



Zo werk je veilig en verantwoord met Microsoft Copilot



Inhoud

Voorwoord	02
-----------	----

Inzichten

1	Copilot werkt pas goed als de basis klopt	04
2	De grootste winst zit niet in de technologie van Copilot, maar in de manier waarop mensen ermee werken	06
3	AI wordt steeds toegankelijker, governance wordt steeds belangrijker	08

Van inzicht naar raamwerk	09
---------------------------	----

Zelfreflectie	10
---------------	----

Spiegel	11
---------	----

Conclusie	12
-----------	----

Voorwoord

Van AI-experiment naar dagelijkse praktijk

Microsoft Copilot maakt AI toegankelijk voor een brede groep organisaties. Waar kunstmatige intelligentie voorheen vooral iets was voor specialisten, krijgt nu vrijwel iedere medewerker toegang tot een AI-assistent binnen de vertrouwde Microsoft 365-omgeving.

Die ontwikkeling biedt kansen voor productiviteit, kennisdeling en efficiënter werken. Tegelijkertijd laat de praktijk zien dat succesvolle inzet van Copilot niet begint bij de technologie zelf. Organisaties lopen vooral tegen vraagstukken aan rondom informatiebeheer, adoptie en governance.

Copilot maakt zichtbaar wat er al aanwezig is binnen een organisatie. Hoe goed zijn toegangsrechten ingericht? Hoe wordt informatie beheerd? En weten medewerkers hoe zij AI verantwoord kunnen gebruiken?

Juist daarom verschuift de aandacht. Niet de technologie staat centraal, maar de manier waarop organisaties AI organiseren, beveiligen en inzetten binnen hun dagelijkse processen.

In dit rapport delen we eerst drie inzichten die we steeds vaker terugzien bij organisaties die Copilot succesvol inzetten. Daarna vertalen we die inzichten naar een concreet raamwerk, een self-checklist en drie herkenbare profielen, zodat je zelf kunt bepalen waar jouw organisatie staat.



Dennis Wennekers, Technisch Business Consultant
KNNS

1 Copilot werkt pas goed als de basis klopt

Inzicht 1

Copilot werkt pas goed als de basis klopt

De inzet van Microsoft Copilot groeit snel. Tegelijkertijd maakt Copilot zichtbaar hoe goed de digitale basis van een organisatie daadwerkelijk is ingericht.

Copilot werkt namelijk met de informatie en toegangsrechten die al binnen Microsoft 365 aanwezig zijn. Daardoor worden bestaande uitdagingen rondom informatiebeheer, toegangsrechten en beveiliging direct zichtbaar.

Wat voorheen verborgen bleef in systemen en processen, krijgt met AI ineens een grotere impact. Opvallend daarbij is dat Copilot niet méér informatie toegankelijk maakt, maar bestaande toegang zichtbaarder maakt. De vraag is daardoor niet wat Copilot mag zien, maar wie binnen de organisatie al toegang heeft tot bepaalde informatie.

Organisaties die succesvol starten met Copilot zorgen daarom eerst voor een sterke basis:

- duidelijke toegangsrechten;
- goed informatiebeheer en eigenaarschap;
- compliance en DLP-beleid;
- inzicht in gevoelige informatie.

Technologieën zoals Microsoft Purview spelen daarbij een steeds grotere rol. Niet om AI te beperken, maar om deze verantwoord in zetbaar te maken.



2 De grootste winst zit niet in de AI-tool Copilot, maar in de manier waarop mensen werken

Inzicht 2

De grootste winst zit niet in de AI-tool Copilot, maar in de manier waarop mensen ermee werken

AI-functionaliteiten worden in hoog tempo onderdeel van de dagelijkse werkomgeving. Daardoor krijgen steeds meer organisaties toegang tot vergelijkbare technologie.

Het verschil ontstaat daardoor niet langer door de tool zelf, maar door de manier waarop medewerkers deze gebruiken.

Opvallend is dat organisaties Copilot steeds vaker zien als ondersteuning van kenniswerk, niet als vervanging van expertise. De grootste waarde ontstaat wanneer AI medewerkers helpt informatie sneller te verwerken, structureren en terug te vinden, terwijl inhoudelijke beoordeling bij mensen blijft liggen.

Succesvolle organisaties maken AI daarom tastbaar. Zij koppelen Copilot aan dagelijkse werkzaamheden, zoals het samenvatten van Teams-vergaderingen, het voorbereiden van afspraken of het opstellen van documenten.

Daarnaast groeit het belang van AI-vaardigheden. Medewerkers moeten leren hoe zij goede prompts schrijven, resultaten beoordelen en begrijpen waar de grenzen van AI liggen.

De grootste productiviteitswinst ontstaat daardoor niet door Copilot beschikbaar te maken, maar door medewerkers te leren hoe zij AI verantwoord en effectief inzetten.



3 Al wordt steeds toegankelijker, governance wordt steeds belangrijker.

Inzicht 3

AI wordt toegankelijker, governance belangrijker

Waar organisaties zich vandaag nog onderscheiden met AI-pilots en experimenten, wordt AI steeds meer een standaard onderdeel van de werkplek. AI-functionaliteiten worden toegankelijker, terwijl AI-agents en automatiseringen steeds vaker onderdeel worden van bestaande platformen.

Daardoor verschuift het onderscheidend vermogen. Niet de technologie zelf maakt het verschil, maar de manier waarop organisaties deze technologie organiseren, beveiligen en beheersen.

Tegelijkertijd zien we dat organisaties steeds vaker onderscheid maken tussen gecontroleerde en ongecontroleerde AI.

Binnen beheerde omgevingen zoals Microsoft Copilot blijven bestaande rechtenstructuren, beveiligingsmaatregelen en compliance-afspraken van kracht. Bij ongecontroleerde AI-oplossingen ontbreekt die grip vaak.

Juist daarom worden onderwerpen zoals governance, beleid en risicobeheersing steeds belangrijker.

Een voorbeeld hiervan is Shadow AI. Medewerkers gebruiken steeds vaker AI-oplossingen buiten de officiële organisatieomgeving. Denk aan privé AI-accounts of onbeheerde tools waarin bedrijfsinformatie wordt gedeeld zonder toezicht. Juist daarom worden governance, beleid en risicobeheersing steeds belangrijker.



Van inzicht naar raamwerk

De drie voorwaarden voor veilig Copilot-gebruik

De drie inzichten komen samen in drie concrete voorwaarden. Copilot werkt pas goed als ze alle drie op orde zijn, pas dan wordt Copilot een versneller in plaats van een risico. Elk inzicht vertaalt zich rechtstreeks naar één voorwaarde, en die drie vormen ook de structuur van de zelfreflectie hierna.

1. Een sterke basis: data & rechten

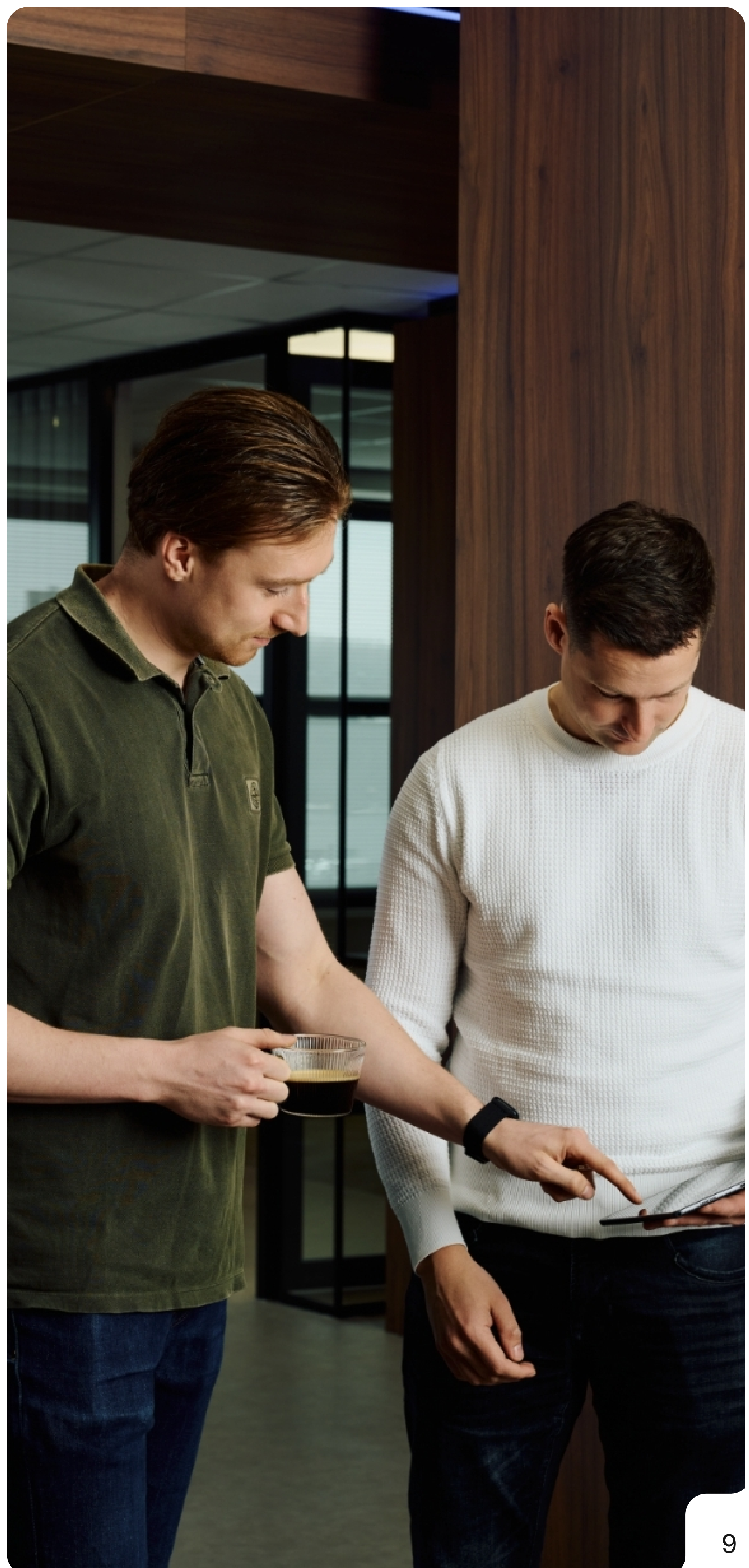
Voortbouwend op inzicht 1. Copilot maakt geen nieuwe informatie toegankelijk: het maakt bestaande toegang zichtbaar. De vraag is niet wát Copilot mag zien, maar wie binnen je organisatie al toegang heeft tot welke informatie. Heldere toegangsrechten, dataclassificatie en inzicht in gevoelige informatie zijn het fundament.

2. Betrokken medewerkers: adoptie & gedrag

Voortbouwend op inzicht 2. De grootste winst zit niet in de tool, maar in de manier waarop mensen ermee werken. Een licentie is geen gebruik, en gebruik is geen veilig gebruik. Training, interne voorbeelden en een aanspreekpunt maken het verschil tussen ad-hoc gebruik en bewuste inzet.

3. Duidelijke kaders: beleid, governance & monitoring

Voortbouwend op inzicht 3. Techniek zonder kaders leidt tot gedogen. Een vastgelegd AI-beleid maakt duidelijk wat wel en niet mag, wie eigenaar is en hoe je voldoet aan AVG en NIS2. En omdat beleid zonder regie een gebed zonder eind is, hoort monitoring hier onlosmakelijk bij: zien of gevoelige informatie naar buiten kan stromen, en weten wie handelt als er een incident is. Beleid is geen rem: het is de stuurinrichting die veilige versnelling mogelijk maakt.



Zelfreflectie

Zes vragen voor besluitvormers

Deze zes vragen, twee per voorwaarde, helpen je je eigen organisatie te herkennen. Ze zijn zo geformuleerd dat je merkt waar je het antwoord wél en waar je het níet met zekerheid hebt. Dat bewustzijn is de waarde, niet het antwoord. De vragen die je niet met zekerheid kunt beantwoorden, zijn je prioriteiten. Een volledige, diepgaande diagnose volgt in de AI Readiness Check.

1. Een sterke basis: data & rechten

- Weet je welke medewerkers toegang hebben tot welke bestanden in je Microsoft 365-omgeving?
- Weet je welke data Copilot straks te zien krijgt op basis van de huidige rechtenstructuur?

2. Betrokken medewerkers: adoptie & gedrag

- Hebben je medewerkers training gehad over veilig en effectief gebruik van Copilot?
- Weet elke medewerker wat hij of zij wel en niet mag invoeren in Copilot?

3. Duidelijke kaders: beleid, governance & monitoring

- Heeft je organisatie een vastgelegd AI-beleid en een aangewezen eigenaar voor governance?
- Weet je of gevoelige informatie via Copilot naar buiten kan stromen en wie handelt bij een incident?



Spiegel

De drie profielen. Waar staat jouw organisatie?

De drie inzichten komen samen in drie concrete voorwaarden. Copilot werkt pas goed als ze alle drie op orde zijn, pas dan wordt Copilot een versneller in plaats van een risico. Elk inzicht vertaalt zich rechtstreeks naar één voorwaarde, en die drie vormen ook de structuur van de zelfreflectie hierna.

• Startend

0 - 2 vragen met een helder antwoord

Je organisatie heeft Copilot nog niet structureel ingericht. Dat is geen tekortkoming, het is het startpunt. Prioriteit: eerst het fundament, dan beleid, dan adoptie. Een AI Readiness Check brengt in kaart wat je eerste concrete stap is.

• Groeiend

3- 4 vragen met een helder antwoord

Je hebt een basis gelegd, maar loopt aan tegen de grenzen van ad-hoc governance. Beleid bestaat, maar is niet volledig geïmplementeerd. Prioriteit: blinde vlekken dichten op rechten, monitoring en eigenaarschap.

• Volwassen

5 - 6 vragen met een helder antwoord

Je organisatie heeft een solide basis. De vraag is of je governance gelijke tred houdt met het groeiende gebruik. Een AI Readiness Check bevestigt wat staat en scherpt aan wat beter kan.

Let op: dit profiel is geen score. Het is een spiegel. De waarde zit in de vragen die je niet met zekerheid kunt beantwoorden, dat zijn je prioriteiten.



Conclusie

Copilot levert pas waarde als de organisatie er klaar voor is

Microsoft Copilot maakt AI toegankelijk voor een brede groep organisaties. Daarmee verschuift de aandacht van technologie zelf naar de manier waarop organisaties deze inzetten.

Wat daarbij opvalt, is dat de grootste uitdagingen niet liggen de mogelijkheden van Copilot, maar in de voorwaarden voor succesvol gebruik. Een sterke digitale basis blijft essentieel om informatie veilig en verantwoord toegankelijk te maken. Tegelijkertijd ontstaat de grootste waarde wanneer medewerkers begrijpen hoe zij AI kunnen inzetten binnen hun dagelijkse werkzaamheden.

Naarmate AI een vanzelfsprekend onderdeel wordt van de werkplek, groeit ook het belang van governance. Organisaties moeten niet alleen bepalen wat technisch mogelijk is, maar ook hoe zij grip houden op gebruik, risico's en verantwoordelijkheden.

Veilig en verantwoord werken met Copilot vraagt daarom om meer dan technologie alleen. Het vraagt om een combinatie van een sterke basis, betrokken medewerkers en duidelijke kaders voor gebruik. Organisaties die daarin investeren, leggen niet alleen de

De logische vervolgstap

Wil je je situatie concreet in kaart brengen? De AI Readiness Check is een laagdrempelig, strategisch startpunt. Geen audit, geen verkooppraatje, maar een volwassenheidsscan die laat zien waar je staat en hoe je veilig kunt versnellen.

Bekijk hier de AI Readiness Check

