# Is Microsoft Office 365 AVG Proof in Nederland?



## Juridische en Technische Analyse per 18 april 2025

## 1. Inleiding

De vraag of Microsoft Office 365 (hierna: M365) voldoet aan de eisen van de Algemene Verordening Gegevensbescherming (AVG) [1] is van significant belang voor talloze organisaties in Nederland. Gezien de wijdverbreide adoptie van M365 binnen zowel de publieke als private sector, inclusief overheidsinstanties, onderwijsinstellingen en het bedrijfsleven [3], raakt de AVG-compliance status van deze clouddienst een aanzienlijk deel van de Nederlandse digitale infrastructuur. De aantrekkingskracht van clouddiensten zoals M365 ligt in de beloofde voordelen van efficiëntie, schaalbaarheid en flexibiliteit.[3] Echter, deze voordelen gaan gepaard met inherente uitdagingen op het gebied van gegevensbescherming, met name wanneer gebruik wordt gemaakt van diensten aangeboden door grote, vaak in de Verenigde Staten gevestigde, technologieleveranciers zoals Microsoft.[6]

Het belang van dit onderzoek wordt onderstreept door de strikte verplichtingen die de AVG oplegt aan zowel verwerkingsverantwoordelijken als verwerkers.[1] Non-compliance kan leiden tot aanzienlijke financiële sancties [1] en reputatieschade. Binnen M365 worden potentieel grote hoeveelheden persoonsgegevens verwerkt, waaronder mogelijk ook gevoelige en bijzondere persoonsgegevens zoals gedefinieerd in de AVG (bijvoorbeeld gezondheidsgegevens in de zorg of gegevens over ras of religie).[11] Dit vereist een grondige

risicoanalyse en de implementatie van passende technische en organisatorische waarborgen.

De relevantie van de onderzoeksvraag wordt verder versterkt door recente juridische en technologische ontwikkelingen. De uitspraak van het Hof van Justitie van de Europese Unie in de zaak Schrems II [9] heeft de juridische basis voor gegevensoverdracht naar de Verenigde Staten fundamenteel ter discussie gesteld, met directe implicaties voor Amerikaanse cloudproviders. Technologische innovaties, zoals de integratie van kunstmatige intelligentie (AI) in M365 via Copilot [20], introduceren nieuwe complexiteiten en potentiële privacyrisico's. Daarnaast hebben beleidsmatige discussies, zoals die rondom het Rijksbreed cloudbeleid [3] en Microsoft's eigen initiatieven zoals de EU Data Boundary [30], de context voortdurend veranderd.

Specifiek voor de Nederlandse situatie zijn de onderzoeken en Data Protection Impact Assessments (DPIA's) uitgevoerd door de Autoriteit Persoonsgegevens (AP) en het Strategisch Leveranciersmanagement Rijk (SLM Rijk) van cruciaal belang.[8] Deze bieden unieke, op de Nederlandse context gerichte inzichten in de risico's en de (on)volkomenheden van de door Microsoft geboden waarborgen.

Dit academische paper beoogt een kritische evaluatie te bieden van de AVG-compliance status van M365 in Nederland, actueel tot 18 april 2025. De analyse richt zich op de kerncomponenten van M365, waaronder Exchange Online, SharePoint Online, OneDrive for Business, Teams en relevante aspecten van Copilot voor M365. De focus ligt op de Nederlandse juridische en praktische context, waarbij EU-regelgeving (AVG) en jurisprudentie (Schrems II) die direct relevant zijn voor Nederland, worden meegenomen. De paper is gestructureerd volgens de academische conventies, beginnend met de methodologie, gevolgd door de presentatie van de resultaten, een kritische discussie en synthese van de bevindingen, en afgesloten met een summarium en referentielijst.

## 2. Methodologie

De onderzoeksaanpak voor dit paper is gebaseerd op een kwalitatieve, desk-research gebaseerde analyse. Er is een systematische review uitgevoerd van diverse relevante bronnen om een alomvattend en genuanceerd beeld te vormen van de AVG-compliance van M365 in Nederland per 18 april 2025.

De primaire juridische bronnen omvatten de tekst van de Algemene Verordening Gegevensbescherming (AVG) zelf, alsmede relevante Nederlandse wetgeving zoals de Uitvoeringswet AVG (UAVG) en de Telecommunicatiewet, met name waar deze specifieke eisen stelt aan gegevensverwerking of toestemming (bijvoorbeeld artikel 11.7a Tw voor cookies/opslag op eindapparatuur).[1]

Een breed scala aan secundaire bronnen is geanalyseerd:

1. **Officiële Microsoft-documentatie:** Dit omvat publieke informatie uit het Microsoft Trust Center [30], de contractuele Data Processing Addendums (DPA's) of Bijlagen Bescherming Persoonsgegevens (BBP) [43], de Productvoorwaarden [37], specifieke documentatie over de EU Data Boundary [30], informatie over Required Service Data en Diagnostic Data [33], en privacy-gerelateerde documentatie voor Copilot.[20]
2. **Publicaties van Nederlandse toezichthouders en overheidsinstanties:** Rapporten, adviezen, DPIA's en correspondentie van de Autoriteit Persoonsgegevens (AP) [1] en SLM Rijk [5] zijn grondig bestudeerd. Ook relevante rapporten van de Algemene Rekenkamer [3] en de Autoriteit Consument & Markt (ACM) [4] zijn meegenomen voor contextuele factoren zoals afhankelijkheid en marktconcentratie.
3. **Jurisprudentie:** De analyse omvat de implicaties van het Schrems II-arrest van het Hof van Justitie van de Europese Unie [9] en relevante Nederlandse rechtspraak, zoals een uitspraak over tracking cookies ter illustratie van handhaving op het gebied van toestemming.[36]
4. **Academische literatuur en expertanalyses:** Hoewel specifiek op M365 en de Nederlandse AVG-context gerichte peer-reviewed artikelen of proefschriften schaars bleken [71], is gebruik gemaakt van rapporten van juridische experts, consultancyfirma's met expertise in dit domein (zoals Privacy Company, die DPIA's uitvoerde voor SLM Rijk) [22], en diepgaande analyses uit betrouwbare (vak)publicaties en blogs.[6]

De selectie van bronnen is gebaseerd op criteria van autoriteit (officieel document, toezichthouder, erkende expert, peer-review), relevantie voor de onderzoeksvraag en de Nederlandse context, en actualiteit (gepubliceerd of relevant tot 18 april 2025). De verwerking van de bronnen omvatte een kritische evaluatie van de inhoud, het vergelijken van verschillende perspectieven (bijvoorbeeld de claims van Microsoft versus de bevindingen van toezichthouders), en het synthetiseren van de bevindingen tot een coherent en onderbouwd beeld. Bronvermelding volgt de Harvard-stijl.

De analysemethode combineert juridische interpretatie (toepassing van AVG-normen op M365), technische analyse (beoordeling van beschreven maatregelen en geïdentificeerde risico's) en beleidsanalyse (evaluatie van Nederlands beleid en de interactie tussen overheid en Microsoft). Door deze verschillende invalshoeken te integreren, wordt gestreefd naar een holistische beoordeling van de AVG-compliance status van M365 in Nederland.

# 3. Resultaten

## 3.1 De AVG en Clouddiensten: Kernprincipes in de Nederlandse Context

De Algemene Verordening Gegevensbescherming (AVG), die sinds mei 2018 van kracht is, vormt het centrale juridische kader voor de bescherming van persoonsgegevens binnen de

Europese Unie. De verordening legt een reeks kernbeginselen vast waaraan elke verwerking van persoonsgegevens moet voldoen. Deze beginselen omvatten rechtmatigheid, behoorlijkheid en transparantie; doelbinding (gegevens mogen alleen worden verzameld voor specifieke, vooraf bepaalde doelen); dataminimalisatie (niet meer gegevens verzamelen dan nodig); juistheid (gegevens moeten accuraat zijn); opslagbeperking (gegevens niet langer bewaren dan noodzakelijk); en integriteit en vertrouwelijkheid (gegevens moeten adequaat beveiligd worden).[1] Deze principes vormen het toetsingskader voor de beoordeling van clouddiensten zoals M365.

De AVG is breed van toepassing en geldt voor elke geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede voor de verwerking van persoonsgegevens die in een bestand zijn opgenomen of daarvoor bestemd zijn.[1] Dit omvat vrijwel alle activiteiten die met persoonsgegevens kunnen worden uitgevoerd, van verzamelen en opslaan tot analyseren en vernietigen.[1] De verordening is van toepassing op organisaties die in de EU gevestigd zijn, maar ook op organisaties buiten de EU die goederen of diensten aanbieden aan personen in de EU of hun gedrag monitoren binnen de EU.[2] Clouddienstverleners zoals Microsoft, die diensten aanbieden aan Nederlandse organisaties en daarbij persoonsgegevens van EU-burgers verwerken, vallen dus onmiskenbaar onder de reikwijdte van de AVG.[4]

Een cruciaal concept binnen de AVG is het onderscheid tussen de 'verwerkingsverantwoordelijke' en de 'verwerker'.[10] De verwerkingsverantwoordelijke is de entiteit die het doel van en de middelen voor de gegevensverwerking bepaalt (bijvoorbeeld de Nederlandse organisatie die M365 gebruikt voor haar bedrijfsvoering of dienstverlening). De verwerker is de entiteit die persoonsgegevens verwerkt ten behoeve van de verwerkingsverantwoordelijke, op basis van diens instructies (bijvoorbeeld Microsoft voor de kernfunctionaliteiten van M365).[10] Dit onderscheid is van fundamenteel belang, omdat de AVG verschillende verantwoordelijkheden en verplichtingen toekent aan beide rollen. Hoewel Microsoft zichzelf contractueel primair positioneert als verwerker voor de meeste M365-diensten [37], hebben Nederlandse DPIA's situaties geïdentificeerd waarin Microsoft feitelijk ook als (gezamenlijk) verwerkingsverantwoordelijke optreedt, bijvoorbeeld voor bepaalde diagnostische gegevens of mobiele applicaties.[22]

Voor het gebruik van clouddiensten stelt de AVG specifieke eisen. Organisaties (verwerkingsverantwoordelijken) moeten een verwerkersovereenkomst (in Microsoft-terminologie vaak onderdeel van de Data Processing Addendum of DPA/BBP) afsluiten met hun cloudprovider (verwerker).[10] Deze overeenkomst moet onder meer afspraken bevatten over het onderwerp, de duur, de aard en het doel van de verwerking, het soort persoonsgegevens, de categorieën betrokkenen, en de rechten en plichten van de verantwoordelijke, alsmede de verplichtingen van de verwerker (zoals het treffen van passende beveiligingsmaatregelen, het bijstaan van de verantwoordelijke, en het omgaan

met datalekken en subverwerkers).[85] Bij verwerkingen die waarschijnlijk een hoog risico inhouden voor de rechten en vrijheden van natuurlijke personen, is de verwerkingsverantwoordelijke verplicht een DPIA uit te voeren.[1] Zowel de verantwoordelijke als de verwerker moeten passende technische en organisatorische maatregelen (TOMs) implementeren om een op het risico afgestemd beveiligingsniveau te waarborgen.[2] Tot slot gelden er strenge regels voor de doorgifte van persoonsgegevens naar landen buiten de Europese Economische Ruimte (EER), waarover later meer.[6]

n de Nederlandse context houdt de Autoriteit Persoonsgegevens (AP) toezicht op de naleving van de AVG.[1] De AP heeft zich meermaals kritisch uitgelaten over het gebruik van clouddiensten, met name door de overheid. In reactie op het "Rijksbreed cloudbeleid 2022" benadrukte de AP dat de privacyrisico's, onafhankelijk van de vraag of het een publieke, private of hybride cloud betreft, leidend moeten zijn bij de beslissing om een clouddienst in te zetten.[8] De AP wees specifiek op de risico's van gegevensdoorgifte naar landen buiten de EER en de noodzaak van een controleerbare implementatie en naleving van het beleid.[28] SLM Rijk speelt namens de Rijksoverheid een centrale rol in de onderhandelingen met Microsoft en het (laten) uitvoeren van DPIA's naar Microsoft-producten.[3]

Deze Nederlandse context laat zien dat er een kritische houding wordt aangenomen ten opzichte van de claims en contracten van grote cloudleveranciers. De AVG legt de primaire verantwoordelijkheid voor compliance bij de gebruiker van de dienst (de verwerkingsverantwoordelijke).[10] Nederlandse (overheids)organisaties, vaak ondersteund door SLM Rijk of sectorale organisaties zoals SIVON in het onderwijs, varen niet blind op de standaard DPA's van Microsoft, maar voeren eigen risicoanalyses (DPIA's en DTIA's) uit om de feitelijke gegevensverwerkingen en de daaraan verbonden risico's te beoordelen.[6] De kritiek van de AP op het Rijkscloudbeleid onderstreept de noodzaak om fundamentele privacyrisico's, met name rondom gegevensoverdracht, adequaat te adresseren en niet te laten ondersneeuwen door de operationele voordelen van de cloud.[8] Deze proactieve en kritische benadering impliceert dat formele juridische claims en technische specificaties van leveranciers worden getoetst aan de realiteit van gegevensverwerking en de potentiële impact op de grondrechten van burgers.

## 3.2 Microsoft's Compliance Framework: Documentatie, Contracten (DPA) en Maatregelen

Microsoft heeft een omvangrijk raamwerk opgetuigd om aan te tonen dat zijn clouddiensten, waaronder M365, voldoen aan de AVG en andere privacyregelgeving. Dit raamwerk bestaat uit publieke documentatie, contractuele afspraken en een reeks technische en organisatorische maatregelen.

Het **Microsoft Trust Center** fungeert als het centrale, publiek toegankelijke portaal waar Microsoft informatie deelt over beveiliging, privacy en compliance van zijn diensten.[37] Hier

vinden klanten en geïnteresseerden informatie over hoe Microsoft omgaat met de AVG/GDPR [2], waar klantgegevens worden opgeslagen (datalocatie) [30], het EU Data Boundary-initiatief [30], het gebruik van subverwerkers [37] en de procedures voor het reageren op verzoeken van overheden om toegang tot gegevens.[37]

De contractuele basis voor de gegevensverwerking wordt gevormd door de **Data Processing Addendum (DPA)**, in het Nederlands vaak aangeduid als de Bijlage Bescherming Persoonsgegevens (BBP).[43] Deze DPA is een addendum bij de algemene productvoorwaarden en legt de verplichtingen van Microsoft als verwerker vast conform Artikel 28 van de AVG.[43] Microsoft heeft de DPA in de loop der tijd aangepast, mede naar aanleiding van kritiek van Europese toezichthouders. De DPA-versie van begin 2023 bevatte bijvoorbeeld wijzigingen om klanten beter te ondersteunen bij hun verantwoordingsplicht (accountability), verduidelijkingen rondom het telecommunicatiegeheim in Duitsland, de contractuele verankering van de EU Data Boundary, explicietere verwijzingen naar geïmplementeerde technische en organisatorische maatregelen (TOMs) uit de Standard Contractual Clauses (SCCs), en een uitbreiding van de reikwijdte naar alle klanten met een bestaande product- en serviceovereenkomst.[47]

In zijn documentatie en contracten doet Microsoft een aantal belangrijke **claims en toezeggingen**. Centraal staat de claim dat de klant eigenaar is van en controle heeft over zijn data.[37] Microsoft stelt dat het klantgegevens alleen verwerkt op basis van de overeenkomst met de klant en voor het leveren van de gekozen diensten, en niet zonder toestemming.[37] Het bedrijf claimt klantgegevens niet te delen met door adverteerders ondersteunde diensten of te gebruiken voor eigen doeleinden zoals marketingonderzoek of advertenties.[37] Verder belooft Microsoft overheidsverzoeken om data juridisch te toetsen en waar mogelijk aan te vechten, en de klant te informeren tenzij dit wettelijk verboden is.[37] Als extra waarborg biedt Microsoft commerciële en publieke sector klanten financiële compensatie indien hun data wordt vrijgegeven aan een overheid in strijd met de AVG.[37]

Ter ondersteuning van deze claims verwijst Microsoft naar een breed scala aan **Technische en Organisatorische Maatregelen (TOMs)**. Dit omvat maatregelen zoals encryptie van data, zowel 'in transit' (onderweg) als 'at rest' (in opslag) [11], geavanceerde toegangscontrolemechanismen [11], en het voldoen aan diverse internationale beveiligings- en privacystandaarden en -certificeringen, zoals ISO/IEC 27001 (informatiebeveiliging), ISO/IEC 27018 (privacy in public clouds), ISO/IEC 27701 (privacy information management) en SOC-rapportages.[11] Onafhankelijke auditrapporten hierover zijn beschikbaar voor klanten via het Trust Center of de Service Trust Portal.[37] Daarnaast biedt Microsoft tools zoals Microsoft Purview, de Compliance Score en audit logs om organisaties te helpen bij het beheren van hun compliance en het verkrijgen van inzicht in gegevensverwerkingen.[14]

Ondanks deze aanzienlijke investeringen in een gelaagd compliance-raamwerk, blijkt uit de aanhoudende kritiek en de bevindingen van DPIA's dat de effectiviteit en volledigheid ervan voortdurend ter discussie staan. Microsoft presenteert een uitgebreid pakket aan documentatie, contractuele garanties en technologische hulpmiddelen.[37] Updates, zoals de DPA van 2023, zijn vaak een directe reactie op de zorgen die door Europese en nationale toezichthouders worden geuit.[47] Desalniettemin blijven toezichthouders in Duitsland [47], de Europese privacytoezichthouder EDPS [18], de Nederlandse AP [8] en SLM Rijk [15] kritisch over fundamentele aspecten, zoals de daadwerkelijke transparantie van gegevensverwerkingen, de risico's van gegevensoverdracht naar de VS (zelfs met de EU Data Boundary), en de mate waarin Microsoft feitelijk controle uitoefent over bepaalde data. Dit suggereert een dynamiek waarbij Microsoft reageert op externe druk, maar de onderliggende problemen – zoals de impact van Amerikaanse wetgeving of onduidelijkheid over de verwerking van bijvoorbeeld diagnostische data – complexer zijn en niet altijd volledig worden opgelost met contractuele aanpassingen of nieuwe technische features alleen. De voortdurende noodzaak voor Nederlandse organisaties om zelfstandig DPIA's en DTIA's uit te voeren en waar nodig aanvullende maatregelen te treffen [6], onderstreept dat het raamwerk van Microsoft op zichzelf door velen niet als voldoende wordt beschouwd om AVG-compliance te garanderen.

## 3.3 De EU Data Boundary: Status, Scope en Beperkingen per april 2025

Als antwoord op de groeiende zorgen in Europa over datalocatie en internationale gegevensoverdrachten, met name na het Schrems II-arrest, heeft Microsoft het EU Data Boundary-initiatief gelanceerd. Het doel van dit initiatief is om commerciële en publieke sector klanten in de Europese Unie (EU) en de Europese Vrijhandelsassociatie (EFTA) de garantie te bieden dat hun belangrijkste gegevens binnen deze geografische grenzen worden opgeslagen en verwerkt.[30] Microsoft positioneert dit als een "industry-leading solution" die Europese transparantie, privacybescherming en klantcontrole ondersteunt.[31]

De EU Data Boundary omvat volgens Microsoft's toezeggingen de opslag en verwerking van:

1. **Klantgegevens (Customer Data):** Alle data die door of namens de klant aan Microsoft wordt verstrekt via het gebruik van de onlinedienst, zoals tekst-, geluids-, video- of afbeeldingsbestanden en software.[51] Dit was de focus van Fase 1, gestart op 1 januari 2023.[53]
2. **Gepseudonimiseerde persoonsgegevens (Pseudonymized Personal Data):** Data gegenereerd tijdens de werking van de dienst, zoals bepaalde systeemgegenereerde logs, waarbij identificatoren zijn vervangen door pseudoniemen.[31] Dit werd toegevoegd in Fase 2, gelanceerd in januari 2024.[31]
3. **Professional Services Data:** Gegevens uit technische supportinteracties, zoals door de klant verstrekte logs of door Microsoft gegenereerde case notes, voor kernclouddiensten zoals M365, Power Platform en Dynamics 365.[31] Dit was het sluitstuk in Fase 3, waarvan de voltooiing werd aangekondigd in februari 2025.[31]

De boundary geldt voor de kernclouddiensten: Microsoft 365, Dynamics 365, Power Platform en de meeste Azure-diensten.[31] Klanten binnen de EU/EFTA vallen onder deze toezegging. Gedetailleerde documentatie over de scope, data flows en eventuele uitzonderingen is beschikbaar via het Microsoft Trust Center en specifieke leerpaden.[30] Voor bepaalde (met name Azure) diensten moeten klanten mogelijk specifieke configuraties kiezen (bijvoorbeeld Azure-regio's binnen de EU/EFTA) om volledig binnen de boundary te blijven.[51]

Ondanks de voltooiing van de implementatie, erkent Microsoft zelf dat er **beperkingen en uitzonderingen** zijn op de EU Data Boundary:

- **Noodzakelijke transfers buiten de EUDB:** Microsoft stelt dat in beperkte omstandigheden data buiten de EUDB getransfereerd kan worden. Dit betreft met name data die nodig is voor wereldwijde beveiligingsoperaties (zoals het detecteren van en reageren op cyberdreigingen die grensoverschrijdend zijn) en voor bepaalde service operations om de stabiliteit en functionaliteit van de diensten te waarborgen.[31] Ook bepaalde globale features (zoals Content Delivery Networks - CDN's) of preview-diensten kunnen data buiten de boundary verwerken of opslaan.[51] Microsoft claimt dat dergelijke transfers plaatsvinden met "robuuste beschermingsmaatregelen".[31]
- **Remote Access:** Microsoft-personeel van buiten de EUDB kan op afstand toegang krijgen tot data die binnen de boundary is opgeslagen, bijvoorbeeld voor technische ondersteuning of troubleshooting.[54] Hoewel de data fysiek binnen de EUDB blijft, wordt deze toegang onder Europese privacywetgeving beschouwd als een doorgifte.[89] Microsoft stelt dat deze toegang strikt gecontroleerd wordt via maatregelen zoals Just-in-Time (JIT) access, Role-Based Access Control (RBAC), het gebruik van Secure Admin Workstations (SAWs), en de mogelijkheid voor klanten om Customer Lockbox te activeren voor extra controle.[89]
- **Definities en Scope:** De definitie van 'Customer Data' sluit expliciet Professional Services Data uit (tenzij specifiek toegevoegd in Fase 3) en ook configuratiegegevens van resources.[51] De boundary geldt primair voor de 'major' of 'core' enterprise online services; niet noodzakelijkerwijs voor alle Microsoft-producten of -diensten, en voor sommige Azure-diensten kan extra configuratie door de klant nodig zijn.[31]

De effectiviteit van de EU Data Boundary wordt door critici, waaronder Europese cloudproviders en analisten, in twijfel getrokken.[78] Het belangrijkste kritiekpunt is dat de boundary zich richt op **data residency** (de fysieke locatie van dataopslag en -verwerking), maar geen **data soevereiniteit** (volledige juridische controle, onafhankelijk van buitenlandse wetgeving) garandeert.[78] Omdat Microsoft een Amerikaans bedrijf blijft, is het onderhevig aan Amerikaanse wetgeving zoals de CLOUD Act en FISA, die potentieel toegang tot gegevens kunnen afdwingen, ongeacht waar deze wereldwijd zijn opgeslagen.[7] De door

Microsoft erkende uitzonderingen voor noodzakelijke transfers worden eveneens gezien als een potentieel risico dat de waterdichtheid van de boundary ondermijnt.[31]

De EU Data Boundary is onmiskenbaar een significante technische en logistieke inspanning van Microsoft, direct ingegeven door Europese regelgeving en zorgen.[30] Het initiatief focust op het fysiek binnen de EU/EFTA houden van specifieke categorieën data [51] en vergroot de transparantie hierover. Echter, het lost het fundamentele juridische conflict dat aan de basis ligt van de Schrems II-uitspraak – namelijk de potentiële toegang door Amerikaanse autoriteiten tot data onder beheer van Amerikaanse bedrijven – niet volledig op. De erkende uitzonderingen [31] en de kritiek op het onderscheid tussen residency en soevereiniteit [7] maken duidelijk dat de EU Data Boundary de hoeveelheid data die de EU verlaat weliswaar reduceert, maar geen absolute garantie biedt tegen alle vormen van internationale gegevensoverdracht of toegang van buitenaf. De effectiviteit ervan als oplossing voor *alle* Schrems II-gerelateerde problemen is daarmee beperkt.

## 3.4 Nederlandse Toetsing: Bevindingen AP en SLM Rijk DPIA's

De Nederlandse overheid en toezichthouders hebben het gebruik van Microsoft clouddiensten, waaronder M365, aan een kritische blik onderworpen. De Algemene Rekenkamer constateerde in 2025 dat het Rijk beperkt zicht heeft op de gebruikte clouddiensten, onvoldoende strategische risicoafwegingen maakt, en dat de principes van digitale soevereiniteit, continuïteit en gegevensbescherming onvoldoende gewaarborgd zijn in onderzochte public cloud-contracten.[3] De Autoriteit Persoonsgegevens (AP) uitte in 2022 kritiek op het Rijksbreed cloudbeleid, waarbij ze benadrukte dat privacyrisico's, met name rondom gegevensdoorgifte naar landen buiten de EER, leidend moeten zijn en dat het beleid beter gehandhaafd moet worden.[8]

Strategisch Leveranciersmanagement Rijk (SLM Rijk) heeft, vaak in samenwerking met externe experts zoals Privacy Company, een reeks Data Protection Impact Assessments (DPIA's) laten uitvoeren specifiek gericht op Microsoft-diensten.[21] Deze DPIA's hebben niet alleen risico's geïdentificeerd, maar ook geleid tot onderhandelingen met Microsoft en concrete aanpassingen in contracten en technische instellingen.[33]

- **DPIA Office Online & Mobile (Juli 2019):** Deze DPIA identificeerde vijf hoge risico's. Een belangrijk punt was dat Microsoft optrad als verwerkingsverantwoordelijke voor de mobiele Office-apps en de daarbij verzamelde gegevens verwerkte voor eigen doeleinden, inclusief het delen van data met een Amerikaans marketingbedrijf.[33] Ook was er onduidelijkheid over de verzameling en het gebruik van diagnostische gegevens.[33] Mitigatie vereiste aanpassingen in het overheidsbeleid (bv. werknemers waarschuwen de mobiele apps niet te gebruiken) en technische/contractuele aanpassingen door Microsoft.[33]
- **DPIA Office 365 ProPlus (na onderhandelingen, Juni/Juli 2019):** Na onderhandelingen en toezeggingen van Microsoft concludeerde een geüpdatete DPIA dat er geen

bekende hoge risico's meer waren voor het gebruik van Office 365 ProPlus door de Nederlandse overheid, *mits* organisaties specifieke aanbevelingen opvolgden, zoals het instellen van het telemetrieniveau op 'Neither' (geen).[33]

- **DPIA Teams/OneDrive/SharePoint (SIVON/SLBdiensten, April 2022):** Hoewel primair gericht op de onderwijssector, reflecteren de bevindingen bredere zorgen. Deze DPIA identificeerde een hoog risico gerelateerd aan gegevensoverdracht naar de VS in het licht van Schrems II, met name omdat Microsoft de encryptiesleutels beheert en geplande Teams-vergaderingen niet end-to-end versleuteld waren.[15] Dit vormde een significant risico bij de verwerking van bijzondere persoonsgegevens (bv. in gesprekken over leerlingenzorg). Aanbevolen werd om Double Key Encryption (DKE) te gebruiken voor gevoelige data in OneDrive/SharePoint en end-to-end encryptie (E2EE) te activeren voor één-op-één Teams-gesprekken.[15] Ook werd gewezen op een gebrek aan transparantie over de zogenaamde 'Required Service Data'.[35]
- **DPIA Microsoft 365 Copilot (SLM Rijk, December 2024):** De meest recente grote DPIA richtte zich op de generatieve AI-tool Copilot binnen M365. Deze identificeerde vier hoge en zes lage gegevensbeschermingsrisico's.[22] De hoge risico's betroffen [22]:
    1. **Inzagerecht Diagnostische Data:** Onmogelijkheid voor betrokkenen (via de overheidsorganisatie) om hun recht op inzage effectief uit te oefenen met betrekking tot diagnostische gegevens die Copilot verzamelt, vanwege gebrek aan transparantie en toegankelijkheid van de DSAR-output (Data Subject Access Request).
    2. **Onjuiste Persoonsgegevens in Output:** Het risico dat Copilot onjuiste of verouderde persoonsgegevens genereert, wat kan leiden tot significante nadelen voor betrokkenen. Dit hangt samen met een gebrek aan transparantie over de werking van Microsoft's Responsible AI (RAI) filters, de kwaliteit van de output (met name in het Nederlands), en het potentiële gebruik van verouderde trainingsdata of broninformatie uit de M365-omgeving van de gebruiker.
    3. **Controleverlies door Gebrek aan Transparantie over Required Service Data (RSD):** Onvoldoende duidelijkheid vanuit Microsoft over welke specifieke RSD (zowel inhoud als metadata) wordt verzameld bij het gebruik van Copilot, voor welke doeleinden, en hoe deze zich verhouden tot de instructies van de verwerkingsverantwoordelijke.
    4. **Heridentificatierisico door Onbekende Bewaartermijnen RSD:** Het risico dat gepseudonimiseerde RSD herleidbaar wordt naar individuen doordat Microsoft geen duidelijke, specifieke bewaartermijnen publiceert voor de verschillende soorten RSD.

Op basis van deze hoge risico's concludeerde SLM Rijk in december 2024 dat M365 Copilot **nog niet AVG-compliant te gebruiken** was door Nederlandse overheidsorganisaties.[23] Dit leidde ertoe dat bijvoorbeeld de gemeente Amsterdam een geplande pilot met Copilot

uitstelde [24] en dat SURF het gebruik door Nederlandse onderwijs- en onderzoeksinstellingen vooralsnog afraadde.[24]

Naar aanleiding van de Copilot DPIA zijn SLM Rijk en Microsoft opnieuw in gesprek gegaan. Microsoft heeft een aantal **toezeggingen** gedaan met als deadline **4 april 2025** om de belangrijkste zorgen te adresseren [21]:

- Implementatie van een beleid om diagnostische data maximaal 18 maanden te bewaren (met uitzonderingen).
- Samenwerken met SLM Rijk om het DSAR-proces en de output te verbeteren.
- Meer transparantie bieden over de categorieën, doeleinden en bewaartermijnen van RSD gerelateerd aan Copilot.
- In gesprek gaan over een industriestandaard voor Responsible AI (RAI), opties bieden voor impact assessments door data controllers, en meer inzicht geven in privacy binnen Microsoft's RAI-praktijken en de accuratesse van persoonsgegevens in Copilot-output.

**Status per 18 april 2025:** Hoewel Microsoft in april 2025 diverse updates heeft uitgebracht (o.a. security patches, wijzigingen in partnerprogramma's, API's, prijsstelling, en nieuwe Security Copilot agents) [50], is er op basis van de beschikbare informatie **geen publieke bevestiging** gevonden dat de specifieke toezeggingen aan SLM Rijk met betrekking tot de Copilot DPIA-risico's volledig zijn geïmplementeerd én door SLM Rijk als voldoende zijn beoordeeld en geaccepteerd. De dialoog was gepland om door te lopen tot de deadline van 4 april 2025.[21] De onzekerheid over de status van deze toezeggingen is een belangrijk element in de beoordeling van de AVG-compliance van M365 (met Copilot) per medio april 2025.

De onderstaande tabel vat enkele kernbevindingen uit de Nederlandse DPIA's samen.

**Tabel 1: Samenvatting Hoge Risico's geïdentificeerd in SLM Rijk DPIA's voor Microsoft 365 (Selectie)**

| DPIA Focus | Publicatiedatum | Kernbevinding (Hoog Risico) | Status/Mitigatie (per apr 2025) |
|---|---|---|---|
| Office Online/Mobile | Juli 2019 | Microsoft als controller mobiele apps; onduidelijkheid diagnostiek | Deels gemitigeerd door latere MS aanpassingen & beleid [33], maar controller-rol blijft aandachtspunt. |
| Teams/OneDrive/SP (SIVON) | April 2022 | Data transfer risico (Schrems II); gebrek | EUDB geïmplementeerd [31], maar transferrisico |

| | | | |
|---|---|---|---|
| | | E2EE geplande meetings | blijft discussiepunt [78]; E2EE status onbekend; DKE/beleid aangeraden.[15] |
| M365 Copilot | Dec 2024 | Inzagerecht diagnostische data | MS toezegging voor verbetering DSAR per 4 apr 2025 [21]; status implementatie/acceptatie onbevestigd. |
| M365 Copilot | Dec 2024 | Onjuiste persoonsgegevens in output (RAI filter transparantie) | MS toezegging voor discussie RAI/inzichten per 4 apr 2025 [21]; status implementatie/acceptatie onbevestigd. |
| M365 Copilot | Dec 2024 | Transparantie Required Service Data (RSD) | MS toezegging voor meer transparantie per 4 apr 2025 [21]; status implementatie/acceptatie onbevestigd. |
| M365 Copilot | Dec 2024 | Heridentificatie risico (bewaartermijnen RSD) | MS toezegging max 18 mnd bewaartermijn diagnostiek per 4 apr 2025 [21]; status implementatie/acceptatie onbevestigd. |

*Bron: Samengesteld door auteur op basis van.[15]*

De interactie tussen de Nederlandse overheid (via SLM Rijk) en Microsoft illustreert een patroon van voortdurende dialoog en aanpassing. DPIA's identificeren risico's, wat leidt tot onderhandelingen en toezeggingen van Microsoft, die soms resulteren in acceptabele mitigaties (zoals bij Office ProPlus in 2019 [33]). Echter, de introductie van nieuwe technologieën zoals Copilot brengt nieuwe, significante risico's met zich mee die opnieuw een cyclus van onderzoek, onderhandeling en (nog onbevestigde) toezeggingen noodzakelijk maken.[21] Dit patroon suggereert dat een definitieve, stabiele "AVG-proof" status voor het continu evoluerende M365-platform moeilijk te bereiken is, mede door de combinatie van snelle technologische veranderingen en hardnekkige fundamentele juridische knelpunten, zoals de problematiek rond internationale gegevensoverdracht.

## 3.5 Internationale Gegevensoverdracht post-Schrems II: Risico's en Maatregelen

De uitspraak van het Hof van Justitie van de Europese Unie (HvJEU) in de zaak Data Protection Commissioner - Facebook Ireland Ltd en Maximillian Schrems (Schrems II) op 16 juli 2020 [9] heeft het landschap voor internationale gegevensoverdrachten vanuit de EU drastisch veranderd. Het Hof invalideerde het EU-VS Privacy Shield Framework als geldig doorgiftemechanisme, primair vanwege zorgen over de vergaande toegangsmogelijkheden van Amerikaanse inlichtingen- en veiligheidsdiensten tot persoonsgegevens van EU-burgers (onder wetgeving zoals FISA Section 702 en Executive Order 12333) en het gebrek aan effectieve rechtsbescherming voor die burgers tegen dergelijke surveillance.[18]

Tegelijkertijd bevestigde het Hof de principiële geldigheid van Standard Contractual Clauses (SCCs) als doorgifte-instrument onder Artikel 46 AVG. Echter, het Hof benadrukte dat het gebruik van SCCs geen papieren exercitie mag zijn. De gegevensexporteur (de organisatie in de EU die data doorgeeft) en de gegevensimporteur (de organisatie buiten de EER die data ontvangt) moeten, voorafgaand aan de doorgifte, per geval beoordelen of de wetgeving en praktijken in het derde land van bestemming een beschermingsniveau bieden dat wezenlijk gelijkwaardig is aan dat binnen de EU.[9] Indien dit niet het geval is – zoals het Hof oordeelde voor de VS – moeten er aanvullende maatregelen (supplementary measures) worden getroffen om eventuele tekortkomingen in de bescherming te compenseren.[6] Deze beoordeling wordt vaak een Transfer Impact Assessment (TIA) of Data Transfer Impact Assessment (DTIA) genoemd.[6]

De Schrems II-uitspraak heeft directe en significante gevolgen voor het gebruik van M365 door Nederlandse organisaties. Microsoft is een Amerikaans bedrijf en valt daarmee onder de Amerikaanse wetgeving die centraal stond in de zorgen van het HvJEU.[7] Bovendien kan de Amerikaanse CLOUD Act Amerikaanse autoriteiten onder bepaalde omstandigheden verplichten om toegang te verlenen tot data die door Amerikaanse bedrijven wordt beheerd, zelfs als die data buiten de VS is opgeslagen.[5] Dit creëert een fundamenteel juridisch spanningsveld met de eisen van de AVG zoals geïnterpreteerd in Schrems II.[6]
Microsoft heeft diverse stappen ondernomen in reactie op Schrems II:

- Het bedrijf stopte met het vertrouwen op het Privacy Shield en baseert doorgiftes nu primair op de **nieuwe SCCs** die door de Europese Commissie in juni 2021 zijn aangenomen. Microsoft implementeerde deze nieuwe SCCs in september 2021.[62]
- Microsoft publiceerde **documentatie** en whitepapers om klanten te ondersteunen bij het uitvoeren van hun TIA's, waarin het zijn interpretatie van de Amerikaanse wetgeving en de getroffen maatregelen uiteenzet.[9]
- In de DPA is een **"Additional Safeguards Addendum"** opgenomen, waarin Microsoft contractueel toezegt overheidsverzoeken juridisch aan te vechten, transparantie te bieden (tenzij wettelijk verboden) en financiële compensatie te bieden bij

onrechtmatige openbaarmaking.[37]

- Het **EU Data Boundary**-initiatief (zie sectie 3.3) is ontwikkeld en geïmplementeerd, met als doel de hoeveelheid data die de EU/EFTA verlaat te minimaliseren.[30]

Ondanks deze maatregelen concluderen Nederlandse DPIA's die een DTIA bevatten (uitgevoerd door of in opdracht van SLM Rijk en SIVON) consistent dat er een **hoog restrisico** blijft bestaan met betrekking tot mogelijke toegang tot persoonsgegevens door Amerikaanse inlichtingen- en opsporingsdiensten.[15] De redenering is dat noch de SCCs, noch de door Microsoft getroffen contractuele en organisatorische maatregelen, noch de EU Data Boundary de juridische mogelijkheid van toegang onder Amerikaanse wetgeving volledig kunnen wegnemen of neutraliseren.[7] De EU Data Boundary wordt weliswaar als een positieve stap gezien die de *kans* op of *omvang* van doorgifte reduceert, maar het lost het fundamentele juridische conflict niet op.[35]

Als gevolg hiervan adviseren deze Nederlandse DPIA's **aanvullende maatregelen** die door de *gebruikersorganisatie zelf* moeten worden geïmplementeerd, met name voor de verwerking van bijzondere of zeer gevoelige persoonsgegevens:

- **Encryptie met zelfbeheerde sleutels:** Technologieën zoals Bring Your Own Key (BYOK), Hold Your Own Key (HYOK) of Double Key Encryption (DKE) worden aanbevolen.[15] Hierbij houdt de organisatie zelf (een deel van) de encryptiesleutel(s) in beheer, waardoor Microsoft (en daarmee potentieel Amerikaanse autoriteiten) geen toegang heeft tot de leesbare data. Een belangrijk nadeel is echter dat deze vormen van encryptie de functionaliteit van M365 aanzienlijk kunnen beperken, bijvoorbeeld bij online samenwerken, zoeken in documenten of het gebruik van bepaalde webversies van Office-applicaties.[15] Het wordt daarom vaak alleen aangeraden voor specifieke, zeer gevoelige datasets.
- **Pseudonimisering:** Waar mogelijk, zoals bij admin-accountgegevens, kan pseudonimisering helpen het risico te verkleinen.[76]
- **Beleid en Training:** Organisaties moeten duidelijk beleid opstellen en gebruikers trainen om geen (bijzonder) gevoelige persoonsgegevens onversleuteld op te slaan in M365 of te delen via kanalen die niet adequaat beveiligd zijn (zoals geplande Teams-vergaderingen zonder E2EE).[15]

Hoewel er inmiddels een opvolger van het Privacy Shield is, het EU-US Data Privacy Framework (DPF), is de juridische houdbaarheid hiervan eveneens onzeker en wordt het al aangevochten.[83] De onderliggende problematiek van Amerikaanse surveillancewetgeving en het gebrek aan effectieve rechtsbescherming voor EU-burgers blijft een punt van zorg.
De Schrems II-uitspraak heeft dus een fundamentele en blijvende impact. Het maakt duidelijk dat technische oplossingen zoals de EU Data Boundary en contractuele clausules zoals SCCs en DPA-addenda, hoewel nuttig, door Nederlandse instanties als onvoldoende worden beschouwd om het kernrisico van Amerikaanse overheidsinmenging volledig te

mitigeren.[7] Compliance met de AVG bij het gebruik van M365 in de post-Schrems II-wereld is hierdoor niet langer een gegeven dat inherent is aan het platform, maar wordt afhankelijk van actieve, risico-gebaseerde beslissingen en de implementatie van aanvullende, vaak complexe en potentieel beperkende, maatregelen door de Nederlandse gebruikersorganisatie zelf.[6] Dit legt een aanzienlijke last bij de verwerkingsverantwoordelijke en creëert een situatie van voortdurende juridische onzekerheid.

## 3.6 Specifieke Verwerkingen onder de Loep: Telemetrie, Required Service Data, Subverwerkers, Copilot

Naast de overkoepelende problematiek van internationale gegevensoverdracht, roept ook de verwerking van specifieke datastromen *binnen* het M365-ecosysteem vragen op in het kader van de AVG. Met name de verwerking van diagnostische gegevens, de introductie van AI-functionaliteiten en het gebruik van subverwerkers vereisen nadere beschouwing.

**Telemetrie / Diagnostische Data:** Microsoft verzamelt gegevens over het apparaat, de geïnstalleerde software, het gebruik en de prestaties van M365-applicaties.[32] Een vroeg onderzoek van de AP naar Windows 10 (2017) uitte al zorgen over een gebrek aan transparantie, doelbinding en een geldige wettelijke grondslag voor de verzameling van (uitgebreide) telemetriegegevens.[32] Latere DPIA's, specifiek gericht op Office 365 ProPlus en uitgevoerd na onderhandelingen met SLM Rijk, concludeerden dat er geen hoge risico's meer waren *indien* het telemetrieniveau door de organisatie centraal werd ingesteld op 'Neither' (geen/minimaal).[33] Desondanks blijven er zorgen bestaan over de transparantie en controle, met name met betrekking tot een categorie data die Microsoft 'Required Service Data' noemt.

**Required Service Data (RSD):** Dit is data die Microsoft stelt nodig te hebben om zogenaamde 'connected experiences' (cloud-ondersteunde functies zoals spellingcontrole, vertaling, ontwerpideeën in PowerPoint) en essentiële services (zoals licentiebeheer) te laten functioneren.[56] Volgens Microsoft omvat RSD operationele data, configuratie-informatie en soms zelfs inhoudelijke data (zoals de tekst of afbeeldingen op een slide die naar de PowerPoint Designer-service wordt gestuurd).[56] Cruciaal is Microsoft's stelling dat RSD losstaat van de instellingen voor diagnostische data (telemetrie) en dat de verzameling ervan niet kan worden uitgeschakeld via die instellingen.[56] Juist dit gebrek aan controle en transparantie is een bron van zorg in Nederlandse DPIA's (voor Teams/OneDrive/SharePoint en met name voor Copilot).[22] Deze DPIA's identificeren een hoog risico omdat het voor organisaties onvoldoende duidelijk is *welke* data precies als RSD wordt verzameld, voor *welke* specifieke (sub)doeleinden, en hoe lang deze data wordt bewaard.[22] Dit leidt tot een verlies van controle voor de verwerkingsverantwoordelijke. Microsoft heeft naar aanleiding van de Copilot DPIA toegezegd hierover meer transparantie te bieden (deadline 4 april 2025) [21], maar de status hiervan is per 18 april 2025 onbekend.

**Subverwerkers:** Microsoft schakelt andere bedrijven (subverwerkers) in om te helpen bij het leveren van zijn diensten.[37] Klanten worden hierover geïnformeerd via een publieke lijst.[37] De DPA van Microsoft legt deze subverwerkers contractueel dezelfde gegevensbeschermingsverplichtingen op als Microsoft zelf heeft ten opzichte van de klant.[37] Echter, het gebruik van subverwerkers, met name als deze buiten de EER gevestigd zijn of daar data verwerken, voegt een extra laag van complexiteit toe aan de analyse van internationale gegevensoverdrachten (DTIA) en vereist dat de verwerkingsverantwoordelijke ook de waarborgen van deze subverwerkers beoordeelt.[6]

**Microsoft 365 Copilot:** De integratie van generatieve AI in M365-applicaties [20] introduceert nieuwe, complexe gegevensverwerkingen. Copilot verwerkt de input van de gebruiker (prompts), haalt relevante data op uit de M365-omgeving van de gebruiker (via Microsoft Graph, zoals e-mails, documenten, chats) [20], interageert met Large Language Models (LLMs) gehost op Azure OpenAI [20], en genereert output. Microsoft claimt hierbij dat de dataverwerking binnen de M365-servicegrens blijft, dat Azure OpenAI-services worden gebruikt (die geen klantinhoud opslaan voor training), en dat bepaalde vormen van monitoring (zoals menselijke review van prompts/output voor misbruikdetectie) zijn uitgeschakeld voor M365 Copilot.[20] Desondanks identificeerde de SLM Rijk DPIA van december 2024 juist op dit vlak hoge risico's.[22] Deze risico's betreffen, zoals eerder genoemd, de transparantie rondom diagnostische data en RSD die specifiek door Copilot worden gegenereerd, het inzagerecht in deze data, de nauwkeurigheid en potentiële bias van de gegenereerde output (mede door onduidelijkheid over de RAI-filters), en de bewaartermijnen van verwerkte data.[22] Een bijkomend risico ontstaat wanneer Copilot wordt geconfigureerd om informatie van het web te halen via Bing; in dat geval kunnen prompts en mogelijk andere data worden gedeeld met Bing, waarbij Microsoft als verwerkingsverantwoordelijke optreedt onder zijn algemene privacybeleid.[22] Mitigatie van deze Copilot-specifieke risico's vereist zowel actie van Microsoft (de toezeggingen met deadline april 2025 [21]) als van de gebruikersorganisatie zelf (zoals het ontwikkelen van een AI-gebruiksbeleid, training van medewerkers, adequaat Identity and Access Management (IAM), en zorgvuldige data governance).[23]

De analyse van deze specifieke verwerkingen legt een dieperliggend probleem bloot. Los van de uitdagingen rond internationale gegevensoverdrachten, vormt de toenemende complexiteit en deels ondoorzichtige aard van gegevensverwerkingen *binnen* het M365-platform zelf een groeiende uitdaging voor AVG-compliance. De introductie van concepten als Required Service Data, die buiten de directe controle van de gebruiker lijken te vallen [35], en de 'black box'-achtige aard van AI-systemen zoals Copilot [22], maken het voor Nederlandse organisaties moeilijk om volledig te voldoen aan de AVG-principes van doelbinding, dataminimalisatie en vooral transparantie. Het gebrek aan volledige transparantie en controle over deze interne verwerkingen ondermijnt de mogelijkheid voor de

verwerkingsverantwoordelijke om zijn verantwoordingsplicht onder de AVG na te komen, zelfs indien alle data fysiek binnen de EU Data Boundary zou blijven.

## 3.7 Kwantitatieve Aspecten en Audits

Naast de juridische en technische aspecten zijn er ook kwantitatieve en economische factoren die de context van AVG-compliance voor M365 in Nederland beïnvloeden.
Een belangrijk aspect is de **marktconcentratie**. Microsoft (met Azure en M365) heeft, samen met Amazon Web Services (AWS), een zeer dominant marktaandeel op de Europese en Nederlandse markt voor cloudinfrastructuur (IaaS) en platformdiensten (PaaS), geschat op elk 35-40%.[4] Deze hoge concentratie leidt tot zorgen bij toezichthouders zoals de ACM en de Algemene Rekenkamer over afhankelijkheid, verminderde concurrentie en het risico op vendor lock-in.[3] Organisaties die eenmaal diep geïntegreerd zijn met het M365-ecosysteem, kunnen het moeilijk vinden om over te stappen naar alternatieve aanbieders.

Dit wordt versterkt door de kostenstructuur voor **data transfer**, met name de zogenaamde **egress fees**. Terwijl het invoeren van data in de cloud (ingress) vaak gratis is, rekenen grote hyperscalers zoals Microsoft, AWS en Google Cloud aanzienlijke kosten voor het uitvoeren van data (egress), bijvoorbeeld bij een migratie naar een andere provider of een on-premise omgeving.[59] Deze egress fees zijn vaak significant hoger dan de tarieven van kleinere (Europese) aanbieders en zijn de afgelopen jaren minder gedaald dan de groothandelsprijzen voor data transit.[59] Hoewel specifieke egress fees voor M365 niet direct in de onderzoeksgegevens zijn gevonden, illustreert de prijsstelling van bijvoorbeeld Google Cloud de orde van grootte: tarieven variëren per regio en volume, maar kunnen oplopen van $0.08 tot $0.12 of meer per Gigabyte voor de eerste 10 Terabyte.[98] Dit kan een aanzienlijke financiële drempel vormen voor organisaties die overwegen over te stappen.

**Tabel 2: Indicatieve Egress Fee Vergelijking (Illustratief, Gebaseerd op Algemene Cloud Markt)**

| Provider Type | Data Volume | Geschatte Egress Fee (per GB) | Bron Indicatie |
|---|---|---|---|
| Grote Hyperscaler (AWS/Azure/GCP) | 1-10 TB | $0.08 - $0.12+ | [59] |
| Grote Hyperscaler (AWS/Azure/GCP) | > 10 TB | $0.05 - $0.085+ | [59] |
| Kleinere/Europese Provider | Variabel | Vaak significant lager / geen | [59] (impl.) |

*Bron: Samengesteld door auteur op basis van.[59] Tarieven zijn indicatief en kunnen variëren.*

Deze tabel, hoewel illustratief, benadrukt een kwantitatieve factor die bijdraagt aan vendor lock-in. De hoge kosten voor data-uitvoer vormen een concrete barrière voor het wisselen

van provider, zoals ook erkend door de ACM.[59] Dit is relevant voor de AVG-discussie, omdat het de strategische opties van organisaties beperkt wanneer zij geconfronteerd worden met compliance-problemen.

Aan de andere kant investeert Microsoft in **audits en certificeringen** om vertrouwen te wekken. Het bedrijf ondergaat regelmatig audits door onafhankelijke derde partijen en beschikt over een breed scala aan certificeringen (zoals ISO 27001, 27018, 27701, SOC 1/2/3).[11] De bijbehorende auditrapporten zijn vaak beschikbaar voor klanten via het Trust Center of de Service Trust Portal.[37] Deze audits bieden een zekere mate van assurance over de implementatie van specifieke controles en processen. Echter, ze dekken niet noodzakelijkerwijs alle juridische risico's die voortvloeien uit de AVG, zoals de impact van buitenlandse wetgeving op gegevenstoegang. Nederlandse DPIA's bevelen soms dan ook aanvullende, specifiek gerichte audits aan, bijvoorbeeld naar de bewaartermijnen van Required Service Data.[22]

De combinatie van hoge marktconcentratie en significante egress fees creëert een economische realiteit die de juridische en technische discussies over AVG-compliance beïnvloedt. De resulterende vendor lock-in [3] kan ertoe leiden dat organisaties zich genoodzaakt zien om binnen het M365-ecosysteem naar oplossingen te zoeken, zelfs als deze suboptimaal of complex zijn (zoals DKE [15]), of om resterende risico's te accepteren, simpelweg omdat overstappen naar een potentieel meer compliant (bijvoorbeeld Europees) alternatief te kostbaar of operationeel ontwrichtend is. Dit economische krachtenveld vormt een belangrijke, vaak onderbelichte, factor die de praktische keuzes en mogelijkheden van Nederlandse organisaties met betrekking tot AVG-compliance mede bepaalt.

# 4. Discussie

De analyse van de AVG-compliance van Microsoft Office 365 in Nederland per 18 april 2025 levert een complex en genuanceerd beeld op. Microsoft heeft ontegenzeggelijk geïnvesteerd in een omvangrijk compliance-framework, maar tegelijkertijd blijven er significante juridische en technische uitdagingen bestaan, met name in de Nederlandse context waar toezichthouders en overheidsinstanties een kritische houding aannemen.

**Kritische Analyse van Microsoft's Maatregelen:**

- **DPA/BBP:** De Data Processing Addendum, inclusief recente updates zoals die van 2023 [47], vormt de contractuele basis en poogt te voldoen aan AVG Artikel 28 en de zorgen na Schrems II (bv. via het Additional Safeguards Addendum [64]). Echter, toezichthouders en experts blijven vraagtekens zetten bij de effectiviteit van deze contractuele waarborgen, met name wat betreft de reële bescherming tegen toegang door Amerikaanse autoriteiten en de mate van transparantie over bepaalde verwerkingen.[7] De DPA wordt gezien als een noodzakelijke, maar niet voldoende voorwaarde voor compliance.
- **EU Data Boundary:** De voltooiing van de EU Data Boundary in februari 2025 [31] is een

belangrijke stap richting data residency binnen de EU/EFTA voor veel klantgegevens, pseudonieme data en supportdata. Dit vermindert de hoeveelheid data die de regio verlaat. De effectiviteit wordt echter beperkt door de erkende uitzonderingen voor noodzakelijke transfers (bv. security, support) [31], de mogelijkheid van remote access van buiten de EUDB [89], en het fundamentele punt dat data residency geen data soevereiniteit garandeert; Microsoft blijft als Amerikaans bedrijf onderworpen aan Amerikaanse wetgeving.[7] Het lost daarmee het kernprobleem van Schrems II niet volledig op.

- **Transparantie (RSD, Copilot):** Er bestaat een duidelijke discrepantie tussen Microsoft's claims van transparantie (via Trust Center, DSAR-mogelijkheden) [37] en de bevindingen in Nederlandse DPIA's, die juist een gebrek aan transparantie over Required Service Data en de werking van Copilot (incl. RAI-filters) als hoge risico's identificeren.[22] De onzekere status van de implementatie en acceptatie van Microsoft's toezeggingen van april 2025 om deze transparantie te verbeteren [21] is een kritiek punt per de peildatum van dit paper.
- **Technische Maatregelen:** M365 biedt een robuuste basisbeveiliging met diverse certificeringen en standaardmaatregelen zoals encryptie.[11] Echter, voor specifieke hoge risico's, zoals de verwerking van bijzondere persoonsgegevens of de risico's van gegevensoverdracht, worden deze standaardmaatregelen als onvoldoende beschouwd in Nederlandse DPIA's.[15] Aanvullende, door de gebruiker te implementeren maatregelen zoals Double Key Encryption (DKE) zijn nodig, maar brengen complexiteit en functionele beperkingen met zich mee.[15]

## Weging van Argumenten: Is M365 "AVG-Proof" in Nederland?

Een eenduidig "ja" of "nee" op de vraag of M365 "AVG-proof" is in Nederland per 18 april 2025, is niet mogelijk. Er zijn argumenten die pleiten voor een *mogelijke* compliance onder voorwaarden, en argumenten die wijzen op significante resterende risico's.

- **Argumenten richting compliance:** Microsoft biedt een uitgebreid compliance-framework met een DPA, TOMs, certificeringen en tools voor beheer.[16] De implementatie van de EU Data Boundary vermindert data-uitstroom.[31] Microsoft heeft aantoonbaar gereageerd op Nederlandse zorgen en aanpassingen doorgevoerd of toegezegd.[21] Contractuele garanties worden geboden.[37]
- **Argumenten tegen / Resterende risico's:** Het fundamentele probleem van mogelijke toegang door Amerikaanse autoriteiten (Schrems II / CLOUD Act) blijft bestaan, ondanks de EUDB.[7] Er is een significant gebrek aan transparantie geconstateerd over interne dataverwerkingen zoals RSD en de werking van Copilot AI.[22] Microsoft's rol is niet altijd beperkt tot die van verwerker.[22] Compliance vereist vaak complexe en potentieel beperkende aanvullende maatregelen van de gebruiker zelf.[15] De status van cruciale toezeggingen (n.a.v. Copilot DPIA) is onzeker.[21]

**Synthese:** M365 is **niet inherent of automatisch AVG-proof** in Nederland. De mogelijkheid om M365 compliant te gebruiken is **voorwaardelijk** en sterk afhankelijk van de specifieke context. Factoren die de mate van compliance bepalen zijn: de gebruikte M365-modules, de aard van de verwerkte gegevens (met name de aanwezigheid van bijzondere of gevoelige persoonsgegevens), de correcte configuratie van door Microsoft geboden tools en instellingen, de implementatie van noodzakelijke *aanvullende* technische en organisatorische maatregelen door de Nederlandse organisatie zelf (gebaseerd op een eigen, grondige DPIA en DTIA), de bereidheid van de organisatie om resterende (lage en mogelijk zelfs hoge) risico's bewust te accepteren, en de voortdurende monitoring van juridische, technische en contractuele ontwikkelingen.

## Impact van Nederlandse DPIA's en Schrems II op de Praktijk:

De Nederlandse aanpak, met name via SLM Rijk, toont aan dat gestructureerde DPIA's en daaropvolgende onderhandelingen een effectief middel kunnen zijn om druk uit te oefenen op grote leveranciers en concrete verbeteringen af te dwingen.[23] Deze onderzoeken hebben de bewustwording van AVG-risico's bij Nederlandse (overheids)organisaties aanzienlijk vergroot. Tegelijkertijd hebben ze de complexiteit van het bereiken en aantonen van compliance blootgelegd, wat specialistische juridische en technische kennis vereist.[3] Het Schrems II-arrest fungeert als een 'gamechanger' die de lat voor internationale gegevensoverdrachten permanent heeft verhoogd en een structureel obstakel vormt voor het gebruik van Amerikaanse clouddiensten zonder aanvullende waarborgen.[6] In de praktijk betekent dit dat Nederlandse organisaties moeten investeren in eigen risicoanalyses (DPIA/DTIA), mogelijk duurdere of complexere technologie (zoals DKE), de ontwikkeling van intern beleid, en training van medewerkers.[15] De verantwoordingsplicht onder de AVG wordt hiermee een actieve en continue inspanning.

## Resterende Risico's, Onduidelijkheden en Uitdagingen:

Per 18 april 2025 blijven er belangrijke risico's en onduidelijkheden bestaan:

- **Fundamenteel Transferrisico VS:** Dit kernprobleem blijft onopgelost zolang de Amerikaanse surveillancewetgeving niet wezenlijk verandert of er een nieuw, stabiel en juridisch robuust doorgiftemechanisme komt dat standhoudt voor het HvJEU.[7]
- **Transparantie RSD & AI:** Het gebrek aan volledige transparantie over welke data Microsoft verzamelt als RSD en hoe AI-algoritmes (zoals de RAI-filters in Copilot) precies werken en welke persoonsgegevens ze verwerken, blijft een significant risico.[22] De onzekere status van Microsoft's toezeggingen hieromtrent verergert dit.[21]
- **Handhaving:** Het is onduidelijk hoe de AP en andere Europese toezichthouders (zoals de EDPS, die onderzoek doet naar het gebruik van M365 door de Europese Commissie [18]) de resterende risico's op termijn zullen handhaven. Recente kritische standpunten uit Duitsland [47] en Frankrijk [80] suggereren aanhoudende druk.
- **Vendor Lock-in:** De economische realiteit van marktconcentratie en hoge egress fees

beperkt de keuzevrijheid en onderhandelingspositie van Nederlandse organisaties, wat hen kan dwingen risico's te accepteren.[3]

- **Complexiteit voor Gebruikers:** De primaire verantwoordelijkheid voor compliance ligt bij de gebruikersorganisatie, die vaak niet de middelen of expertise heeft om de complexe juridische en technische analyses volledig uit te voeren en de benodigde maatregelen te implementeren.

## Summarium en Conclusie:

De centrale vraag van dit paper is of Microsoft Office 365 per 18 april 2025 als "AVG-proof" kan worden beschouwd in Nederland. De analyse van juridische kaders, Microsoft's documentatie en maatregelen, Nederlandse DPIA-bevindingen, en de impact van Schrems II leidt tot de conclusie dat M365 **niet onvoorwaardelijk AVG-proof** is.

Microsoft biedt een geavanceerd platform met uitgebreide functionaliteiten en een gelaagd compliance-framework. Initiatieven zoals de EU Data Boundary en aanpassingen naar aanleiding van Nederlandse DPIA's tonen een bereidheid om tegemoet te komen aan Europese zorgen. Echter, fundamentele problemen blijven bestaan. Het risico van toegang tot gegevens door Amerikaanse autoriteiten, de kern van de Schrems II-problematiek, wordt door Nederlandse instanties als onvoldoende gemitigeerd door de huidige maatregelen, inclusief de EU Data Boundary. Daarnaast is er een significant gebrek aan transparantie geconstateerd met betrekking tot interne gegevensverwerkingen, met name rondom Required Service Data en de nieuwe AI-functionaliteiten in Copilot, wat de controle door de verwerkingsverantwoordelijke ondermijnt.

Het bereiken van een acceptabel niveau van AVG-compliance bij het gebruik van M365 in Nederland vereist daarom een **proactieve, risico-gebaseerde en context-specifieke aanpak van de gebruikersorganisatie**. Dit omvat het uitvoeren van grondige eigen DPIA's en DTIA's, het zorgvuldig configureren van beschikbare privacy-instellingen, het implementeren van aanvullende technische (zoals DKE voor zeer gevoelige data) en organisatorische maatregelen, het ontwikkelen van helder intern beleid, het trainen van medewerkers, en het bewust accepteren van de resterende, niet-mitigeerbare risico's. De mate waarin M365 als "AVG-proof" kan worden beschouwd, is dus geen statisch gegeven, maar een dynamisch resultaat van continue inspanningen en afwegingen door de Nederlandse organisatie zelf, binnen een complex en voortdurend veranderend juridisch en technologisch landschap.

## Aanbevelingen:

- **Voor Nederlandse Organisaties:**
  - Voer altijd een eigen, grondige en actuele DPIA en DTIA uit, specifiek toegesneden op het eigen gebruik van M365 en de aard van de verwerkte gegevens.
  - Implementeer de relevante aanbevelingen uit de DPIA's van SLM Rijk en/of SIVON.
  - Overweeg het gebruik van Double Key Encryption (DKE) of vergelijkbare technologieën voor de opslag van bijzondere en zeer gevoelige persoonsgegevens, rekening houdend met de functionele beperkingen.
  - Ontwikkel duidelijk intern gebruiksbeleid voor M365 (inclusief Copilot), met specifieke aandacht voor gegevensbescherming, en zorg voor adequate training van medewerkers.
  - Monitor actief de status van Microsoft's toezeggingen (met name die n.a.v. de Copilot DPIA) en volg juridische en technologische ontwikkelingen.
  - Maak een expliciete, gedocumenteerde afweging van de resterende risico's versus de baten van het gebruik van M365.[24]
- **Voor Vervolgonderzoek:**
  - Continue monitoring van de implementatie en effectiviteit van Microsoft's toezeggingen van april 2025 en de beoordeling hiervan door SLM Rijk.
  - Analyse van de impact van toekomstige jurisprudentie, met name met betrekking tot het EU-US Data Privacy Framework en eventuele opvolgers van Schrems II.
  - Onderzoek naar de praktische haalbaarheid, kosten en effectiviteit van aanvullende maatregelen zoals DKE in verschillende Nederlandse sectoren.
  - Evaluatie van de implicaties van de Europese AI Act voor het gebruik van AI-functionaliteiten zoals Copilot binnen M365.
  - Verder onderzoek naar de ontwikkeling en adoptie van Europese cloudalternatieven en hun potentieel om de geïdentificeerde AVG-risico's te mitigeren.[5]

# 5. Productie - Auteur

## Tooling

Dit rapport is tot stand gekomen door het gebruik van Litic Co-Intelligence, ChatGPT-o3, Claude 3.7 Sonnet Extended, Perplexity Pro, Mistral Le Chat Pro en Google.

## Prompting & refinement

Anthony Loeff – Litic.AI – 18 april 2025 (submitted for review)

# 6. Referentielijst

*Geciteerd werk*


1. De AVG in het kort - Autoriteit Persoonsgegevens, geopend op april 18, 2025, https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/avg-algemeen/de-avg-in-het-kort
2. What is GDPR Compliance? | Microsoft Security, geopend op april 18, 2025, https://www.microsoft.com/en-us/security/business/security-101/what-is-gdpr-compliance
3. Het Rijk in de cloud - Algemene Rekenkamer, geopend op april 18, 2025, https://www.rekenkamer.nl/binaries/rekenkamer/documenten/rapporten/2025/01/15/het-rijk-in-de-cloud/Het+Rijk+in+de+cloud.pdf
4. Marktstudie Clouddiensten - ACM, geopend op april 18, 2025, https://www.acm.nl/system/files/documents/marktstudie-clouddiensten.pdf
5. Autoriteit Financiële Markten De AFM doet geen mededelingen over de keuzes die worden gemaakt in de bedrijfsvoering. Tweede Kam - NOS, geopend op april 18, 2025, https://app.nos.nl/nieuws/mailservers/reacties.pdf
6. Verwerking en doorgifte van persoonsgegevens bij het gebruik van Amerikaanse clouddiensten - NGB, geopend op april 18, 2025, https://www.ngb.nl/nieuws-detailpagina?weblog-year=2022&weblog-month=08&weblog-day=18&weblog-postTitle=Verwerking-en-doorgifte-van-persoonsgegevens-bij-het-gebruik-van-Amerikaanse-clouddiensten
7. Is Microsoft 365 AVG-veilig? Spoiler alert: nee - Smartlockr, geopend op april 18, 2025, https://www.smartlockr.io/nl/blog/is-microsoft-office-365-avg-compliant-spoiler-alert-nee
8. Autoriteit Persoonsgegevens waarschuwt kabinet voor privacyrisico's cloudbeleid, geopend op april 18, 2025, https://www.security.nl/posting/774431/Autoriteit+Persoonsgegevens+waarschuwt+kabinet+voor+privacyrisico%27s+cloudbeleid
9. The Impact of Schrems II & Key Considerations for Companies Using M365: The Background - Lighthouse eDiscovery, geopend op april 18, 2025, https://www.lighthouseglobal.com/blog/the-impact-of-schrems-ii-key-considerations-for-companies-using-m365-the-background
10. Verantwoordelijke en verwerker - Autoriteit Persoonsgegevens, geopend op april 18, 2025, https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/avg-algemeen/verantwoordelijke-en-verwerker

11. Praktijkgids Patiëntgegevens in de cloud | AVG-Helpdesk, geopend op april 18, 2025, https://www.avghelpdeskzorg.nl/binaries/avghelpdeskzorg/documenten/publicaties/2023/05/08/praktijkgids-patientgegevens-in-de-cloud/AP+praktijkgids_patientgegevens_in_de_cloud_def.pdf
12. Advies opslag medische data in de cloud - Tweede Kamer, geopend op april 18, 2025, https://www.tweedekamer.nl/downloads/document?id=2019D39706
13. Patiëntgegevens in de cloud: altijd onverstandig? - Privacy1, geopend op april 18, 2025, https://privacy1.nl/algemeen/patientgegevens-in-de-cloud-altijd-onverstandig/
14. Microsoft Teams, SharePoint en bijzondere persoonsgegevens, geopend op april 18, 2025, https://ericburger.nl/microsoft365/microsoft-teams-sharepoint-en-bijzondere-persoonsgegevens/
15. Veelgestelde vragen over privacytoets op Microsoft Teams ... - SIVON, geopend op april 18, 2025, https://sivon.nl/2022/04/veelgestelde-vragen-over-privacytoets-op-microsoft-teams-onedrive-en-sharepoint/
16. AVG vereenvoudigd: Een handleiding voor kleine bedrijven - Microsoft 365 admin, geopend op april 18, 2025, https://learn.microsoft.com/nl-nl/microsoft-365/admin/security-and-compliance/gdpr-compliance?view=o365-worldwide
17. Algemene verordening gegevensbescherming (AVG) | Onderzoekers | Centrale Commissie Mensgebonden Onderzoek, geopend op april 18, 2025, https://www.ccmo.nl/onderzoekers/wet-en-regelgeving-voor-medisch-wetenschappelijk-onderzoek/wetten/algemene-verordening-gegevensbescherming-avg
18. The EDPS opens two investigations following the “Schrems II” Judgement, geopend op april 18, 2025, https://www.edps.europa.eu/press-publications/press-news/press-releases/2021/edps-opens-two-investigations-following-schrems_en
19. The Definitive Guide to Schrems II | Resource - DataGuidance, geopend op april 18, 2025, https://www.dataguidance.com/resource/definitive-guide-schrems-ii
20. Gegevens, privacy en beveiliging voor Microsoft 365 Copilot, geopend op april 18, 2025, https://learn.microsoft.com/nl-nl/copilot/microsoft-365/microsoft-365-copilot-privacy
21. Microsoft commitments to M365 Copilot DPIA, geopend op april 18, 2025, https://pulse.microsoft.com/nl-be/work-productivity-nl-be/na/fa2-979641/
22. DPIA Microsoft 365 Copilot, geopend op april 18, 2025, https://slmmicrosoftrijk.nl/wp-content/uploads/2024/12/20241218-Public-version-DPIA-Microsoft-365-Copilot-for-SLM-Rijk.pdf
23. Memo - M365 Copilot DPIA en FRAIA - SLM Microsoft Rijk, geopend op april 18, 2025, https://slmmicrosoftrijk.nl/wp-content/uploads/2024/12/20241217-Memo-M365-Copilot-DPIA-en-FRAIA.pdf
24. Amsterdam doet geen pilot met Microsoft Copilot wegens privacyrisico's - update - Tweakers, geopend op april 18, 2025, https://tweakers.net/nieuws/232334/amsterdam-doet-geen-pilot-met-microsoft-copilot-wegens-privacyrisicos.html
25. Rijk en Microsoft in overleg over privacyrisico's Copilot - iBestuur, geopend op april 18, 2025, https://ibestuur.nl/artikel/rijk-en-microsoft-in-overleg-over-privacyrisicos-copilot/
26. Gemeenten gewaarschuwd voor risico's Microsoft Copilot - Dutch IT Channel, geopend op april 18, 2025, https://www.dutchitchannel.nl/news/596038/gemeenten-

gewaarschuwd-voor-risicos-microsoft-copilot
27. Update DPIA Microsoft365 Copilot - SLBdiensten, geopend op april 18, 2025, https://www.slbdiensten.nl/nieuws-overzicht/update-dpia-microsoft365-copilot/
28. brief_over_rijksbreed_cloudbelei, geopend op april 18, 2025, https://autoriteitpersoonsgegevens.nl/uploads/imported/brief_over_rijksbreed_cloudbeleid_2022.pdf
29. Gegevensbescherming in de publieke cloud - iBestuur, geopend op april 18, 2025, https://ibestuur.nl/artikel/gegevensbescherming-in-de-publieke-cloud/
30. Microsoft EU Data Boundary Overview | Microsoft Trust Center, geopend op april 18, 2025, https://www.microsoft.com/en-us/trust-center/privacy/european-data-boundary-eudb
31. Microsoft completes landmark EU Data Boundary, offering enhanced data residency and transparency - Microsoft On the Issues, geopend op april 18, 2025, https://blogs.microsoft.com/on-the-issues/2025/02/26/microsoft-completes-landmark-eu-data-boundary-offering-enhanced-data-residency-and-transparency/
32. Microsoft Windows 10 De verwerking van persoonsgegevens via telemetrie, geopend op april 18, 2025, https://autoriteitpersoonsgegevens.nl/uploads/imported/01_onderzoek_microsoft_windows_10_okt_2017.pdf
33. DPIA Office 365 Online and mobile Office apps (June 2019) Data protection impact assessment on the processing of diagnostic data - Government.nl, geopend op april 18, 2025, https://www.government.nl/binaries/government/documenten/publications/2019/07/23/dpia-microsoft-office-365-online-and-mobile-slm-rijk-23-july/DPIA+Microsoft+Office+365+Online+and+Mobile+SLM+Rijk+23+july.pdf
34. Ministry of Justice and Security - SLM Microsoft, Google Cloud en Amazon Web Services, geopend op april 18, 2025, https://slmmicrosoftrijk.nl/wp-content/uploads/2021/04/REQ5267448-B-MinJen-V-Summary-report-Profiling-restrictions-Microsoft-final-wg-versie.pdf
35. New DPIA for the Dutch government and universities on Microsoft Teams, OneDrive and SharePoint Online | Privacy Company Blog, geopend op april 18, 2025, https://www.privacycompany.eu/blog/new-dpia-for-the-dutch-government-and-universities-on-microsoft-teams-onedrive-and-sharepoint-online
36. ECLI:NL:RBAMS:2024:3331, Rechtbank Amsterdam, C/13/747731 / KG ZA 24-199 - Uitspraken, geopend op april 18, 2025, https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBAMS:2024:3331
37. Data protection and privacy - Microsoft Trust Center, geopend op april 18, 2025, https://www.microsoft.com/en-us/trust-center/privacy
38. The Microsoft Trust Center & Service Trust Portal - intercept.cloud, geopend op april 18, 2025, https://intercept.cloud/en-gb/blogs/the-microsoft-trust-center-and-service-trust-portal
39. General Data Protection Regulation, GDPR Overview - Microsoft, geopend op april 18, 2025, https://www.microsoft.com/en-us/trust-center/privacy/gdpr-overview
40. Microsoft Trust Center - choose your locale, geopend op april 18, 2025, https://www.microsoft.com/en-us/trust-center/locale
41. Gegevensbescherming met Microsoft-privacyprincipes, geopend op april 18, 2025, https://www.microsoft.com/nl-nl/trust-center/privacy

42. Informatiebronnen over privacy en AVG in Microsoft, geopend op april 18, 2025, https://www.microsoft.com/nl-nl/trust-center/privacy/resources
43. General Data Protection Regulation (GDPR) | Microsoft Learn, geopend op april 18, 2025, https://learn.microsoft.com/en-us/legal/gdpr
44. Chat GPT advised me that having a DPA with Microsoft is crucial to ensure GDPR compliance when processing personal data for your EU-based clients through OpenAI LLM API services provided by Microsoft. Please confirm this requirement. If yes ,tell me how?, geopend op april 18, 2025, https://learn.microsoft.com/en-us/answers/questions/1857439/chat-gpt-advised-me-that-having-a-dpa-with-microso
45. Professional Services GDPR - Microsoft, geopend op april 18, 2025, https://www.microsoft.com/en-us/professionalservices/gdpr
46. Microsoft Products and Services Data Protection Addendum - SDPC Resource Registry, geopend op april 18, 2025, https://sdpc.a4l.org/agreements/2024-02-08_6583_456_signed_agreement_file.pdf
47. MS 365 data protection - new DPA for 2023 published | reuschlaw ..., geopend op april 18, 2025, https://www.reuschlaw.de/en/news/ms-365-data-protection/
48. Microsoft Products and Services Data Protection Addendum (DPA) - Licensing Documents, geopend op april 18, 2025, https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA
49. Algemene Verordening Gegevensbescherming (AVG) - Learn Microsoft, geopend op april 18, 2025, https://learn.microsoft.com/nl-nl/legal/gdpr
50. Microsoft Licensing Update April 2025 - LicenseQ, geopend op april 18, 2025, https://licenseq.com/microsoft-licensing-update-april-2025/
51. EU Data Boundary - Microsoft Cloud for Sovereignty, geopend op april 18, 2025, https://learn.microsoft.com/en-us/industry/sovereignty/eu-data-boundary
52. What is the EU Data Boundary? - Microsoft Privacy, geopend op april 18, 2025, https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-learn
53. Microsoft EU Data Boundary: Enhanced Data Residency and Transparency, geopend op april 18, 2025, https://www.schneider.im/microsoft-eu-data-boundary-enhanced-data-residency-and-transparency/
54. Understanding the Microsoft EU Data Boundary Roadmap: Background, Recap, and Updates December 2023, geopend op april 18, 2025, https://www.microsoft.com/content/dam/microsoft/final/en-us/microsoft-brand/documents/Understanding-the-EU-Data-Boundary-External-01-12-2024.pdf?culture=en-us&country=us
55. Required diagnostic data for Office - Microsoft 365 Apps, geopend op april 18, 2025, https://learn.microsoft.com/en-us/microsoft-365-apps/privacy/required-diagnostic-data
56. Required service data for Office - Microsoft 365 Apps, geopend op april 18, 2025, https://learn.microsoft.com/en-us/microsoft-365-apps/privacy/required-service-data
57. Verwerkersovereenkomst | Autoriteit Persoonsgegevens, geopend op april 18, 2025, https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/avg-algemeen/verwerkersovereenkomst
58. Duitse toezichthouders: 'MS Office 365 in strijd met AVG' - PONT | Data & Privacy, geopend op april 18, 2025, https://privacy-web.nl/nieuws/duitse-toezichthouders-ms-office-365-in-strijd-met-avg/

59. Public Market Study Cloud services - ACM, geopend op april 18, 2025, https://www.acm.nl/system/files/documents/public-market-study-cloud-services.pdf
60. ACM: amendments to Data Act necessary for promoting competition among cloud providers, geopend op april 18, 2025, https://www.acm.nl/en/publications/acm-amendments-data-act-necessary-promoting-competition-among-cloud-providers
61. Ongoing investigation into the use of M365 by EUIs after Schrems II | European Data Protection Supervisor, geopend op april 18, 2025, https://www.edps.europa.eu/data-protection/our-work/publications/factsheets/ongoing-investigation-use-m365-euis-after-schrems_en
62. Compliance with EU transfer requirements for personal data in the Microsoft Cloud, geopend op april 18, 2025, https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Compliance-with-EU-transfer-requirements-for-personal-data-Jan-27.pdf
63. Schrems II landmark ruling: A detailed analysis | Netherlands | Global law firm, geopend op april 18, 2025, https://www.nortonrosefulbright.com/en-nl/knowledge/publications/ad5f304c/schrems-ii-landmark-ruling-a-detailed-analysis
64. The Impact of Schrems II & Key Considerations for Companies Using M365: Microsoft's Response - Lighthouse eDiscovery, geopend op april 18, 2025, https://www.lighthouseglobal.com/blog/the-impact-of-schrems-ii-key-considerations-for-companies-using-m365-microsoft-s-response
65. The Impact of Schrems II & Key Considerations for Companies Using M365: The Cloud Environment | Lighthouse - JDSupra, geopend op april 18, 2025, https://www.jdsupra.com/legalnews/the-impact-of-schrems-ii-key-1555178/
66. Juridische haken en ogen bij inzet commerciële clouddiensten, geopend op april 18, 2025, https://ibestuur.nl/artikel/juridische-haken-en-ogen-bij-inzet-commerciele-clouddiensten/
67. De EDPS opent twee onderzoeken naar aanleiding van het, geopend op april 18, 2025, https://privacy-web.nl/nieuws/de-edps-opent-twee-onderzoeken-naar-aanleiding-van-het-schrems-ii-arrest/
68. Antwoorden op de vragen uit het webinar 'Schrems II, Brexit en het gebruik van de cloud', geopend op april 18, 2025, https://www.nen.nl/nieuws/ict/antwoorden-op-devragen-uit-het-webinar-schrems-ii-brexit-en-het-gebruik-van-de-cloud/
69. Schrems II, Brexit en het gebruik van de cloud - NEN, geopend op april 18, 2025, https://www.nen.nl/media/PDF/nen-powerpoint-webinar-schrems.pdf
70. De noodzaak van een multi-cloudstrategie - ICT/Magazine, geopend op april 18, 2025, https://www.ictmagazine.nl/de-noodzaak-van-een-multi-cloudstrategie/
71. optimal dynamic resource allocation for heterogenous cloud data, geopend op april 18, 2025, https://etd.lib.metu.edu.tr/upload/12624630/index.pdf
72. Master thesis - report v128 - GDMC, geopend op april 18, 2025, https://gdmc.nl/publications/2012/Point_Clouds_Database.pdf
73. Vulnerabilities, Cybersecurity, and the Role of Law and Regulation, geopend op april 18, 2025, https://repub.eur.nl/pub/136974/thesis-Jian-Jiang.pdf
74. Master Thesis Strategic Management, geopend op april 18, 2025, https://theses.ubn.ru.nl/bitstreams/2fdfb562-a8a9-4f8f-a027-6531ea0ce614/download
75. Fusion Approaches for Monocular Depth Estimation - LIACS Thesis, geopend op april

18, 2025, https://theses.liacs.nl/pdf/2019-2020-SchepD.pdf
76. New DPIA and DTIA on AWS for the Dutch government: all high risks solved, geopend op april 18, 2025, https://www.privacycompany.eu/blog/new-dpia-and-dtia-on-aws-for-the-dutch-government-all-high-risks-solved
77. Response to German findings regarding Microsoft 365 | SURF.nl, geopend op april 18, 2025, https://www.surf.nl/en/response-to-german-findings-regarding-microsoft-365
78. Microsoft unveils finalized EU Data Boundary - The Register, geopend op april 18, 2025, https://www.theregister.com/2025/03/03/microsoft_unveils_a_finalized_eu/
79. Microsoft 365 mag niet voor Europese Commissie, van Europese privacywaakhond, geopend op april 18, 2025, https://www.agconnect.nl/business/datamanagement/microsoft-365-mag-niet-voor-ec-van-europese-privacywaakhond
80. Microsoft 365 is onwettig, concludeert Duitsland - AG Connect, geopend op april 18, 2025, https://www.agconnect.nl/tech-en-toekomst/juridisch/microsoft-365-is-onwettig-concludeert-duitsland
81. SURF raadt Nederlandse scholen af Microsoft 365 Copilot te gebruiken - update - Tweakers, geopend op april 18, 2025, https://tweakers.net/nieuws/229936/surf-raadt-nederlandse-scholen-af-microsoft-365-copilot-te-gebruiken.html
82. Landmark EU Data Boundary for Microsoft Cloud is Complete - TechRepublic, geopend op april 18, 2025, https://www.techrepublic.com/article/microsoft-cloud-eu-data-boundary/
83. Microsoft completes EU Data Boundary for Microsoft Cloud - DCD - Data Center Dynamics, geopend op april 18, 2025, https://www.datacenterdynamics.com/en/news/microsoft-completes-eu-data-boundary-for-microsoft-cloud/
84. Egress fees in the Cloud market: a powerful tool to lock users in - Open Internet Project, geopend op april 18, 2025, https://www.openinternetproject.eu/en/2022/12/15/egress-fees-in-the-cloud-market-a-powerful-tool-to-lock-users-in/
85. Verwerkersovereenkomst: 9 veelgestelde vragen - INVOLV, geopend op april 18, 2025, https://www.involv.nl/kennisbank/verwerkersovereenkomst-9-veelgestelde-vragen
86. Wat is een verwerkersovereenkomst? - AVG compleet, geopend op april 18, 2025, https://avg-compleet.nl/verwerkersovereenkomst/
87. Microsoft Copilot: Privacy concerns and compliance tips for 2025 - DPO Centre, geopend op april 18, 2025, https://www.dpocentre.com/microsoft-copilot-privacy-compliance-tips/
88. Algemene verordening gegevensbescherming, overzicht van de AVG - Microsoft, geopend op april 18, 2025, https://www.microsoft.com/nl-nl/trust-center/privacy/gdpr-overview
89. Continuing data transfers that apply to all EU Data Boundary Services - Microsoft Privacy, geopend op april 18, 2025, https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-transfers-for-all-services
90. Data Residency for Other Microsoft 365 Services, geopend op april 18, 2025, https://learn.microsoft.com/en-us/microsoft-365/enterprise/m365-dr-workload-other?view=o365-worldwide
91. April 2025 updates for Microsoft Office, geopend op april 18, 2025, https://support.microsoft.com/en-us/topic/april-2025-updates-for-microsoft-office-

5ac73359-8e7f-48d1-9966-ac9d5e4cd140
92. April 2025 announcements - Partner Center announcements | Microsoft Learn, geopend op april 18, 2025, https://learn.microsoft.com/en-us/partner-center/announcements/2025-april
93. March 2025 announcements - Partner Center announcements | Microsoft Learn, geopend op april 18, 2025, https://learn.microsoft.com/en-us/partner-center/announcements/2025-march
94. Microsoft and Adobe Patch Tuesday, April 2025 Security Update Review - Qualys Blog, geopend op april 18, 2025, https://blog.qualys.com/vulnerabilities-threat-research/2025/04/08/microsoft-patch-tuesday-april-2025-security-update-review
95. The April 2025 Security Update Review - Zero Day Initiative, geopend op april 18, 2025, https://www.zerodayinitiative.com/blog/2025/4/8/the-april-2025-security-update-review
96. April 2025 Microsoft 365 Changes: What's New and What's Gone? : r/sysadmin - Reddit, geopend op april 18, 2025, https://www.reddit.com/r/sysadmin/comments/1jot7ou/april_2025_microsoft_365_changes_whats_new_and/
97. Microsoft unveils Microsoft Security Copilot agents and new protections for AI, geopend op april 18, 2025, https://www.microsoft.com/en-us/security/blog/2025/03/24/microsoft-unveils-microsoft-security-copilot-agents-and-new-protections-for-ai/
98. Network pricing | Google Cloud, geopend op april 18, 2025, https://cloud.google.com/vpc/network-pricing