Microsoft Dragon Copilot

Privacy en beveiliging van patiëntgegevens

Praktisch overzicht voor artsen en zorgorganisaties
Met verdieping voor ICT, FG, DPO en compliance officers

Versie 1.0 | 16 oktober 2026 | Nederland en België

Wat dit document u helpt beoordelen

Microsoft documenteert voor Dragon Copilot maatregelen voor de verwerking en bescherming van medische gegevens. Verantwoord gebruik vraagt daarnaast om een beoordeling van de eigen zorgpraktijk, contracten, gegevensstromen en inrichting. Dit overzicht ondersteunt die beoordeling en wijst de weg naar de formele bronnen.

Onderwerp	Kernpunt en grens
Patiëntgegevens	Audio, transcripties, concepten en correcties worden verwerkt in de cloud. [1, 3]
Opslaglocatie	Voor een Belgische tenant: Frankrijk. Voor een Nederlandse tenant: Duitsland. Voorwaarden en configuratie controleren. [4]
AI en menselijke inzage	Microsoft beschrijft anonimisering voor modelverbetering en beperkte menselijke toegang. Geen algemene belofte dat gegevens nooit worden gebruikt voor AI. [1, 4]
Bewaren	De FAQ noemt tot 90 dagen voor bepaalde gegevens. Dit is geen universele termijn voor alle gegevens en kopieën. [2]
Beveiliging	Versleuteling, Entra ID, logging en klantscheiding zijn gedocumenteerd. De lokale inrichting blijft essentieel. [5]
AVG	Een leveranciersverklaring vervangt geen eigen grondslag, DPIA of verantwoordingsdossier. [8, 9]

Zo leest u de bewijsstatus

BEVESTIGD betekent dat de genoemde bron de uitspraak ondersteunt; het is geen onafhankelijke technische audit. VOORBEHOUD benoemt een beperking of interpretatie. OPEN VRAAG vraagt om organisatiegebonden bewijs of schriftelijke bevestiging. Nummers verwijzen naar de bronnen op pagina 6.

Dit document is een informatieve toelichting van AVT Benelux, geen juridisch advies of garantie van compliance. Het vervangt geen DPIA, leveranciersbeoordeling of advies van een FG, DPO of jurist. Controleer bij besluitvorming de dan geldende Microsoft-documentatie en contractversies.

Gegevens en verantwoordelijkheden

Van opname naar gecontroleerde documentatie

BEVESTIGD Dragon Copilot verwerkt gesprekken en dicteeraudio tot transcripties en conceptdocumentatie. De zorgverlener controleert en corrigeert de uitkomst. Ook correcties en definitief ondertekende documentatie kunnen worden verzameld. [1, PDF p. 168–169]

Categorie	Voorbeelden en aandachtspunt
Medische inhoud	Gespreksaudio, transcript, concepten, correcties en eindversies. Audio kan ook informatie bevatten die niet in de samenvatting terechtkomt. [1, 3]
Gebruikers en beheer	Naam, e-mailadres, specialisme, organisatie-instellingen en sjablonen. [3]
Gebruik en diagnostiek	Opnameduur, verwerkingsduur, feedback, versies en servicelogs. Neem deze mee in het verwerkingsregister. [3]
EPD-koppeling	Optionele FHIR-, HL7- of EPD-gegevens over patiënt, zorgverlener en consult. Een integratiepartner kan aanvullende gegevensstromen toevoegen. [3]

VOORBEHOUD De feitelijke stroom hangt af van app, functionaliteit, land en EPD-koppeling. Beschouw medische concepten, metadata en supportbijlagen eveneens als te beschermen informatie. Gebruik geen algemene Microsoft 365 Copilot-privacytekst als bewijs voor Dragon Copilot.

De arts en de organisatie houden de regie

Dragon Copilot ondersteunt documentatie en vervangt het patiëntendossier niet. De zorgverlener moet relevante output controleren, exporteren en in het daarvoor aangewezen dossier vastleggen. Controleer onder meer medicatie, ontkenningen, identiteit en weggelaten of verzonnen informatie. [6; PDF p. 181; 7]

De organisatie bepaalt wie toegang krijgt en zorgt dat toegang past bij de behandelrelatie. Richt individuele accounts, functiescheiding, tijdige intrekking van toegang en beveiligde apparaten in. [1, 5]

OPEN VRAAG AAN DE ZORGINSTELLING Welke onderdelen zijn actief, welke gegevens worden naar welke partij verzonden en wie controleert de overdracht naar het EPD? Leg ook de rol van AVT, de integratieleverancier en eventuele supportpartijen per verwerking vast.

Patiëntinformatie en opname

Microsoft noemt patiënttoestemming voor opnamen volgens organisatiebeleid. Laat de organisatie vaststellen hoe patiënten vooraf worden geïnformeerd, hoe toestemming of weigering wordt vastgelegd en welk alternatief beschikbaar is. [7]

VOORBEHOUD Toestemming voor een opname is niet automatisch de AVG-grondslag voor alle verdere verwerking. Laat de FG of DPO de grondslag, uitzondering voor gezondheidsgegevens en het beroepsgeheim afzonderlijk beoordelen. De Nederlandse AP licht toe dat reguliere zorgverwerking vaak op een wettelijke basis rust. Voor België is een lokale juridische toets nodig. [8]

AI en gebruik van gegevens

Anonimisering en modelverbetering

BEVESTIGD De privacywhitepaper beschrijft dat geselecteerde klantgegevens naar een aangewezen researchomgeving gaan en binnen 90 dagen na vastlegging of generatie worden geanonimiseerd. De resulterende data wordt gebruikt voor verbetering van Dragon Copilot en zijn AI/ML-modellen. Microsoft stelt dat die modellen uitsluitend op geanonimiseerde gegevens worden getraind. [1, §4; PDF p. 169]

VOORBEHOUD Het selecteren, kopiëren en anonimiseren vindt plaats voordat de gegevens anoniem zijn. Die stappen vragen dus zelf om bescherming en juridische beoordeling. Pseudonimisering is geen anonimisering; een verwijderd patiëntnummer maakt klinische inhoud of stemdata niet vanzelf onherleidbaar.

Contracttekst en whitepaper samen beoordelen

De Privacy & Security Terms bevatten voor Dragon Copilot een ruime verwerkingsinstructie, inclusief menselijke beoordeling voor het trainen en ontwikkelen van modellen en functies, ook voor opvolgende producten en diensten. De whitepaper beschrijft de operationele beperking tot geanonimiseerde trainingsdata. Laat Microsoft schriftelijk bevestigen hoe beide teksten voor de aangeschafte dienst en regio samen gelden. [4, onderdeel Microsoft Dragon Copilot; 1]

OPEN VRAAG AAN MICROSOFT Welke datasets, modellen en opvolgende diensten vallen onder deze instructie? Hoe wordt anonimisering van audio en zeldzame medische casussen getoetst? Welke onafhankelijke assurance is beschikbaar? Is uitsluiten van researchverwerking mogelijk en zo ja, voor welke licentie en met welke werking?

Menselijke toegang en subprocessors

Microsoft beschrijft beperkte menselijke toegang voor support, betrouwbare werking, kwaliteitscontrole en het maken van geanonimiseerde datasets. Die toegang kan selecte medewerkers en subprocessors omvatten. [1, §4; PDF p. 170]

Microsoft verwijst voor de betrokken subprocessors naar de Health and Life Sciences Subprocessor List. De actuele namen, locaties en taken moeten uit de geldende lijst worden vastgelegd; dit document bevestigt geen volledige actuele lijst. [1, §7; 10]

OPEN VRAAG AAN MICROSOFT Lever de actuele lijst met versie, functie, verwerkingsland en toegang tot herkenbare patiëntgegevens. Bevestig hoe wijzigingen, bezwaar, geheimhouding, toegangstoestemming en logging zijn geregeld, ook voor annotatie en support.

Verkoop en advertenties

VOORBEHOUD De onderzochte productwhitepapers beschrijven geen verkoop van patiëntgegevens voor advertenties. Dat is geen bewijs voor een onbeperkte garantie dat gegevens nooit worden gedeeld of commercieel benut. De voorwaarden bevatten gebruiksrechten voor gedeïdentificeerde informatie. Vraag expliciete contractuele bevestiging over verkoop, reclamegebruik en verdere verstrekking, inclusief geanonimiseerde datasets. [1, 4]

Locatie en bewaartermijnen

Opslag in Europa en de EU Data Boundary

BEVESTIGD De Product Terms koppelen opslag in rust aan de tenantlocatie: België en Ierland naar Frankrijk; Nederland en Oostenrijk naar Duitsland, behoudens beschreven productuitzonderingen. Voor Dragon Copilot wordt de EU Data Boundary automatisch ingesteld bij een EU- of EFTA-tenant. [4]

VOORBEHOUD Opslag in rust is iets anders dan verwerking, remote toegang en support. De EU Data Boundary omvat EU en EFTA en kent beperkte doorgiften. Algemene Microsoft-documentatie noemt onder meer toegang van buiten de grens en mondiale beveiligingsactiviteiten. Dit zijn mogelijke uitzonderingscategorieën, geen vaststelling dat elke categorie in uw Dragon-omgeving optreedt. [11, 12]

OPEN VRAAG AAN MICROSOFT Bevestig de tenantregio en locaties van productie, research, back-ups, diagnostiek en support. Geef per toepasselijke grensoverschrijdende stroom de ontvanger, noodzaak, doorgiftegrondslag en aanvullende maatregelen. Laat dit aansluiten op de eigen doorgiftebeoordeling.

Drie verschillende termijnen

Gegevens of gebeurtenis	Gedocumenteerd en nog te toetsen
Operationele gegevens	FAQ: audio, herkende tekst, transcript en flowsheetwaarden tot 90 dagen. Vraag startmoment, uitzonderingen en verwijdering van kopieën na. [2]
Research vóór anonimisering	Privacywhitepaper: anonimisering binnen 90 dagen na vastlegging of generatie. Dit is een afzonderlijk proces. [1, §4]
Na beëindiging of proefgebruik	Product Terms noemen toepassing van de standaard DPA-regeling op gratis trials, inclusief 90 dagen na einde abonnement. Controleer de toepasselijke DPA voor de volledige cyclus. [4]
Anonieme data en eigen EPD	Reeds geanonimiseerde data wordt volgens Microsoft niet gewist bij latere intrekking. Het eigen patiëntendossier valt onder de eigen dossier- en bewaarplichten. [1, §5; 6]

Verwijdering en rechten van patiënten

De privacywhitepaper verwijst naar de DPA voor bewaren en wissen. Bij intrekking van eerder gegeven toestemming kan de klant een supportticket indienen voor verwijdering van herleidbare klantgegevens uit operationele en researchsystemen. Reeds anonieme gegevens worden daarbij niet verwijderd. [1, §5 en §9; PDF p. 170–171]

OPEN VRAAG AAN MICROSOFT Geef een bewaarmatrix voor elke gegevenscategorie, inclusief logs, feedback, back-ups en support. Wat is de maximale technische wistijd, welke uitzonderingen gelden en welk verwijderbewijs ontvangt de klant?

Beveiliging en AVG beoordeling

Gedocumenteerde beveiligingsmaatregelen

BEVESTIGD De securitywhitepaper noemt TLS 1.3 tijdens transport, AES-256 bij opslag, Microsoft-beheerde sleutels, Entra ID, auditlogging, logische scheiding van klantdata en periodieke penetratietests. De FAQ noemt TLS 1.2 of 1.3. Vraag bij technische eisen welke versie elke gebruikte verbinding daadwerkelijk ondersteunt. [5; PDF p. 175–179; 2]

VOORBEHOUD Transport- en opslagversleuteling betekenen hier niet dat Microsoft de inhoud technisch niet kan ontsleutelen. Vraag naar sleutelbeheer, lokale mobiele buffers, auditexport en logretentie. De beschreven maatregelen zijn leveranciersclaims; hun werking moet blijken uit passend bewijs en de eigen inrichting.

Normen en certificering

Microsoft noemt meerdere zorg- en beveiligingskaders. Maak onderscheid tussen het Azure-platform, de Dragon-dienst en de eigen zorginstelling. De FAQ noemt bij ISO 27001 en ISO 27701 expliciet een nog lopende certificering; andere verwijzingen hebben een andere scope. Een algemene normvermelding is daarom geen bewijs van actuele certificering voor uw volledige oplossing. [2, 5]

OPEN VRAAG AAN MICROSOFT Lever geldige certificaten en auditrapporten met scope, periode, regio en eventuele uitsluitingen. Verifieer afzonderlijk de relevantie van SOC, NEN 7510, HDS en andere lokaal vereiste normen. Leg bevindingen en opvolging vast.

Checklist voor FG en DPO

Onderstaande punten zijn AVT-beoordelingsadviezen. De instelling legt eigenaar, bewijs en besluit per punt vast. [8, 9]

Te beoordelen	Vast te leggen bewijs of besluit
Doel en rechtmatigheid	Doelen, rollen per partij, grondslag, uitzondering voor gezondheidsgegevens, beroepsgeheim en patiëntinformatie.
DPIA en proportionaliteit	Beoordeel DPIA-plicht vóór ingebruikname; toets noodzaak, alternatieven, modelverbetering en resterende risico's.
Contract en keten	Toepasselijke DPA en productvoorwaarden, licentie, subprocessors, onderzoek en doorgiften.
Inrichting en beheer	Individuele accounts, MFA-beleid, minimale rechten, apparaatbeheer, updates, logging en periodieke toegangscontrole.
Rechten en continuïteit	Geteste inzage-, correctie- en wisprocedure, EPD-export, uitvalscenario, incidentcontacten en contractuele meldafspraken.
Vrijgave en onderhoud	Besluit door de bevoegde instelling; herbeoordeling bij nieuwe functies, voorwaarden of gegevensstromen.

HIPAA, GDPR-ondersteuning of een leverancierscertificaat geven op zichzelf geen toestemming voor iedere toepassing. Laat ook de toepasselijke zorgwetgeving en eventuele AI-regelgeving voor de concrete functie beoordelen. Deze publicatie bevat geen individuele juridische vrijgave.

Bronnen en verder onderzoek

Raadpleegdatum 16 oktober 2026. Gebruik de actuele webbronnen voor besluitvorming en bewaar de toepasselijke contractversies in het eigen dossier. De aangeleverde Microsoft-PDF telt 975 pagina's; onderstaande paginanummers zijn de fysieke PDF-pagina's.

[1] Privacy white paper

https://learn.microsoft.com/en-us/industry/healthcare/dragon-copilot/whitepapers/privacy

§3–9; aangeleverde PDF p. 167–172. Webversie bijgewerkt 13 oktober 2026; PDF-hoofdstuk vermeldt 20 augustus 2026.

[2] Dragon Copilot FAQ

https://learn.microsoft.com/en-us/industry/healthcare/dragon-copilot/about/faqs

Bewaren, encryptie en auditstatus; webversie 27 juli 2026.

[3] Data collection white paper

https://learn.microsoft.com/en-us/industry/healthcare/dragon-copilot/whitepapers/data-collection

Required en Optional service data; webversie 13 oktober 2026.

[4] Privacy and Security Terms

https://www.microsoft.com/licensing/terms/en-US/product/PrivacyandSecurityTerms/all

Dragon Copilot data use, Core Online Services, data at rest en EU Data Boundary Services. Verifieer het eigen licentieprogramma.

[5] Security white paper

https://learn.microsoft.com/en-us/industry/healthcare/dragon-copilot/whitepapers/security

Security and controls en Customer responsibilities; PDF p. 173–180. Webversie 13 oktober 2026.

[6] Use cases white paper

https://learn.microsoft.com/en-us/industry/healthcare/dragon-copilot/whitepapers/use-cases

Customer responsibility for EHR filing; aangeleverde PDF p. 181.

[7] Transparency white paper

https://learn.microsoft.com/en-us/industry/healthcare/dragon-copilot/whitepapers/transparency

Menselijke controle, toestemming en beperkingen van AI.

[8] AP over gezondheidsgegevens

https://autoriteitpersoonsgegevens.nl/themas/gezondheid/gezondheidsgegevens-gebruiken-en-delen/gezondheidsgegevens-verwerken

Nederlandse toelichting op grondslagen; geen Belgische juridische beoordeling.

[9] AP over DPIA

https://autoriteitpersoonsgegevens.nl/themas/avg-privacy/praktisch-avg/data-protection-impact-assessment-dpia

Beoordeel hoog risico en de toepasselijke verplichte DPIA-lijst.

[10] Health and Life Sciences Subprocessor List

https://servicetrust.microsoft.com/DocumentPage/982cf921-f876-421a-b368-a18fd468ce67

Door privacywhitepaper aangewezen lijst. Actuele inhoud en versie opvragen en archiveren.

[11] EU Data Boundary overzicht

https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-learn

Reikwijdte en EU/EFTA; lees samen met productspecifieke voorwaarden.

[12] EU Data Boundary continuing transfers

https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-transfers-for-all-services

Algemene uitzonderingen, waaronder remote toegang en beveiligingsactiviteiten.

Aanvullend op te vragen: de contractueel toepasselijke Microsoft Products and Services DPA (https://aka.ms/DPA), productspecifieke licentievoorwaarden en auditstukken uit het Service Trust Portal. Deze verwijzingen zijn opvraagpunten; een toepasselijke DPA-versie is hier niet inhoudelijk gevalideerd.