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.

44726565 0006

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

44726565 0006