vooraf aangevinkte vakjes op de openbare ‘learn’ pagina’s van Microsoft.	Stop met het uitnodigen van aangemelde gebruikers met een vooraf ingevuld formulier om in te stemmen met commerciële mailings.

10.	Verlies van controle door onjuiste auteursnamen in Copilot antwoorden.	Leg gebruikers uit dat ze de auteursnamen moeten opzoeken van documenten in de 'Graph' die door Microsoft worden geciteerd.	Verbeter de metadata van auteurs van documenten in de 'Graph': wijs de inhoud niet toe aan de persoon die het bestand naar SharePoint of OneDrive heeft geüpload.
11.	Afschrikkend effect van gebruik van Copilot als personeelsvolgsysteem	Vul het interne privacybeleid voor de verwerking van persoonsgegevens van werknemers aan met regels voor de specifieke doeleinden waarvoor specifieke persoonsgegevens in de Microsoft 365 Copilot-dialoog en logbestanden (verder) mogen worden verwerkt en geanalyseerd. Dit omvat het opsommen van de specifieke risico's waartegen de historische dialoog- en logbestanden zullen worden gecontroleerd, en welke maatregelen de organisaties zullen nemen om doelbinding te waarborgen. Volg de aanbeveling uit eerdere DPIAs om de logbestanden van gebruikersactiviteiten gepseudonimiseerd weer te geven.	-geen maatregelen nodig-
12.	Verlies van controle over inhoudelijke gegevens in de Graph	Gebruik de nieuwe DLP-opties voor Microsoft 365 Copilot. Pas labeling toe om ervoor te zorgen dat adequate autorisaties kunnen worden ingesteld. Organiseer grondige opschoningssessies voor SharePoint en Outlook in overeenstemming met het bewaarbeleid voorafgaand aan gebruik van Microsoft 365 Copilot. Raadpleeg de richtlijnen van Microsoft.	Microsoft heeft Purview Data Loss Prevention (DLP) ingeschakeld voor Copilot prompts in Enterprise tenants.

Deel C. Bespreking en beoordeling van de risico's

Dit deel betreft de beschrijving en beoordeling van de risico's voor betrokkenen. Dit deel begint met een algemene identificatie van de risico's voor de rechten en vrijheden van betrokkenen als gevolg van de verwerking van de Inhoud en de Diagnostische Gegevens (inclusief de doeleinden van de verwerking van Accountgegevens).¹ De risico's worden vervolgens ingedeeld op basis van de waarschijnlijkheid dat ze zich voordoen en de impact op de rechten en vrijheden van de betrokkenen wanneer ze zich voordoen.

1. Risico's

1.1. Identificatie van risico's

Hieronder wordt een algemeen onderscheid gemaakt tussen de risico's van de verwerking van metagegevens enerzijds en de inhoudsgegevens anderzijds. Vervolgens worden 10 specifieke gegevensbeschermingsrisico's beschreven, waarvan er 7 betrekking hebben op de verwerking van diagnostische gegevens en 3 op de inhoudsgegevens.

In het algemeen kunnen gegevensbeschermingsrisico's in de volgende categorieën voorkomen:

- het onvermogen om rechten uit te oefenen (met inbegrip van, maar niet beperkt tot, privacyrechten)
- het onvermogen om toegang te krijgen tot diensten of mogelijkheden
- verlies van controle over het gebruik van persoonsgegevens
- discriminatie
- identiteitsdiefstal of fraude
- financieel verlies
- reputatieschade
- fysiek letsel
- verlies van vertrouwelijkheid
- heridentificatie van gepseudonimiseerde gegevens of
- enige andere aanzienlijke economische of maatschappelijke nadelen²

¹ In dit hoofdstuk wordt niet ingegaan op websitegegevens, omdat bij deze DPIA geen risico's met betrekking tot de cookiegegevens zijn vastgesteld.

² Lijst verstrekt door de ICO in de pre-Brexit-richtlijnen over DPIA's, niet langer openbaar beschikbaar.

Deze risico's moeten worden beoordeeld aan de hand van de waarschijnlijkheid dat ze zich voordoen (de kans) en de ernst van de gevolgen. De Nederlandse overheid biedt een risicoscoretabel aan in de model DPIA.³

Om de ernst van de gevolgen en de waarschijnlijkheid van de schade voor deze generieke risico's af te wegen, combineert dit rapport een lijst van specifieke risico's met de specifieke omstandigheden van de onderzochte gegevensverwerking.

1.2. Beoordeling van risico's

1.2.1. Aanzienlijk economisch of sociaal nadeel en verlies van controle als gevolg van het gebruik van gegenereerde teksten met onjuiste persoonsgegevens

Naast de mogelijkheid om via een (Professional Services) supportticket een individuele klacht in te dienen over onjuiste persoonsgegevens, moeten Microsoft en de Nederlandse onderwijsinstellingen ook generieke maatregelen nemen om ervoor te zorgen dat documenten met gegenereerde persoonsgegevens juist zijn.

Microsoft beveelt twee strategieën aan om de kwaliteit van de output van Microsoft 365 Copilot te verbeteren, zoals beschreven in sectie Error! Reference source not found.: het gebruik van Bing en het in staat stellen van medewerkers om feedbackgegevens naar Microsoft te verzenden.

Wanneer Microsoft verwijst naar het gebruik van Bing om de nauwkeurigheid van persoonsgegevens te verbeteren, baseert het zich op het gebruik van een dienst waarvan het de verwerkingsverantwoordelijke is. Testscenario 4 (over politicus Geert Wilders) laat zien dat de inzet van Bing resulteerde in een neutralere tekst, hoewel deze niet noodzakelijkerwijs nauwkeuriger was. Zoals geanalyseerd in sectie Error! Reference source not found. leidt het toestaan dat medewerkers persoonsgegevens en mogelijk vertrouwelijke gegevens delen met Microsoft als verwerkingsverantwoordelijke tot een onverenigbare verdere verwerking van inhoudsgegevens voor Microsofts eigen commerciële doeleinden. Dit is geen uniek standpunt voor Nederland of de EU: voor het Amerikaanse Congres heeft Microsoft de gegevensbescherming verbeterd door een versie aan te bieden waarin de toegang tot Bing standaard is uitgeschakeld.

Wat feedbackgegevens betreft, is Microsoft verwerkingsverantwoordelijke geworden voor 3 van de 4 soorten feedbackverzameling. Het versturen van feedback leidt echter niet tot een antwoord en kan organisaties niet helpen om aan te tonen dat zij voldoen aan het nauwkeurigheidsbeginsel uit artikel 5, lid 1, onder d, van de AVG.

Daarom kan noch het gebruik van Bing, noch het verzenden van feedbackgegevens onderwijsinstellingen helpen bij het oplossen van het probleem met onjuiste persoonsgegevens, met name wat betreft verouderde persoonsgegevens.

³ Model-DPIA Rijksdienst v3.0, september 2023, URL: <https://www.kcbr.nl/sites/default/files/2023-08/Rapportagemodel%20DPIA%20Rijksdienst%20v3.0.docx>.

Een ander obstakel is het ontwerp van de gebruikersinterface van Microsoft 365 Copilot. De dienst ziet eruit als een chatvenster, in plaats van als een venster waarin tekst kan worden geplakt en Copilot kan worden gevraagd deze uit te breiden. Dit ontwerp wekt bij gebruikers de illusie dat de tool feitelijke informatie ophaalt zoals een zoekmachine dat doet, in plaats van woorden te genereren in een statistisch waarschijnlijke volgorde, zoals een hulpmiddel voor het aanvullen van woorden op een smartphone werkt.

De illusie die voortvloeit uit dit ‘chat’ ontwerp wordt ook wel “The prompt myth” genoemd.⁴ De interface kan gebruikers gemakkelijk doen geloven dat ze een gesprek voeren met een actor die waarheidsgetrouw (en neutraal) reageert. Dit draagt verder bij aan de kans dat eindgebruikers onjuiste gegevens niet herkennen, zoals blijkt uit het gebruik van verzonnen bronnen, citaten en jurisprudentie door de meest gekwalificeerde professionals (universiteitsrector, hoofdredacteur en advocaten in Nederlandse rechtszaken).

Een ander punt met betrekking tot de nauwkeurigheid is de wijziging van inhoudsgegevens door middel van RAI-filtering. Zowel de prompt aan het LLM als de output van het LLM worden eerst door het filter voor schadelijke inhoud van Microsoft en het nieuwe Workplace Harms filter geleid.

De definitie van ‘schadelijk’ verschilt per land, afhankelijk van de culturele, religieuze, ethische en historische context. Aangezien Microsoft wereldwijd actief is, is het onduidelijk of deze filters de Europese mensenrechten respecteren.

Onderwijsinstellingen kunnen en moeten investeren in bewustwording van de risico’s van het gebruik van generatieve AI, maar zolang Microsoft zijn rol in het kader van de AVG bij de verwerking van persoonsgegevens via Bing niet wijzigt, is de kans redelijk groot dat docenten en studenten onjuiste persoonsgegevens niet altijd zullen herkennen, ondanks formele controles door meerdere lezers. Als gegenereerde documenten met dergelijke fouten onderdeel worden van de *Graph* en intern veelvuldig worden gedeeld, kunnen ze deel gaan uitmaken van een feedbackloop die de onjuistheden versterkt.

In reactie op deze beoordeling heeft Microsoft vier mitigerende maatregelen aangekondigd om de gebruikersinterface te bemoeilijken, zodat gebruikers zich meer bewust worden van het risico van overmatig vertrouwen op AI.

1. Beheerders de mogelijkheid bieden om de filter voor schadelijke inhoud (maar niet het Workplace Harms filter) uit te schakelen;
2. Beheerders de mogelijkheid geven om het lettertype van de AI-disclaimer vetgedrukt te maken
3. Geef de bronvermeldingen weer in de zijbalk
4. Toon gedetailleerde bronvermeldingen in de zijbalk – uitgesteld tot juni 2026

Microsoft heeft zich niet verplicht om als gegevensverwerker op te treden voor de Bing zoekopdrachten, noch om gelijkwaardige maatregelen te nemen voor de diagnostische gegevens die

⁴ Eryk Salvaggio, Challenging The Myths of Generative AI, 29 augustus 2024, URL: <https://www.techpolicy.press/challenging-the-myths-of-generative-ai/>.

het al verzamelt over de inhoud van de zoekopdrachten, noch om klanten de mogelijkheid te bieden het Workplace Harms filter uit te schakelen of aan te passen. Aangezien onderwijsinstellingen geen invloed kunnen uitoefenen op de instellingen en beslissingen van dit filter, kunnen zij alleen een (Professional Services) ondersteuningsverzoek indienen als zij vermoeden dat informatie ten onrechte wordt gefilterd. Het filteren van informatie die de Europese mensenrechtenwaarden correct weerspiegelt, is echter notoir moeilijker te detecteren dan de aanwezigheid van duidelijk onjuiste gegevens in gegenereerde teksten. Daarom bestaat er een redelijke kans dat eindgebruikers zich er niet van bewust zijn dat het filter te ver is gegaan. Het ontbreken van informatie over de werking van dit filter, in hoeverre het de Europese mensenrechtenwaarden correct weerspiegelt, kan zowel leiden tot een verlies van controle als tot aanzienlijke maatschappelijke achterstand. In reactie op deze analyse heeft Microsoft uitgelegd dat Copilot zal toelichten waarom het geen inhoud genereert die individuen beoordeelt of veroordeelt. Volgens Microsoft is er daarom geen redelijke kans dat de gebruiker zich niet bewust is van het filter.⁵

Microsoft heeft geweigerd zijn eigen kwaliteits- en nauwkeurigheidsstatistieken met SURF te delen om de toenemende nauwkeurigheid aan te tonen. Microsoft stemt er alleen mee in om algemene functionele ontwikkelingen te bespreken die verband houden met de verbetering van de nauwkeurigheid van het systeem.

Kortom, Microsoft heeft enkele belangrijke mitigerende maatregelen genomen of aangekondigd om de kans te verkleinen dat Microsoft 365 Copilot onnauwkeurige, onvolledige en verzonden persoonsgegevens genereert. Vanwege het ontbreken van adequate maatregelen voor het Workplace Harms filter en omdat de diepgaande bronvermeldingen nog niet beschikbaar zijn, kan de kans op het optreden van dergelijke gevallen nog niet tot verwaarloosbaar laag worden teruggebracht. De impact voor betrokkenen (groepen in de samenleving) kan groot zijn, indien medewerkers in het onderwijs onjuiste of ten onrechte ontbrekende persoonsgegevens in gegenereerde teksten, zoals samenvattingen, niet opmerken, of indien zij citaten of artikelen toeschrijven aan niet-bestaande auteurs. Afhankelijk van de context van de onnauwkeurigheid kan de impact van een weglating groot zijn. Bijvoorbeeld wanneer wetenschappelijke artikelen van nieuwe medewerkers systematisch worden genegeerd ten gunste van eerdere bijdragen, terwijl het aantal verwijzingen naar artikelen een belangrijke rol speelt in wetenschappelijke loopbanen. Daarom moeten de risico's voor betrokkenen (nog steeds) als medium worden aangemerkt.

1.2.2. Heridentificatie van gepseudonimiseerde gegevens door onbekende bewaartermijnen van *vereiste servicegegevens* (waaronder zowel inhouds- als diagnostische gegevens)

Zoals beschreven in sectie **Error! Reference source not found.**, bestaat er een discrepantie tussen de openbare documentatie van Microsoft over bewaartermijnen en de feitelijke bewaartermijnen. De openbare bewaartabel van Microsoft suggereert dat telemetriegegevens tot 6 maanden na beëindiging van het contract door de klant kunnen worden bewaard (passieve verwijdering, max. 180 dagen). In werkelijkheid bewaart Microsoft de telemetriegegevens van de geïnstalleerde M365 apps

⁵ Input van Microsoft van 22 mei 2026 over de definitieve versie van deze ^{2e} update van de DPIA.

gedurende een periode van maximaal 18 maanden. Evenzo verwijdt Microsoft de diagnostische vereiste servicegegevens na een periode van maximaal 18 maanden.

Microsoft geeft niet voldoende onderbouwing voor de noodzaak van deze lange bewaartermijn, noch een uitleg over hoe het bepaalt wanneer de gegevens voor een kortere periode moeten worden bewaard. Microsoft benadrukt dat deze periode geen hoge risico's met zich meebrengt: „*dankzij de maatregelen die worden toegepast bij het genereren en verwerken van service gerelateerde diagnostische gegevens, worden de risico's die verband houden met het opslaan van dergelijke gegevens tot een minimum beperkt.*”⁶

Bij gebrek aan meer gedetailleerde informatie over de daadwerkelijke bewaartermijn en de criteria die Microsoft hanteert om te bepalen wanneer gebeurtenissen eerder moeten worden verwijderd, moet SURF ervan uitgaan dat alle gepseudonimiseerde vereiste servicegegevens en telemetriegegevens maximaal 18 maanden worden bewaard. SURF neemt kennis van de verklaring van Microsoft, zoals geciteerd in de paragrafen **Error! Reference source not found.** en **Error! Reference source not found.**, dat het in zijn rol als gegevensverwerker precies dezelfde gecontroleerde procedures en maatregelen toepast op de verwerking van de gepseudonimiseerde vereiste servicegegevens.

Niettemin heeft SURF de feitelijke bewaartermijnen nog niet via een onafhankelijke audit geverifieerd, en biedt Microsoft geen auditrapporten aan waarin de naleving van de bewaartermijnen wordt geverifieerd. Daarom kan SURF het risico voor betrokkenen niet als laag beoordelen, zoals Microsoft voorstelt.

De kans op heridentificatie van gepseudonimiseerde gegevens neemt toe naarmate de gegevens langer worden bewaard, omdat de dataset in de loop van de tijd toeneemt. Bij gebrek aan meer details over hoe Microsoft bepaalt welke gegevens 18 maanden moeten worden bewaard en welke gegevens veel korter worden bewaard, kan de kans op heridentificatie niet als verwaarloosbaar worden aangemerkt. De impact van de verwerking van gepseudonimiseerde gegevens is niet groot, maar ook niet klein. Potentiële heridentificatie stelt de betrokkene bloot aan het risico om het doelwit te worden van social engineering, spear phishing en/of chantage. Daarom zijn de risico's voor betrokkenen (nog steeds) medium.

1.2.3. Verlies van controle door gebrek aan transparantie: vereiste servicegegevens, waaronder telemetriegebeurtenissen van webapp gebruikers

Zoals beschreven in sectie **Error! Reference source not found.** heeft Microsoft tijdens het bijwerken van deze DPIA uitgebreide nieuwe documentatie gepubliceerd over het verschil tussen telemetriegegevens en vereiste servicegegevens, en uitgelegd dat er verschillende gegevensstromen zijn voor inhoudsgegevens in de RSD en diagnostische gegevens in de RSD. Om gebruikers te helpen de telemetriegegevens die Microsoft verzamelt op een hoog niveau te begrijpen, heeft Microsoft een overzicht gepubliceerd van veelvoorkomende naamruimten ('name spaces') voor Microsoft 365 voor diagnostische gegevens (zowel de diagnostische gegevens die deel uitmaken van de RSD als de

⁶ Brief van Microsoft aan SLM Rijk, 15 augustus 2025.

telemetriegegevens). Microsoft heeft ook uitgelegd dat al deze naamruimten relevant kunnen zijn voor het gebruik van Microsoft 365 Copilot. Elke naamruimte kan veel verschillende gebeurtenissen omvatten, maar veel gebeurtenissen bevatten dezelfde informatie. Microsoft publiceert ook enkele voorbeelden van de RSD die het verzamelt met betrekking tot de Microsoft 365 Copilot-chat (de browser gebaseerde toegang).

Privacy Company kon geen exacte documentatie vinden voor de 208 waargenomen soorten telemetriegebeurtenissen op het minimale 'vereiste' niveau, alleen beschrijvingen van de naamruimten. Deze beschrijvingen zijn zeer algemeen. Zoals beoordeeld in sectie stelt deze documentatie verwerkingsverantwoordelijken in staat om gebruikers op een zeer hoog niveau te informeren over de verwerking van persoonsgegevens, maar niet op het niveau van individuele gebeurtenissen.

De nieuwe documentatie van Microsoft over het bestaan, de inhoud en de doeleinden van de RSD van Microsoft 365 Copilot, inclusief de telemetrie van de webapp-gebruiker houdt in dat verwerkingsverantwoordelijken gebruikers op een hoog niveau kunnen informeren over de verwerking van persoonsgegevens in overeenstemming met artikel 14 AVG. Dit betekent dat de kans op verlies van controle voor Nederlandse onderwijsinstellingen zeer klein is.

De impact op betrokkenen van de verwerking van de gepseudonimiseerde telemetriegegevens en diagnostische RSD kan variëren van laag tot hoog (in geval van heridentificatie met het oog op openbaarmaking aan een buitenlandse overheidsinstantie).

Gezien de zeer geringe kans zijn de risico's voor betrokkenen laag, ook al kan de impact van de verwerking groot zijn.

1.2.4. Onvermogen om de toegangsrechten van betrokkenen tot diagnostische gegevens uit te oefenen

Zoals beoordeeld in sectie **Error! Reference source not found.** heeft Microsoft toegezegd toegang te verlenen tot de belangrijkste diagnostische gegevens (zowel de telemetriegegevens als de diagnostische vereiste servicegegevens).

Microsoft publiceert nu documentatie over wat gebruikers kunnen verwachten wanneer zij toegang aanvragen, inclusief een Readme bestand. Microsoft verbindt zich ertoe om op een transparante, begrijpelijke en gemakkelijk toegankelijke manier toegang te verlenen tot de telemetriegegevens en de diagnostische vereiste servicegegevens over het gebruik van Microsoft 365 Copilot, met beschrijvende namen voor de bestanden en mappen.⁷ Microsoft legt ook uit waarom sommige velden in gebeurtenissen leeg zijn.⁸

Het kostte Microsoft 30 dagen om de gevraagde gegevensexport van de diagnostische gegevens in de kleine testtenant van Privacy Company en van SURF te voltooien. Microsoft verbindt zich ertoe zo snel

⁷ Microsoft, Inzicht in Microsoft 365-diagnostische gebeurtenissen in geëxporteerde gegevens, 30 april 2026, URL: <https://learn.microsoft.com/en-us/microsoft-365-apps/privacy/diagnostic-events-exported-data>.

⁸ Microsoft, 'Hoe zien diagnostische gebeurtenissen in exporten eruit?', 30 april 2026, URL: <https://learn.microsoft.com/en-us/microsoft-365-apps/privacy/diagnostic-events-exported-data#what-do-diagnostic-events-in-exports-look-like>.

mogelijk toegang te verlenen, zonder dat gegevens verloren gaan die voor kortere periodes worden opgeslagen.

Wat betreft de toegang tot de inhoudsgegevens: de historische Microsoft 365 Copilot dialogen worden opgeslagen in een verborgen e-mailmap van een gebruiker, in een afzonderlijk bericht per vraag en elk antwoord als een HTML-bijlage in een volgend e-mailbericht. Het vergt veel inspanning van een beheerder om een betrokkene toegang te verlenen tot deze gegevens, maar het is mogelijk. Microsoft biedt wel een gebruiksvriendelijker alternatief, namelijk eDiscovery via Purview, maar deze toegang is alleen beschikbaar als onderdeel van een A5-licentie, terwijl veel onderwijsinstellingen een A3-licentie gebruiken.

Dankzij de risicobeperkende maatregelen van Microsoft is de kans op onvolledige toegang tot de diagnostische gegevens zeer klein. Hoewel de impact van een toegangsbeperking groot is, omdat toegang tot persoonsgegevens een grondrecht is, kunnen de risico's voor betrokkenen als laag worden aangemerkt.

1.2.5. Openbaarmaking van of toegang tot persoonsgegevens als gevolg van incidentele doorgifte aan ingehuurd personeel in 30 derde landen

In deze DPIA wordt ervan uitgegaan dat onderwijsinstellingen de aanbeveling zullen opvolgen om de toegang tot Bing, het openbare feedbackforum en de consumenten/gratis versies van Copilot uit te schakelen, aangezien Microsoft geen specifieke informatie verstrekt over gegevensoverdrachten naar derde landen wanneer Microsoft als verwerkingsverantwoordelijke optreedt. Deze overdrachten vallen buiten het bestek van de onderstaande beoordeling.

Hoewel Nederlandse onderwijsinstellingen de gegevensoverdracht vanuit Microsoft 365 Copilot naar derde landen kunnen beperken door de „EU Data Boundary“ te selecteren, geldt deze geolocatiebeperking niet voor alle persoonsgegevens. Microsoft draagt nog steeds incidenteel en systematisch bepaalde persoonsgegevens over naar derde landen, doordat het personeel in de VS en in derde landen toegang krijgt tot deze persoonsgegevens. De toegang kan betrekking hebben op accountgegevens, inhoudsgegevens, diagnostische gegevens, de inhoud van supporttickets en websitegegevens. In tegenstelling tot andere 'Big Tech' aanbieders beschikt Microsoft niet over een in de EU gevestigde helpdesk en biedt het zijn Professional Services klanten geen mogelijkheid om hulp te vragen aan medewerkers die in de EU zijn gevestigd.

Er zijn twee relevante soorten gegevensoverdrachten: (i) persoonsgegevens die mogelijk toegankelijk zijn voor ingehuurd personeel in 30 geïdentificeerde 'derde' landen (landen zonder adequate wetgeving inzake gegevensbescherming) en (ii) gepseudonimiseerde logbestanden die worden gebruikt voor beveiligingsdoeleinden en die via beveiligde terminals vanuit de VS en door technici in de derde landen kunnen worden geraadpleegd, of die in de VS worden geaggregeerd en opgeslagen en 'in alle Azure-regio's' beschikbaar worden gesteld.

Voor doorgiften naar de VS en naar derde landen (door Microsoft als gegevensverwerker) blijft SURF vertrouwen op de SCC's. Zolang de VS worden geacht een adequaat niveau van gegevensbescherming te hebben, hoeven organisaties geen extra maatregelen te nemen naast de SCC's voor de doorgifte naar de VS van geaggregeerde beveiligingslogbestanden, of voor de verdere doorgifte van dergelijke

logbestanden op basis van het EU-VS-kader voor gegevensbescherming. Daarom gaat dit hoofdstuk uitsluitend in op de toegang van Microsoft-personeel in de derde landen tot gegevens die in de EU zijn opgeslagen.

Microsoft heeft geen statistieken verstrekt over de frequentie waarmee zijn ingehuurd personeel in de 30 geïdentificeerde derde landen daadwerkelijk toegang heeft gehad tot persoonsgegevens van Nederlandse klanten uit de publieke sector via Office 365, noch biedt Microsoft specifieke statistieken over dergelijke toegang in verband met het specifieke gebruik van Microsoft 365 Copilot.

Microsoft past een combinatie van technische en organisatorische maatregelen toe om ongeoorloofde toegang tot persoonsgegevens door (extern ingehuurde) medewerkers in de 30 geïdentificeerde derde landen te voorkomen, bijvoorbeeld door de export van de gegevens te verhinderen. Microsoft legt uit dat deze toegang betrekking kan hebben op klantgegevens en gepseudonimiseerde persoonsgegevens, maar stelt dat de waarschijnlijkheid van dergelijke toegang zeer laag is.

Om de waarschijnlijkheid van toegang op afstand vanuit derde landen beter te begrijpen, heeft Microsoft uitgelegd dat er drie relevante factoren zijn. Ten eerste worden problemen doorgaans opgelost door middel van serviceautomatisering. Ten tweede is de kans zeer klein dat, indien een technicus handmatig moet ingrijpen, specifieke Nederlandse onderwijsgegevens deel uitmaken van de gegevens waartoe die technicus toegang heeft. En ten derde is de waarschijnlijkheid dat een overheidsfunctionaris geduldig naast een technicus zal wachten tot dergelijke gegevens verschijnen en vervolgens openbaarmaking zal afdwingen, uiterst klein.⁹

In reactie op deze DPIA heeft Microsoft bevestigd dat het **nooit** persoonsgegevens van Enterprise en Education klanten in EU/EVA landen aan overheidsinstanties heeft verstrekt. Dit omvat ook de mogelijke verstrekking door zijn subverwerkers in derde landen.

Gezien de lage kans dat Microsoft (en zijn subverwerkers) worden gedwongen om persoonsgegevens van Nederlandse onderwijsinstellingen aan een overheidsinstantie openbaar te maken, kunnen organisaties ervan uitgaan dat de kans dat hun persoonsgegevens in derde landen worden geraadpleegd zeer klein is. Hoewel de impact van gedwongen openbaarmaking van persoonsgegevens aan een overheidsinstantie in een derde land zeer groot kan zijn, zijn de risico's voor betrokkenen laag.

1.2.6. Openbaarmaking van of toegang tot persoonsgegevens buiten de EU als gevolg van Copilot Flex Routing.

Zoals beschreven in sectie **Error! Reference source not found.** heeft Microsoft in april 2026 een nieuwe 'Flex Routing'-uitzondering ingevoerd op zijn EU Data Boundary toezegging voor Microsoft 365 Copilot klanten. Tijdens piekuren wil Microsoft de zoekopdrachten (inhoudsgegevens) kunnen verwerken in LLM's buiten de EU, namelijk in de VS, Canada en Australië. Nieuwe M365 klanten kunnen deze nieuwe instelling uitschakelen; bestaande klanten moeten controleren of Microsoft de

⁹ Antwoorden van Microsoft op de DPIA's van SLM en SURF, 8 november 2024.

instellingen heeft gewijzigd. Privacy Company heeft in de Nederlandse onderwijs A5 testtenant geverifieerd dat de instellingen niet waren gewijzigd.

De impact van deze gegevensoverdracht kan groot zijn, aangezien de adequaatheidsstatus van de VS omstreden is en Australië geen adequaatheidsstatus heeft. Als nieuwe Nederlandse onderwijsinstellingen 'Flex Routing' voorkomen, kan het risico hierop tot een laag niveau worden teruggebracht. Bestaande klanten zullen echter ook hun instellingen in de gaten moeten houden, aangezien Microsoft zich het recht voorbehoudt om nieuwe permanente uitzonderingen op de EU-Data Boundary in te voeren.

Door nieuwe gegevensoverdrachten te voorkomen, kan de grote impact worden beperkt en kunnen de risico's voor de betrokkenen als laag worden aangemerkt.

1.2.7. Reputatieschade: het onvermogen om te voorkomen dat onjuiste persoonsgegevens in de uitvoer (opnieuw) worden gegenereerd nadat een betrokkene een klacht heeft ingediend.

Microsoft 365 Copilot kan aannemelijk klinkende maar onjuiste uitspraken over personen genereren, zoals beschreven in sectie **Error! Reference source not found.** De gevolgen van dergelijke onjuiste informatie kunnen ernstig zijn voor deze betrokkenen en leiden tot ernstige reputatieschade. In sectie **Error! Reference source not found.** worden de voorbeelden van de Noorse vader en de Duitse rechtbankverslaggever genoemd.

Zoals beoordeeld in sectie 1.2.1 hierboven, is de kans dat onjuiste en verzonnen persoonsgegevens voorkomen groter dan dat dit niet het geval is. De impact kan zeer groot zijn, indien een betrokkene ten onrechte wordt beschuldigd of in verband wordt gebracht met onwettig gedrag, of indien verzonnen citaten aan echte personen worden toegeschreven.

Mocht het echter voorkomen dat gebruikers schadelijke onjuiste persoonsgegevens over zichzelf of collega's waarnemen, dan nodigt Microsoft onderwijsinstellingen uit om een (Professional Services) supportticket in te dienen. Microsoft heeft SURF verzekerd dat het klachten over onjuiste persoonsgegevens kan aanpakken met behulp van diverse technische oplossingen, afhankelijk van de specifieke situatie. Dergelijke oplossingen omvatten hertraining, filtering, finetuning of escalatie naar OpenAI. Microsoft heeft hieraan toegevoegd:

„Onjuiste output met betrekking tot persoonsgegevens kan het gevolg zijn van situaties waarop Microsoft geen invloed heeft. Bijvoorbeeld als gevolg van onjuiste basisgegevens in de Graph van de klant, of het ontbreken van webverankering. In dergelijke gevallen is de gebruiker verantwoordelijk voor het nemen van passende maatregelen om de schade te beperken.”¹⁰

Microsoft heeft uitgelegd dat het contractueel verboden is om statistieken op te stellen over het aantal klachten dat door onderwijsinstellingen in Nederland wordt ingediend over onjuiste persoonsgegevens, maar als SURF dergelijke klachten van instellingen verzamelt, zal Microsoft tijdens een jaarlijkse bijeenkomst met SURF bespreken hoe het deze klachten heeft opgelost, afgezien van enkele niet nader genoemde uitzonderingen.

¹⁰ Antwoord van Microsoft op de eerste bijgewerkte DPIA, 10 september 2025.

Ervan uitgaande dat onderwijsinstellingen hun medewerkers en volwassen studenten zullen aanmoedigen om dergelijke tickets bij Microsoft in te dienen en een kopie naar SURF te sturen, kan Microsoft op basis van het supportticket effectieve maatregelen nemen om te voorkomen dat de betwiste gegevens opnieuw worden gegenereerd. Als SURF inderdaad kopieën van klachten ontvangt, kan het de effectiviteit van de mitigerende oplossingen monitoren. In dat geval kan de grote impact worden beperkt en kunnen de risico's voor de betrokkenen als laag worden aangemerkt.

1.2.8. Verlies van controle / verlies van vertrouwelijkheid als gevolg van verdere verwerking door Microsoft

Microsoft schakelt standaard drie diensten als verwerkingsverantwoordelijke in, zoals beschreven in sectie 6.3.4. Dit betreft toegang tot de Bing webchat, toegang tot consumentenversies van Copilot en feedback aan het openbare feedbackforum. Het toestaan dat medewerkers persoonsgegevens delen met Microsoft als verwerkingsverantwoordelijke leidt tot een onverenigbare verdere verwerking van inhoudsgegevens voor Microsofts eigen commerciële doeleinden, zoals beoordeeld in de paragrafen Error! Reference source not found. tot en met Error! Reference source not found.

De kans dat Microsoft als verwerkingsverantwoordelijke persoonsgegevens verder verwerkt, is echter klein, omdat in deze DPIA wordt aangenomen dat onderwijsinstellingen de toegang tot de Bing webchat, de gratis versies van Copilot en het openbare feedbackforum zullen uitschakelen.

De impact van een verlies van vertrouwelijkheid is groot. Indien onderwijsinstellingen de diensten van de verwerkingsverantwoordelijke ingeschakeld laten, delen zij inhoudsgegevens die vertrouwelijk of zeer gevoelig kunnen zijn of bijzondere categorieën persoonsgegevens kunnen bevatten, met Microsoft als verwerkingsverantwoordelijke. Microsoft erkent dit risico eveneens. Zoals vermeld in sectie Error! Reference source not found. biedt Microsoft nu een versie van Copilot aan voor klanten van de Amerikaanse overheid, waarin de toegang tot de Bing webchat standaard is uitgeschakeld.

Ervan uitgaande dat onderwijsinstellingen de drie bovengenoemde diensten van de verwerkingsverantwoordelijke uitschakelen, kan het risico voor betrokkenen als laag worden aangemerkt.

1.2.9. Tijdverlies en concentratieverlies: ongevraagde e-mails van Microsoft

Privacy Company heeft vastgesteld dat Microsoft de accountgegevens van gebruikers gebruikt om een uitnodigingsscherm voor aanmelding voor commerciële e-mails vooraf in te vullen.

De kans dat dit risico zich voordoet, is groter dan dat het niet gebeurt. De gevolgen voor de betrokkenen variëren. Het ontvangen van ongevraagde commerciële e-mails leidt over het algemeen alleen tot ergernis bij de ontvangers (een verlies van tijd en aandacht), maar de accountgegevens van hooggeplaatste medewerkers in het onderwijs en systeembeheerders zijn gevoelige gegevens, zoals beschreven in sectie Error! Reference source not found. Als dergelijke gegevens terechtkomen in systemen buiten de grenzen van de verwerkers van Microsoft, verliezen Nederlandse onderwijsinstellingen de controle over de doeleinden van de verwerking. Microsoft maakt zelfs gebruik van een 'dark pattern' om gebruikers te misleiden en hen te laten inschrijven op een mailinglijst waarover Microsoft als verwerkingsverantwoordelijke de controle heeft.

Als onderwijsinstellingen hun medewerkers en studenten voor deze praktijk waarschuwen, kunnen ze de meeste onbedoelde inschrijvingen voorkomen. De ontvangers kunnen zich bovendien in elke e-mail die ze ontvangen uitschrijven. Samen verminderen deze maatregelen de kans dat het risico zich voordoet.

Op basis van het inschrijvingskader met SURF mag Microsoft de accountgegevens van medewerkers of beheerders niet gebruiken om hen ongevraagde commerciële e-mails te sturen over Microsoft producten of diensten die de klant niet gebruikt. Microsoft is echter contractueel gerechtigd om e-mails te sturen naar eindgebruikers voor wie een Microsoft 365 Copilot licentie is aangeschaft, zelfs als de gebruiker de dienst nog nooit heeft gebruikt. Privacy Company heeft herhaaldelijk gevallen van dergelijke ongevraagde e-mails geconstateerd. Het lezen van dergelijke e-mails kost tijd en concentratie, zelfs als ze onmiddellijk worden verwijderd. Microsoft biedt beheerders een effectieve en collectieve afmeldingsmogelijkheid om deze overlast te verminderen.

Als beheerders gebruikmaken van de collectieve afmeldingsmogelijkheid voor de mailings aan eindgebruikers, kunnen zij de kans dat dit risico zich voordoet tot bijna nul terugbrengen. De impact voor de twee gevallen varieert van minimaal tot enige impact (indien direct identificeerbare contactgegevens van hooggeplaatste medewerkers in het onderwijs en systeembeheerders buiten de grenzen van de gegevensverwerker zouden worden verwerkt). Vanwege de mogelijkheden om de kans op het optreden van dit risico te verlagen, kan het risico voor betrokkenen als laag worden aangemerkt.

1.2.10. Verlies van controle als gevolg van onnauwkeurige auteursnamen in antwoorden van Microsoft 365 Copilot

Zoals beoordeeld in sectie **Error! Reference source not found.** genereert Microsoft 365 Copilot niet altijd de juiste auteursnamen. Microsoft 365 Copilot lijkt soms uit te gaan van de kolom 'gewijzigd door', in plaats van de naam van de auteur in de PDF.

Volgens Microsoft is dit probleem te wijten aan het gebrek aan historische activiteit in de testtenant **[vertrouwelijk]**.

Maar zelfs als een klant een actieve tenant zou hebben, zou dit de onnauwkeurigheid in deze specifieke test niet hebben voorkomen. Een student zou de 10 wetenschappelijke artikelen in SharePoint kunnen uploaden zonder deze artikelen te delen, d.w.z. zonder metadata waarmee Microsoft 365 Copilot deze artikelen op populariteit kan rangschikken en de juiste auteursnaam kan detecteren.

Aangezien de onjuiste toeschrijvingen tijdens de tests zijn waargenomen en de beschikbaarheid van meer historische metadata in actieve tenants het optreden van dit probleem niet volledig kan voorkomen, is er een redelijke kans dat dit risico zich zal voordoen. Deze DPIA gaat er echter van uit dat onderwijsinstellingen hun medewerkers en volwassen studenten zullen instrueren om auteursnamen in bronnen uit de *Graph* te verifiëren. Aangezien Microsoft 365 Copilot (nog) niet beschikbaar is voor gebruikers jonger dan 18 jaar, kunnen dergelijke instructies helpen de kans op het optreden van dit risico tot verwaarloosbaar te verminderen.

Er zijn twee soorten gevolgen voor betrokkenen: voor de docenten en studenten als hun auteursvermeldingen onjuist zijn, en voor de auteurs die ofwel worden genegeerd ofwel ten onrechte als auteur worden aangemerkt. Afhankelijk van de context van de onnauwkeurigheid kunnen de gevolgen van deze onnauwkeurigheden groot zijn, bijvoorbeeld als wetenschappelijke artikelen van nieuwe medewerkers systematisch worden genegeerd ten gunste van eerdere bijdragen, terwijl het aantal verwijzingen naar artikelen een belangrijke rol speelt in wetenschappelijke loopbanen.

Ervan uitgaande dat onderwijsinstellingen de aanbevolen maatregelen toepassen en dat huurders doorgaans over meer historische metadata beschikken, kunnen de risico's voor betrokkenen als laag worden aangemerkt.

1.2.11. Afschrikkend effect van het systeem voor werknemersmonitoring

Onderwijsinstellingen hebben toegang tot auditlogboeken met informatie over de specifieke acties en documenten die door Microsoft 365 Copilot zijn beoordeeld, zoals beschreven in de secties **Error! Reference source not found.** en **Error! Reference source not found.**. De logboeken bevatten direct en indirect identificeerbare gegevens. Daarnaast stelt Microsoft de gebruikersactiviteiten logboeken van Microsoft 365 Copilot beschikbaar als individuele logboeken en in de vorm van geaggregeerde gegevens, en kunnen beheerders de historische dialogen (inhoudsgegevens) raadplegen via de eDiscovery tool, zoals beschreven in de sectie **Error! Reference source not found.**

De inhoudsgegevens en diagnostische gegevens kunnen beheerders gedetailleerde inzichten verschaffen in het individuele werkgedrag. Op basis van de rapporten zouden managers vergelijkingen kunnen maken tussen medewerkers met betrekking tot hun gebruik van Microsoft 365 Copilot, bijvoorbeeld over hoe en wanneer medewerkers met Copilot communiceren en welke documenten Microsoft 365 Copilot heeft geopend. De historische dialoogbestanden maken een nog specifiekere monitoring mogelijk.

Mocht diagnostische data worden gebruikt als systeem voor het monitoren van medewerkers, dan zouden de gevolgen zeer groot kunnen zijn. De wetenschap dat een werkgever gedetailleerde gebruiksgegevens voor evaluatiedoeleinden kan verwerken, kan een *afschrikkend effect* hebben op docenten en studenten die Microsoft 365 Copilot gebruiken. Zij kunnen vrezen dat het monitoring ma zou kunnen worden gebruikt voor een negatieve prestatiebeoordeling, indien dit niet specifiek is uitgesloten in een (intern) privacybeleid voor de verwerking van persoonsgegevens van werknemers. Een dergelijke monitoring kan hen beletten legitiem gebruik te maken van daarmee samenhangende grondrechten, zoals de vrijheid om informatie te verzenden en te ontvangen.

Voor bepaalde categorieën medewerkers in het onderwijs bestaat er een extra risico wanneer uit de logbestanden blijkt dat Microsoft 365 Copilot regelmatig toegang heeft tot vertrouwelijke of anderszins gevoelige informatie. Dergelijke medewerkers kunnen het doelwit worden van spearphishing (een vorm van oplichting via e-mail of andere elektronische communicatie die specifiek gericht is op een persoon of organisatie), social engineering (een aanvalstechniek die misbruik maakt van menselijke eigenschappen zoals nieuwsgierigheid, vertrouwen en hebzucht om vertrouwelijke informatie te verkrijgen of het slachtoffer een bepaalde handeling te laten verrichten) of chantage.

In de context van de Nederlandse onderwijssector is de kans dat deze gegevensverwerking tot afschrikkende effecten leidt, zeer klein. Deze DPIA gaat ervan uit dat onderwijsinstellingen de aanbeveling voor Nederlandse Microsoft 365-beheerders opvolgen om pseudonimisering toe te passen op alle gebruikerslogs binnen de verschillende diensten.¹¹ Bovendien gaat deze DPIA ervan uit dat onderwijsinstellingen een intern privacybeleid zullen implementeren met regels en legitieme, specifieke doeleinden voor de (verdere) verwerking van deze dialogen en logbestanden, inclusief toezicht op de toegang door (globale) beheerders tot de diagnostische gegevens.

Ervan uitgaande dat onderwijsinstellingen een adequaat intern privacybeleid implementeren en de naleving daarvan controleren, kunnen de risico's voor betrokkenen als laag worden aangemerkt.

1.2.12. Verlies van controle over inhoudsgegevens in de Graph

Microsoft 365 Copilot heeft toegang tot alle informatie in de *Graph* die voor een gebruiker toegankelijk is via het 'grounding' proces, zoals beschreven in de secties **Error! Reference source not found.** en **Error! Reference source not found.**. Als onderwijsinstellingen nalaten toegangsrechten adequaat vast te stellen en te beperken, bestaat bij het gebruik van Microsoft 365 Copilot het risico dat medewerkers toegang krijgen tot informatie uit documenten waartoe zij geen toegang zouden mogen hebben.

De gevolgen van onbedoelde interne toegang kunnen zeer groot zijn, omdat onderwijsinstellingen in SharePoint, OneDrive en Exchange Online documenten opslaan die vertrouwelijk kunnen zijn en/of gevoelige persoonsgegevens en/of bijzondere categorieën van persoonsgegevens kunnen bevatten, zoals beschreven in sectie 2.2. Voorbeelden hiervan zijn salarisinformatie, sollicitatiebrieven en persoonsgegevens van VIP's. Als Copilot bijvoorbeeld toegang zou krijgen tot salarisstroken die per ongeluk door een HR-medewerker naar een niet-beveiligde SharePoint-map zijn gekopieerd, zouden collega's mogelijk elkaars salaris te weten kunnen komen. In de Nederlandse context, waar salarisgegevens als zeer gevoelig en zeer intiem worden beschouwd, zou een dergelijke toegang moeten worden aangemerkt als een datalek met ernstige gevolgen voor de betrokkene. Zoals beschreven in sectie 2.2.1 staan veel SharePoint-intranetsites, Exchange Online-servers en OneDrive-servers van onderwijsinstellingen vol met verouderde gegevens, zonder dat er een natuurlijke prikkel is om deze gegevens op te schonen.

Deze DPIA gaat ervan uit dat alle onderwijsinstellingen eerst SharePoint, OneDrive en Exchange Online grondig opschonen in overeenstemming met het bewaarbeleid, alvorens Microsoft 365 Copilot te gebruiken. Deze DPIA gaat er tevens van uit dat onderwijsinstellingen ervoor zorgen dat de toegang tot persoonsgegevens in de *Graph* strikt beperkt blijft tot de rollen waarvoor toegang noodzakelijk is, met behulp van op rollen gebaseerde toegangscontroles (Role Based Access Controls).

Ervan uitgaande dat onderwijsinstellingen aan deze drie voorwaarden zullen voldoen (markeren of anderszins voorkomen van toegang door Microsoft 365 Copilot, opschonen van verouderde gegevens en controleren van RBAC's), is de waarschijnlijkheid van het risico op verlies van controle gering, ook al kan de impact groot zijn. Daarom kunnen de risico's voor betrokkenen als laag worden aangemerkt.

¹¹ SLM Rijk, Handleiding privacyvriendelijke instellingen Microsoft 365 voor beheerders, versie 3.3, 7 augustus 2025, URL: <https://slmmicrosoftrijk.nl/wp-content/uploads/2025/07/20250704-Handleiding-privacyvriendelijke-instellingen-Microsoft-365-definitief.pdf>.

Tabel1: Berekende hoge en lage gegevensbeschermingsrisico's

Ernst van de impact	Ernstige gevolgen	Laag risico 3, 4, 5, 6, 7, 8, 10, 11, 12	Hoog risico	Hoog risico
	Enige negatieve gevolgen	Laag risico 9	Medium risico 1,2	Hoog risico
	Minimale gevolgen	Laag risico	Laag risico	Laag risico
		Heel klein	Redelijke mogelijkheid	Waarschijnlijker dan niet
		Kans (waarschijnlijkheid) dat het risico zich voordoet		

Deel D. Beschrijving van risicobeperkende maatregelen

Het volgende gedeelte bevat een tabel met de technische, organisatorische en juridische risicobeperkende maatregelen die door de onderwijsinstelling of door Microsoft moeten worden genomen om de geïdentificeerde 2 medium en 10 (inclusief het nieuwe risico op gegevensoverdracht) lage risico's voor de betrokkenen te verminderen of op te lossen.

De uitkomst van deze tweede bijgewerkte DPIA is dat Microsoft maatregelen heeft genomen om de vier eerder geïdentificeerde hoge risico's te beperken, maar dat deze maatregelen niet effectief waren of nog niet konden worden getest om alle vier de risico's tot een laag niveau terug te brengen. Daarom zijn er geen wijzigingen in de beoordeling van de twee medium risico's. Microsoft heeft niet gereageerd op de voorgestelde maatregelen voor de zeven oorspronkelijk geïdentificeerde lage risico's op het gebied van gegevensbescherming.

Risico's worden aangemerkt als hoge risico's op basis van een vermenigvuldiging van de waarschijnlijkheid van optreden met de impact op betrokkenen. De eerste twee risico's worden aangemerkt als medium risico's omdat de organisaties zelf geen toereikende maatregelen kunnen nemen om het risico te beperken, behalve door geen gebruik te maken van Microsoft 365 Copilot.

De onderste tien risico's worden als laag aangemerkt omdat de onderwijs- en onderzoeksorganisaties effectieve maatregelen kunnen nemen om de kans op het optreden ervan tot verwaarloosbaar (of nul) te verlagen, ook al kan de impact nog steeds groot zijn. Deze DPIA gaat ervan uit dat de organisaties deze maatregelen zullen nemen.

1.3. Maatregelen die moeten worden genomen om medium en lage risico's te beperken

Nr.	Medium risico	Maatregelen onderwijsinstellingen	Maatregelen genomen door of voorgesteld aan Microsoft
13.	Aanzienlijk economisch of sociaal nadeel door het gebruik van gegenereerde teksten met onjuiste persoonsgegevens.	Overweeg om geen Microsoft 365 Copilot met een A3-licentie te gebruiken totdat Microsoft organisaties in staat stelt om het filter tegen schadelijke inhoud (Harmful Content) uit te zetten, en adequate transparantie geeft over het filter tegen werkplek schade (Workplace Harms). Met A5: Implementeer een beleid waarin wordt vastgelegd door welke eindgebruikers en wanneer de filtering van schadelijke inhoud uitgeschakeld mag worden. Stel een beleid op voor het gebruik van generatieve AI door medewerkers om correct gebruik te definiëren en, indien geactiveerd, DLP regels uit te leggen. Gebruik de nieuwe optie om het lettertype van de nauwkeurigheidswaarschuwing vetgedrukt te maken. Wijs gebruikers op de opties om bronverwijzingen te controleren en gebruik de nieuwe optie om de diepgaande bronvermeldingen voor elke bron waarnaar wordt verwezen te controleren wanneer Microsoft deze beschikbaar stelt. Geef instructies aan gebruikers om problemen met de RAI-filtering (tegen zowel schadelijke inhoud als werkplek schade), en problemen met gefilterde persoonsgegevens te melden aan copilotklacht@surf.nl	Beheerders kunnen een policy opstellen om (groepen) eindgebruikers toe te staan de Harmful Content filtering per chat uit te schakelen. Microsoft heeft Purview Data Loss Prevention (DLP) ingeschakeld voor Copilot prompts in Enterprise-Klanten. Microsoft biedt beheerders de mogelijkheid om het lettertype van de nauwkeurigheidswaarschuwing vetgedrukt te maken (door AI gegenereerde resultaten kunnen onnauwkeurig zijn) en een hyperlink naar het interne AI-beleid toe te voegen. Microsoft heeft duidelijke bronverwijzingen toegevoegd aan een nieuwe zijbalk en zal per juni 2026 diepgaande bronvermeldingen beschikbaar maken binnen de bronnen waarnaar wordt verwezen. Microsoft heeft twee zinnen gepubliceerd over het doel van het nieuwe filter voor schade op de werkplek (Workplace Harms filter). Microsoft heeft geweigerd om bedieningselementen aan te bieden om het Workplace Harmfilter uit te schakelen en om definities van Workplace Harmfilter te documenteren met voorbeelden die even gedetailleerd zijn als die van het Harmful Content filter. Microsoft zal gebruikers niet informeren dat er een filter is toegepast.

	Geef gebruikers de instructie om klachten of feedback over onjuiste persoonsgegevens te melden aan copilotklacht@surf.nl .	Microsoft zal: “de supportaanvraag waar nodig doorsturen naar de betreffende product- en feedbackteams. Indien nodig kunnen klanten ervoor kiezen om de ernstgraad te verhogen. Het supportteam houdt de klant op de hoogte van de voortgang en de uitkomst.” Microsoft heeft uitgelegd dat het supportaanvragen over onjuiste persoonsgegevens effectief kan oplossen door OpenAI opnieuw te trainen, te filteren, te verfijnen of te escaleren.
	Beheerders hebben toegang tot ingediende feedbackverzoeken van eindgebruikers en kunnen deze ook rapporteren aan SURF.	Microsoft zal klachten die naar SURF zijn gestuurd bespreken in een jaarlijkse vergadering, en met welke technologie het verzoek is opgelost, met enkele ongedefinieerde uitzonderingen.
	Instrueer/train gebruikers om de door Copilot gegenereerde persoonsgegevens altijd te controleren aan de hand van een onafhankelijke boordeling (door een collega) en betrouwbare bronnen.	Geen toezegging om statistieken te verstrekken over Microsofts eigen metingen van de kwaliteit en de onderbouwing van de output van Microsoft 365 Copilot, of inzage in tests en beoordelingen door derden om Microsoft's beweringen over voortdurende verbetering te verifiëren, met name in het Nederlands.
	Waarschuw gebruikers dat persoonsgegevens, met name over VIP's en professoren, gebaseerd kunnen zijn op verouderde en onjuiste trainingsgegevens die voor de LLM zijn gebruikt.	
	Voorkom de toewijzing van licenties aan accounts die toegang hebben tot (veel) bijzondere persoonsgegevens, zoals HR-gegevens	
	Schakel de toegang tot Bing uit en informeer gebruikers over de risico's voor betrokkenen als gevolg van de beperkingen van Copilot met betrekking tot de nauwkeurigheid van de gegenereerde gegevens.	Geen toezegging om de gegevensverwerking en doeleinden verder te beperken wanneer Bing is ingeschakeld.
	Schakel auditlogging in en stel regels op voor de controle op de naleving van het interne generatieve AI beleid, onder meer door controle op steekproeven van dialogen en diagnostische gegevens.	
	Houd de door Microsoft aangekondigde verbeteringen aan Copilot bij via meldingen in het Berichtencentrum en de M365-roadmap en lees het jaarlijkse RAI-filtrerapport .	

14.	Heridentificatie van gepseudonimiseerde gegevens door onbekende bewaartermijnen van <i>vereiste servicegegevens</i> (zowel inhoudelijke als diagnostische gegevens).	Geen maatregelen mogelijk, behalve het verwijderen van een account of het beëindigen van het contract voor M365-diensten.	Microsoft heeft bekendgemaakt dat het de diagnostische gebeurtenis gegevens voor Microsoft 365 apps en diensten, waaronder Microsoft 365 Copilot, tot 18 maanden bewaart , zonder voldoende motivering van de noodzaak van deze bewaartermijn, of uitleg over hoe het bepaalt wanneer gegevens voor een kortere periode moeten worden bewaard. Microsoft heeft uitgelegd dat het voor het verzamelen van deze gegevens als verwerker dezelfde evenredigheidseisen hanteert als bij de gecontroleerde, geautoriseerde verdere verwerking voor de legitieme zakelijke doeleinden van Microsoft.
-----	--	---	---

Nr.	Laag risico	Maatregelen onderwijsinstellingen	Maatregelen genomen door of voorgesteld aan Microsoft
15.	Verlies van controle door gebrek aan transparantie <i>Vereiste servicegegevens en de telemetrie</i> gebeurtenissen van Webapp gebruikers.	Bestudeer de nieuwe publieke documentatie van Microsoft over de RSD en telemetriegegevens om de betrokkenen goed te kunnen informeren over de gegevensverwerkingen door een betaalde Copilot-licentie.	Microsoft heeft uitgebreide nieuwe documentatie gepubliceerd over het verschil tussen telemetriegegevens en RSD, en heeft uitgelegd dat er verschillende gegevensstromen zijn voor inhoudelijke gegevens in de RSD en diagnostische gegevens in de RSD.
		Stel het telemetrieniveau in Windows en Office 365 in op het minst ingrijpende niveau 'beveiligings'-'vereist'- niveau.	Microsoft bevestigt dat de diagnostische RSD geen inhoudelijke gegevens bevat, met uitzondering van bestandsnamen bij het delen van OneDrive-bestanden.
16.	Onvermogen van betrokkenen om inzagerechten uit te oefenen in hun diagnostische gegevens.	Dien een DSAR in en vergelijk de resultaten met de nieuwe openbare documentatie van Microsoft over de verschillende diagnostische gegevens (telemetriegegevens en RSD).	Microsoft heeft nieuwe documentatie gepubliceerd, waaronder een Readme-bestand, en biedt op een transparante, begrijpelijke en gemakkelijk toegankelijke manier toegang tot de telemetriegegevens en de vereiste servicegegevens over het gebruik van Microsoft 365 Copilot, met beschrijvende namen voor de bestanden en mappen. Microsoft legt ook uit waarom sommige velden leeg zijn.
			Microsoft documenteert alle RSD-name spaces en legt uit waarom het geen inzage geeft in meerdere telemetrieberichten die verwijzen naar dezelfde gebruikersactie.
			Microsoft verbindt zich ertoe een inzageverzoek in te willigen zonder dat de gegevens worden gewist terwijl het verzoek nog in behandeling is.
17.	Openbaarmaking van of toegang tot persoonsgegevens als gevolg van incidentele doorgiften aan ingehuurd personeel in 30 derde landen.	Maak gebruik van de professionele ondersteuningsdiensten, niet van de in-app ondersteuningsopties.	Geef specifiekere en consistente openbare uitleg over de waarschijnlijkheid van gegevensdoorgifte naar de VS voor veiligheidsdoeleinden en verdere doorgifte.

18.	Openbaarmaking van of toegang tot persoonsgegevens buiten de EU als gevolg van Copilot flex routing.	Nieuwe klanten: wijzig de standaardinstelling en schakel flex routing uit.	Schend de EU Data Boundary verbintenis, waarbij alle gegevensverwerking voor Core Services uitsluitend in de EU plaatsvindt, met SURF niet. Met uitzondering van beperkte doorgiften voor veiligheidsdoeleinden.
19.	Reputatieschade: onvermogen om (her)generatie van onjuiste persoonsgegevens in de output te voorkomen nadat een betrokkene een klacht heeft ingediend.	Dien een (Professional Services) ondersteuningsverzoek in om Microsoft te vragen het opnieuw genereren van duidelijk onjuiste persoonsgegevens te voorkomen. Geef gebruikers de instructie om onjuiste persoonsgegevens te melden aan copilotklacht@surf.nl Dien alleen feedbackverzoeken in bij meer algemene/minder urgente zaken.	Microsoft zal: <i>“het ondersteuningsverzoek doorsturen naar de betreffende product- en feedbackteams, indien van toepassing. Indien nodig kunnen klanten ervoor kiezen om de urgentie te verhogen. Het supportteam houdt de klant op de hoogte van de voortgang en het resultaat.”</i> Microsoft heeft uitgelegd dat het ondersteuningsverzoeken over onjuiste persoonsgegevens effectief kan oplossen door hertraining, filtering, finetuning of escalatie naar OpenAI toe te passen.
20.	Verlies van controle / verlies van vertrouwelijkheid als gevolg van verdere verwerking door Microsoft (als gevolg van standaardinstellingen).	Schakel de toegang tot de webchat (Bing) uit in zowel Microsoft 365 Copilot als in Copilot Chat. Raadpleeg de SLM-handleiding met privacy vriendelijke instellingen voor M365. Schakel de optie uit om feedback te geven aan het openbare (verantwoordelijke) feedbackforum. Als andere soorten (verwerkers)feedbackdiensten niet zijn uitgeschakeld: bekijk de ingediende feedback via de beheerconsole. Schakel de toegang tot de gratis versies van Copilot in Bing, Edge, Windows, Office en alle M365 services uit waar Microsoft toegang mogelijk maakt tot deze ‘Microsoft als verantwoordelijke’-versies van Copilot. Schakel aanvullende optionele verbonden ervaringen in Office 365 uit.	Voldoe aan de wettelijke verplichting voor privacy by design en by default: wanneer Microsoft als gegevensverwerker wordt ingeschakeld, moet alle gegevensverwerking in de rol van verwerkingsverantwoordelijke standaard worden uitgeschakeld, inclusief toegang tot Bing via Copilot Chat. Microsoft heeft de geconstateerde glitch verholpen die optrad wanneer ‘Additional Optional Connected Experiences’ waren uitgeschakeld, en raadt nu aan om een groepsbeleid te gebruiken om de toegang tot Bing uit te schakelen, zowel in de gratis (consumenten)versie als in de betaalde versie.
21.	Verlies van tijd en concentratie: gebruik van accountgegevens om e-mails te versturen.	Gebruik de centrale opt-out-functionaliteit voor alle of sommige gebruikers in de organisatie voor mailings over Microsoft 365 Copilot. Geef gebruikers de instructie om alert te zijn op vooraf aangevinkte vakjes op de openbare ‘learn’ pagina’s van Microsoft.	Overweeg opnieuw om e-mails naar gebruikers met een licentie te willen sturen. Deze verwerking is contractueel toegestaan, maar ethisch ongewenst. Stop met het uitnodigen van aangemelde gebruikers met een vooraf ingevuld formulier om in te stemmen met commerciële mailings.

22.	Verlies van controle door onjuiste auteursnamen in Copilot antwoorden.	Leg gebruikers uit dat ze de auteursnamen moeten opzoeken van documenten in de 'Graph' die door Microsoft worden geciteerd.	Verbeter de metadata van auteurs van documenten in de 'Graph': wijs de inhoud niet toe aan de persoon die het bestand naar SharePoint of OneDrive heeft geüpload.
23.	Afschrikkend effect van gebruik van Copilot als personeelsvolgsysteem	Vul het interne privacybeleid voor de verwerking van persoonsgegevens van werknemers aan met regels voor de specifieke doeleinden waarvoor specifieke persoonsgegevens in de Microsoft 365 Copilot-dialoog en logbestanden (verder) mogen worden verwerkt en geanalyseerd. Dit omvat het opsommen van de specifieke risico's waartegen de historische dialoog- en logbestanden zullen worden gecontroleerd, en welke maatregelen de organisaties zullen nemen om doelbinding te waarborgen. Volg de aanbeveling uit eerdere DPIAs om de logbestanden van gebruikersactiviteiten gepseudonimiseerd weer te geven.	-geen maatregelen nodig-
24.	Verlies van controle over inhoudelijke gegevens in de Graph	Gebruik de nieuwe DLP-opties voor Microsoft 365 Copilot. Pas labeling toe om ervoor te zorgen dat adequate autorisaties kunnen worden ingesteld. Organiseer grondige opschoningssessies voor SharePoint en Outlook in overeenstemming met het bewaarbeleid voorafgaand aan gebruik van Microsoft 365 Copilot. Raadpleeg de richtlijnen van Microsoft.	Microsoft heeft Purview Data Loss Prevention (DLP) ingeschakeld voor Copilot prompts in Enterprise tenants.