Copilot DPIA

Overzicht

Organisatie	Provincie Gelderland
Gekoppeld item	Geen gekoppeld item
Analyse van verwerkingen model	Provincie Gelderland | DPIA
Status	afgerond
Datum afgerond	nog niet afgerond
Interne Toezichthouder	5.1.2e

Advies

Eindoordeel

Inleiding

Vanuit het oogpunt van een zorgvuldige omgang met persoonsgegevens is de Provincie Gelderland, volgens de Algemene Verordening Gegevensbescherming (AVG) verplicht een Data Protection Impact Assessment (DPIA) uit te voeren over nieuwe verwerkingen, die waarschijnlijk een hoog risico opleveren voor de betrokkenen van wie de persoonsgegevens worden verwerkt en/of van verwerkingen, waarbij nieuwe technologieën worden gebruikt. Daarnaast heeft de Autoriteit Persoonsgegevens (AP) een lijst opgesteld van soorten verwerkingen, waarvoor verplicht een DPIA moet worden uitgevoerd. Via deze link kan meer informatie worden gevonden.

Het doel van de DPIA is om vooraf de privacy risico's van een gegevensverwerking in kaart te brengen zodat maatregelen kunnen worden genomen om deze risico's weg te nemen of te verkleinen.

Een DPIA moet ten minste aan de volgende vereisten voldoen :

- Beschrijving geven van de beoogde verwerking en de doeleinden daarvan;
- Beoordeling van de rechtmatigheid van de beoogde verwerking, dat wil zeggen een beoordeling van de rechtsgrond, de noodzaak en de evenredigheid van de verwerking in relatie tot het beoogde doel;
- Beschrijving en beoordeling van de risico's voor betrokkenen;
- Beschrijving en beoordeling van de maatregelen om de risico's voor betrokkenen tegen te gaan of te beperken.

Een DPIA wordt ingevuld onder verantwoordelijkheid van de proceseigenaar en door de Privacy Officer. Er wordt aangeraden om bij het invullen ook inhoudelijke experts te betrekken. Nadat de DPIA is uitgevoerd wordt deze voor het uitbrengen van een advies voorgelegd aan de Functionaris Gegevensbescherming (FG) van de Provincie Gelderland.

Wanneer de maatregelen naar het oordeel van de FG niet of onvoldoende zorgen voor een inperking van de risico's voor betrokkene - en er een hoog (rest)risico voor de rechten en vrijheden van betrokkenen blijft bestaan - moet hierover voor aanvang van de verwerking een voorafgaande raadpleging worden aangevraagd bij de Autoriteit Persoonsgegevens (AP). In voorkomend geval informeert de FG de betreffende afdeling / proceseigenaar over zijn advies een voorafgaande raadpleging bij de AP aan te vragen.

Bij deze DPIA rapportage hoort ook een handleiding, die extra uitleg - en te beantwoorden vragen - geeft bij de normen in de deze rapportage.

Geadviseerd wordt deze handleiding bij het opstellen van deze rapportage te gebruiken

1. Wie voert de DPIA uit?

Gelieve naam en contactgegevens toe te voegen.

Antwoord:

Deze DPIA is opgesteld onder verantwoordelijkheid van de proceseigenaar (CIO-office / I&A) in samenwerking met de Centrale Privacy Officer (5.1.2e 5.1.2i @gelderland.nl). Voor de inhoudelijke toetsing zijn onder meer functioneel beheer Microsoft 365, informatiebeveiliging en relevante inhoudelijke stakeholders betrokken. De Functionaris Gegevensbescherming (FG) heeft een eerdere versie van de DPIA

beoordeeld en daarbij een zwaarwegend advies uitgebracht. Naar aanleiding hiervan is de DPIA integraal herzien en op essentiële onderdelen verdiept, waaronder de noodzakelijkheidstoets, risicobeoordeling, governance en beheersmaatregelen. De FG wordt verzocht deze herijkte DPIA opnieuw te beoordelen en te adviseren over de voorgenomen inzet van Microsoft 365 Copilot.
Randvoorwaarden voorafgaand aan inzet:

Voorafgaand aan ingebruikname van Microsoft 365 Copilot voert de provincie een risicogerichte opschoningsactie uit binnen documentomgevingen waarin mogelijk gevoelige persoonsgegevens voorkomen (zoals CV?s, BSN's). Waar mogelijk worden deze documenten verwijderd, verplaatst naar adequaat afgeschermde omgevingen of voorzien van passende classificatie. De pilotfase start uitsluitend nadat deze eerste opschoningsronde aantoonbaar is uitgevoerd. Daarnaast is de provincie in project IHOO bezig met laten opschonen van onnodige data in de tevens de omgevingen van Microsoft.

2. Motiveer waarom het noodzakelijk is om een DPIA uit te voeren.

Noodzaak van de DPIA (par. 3.1 handleiding)

Wat is de uitkomst van de Verkennende Gegevensbeschermingseffectbeoordeling (Pre-DPIA) en eerste inventarisatie?

Antwoord:

Een DPIA is noodzakelijk omdat Microsoft 365 Copilot generatieve AI toepast binnen de digitale werkomgeving van de provincie. Het betreft een nieuwe technologie waarvan vooraf moet worden beoordeeld welke gevolgen deze kan hebben voor de bescherming van persoonsgegevens en de vertrouwelijkheid van informatie.

Copilot kan gegevens uit de Microsoft 365-omgeving analyseren en combineren, waaronder communicatie en documenten. Hierdoor bestaat een verhoogd risico op ongewenste inzage of het breder beschikbaar worden van persoonsgegevens wanneer autorisaties, classificatie en informatiebeheer niet volledig op orde zijn. Dat is nu ook al het geval, doch co-pilot maakt dit mogelijk zichtbaarder. Dit hangt mede samen met het feit dat classificatie-, retentie- en labelingsmaatregelen binnen de Microsoft 365-omgeving nog niet organisatiebreed volwassen en aantoonbaar consistent zijn ingericht. Gelet op het gebruik van nieuwe technologie, de verwerking van communicatiegegevens en het potentiële risico op oversharing, is het uitvoeren van een DPIA noodzakelijk en proportioneel.

Omschrijving van de verwerking

Het doel van dit hoofdstuk is om lezers van deze rapportage, die geen voorkennis hebben van het proces, te laten begrijpen wat er exact met de persoonsgegevens in de hier beschreven verwerking gebeurt.

3.1. Doel

omschrijf hier helder en duidelijk het doel van de voorgenomen verwerking

!! Wanneer het doel niet is vastgesteld of helder is omschreven, mag de verwerking niet plaatsvinden. Stop met invullen en neem contact op met de Privacy Officer/Functionaris voor Gegevensbescherming.

Antwoord:

De provincie zet Microsoft 365 Copilot in als ondersteunende functionaliteit binnen de bestaande Microsoft 365-werkomgeving. Copilot helpt medewerkers bij het opstellen, samenvatten en structureren van documenten, e-mails en presentaties, ter ondersteuning van de uitvoering van provinciale taken van algemeen belang, zoals beleidsvoorbereiding, besluitvorming, interne advisering en communicatie.Copilot heeft uitsluitend een ondersteunend karakter: medewerkers blijven verantwoordelijk voor de inhoudelijke beoordeling en besluitvorming. De inzet is nadrukkelijk begrensd. Copilot wordt niet gebruikt voor geautomatiseerde besluitvorming, profilering of het monitoren en beoordelen van medewerkers. Het gebruik voor de verwerking van bijzondere persoonsgegevens of strafrechtelijke gegevens is niet toegestaan.

3.2. Omschrijving van de verwerking

Geef hier een heldere en duidelijke omschrijving van de voorgenomen verwerking

Antwoord:

Copilot verwerkt gebruikersinvoer (prompts) en raadpleegt, binnen de rechten van de ingelogde gebruiker, gegevens in de Microsoft 365-omgeving, zoals: documenten, e-mails en Teams-content. Op basis hiervan genereert Copilot output (bijvoorbeeld samenvattingen of tekstvoorstellen) die door de gebruiker wordt beoordeeld, aangepast en eventueel opgeslagen binnen de provinciale omgeving. Copilot heeft uitsluitend een ondersteunend karakter. De gebruiker blijft eindverantwoordelijk voor het gebruik van de output. De verwerking vindt plaats binnen het interne werkdomein van de provincie. Co-pilot kijkt niet heel diep in bestanden in sharepoint, gaat in lagen. De exacte wijze waarop Copilot informatie uit verschillende documentstructuren en onderliggende mappen presenteert, wordt technisch nog nader gevalideerd. Denk aan chatgpt die alleen hogere rechtspraak meeneemt en lagere niet.

3.3. Uitgesloten van de scope

Geef aan wat wel en wat niet binnen de scope van het traject/project valt.

Antwoord:

Buiten scope valt:
- gebruik van Copilot voor geautomatiseerde besluitvorming of besluitvoorbereiding waarbij output direct wordt overgenomen zonder menselijke controle;
- inzet voor monitoring, beoordeling of selectie van medewerkers;
- gebruik voor dossiers met bijzondere persoonsgegevens (zoals gezondheid, strafrecht, integriteit), HR-dossiers, en andere risicovolle informatiecategorieën. Deze staan daarom ook elders en niet op microsoft omgevingen.
- gebruik van consumentenvarianten van Copilot of niet-goedgekeurde AI-diensten;

3.4. Betrokken partijen

Geef aan welke partijen, zowel intern als extern, betrokken zijn bij de voorgenomen verwerking

Antwoord:

Intern: CIO-office/I&A (proceseigenaar), Functioneel beheer M365, Informatiebeveiliging (CISO/BIO), privacyorganisatie CIO, FG, key users/pilotgroep.
Extern: Microsoft Ireland Operations Ltd. (leverancier/verwerker).

3.5. Beschrijving van de persoonsgegevens die worden verwerkt

Geef in onderstaande tabel aan welke categorieën van betrokkenen en persoonsgegevens worden verwerkt. Maak daarbij gebruik van de voorbeelden, weergegeven op de volgende pagina

Antwoord:

- Medewerkers van Provincie Gelderland (incl. ingehuurde krachten zoals zzp'ers met account).
- Mogelijk externe betrokkenen (burgers/leveranciers/partners) van wie persoonsgegevens in bestaande M365-content staan (bijv. in documenten, e-mails, bijlagen).

Categorieën persoonsgegevens:
- Identificatie- en contactgegevens: naam, gebruikersnaam, e-mailadres, functietitel/afdeling.
- Werkgerelateerde communicatie-inhoud: e-mails, Teams-berichten, agenda-items, notities, documenten (Word/Excel/PowerPoint) en bijlagen waarin persoonsgegevens kunnen voorkomen.
- Prompts en gegenereerde output: vragen/instructies van de gebruiker (prompts) en de antwoorden/samenvattingen/teksten die Copilot produceert. (NB: SLM beschrijft dat prompts/antwoorden per gebruiker in Exchange worden bewaard in een (verborgen) mailboxfolder en dat auditlogs standaard 1 jaar worden bewaard, uitbreidbaar.) (bron: 20250911-SLM-update-DPIA-Copilot?)
- Je prompts worden bewaard, maar Co pilot heeft aantal beveiligingsmechanismen wanneer het gaat om detectie van persoonsgegevens. We kunnen DLP gebruiken om bepaalde persoonsgegevens te detecteren en daar vervolgens geanonimiseerd antwoord op wordt gegeven. DLP is bijv. dat je aangeeft dat namen, woonplaatsen en telefoonnummers worden geanonimiseerd.
- Diagnostische/telemetriegegevens (Required Service Data/Telemetry): wij doen dit minimaal laten toestaan (zoveel mogelijk uitgezet). Hele beperkte set wordt gedeeld > pseudonieme diagnostische gegevens die Microsoft verwerkt voor werking/beveiliging van de dienst, met in SLM beschreven retentie tot maximaal 18 maanden.
- De provincie beoogt geen bijzondere persoonsgegevens te verwerken met Copilot, maar kan niet uitsluiten dat dergelijke gegevens aanwezig zijn in bestaande M365-content (bijv. in oude documenten). Via pilot kunnen we deze tijdig opzoeken en laten verwijderen.

1. Rechtsgrond van de verwerking (artikel 6) (norm 1 t/m 5)

Onderstaande normen hebben betrekking op de rechtmatigheid van de verwerking van de persoonsgegevens.

1. Norm 1: Persoonsgegevens mogen alleen rechtmatig worden verwerkt. Dit betekent dat de verwerking een helder omschreven doel moet hebben (zie hoofdstuk 3) én er een wettelijke grondslag volgens de AVG (artikel 6 lid 1) is.

AVG-grondslagen (AVG artikel 6 lid 1..)

1.1. Hoe wordt voldaan aan de norm?

Antwoord:

De verwerking vindt plaats op basis van artikel 6 lid 1 sub e AVG (taak van algemeen belang / uitoefening van openbaar gezag). Copilot ondersteunt medewerkers bij bestaande provinciale werkzaamheden en leidt niet tot een wijziging van de oorspronkelijke doeleinden van de onderliggende gegevensverwerkingen.

De inzet is beperkt tot interne werkprocessen en vindt plaats onder vastgestelde randvoorwaarden, waaronder scopebeperking, passend autorisatiebeheer, labeling en retentie, auditlogging, training en vastgesteld AI-beleid.

Copilot wordt niet gebruikt voor (bijzondere) persoonsgegevens, tenzij deze aantoonbaar zijn afgeschermd en inzet expliciet is toegestaan binnen een gecontroleerde pilot.

Gelet op deze begrenzing en beheersmaatregelen wordt de inzet als noodzakelijk en evenredig beoordeeld ten opzichte van het beoogde doel.

1.2. Wat zijn de risico's die overblijven?

Antwoord:

Het belangrijkste restrisico betreft ongewenste inzage (?oversharing?). Copilot volgt bestaande autorisaties, terwijl opschoning, labeling, retentie en toegangsbeheer nog niet provinciebreed aantoonbaar op orde zijn. Hierdoor kan output persoonsgegevens bevatten uit verouderde of onjuist geclassificeerde documenten. Daarnaast bestaat risico op onvoldoende duidelijkheid richting medewerkers over toegestaan gebruik, en op onjuiste of verouderde output als gevolg van gebrekkige bronkwaliteit.

1.3. Hoe hoog is de kans dat het risico zich voordoet?

Antwoord:

Midden (zolang autorisatiestructuur en labeling niet aantoonbaar op orde zijn en auditlogging beperkt is).

1.4. Wat is de impact voor betrokkene?

Antwoord:

Midden voor medewerkers (en mogelijk derden) door verlies van vertrouwelijkheid, reputatieschade, interne verspreiding van gevoelige informatie en risico op datalekmeldingen. De helft van de provinciale medewerkers hebben prompt training (d.m.v. AI-kampvuurtjes) gehad waarom dit is uitgelegd.

1.5. Aanvullende maatregelen?

Antwoord:

Gefaseerde inzet (pilot), vooraf risicogerichte opschoning (cv's paspoort), labeling, retentie, centraal uitschakelen/afschermen van externe integraties (Bing/preview) waar mogelijk, en verplicht beleid + training.

2. Norm 2: Wanneer de verwerking is gebaseerd op toestemming, dient aan de eisen t.a.v. toestemming in de AVG te worden voldaan.

Risico op basis van de norm.

2.1. Hoe wordt voldaan aan de norm?

Antwoord:

Niet van toepassing. De verwerking is niet gebaseerd op toestemming. De grondslag is artikel 6 lid 1 sub e AVG (taak van algemeen belang / openbaar gezag).

2.2. Wat zijn de risico's die overblijven?

Antwoord:

Risico op ?schijn-toestemming? of impliciete instemming wordt voorkomen door Copilot niet als opt-in/toestemmingsverwerking te positioneren maar als gecontroleerde werkvoorziening met beleid en randvoorwaarden.

2.3. Hoe hoog is de kans dat het risico zich voordoet?

Antwoord:

Laag.

2.4. Wat is de impact voor betrokkene?

Antwoord:

Middel (als het toch verkeerd wordt geframed kan dat tot verwarring/klachten leiden).

2.5. Aanvullende maatregelen?

Antwoord:

Communicatie/beleid: ?geen toestemming, maar regels en toezicht".

3. Norm 3: Wanneer de verwerking plaatsvindt op basis van toestemming heeft de betrokkene het recht om toestemming te allen tijde in te trekken.

Risico op basis van de norm.

3.1. Hoe wordt voldaan aan de norm?

Antwoord:

Zelfde lijn als Norm 2: ?Niet van toepassing.?

3.2. Wat zijn de risico's die overblijven?

Antwoord:

niet van toepassing

3.3. Hoe hoog is de kans dat het risico zich voordoet?

Antwoord:

N.v.t.

3.4. Wat is de impact voor betrokkene?

Antwoord:

n.v.t.

3.5. Aanvullende maatregelen?

Antwoord:

n.v.t.

4. Norm 4: Het verwerken van bijzondere persoonsgegevens is alleen toegestaan, wanneer wordt voldaan aan het gestelde in AVG artikel 9, lid 2.

Risico op basis van de norm.

4.1. Hoe wordt voldaan aan de norm?

Antwoord:

De provincie gebruikt Microsoft 365 Copilot niet voor verwerkingen waarbij bijzondere persoonsgegevens een rol spelen. In beleid, werkinstructies en training is expliciet vastgelegd dat dergelijke gegevens niet in prompts mogen worden opgenomen.
Risicovolle gegevenslocaties worden vooraf risicogericht opgeschoond en waar nodig afgeschermd of gelabeld. Dit voorkomt dat Copilot deze informatie kan raadplegen. De inzet start gefaseerd binnen een gecontroleerde pilot en blijft beperkt tot vooraf afgebakende teams en omgevingen. Deze begrenzingen gelden als randvoorwaarde voor ingebruikname.

4.2. Wat zijn de risico's die overblijven?

Antwoord:

Er blijft een risico bestaan dat bijzondere persoonsgegevens al aanwezig zijn in bestaande M365-content, zoals verouderde documenten, bijlagen of historische dossiers, en via Copilot onbedoeld zichtbaar worden in gegenereerde output. Dit risico hangt direct samen met de mate waarin autorisaties, opschoning en labeling binnen de organisatie aantoonbaar op orde zijn.

4.3. Hoe hoog is de kans dat het risico zich voordoet?

Antwoord:

Hoog zolang labeling/retentie en autorisaties niet aantoonbaar op orde zijn.

4.4. Wat is de impact voor betrokkene?

Antwoord:

Hoog: ongewenste openbaarmaking van bijzondere gegevens leidt snel tot ernstig nadeel voor betrokkenen en meldplichtige incidenten.

4.5. Aanvullende maatregelen?

Antwoord:

- Start met pilot
- labeling/retentie + opschoningacties.
- Periodieke audits op toegangsrechten en risicolocaties.
- Heldere escalatieprocedure bij oversharing/datalek.

5. Norm 5: Het BSN is gelijk gesteld aan een bijzonder persoonsgegeven en mag alleen worden verwerkt als dit expliciet is vastgelegd in een wet; m.a.w. er moet sprake zijn van een wettelijke verplichting (bijv. de Wet algemene bepalingen BSN).

Risico op basis van de norm.

5.1. Hoe wordt voldaan aan de norm?

Antwoord:

BSN wordt niet beoogd verwerkt via Copilot. Dit wordt tevens vastgelegd in beleid/training.

5.2. Wat zijn de risico's die overblijven?

Antwoord:

BSN kan eventueel voorkomen in oude documenten. Bij onvoldoende opschoning/labeling blijft risico op onbedoelde inzage.

5.3. Hoe hoog is de kans dat het risico zich voordoet?

Antwoord:

Laag - middel (afhankelijk van opschoningsniveau)

5.4. Wat is de impact voor betrokkene?

Antwoord:

Hoog

5.5. Aanvullende maatregelen?

Antwoord:

Waar technisch mogelijk worden aanvullende DLP- en detectiemechanismen ingezet om verwerking van BSN?s te signaleren of te beperken.

2 Doelbinding (artikel 5) (norm 6 & 7)

(par. 3.3.2 handleiding)

6. Norm 6: Bron van de persoonsgegevens. Met de bron van de persoonsgegevens wordt aangegeven waaruit en/of van welke personen of organisaties de persoonsgegevens worden verkregen.

Risico op basis van de norm.

6.1. Hoe wordt voldaan aan de norm?

Antwoord:

De persoonsgegevens zijn niet afkomstig uit een nieuwe bron, maar uit bestaande Microsoft 365-omgevingen binnen de tenant van de provincie, waaronder SharePoint, Exchange Online en Teams. Copilot raadpleegt deze content uitsluitend binnen de machtigingen van de ingelogde gebruiker. Beperkt tot bepaalde lagen. Dit laatste werkt tot map in map. Je kunt wel in je eigen onedrive persoonsgegevens tegenkomen in co pilot, omdat je het zelf hebt opgeslagen. Je kunt globaal instelling aanpassen zodat co pilot niet in onedrive kijkt. daar staan immers de meeste persoonsgegevens! De provincie borgt dat Copilot alleen wordt ingezet binnen afgebakende werkprocessen en dat risicolocaties vooraf risicogericht worden opgeschoond.
De landelijke SLM-DPIA bevestigt dat Microsoft 365 Copilot gebruikmaakt van Microsoft Graph om content

en context uit deze bronnen te ontsluiten. Dit onderstreept dat zorgvuldig bronbeheer en passende autorisaties essentieel zijn voor een beheerste inzet.

6.2. Wat zijn de risico's die overblijven?

Antwoord:

De kwaliteit en afscherming van brondata zijn nog niet (overal) aantoonbaar consistent ingericht. Verouderde documenten, te ruime toegangsrechten en ontbrekende labeling kunnen ertoe leiden dat Copilot persoonsgegevens uit niet-actuele of onjuist geclassificeerde bronnen verwerkt en presenteert als bruikbare output.

6.3. Hoe hoog is de kans dat het risico zich voordoet?

Antwoord:

Hoog.

6.4. Wat is de impact voor betrokkene?

Antwoord:

HOog.

6.5. Aanvullende maatregelen?

Antwoord:

Opschoning/labeling, autorisatieherziening, gefaseerde scope van gebruikers.

7. Norm 7: Gegevens die in deze verwerking worden verwerkt, mogen alleen in andere verwerkingen worden gebruikt als het doel van die verdere verwerking verenigbaar is met het oorspronkelijke doel van de verwerking.

Risico op basis van de norm.

7.1. Hoe wordt voldaan aan de norm?

Antwoord:

Copilot wordt uitsluitend ingezet als ondersteunend hulpmiddel binnen bestaande provinciale werkprocessen, zoals het opstellen, samenvatten en structureren van informatie. De inzet leidt niet tot nieuwe verwerkingsdoeleinden en wordt niet gebruikt voor toezicht, profilering of geautomatiseerde besluitvorming.

7.2. Wat zijn de risico's die overblijven?

Antwoord:

Doelverschuiving vormt een aandachtspunt. Copilot kan aantrekkelijk worden voor gebruik buiten de vastgestelde scope.

7.3. Hoe hoog is de kans dat het risico zich voordoet?

Antwoord:

Laag - middel (met governance, cursussen gaan wij uit van laag tot middel).

7.4. Wat is de impact voor betrokkene?

Antwoord:

middel.

7.5. Aanvullende maatregelen?

Antwoord:

- Vastgesteld AI-beleid, privacybeleid + verplichte training
- Pilot + evaluatiemomenten

3 Juist, actueel en volledig (norm 8)

(par. 3.3.3 handleiding)

8. Norm 8: Persoonsgegevens zijn juist, actueel en volledig.

Risico op basis van de norm.

8.1. Hoe wordt voldaan aan de norm?

Antwoord:

De provincie borgt dat medewerkers eindverantwoordelijk blijven voor het controleren van door Copilot gegenereerde output voordat deze wordt gebruikt of gedeeld. Copilot wordt nadrukkelijk gepositioneerd als ondersteunend hulpmiddel en niet als bron van waarheid.

Daarnaast worden structurele maatregelen getroffen om de kwaliteit van brondata te verbeteren, waaronder gerichte opschoningsacties binnen SharePoint en OneDrive en het stimuleren van eigenaarschap bij documentbeheerders. In beleid en training wordt expliciet opgenomen dat medewerkers niet blind mogen vertrouwen op Copilot-antwoorden en deze altijd moeten verifiëren, met name wanneer persoonsgegevens onderdeel kunnen zijn van de output.

8.2. Wat zijn de risico's die overblijven?

Antwoord:

Copilot kan verouderde documenten raadplegen of onjuiste verbanden leggen tussen gegevens, waardoor output feitelijk onjuist kan zijn. Wanneer medewerkers hier te sterk op vertrouwen, kan dit leiden tot verkeerde besluitvorming, interne verspreiding van onjuiste persoonsgegevens of zelfs reputatieschade.

8.3. Hoe hoog is de kans dat het risico zich voordoet?

Antwoord:

Middel - hoog (zolang informatiehuishouding niet volledig op orde is, blijft deze hoog).

8.4. Wat is de impact voor betrokkene?

Antwoord:

Middel - hoog (afhankelijk van gebruik, bij beleidscontext snel hoog).

8.5. Aanvullende maatregelen?

Antwoord:

- in training meegeven + in beleid opnemen.

4 Dataminimalisatie (norm 9 t/m 11)

(par. 3.3.4 handleiding)

9. Norm 9: Er worden niet meer persoonsgegevens gebruikt dan noodzakelijk voor het bereiken van het doel van de verwerking. Van elk persoonsgegeven is vastgesteld dat het noodzakelijk is.

Risico op basis van de norm.

9.1. Hoe wordt voldaan aan de norm?

Antwoord:

Medewerkers worden geïnstrueerd om geen persoonsgegevens in prompts op te nemen in het beleid + training.

9.2. Wat zijn de risico's die overblijven?

Antwoord:

Gebruikers kunnen geneigd zijn meer context of persoonsgegevens te delen dan noodzakelijk om betere output te verkrijgen (?prompt creep?)

9.3. Hoe hoog is de kans dat het risico zich voordoet?

Antwoord:

Middel

9.4. Wat is de impact voor betrokkene?

Antwoord:

Laag-middel

9.5. Aanvullende maatregelen?

Antwoord:

- Prompt-richtlijnen (eventueel in AI - beleid)
- Training
- AI-beleid met verboden categorieën
- DLP-maatregelen > data loss preventie > je geeft aan hoe termen zijn opgebouwd en als dat voorkomt, dan zegt hij: weet je zeker dat je dit wil delen.

10. Norm 10: Het gebruik van bijzondere persoonsgegevens en/of gebruik van gevoelige gegevens moet zo veel mogelijk worden vermeden wanneer ze niet strikt noodzakelijk zijn.

Risico op basis van de norm.

10.1. Hoe wordt voldaan aan de norm?

Antwoord:

Het is verboden.

10.2. Wat zijn de risico's die overblijven?

Antwoord:

Bijzondere persoonsgegevens kunnen aanwezig zijn in historische documenten en onbedoeld worden geraadpleegd door Copilot.

10.3. Hoe hoog is de kans dat het risico zich voordoet?

Antwoord:

Hoog (we moeten realistisch blijven).

10.4. Wat is de impact voor betrokkene?

Antwoord:

Hoog.

10.5. Aanvullende maatregelen?

Antwoord:

-Gefaseerde implementatie
-Risicogerichte opschoning
-Labeling versnellen?
- Autorisaties toepassen.

11. Norm 11: Vrije tekstvelden in applicaties moeten, wanneer mogelijk, worden vermeden.

Risico op basis van de norm.

11.1. Hoe wordt voldaan aan de norm?

Antwoord:

SLM beschrijft dat prompts en antwoorden worden opgeslagen en gelogd. (zie slmrijk dpia). Afgescheiden gebied in exchange. is bij ons ook zo. Geldt alleen voor deze betaalde licentie. Dit is vooral voor jezelf zodat je die ziet.

11.2. Wat zijn de risico's die overblijven?

Antwoord:

Hoewel Copilot werkt met vrije tekstinvoer, beperkt de provincie de risico?s door duidelijke gebruikersrichtlijnen vast te stellen. Medewerkers worden geïnstrueerd geen (bijzondere) persoonsgegevens, vertrouwelijke bestuurlijke informatie of andere gevoelige gegevens in prompts op te nemen.

11.3. Hoe hoog is de kans dat het risico zich voordoet?

Antwoord:

Gebruikers kunnen toch gevoelige informatie invoeren, bewust of onbewust. Omdat realtime controle op prompts beperkt mogelijk is, blijft dit een inherent risico.

11.4. Wat is de impact voor betrokkene?

Antwoord:

Middel

11.5. Aanvullende maatregelen?

Antwoord:

Hoog

5 Bewaartermijn (norm 12)
(par. 3.3.5 handleiding)

12. Norm 12: Persoonsgegevens worden niet langer bewaard dan noodzakelijk is voor het realiseren van het doel of wanneer dit wettelijk is voorgeschreven. Maak gebruik van de selectielijst voor het vaststellen van de bewaartermijn.

Risico op basis van de norm.

12.1. Hoe wordt voldaan aan de norm?

Antwoord:

Microsoft 365 Copilot verwerkt verschillende categorieën persoonsgegevens waarvoor uiteenlopende bewaartermijnen gelden.
Auditlogs worden bewaard. Prompts en gegenereerde antwoorden worden per gebruiker opgeslagen in een verborgen map binnen de Exchange Online-mailbox en blijven beschikbaar totdat deze door de gebruiker of organisatie worden verwijderd.

12.2. Wat zijn de risico's die overblijven?

Antwoord:

Voor zover bewaartermijnen niet door de provincie kunnen worden beïnvloed, wordt dit betrokken bij de periodieke herbeoordeling van het restrisico. De provincie beschikt nog niet over specifiek uitgewerkte retentierichtlijnen voor Copilot-interactiedata. Dit vormt een aandachtspunt voor verdere governanceontwikkeling.

12.3. Hoe hoog is de kans dat het risico zich voordoet?

Antwoord:

Middel-Hoog

12.4. Wat is de impact voor betrokkene?

Antwoord:

MIddel

12.5. Aanvullende maatregelen?

Antwoord:

prompt-richtlijnen;
training;
AI-gebruiksbeleid;
waar mogelijk inzet van DLP/detectiemechanismen.

6 Verwijdering (norm 13)
(par. 3.3.6 handleiding)

13. Norm 13: Wanneer persoonsgegevens niet langer nodig zijn, moeten ze worden vernietigd. De persoonsgegevens moeten op een dusdanige manier worden verwijderd dat ze niet meer terug te halen zijn.

Risico op basis van de norm.

13.1. Hoe wordt voldaan aan de norm?

Antwoord:

Gebruikers kunnen individuele Copilot-dialogen of hun volledige interactiegeschiedenis verwijderen via het gebruikersportaal. Organisaties kunnen daarnaast organisatiebrede retentie- en verwijderingsinstellingen configureren voor Content Data. Het verwijderen van Content Data leidt echter niet automatisch tot verwijdering van diagnostische gegevens of service-gegenereerde data. Microsoft biedt bovendien geen mogelijkheid om verouderde Telemetry Data of serverlogs per apparaat-ID te verwijderen > volledige verwijdering is in de praktijk alleen mogelijk door het beëindigen van het Microsoft 365-gebruik.
De Provincie Gelderland beperkt dit risico door: gebruikers actief te instrueren over het verwijderen van Copilot-dialogen, periodiek te toetsen of opgeslagen interactiegegevens nog noodzakelijk zijn.

13.2. Wat zijn de risico's die overblijven?

Antwoord:

Dat het langer blijft dan noodzakelijk.

13.3. Hoe hoog is de kans dat het risico zich voordoet?

Antwoord:

Middel.

13.4. Wat is de impact voor betrokkene?

Antwoord:

Middel. Onzorgvuldige invoer van persoonsgegevens in vrije tekstvelden kan leiden tot ongewenste verwerking en oplsag van persoonsgegevens.

13.5. Aanvullende maatregelen?

Antwoord:

Zie 13.1 De Provincie Gelderland beperkt dit risico door: gebruikers actief te instrueren over het verwijderen van Copilot-dialogen, periodiek te toetsen of opgeslagen interactiegegevens nog noodzakelijk zijn.

7 Locatie (norm 14)
(par. 3.3.7 handleiding)

14. Norm 14: Verwerking van persoonsgegevens buiten de EU/EER is alleen toegestaan, indien het derde land over een passend beschermingsniveau beschikt

Risico op basis van de norm.

14.1. Hoe wordt voldaan aan de norm?

Antwoord:

Microsoft verwerkt Customer Content Data binnen de EU Data Boundary, doorgaans in datacenters in onder meer Amsterdam en Ierland. Deze geografische beperking geldt echter niet voor alle gegevensstromen. In bepaalde gevallen kunnen persoonsgegevens worden opgeslagen of verwerkt in andere regio?s waar Microsoft of diens dienstverleners faciliteiten hebben.
Daarnaast kan toegang tot gegevens plaatsvinden vanuit derde landen, bijvoorbeeld door support- of engineeringpersoneel. Voor dergelijke doorgiften maakt Microsoft gebruik van de Standard Contractual Clauses en deelname aan het EU US Data Privacy Framework. De landelijke SLM-DPIA benadrukt dat organisaties, ondanks de EU Data Boundary, zelfstandig moeten beoordelen welke risico?s samenhangen met toegang tot Account Data, Content Data en diagnostische gegevens vanuit derde landen.
De provincie beperkt deze risico?s door de tenant binnen de EU te positioneren, consumerdiensten en Bing-integraties waar mogelijk uit te schakelen, contractuele waarborgen te hanteren via de Microsoft-voorwaarden en aanvullende organisatorische maatregelen te treffen gericht op dataminimalisatie en beperkte inzet.

14.2. Wat zijn de risico’s die overblijven?

Antwoord:

Zie 14.1

14.3. Hoe hoog is de kans dat het risico zich voordoet?

Antwoord:

Middel

14.4. Wat is de impact voor betrokkene?

Antwoord:

Middel

14.5. Aanvullende maatregelen?

Antwoord:

Zie 14.1

8 Technische en organisatorische beveiligingsmaatregelen (norm 15 t/m 23)

Controleer voor deze par. (4.8) bij het team Informatieveiligheid of er een Business Impact Assessment (BIA) is uitgevoerd. Onderstaande vragen kunnen deels aan de hand van de uitgevoerde BIA worden beantwoord. Is er geen BIA uitgevoerd, betrek dan het team Informatieveiligheid bij de beantwoording van deze vragen. (par. 3.3.8 handleiding)

15. Norm 15: De methodiek van anonimiseren (herleiden naar de persoon is NIET meer mogelijk en de AVG is niet meer van toepassing) of pseudonimiseren (herleiden naar de persoon is mogelijk m.b.v. de sleutel; de AVG blijft van toepassing) worden optimaal benut.

Risico op basis van de norm.

15.1. Hoe wordt voldaan aan de norm?

Antwoord:

Microsoft 365 Copilot is niet ontworpen voor geanonimiseerde gegevensverwerking, aangezien de functionaliteit afhankelijk is van contextuele informatie uit documenten, communicatie en gebruikersinteracties. De Provincie Gelderland zet daarom primair in op dataminimalisatie en toegangsbeperking in plaats van anonimisering. Waar mogelijk worden persoonsgegevens vooraf verwijderd uit risicovolle documentlocaties. Daarnaast wordt het medewerkers verboden om persoonsgegevens in prompts op te nemen.

15.2. Wat zijn de risico's die overblijven?

Antwoord:

Middel, Omdat Copilot afhankelijk is van contextuele informatie blijft het risico bestaan dat persoonsgegevens zichtbaar worden in prompts of output.

15.3. Hoe hoog is de kans dat het risico zich voordoet?

Antwoord:

Middel

15.4. Wat is de impact voor betrokkene?

Antwoord:

Middel. In het ongunstigste geval kunnen persoonsgegevens breder zichtbaar worden binnen werkprocessen.

15.5. Aanvullende maatregelen?

Antwoord:

Zie 15.1. De Provincie Gelderland zet daarom primair in op dataminimalisatie en toegangsbeperking in plaats van anonimisering. Waar mogelijk worden persoonsgegevens vooraf verwijderd uit risicovolle documentlocaties. Daarnaast wordt het medewerkers verboden om persoonsgegevens in prompts op te nemen.

16. Norm 16: Persoonsgegevens moeten zowel fysiek (tegen diefstal, denk aan niet afgesloten dossierkasten) als technisch (logische toegangsbeveiliging, firewall, encryptie) worden beveiligd. Zowel bij de verwerkingsverantwoor-delijke als bij de verwerker.</w:t><w:br/><w:t>IT-voorzieningen en apparatuur zijn fysiek beschermd tegen toegang door onbevoegden en tegen schade en storingen. De geboden bescherming is in overeenstemming met de vastgestelde risico's.</w:t><w:br/><w:t>

Risico op basis van de norm.

16.1. Hoe wordt voldaan aan de norm?

Antwoord:

Microsoft 365 Copilot draait binnen de bestaande beveiligingsarchitectuur van de provinciale Microsoft 365-tenant en valt daarmee onder de reeds geïmplementeerde informatiebeveiligingsmaatregelen gebaseerd op de BIO. Toegang tot Copilot vereist authenticatie via het bestaande identity-platform, inclusief multi-factor authenticatie en voorwaardelijke toegangsregels waar ingericht. Daarnaast profiteert Copilot van Microsoft-beveiligingsmaatregelen zoals encryptie van data in transit en at rest, netwerkbeveiliging en continue monitoring van de cloudomgeving.

16.2. Wat zijn de risico's die overblijven?

Antwoord:

Middel

16.3. Hoe hoog is de kans dat het risico zich voordoet?

Antwoord:

Middel

16.4. Wat is de impact voor betrokkene?

Antwoord:

Middel

16.5. Aanvullende maatregelen?

Antwoord:

Zie 16.1

17. Norm 17: Alleen bevoegde gebruikers mogen toegang hebben tot de informatiesystemen en -diensten die ze voor de uitvoering van hun taken nodig hebben en om onbevoegde toegang tot informatiesystemen te voorkomen. Leg vast hoe dit is gerealiseerd.

Risico op basis van de norm.

17.1. Hoe wordt voldaan aan de norm?

Antwoord:

Copilot maakt gebruik van bestaande gebruikersmachtigingen binnen Microsoft 365.
Microsoft 365 Copilot maakt gebruik van bestaande gebruikersautorisaties en toegangsrechten binnen de Microsoft 365-omgeving van de provincie. Copilot kan uitsluitend informatie raadplegen waarvoor een gebruiker reeds geautoriseerde toegang heeft binnen systemen zoals SharePoint, Teams, OneDrive en Exchange. Authenticatie en toegangsbeheer verlopen via de bestaande Microsoft 365-beveiligings- en identityvoorzieningen van de provincie, waaronder rolgebaseerde toegang en accountbeheer.

17.2. Wat zijn de risico's die overblijven?

Antwoord:

Ondanks bestaande autorisatie- en toegangsmaatregelen blijft het risico bestaan dat persoonsgegevens of documenten breder toegankelijk zijn ingericht binnen Microsoft 365 dan organisatorisch beoogd.

17.3. Hoe hoog is de kans dat het risico zich voordoet?

Antwoord:

Middel. De kans wordt beperkt doordat Copilot bestaande autorisaties respecteert en geen toegang biedt buiten de rechten van de gebruiker.

17.4. Wat is de impact voor betrokkene?

Antwoord:

Middel tot hoog. In het ongunstigste geval kunnen persoonsgegevens of gevoelige gegevens toegankelijk worden voor een bredere interne groep medewerkers dan noodzakelijk voor de uitvoering van hun werkzaamheden. Dit kan leiden tot ongewenste kennisname, vermindering van vertrouwelijkheid en aantasting van de persoonlijke levenssfeer van betrokkenen.

17.5. Aanvullende maatregelen?

Antwoord:

bewustwording bij medewerkers over zorgvuldig delen en opslaan van informatie binnen Microsoft 365;
monitoring van ontwikkelingen rondom logging, auditing en governancefunctionaliteiten binnen Copilot en Microsoft 365;
gefaseerde implementatie van Copilot binnen de organisatie, waarbij rekening wordt gehouden met de volwassenheid van informatiebeheer en autorisatiestructuren.

18. Norm 18: Activiteiten die gebruikers en beheerders uitvoeren met persoonsgegevens worden vastgelegd in logbestanden . Dit geldt ook voor andere gebeurtenis-sen, zoals pogingen om ongeautoriseerd toegang te krijgen tot persoons-gegevens en verstoringen,

die kunnen leiden tot verminking of verlies van persoonsgegevens. De logbestanden worden periodiek gecontroleerd op indicaties van onrechtmatige toegang of onrechtmatig gebruik van de persoonsgegevens en waar nodig wordt actie ondernomen.

Risico op basis van de norm.

18.1. Hoe wordt voldaan aan de norm?

Antwoord:

De provincie De provincie onderzoekt en implementeert waar mogelijk aanvullende audit- en loggingfunctionaliteiten
om inzicht te verkrijgen in gebruikersactiviteiten, documenttoegang met Copilot.

18.2. Wat zijn de risico's die overblijven?

Antwoord:

De huidige auditmogelijkheden bieden beperkt inzicht in specifieke prompts, gegenereerde output en de volledige context van AI-interacties.

18.3. Hoe hoog is de kans dat het risico zich voordoet?

Antwoord:

Middel.

18.4. Wat is de impact voor betrokkene?

Antwoord:

Middel tot hoog. Wanneer ongewenste toegang of onrechtmatige verwerking onvoldoende zichtbaar of herleidbaar is, kan dit gevolgen hebben voor de vertrouwelijkheid en controleerbaarheid van persoonsgegevens.

18.5. Aanvullende maatregelen?

Antwoord:

monitoring Copilot-governance;
herbeoordeling loggingmogelijkheden;
beperking hoogrisico-omgevingen.

19. Norm 19: Medewerkers zijn zich bewust van hun rol t.a.v. privacy en weten hoe om te gaan met persoonsgegevens. Bewustwording wordt periodiek getraind. E.e.a. is vastgelegd in (werk)instructies/handleidingen.

Risico op basis van de norm.

19.1. Hoe wordt voldaan aan de norm?

Antwoord:

Voorafgaand aan toegang tot Copilot volgen medewerkers een verplichte instructie over verantwoord AI-gebruik, privacyrisico?s en omgang met persoonsgegevens. Deze instructie wordt ondersteund door een

vastgesteld AI-gebruiksbeleid waarin duidelijk staat: welke gegevens niet mogen worden ingevoerd, dat medewerkers eindverantwoordelijk blijven, dat output altijd moet worden gecontroleerd en dat er geen persoonsgegevens in mogen. Dit staat letterlijk in ai-beleid.

19.2. Wat zijn de risico's die overblijven?

Antwoord:

middel

19.3. Hoe hoog is de kans dat het risico zich voordoet?

Antwoord:

middel -hoog

19.4. Wat is de impact voor betrokkene?

Antwoord:

middel

19.5. Aanvullende maatregelen?

Antwoord:

zie 19.1

20. Norm 20: Er zijn beheersmaatregelen getroffen om systemen en software te beschermen en up to date te houden. Beschrijf deze.

Risico op basis van de norm.

20.1. Hoe wordt voldaan aan de norm?

Antwoord:

Microsoft is verantwoordelijk voor het technisch beheer, patchmanagement en beveiligingsupdates van de Copilot-dienst. De provincie borgt dat alleen ondersteunde versies worden gebruikt en volgt beveiligingsadviezen vanuit Microsoft actief op.

20.2. Wat zijn de risico's die overblijven?

Antwoord:

Afhankelijkheid van updates en beveiligingsmaatregelen van de leverancier.

20.3. Hoe hoog is de kans dat het risico zich voordoet?

Antwoord:

Middel

20.4. Wat is de impact voor betrokkene?

Antwoord:

Laag - middel

20.5. Aanvullende maatregelen?

Antwoord:

monitoring Microsoft security-updates;
aansluiting bestaande patch- en incidentprocessen;
periodieke herbeoordeling leveranciermaatregelen.

21. Norm 21: Er zijn procedures voor het tijdig en doeltreffend signaleren en behandelen van informatiebeveiligingsincidenten, waaronder datalekken, en zwakke plekken in de beveiliging. Het beoordelen van de risico's voor de betrokkenen en het effectief informeren van de betrokkenen en, waar van toepassing, de toezichthouder is in de procedures opgenomen. Lessen, getrokken uit de afgehandelde incidenten worden gebruikt om de beveiliging (structureel) te verbeteren. </w:t><w:br/><w:t>Wanneer een vervolgprocedure na een informatiebeveiligingsincident/datalek juridische maatregelen omvat (civiel- of strafrechtelijk), wordt het bewijsmateriaal verzameld, bewaard en gepresenteerd overeenkomstig de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd.</w:t><w:br/><w:t>

Risico op basis van de norm.

21.1. Hoe wordt voldaan aan de norm?

Antwoord:

Beveiligingsincidenten, kwetsbaarheden en mogelijke datalekken worden afgehandeld volgens het provinciale datalek- en incidentmanagementproces via Het Plein en de bestaande beveiligings- en privacyprocedures. Incidenten met betrekking tot Microsoft 365 Copilot vallen binnen deze bestaande processen en worden beoordeeld door de daarvoor bevoegde functionarissen, waaronder informatiebeveiliging, privacy en beheer. De procedures omvatten onder meer:
signalering en registratie van incidenten;
beoordeling van risico?s voor betrokkenen;
afhandeling van datalekken en beveiligingsincidenten;
melding aan de Autoriteit Persoonsgegevens indien vereist;
communicatie richting betrokkenen waar noodzakelijk;
evaluatie van incidenten en structurele verbetering van beleid, beveiliging en werkwijzen.

21.2. Wat zijn de risico's die overblijven?

Antwoord:

Nieuwe technologie kan leiden tot incidenttypen die nog niet eerder zijn voorgekomen.

21.3. Hoe hoog is de kans dat het risico zich voordoet?

Antwoord:

Middel. De kans wordt beperkt door bestaande beveiligings- en incidentmanagementprocessen binnen de provincie.

21.4. Wat is de impact voor betrokkene?

Antwoord:

Middel tot hoog. In het ongunstigste geval kunnen persoonsgegevens ongewenst toegankelijk worden, onjuist worden verwerkt of breder zichtbaar worden binnen de organisatie.

21.5. Aanvullende maatregelen?

Antwoord:

aanvullende bewustwording bij medewerkers over risico?s van generatieve AI en verantwoord gebruik van Copilot;
periodieke evaluatie van incidenten, signalen en praktijkervaringen rondom Copilot;
monitoring van ontwikkelingen rondom logging, auditing en AI-governancefunctionaliteiten binnen Microsoft 365;
gefaseerde implementatie van Copilot binnen de organisatie;
periodieke herbeoordeling van technische en organisatorische maatregelen rondom AI-toepassingen.

22. Norm 22: Continuïteitsbeheer, waarbij gebruik wordt gemaakt van een combinatie van preventieve maatregelen en herstelmaatregelen om gevolgen van incidenten tot een aanvaardbaar niveau te beperken, is ingericht. Hiermee wordt voorkomen dat persoonsgegevens door bijv. natuurrampen, ongevallen, uitval van apparatuur of opzettelijk handelen verloren gaan.</w:t><w:br/><w:t>

Risico op basis van de norm.

22.1. Hoe wordt voldaan aan de norm?

Antwoord:

Microsoft 365 Copilot maakt gebruik van de bestaande Microsoft 365-cloudinfrastructuur. Microsoft treft maatregelen voor beschikbaarheid, continuïteit en herstel, waaronder redundante infrastructuur, back-upvoorzieningen en disaster recovery-mechanismen binnen de cloudomgeving.

Daarnaast sluit de inzet van Copilot aan op de bestaande continuïteits- en informatiebeveiligingsmaatregelen van de provincie voor Microsoft 365-diensten. Verstoring of uitval van Copilot leidt niet tot verlies van persoonsgegevens in de onderliggende bronsystemen, omdat gegevens primair worden opgeslagen binnen bestaande Microsoft 365-omgevingen zoals SharePoint, Exchange, Teams en OneDrive.

22.2. Wat zijn de risico's die overblijven?

Antwoord:

Ondanks de getroffen continuïteitsmaatregelen blijft het risico bestaan dat storingen, uitval of verstoringen binnen Microsoft 365 of Copilot tijdelijk gevolgen hebben voor de beschikbaarheid van informatie en ondersteuning van werkprocessen.

22.3. Hoe hoog is de kans dat het risico zich voordoet?

Antwoord:

laag. Grote cloudplatformen zoals Microsoft 365 beschikken over uitgebreide continuïteits- en herstelvoorzieningen.

22.4. Wat is de impact voor betrokkene?

Antwoord:

Laag.

22.5. Aanvullende maatregelen?

Antwoord:

monitoring van storingen.

23. Norm 23: Wanneer (een deel van) de verwerking van persoonsgegevens bij een andere partij plaatsvindt in opdracht en volgens de eisen van de verwerkingsverantwoordelijke plaatsvindt, moet voorafgaand aan de verwerking, een verwerkersovereenkomst worden afgesloten. </w:t><w:br/><w:t>

Risico op basis van de norm.

23.1. Hoe wordt voldaan aan de norm?

Antwoord:

Microsoft treedt op als verwerker voor persoonsgegevens die binnen Microsoft 365 worden verwerkt. De afspraken hierover zijn vastgelegd in de bestaande contractuele afspraken, waaronder de verwerkersovereenkomst en het Microsoft Data Protection Addendum (DPA). Hierin zijn afspraken opgenomen over beveiliging, vertrouwelijkheid, subverwerkers, auditmogelijkheden en gegevensbescherming conform de AVG.

23.2. Wat zijn de risico's die overblijven?

Antwoord:

Ondanks de bestaande contractuele afspraken blijft sprake van afhankelijkheid van een grote internationale cloudleverancier, waarbij de mogelijkheden tot maatwerk of aanvullende onderhandelingen beperkt zijn.

23.3. Hoe hoog is de kans dat het risico zich voordoet?

Antwoord:

Middel. Microsoft beschikt over uitgebreide beveiligings- en compliancevoorzieningen en contractuele afspraken conform de AVG.

23.4. Wat is de impact voor betrokkene?

Antwoord:

laag.

23.5. Aanvullende maatregelen?

Antwoord:

monitoring van ontwikkelingen rondom Europese regelgeving, internationale doorgifte en cloudjurisprudentie;
toepassing van aanvullende organisatorische maatregelen, zoals autorisatiebeheer, classificatie en bewustwording;
afstemming met informatiebeveiliging, privacy en juridische functies over ontwikkelingen rondom Microsoft 365 en Copilot.

9 Informatieplicht (norm 24 t/m 26)

par. 3.3.9 handleiding

24. Norm 24: Betrokkenen moeten, op het moment dat zij persoonsgegevens hebben verstrekt, worden geïnformeerd over de verwerking. Zie het gestelde in AVG, artikel 13.</w:t><w:br/><w:t>

Risico op basis van de norm.

24.1. Hoe wordt voldaan aan de norm?

Antwoord:

Provincie Gelderland informeert medewerkers transparant over het gebruik van Microsoft 365 Copilot en de mogelijke verwerking van persoonsgegevens binnen deze werkomgeving. Deze informatie wordt opgenomen in onder meer:

het privacybeleid;
het AI-gebruiksbeleid;
interne communicatie voorafgaand aan implementatie;
gebruikersrichtlijnen;
trainingen en bewustwordingsactiviteiten.

Hierin wordt toegelicht welke typen gegevens Copilot kan verwerken, voor welke doeleinden de technologie wordt ingezet en welke verantwoordelijkheden medewerkers hebben bij zorgvuldig gebruik van AI-functionaliteiten. Daarnaast blijft de bestaande privacyinformatie van Provincie Gelderland van toepassing op de verwerking van persoonsgegevens binnen de Microsoft 365-omgeving.

24.2. Wat zijn de risico's die overblijven?

Antwoord:

Ondanks de getroffen maatregelen blijft het risico bestaan dat betrokkenen niet volledig bekend zijn met de wijze waarop generatieve AI-functionaliteiten zoals Copilot persoonsgegevens binnen bestaande werkprocessen kunnen verwerken, combineren of presenteren. Daarnaast bestaat het risico dat medewerkers zich onvoldoende bewust zijn van hun eigen verantwoordelijkheid bij het verwerken van persoonsgegevens met behulp van Copilot.

24.3. Hoe hoog is de kans dat het risico zich voordoet?

Antwoord:

Laag-middel. De kans wordt beperkt door actieve communicatie, beleid, richtlijnen en bewustwording rondom het gebruik van Copilot.

24.4. Wat is de impact voor betrokkene?

Antwoord:

Laag tot middel. In het ongunstigste geval kunnen betrokkenen onvoldoende inzicht ervaren in de wijze waarop persoonsgegevens binnen AI-ondersteunde werkprocessen worden verwerkt.

24.5. Aanvullende maatregelen?

Antwoord:

periodieke actualisatie van privacyinformatie en AI-gerelateerde richtlijnen;
aanvullende bewustwording en training voor medewerkers;
heldere interne communicatie over verantwoord gebruik van Copilot;
evaluatie van signalen, vragen en incidenten rondom transparantie en AI-gebruik;
periodieke herbeoordeling van de informatievoorziening rondom AI-functionaliteiten binnen Microsoft 365.

25. Norm 25: Wanneer de persoonsgegevens niet van betrokkene zelf zijn verkregen moet betrokkene uiterlijk een maand na het verkrijgen worden geïnformeerd.De informatie moet voldoen aan AVG, artikel 14.</w:t><w:br/><w:t>

Risico op basis van de norm.

25.1. Hoe wordt voldaan aan de norm?

Antwoord:

Microsoft 365 Copilot verwerkt persoonsgegevens die reeds binnen de provinciale Microsoft 365-omgeving aanwezig zijn en toegankelijk zijn op basis van bestaande autorisaties. Copilot fungeert daarbij als ondersteunende functionaliteit binnen de bestaande digitale werkomgeving en vormt geen zelfstandige nieuwe gegevensbron. De inzet van Copilot is gericht op ondersteuning van interne werkprocessen, zoals samenvatten, structureren en raadplegen van informatie waarvoor medewerkers reeds geautoriseerde toegang hebben. Er worden geen persoonsgegevens actief bij derden verzameld ten behoeve van Copilot. Omdat Copilot persoonsgegevens verwerkt binnen reeds bestaande informatiestromen en autorisaties, en geen sprake is van een afzonderlijk contactmoment of rechtstreekse gegevensverzameling bij betrokkenen, wordt aanvullende individuele informatieverstrekking op grond van artikel 14 AVG niet proportioneel en redelijkerwijs niet noodzakelijk geacht. transparantie woredt geborgd via interne kaders en communicatie binnen de organisatie.

25.2. Wat zijn de risico's die overblijven?

Antwoord:

Ondanks de getroffen maatregelen blijft het risico bestaan dat persoonsgegevens via Microsoft 365 Copilot worden verwerkt op een wijze die betrokkenen niet volledig hadden verwacht. Daarnaast bestaat een restrisico dat medewerkers via prompts of samenvattingen toegang krijgen tot persoonsgegevens uit documenten of samenwerkingsomgevingen waarvoor autorisaties technisch correct zijn ingericht, maar waarvan de inhoud breder beschikbaar blijkt dan organisatorisch wenselijk was.

25.3. Hoe hoog is de kans dat het risico zich voordoet?

Antwoord:

Laag tot middel. De kans wordt beperkt doordat Copilot uitsluitend werkt binnen bestaande Microsoft 365-autorisaties en geen zelfstandige gegevensbron vormt.

25.4. Wat is de impact voor betrokkene?

Antwoord:

De impact voor betrokkenen is over het algemeen beperkt tot middelgroot. In het ongunstigste geval kunnen persoonsgegevens breder inzichtelijk of makkelijker doorzoekbaar worden binnen de bestaande werkomgeving dan oorspronkelijk beoogd. Dit kan leiden tot vermindering van de ervaren controle over persoonsgegevens of ongewenste kennisname door interne medewerkers. Er is geen sprake van geautomatiseerde besluitvorming of profiling door Copilot binnen deze verwerking.

25.5. Aanvullende maatregelen?

Antwoord:

Aanvullende maatregelen bestaan uit:
bewustwording en training van medewerkers over zorgvuldig gebruik van Copilot en omgang met persoonsgegevens;
monitoring van ontwikkelingen rondom logging, auditing en governance-functionaliteiten binnen Microsoft 365 Copilot;
het opnemen van transparantie over AI-functionaliteiten
periodieke evaluatie van de risico?s en het gebruik van Copilot binnen de organisatie.

26. Norm 26: Geautomatiseerde besluitvorming (waaronder ook profilering), zonder menselijke tussenkomst, is niet toegestaan. Zie het gestelde in AVG, artikel 22.</w:t><w:br/><w:t>

Risico op basis van de norm.

26.1. Hoe wordt voldaan aan de norm?

Antwoord:

Microsoft 365 Copilot wordt niet ingezet voor geautomatiseerde besluitvorming of profilering met rechtsgevolgen voor betrokkenen. Copilot ondersteunt uitsluitend medewerkers bij het opstellen en structureren van informatie. Menselijke beoordeling en besluitvorming blijven te allen tijde vereist.

26.2. Wat zijn de risico’s die overblijven?

Antwoord:

Medewerkers kunnen geneigd zijn sterk te vertrouwen op AI-output.

26.3. Hoe hoog is de kans dat het risico zich voordoet?

Antwoord:

Middel

26.4. Wat is de impact voor betrokkene?

Antwoord:

Middel

26.5. Aanvullende maatregelen?

Antwoord:

Zie 26.1

10 Overige risico's (norm 27)

27. Norm 27: Zijn er andere hoge risico's met betrekking tot de verwerking van persoonsgegevens die nog niet genoemd zijn?</w:t><w:br/><w:t>

Risico op basis van de norm.

27.1. Hoe wordt voldaan aan de norm?

Antwoord:

1. Door de natuurlijke taal en overtuigende formulering van Copilot-antwoorden kunnen medewerkers geneigd zijn output als feitelijk juist te beschouwen, ook wanneer deze gebaseerd is op verouderde of onvolledige broninformatie.
2. Generatieve AI maakt gegevensstromen minder zichtbaar voor gebruikers en beheerders. Hierdoor wordt het lastiger om volledig inzicht te houden in hoe informatie wordt gebruikt en gecombineerd.

De provincie onderkent deze risico?s en adresseert deze via versterkte AI-governance, gefaseerde implementatie en periodieke herbeoordeling van de inzet van Copilot.

27.2. Wat zijn de risico's die overblijven?

Antwoord:

Generatieve AI-toepassingen zoals Copilot zijn ontworpen om overtuigende en natuurlijk geformuleerde antwoorden te geven, waardoor gebruikers sneller geneigd kunnen zijn de output als betrouwbaar te beschouwen. De kans wordt beperkt door interne richtlijnen, bewustwording en gefaseerde implementatie, maar kan niet volledig worden weggenomen.

27.3. Hoe hoog is de kans dat het risico zich voordoet?

Antwoord:

middel

27.4. Wat is de impact voor betrokkene?

Antwoord:

De impact voor betrokkenen is beperkt tot middelgroot. In het ongunstigste geval kunnen persoonsgegevens onjuist worden geïnterpreteerd, in een verkeerde context worden gebruikt of breder inzichtelijk worden binnen bestaande werkprocessen.Er is geen sprake van volledig geautomatiseerde besluitvorming of profiling zonder menselijke tussenkomst.

27.5. Aanvullende maatregelen?

Antwoord:

bewustwordingstrainingen over hallucinerende output, bias, verouderde informatie en verantwoord gebruik van generatieve AI;

11 Rechten van betrokkene (norm 28)

28. Norm 28: Beschrijf de procedure waarmee invulling wordt gegeven aan de rechten van de betrokkenen. Als de rechten van de betrokkene worden beperkt, beschrijf op grond van welke wettelijke uitzondering dat is toegestaan.</w:t><w:br/><w:t>

Risico op basis van de norm.

28.1. Hoe wordt voldaan aan de norm?

Antwoord:

De inzet van Microsoft 365 Copilot verandert de bestaande rechten van betrokkenen niet. Persoonsgegevens die via Copilot worden geraadpleegd of verwerkt, zijn afkomstig uit reeds bestaande provinciale informatiesystemen zoals SharePoint, OneDrive, Exchange en Teams. Betrokkenen kunnen hun AVG-rechten uitoefenen via de reguliere provinciale procedures (via "Het Plein') die tevens gelden voor deze bronsystemen. Copilot fungeert hierbij uitsluitend als ondersteunende technologie en vormt geen zelfstandige gegevensbron. Wanneer persoonsgegevens in bronbestanden worden gecorrigeerd of verwijderd, werkt dit automatisch door in de informatie die Copilot kan raadplegen.

28.2. Wat zijn de risico's die overblijven?

Antwoord:

Ondanks de bestaande procedures voor het uitoefenen van AVG-rechten blijft het risico bestaan dat betrokkenen onvoldoende inzicht hebben in de wijze waarop persoonsgegevens via Copilot worden geraadpleegd, gecombineerd of weergegeven binnen de Microsoft 365-omgeving. Daarnaast kan het in de praktijk complex zijn om volledig te overzien in welke documenten, samenvattingen of contexten persoonsgegevens via Copilot zichtbaar zijn geweest. Ook bestaat een restrisico dat verouderde, dubbele of onjuist opgeslagen informatie in onderliggende bronsystemen indirect invloed heeft op de output van Copilot.

28.3. Hoe hoog is de kans dat het risico zich voordoet?

Antwoord:

Laag tot middel. De kans wordt beperkt doordat Copilot werkt binnen bestaande Microsoft 365-autorisaties en rechtstreeks gebruikmaakt van actuele informatie uit de bronsystemen. Daarnaast blijven bestaande processen voor correctie, verwijdering en afhandeling van AVG-verzoeken van toepassing. Het restrisico blijft aanwezig vanwege de complexiteit van generatieve AI-functionaliteiten en de afhankelijkheid van de kwaliteit van brondata en autorisatiestructuren.

28.4. Wat is de impact voor betrokkene?

Antwoord:

Laag tot middel. In het ongunstigste geval kunnen betrokkenen tijdelijk verminderde controle ervaren over hoe persoonsgegevens binnen interne werkprocessen worden weergegeven of gecombineerd via Copilot. Dit kan leiden tot onduidelijkheid over de context waarin gegevens zichtbaar zijn geweest of zijn gebruikt.

28.5. Aanvullende maatregelen?

Antwoord:

duidelijke procedures AVG-verzoeken;
bewustwording medewerkers;
herbeoordeling invloed Copilot op betrokkenenrechten.

Advies FG

De DPIA moetverplicht worden voorgelegdaan de FG zodat hij/zij een advies op kan stellen. In het rapport over de DPIA moet het advies van de FG worden opgenomen en wordt aangegeven wat de verantwoordelijke daarmee heeft gedaan. De FG heeft ook als taak de uitvoering van de DPIA te bewaken.

De FG geeftgéén akkoordover een DPIA, dat is voorbehouden aan de proceseigenaar/ afdelingsmanager; de FG geeft eenzwaarwegend advies.

De FG geeft een advies over de uitgevoerde DPIA. Het advies van de FG is zwaarwegend, dat wil zeggen dat het advies van de FG in principe moet worden opgevolgd. Besluit de proceseigenaar/ lijnverantwoordelijke af te wijken van het (negatieve) advies van de FG dan moet dit gemotiveerd geschieden. Deze motivatie moet schriftelijk worden vastgelegd, zodat de organisatie zich - wanneer nodig - verantwoorden.

De FG kan ook een positief advies met aanvullende voorwaarden/maatregelen geven. D.w.z. dat aanvullende maatregelen moeten worden genomen om bepaalde risico's verder te verkleinen. In dit geval neemt de proceseigenaar/lijnverantwoordelijke deze aanvullende maatregelen op in een de projectdocumentatie / implementatieplan en bewaakt de realisatie van de aanvullende maatregelen.

176. Advies van de FG

In dit hoofdstuk geeft de FG aan wat zijn zwaarwegend advies is. Ook kan hij/zij aanvullende maatregelen voorstellen als er naar zijn/haar oordeel nog te grote restrisico's bestaan na de getroffen (informatiebeveiliging en organisatorische) maatregelen.

Antwoord:

De FG heeft bij de eerdere beoordeling vastgesteld dat de DPIA op enkele essentiële onderdelen nadere uitwerking vereiste, met name ten aanzien van de noodzakelijkheidstoets, proportionaliteit, de systematische risicobeoordeling, governance, internationale gegevensdoorgifte en de afhankelijkheid van beheersmaatregelen die nog niet waren geïmplementeerd. Tevens werd het restrisico als hoog beoordeeld en ontbrak een expliciete bestuurlijke afweging.

Naar aanleiding hiervan is de DPIA integraal herzien. In deze versie zijn de risico?s methodisch uitgewerkt, inclusief kans en impact, is de inzet van Copilot begrensd tot een gefaseerde pilot en zijn aanvullende

technische en organisatorische maatregelen geconcretiseerd. Ook is verduidelijkt onder welke voorwaarden verdere uitrol verantwoord kan plaatsvinden.

De provincie verzoekt de FG deze herijkte DPIA opnieuw te beoordelen en te adviseren over de toelaatbaarheid van inzet binnen een gecontroleerde pilotfase.

Beoogde aanvullende maatregelen richting implementatie:
-versnelde opschoning en labeling (dit zijn retentielabels en sensitivity labels en DLP) van documentomgevingen
-inrichting van tenantbrede auditlogging
-vaststelling van AI-gebruiksbeleid en verplichte training

Verdere opschaling buiten de pilotfase vindt uitsluitend plaats nadat de aanvullende beheersmaatregelen aantoonbaar zijn ingericht en opnieuw zijn beoordeeld op effectiviteit en proportionaliteit.

++

Hernieuwd FG-advies MS365 Copilot binnen de Provincie Gelderland

1. Inleiding
Voorliggend advies betreft de herbeoordeling van de aangevulde DPIA over het voorgenomen gebruik van Microsoft 365 Copilot binnen de Provincie Gelderland.

De eerdere versie van de DPIA is door mij beoordeeld, waarna ik concludeer dat de DPIA op meerdere essentiële onderdelen nadere uitwerking vereiste en dat het restrisico op dat moment als hoog moest worden aangemerkt.

De voorliggende, aangevulde DPIA is op relevante onderdelen verdiept. Daarbij zijn met name de noodzakelijkheidstoets, de afbakening van de voorgenomen inzet, de risicobeoordeling per norm, de governance en de voorgenomen technische en organisatorische maatregelen verder uitgewerkt. De herbeoordeling richt zich daarom op twee vragen:
1. Of de aangevulde DPIA op dit moment als voldoende kan worden beschouwd voor besluitvorming over een gecontroleerde pilot;
2. Onder welke voorwaarden inzet van Copilot privacyrechtelijk verantwoord kan plaatsvinden.

Dit zwaarwegend advies is opgesteld met inachtneming van artikel 35 en 36 AVG, de EDPB-richtsnoeren voor DPIA?s, de in de DPIA verwerkte landelijke bevindingen over Copilot en de specifieke provinciale context zoals beschreven in de aangevulde DPIA.
2. Samenvatting van de herbeoordeling
De aangevulde DPIA is inhoudelijk en methodisch duidelijk sterker dan de eerdere versie. De DPIA bevat nu een duidelijkere afbakening van het doel van Copilot, een expliciet ondersteunend karakter van de toepassing, een uitsluiting van geautomatiseerde besluitvorming en profilering, en een uitwerking van risico?s en maatregelen over meerdere AVG-normen heen.

Daarnaast is de inzet van Copilot expliciet begrensd tot een gefaseerde en gecontroleerde pilot, waarbij vooraf een risicogerichte opschoningsactie wordt uitgevoerd binnen documentomgevingen waarin mogelijk gevoelige persoonsgegevens voorkomen, zoals cv?s en BSN?s. Ook is beschreven dat hoge-risico-toepassingen, zoals inzet in HR-dossiers, integriteitscontexten en andere dossiers met bijzondere

persoonsgegevens, buiten de scope van de voorgenomen inzet vallen.

Daarmee is de DPIA op dit moment voldoende verbeterd om als basis te dienen voor een besluit over een strikt afgebakende pilotfase. Voor organisatiebrede uitrol geldt dat oordeel echter nadrukkelijk niet. De organisatiebrede informatiehuishouding, autorisatiestructuur, labeling, retentie en logging zijn daarvoor nog niet aantoonbaar op een zodanig niveau ingericht dat het restrisico buiten de pilotfase als voldoende beheerst kan worden beschouwd.

3. Beoordeling van de aangevulde DPIA

3.1 Compleetheid en methodologie
In vergelijking met de eerdere versie bevat de aangevulde DPIA een duidelijk meer systematische opzet. De risico?s zijn per norm uitgewerkt en in meerdere gevallen voorzien van een expliciete beoordeling van kans en impact. Ook is de relatie tussen de voorgenomen inzet van Copilot, de bestaande Microsoft 365-omgeving en de kwaliteit van brondata en autorisaties scherper beschreven dan in de eerdere versie.

Nog steeds geldt dat de kwaliteit van de risicobeoordeling in belangrijke mate staat of valt met de feitelijke uitvoering van de beschreven maatregelen. Waar de DPIA maatregelen benoemt als randvoorwaarde voorafgaand aan de pilot, kunnen deze in de beoordeling worden betrokken; waar maatregelen nog toekomstig of onzeker zijn, mogen zij niet zonder meer als gerealiseerde risicoreductie worden meegewogen.

3.2 Doel, grondslag en afbakening
De DPIA positioneert Copilot als een ondersteunende functionaliteit binnen bestaande provinciale werkprocessen, zoals het opstellen, samenvatten en structureren van documenten, e-mails en presentaties. Daarbij is expliciet opgenomen dat Copilot niet wordt gebruikt voor geautomatiseerde besluitvorming, profilering of monitoring van medewerkers.

De gekozen grondslag van artikel 6 lid 1 sub e AVG, taak van algemeen belang / uitoefening van openbaar gezag, is in deze context in beginsel verdedigbaar, nu de inzet volgens de DPIA ondersteunend is aan al bestaande provinciale taken en niet is gericht op nieuwe, zelfstandige verwerkingsdoeleinden. Wel blijft van belang dat de feitelijke inzet in de praktijk ook binnen deze afbakening blijft en niet opschuift naar toepassingen met een zwaarder risicoprofiel.

3.3 Praktische inrichting en bronrisico?s
De kern van het privacyrisico bij Copilot ligt ook in de aangevulde DPIA nog steeds bij de bestaande kwaliteit van de informatiehuishouding. De DPIA benoemt uitdrukkelijk dat Copilot gegevens uit bestaande Microsoft 365-bronnen ontsluit, waaronder SharePoint, Exchange Online en Teams, en dat verouderde documenten, te ruime toegangsrechten en ontbrekende labeling ertoe kunnen leiden dat persoonsgegevens via Copilot als bruikbare output beschikbaar komen.

Deze analyse is juist en sluit aan bij het eerdere FG-advies, waarin werd vastgesteld dat SharePoint-omgevingen verouderde documenten, te ruime autorisaties en ontbrekende labeling bevatten, waardoor oversharing een substantieel risico vormt. Positief is dat de aangevulde DPIA hier nu niet omheen werkt, maar juist expliciet als randvoorwaarde voor inzet opneemt dat voorafgaand aan de pilot risicogerichte opschoning van documentomgevingen moet plaatsvinden.

3.4 Bijzondere persoonsgegevens, BSN en promptgebruik
De DPIA stelt uitdrukkelijk dat het gebruik van Copilot voor bijzondere persoonsgegevens, strafrechtelijke

gegevens en BSN?s niet is toegestaan, en dat dit in beleid, werkinstructies en training wordt vastgelegd. Tegelijkertijd wordt onderkend dat dergelijke gegevens ondanks dat aanwezig kunnen zijn in bestaande content, bijvoorbeeld in oude documenten of bijlagen, en dat dit juist een kernrisico vormt voor de inzet van Copilot.

Deze erkenning is van groot belang. Het restrisico rond bijzondere persoonsgegevens en BSN?s kan alleen dalen wanneer de pilot daadwerkelijk wordt beperkt tot geselecteerde omgevingen, vooraf risicogericht wordt opgeschoond en risicolocaties aantoonbaar buiten de pilotscope blijven. Zonder deze feitelijke begrenzing zou het restrisico op dit punt hoog blijven.

3.5 Transparantie, logging en governance
De DPIA bevat een duidelijker beschrijving van prompts, gegenereerde output, bewaartermijnen en de opslag van interactiegegevens dan de eerdere versie. Ook wordt onderkend dat de provincie nog niet beschikt over volledig uitgewerkte retentierichtlijnen voor Copilot-interactiedata en dat logging en monitoring een belangrijk aandachtspunt blijven.

Dit betekent dat governance, logging en evaluatie niet als randverschijnselen mogen worden behandeld, maar als noodzakelijke voorwaarden voor een verantwoorde pilot. Mijn eerdere FG-advies benadrukte al dat het ontbreken van tenantbrede auditlogging en een duidelijke AI-governance een wezenlijk tekort was. Die constatering is met de aangevulde DPIA niet volledig weggenomen, echter wel beter geadresseerd voor zover het de pilotfase betreft.

4. Beoordeling van het restrisico
4.1 Restrisico in de pilotfase
De beoordeling van het restrisico moet nadrukkelijk worden onderscheiden tussen de pilotfase en organisatiebrede uitrol. De aangevulde DPIA beschrijft dat de pilot pas start nadat een eerste risicogerichte opschoningsronde aantoonbaar is uitgevoerd en dat de inzet beperkt blijft tot afgebakende teams en omgevingen.

Wanneer deze randvoorwaarden daadwerkelijk vooraf zijn gerealiseerd, acht ik het verdedigbaar om het restrisico binnen de pilotfase als middel te kwalificeren. Dat oordeel steunt op de combinatie van voorafgaande opschoning, beperkte scope, uitsluiting van hoge-risico-dossiers, verplichte training, beleidsmatige begrenzing en periodieke evaluatie.

Dit betekent niet dat de risico?s gering zijn. Ook in de pilot blijft sprake van reële risico?s op oversharing, onjuiste of verouderde output, onbedoelde verwerking van persoonsgegevens uit historische documenten en oneigenlijk promptgebruik. Het verschil is dat deze risico?s binnen de afgebakende pilotcontext naar mijn oordeel beheersbaar kunnen worden gemaakt, onder de voorwaarde dat de beschreven maatregelen niet alleen op papier bestaan maar aantoonbaar zijn gerealiseerd en actief worden bewaakt.

4.2 Restrisico buiten de pilotfase
Voor organisatiebrede uitrol luidt het oordeel anders. Buiten de afgebakende pilotcontext geldt nog steeds dat de provinciale Microsoft 365-omgeving niet organisatiebreed aantoonbaar is opgeschoond, dat labeling, retentie en autorisatiebeheer nog niet volledig op orde zijn en dat logging en governance nog verdere versterking behoeven.

Daarom blijft het restrisico buiten de pilotfase op dit moment hoog. De aangevulde DPIA biedt onvoldoende basis om nu al te concluderen dat organisatiebrede inzet van Copilot rechtmatig en verantwoord kan plaatsvinden.

5. Hernieuwd FG-oordeel
Als FG beoordeel ik de aangevulde DPIA als voldoende verbeterd om een besluit over een strikt afgebakende en gecontroleerde pilot met Microsoft 365 Copilot te kunnen dragen. De DPIA is niet meer op dezelfde wijze onvolledig als de eerdere versie en bevat nu een duidelijker afbakening van doel, scope, restrisico?s en randvoorwaarden.

Daarmee luidt het hernieuwde oordeel als volgt:
? Voor een gecontroleerde pilotfase met een beperkte gebruikersgroep en afgebakende omgevingen, onder vooraf aantoonbaar gerealiseerde randvoorwaarden, acht ik de inzet van Microsoft 365 Copilot toelaatbaar;
? Het restrisico wordt in die pilotfase beoordeeld als middel;
? Voor organisatiebrede uitrol blijft het restrisico op dit moment hoog en is verdere opschaling nog niet verantwoord.

Als FG geef ik geen ?akkoord? in bestuurlijke zin, echter een zwaarwegend advies. De verantwoordelijkheid voor het al dan niet opvolgen van dit advies ligt bij de proceseigenaar en het bevoegd management, waarbij afwijking van het FG-advies schriftelijk en gemotiveerd moet worden vastgelegd.

6. Voorwaarden voor de pilot
Als FG adviseer ik de pilot uitsluitend toe te staan onder de volgende cumulatieve voorwaarden:
1. Voorafgaande risicogerichte opschoning
Binnen de pilotscope moet aantoonbaar een opschoningsactie zijn uitgevoerd, met bijzondere aandacht voor documenten en omgevingen waarin cv?s, BSN?s, HR-gerelateerde gegevens, integriteitsinformatie, medische gegevens of andere gevoelige persoonsgegevens kunnen voorkomen;
2. Strikte scopebeperking
Copilot wordt uitsluitend geactiveerd voor een beperkte en geselecteerde pilotgroep en alleen binnen vooraf aangewezen omgevingen. Hoge-risico-dossiers en andere uitgesloten categorieën blijven aantoonbaar buiten de pilotscope;
3. Vastgesteld AI-gebruiksbeleid
Voor aanvang van de pilot moet een vastgesteld beleidskader beschikbaar zijn waarin ten minste is opgenomen welke gegevens niet via Copilot mogen worden verwerkt, dat bijzondere persoonsgegevens en BSN?s verboden zijn, dat output altijd moet worden geverifieerd en dat incidenten en fouten gemeld moeten worden;
4. Verplichte training en bewustwording
Alle pilotgebruikers moeten voorafgaand aan ingebruikname aantoonbaar zijn geïnstrueerd over zorgvuldig promptgebruik, dataminimalisatie, verificatie van output en meldplicht bij incidenten;
5. Logging, monitoring en evaluatie
Voor zover technisch haalbaar moeten logging en monitoring worden ingericht voor de pilot, inclusief periodieke evaluatie van incidenten, oversharinggevallen, promptgebruik en de effectiviteit van de getroffen maatregelen;
6. Bestuurlijke herbeoordeling vóór opschaling
Na afronding van de pilot moet expliciet worden beoordeeld of de risico?s daadwerkelijk zijn verminderd, of de maatregelen effectief zijn gebleken en of de voorwaarden voor eventuele verdere uitrol zijn vervuld. Zonder herbeoordeling mag geen opschaling plaatsvinden.

7. Voorwaarden voor verdere uitrol
Voordat een besluit over bredere uitrol kan worden genomen, moeten in ieder geval de volgende punten aantoonbaar verder zijn ingericht:

? Structurele verbetering van IAM en need-to-know-autorisaties;
? Verdere opschoning van SharePoint- en OneDrive-omgevingen;
? Bredere en bestendige toepassing van labeling, retentie en DLP-maatregelen;
? Volwassen logging, auditing en governance rondom Copilot-gebruik;
? Aantoonbare evaluatie van de pilotresultaten en van feitelijke incidenten of oversharingbevindingen.

Zolang deze punten niet aantoonbaar zijn gerealiseerd, kan organisatiebrede uitrol niet als voldoende zorgvuldig en proportioneel worden beschouwd.

8. Eindoordeel
Als FG adviseer ik de Provincie Gelderland om de aangevulde DPIA vast te stellen als basis voor een beperkte en gecontroleerde pilot met Microsoft 365 Copilot, onder de in dit advies genoemde voorwaarden. Voor die pilotfase kan het restrisico, gelet op de beschreven begrenzingen en randvoorwaarden, als middel worden beoordeeld.

Ik adviseer nadrukkelijk niet om op basis van de huidige situatie over te gaan tot organisatiebrede uitrol. Daarvoor blijft het restrisico op dit moment hoog, met name vanwege de huidige staat van de informatiehuishouding, autorisaties, labeling, retentie en logging buiten de afgebakende pilotcontext.

Samengavat luidt het advies luidt dan ook:

Sta een strikt afgebakende pilot toe onder vooraf aantoonbaar gerealiseerde voorwaarden, evalueer deze pilot zorgvuldig en besluit pas daarna, op basis van een hernieuwde beoordeling, of verdere opschaling verantwoord is.

Opgesteld, 2 juni 2026

5.1.2e
Functionaris Gegevensbescherming