Copilot voor Microsoft 365: Een kans voor productiviteit of een risico voor je data?

DOOR JUSTINE WOLTERS

JUSTINE WOLTERS

Data Security Consultant @ Cloud Life

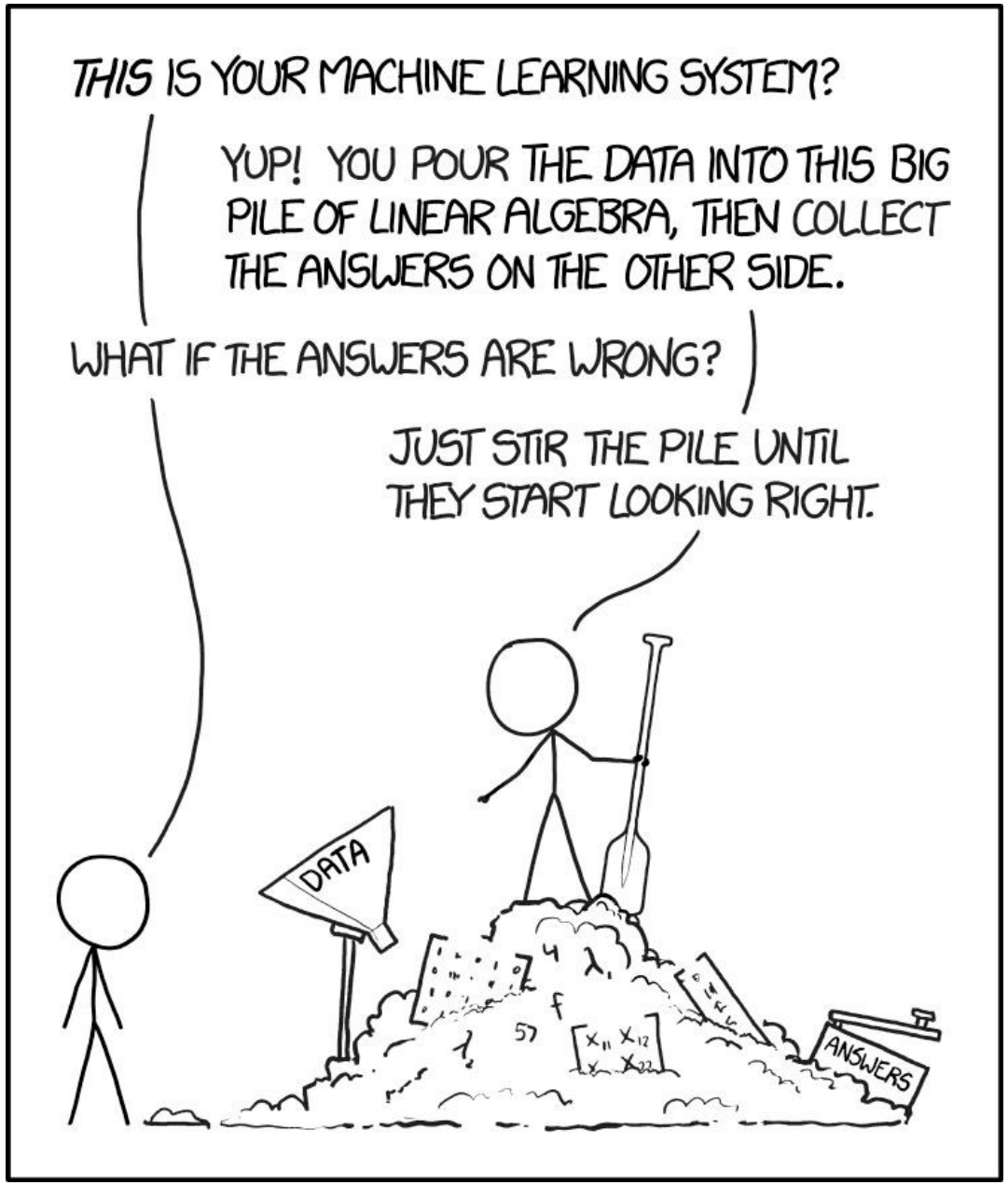
Ambassadeur Dutch Women in Tech (DWIT)


Denemarken & LEGO


Reizen met T3-
Tommie

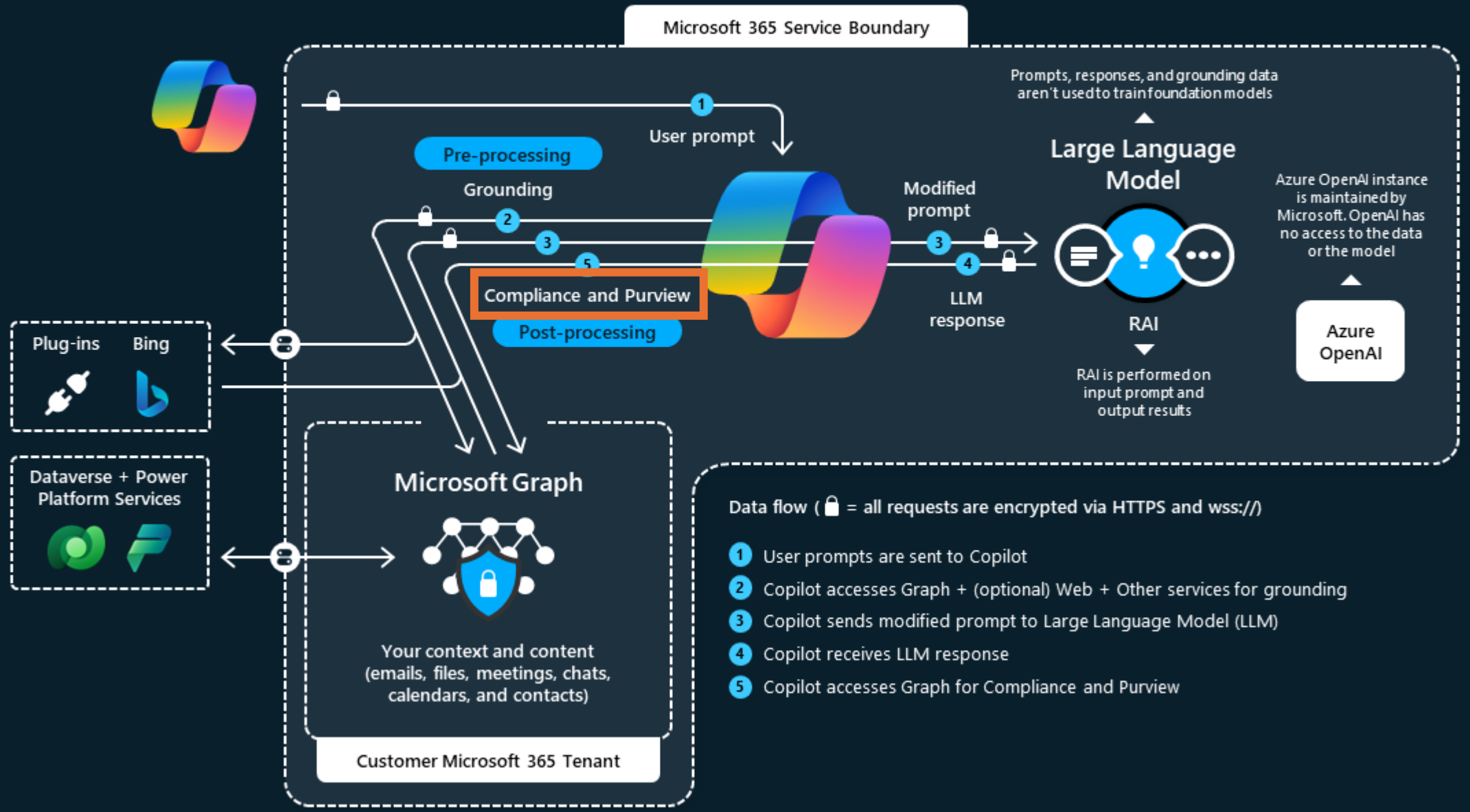
Agenda

- Copilot ecosystem
- Waarom data security?
- Stappenplan + demo's
- Issues along the way
- Takeaways

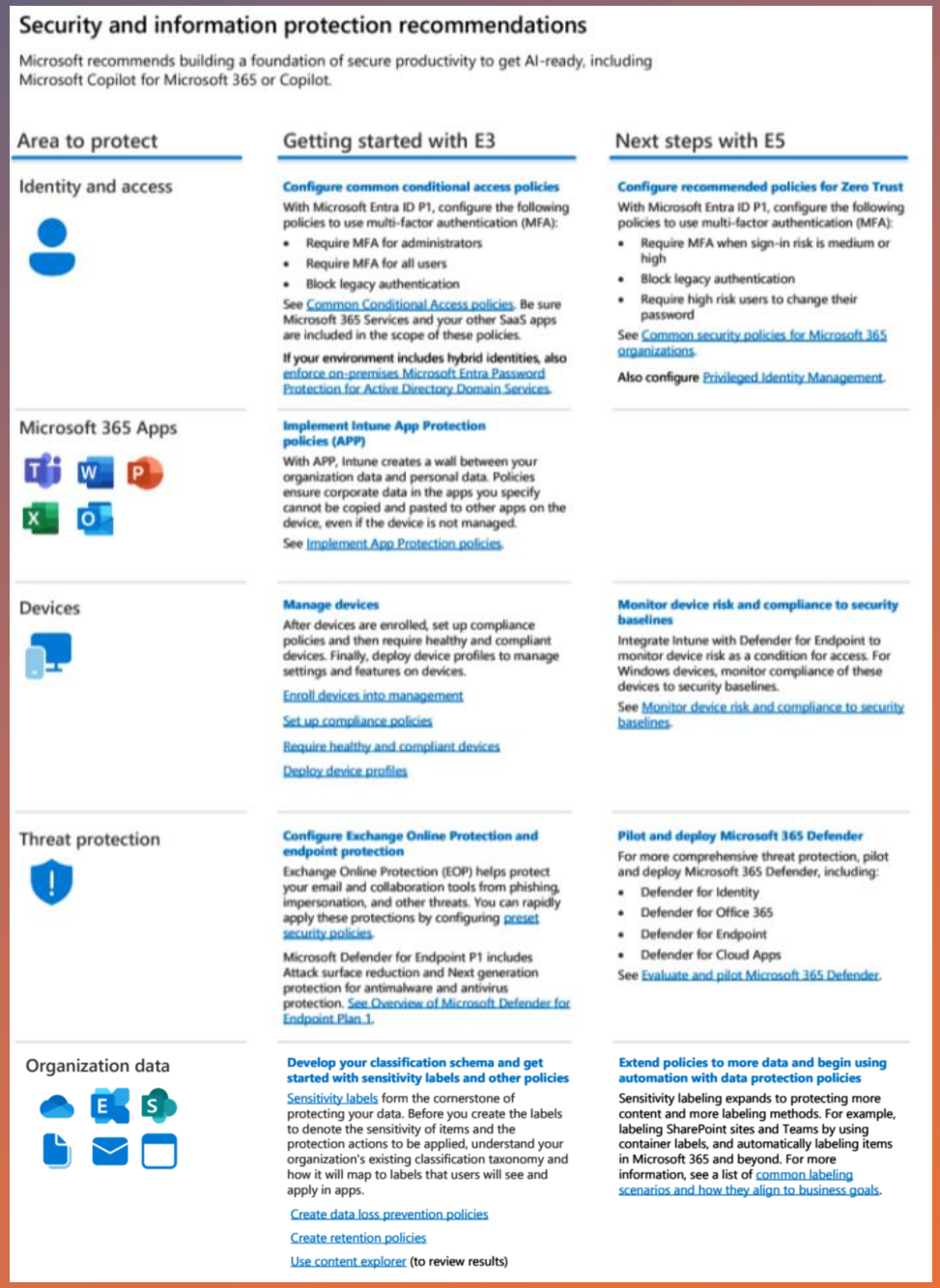


Bron: https://xkcd.com/1838/

Microsoft Copilot for Microsoft 365 architecture



How to make your workplace Copilot secure?

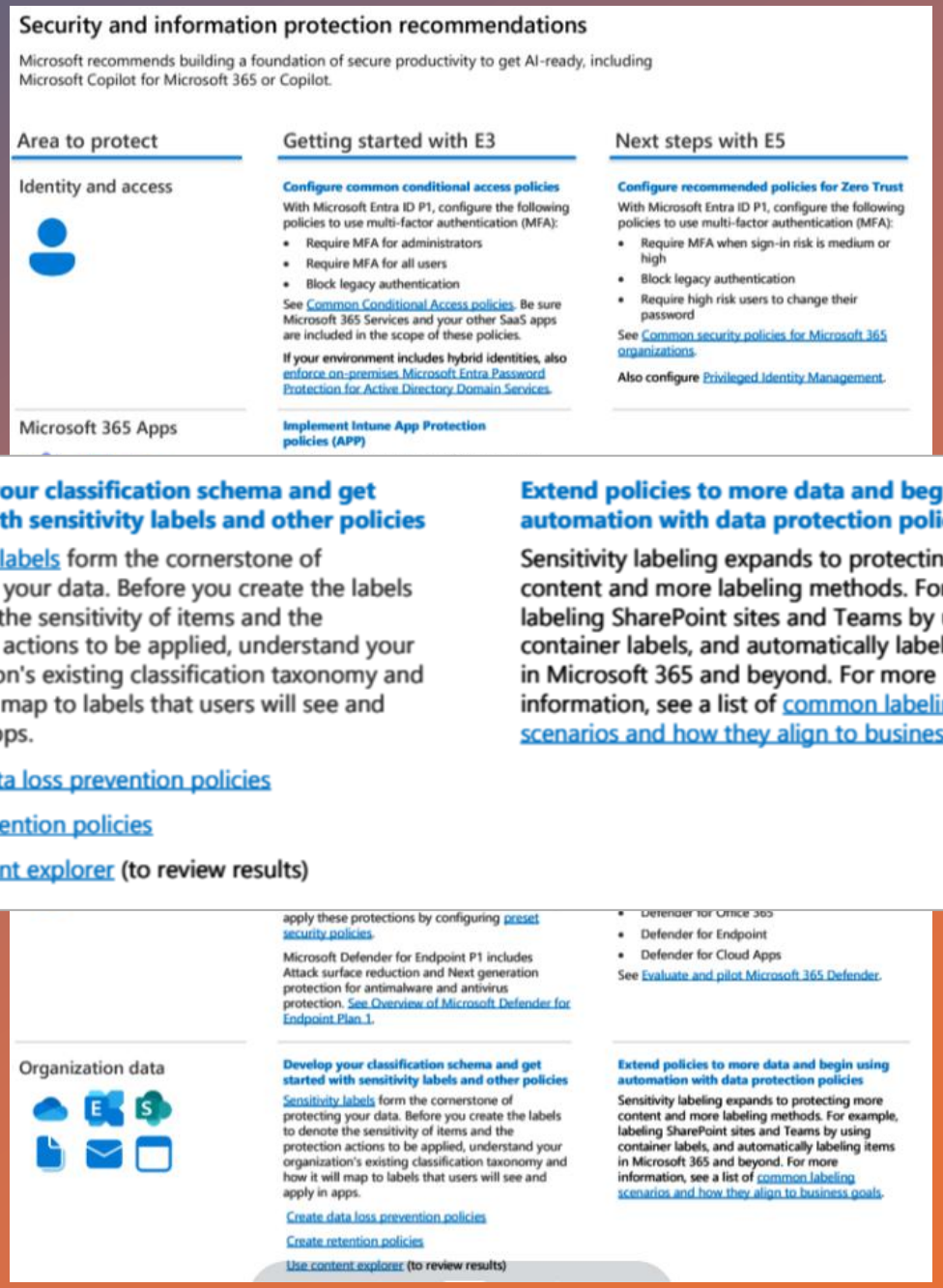


Security and information protection recommendations

Microsoft recommends building a foundation of secure productivity to get AI-ready, including Microsoft Copilot for Microsoft 365 or Copilot.

Area to protect	Getting started with E3	Next steps with E5
Identity and access	**Configure common conditional access policies** With Microsoft Entra ID P1, configure the following policies to use multi-factor authentication (MFA): • Require MFA for administrators • Require MFA for all users • Block legacy authentication See Common Conditional Access policies. Be sure Microsoft 365 Services and your other SaaS apps are included in the scope of these policies. If your environment includes hybrid identities, also enforce on-premises Microsoft Entra Password Protection for Active Directory Domain Services.	**Configure recommended policies for Zero Trust** With Microsoft Entra ID P1, configure the following policies to use multi-factor authentication (MFA): • Require MFA when sign-in risk is medium or high • Block legacy authentication • Require high risk users to change their password See Common security policies for Microsoft 365 organizations. Also configure Privileged Identity Management.
Microsoft 365 Apps	**Implement Intune App Protection policies (APP)** With APP, Intune creates a wall between your organization data and personal data. Policies ensure corporate data in the apps you specify cannot be copied and pasted to other apps on the device, even if the device is not managed. See Implement App Protection policies.	
Devices	**Manage devices** After devices are enrolled, set up compliance policies and then require healthy and compliant devices. Finally, deploy device profiles to manage settings and features on devices. Enroll devices into management Set up compliance policies Require healthy and compliant devices Deploy device profiles	**Monitor device risk and compliance to security baselines** Integrate Intune with Defender for Endpoint to monitor device risk as a condition for access. For Windows devices, monitor compliance of these devices to security baselines. See Monitor device risk and compliance to security baselines.
Threat protection	**Configure Exchange Online Protection and endpoint protection** Exchange Online Protection (EOP) helps protect your email and collaboration tools from phishing, impersonation, and other threats. You can rapidly apply these protections by configuring preset security policies. Microsoft Defender for Endpoint P1 includes Attack surface reduction and Next generation protection for antimalware and antivirus protection. See Overview of Microsoft Defender for Endpoint Plan 1.	**Pilot and deploy Microsoft 365 Defender** For more comprehensive threat protection, pilot and deploy Microsoft 365 Defender, including: • Defender for Identity • Defender for Office 365 • Defender for Endpoint • Defender for Cloud Apps See Evaluate and pilot Microsoft 365 Defender.
Organization data	**Develop your classification schema and get started with sensitivity labels and other policies** Sensitivity labels form the cornerstone of protecting your data. Before you create the labels to denote the sensitivity of items and the protection actions to be applied, understand your organization's existing classification taxonomy and how it will map to labels that users will see and apply in apps. Create data loss prevention policies Create retention policies Use content explorer (to review results)	**Extend policies to more data and begin using automation with data protection policies** Sensitivity labeling expands to protecting more content and more labeling methods. For example, labeling SharePoint sites and Teams by using container labels, and automatically labeling items in Microsoft 365 and beyond. For more information, see a list of common labeling scenarios and how they align to business goals.

How to make your wor
Copilot s



Wat zijn de drijfveren om aan de slag te gaan met informatiebeveiliging?

AUTORITEIT PERSOONSGEGEVENS

Waar bent u naar op zoek?

Datalek melden | Klacht indiene

Home | Thema's | Actueel | Documenten | Contact | FG's

Home > Actueel >

Let op: gebruik AI-chatbot kan leiden tot datalekken

06 augustus 2024 Thema's: Datalekken, Algoritmes, AI en de AVG

De Autoriteit Persoonsgegevens (AP) heeft de afgelopen tijd meerdere meldingen binnengekregen van datalekken doordat medewerkers persoonsgegevens van bijvoorbeeld patiënten of klanten deelden met een chatbot die gebruikmaakt van kunstmatige intelligentie (AI). Door het invoeren van persoonsgegevens in AI-chatbots kunnen de bedrijven die de chatbot aanbieden ongeoorloofd toegang krijgen tot die persoonsgegevens.

Medische gegevens en adressen van klanten

Bij een van de datalekken waarvan de AP een melding kreeg, had een medewerker van een huisartsenpraktijk – tegen de afspraken in – medische gegevens van patiënten ingevoerd in een AI-chatbot. Medische gegevens zijn zeer gevoelige gegevens en krijgen niet voor niets extra bescherming in de wet. Die gegevens zomaar delen met een techbedrijf is een grote schending van de privacy van de mensen om wie het gaat.

Ook kreeg de AP een melding binnen van een telecombedrijf, waar een medewerker een bestand met onder meer adressen van klanten had ingevoerd in een AI-chatbot.

BUSINESS INSIDER

TECH

Samsung bans employees from using AI tools like ChatGPT and Google Bard after an accidental data leak, report says

Sawdah Bhaimiya May 2, 2023, 3:08 PM CEST Share Save

Samsung has banned the use of AI tools in the workplace. Chung Sung-Jun/Getty Images

- Samsung has banned employees from using ChatGPT in the workplace, per Bloomberg.
- This comes after Samsung engineers accidentally leaked internal source code to ChatGPT in April.
- Other companies including Amazon, JPMorgan, and Goldman Sachs have restricted AI use.

1. Maak een risicoanalyse

Digitale dreigingen kunnen grote risico's met zich meebrengen voor de dienstverlening van jouw organisatie. Via een helder en cyclisch risicomanagementbeleid kun je komen tot een passend niveau van (digitale) weerbaarheid. Dat begint met een risicoanalyse waarin de te beschermen belangen, dreigingen en de huidige weerbaarheid van jouw organisatie worden bekeken. Op basis hiervan kun je weloverwogen keuzes maken hoe om te gaan met de gevonden risico's.

Je kunt jouw risicoanalyse sturen door de volgende vragen te beantwoorden:

Wat zijn te beschermen belangen (kroonjuwelen) van mijn organisatie?

Door in kaart te brengen welke zaken cruciaal zijn voor jouw organisatie en/of dienstverlening, kun je afwegingen maken om de juiste passende maatregelen te nemen om deze belangen te beschermen. Voorbeelden van kroonjuwelen kunnen zijn: klantgegevens, productiemethoden, gegevens over de medewerkers, financiële gegevens of reputatie van jouw organisatie.

De publicatie '[Hoe breng ik mijn te beschermen belangen in kaart?]' biedt organisaties praktische handvatten aan personen die werkzaam zijn op tactisch niveau in de organistie. Wanneer je jouw te beschermen belangen in kaart hebt gebracht, kun je deze gebruiken om een risicoanalyse uit te voeren.

Hoe breng ik mijn technische te beschermen belangen in kaart?

Kroonjuwelen

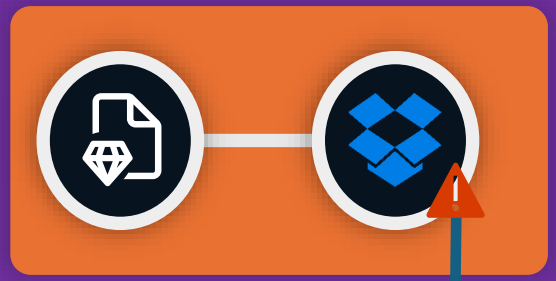
Wet- &
Regelgeving

LLM’s

Waarom is databeveiliging op zichzelfstaand al zo ingewikkeld?

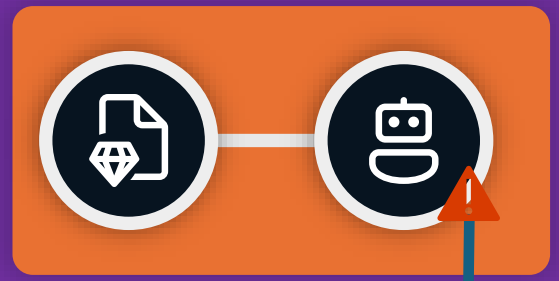
Gebruikers & AI = datalek?

Gebruiker maakt een document zonder de juiste toegangscontroles, waardoor andere gebruikers ernaar kunnen zoeken in Copilot



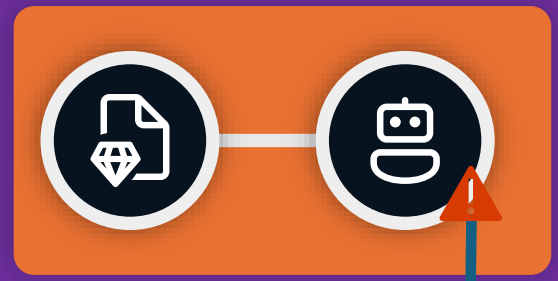
Gegevensblootstelling door nalatige gebruiker

Gebruiker vraagt generatieve AI om informatie over een geheim project te vinden en lekt het naar de pers voor persoonlijk gewin



Gegevenslek door ontevreden gebruiker

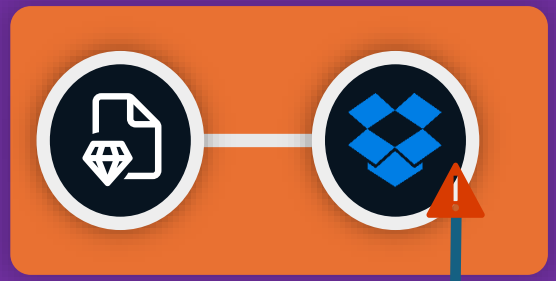
Gebruiker deelt vanuit nalatigheid sensitieve data in de generatieve AI-apps



Datalek door nalatige gebruiker

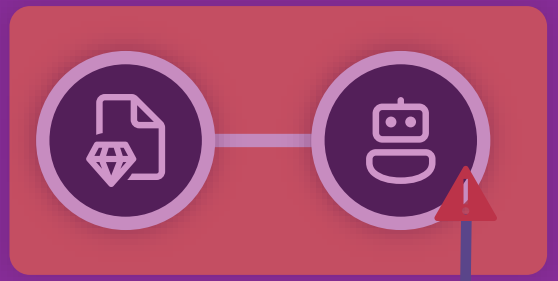
Gebruikers & AI = datalek?

Gebruiker maakt een document zonder de juiste toegangscontroles, waardoor andere gebruikers ernaar kunnen zoeken in Copilot



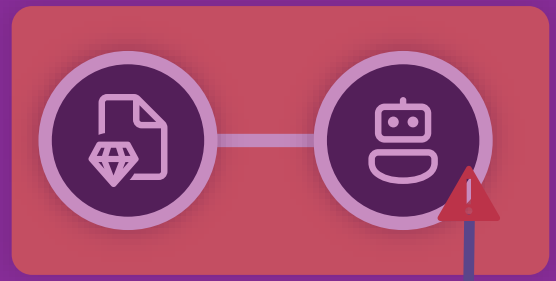
Gegevensblootstelling door nalatige gebruiker

Gebruiker vraagt generatieve AI om informatie over een geheim project te vinden en lekt het naar de pers voor persoonlijk gewin



Gegevenslek door ontevreden gebruiker

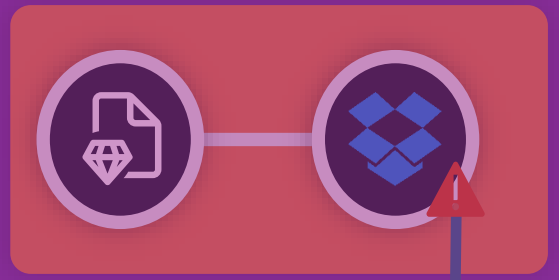
Gebruiker deelt vanuit nalatigheid sensitieve data in de generatieve AI-apps



Datalek door nalatige gebruiker

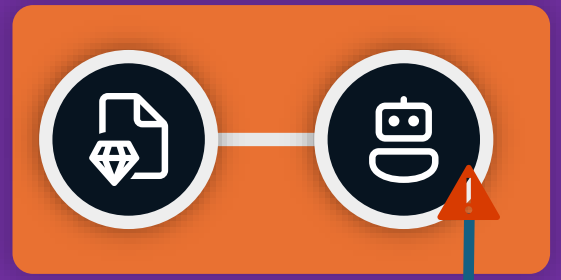
Gebruikers & AI = datalek?

Gebruiker maakt een document zonder de juiste toegangscontroles, waardoor andere gebruikers ernaar kunnen zoeken in Copilot



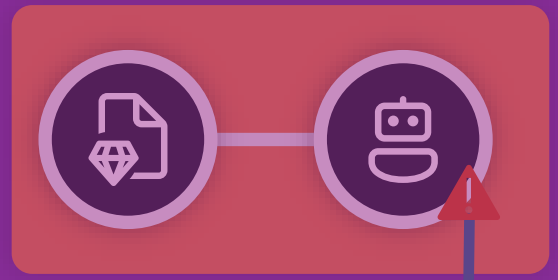
Gegevensblootstelling door nalatige gebruiker

Gebruiker vraagt generatieve AI om informatie over een geheim project te vinden en lekt het naar de pers voor persoonlijk gewin



Gegevenslek door ontevreden gebruiker

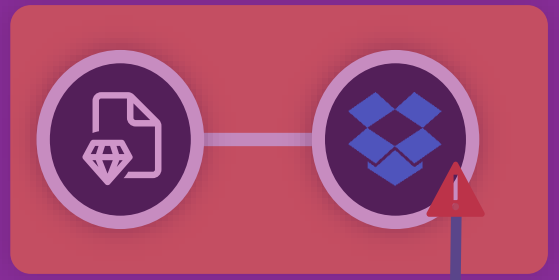
Gebruiker deelt vanuit nalatigheid sensitieve data in de generatieve AI-apps



Datalek door nalatige gebruiker

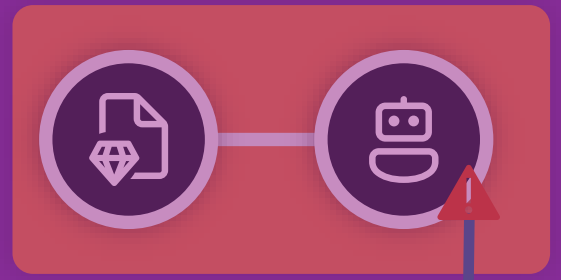
Gebruikers & AI = datalek?

Gebruiker maakt een document zonder de juiste toegangscontroles, waardoor andere gebruikers ernaar kunnen zoeken in Copilot



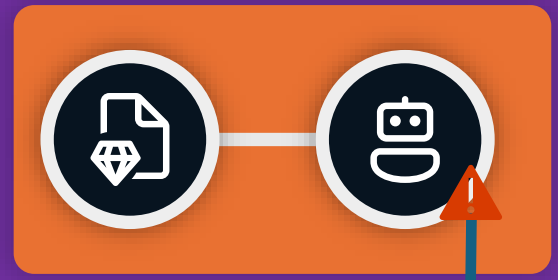
Gegevensblootstelling door nalatige gebruiker

Gebruiker vraagt generatieve AI om informatie over een geheim project te vinden en lekt het naar de pers voor persoonlijk gewin



Gegevenslek door ontevreden gebruiker

Gebruiker deelt vanuit nalatigheid sensitieve data in de generatieve AI-apps



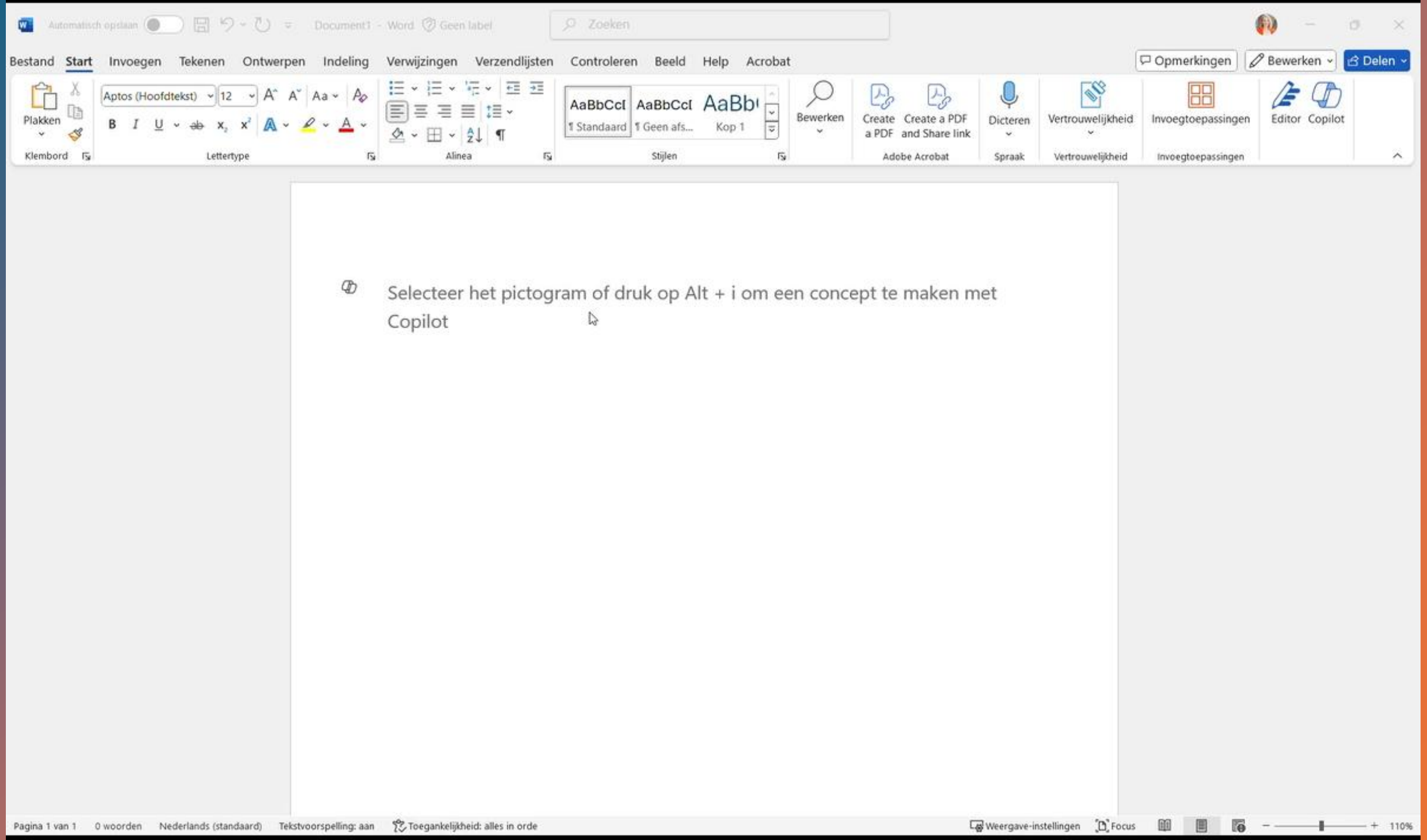
Datalek door nalatige gebruiker

Oke mensen, trek die Copilot licentie maar weer in...

Of toch niet?

- Je kan grip krijgen op je sensitieve informatie!

Productivity meets (& needs!) data security


Automatisch opslaan
Document1 - Word
Geen label
Zoeken
Bestand
Start
Invoegen
Tekenen
Ontwerpen
Indeling
Verwijzingen
Verzendlijsten
Controleren
Beeld
Help
Acrobat
Opmerkingen
Bewerken
Delen
Plakken
Klembord
Aptos (Hoofdtekst)
12
Lettertype
Alinea
AaBbCcI
¶ Standaard
AaBbCcI
¶ Geen afs...
AaBbI
Kop 1
Stijlen
Bewerken
Create a PDF
Create a PDF and Share link
Adobe Acrobat
Dicteren
Spraak
Vertrouwelijkheid
Vertrouwelijkheid
Invoegtoepassingen
Invoegtoepassingen
Editor
Copilot
Selecteer het pictogram of druk op Alt + i om een concept te maken met Copilot
Pagina 1 van 1
0 woorden
Nederlands (standaard)
Tekstvoorspelling: aan
Toegankelijkheid: alles in orde
Weergave-instellingen
Focus
110%

Stappenplan om veilig op reis te gaan

Stap 1

Voorbereiding: de kroonjuwelen bepalen

Stakeholders aanhaken

Chief Information Officer (CIO)

Legal officer

HR

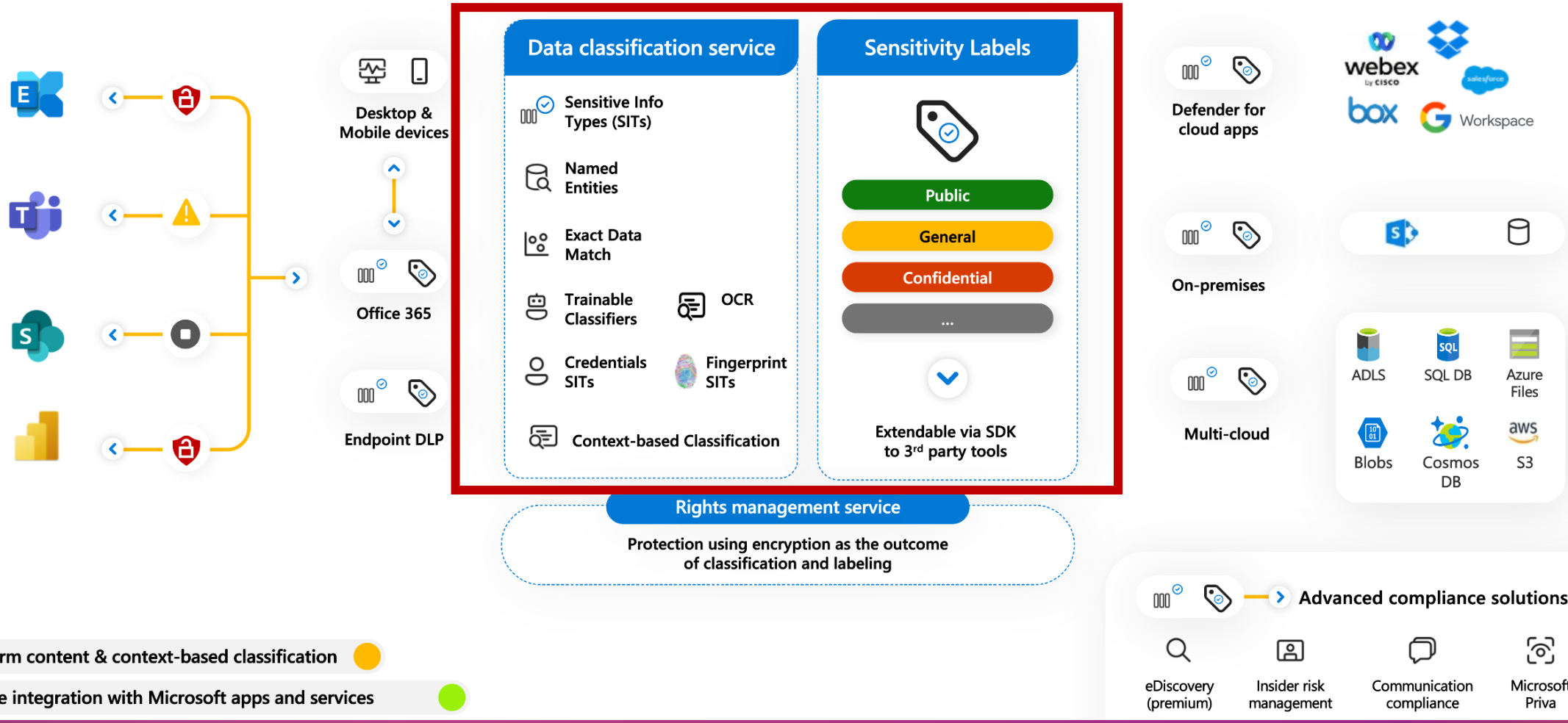
Compliance Officer

Privacy officer

Chief Security Officer (CISO)

Risicomanager

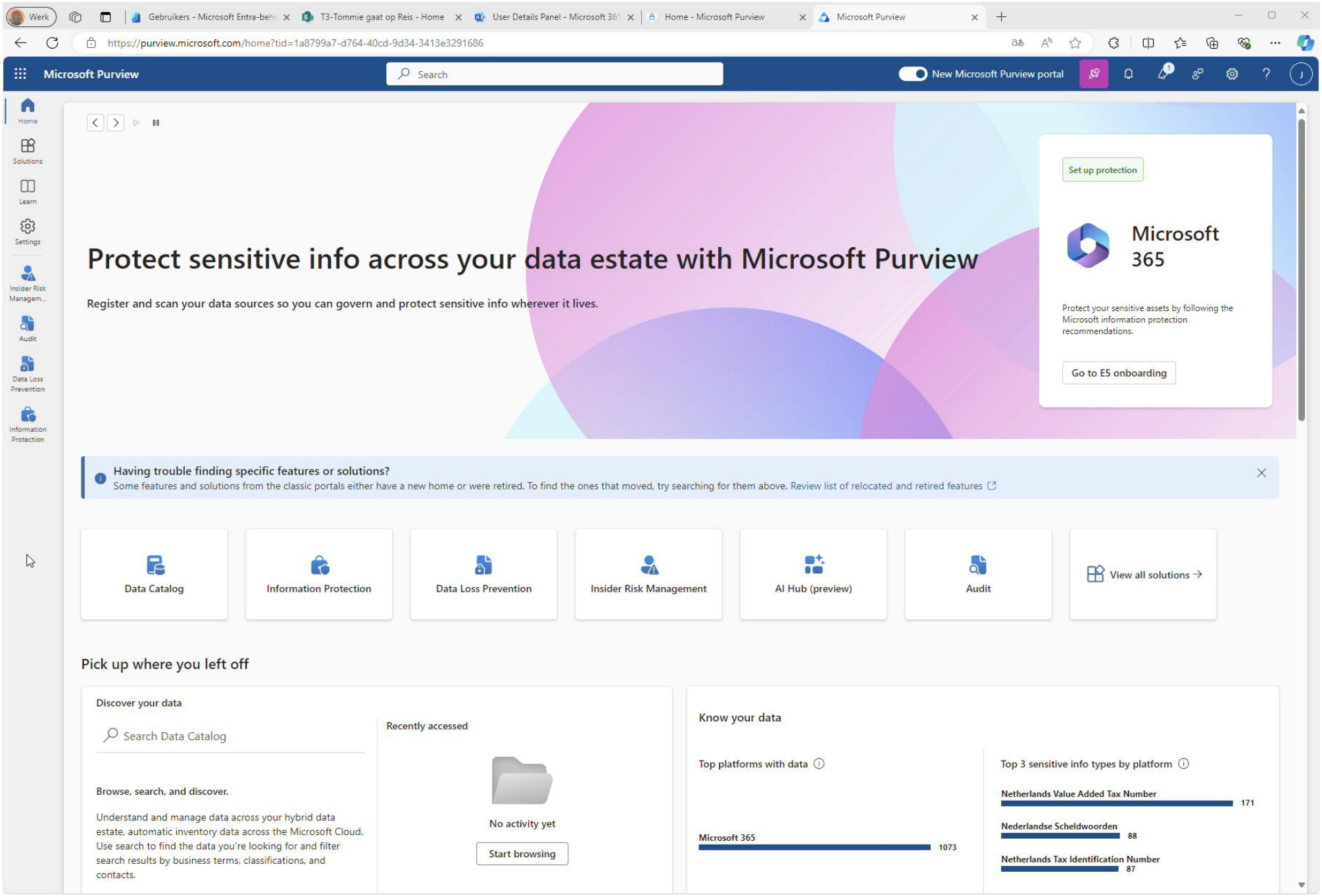
Microsoft Purview Information Protection

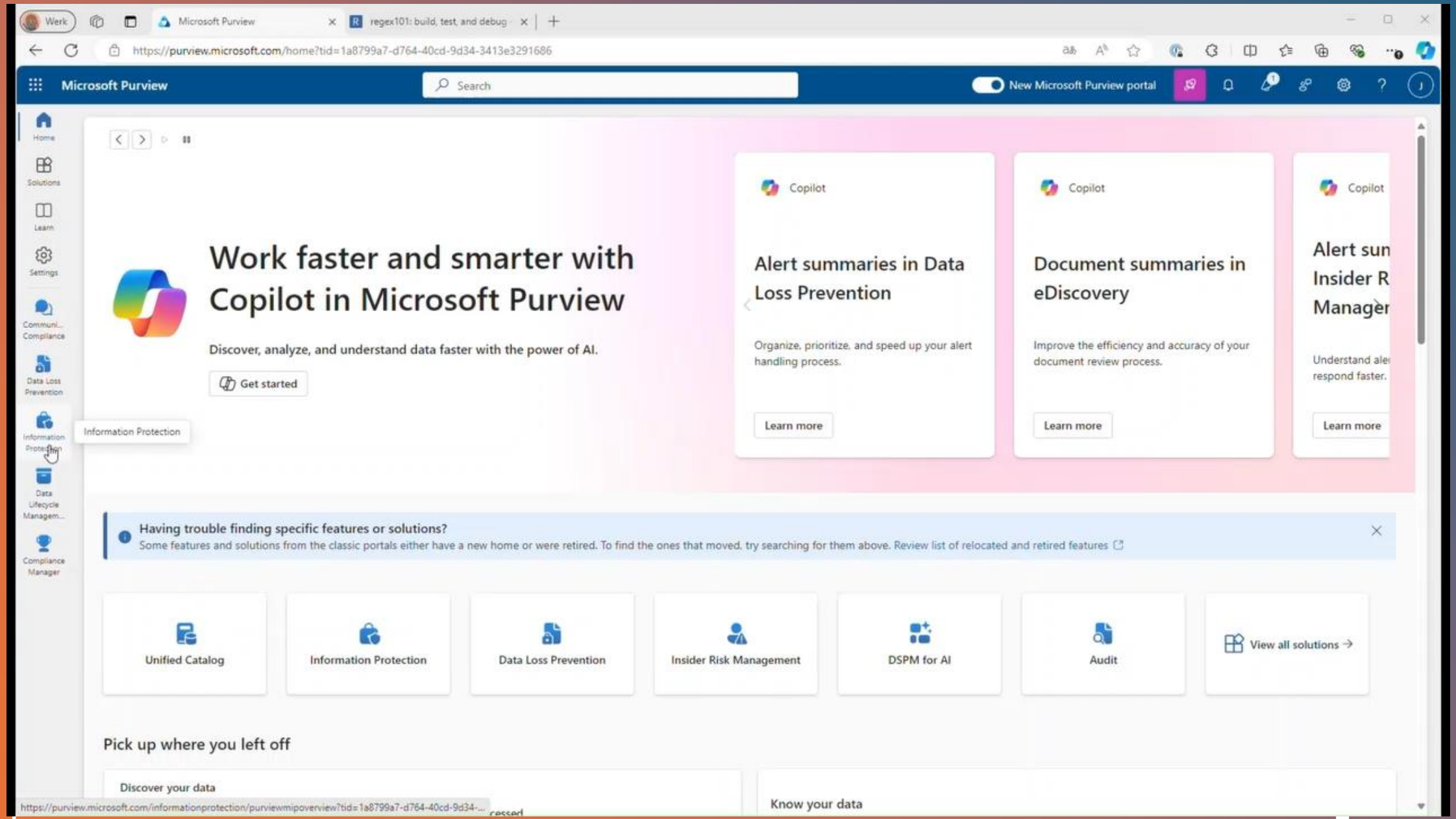


Uniform content & context-based classification

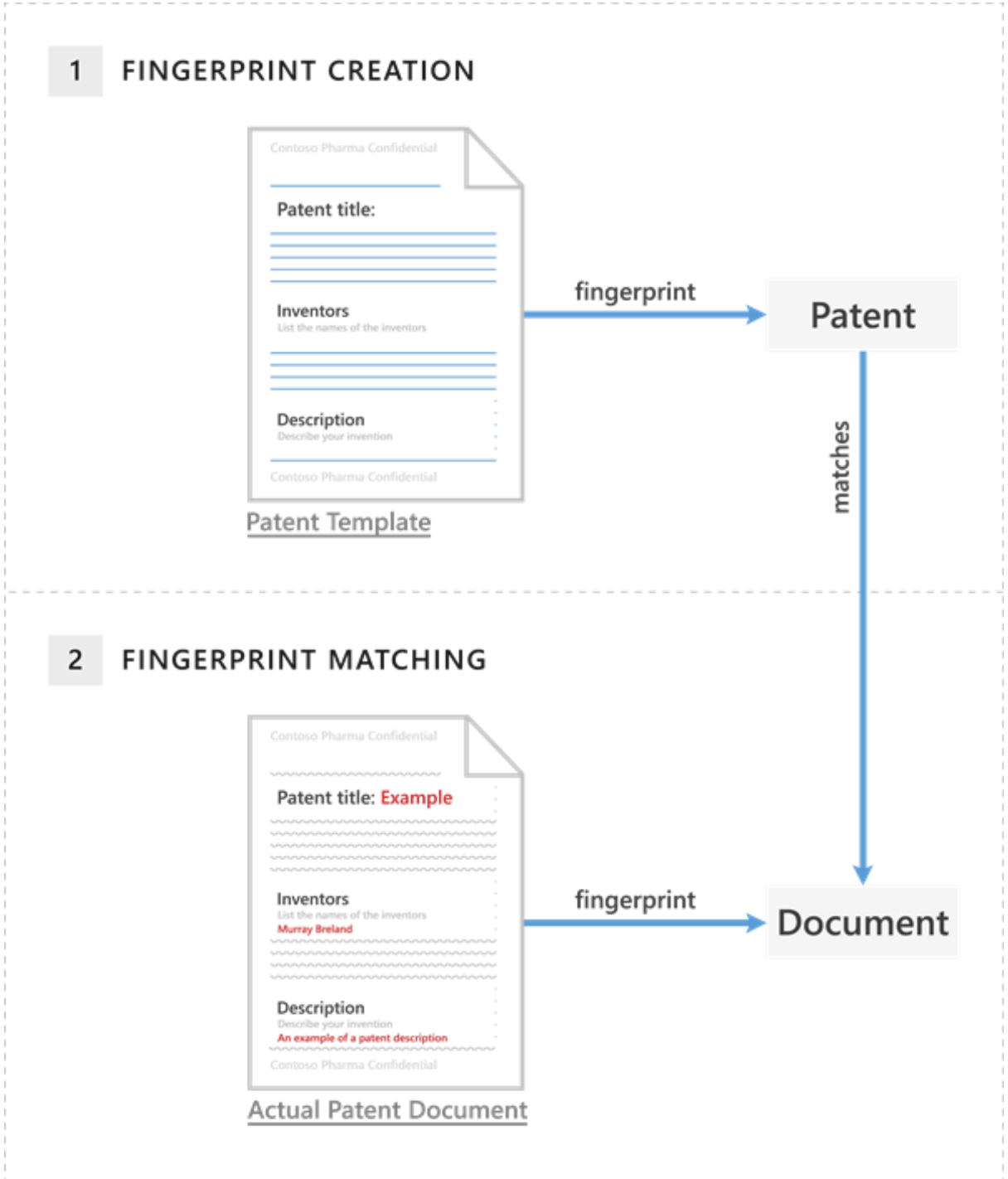
Native integration with Microsoft apps and services

Demo
Out of the box SIT
& Custom SIT


Werk
Gebruikers - Microsoft Entra-beh
T3-Tommie gaat op Reis - Home
User Details Panel - Microsoft 365
Home - Microsoft Purview
Microsoft Purview
https://purview.microsoft.com/home?tid=1a8799a7-d764-40cd-9d34-3413e3291686
Microsoft Purview
Search
New Microsoft Purview portal
Home
Solutions
Learn
Settings
Insider Risk Managem...
Audit
Data Loss Prevention
Information Protection
Protect sensitive info across your data estate with Microsoft Purview
Register and scan your data sources so you can govern and protect sensitive info wherever it lives.
Set up protection
Microsoft 365
Protect your sensitive assets by following the Microsoft information protection recommendations.
Go to E5 onboarding
Having trouble finding specific features or solutions?
Some features and solutions from the classic portals either have a new home or were retired. To find the ones that moved, try searching for them above. Review list of relocated and retired features
Data Catalog
Information Protection
Data Loss Prevention
Insider Risk Management
AI Hub (preview)
Audit
View all solutions
Pick up where you left off
Discover your data
Search Data Catalog
Browse, search, and discover.
Understand and manage data across your hybrid data estate, automatic inventory data across the Microsoft Cloud. Use search to find the data you're looking for and filter search results by business terms, classifications, and contacts.
Recently accessed
No activity yet
Start browsing
Know your data
Top platforms with data
Microsoft 365
1073
Top 3 sensitive info types by platform
Netherlands Value Added Tax Number
171
Nederlandse Scheldwoorden
88
Netherlands Tax Identification Number
87


Microsoft Purview
regex101: build, test, and debug
https://purview.microsoft.com/home?tid=1a8799a7-d764-40cd-9d34-3413e3291686
Microsoft Purview
Search
New Microsoft Purview portal
Home
Solutions
Learn
Settings
Communi... Compliance
Data Loss Prevention
Information Protection
Data Lifecycle Managem...
Compliance Manager
Information Protection
Work faster and smarter with Copilot in Microsoft Purview
Discover, analyze, and understand data faster with the power of AI.
Get started
Copilot
Alert summaries in Data Loss Prevention
Organize, prioritize, and speed up your alert handling process.
Learn more
Copilot
Document summaries in eDiscovery
Improve the efficiency and accuracy of your document review process.
Learn more
Copilot
Alert sun
Insider R
Manager
Understand ale
respond faster.
Learn more
Having trouble finding specific features or solutions?
Some features and solutions from the classic portals either have a new home or were retired. To find the ones that moved, try searching for them above. Review list of relocated and retired features
Unified Catalog
Information Protection
Data Loss Prevention
Insider Risk Management
DSPM for AI
Audit
View all solutions
Pick up where you left off
Discover your data
Know your data
https://purview.microsoft.com/informationprotection/purviewmipoverview?tid=1a8799a7-d764-40cd-9d34-...

Document Fingerprinting

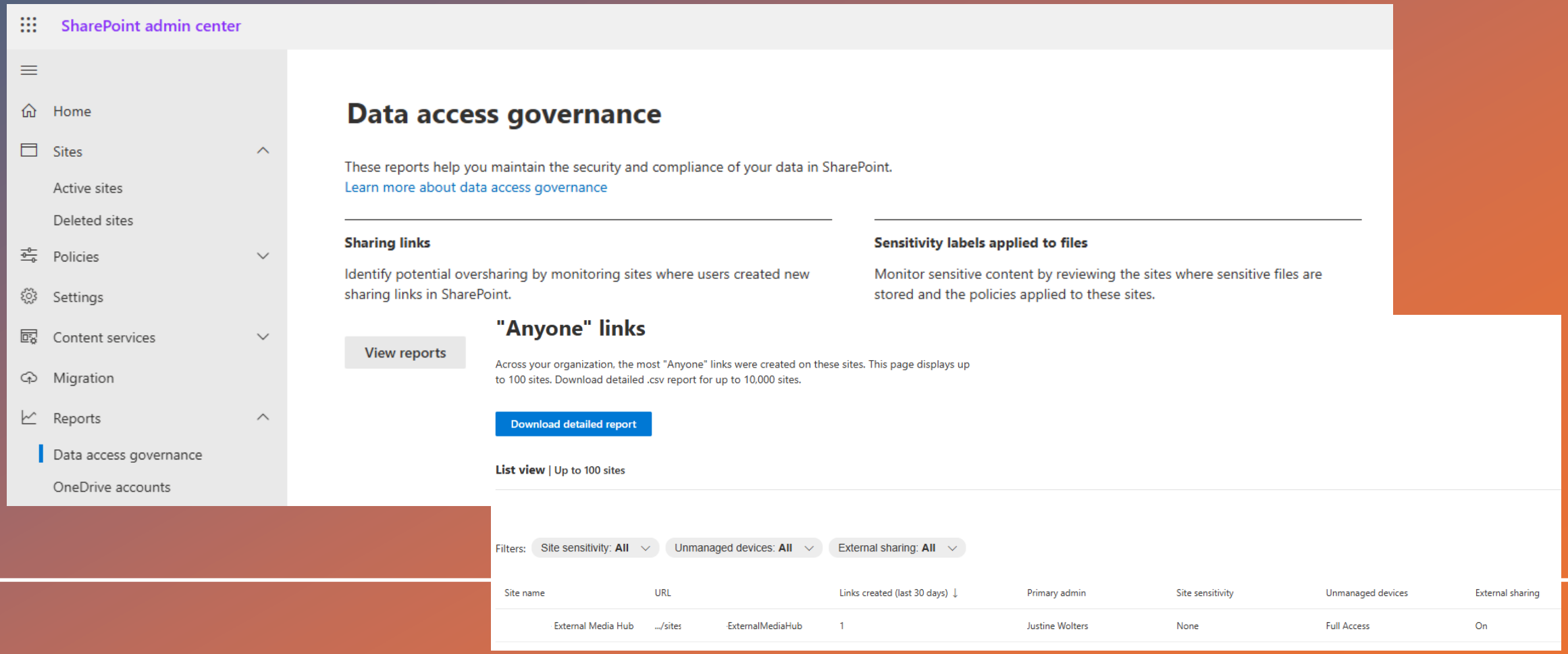


Stap 2

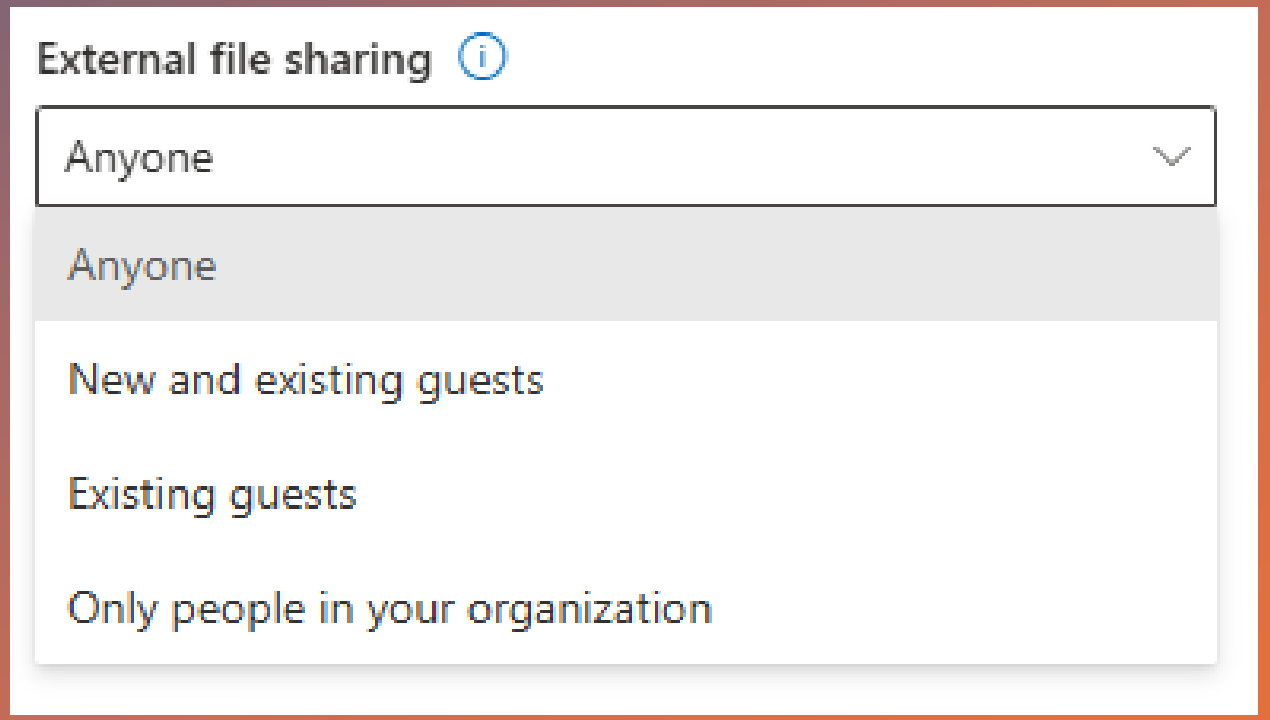
Reisregels

Afspraken maken met elkaar

Sharepoint Advanced Management

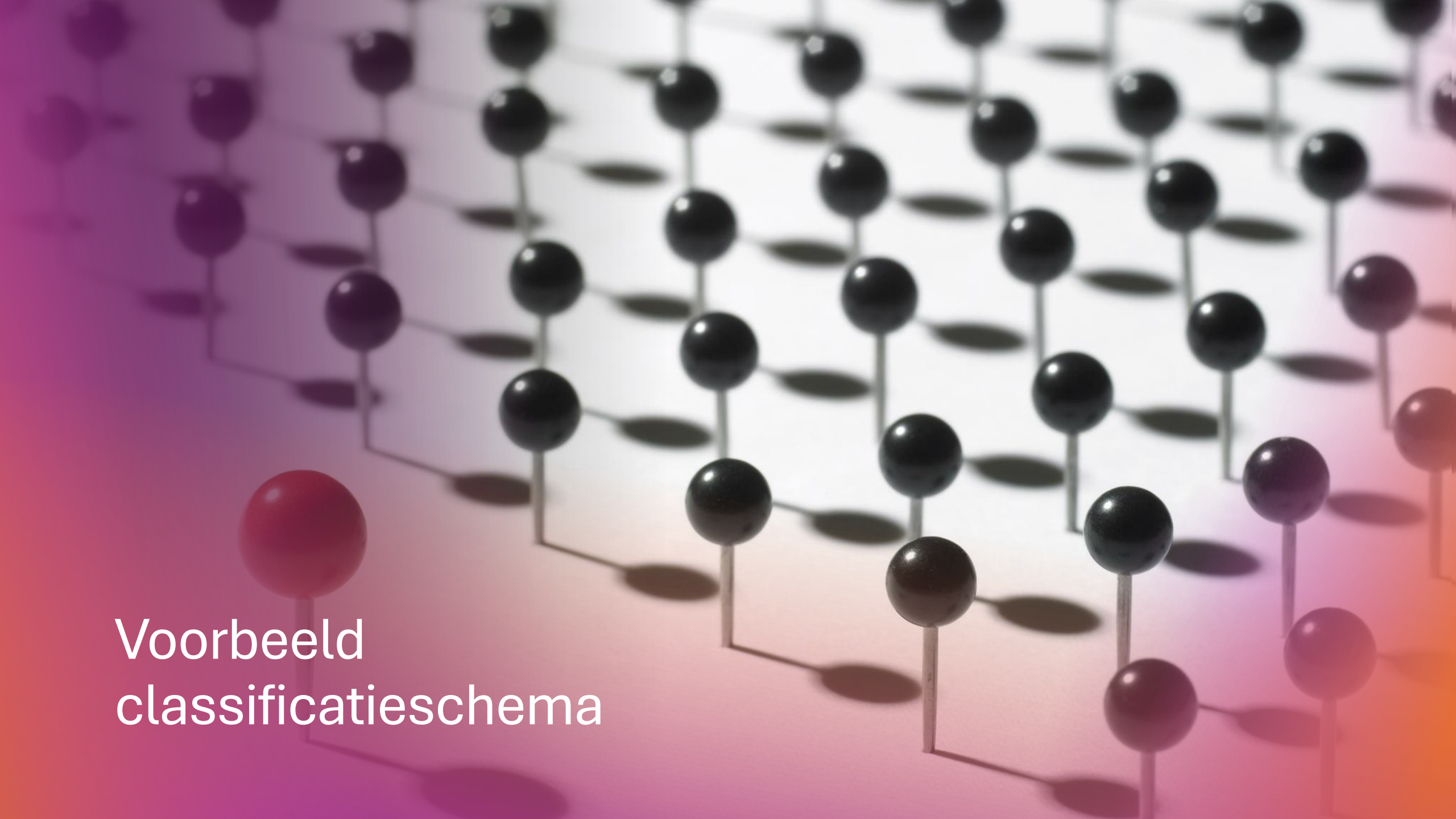


External file sharing settings Sharepointsites



Stap 3

Inrichten en beveiligen



Voorbeeld classificatieschema

Naam	Beschrijving	Voorbeelden	Acties (op basis van je beleid!)
Persoonlijk	Persoonlijke of privédocumenten die zijn opgeslagen op een apparaat van de organisatie.	O.a. factuur nieuwe verrekijker, stappenplan vogelhuisje in elkaar zetten, familiekiekjes.	• Geen versleuteling. • Geen content markering.
Openbaar	Data wat goedgekeurd is om met het publiek te delen.	O.a. publieke jaarverslagen, openbare persberichten, goedgekeurde publiekelijke foto's.	• Geen versleuteling. • Geen content markering.
Algemeen	Dit label geldt voor het overgrote deel van de data. Data gelabeld met dit label is niet bestemd voor het brede publiek maar kan wel worden gedeeld met interne medewerkers en externe gasten waar nodig.	O.a. Templates, algemene presentaties.	• Binnen een team met dit label is wel mogelijk om externe gasten uit te nodigen om samen te werken. • Geen versleuteling. • Geen content markering.
Vertrouwelijk – Extern	Vertrouwelijke email en documenten waarbij informatie gedeeld en/of samengewerkt moet kunnen worden met zowel internen als ook externen.	O.a. Contractovereenkomsten met derde partijen, presentaties die zijn gegeven aan derde partijen, rapporten die beschikbaar moeten zijn voor externen.	• E-mails en documenten voorzien van content-markering. • Policy tip over bevatten potentieel gevoelige informatie.
Vertrouwelijk – Intern	Data welke alleen is bestemd voor medewerkers van de organisatie.	O.a. Contracten, documenten met persoonlijke gegevens (BSN-nummers, salarisgegevens, etc.), beleidsstukken.	• Versleuteling. • Mag niet worden gedeeld met externen. • Gasten binnen de Office 365 tenant waarmee wordt samengewerkt geen toegang tot mail en documenten. • E-mails en documenten voorzien van content-markering.
Geheim	Zeer geheime informatie voor een selecte groep zichtbaar	O.a. Bestuur stukken, geheime projectinformatie, rapporten met strategische beslissingen, salarisinformatie topfunctionarissen.	• Versleuteling. • E-mails en documenten voorzien van content-markering. • Mag beperkt worden gedeeld met internen en niet worden gedeeld met externen.

Choose permissions

Choose which actions would be allowed for this user/group. Learn more about permissions

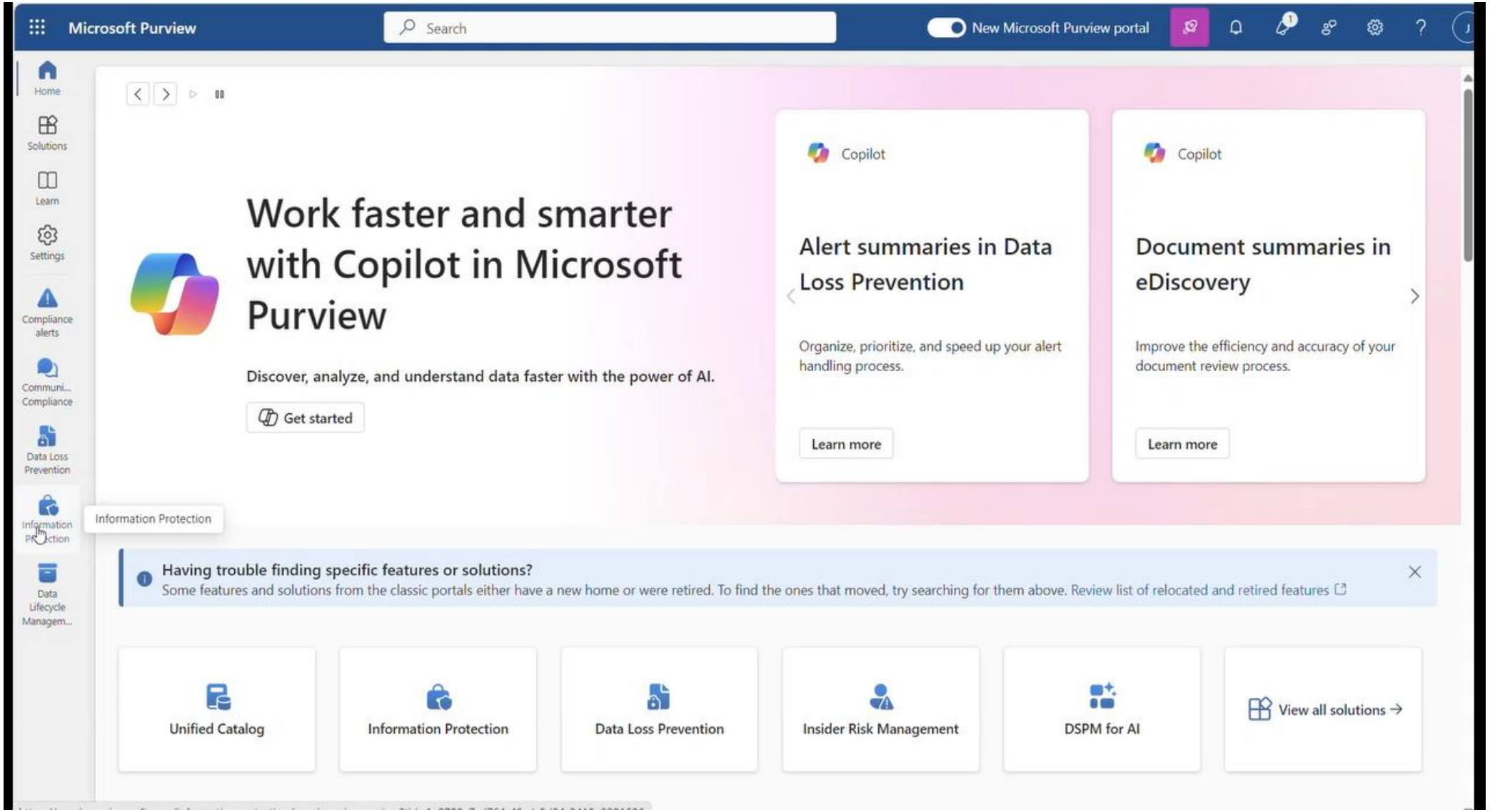
Custom

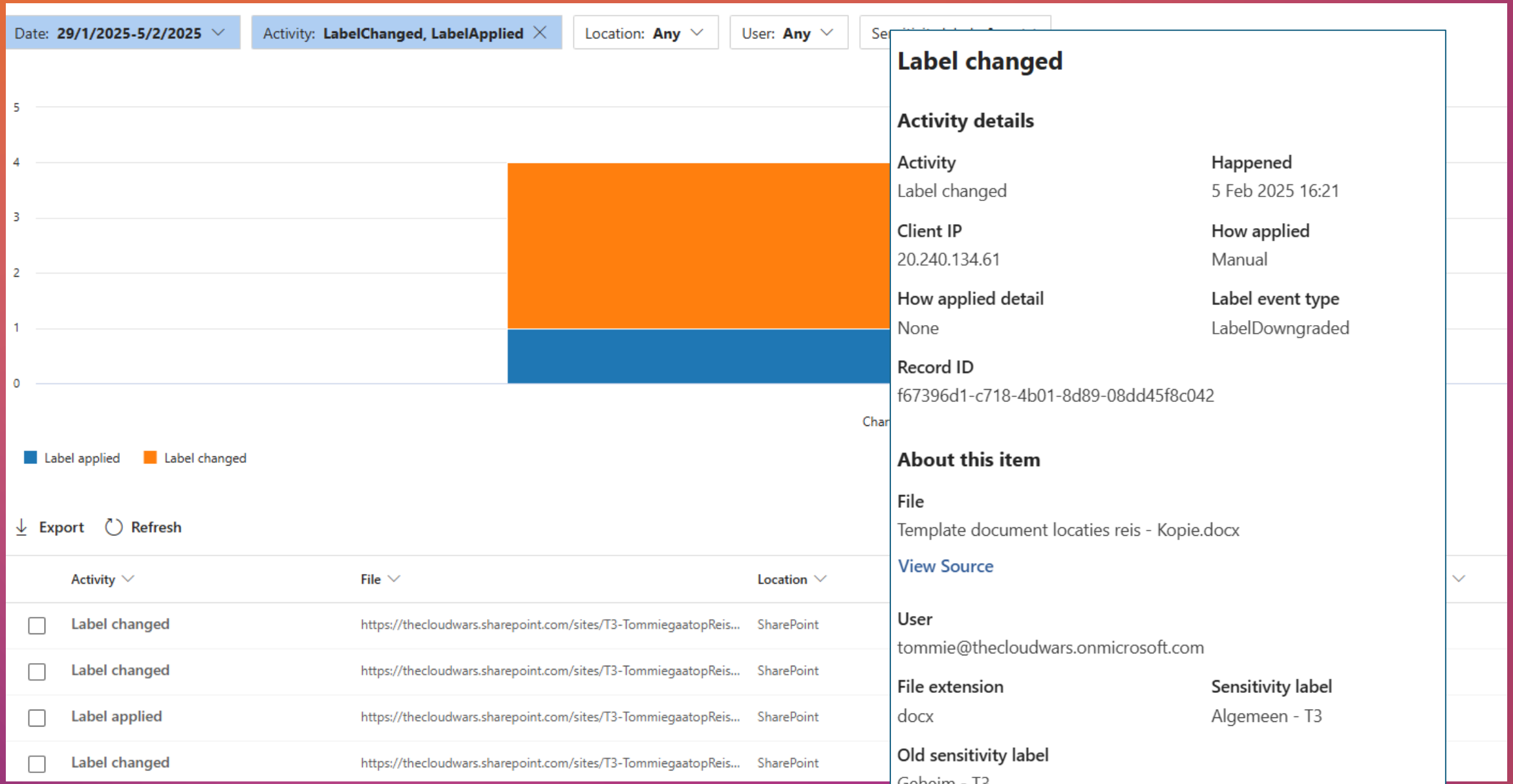
- [x] View content(VIEW)
- [x] View rights(VIEWRIGHTSDATA)
- [ ] Edit content(DOCEDIT)
- [ ] Save(EDIT)
- [x] Print(PRINT)
- [ ] Copy and extract content(EXTRACT)
- [ ] Reply(REPLY)
- [ ] Reply all(REPLYALL)
- [ ] Forward(FORWARD)
- [ ] Edit rights(EDITRIGHTSDATA)
- [x] Export content(EXPORT)
- [ ] Allow macros(OBJMODEL)

Permissions

Stap 4

Monitoren in audit mode


Microsoft Purview
Search
New Microsoft Purview portal
Home
Solutions
Learn
Settings
Compliance alerts
Communi... Compliance
Data Loss Prevention
Information Protection
Data Lifecycle Managem...
Work faster and smarter with Copilot in Microsoft Purview
Discover, analyze, and understand data faster with the power of AI.
Get started
Copilot
Alert summaries in Data Loss Prevention
Organize, prioritize, and speed up your alert handling process.
Learn more
Copilot
Document summaries in eDiscovery
Improve the efficiency and accuracy of your document review process.
Learn more
Having trouble finding specific features or solutions?
Some features and solutions from the classic portals either have a new home or were retired. To find the ones that moved, try searching for them above. Review list of relocated and retired features
Unified Catalog
Information Protection
Data Loss Prevention
Insider Risk Management
DSPM for AI
View all solutions


Date: 29/1/2025-5/2/2025
Activity: LabelChanged, LabelApplied
Location: Any
User: Any
5
4
3
2
1
0
Label applied
Label changed
Export
Refresh
Activity
File
Location
Label changed
https://thecloudwars.sharepoint.com/sites/T3-TommiegaatopReis...
SharePoint
Label changed
https://thecloudwars.sharepoint.com/sites/T3-TommiegaatopReis...
SharePoint
Label applied
https://thecloudwars.sharepoint.com/sites/T3-TommiegaatopReis...
SharePoint
Label changed
https://thecloudwars.sharepoint.com/sites/T3-TommiegaatopReis...
SharePoint
Label changed
Activity details
Activity
Label changed
Happened
5 Feb 2025 16:21
Client IP
20.240.134.61
How applied
Manual
How applied detail
None
Label event type
LabelDowngraded
Record ID
f67396d1-c718-4b01-8d89-08dd45f8c042
About this item
File
Template document locaties reis - Kopie.docx
View Source
User
tommie@thecloudwars.onmicrosoft.com
File extension
docx
Sensitivity label
Algemeen - T3
Old sensitivity label
Geheim - T3

Stap 5

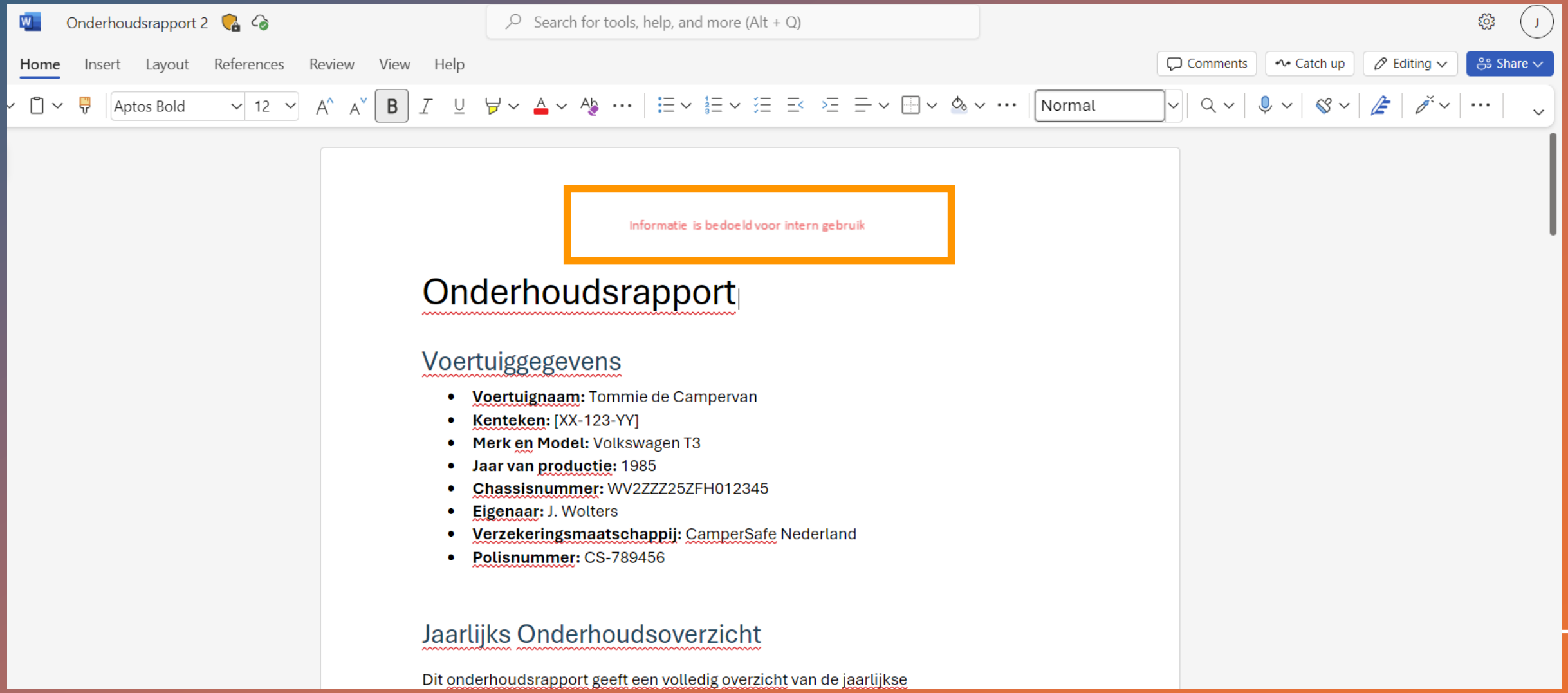
Pilot met gebruikers

Stap 6

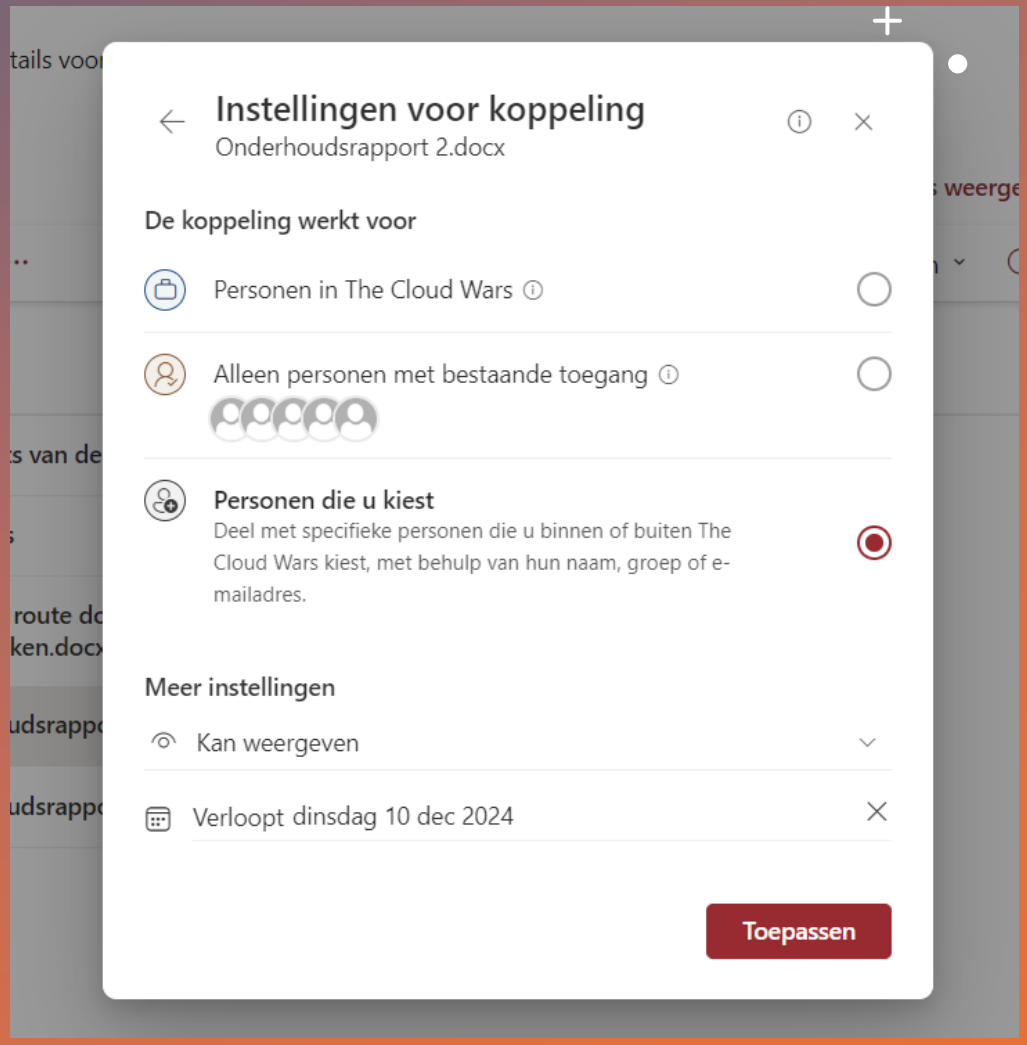
Bewustwording en adoptie


Outlook

Markeringen & beleidstips



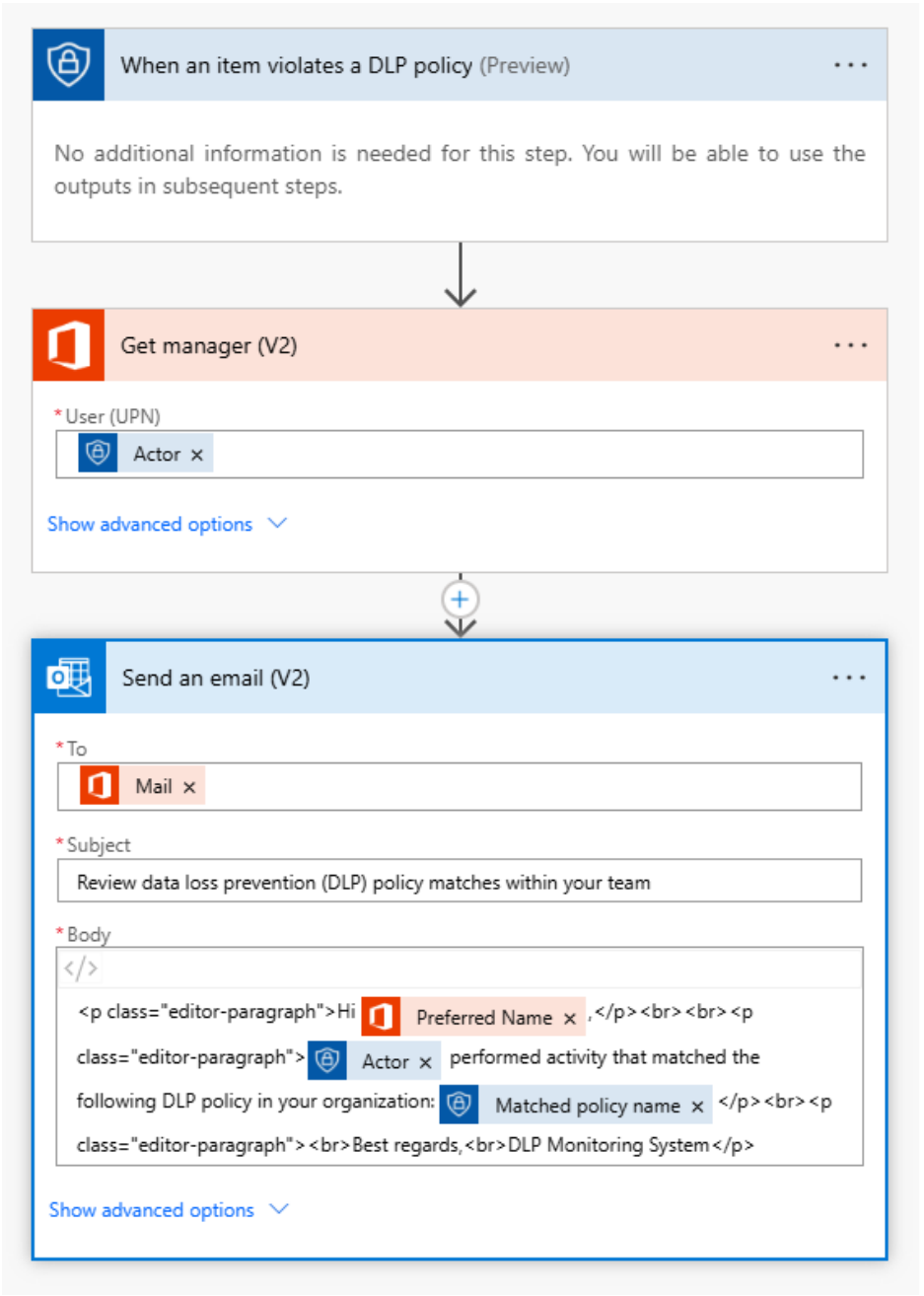
Voor Copilot ook niet onbelangrijk: oversharing!

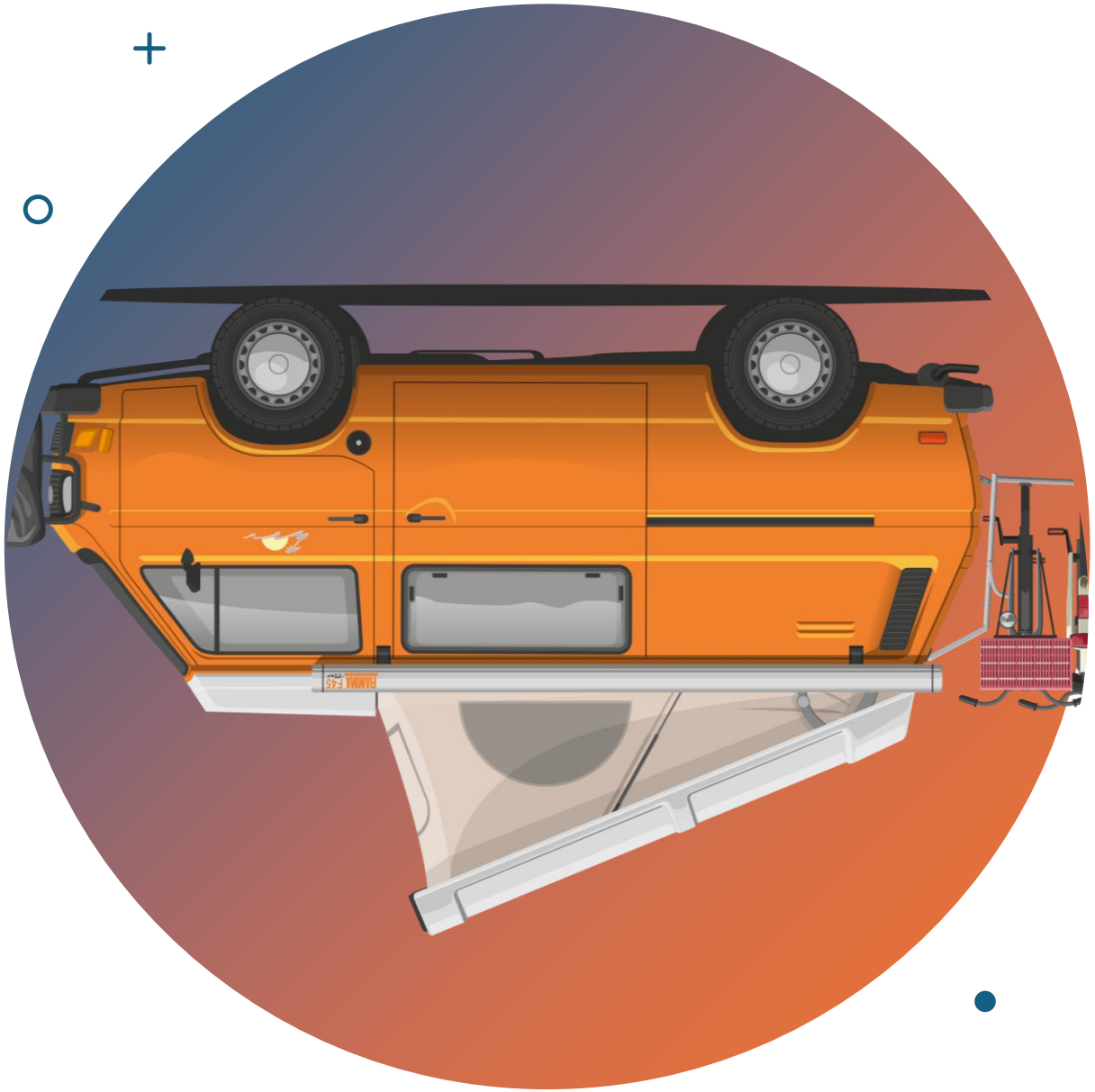


Stap 7

Evalueren, bijstellen en beleggen in staande organisatie

Hoe ga je opvolging beleggen in je organisatie?





Issues along the way

- Niet alle gevoelige data is vanaf het begin inzichtelijk
- Gebrek samenwerking IT & de business
- Gebrek aan duidelijke governance en eigenaarschap
- Onvoldoende monitoring en feedback mechanismen
- Weerstand gebruikers tegen nieuwe processen

Nog een side note

Tweetal DPIA’s (SURF & SLM) waarbij gebruik van Copilot wordt afgeraden.

Key Takeaways

- Copilot, tof ja! Maar implementeer niet zonder dat je de nodige databeveiliging hebt staan
- Ga niet op eigen houtje bepalen voor de organisatie wat sensitieve informatie is, doorgrond het process van de organisatie
- Begin klein met Copilot en laat de gebruikers in de pilot zoeken naar sensitieve informatie
- Het is geen eenmalige implementatie, maar een doorlopend proces

Copilot voor Microsoft 365: Een kans voor productiviteit of een risico voor je data?

The End