

ICTRECHT

FACTSHEET

Microsoft Copilot veilig en verantwoord gebruiken binnen jouw organisatie

Stand van zaken: november 2026. AI-aanbieders passen hun diensten en voorwaarden regelmatig aan; controleer daarom altijd de actuele voorwaarden en instellingen van Microsoft.

Hoe zet je Copilot veilig in als organisatie?

Microsoft Copilot veilig gebruiken binnen je organisatie is mogelijk, ook als er persoonsgegevens in je werk voorkomen. Specifieke wetgeving, zoals de AVG en de AI Act, verbiedt AI niet, maar stelt wel voorwaarden. Ken je die voorwaarden en leg je ze vast, dan haal je de voordelen van Copilot binnen zonder onnodige risico's.

Copilot zit in de Microsoft 365-omgeving die veel organisaties al gebruiken. Dat maakt de drempel laag, maar het vraagt ook om aandacht: Copilot kan relevante informatie gebruiken binnen de rechten en beleidsbeperkingen van een medewerker. Sinds augustus 2026 heet de Microsoft 365 Copilot-app Microsoft Copilot. De betaalde licentie heet nog Microsoft 365 Copilot; in de app zie je het label 'M365 Copilot (Premium)' of 'Copilot Chat (Basic)'. Dezelfde app wordt ook gebruikt met persoonlijke Microsoft-accounts. In deze factsheet bedoelen we met Copilot de zakelijke versies.

Bij ICTRecht gebruiken we AI zelf dagelijks. We hebben de spelregels voor onze eigen praktijk uitgezocht en vertaald naar tools die ook jij direct kunt gebruiken, zoals onze kennisbank in Microsoft Copilot. Zo profiteer je van onze expertise. In deze factsheet beantwoorden we de meest gestelde vragen over Copilot en beveiliging: van datatoegang en privacy tot beleid en doorlopend verantwoord gebruik. Zodat je weet wat je moet regelen, en in welke volgorde.



In het kort:
zeven spelregels

Op basis van onze analyse van de voorwaarden, de instellingen en de beveiliging van Microsoft komen wij tot zeven spelregels:

1. Gebruik alleen je werkaccount.

Alleen als medewerkers inloggen met hun werk- of schoolaccount (Microsoft Entra ID) geldt de zakelijke gegevensbescherming van Microsoft. Je gegevens worden dan niet gebruikt om de onderliggende AI-modellen te trainen.

2. Leg vast wie waarvoor verantwoordelijk is.

Jouw organisatie bepaalt wat er met de gegevens gebeurt; Microsoft treedt voor de gedekte klantgegevens op als verwerker. Dat staat in de verwerkersovereenkomst van Microsoft, die bij zakelijke Microsoft 365-diensten automatisch geldt.

3. Wees je bewust van waar je data naartoe stroomt.

Copilot valt onder de EU Data Boundary van Microsoft, maar er zijn uitzonderingen: zoekopdrachten op het web via Bing, AI-modellen van Anthropic en verwerking buiten de EU bij drukte (flex routing). Sinds april 2026 staat flex routing voor de meeste Europese organisaties standaard aan. Ook de modellen van Anthropic in Word, Excel en PowerPoint, die in de VS worden gehost, kunnen standaard aanstaan. Controleer deze instellingen daarom actief. Gaan gegevens buiten de EU, dan geldt het modelcontract van de Europese Commissie, dat in de verwerkersovereenkomst van Microsoft staat.

4. Maak duidelijke interne afspraken over gegevens en toegang.

Bepaal welke gegevens wel en niet in Copilot mogen, controleer wie toegang heeft tot welke bestanden en beoordeel of een DPIA nodig is: een risicoanalyse voor privacy.

5. Laat altijd een mens meekijken.

Een deskundige medewerker controleert elke uitkomst voordat die wordt gebruikt.

6. Investeer in AI-geletterdheid.

Het vermogen van je medewerkers om AI te begrijpen en verantwoord te gebruiken. De AI Act verplicht organisaties maatregelen te nemen die AI-geletterdheid ondersteunen. Vastleggen is niet verplicht, maar wel verstandig.

7. Respecteer het auteursrecht.

Voer niet zomaar teksten, beelden of code van anderen in. Controleer eerst of je de juiste gebruiksrechten hebt, en besef dat je op uitkomsten van Copilot waarschijnlijk zelf geen auteursrecht hebt.

Hieronder lichten we elke spelregel toe, en lees je wat Microsoft regelt en wat jouw organisatie zelf moet doen.



Welke regels gelden er?

Als je Copilot gebruikt, zijn vooral de AVG, de AI Act en het auteursrecht belangrijk. De AVG beschermt de persoonsgegevens die Copilot verwerkt: wat je invoert, maar ook de mails, documenten en chats die Copilot erbij zoekt. De AI Act stelt eisen aan AI-systemen en aan de manier waarop je ze inzet. Het auteursrecht bepaalt wat je in Copilot mag invoeren en wat je met de uitkomst mag doen.

Voor de AVG en de AI Act geldt hetzelfde uitgangspunt: Microsoft biedt contractuele en technische waarborgen, maar jouw organisatie bepaalt waarvoor en hoe je Copilot gebruikt. De eindverantwoordelijkheid ligt daarom bij jou. Copilot werkt met AI-modellen van onder meer OpenAI en Anthropic. Die makers hebben daarnaast eigen verplichtingen onder de AI Act.

De basis: welke vorm van Copilot kies je?

Copilot is er in verschillende vormen. Begin bij de vraag hoe je organisatie Copilot gaat gebruiken, want dat bepaalt welke afspraken gelden en welke gegevens Copilot kan gebruiken. Daarna kies je de juiste licentie en instellingen.

Hoe gebruik je Copilot?

Copilot met een persoonlijk account

De Copilot-app of website met een privé-Microsoft-account. Dit is een consumentenproduct, zonder verwerkersovereenkomst. Gesprekken kunnen worden gebruikt om AI-modellen te trainen, tenzij de gebruiker dat uitzet, en worden standaard 18 maanden bewaard. Dat geldt ook in Europa. Copilot in Word, Excel en PowerPoint met een Microsoft 365 Personal-, Family- of Premium-abonnement wordt niet voor training gebruikt, maar valt wel onder de consumentenvoorwaarden.

Microsoft Copilot Chat

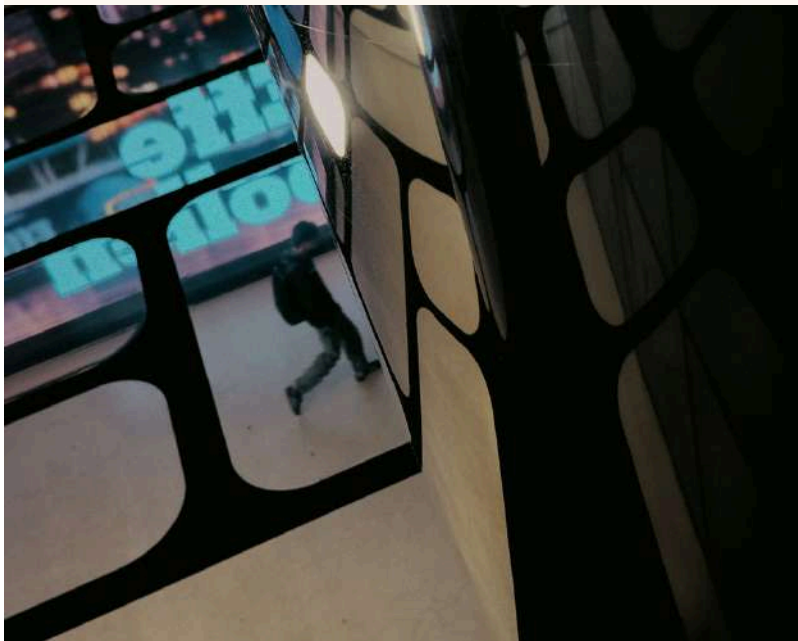
Inbegrepen bij zakelijke Microsoft 365-licenties. Antwoorden zijn vooral gebaseerd op het web en op bestanden die je zelf toevoegt. Sinds 15 april 2026 zit Copilot Chat in grotere organisaties niet meer in Word, Excel, PowerPoint en OneNote. Met een werkaccount geldt de zakelijke gegevensbescherming.

Microsoft Copilot (betaalde licentie)

Werkt in Word, Excel, PowerPoint, Outlook en Teams en zoekt automatisch in je organisatiegegevens via Microsoft Graph: mail, bestanden, chats en agenda. Copilot ziet alles waar de gebruiker toegang toe heeft. Je koopt dit als aanvulling op een zakelijke Microsoft 365-licentie (Microsoft 365 Copilot). Dit kan ook als Microsoft 365 Copilot Business voor organisaties tot 300 gebruikers, of als onderdeel van het pakket Microsoft 365 E7.

Agents en Copilot Studio

Eigen assistenten en koppelingen met andere systemen. Voor agents van andere aanbieders gelden hun eigen voorwaarden. Beheerders bepalen welke agents zijn toegestaan.



	Afspraken over je gegevens	Training van AI-modellen	Gebruik van organisatiegegevens
Persoonlijk account Copilot-app of website, privé-inlog	**Consumentenvoorwaarden** Geen verwerkersovereenkomst	**Ja, tenzij uitgezet** Gebruiker moet zelf afmelden	**Niet bedoeld voor werk** Buiten zicht van de organisatie
Copilot Chat Inbegrepen bij zakelijke licenties	**Zakelijke bescherming** Verwerkersovereenkomst van Microsoft	**Nee** Prompts en antwoorden blijven buiten training	**Alleen wat je zelf toevoegt** Antwoorden vooral op basis van het web
Microsoft Copilot Betaalde licentie, voorheen Microsoft 365 Copilot	**Zakelijke bescherming** Verwerkersovereenkomst van Microsoft	**Nee** Ook niet met gegevens uit Microsoft 365	**Automatisch, via Microsoft Graph** Alles waar de gebruiker toegang toe heeft
Agents en Copilot Studio Eigen assistenten en koppelingen	**Afhankelijk van de agent** Agents van derden: eigen voorwaarden	**Afhankelijk van de agent** Controleer de voorwaarden per agent	**Eigen bronnen en systemen** Beheerder bepaalt wat is toegestaan

Welke vorm van Copilot gebruik je, en wat betekent dat voor je gegevens? Alleen met een werkaccount geldt de zakelijke gegevensbescherming van Microsoft.

- Zakelijk geregeld
- Let op: zelf inrichten
- Niet geschikt voor werk
- Niet bedoeld voor werk



Welk account kies je?

Naast de licentie is het account waarmee medewerkers inloggen bepalend. Microsoft hanteert twee verschillende niveaus van gegevensbescherming. Alleen het werkaccount is geschikt voor gebruik binnen een organisatie.

	Persoonlijk Microsoft-account	Werkaccount (Copilot Chat en Microsoft Copilot)
Afspraken over je gegevens	Consumentenvoorwaarden en privacyverklaring van Microsoft	Productvoorwaarden en verwerkersovereenkomst van Microsoft
Wordt het AI-model getraind met je gegevens?	Nee voor prompts, antwoorden en bestanden in de vernieuwde Copilot-ervaring. Controleer oudere versies	Nee; ook niet met gegevens uit Microsoft 365
Hoe lang worden gegevens bewaard?	Volgens de actuele ervaring en instellingen; de gebruiker kan de geschiedenis beheren	Volgens toepasselijk ingericht beleid; Copilot Memory vereist afzonderlijk beheer. Gebruik Purview voor daadwerkelijk inzicht
Bescherming tegen auteursrechtclaims	Geen	Bij gedekte zakelijke Copilot-diensten staat Microsoft je onder voorwaarden bij
Grip voor de organisatie	Geen centraal organisatiebeheer	Beheer van gebruikers, instellingen, agents, bewaartermijnen en eDiscovery (laatste is licentie-afhankelijk)

Een medewerker die werkinformatie in een privé-account invoert, deelt die gegevens zonder de bescherming van een zakelijk contract. Voor persoonsgegevens is dat in de regel niet toegestaan. Let op: in apps als Outlook, Teams en de Copilot-app kun je met beide soorten accounts inloggen.

> **Advies van ICTRecht:** leg in je AI-beleid vast dat werk alleen via het werkaccount loopt, en communiceer dit actief. Beheerders kunnen het inloggen met persoonlijke accounts beperken. Schaduw-AI (het gebruik van AI-tools buiten de controle en machtigingen van de organisatie) is in de praktijk een belangrijk beheersrisico.
>
> **Onze aanbevolen opzet voor gevoelige gegevens:** gebruik Copilot alleen met werkaccounts, ruim eerst te ruim gedeelde mappen en sites op en controleer drie instellingen in het beheercentrum: zoekopdrachten op het web, de modellen van Anthropic en flex routing. Zet ze uit waar dat nodig is. Dan blijft de verwerking binnen de EU Data Boundary. Let op: voor de modellen van Anthropic zijn er meerdere opties en flex routing voor Copilot Studio staat ook in het beheercentrum van Power Platform. Indien Anthropic als subverwerker fungeert valt dit onder Microsoft-afspraken, maar de aparte opt-in Anthropic models with Data Retention gebruikt Anthropic als zelfstandige verwerker onder eigen afspraken.

Copilot en de AVG

Met een werkaccount kun je Copilot gebruiken in lijn met de AVG. Microsoft regelt de contractuele en technische waarborgen. Jouw organisatie blijft verantwoordelijk voor zorgvuldig gebruik, en bij Copilot hoort daar vooral het beheer van toegangsrechten bij.

Onderwerp	Wat Microsoft regelt	Wat jij regelt
Gebruik van je gegevens	Gebruikt prompts, antwoorden en gegevens uit Microsoft 365 niet om de onderliggende AI-modellen te trainen	Leg per toepassing vast waarvoor je Copilot gebruikt en waarom dat mag
Verwerkersovereenkomst	Zit automatisch in de zakelijke voorwaarden; Microsoft treedt op als verwerker	Controleer of de overeenkomst geldt en bekijk welke andere partijen Microsoft inschakelt, zoals Anthropic
Toegang tot gegevens	Copilot toont alleen informatie waar de gebruiker minimaal leesrechten op heeft	Controleer en beperk te ruim gedeelde sites, mappen en Teams-kanalen, en gebruik gevoeligheidslabels
Gegevens buiten de EU	EU Data Boundary en het modelcontract van de Europese Commissie in de verwerkersovereenkomst; uitzonderingen voor webzoekopdrachten, Anthropic-modellen en flex routing	Bepaal per uitzondering of je die toestaat en leg die keuze vast
Beveiliging	Versleuteling bij opslag en transport, scheiding per organisatie en internationaal gecertificeerd	Beheer accounts, toegangsrechten en gevoeligheidslabels goed
Bewaren en verwijderen	Copilot-gesprekken worden versleuteld opgeslagen bij je overige Microsoft 365-gegevens	Stel een bewaarbeleid in via Microsoft Purview
Vragen van betrokkenen	Copilot-gesprekken zijn doorzoekbaar via de zoek- en eDiscovery-functies van Microsoft 365	Richt een vaste werkwijze in voor inzage- en verwijderverzoeken
Datalekken	Afspraken over het melden van incidenten in de verwerkersovereenkomst	Neem Copilot op in je eigen datalekprocedure
Risicoanalyse (DPIA)	Documentatie en auditrapporten beschikbaar via het Service Trust Portal	Beoordeel of een DPIA nodig is en voer die zo nodig uit.

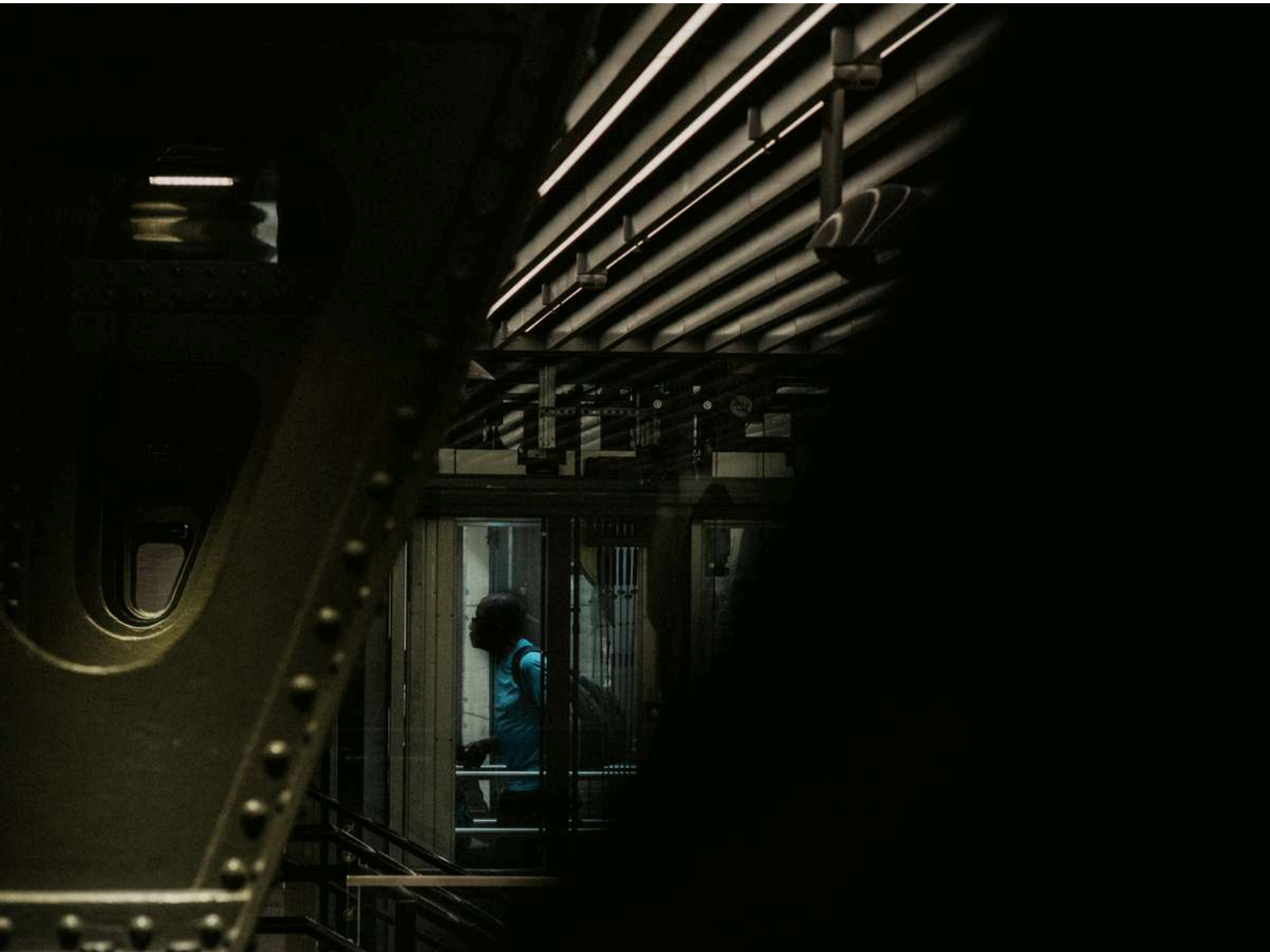


Zoekopdrachten op het web. Als Copilot het web raadpleegt, stuurt het een korte zoekopdracht naar Bing, zonder gebruikers- en organisatie-ID's. De zoekopdracht zelf kan wel woorden uit je prompt bevatten. Bing valt niet onder de verwerkersovereenkomst; Microsoft is daar zelf verantwoordelijk voor de gegevens. Beheerders kunnen het zoeken op het web uitzetten.

Gevoelige gegevens en geheimhouding. Gegevens over bijvoorbeeld gezondheid of strafrechtelijke zaken vragen extra voorzichtigheid. Hetzelfde geldt voor informatie waarover je geheimhouding hebt afgesproken. Omdat Copilot zelf in je mail en documenten zoekt, vraagt goed toegangsbeheer bijzondere aandacht.

Wat zeggen SURF en de Rijksoverheid? In opdracht van SURF en SLM Rijk is een DPIA uitgevoerd op Microsoft 365 Copilot. De vier eerder gevonden hoge risico's zijn in september 2025 weggenomen of verlaagd. Volgens de update van mei 2026 is verantwoord gebruik mogelijk, maar blijven twee middelhoge risico's over, namelijk het tot 18 maanden bewaren van diagnostische gegevens door Microsoft en het 'Workplace Harms'-filter, dat organisaties niet kunnen inzien of aanpassen. Organisaties moeten zelf beslissen of ze die risico's accepteren.

> **Advies van ICTRecht:** deel gegevens op in drie groepen: mag erin, mag erin na anonimiseren, en mag er niet in. Ruim daarnaast de toegangsrechten op voordat je Copilot-licenties uitdeelt. Gebruik je Copilot voor beslissingen over mensen of voor veel persoonsgegevens, voer dan een DPIA uit. De DPIA van SURF en SLM Rijk is daarvoor een goed vertrekpunt.



Copilot en de AI Act

De AI Act verdeelt de verantwoordelijkheid tussen de makers van AI-modellen en de organisaties die ze gebruiken. Voor gangbaar gebruik, zoals schrijven, samenvatten en analyseren, zijn jouw verplichtingen beperkt en goed uit te voeren.

Wat Microsoft en de modelmakers moeten doen

Sinds augustus 2025 moeten de makers van AI-modellen onder meer vastleggen hoe hun model werkt, een auteursrechtbeleid voeren en openbaar maken op welke soorten data het model is getraind. Microsoft, OpenAI en Anthropic hebben de Europese gedragscode voor AI-modellen ondertekend. Daarnaast zijn Microsoft Copilot en Copilot Chat gecertificeerd volgens ISO 42001, de internationale norm voor verantwoord AI-beheer. Deze verplichtingen liggen bij Microsoft en de modelmakers, niet bij jou.

Transparantie

Microsoft legt openbaar uit hoe Copilot werkt. Per dienst publiceert Microsoft documentatie over de werking, de beperkingen en verantwoord gebruik, en in antwoorden toont Copilot waar mogelijk de bronnen waarop het zich baseert. Zo kun je nagaan wat je inzet en dat vastleggen in je eigen AI-beleid.

> **Advies van ICTRecht:** breng per afdeling in kaart waarvoor Copilot wordt gebruikt, en toets elke toepassing aan de risicocategorieën van de AI Act. Zo zie je op tijd of een toepassing onder de strengere regels valt, en voorkom je verrassingen in 2027.

Wanneer gaat wat in?
Bekijk de AI Act-roadmap van ICTRecht voor een overzicht van alle mijlpalen.

Wat jouw organisatie moet doen

- **Zorg voor AI-geletterdheid.**
  Medewerkers die met Copilot werken, moeten weten wat het kan, waar de grenzen liggen en welke regels gelden. Sinds februari 2025 moet je daar maatregelen voor nemen. Leg vast welke training en voorlichting je hebt gegeven, zodat je dat kunt aantonen.

- **Vermijd verboden toepassingen.**
  Sinds februari 2025 zijn onder meer emotieherkenning op de werkvloer, het beoordelen van mensen op hun gedrag (social scoring) en manipulatieve technieken verboden. Zet Copilot daar nooit voor in.

- **Wees open over AI.**
  Sinds augustus 2026 moet je deepfakes in beeld, audio en video herkenbaar maken. Publiceer je met AI geschreven tekst om het publiek te informeren, vermeld dan dat AI is gebruikt, tenzij de tekst inhoudelijk door een mens is gecontroleerd en iemand er redactioneel verantwoordelijk voor is.

- **Let op bij beslissingen over mensen.**
  Gebruik je Copilot bij werving en selectie, het beoordelen van medewerkers of het bepalen van kredietwaardigheid, dan gelden vanaf 2 december 2027 extra strenge eisen. Copilot kan ook mails, chats en vergaderingen over medewerkers samenvatten. Gebruik dat niet om medewerkers te beoordelen zonder dat vooraf goed te toetsen.

Bouw je met Copilot Studio een eigen AI-toepassing die je aan anderen aanbiedt, dan word je mogelijk zelf aanbieder onder de AI Act. Je verplichtingen nemen dan flink toe.

Copilot en het auteursrecht

Voor veel ondernemers is het auteursrecht minstens zo belangrijk als privacy. Let op twee dingen:

- **Maak geen inbreuk.**

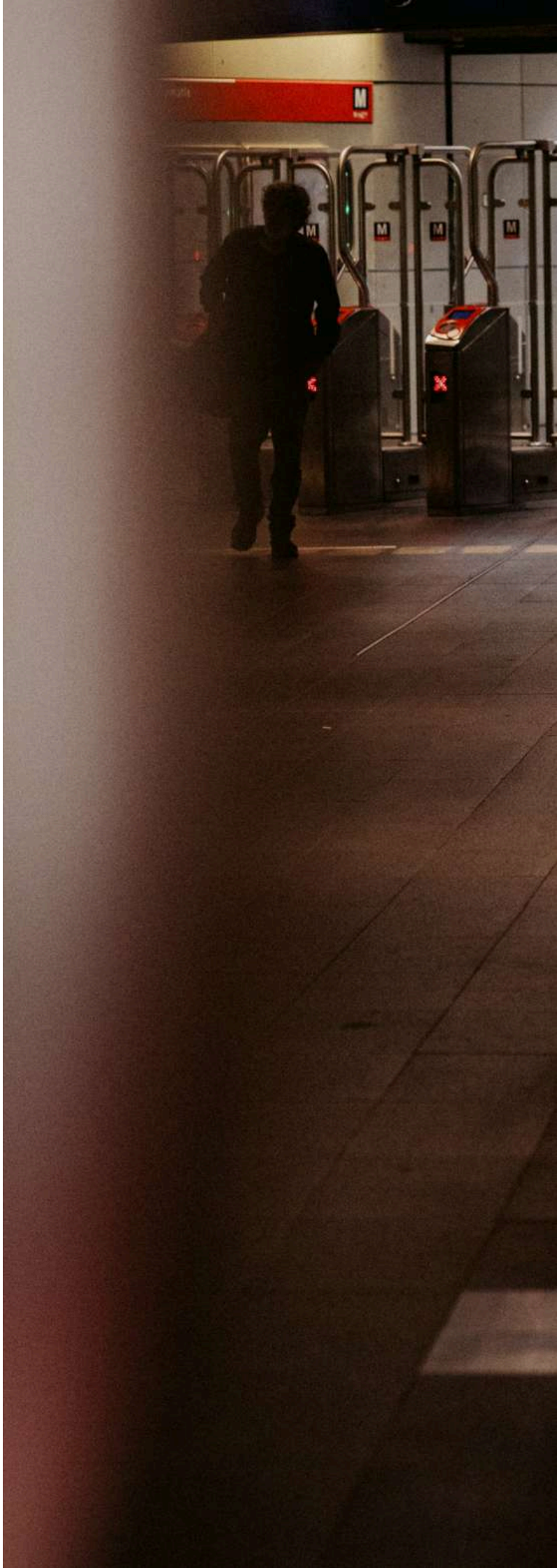
  Voer niet zomaar teksten, afbeeldingen of code van anderen in Copilot in. Controleer eerst of je daar voldoende gebruiksrechten voor hebt. Controleer ook of een uitkomst niet te veel lijkt op bestaand werk van een ander voordat je die publiceert.

- **Je hebt waarschijnlijk geen auteursrecht op de uitkomst.**

  Auteursrecht ontstaat alleen op werk met een eigen, creatieve inbreng van een mens. Een tekst of beeld die Copilot zonder menselijke creatieve bijdrage maakt is daarom meestal niet beschermd. Je kunt anderen dan in principe ook niet verbieden het te gebruiken.

Microsoft claimt zelf geen rechten op de uitkomsten van Copilot. Bij betaalde zakelijke Copilot-diensten staat Microsoft je bovendien bij als iemand claimt dat een uitkomst inbreuk maakt op zijn auteursrecht, mits je de ingebouwde filters gebruikt en niet bewust inbreuk probeert te maken. Vermijden dat je content van anderen zonder juiste gebruiksrechten invoert, draag al bij aan het voorkomen van mogelijk ‘bewuste’ inbreuk. Dit verandert verder niets aan de vraag of jij zelf auteursrecht hebt op de uitkomst.

> **Advies van ICTRecht:** maak afspraken over wat medewerkers in Copilot mogen invoeren en maak ze bewust van mogelijke auteursrechtinbreuken. Is een tekst of ontwerp belangrijk voor je bedrijf, zorg dan voor een duidelijke eigen creatieve inbreng, bijvoorbeeld door het resultaat te sturen met heel gedetailleerde prompts (of context) of door creatieve bewerkingen van het resultaat achteraf.



Beveiliging en certificeringen

Als organisatie kies je een leverancier die aantoonbaar goed omgaat met de beveiliging van jouw gegevens. Bij Microsoft onderbouw je die keuze met internationale certificeringen en onafhankelijke controles. De meeste gelden voor het Microsoft 365-platform als geheel, waar Copilot onder valt:

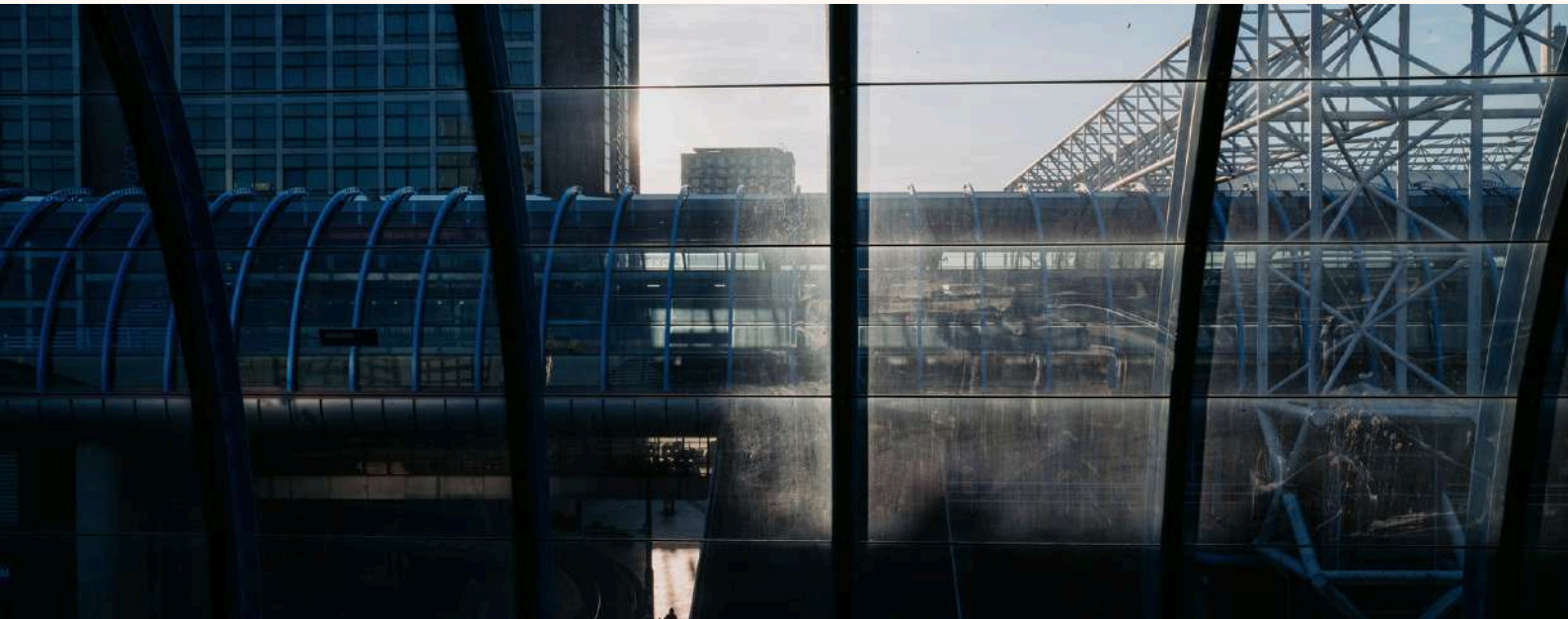
Norm of audit	Wat het betekent
ISO 27001	De informatiebeveiliging is ingericht volgens een internationale norm en wordt regelmatig door een externe partij gecontroleerd
ISO 27017 en 27018	Extra waarborgen voor beveiliging en privacy in de cloud
ISO 27701	Het privacybeheer is ingericht volgens een internationale norm
ISO 42001	AI wordt volgens een internationale norm verantwoord beheerd; Microsoft noemt Copilot en Copilot Chat hier uitdrukkelijk
SOC 1, 2 en 3	Een onafhankelijke auditor heeft de beveiliging over een langere periode getoetst.
C5	Duitse norm voor cloudbeveiliging van de federale dienst voor informatiebeveiliging (BSI)





Daarnaast versleutelt Microsoft de gegevens, zowel onderweg als in opslag, en zijn de gegevens van elke organisatie van elkaar gescheiden. Voor Copilot heeft Microsoft het meelezen door eigen medewerkers ter controle op misbruik uitgezet.

> **Advies van ICTRecht:** vraag de auditrapporten en certificaten op via het Service Trust Portal van Microsoft en bewaar ze bij je leveranciersgegevens. Zo kun je tegenover een toezichthouder of klant laten zien dat je zorgvuldig hebt gekozen.



Werken met agents, Copilot Studio en koppelingen

Copilot wordt krachtiger naarmate je het meer context geeft: eigen assistenten (agents), koppelingen met andere systemen en zelfgebouwde toepassingen in Copilot Studio. Elk van die uitbreidingen vraagt een eigen afweging.

- **Agents**

  Zijn assistenten voor een specifieke taak. Agents van Microsoft vallen onder dezelfde zakelijke voorwaarden. Voor agents van andere aanbieders gelden hun eigen voorwaarden en privacyverklaring. Beheerders bepalen welke agents zijn toegestaan.

- **Koppelingen (ook wel connectoren genoemd)**

  Halen gegevens uit andere systemen naar Copilot. Copilot toont die gegevens alleen aan gebruikers die er toegang toe hebben. Met de koppeling met de ICTRecht-kennisbank haal je onze actuele juridische kennis, rechtspraak en modeldocumenten direct in je eigen Copilot-omgeving.

- **Copilot Studio**

  Is een apart product om zelf agents te bouwen en aan te sluiten op andere gegevensbronnen. Hier gelden aanvullende instellingen in het beheercentrum van Power Platform. Daar bepaal je onder meer of gegevens de regio mogen verlaten, of Bing mag worden gebruikt en of flex routing is toegestaan. Agents in Copilot Studio kunnen ook modellen van Anthropic of eigen modellen uit Microsoft Foundry gebruiken; die vallen niet altijd onder de EU Data Boundary of de auteursrechtgarantie van Microsoft.

- **Microsoft Foundry (voorheen Azure AI Foundry)**

  Is het Azure-platform om zelf AI-toepassingen te bouwen met modellen via een API. Dit is geen Copilot en valt onder de Azure-voorwaarden. Maak onderscheid tussen modellen die Microsoft zelf levert, zoals de GPT-modellen van OpenAI, en modellen van partners, zoals Claude van Anthropic. Voor de eerste groep gelden de voorwaarden en de verwerkersovereenkomst van Microsoft. Voor partnermodellen gelden de voorwaarden van de maker; bij Claude is Anthropic zelf verwerker. Met het implementatietype kies je waar de verwerking plaatsvindt: wereldwijd (Global), binnen de EU (Data Zone EU) of in één regio. Microsoft kan prompts bewaren en laten beoordelen ter controle op misbruik, tenzij je daar een uitzondering voor krijgt.

- **Zelf geïnstalleerde en lokale modellen**

  Open modellen die je in je eigen Azure-omgeving uitrolt of lokaal draait, bijvoorbeeld met Foundry Local of de ingebouwde modellen op Copilot+ pc's, verwerken gegevens in je eigen omgeving of op het apparaat. Jij bent dan zelf verantwoordelijk voor beveiliging, logging en het naleven van de licentie van het model.

- **Andere Copilots**

  GitHub Copilot, Security Copilot en Copilot in Dynamics 365 zijn aparte producten met eigen licenties en voorwaarden. Beoordeel ze afzonderlijk.

> **Advies van ICTRecht:** laat beheerders bepalen welke agents en koppelingen beschikbaar zijn. Neem elke externe koppeling op in je overzicht van gegevensverwerkingen, en controleer of je met die partij een verwerkersovereenkomst nodig hebt. Geef Copilot alleen toegang tot de gegevens die nodig zijn voor de taak.

Meer weten over het verantwoord inzetten van AI-tools? Bekijk onze webinars.

Stappenplan: Copilot verantwoord invoeren

Wij adviseren organisaties om Copilot in acht stappen in te voeren. Zo staat de basis voordat medewerkers aan de slag gaan.

1. **Breng het gebruik in kaart.** Wie gebruikt Copilot al, met welk account en waarvoor? Vaak blijkt schaduw-AI al wijdverbreid.
2. **Werk alleen met werkaccounts.** Zorg dat medewerkers inloggen met hun werkaccount en beperk het gebruik van persoonlijke accounts.
3. **Ruim de toegangsrechten op.** Controleer voordat je licenties uitdeelt welke sites, mappen en Teams-kanalen te ruim gedeeld zijn, en label gevoelige documenten. Gebruik hiervoor Microsoft Purview.
4. **Controleer de leverancier en de instellingen.** Bekijk de verwerkersovereenkomst, de partijen die Microsoft inschakelt en de auditrapporten. Bepaal of je zoeken op het web, de modellen van Anthropic en flex routing toestaat. Denk ook aan externe modelleveranciers, memory, agents en Purview- dan wel cloudinstellingen.
5. **Beoordeel elke toepassing.** Bepaal per gebruik welke gegevens erin gaan, of een DPIA nodig is en of de toepassing onder de strengere regels van de AI Act valt.
6. **Stel een AI-beleid vast.** Leg vast welke gegevens wel en niet in Copilot mogen, dat passende menselijke controle plaatsvindt en wie agents en koppelingen beheert. Stel een bewaarbeleid in en werk je overzicht van gegevensverwerkingen en je datalekprocedure bij.
7. **Richt Copilot in voor jullie werk en train medewerkers.** Voeg betrouwbare agents en koppelingen toe, en organiseer AI-geletterdheid op maat van de functie. Hieronder lees je hoe je daarvoor de kennis van ICTRecht gebruikt.
8. **Evalueer regelmatig.** Volg wijzigingen in de voorwaarden en standaardinstellingen van Microsoft en in de wetgeving, en evalueer je beleid minstens één keer per jaar. Microsoft zet nieuwe functies soms standaard aan, zoals flex routing in april 2026 en de modellen van Anthropic in Word, Excel en PowerPoint in mei 2026.

Medewerkers die bij klanten werken, volgen daarnaast de AI-regels van die klant.

Werk slimmer met de kennis van ICTRecht

Of je nu werkt met Claude, Microsoft Copilot of ChatGPT: met ICTRecht haal je betrouwbare juridische kennis direct in je AI-tool. Geen losse zoekopdrachten of verouderde bronnen meer, maar antwoorden gebaseerd op actuele kennis, gevalideerd door onze juristen.

- **Koppeling met de ICTRecht-kennisbank:** onze actuele juridische kennis, modeldocumenten en rechtspraak, onder meer van rechtspraak.nl, direct in de AI-tool die je al gebruikt. Werkt met Claude, ChatGPT en Microsoft 365 Copilot. Koppel je AI-tool.
- **ICTRecht-skills:** werk volgens de vaste methodes van onze juristen, met rolprofielen voor onder meer privacy officer en bedrijfsjurist, en vaste structuren voor DPIA's, contractreviews en AI Act-checks. Nu beschikbaar voor Claude, binnenkort ook voor ChatGPT en Microsoft 365 Copilot. Vraag de gratis skill aan.
- **AI Pro Pack: alles in één veilige omgeving.** Je eigen AI-omgeving, ingericht en beheerd door ICTRecht. Je gegevens blijven in de EU, onder Nederlands recht, en worden nooit gebruikt om AI-modellen te trainen. Je kiest zelf tussen Claude, GPT of Mistral, met onbeperkte toegang tot al onze AI-assistenten, onze kennisbank en modelcontracten, plus een Word-plugin. Geen installatie, geen IT-project. Probeer het 14 dagen gratis.



FAQ: veelgestelde vragen

Vraag

Mogen we persoonsgegevens in Copilot invoeren?

Antwoord

Ja, met een werkaccount en voor een duidelijk doel. De verwerkersovereenkomst met Microsoft maakt dit mogelijk. Gevoelige gegevens en vertrouwelijke klantinformatie laat je er in de praktijk vaak buiten, tenzij je dat vooraf goed hebt afgewogen.

Vraag

Traint Microsoft zijn AI-modellen met onze gegevens?

Antwoord

Niet bij een werkaccount; prompts, antwoorden en gegevens uit Microsoft 365 worden niet gebruikt om de onderliggende AI-modellen te trainen. Ook de vernieuwde persoonlijke Copilot gebruikt gesprek- en bestandsinhoud niet voor training van basismodellen. Deze ervaring heeft consumentenvoorwaarden en geen gelijkwaardig centraal organisatiebeheer; volg daarom het werkaccountbeleid.

Vraag

Ziet Copilot alles in onze organisatie?

Antwoord

Nee, Copilot gebruikt alleen wat de ingelogde medewerker zelf mag zien. In de praktijk is dat vaak meer dan je denkt: een te ruim gedeelde map of site wordt met Copilot ineens makkelijk vindbaar. Ruim de toegangsrechten daarom op voordat je Copilot breed invoert.

Vraag

Microsoft is een Amerikaans bedrijf. Is dat een probleem?

Antwoord

Niet als het goed is geregeld. Copilot valt onder de EU Data Boundary, waardoor opslag en verwerking in principe binnen de EU blijven. Voor gegevens die toch buiten de EU gaan, geldt het modelcontract van de Europese Commissie in de verwerkersovereenkomst van Microsoft. Let wel op de uitzonderingen: webzoekopdrachten, de modellen van Anthropic en flex routing. Flex routing staat standaard aan. Deze uitzonderingen kun je als beheerder uitzetten.

Vraag

Hebben we een DPIA nodig?

Antwoord

Dat hangt af van het gebruik. Voor algemeen gebruik met duidelijke afspraken over gegevens en goed ingerichte toegangsrechten is het risico vaak beperkt. Verwerk je veel of gevoelige persoonsgegevens, of gebruik je Copilot bij beslissingen over mensen, dan is een DPIA meestal verplicht. De DPIA van SURF en SLM Rijk helpt je op weg.

Vraag

Vallen we onder de strenge regels van de AI Act?

Antwoord

Dat hangt af van de bestemming en invloed van de toepassing. Gebruik je Copilot bij werving en selectie, het beoordelen van medewerkers of andere beslissingen met grote gevolgen voor mensen, dan wel. Die regels gelden vanaf december 2027.

Vraag

Is Copilot veiliger dan andere AI-tools, omdat het in Microsoft 365 zit?

Antwoord

Niet vanzelf. Copilot valt onder dezelfde afspraken als de rest van Microsoft 365, en dat is een sterke basis. Maar Copilot maakt ook zichtbaar hoe goed je toegangsrechten op orde zijn, en sommige functies vallen buiten de EU Data Boundary. Kijk daarom altijd naar je eigen inrichting.

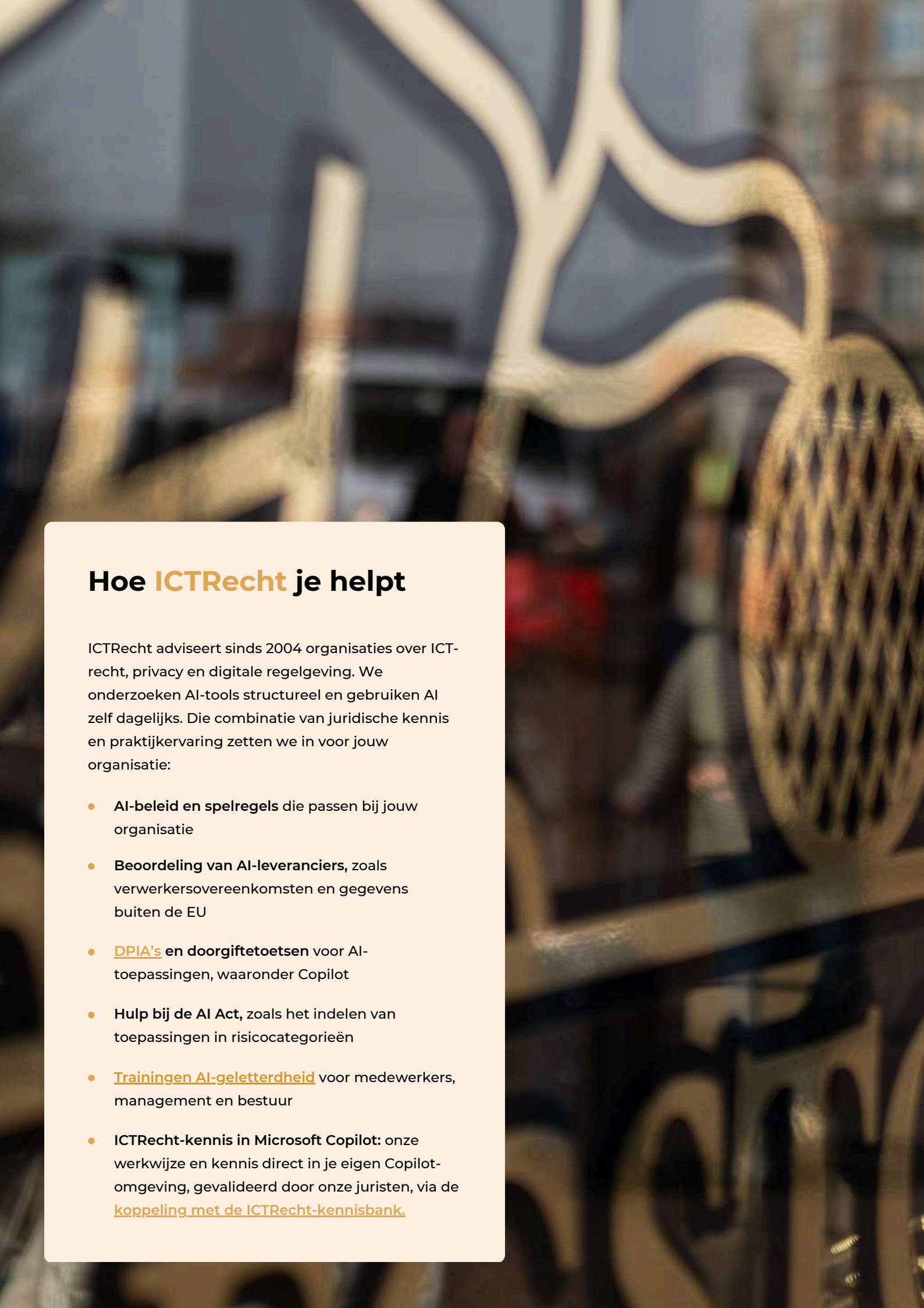
Vraag

Wie is verantwoordelijk voor fouten in de uitkomst?

Antwoord

Jouw organisatie blijft verantwoordelijk voor wat zij met de uitkomst doet. Menselijke controle is daarom geen formaliteit, maar noodzaak. Wel staat Microsoft klanten van gedekte zakelijke diensten onder voorwaarden bij als iemand claimt dat een uitkomst inbreuk maakt op zijn auteursrecht.

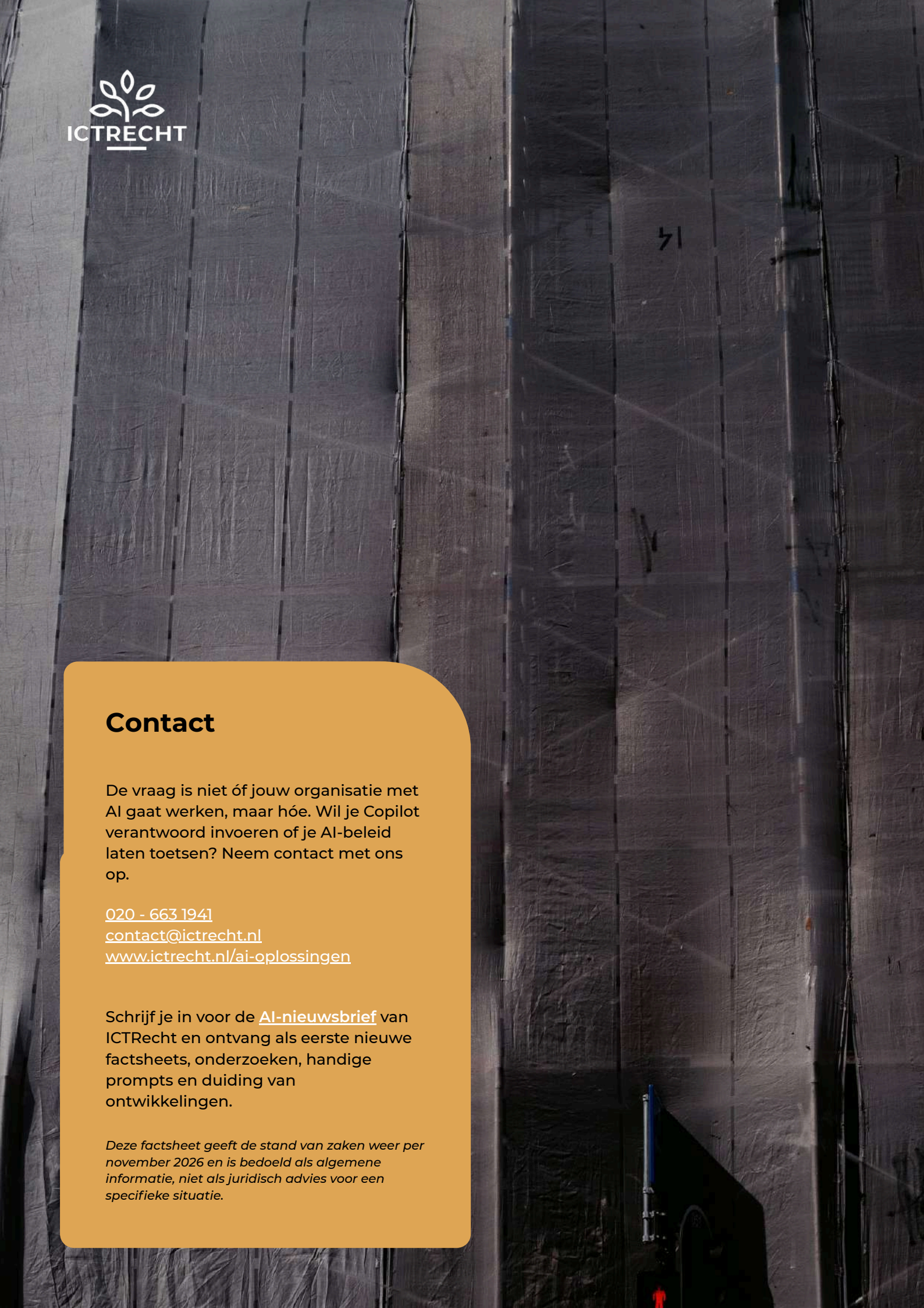




Hoe ICTRecht je helpt

ICTRecht adviseert sinds 2004 organisaties over ICT-recht, privacy en digitale regelgeving. We onderzoeken AI-tools structureel en gebruiken AI zelf dagelijks. Die combinatie van juridische kennis en praktijkervaring zetten we in voor jouw organisatie:

- **AI-beleid en spelregels** die passen bij jouw organisatie
- **Beoordeling van AI-leveranciers,** zoals verwerkersovereenkomsten en gegevens buiten de EU
- DPIA's **en doorgiftetoetsen** voor AI-toepassingen, waaronder Copilot
- **Hulp bij de AI Act,** zoals het indelen van toepassingen in risicocategorieën
- Trainingen AI-geletterdheid voor medewerkers, management en bestuur
- **ICTRecht-kennis in Microsoft Copilot:** onze werkwijze en kennis direct in je eigen Copilot-omgeving, gevalideerd door onze juristen, via de koppeling met de ICTRecht-kennisbank.



Contact

De vraag is niet óf jouw organisatie met AI gaat werken, maar hóe. Wil je Copilot verantwoord invoeren of je AI-beleid laten toetsen? Neem contact met ons op.

020 - 663 1941
contact@ictrecht.nl
www.ictrecht.nl/ai-oplossingen

Schrijf je in voor de AI-nieuwsbrief van ICTRecht en ontvang als eerste nieuwe factsheets, onderzoeken, handige prompts en duiding van ontwikkelingen.

Deze factsheet geeft de stand van zaken weer per november 2026 en is bedoeld als algemene informatie, niet als juridisch advies voor een specifieke situatie.