
MICROSOFT PURVIEW INFORMATION PROTECTION: EEN UITGEBREIDE GIDS VOOR GEVOELIGHEIDSLABELS
Gevoeligheidslabels
Versleuteling
Gegevensstromen

Microsoft Purview Information Protection helpt organisaties om hun gevoelige gegevens te classificeren en te beschermen met *gevoeligheidslabels*. In deze uitgebreide gids verkennen we alle aspecten van labeling: van handmatig en automatisch labelen tot het instellen van encryptie, rollen & verantwoordelijkheden, adoptiestrategieën en de laatste updates (2026) op het gebied van Microsoft Purview en Microsoft 365 Copilot. De insteek is vriendelijk, praktisch en niet-technisch, zodat iedereen – van IT-professionals tot eindgebruikers – inzicht krijgt in hoe labeling werkt en waarom het cruciaal is voor zowel betere databeveiliging als een succesvolle inzet van AI zoals Copilot.

Bovenstaande cijfers illustreren een belangrijk punt: veel organisaties willen profiteren van AI oplossingen zoals Microsoft 365 Copilot, maar worstelen met het vertrouwen in hun eigen data. Grote zorgen zijn dat gevoelige informatie onbedoeld opduikt in AI-antwoorden of bij onbevoegden terechtkomt. Gevoeligheidslabels zijn de sleutel om dit vertrouwen op te bouwen: ze geven data context en beschermingsregels, zodat zowel mensen als AI weten hoe ze correct met informatie moeten omgaan. Met stevige fundamenten in dataclassificatie en -bescherming kun je veilig genieten van de voordelen van AI zonder privacy- of compliance-risico's.

We gaan in op de harde realiteit van wat labeling wel en niet oplost, hoe Purview Information Protection precies werkt, en hoe je een effectief en eenvoudig labelbeleid opzet dat past bij jouw organisatie. Ook behandelen we handmatig vs. automatisch labelen, configuratie-opties (zoals encryptie en visuele markeringen), vereiste licenties, rollen binnen de organisatie, adoptiestrategieën voor draagvlak, en monitoring & auditing (waaronder integratie met Microsoft Sentinel voor rapportage en detectie). Bovendien kijken we naar nieuwe ontwikkelingen zoals label-groepen en de integratie met Microsoft 365 Copilot in 2025/2026. Laten we beginnen met de basis en een paar misverstanden uit de weg ruimen.

De harde waarheid: labeling ruimt de rommel niet op

Voordat we in de techniek duiken, is het belangrijk om te begrijpen wat gevoeligheidslabels níét voor je doen. Labels zijn geen tovermiddel dat al je dataproblemen oplost. Een label beschermt wat er is, maar maakt geen rommelige data netjes.

Met andere woorden: als informatie op de verkeerde plek staat of als te veel mensen er ongecontroleerde toegang toe hebben, dan verandert een label daar dus niets aan.

Begin dus bij de basis: orde op zaken stellen. Idealiter heb je voorafgaand aan labeling al een paar stappen gezet om je informatiehuishouding op te schonen:

- Duidelijke opslagplekken: Maak organisatiebrede afspraken over waar welke informatie hoort. Wanneer gebruik je Teams, SharePoint of OneDrive? Iedereen moet weten *waar* bepaalde documenten thuishoren. Dit voorkomt dat bestanden "**overal en nergens**" rondslingeren.
- Rechten & Toegang: Breng toegangsrechten op orde. Wie mag bij welke informatie en waarom? Verwijder historische excessen en hanteer het principe van *"**least privilege**"* – iedereen alleen toegang tot wat echt nodig is.
- Duidelijke opslagafspraken: "**Waar slaan we dit soort gegevens op?**" Zorg voor consistentie in waar gevoelige gegevens worden opgeslagen (bijv. HR-data alleen in een afgeschermde HR-site).

Pas **daarna** komt labeling in beeld om de inhoud van die informatie te kenmerken. Doe je dit andersom, dan **plak je labels op een chaos**. Dan krijgt Copilot alsnog te maken met half opgeruimde, slecht geclassificeerde informatie, met het welbekende *"**garbage in = garbage out**"*-risico.

Kortom, Purview Information Protection is geen schoonmaakmiddel, maar een markeerstift: het maakt zichtbaar welke informatie gevoelig is en hoe deze behandeld moet worden, maar je moet nog steeds zelf voor een nette basis zorgen.

Wat doet Purview Information Protection wel?

Gevoeligheidslabels geven context aan je data. Een label is eigenlijk een digitaal contract dat aangeeft *hoe gevoelig bepaalde informatie is en wat de consequenties daarvan zijn*. Bijvoorbeeld: een document met label "Vertrouwelijk" kan de regel meekrijgen "mag niet extern gedeeld worden en heeft een watermerk 'Vertrouwelijk' op elke pagina".

Door die context begrijpen gebruikers én services als Copilot wat de bedoeling is. Zo zorgt labeling ervoor dat een AI-assistent geen *ongepaste dingen* doet met jouw gevoelige data. Microsoft 365 Copilot houdt rekening met gevoeligheidslabels:

- Copilot mag alleen content gebruiken die de betreffende gebruiker zelf toegang heeft. Het AI-systeem ziet of een bestand of chatbericht gelabeld is en zal het *niet* opnemen in zijn antwoorden als de huidige gebruiker niet bevoegd is voor dat label. Met andere woorden: een HR-rapport met het label *"Alleen HR"* blijft onzichtbaar voor Copilot als een marketingmedewerker erom vraagt.

- Label-inhoud wordt gerespecteerd en doorgegeven: Vraagt een gebruiker aan Copilot om drie Vertrouwelijk-gelabelde documenten samen te vatten, dan erft het antwoord automatisch datzelfde label. Dit voorkomt dat gevoelige informatie ongezien in een AI-gegenereerde tekst belandt zonder waarschuwing. Headers, voetnoten of watermerken die door het label vereist zijn, worden ook toegepast op de output van Copilot.

- Labels kunnen AI-toegang inperken: Je kunt gevoeligheidslabels combineren met Data Loss Prevention (DLP) om te voorkomen dat Copilot bepaalde content *überhaupt* gebruikt. Zo kun je instellen dat Copilot alle documenten met het label "Geheim" negeert, zelfs als een gebruiker er toegang toe heeft. In 2025 heeft Microsoft specifiek een nieuwe DLP-optie toegevoegd om Copilot te blokkeren bij gelabelde gegevens in e-mails. Dit geeft je als organisatie de touwtjes in handen: jij bepaalt wat AI wel en niet mag zien.

Voorbeeld: Een bedrijf markeert zijn meest gevoelige informatie met een *Geheim* label. Met Purview DLP wordt ingesteld dat Copilot niets met *Geheime* documenten mag doen. Zo zal Copilot weigeren om een vraag te beantwoorden als dat hiervoor een *Geheim* document zou moeten openen of samenvatten. Dit betekent dat zelfs een machtige AI-assistent de **veiligheidsgrenzen respecteert** die je rondom je data hebt gezet.

> **Samengevat:** Microsoft Purview Information Protection geeft je de knoppen om de toegang en verspreiding van gevoelige informatie te sturen. Het label is die "contextstempel" op je data; Copilot en andere systemen zien die stempel en passen hun gedrag dienovereenkomstig aan. Labeling biedt daarmee een onmisbare basis van vertrouwen om veilig met AI-productiviteitstools te werken.

Houd het simpel: **labels die iedereen snapt**

Een grote valkuil bij het opzetten van informatieclassificatie is **over-engineering**. Het lijkt misschien verleidelijk om een waslijst van 10+ labels te maken om *elk* scenario af te dekken, maar in de praktijk werkt dat averechts. Gebruikers raken in de war van te veel keuze en gaan of lukraak iets selecteren, of erger nog, het labelen helemaal vermijden.

De beste aanpak is: begin met een beperkte set labels die voor iedereen duidelijk zijn. Veel experts raden een "Top-4" hiërarchie aan. Bijvoorbeeld de volgende vier categorieën (met mogelijke Nederlandse benamingen):

- **Openbaar** – ***Publiek of voor algemeen gebruik***. Informatie die zonder bezwaar extern gedeeld mag worden, zoals persberichten, marketingmateriaal of openbare website-inhoud.
- **Intern** – ***Alleen voor interne medewerkers***. Bedoeld voor documenten die niet publiek horen te worden, maar die binnen de organisatie vrij gedeeld mogen worden (bijv. interne beleidsstukken, teamupdates).
- **Vertrouwelijk** – ***Beperkt en op basis van need-to-know***. Gevoelige informatie die alleen toegankelijk mag zijn voor specifieke teams of rollen binnen de organisatie. Denk aan financiële rapporten, offertes, klantgegevens, personeelsdossiers, etc.
- **Geheim** – ***Zeer gevoelige data, strikt beperkt toegang***. Alleen bestemd voor een zeer beperkte kring van specifieke medewerkers. Hier horen vaak extra beveiligingsmaatregelen bij, zoals sterke **encryptie** en beperkingen op delen of kopiëren. Voorbeelden: aankomende fusie- of overnamedocumenten, top-level strategische plannen, juridische stukken voor de RvB.

Deze vier hoofdlabels dekken zo'n 95% van de gevallen voor veel organisaties. Iedereen begrijpt intuïtief wat het verschil is tussen openbaar, intern, vertrouwelijk en geheim, en dat is precies wat je wilt. Hoe eenvoudiger en helderder de classificatie, hoe groter de kans dat mensen 'm ook daadwerkelijk juist toepassen. Deze labels zijn natuurlijk slechts een leidraad. Creëer labels die passen bij jou organisatie.

Praktische tip: besteed net zoveel aandacht aan de omschrijving van elk label als aan de naam. In de gebruikersinterface (bijv. in Microsoft 365-apps) krijgt de gebruiker vaak via een tooltip of beschrijving te lezen wat een label betekent. Schrijf die teksten in gewone mensentaal:

- Bij **“Intern”** bijvoorbeeld: *“Voor documenten bedoeld voor collega’s. Niet delen met klanten of externen.”*
- Bij **“Vertrouwelijk”**: *“Bevat gevoelige informatie zoals klantcontracten, financiële gegevens of persoonsgegevens. Alleen delen met interne betrokkenen.”*

Duidelijke uitleg helpt om wildgroei of misbruik te voorkomen. Onthoud ook: liever een paar goed doordachte labels die men consistent gebruikt, dan twintig labels die genegeerd worden. Je kunt later altijd meer detail toevoegen (bijv. sublabels voor specifieke afdelingen of projecten) als dat écht nodig blijkt, zeker nu Microsoft bezig is met Sensitivity Label Groups om labels beter te groeperen in de interface. Maar vermijd die complexiteit in de beginfase.

Houd classificatie simpel

Te veel verschillende categorieën maken gebruikers onzeker. Begin met een duidelijke Top-4 (Openbaar, Intern, Vertrouwelijk, Geheim) die *95%* van de situaties dekt.

Betrek de inhoudsdeskundigen

Definieer samen met business stakeholders (bijv. Data Stewards) wat elke labelcategorie betekent en welke voorbeeldgegevens erin vallen. Zo sluit het beleid aan op de praktijk en snapt iedereen het.

Communiceer in mensentaal

Voorzie elk label van een duidelijke omschrijving in begrijpelijke taal voor eindgebruikers. Een goede toelichting (tooltip) bij het label voorkomt giswerk en verkeerde keuzes.

Voorkom valse zekerheid

Maak niet de fout om alles standaard op één label te zetten “voor de veiligheid”. Dit leidt tot schijnveiligheid en onverschilligheid bij gebruikers. Stimuleer bewust kiezen van het juiste label per geval.

Een sterke labelstrategie is niet in beton gegoten, het is een groeiend proces. Het advies is dan ook: **begin overzichtelijk en breid pas uit wanneer dat echt nodig is.** Hoewel techniek veel kan oplossen, ontslaat het organisaties niet van de plicht om eerst goed na te denken over een *eenvoudige*, *begrijpelijke structuur* voor de eindgebruiker.

De rol van Sensitivity Label Groups

Om organisaties te ondersteunen bij het voorkomen van wildgroei, heeft Microsoft Sensitivity Label Groups geïntroduceerd. Dit is de moderne opvolger van de oude **parent/sublabel-structuur**. Waar de oude hiërarchie soms leidde tot verwarring, werken Label Groups als logische mappen. Dit biedt belangrijke voordelen:

- **Geen keuzestress:** Eindgebruikers verdrinken niet in een eindeloze lijst met labels, maar navigeren via herkenbare categorieën.
- **Hogere adoptie:** Door labels logisch te clusteren (bijvoorbeeld op basis van project of afdeling), vinden medewerkers sneller de juiste beveiliging.
- **Gebruiksvriendelijkheid:** Het werkt intuïtiever dan de traditionele sublabels, wat de drempel om correct te classificeren verlaagt.

Handmatig vs. automatisch labelen: mens of machine?

Gevoeligheidslabels kunnen op twee manieren worden toegewezen: **handmatig** door de gebruiker of **automatisch** door het systeem. De meningen over de beste startmethode verschillen aanzienlijk. Wat mij betreft zit hier geen goed of fout in, de keuze is maatwerk.

Ik kijk persoonlijk zelf altijd naar twee bepalende factoren:

Het volwassenheidsniveau van de organisatie: Moet de focus eerst op bewustwording liggen (*handmatig*), of is de organisatie klaar voor grootschalige systeemlogica (*automatisch*)?

De Microsoft 365-licentie: De licentie bepaalt de technische mogelijkheden. Hierover in de paragraaf "*Licenties: wat kun je met E3 vs. E5?*" meer. In de basis is het grootste verschil qua licenties als volgt:

- **Microsoft 365 Business Premium & E3:** Deze licenties ondersteunen het **handmatig** labelen van documenten en e-mails.
- **Microsoft 365 E5:** Deze licentie stelt de organisatie in staat om labels **automatisch** te laten toewijzen op basis van de inhoud van het bestand.

Hieronder staat iets meer context ten aanzien van handmatig en automatisch labelen:

- Handmatig labelen: Hierbij kiest een gebruiker zelf een label voor een document, e-mail of Teams-chatbericht op basis van de inhoud.

    - **Voordeel** is dat de *inhoudeigenaar* (de maker) vaak het beste weet hoe gevoelig iets is. Bovendien dwingt het handmatig labelen gebruikers om bewust na te denken over de gevoeligheid van informatie, een nuttige oefening die de algehele security awareness verhoogt.

    - **Nadeel** is dat het foutgevoelig is: mensen vergeten wel eens te labelen of kiezen gemakshalve het eerste label in de lijst, zeker als ze de waarde er niet van inzien. Daarom is training en gebruiksvriendelijkheid hier cruciaal.

- **Automatisch labelen**: Bij geavanceerdere licenties (meer hierover in de volgende sectie) kan Microsoft Purview on-the-fly of achteraf labels toepassen op basis van inhoud. Dit gebeurt op basis van regels en AI-modellen. Bijvoorbeeld, je kunt een policy instellen die zoekt naar gevoelige informatie (zoals BSN's, creditcardnummers of bepaalde trefwoorden) in documenten en e-mails, en automatisch een passend label toekent of aanbeveelt.

  Microsoft Purview beschikt over meer dan 300 ingebouwde "**Sensitive Information Types**" (patronen voor bijv. BSN, creditcard, IBAN, medische info) en zelfs trainable classifiers (AI-modellen die complexere categorieën kunnen herkennen, zoals "bedrijfskritische informatie" of "vertrouwelijke HR-gegevens").

Let op: automatische labeling vereist wel de juiste licenties en configuratie (zie volgende sectie). Bovendien moet je zorgvuldig testen, je wilt niet dat het systeem per ongeluk te veel of te weinig labelt. Begin bijvoorbeeld met policies in "alleen aanbevelen" modus, zodat je kunt monitoren hoeveel content in een bepaalde categorie zou vallen voordat je automatische toepassing inschakelt.

Licenties: wat kun je met E3 vs. E5?

Je hebt niet per se een E5-licentie nodig om met gevoeligheidslabels te beginnen. Met een Microsoft 365 E3 (of Business Premium) licentie kun je al veel doen op het gebied van handmatig labelen en basisbescherming. Toch ontgrendelt E5 (of E3 met de *Compliance* addon) een reeks geavanceerde functies die het leven een stuk makkelijker maken. Hieronder zetten we de belangrijkste verschillen op een rij:

Licentie	Mogelijkheden & kenmerken	Aanpak
Microsoft 365 Business Premium / E3	• *Handmatig labelen*: gebruikers kiezen zelf de juiste label in Microsoft 365-apps (Word, Excel, PowerPoint, Outlook, etc.). • Basisbescherming: je kunt labels koppelen aan versleuteling en visual markings zoals kopteksten/watermerken. • **Geen automatische labeling** van opgeslagen data via policies (wel	• **Focus op bewustwording en discipline:** Train medewerkers goed, want correcte labeling hangt vooral af van menselijk handelen en consistent gebruik van labels. • Organiseer awareness-sessies en stel *labelambassadeurs* aan in teams die collega's

	beperkte automatische detectie, bijvoorbeeld dat Office eenmalig een suggestie doet).	kunnen helpen. Zonder geavanceerde automatische tools is een **sterke securitycultuur** essentieel.
Microsoft 365 E5 (of E3 + Compliance-addon)	• *Alles van E3*, **plus**: **Automatisch labelen** van zowel *documenten* als *e-mails* op basis van gevoelige info (SIT's). • **Auto-labeling policies voor data at rest** in SharePoint en OneDrive. • **Trainable classifiers** voor inhoud die je niet met een simpel patroon kunt vangen (AI-gedreven herkenning van bijvoorbeeld "vertrouwelijke projecten"). • **Aanbevolen labels** (suggesties aan gebruikers op basis van inhoud) voor Office-documenten en e-mails. • **Content Explorer** en **Activity Explorer** dashboards voor inzicht in waar labels worden gebruikt en welke acties er plaatsvinden. • Nauw integreren met **DLP** en **Insider Risk Management** voor geautomatiseerde handhaving (bijv. autom. blokkeren of alerten bij ongewenst delen).	• **Focus op technologie & borging:** Maak gebruik van de geavanceerde functies om menselijke fouten te reduceren. Richt automatische labeling in waar mogelijk, zodat vertrouwelijke info ook gelabeld wordt als gebruikers het vergeten. • Gebruik DLP om te voorkomen dat verkeerd omgegaan wordt met gevoelige data. De aanpak verschuift van louter training naar **automatisering die beleid afdwingt,** al blijven training en awareness nog steeds belangrijk om draagvlak te krijgen.

Tip: Begin je met E3, dan kun je al heel wat bereiken met een goede planning en bewustwordingscampagne. Zorg voor management buy-in en creëer bijvoorbeeld een groep *Information Protection Champions* binnen elk afdelingsteam die collega's kunnen coachen in het juiste gebruik van labels. Upgrade je later naar E5, dan kun je de

automatisering stapsgewijs toevoegen aan je bestaande labels en beleid, dat vergt aanvankelijk wat werk, maar levert uiteindelijk veel tijdswinst en minder incidenten op.

> **Belangrijk:** Microsoft is begin 2024 strenger geworden in het handhaven van licentievoorwaarden: bepaalde features zoals automatische labeling kunnen technisch soms (deels) werken op E3, maar zijn formeel alleen toegestaan met de juiste licentie. Voorkom verrassingen en zorg dat je licenties in orde zijn voordat je geavanceerde functies inzet.

Gevoeligheidslabels configureren: opties en best practices

Wat kun je nu allemaal instellen bij een gevoeligheidslabel? In grote lijnen zijn er twee soorten instellingen: *beschermingsacties* die automatisch doorgevoerd worden als het label is toegepast, en *beleidsinstellingen* die bepalen hoe en wanneer het label wordt gebruikt. We lopen de belangrijkste opties langs:

- **Encryptie (versleuteling)**: Hiermee kun je regelen *wie* een gelabeld document of e-mail mag openen en *wat ze ermee mogen doen*. In de Microsoft Purview portal kun je per label instellen of er Azure Rights Management versleuteling moet worden toegepast. Je hebt dan twee keuzes:
    - **Nu machtigingen toewijzen**: Jij bepaalt als admin precies welke personen of groepen toegang krijgen en met welke rechten (lezen, bewerken, printen, doorsturen, etc.). Bijvoorbeeld: alleen mensen van de HR-afdeling mogen “HR Vertrouwelijk” documenten openen, en ze mogen ze niet extern doorsturen of afdrukken.
    - **Gebruikers laten machtigingen kiezen**: Je laat de medewerker zelf bepalen *wie* een specifiek gelabeld document mag lezen (bij het toepassen van het label). Dit geeft wat flexibiliteit, maar minder centrale controle.
- Als encryptie aan een label is gekoppeld, wordt het bestand zelf versleuteld en gebonden aan de Azure Rights Management (RMS) infrastructuur. Dit betekent dat de toegangscontroles onlosmakelijk met het document meereizen, waar het ook gaat. Zelfs buiten de eigen omgeving of na downloaden blijft het bestand beschermd: alleen geautoriseerde accounts kunnen het openen.
- *Voorbeeld:* Een document met label **“Geheim”** kan zo geconfigureerd zijn dat alleen de directie het mag openen en niet mag worden doorgestuurd of geprint. Stuur je per ongeluk toch zo’n document naar een onbevoegd persoon, dan kan die er niets mee beginnen, het blijft **onleesbaar versleuteld**.

- *De superuser-rol is standaard uitgeschakeld* en moet expliciet door een Global Admin worden geactiveerd en toegewezen via PowerShell (**Enable-AipServiceSuperUserFeature**). Gebruik deze rol spaarzaam en alleen voor geautoriseerde personen of services, en schakel hem uit als hij niet nodig is – alle gebruik wordt namelijk gelogd voor auditdoeleinden. Zo kun je altijd nagaan wie, wanneer en waarom iets heeft ontsleuteld.

- **Content markering (visuele markeringen)**: Om gebruikers duidelijk te maken dat iets gevoelig is, kun je labels automatisch een markering laten toevoegen aan documenten en e-mails. Denk aan een koptekst of voettekst ("Vertrouwelijk – niet delen met externen") of een watermerk diagonaal over een document ("Internal Use Only"). Zulke zichtbare indicaties waarschuwen lezers om voorzichtig te zijn met de inhoud. *Dynamic watermarks* (watermerken die bijvoorbeeld de gebruikersnaam of tijdstip bevatten) zijn inmiddels mogelijk in Microsoft 365-documenten, al werken ze niet in alle scenario's; Microsoft 365 zal anders het openen blokkeren als de client het watermerk niet aankan.

- Content markering is met name handig als je géén encryptie toepast (Route A uit mijn voorbeeld hieronder). Het verhoogt de bewustwording bij de ontvanger: een duidelijk **"Vertrouwelijk – bedrijf X"** watermerk op een document herinnert iedereen eraan dat dit document gevoelige informatie bevat. Het is geen technische barrière, maar wel een *mentale stop*.

- **Site- en Team-labeling (containers)**: Naast individuele documenten en e-mails kun je ook complete SharePoint-sites, Teams en Microsoft 365 Groepen een gevoeligheidslabel geven. Dit wordt ook wel *container labeling* genoemd. Het idee: je markeert een volledige locatie als bijv. "Vertrouwelijk", waarna automatisch bepaalde beveiligingsinstellingen voor die héle site of team gelden.

  Bijvoorbeeld: een Team met het label Vertrouwelijk kan zo worden ingesteld dat:
  - Toegang beperkt is tot alleen leden (privé-team) en gastgebruikers *zijn niet toegestaan*.
  - Bestanden in dat team alleen vanaf bedrijf managed devices geopend mogen worden (blokkeert downloaden naar onbeheerde apparaten).
  - Optioneel: de SharePoint-site krijgt automatisch bepaalde share-instellingen (bijv. geen *extern delen* toegestaan voor sites met een streng label). Container labeling helpt om de *omgeving waarin gevoelige data leeft* te beveiligen en gebruikers te laten weten dat alles in die ruimte vertrouwelijk is.

Let op: een site- of teamlabel versleutelt niet alle individuele bestanden daarin; het beschermt vooral de *toegangsgrenzen van de locatie*. Wel registreert Purview het als er een bestand met een hoger label (bijv. Geheim) in een lager gelabelde site (bijv. Intern) wordt geplaatst – zo'n mismatch komt als event in de audit logs, zodat je erop kunt acteren.

- **"Downgrade" instellingen**: Je kunt bij labels instellen dat verlaging of verwijdering van een label een *justificatie* vereist. Dit betekent dat als iemand een document van Vertrouwelijk terugzet naar Intern of Openbaar, hij/zij wordt gevraagd om een reden op te geven. Die reden wordt mee vastgelegd in de logbestanden.

  Dit is geen keiharde beveiliging (iedereen kan iets intypen), maar het zorgt wél voor bewustwording ("weet je zeker dat je dit label wilt verwijderen? Waarom?") *en* het geeft beheerders inzicht in waarom labelwijzigingen plaatsvinden. Vaak werkt zo'n drempel al preventief tegen het lukraak weghalen van labels, en als het toch gebeurt kun je in de audit logs nagaan of de reden legitiem was.

- **Label policies**: Nadat je labels hebt aangemaakt, publiceer je ze naar gebruikers via *Label Policies*. Hierin stel je in welke gebruikers of groepen de labels te zien krijgen in hun apps. Ook kun je per policy regels instellen zoals:
  - Welk label is standaard voor nieuwe documenten/e-mails (indien je een default label wilt toewijzen).
  - Of een label verplicht is (bijv. dat gebruikers een label móéten kiezen voordat ze iets kunnen opslaan of verzenden).
  - Of gebruikers labels zelf mogen overschrijven of verwijderen van bepaalde content.
  - Specifieke instellingen voor Outlook (bijv. verplicht labelen van mails die bepaald type gegevens bevatten). Denk goed na voordat je labeling *verplicht* stelt voor de hele organisatie. Vaak is het slim om dit gefaseerd te doen: eerst ervaring opdoen met vrijwillig labelen in een pilot, dan pas eventueel verplichtingen invoeren (zie ook *Adoptiestrategie*). Als je direct iedereen dwingt een label te kiezen zonder dat men goed begrijpt waarom, loop je risico op weerstand of foutieve labeling (bijv. iedereen kiest maar lukraak iets om van de pop-up af te zijn).

- **Scope en uitzonderingen**: Standaard gelden gevoeligheidslabels voor Microsoft 365-bestanden (Word, Excel, PowerPoint), e-mails en (recent) ook voor dingen als PDF's en sommige afbeeldingen (middels de AIP client die classificatie-

informatie kan insluiten in PDF/JPG-bestanden). Containerlabels gelden voor SharePoint, Teams, Microsoft 365 Groups.

Je kunt in Purview aangeven welke soorten items onder een label vallen. Zo kun je bijvoorbeeld een label maken dat *alleen voor e-mails* te gebruiken is, of juist een label dat *alleen voor SharePoint-sites* bedoeld is. Dit gebruik je bijv. voor een label "Publiek extern" dat alleen als sitelabel bestaat maar niet voor documenten.

Tot zover de belangrijkste instellingen. Huawei's motto ***"Make it simple"*** gaat ook hier op: **je hoeft niet alles in één keer te configureren**. Sommige organisaties kiezen er bewust voor om in eerste instantie geen encryptie toe te passen op een label om de impact op de gebruiker laag te houden, en zetten dat pas later aan als de adoptie op orde is. Denk in termen van *"Minimum Viable Product"*: begin met wat nodig is om duidelijkheid te scheppen (bijv. visual markings en simpele policies), en voeg complexere beveiliging toe naarmate de organisatie eraan toe is.

Rollen en verantwoordelijkheden bij informatiebescherming

Een succesvol Information Protection programma is **teamwerk**. Het is belangrijk om de juiste mensen te betrekken en duidelijke verantwoordelijkheden toe te kennen. Hier zijn de belangrijkste rollen die in de praktijk vaak een rol spelen bij het implementeren en beheren van gevoeligheidslabels:

Rol	Verantwoordelijkheden
Information Protection Administrator	*"Knoppendraaier" en technisch eigenaar van de labeling-oplossing*. Deze beheerder richt de gevoeligheidslabels in via de Purview portal. Hij/Zij bepaalt welke labels er zijn, hoe ze geconfigureerd zijn (encryptie ja/nee, markeringen, etc.), en publiceert ze naar de juiste gebruikers of groepen. Vaak is dit iemand vanuit IT of Security. De IP Admin bewaakt ook de dagelijke werking: kloppen de instellingen nog, moeten er nieuwe labels komen, etc.
Compliance / Security Administrator	*Bewaker van het brede compliance- en securitybeleid*. Deze persoon of team houdt het totaaloverzicht over alle **Microsoft Purview** onderdelen: niet alleen labeling, maar ook **Data Loss Prevention**, **eDiscovery**, **retentie** en eventueel **Insider Risk Management**. Ze zorgen voor samenhang tussen de verschillende maatregelen en dat de organisatie voldoet aan relevante wet- en regelgeving. Ook monitoren ze rapportages en alerts (bijv. in het Compliance Center of Sentinel) om in te grijpen bij afwijkingen of incidenten.

Data Steward / Gegevens-eigenaar	*Inhoudsdeskundige vanuit de business*. Dit is meestal iemand uit een bepaalde afdeling (bv. HR, Financiën, Legal) die begrijpt **wat** er gevoelig is binnen die afdeling en **waarom**. De Data Steward helpt bij het definiëren van de classificaties, welke informatie krijgt welk label, in begrijpelijke taal voor collega's. Hij/Zij fungeert als schakel tussen IT en de eindgebruikers: helpt bij het opstellen van goede labelomschrijvingen, denkt mee over uitzonderingen, en treedt soms op als **ambassadeur** of vraagbaak binnen de eigen afdeling.

Afhankelijk van de grootte van je organisatie kunnen deze rollen anders heten of door dezelfde personen worden vervuld. Het belangrijkste is **dat de verantwoordelijkheden geborgd zijn**:

- Iemand moet de technische kant inrichten en beheren.
- Iemand moet de beleidsmatige kant bewaken (en zorgen dat alle compliance-eisen worden afgedekt).
- Iemand uit de *business* moet meedenken over wat beschermd moet worden en helpt de vertaalslag te maken naar praktische richtlijnen voor collega's.

Zet deze mensen bij elkaar aan tafel, bijvoorbeeld in een projectteam of werkgroep informatiebeveiliging, om samen het labelbeleid vorm te geven. En vergeet niet de gewone medewerker: uiteindelijk is elke collega onderdeel van het succes. Zorg dat iedereen weet waarom jullie dit doen en bij wie ze terecht kunnen met vragen ("Mag dit bestand naar buiten? Welk label moet ik kiezen voor *dit* document?").

Adoptie en veranderaanpak: mens & proces voorop

Technologie is slechts één kant van de medaille, voor een succesvolle implementatie van labeling is aandacht voor **mens en proces** net zo belangrijk. Hier zijn enkele **adoptiestrategieën** en *best practices* om medewerkers mee te krijgen en het beleid duurzaam te verankeren:

- **Top-down support en communicatie**: Zorg voor duidelijke communicatie vanuit het management over het *waarom* van informatiebescherming. Koppel het bijvoorbeeld aan de bedrijfswaarden ("Wij beschermen klantvertrouwelijkheid") en benoem het als enabler voor moderne oplossingen als Copilot (je hebt goede data nodig voor goede AI). Een duidelijke boodschap van de directie helpt om het belang te onderstrepen.

- **Training en bewustwording**: Organiseer praktische workshops, e-learnings en intranetcampagnes om medewerkers wegwijs te maken in de nieuwe labels. Laat zien *hoe* ze een label kunnen toepassen in Word, Outlook etc., maar besteed vooral aandacht aan *wanneer en waarom* ze een bepaald label moeten

kiezen. Gebruik herkenbare voorbeelden (“Stel, je maakt een lijst met klantgegevens – welk label kies je?”) en geef mensen de kans om vragen te stellen. Dit is vooral van belang als je labeling eerst handmatig door gebruikers laat doen (E3-scenario) – de consistentie valt of staat met hun begrip.

- **Gebruik ambassadeurs**: Identificeer per afdeling één of meerdere security champions of label-ambassadeurs (vaak de Data Stewards of een key user) die extra getraind worden. Zij kunnen collega’s ondersteunen op de werkvloer bij vragen of onduidelijkheden, en ze kunnen feedback uit de praktijk terugkoppelen aan het projectteam voor verbetering.

- **Maak het gebruikersvriendelijk**: Integreer labeling zo frictieloos mogelijk in bestaande werkprocessen. Bijvoorbeeld: als je het label “Vertrouwelijk” invoert, overweeg om *geen al te hinderlijke restricties* in eerste instantie op te leggen (zoals in Route A zonder encryptie – zie verderop). Zo ervaren gebruikers wel de *visuele en culturele impact* van labeling, zonder dat hun dagelijkse werk te veel gehinderd wordt. Daarna kun je de touwtjes geleidelijk aantrekken (bijv. later encryptie aanzetten of labels verplicht maken) zodra men gewend is.

- **Vier successen & leer van fouten**: Deel positieve verhalen. Bijvoorbeeld: “Afdeling Financiën heeft in 3 maanden 90% van alle vertrouwelijke documenten netjes gelabeld!” of “Dankzij labeling heeft HR voorkomen dat gevoelige info naar buiten ging.” Dit motiveert anderen. En als er iets misgaat (bijv. per ongeluk verkeerd gelabeld): gebruik dat als leermoment in plaats van meteen met het vingertje te wijzen.

- **Veranderende cultuur**: Onderstreep dat labeling niet bedoeld is als controle-instrument om mensen te straffen, maar als gezamenlijk hulpmiddel om de organisatie en elkaar te beschermen. Een quote uit de praktijk: *“***Door elke keer een label te kiezen, leer je eigenlijk zelf bewuster om te gaan met informatie.***”* Dit creëert een cultuur waarin informatieveiligheid ieders verantwoordelijkheid is. Die cultuurverandering is minstens zo waardevol als de technologie zelf.

Uiteindelijk draait adoptie om het vinden van de juiste balans tussen menselijk gedrag en technologische hulpmiddelen. Met Purview E5 kun je meer automatiseren (labels worden dan op de achtergrond toegepast), maar ook dán is duidelijke

communicatie en opleiding nodig om ervoor te zorgen dat medewerkers begrijpen wat er gebeurt en waarom.

Monitoring en sturing: **zicht houden op je data**

Zodra je labels in gebruik zijn, wil je uiteraard weten wat er met je gelabelde data gebeurt. Microsoft Purview biedt hiervoor een paar krachtige tools, en je kunt de informatie uit het systeem ook koppelen aan je eigen monitoring-oplossingen:

- **Content Explorer (Dataverkenner)** – Dit dashboard geeft je een live overzicht van *waar je gelabelde (of anderzins gevoelige) informatie zich bevindt*. Je ziet bijvoorbeeld: *"1200 documenten met label Vertrouwelijk op SharePoint-site X, 300 documenten met BSN-informatie in OneDrive van gebruiker Y"*. Content Explorer laat hotspots zien: waar zit de gevoelige data geconcentreerd? Gebruik dit om op te sporen of gegevens misschien op verkeerde plekken staan.

  Voorbeeld: ontdek je honderden **Geheim**-bestanden op een SharePoint die openstaat voor het hele bedrijf, dan weet je dat je direct moet ingrijpen. Zeker vóór je met Copilot start, is het slim om via Content Explorer te checken of er geen kroonjuwelen op straat liggen.

- **Activity Explorer (Activiteitenverkenner)** – Dit is als een beveiligingscamera voor acties op gelabelde content. Het laat zien *wie wat doet met je gevoelige informatie*. Bijvoorbeeld: wie past een label toe, wie wijzigt of verwijdert een label, wie opent een gelabeld document, etc. Deze gebeurtenissen komen uit het Unified Audit Log van Microsoft 365 en worden in Activity Explorer overzichtelijk getoond met filters. Je kunt bijvoorbeeld specifiek zoeken op "Sensitivity label changed" of "Sensitivity label removed" acties. Daarmee kun je al snel zien of er opvallende dingen gebeuren.

  - **Copilot-monitoring:** Je kunt checken of **Copilot-gegenereerde content** netjes een label krijgt (de regel is: hoogst gevoelige bron bepaalt het output-label). Ook kun je zien of gebruikers zelf stiekem labels verlagen. Als je bijvoorbeeld merkt dat een bepaalde gebruiker structureel het label *Vertrouwelijk* verwijdert van documenten ("downgraden"), kun je dat gesprek aangaan of extra maatregelen nemen. Heb je *downgrade justification* aanstaan, dan zie je ook meteen de reden die de gebruiker invulde bij het verwijderen van het label.

  - **Auditing & rapportage:** Al deze acties – het toekennen, wijzigen en verwijderen van labels, worden ook centraal gelogd in de audit logs van

Microsoft 365. Je kunt deze logs zelf opvragen via de Purview Audit (eDiscovery) of PowerShell, en erover rapporteren.

Zo blijkt bijvoorbeeld uit praktijkcases dat het bijhouden van label-downgrades een goede indicator kan zijn voor risico's: medewerkers die repetitief labels omlaag bijstellen of verwijderen zouden potentieel data kunnen willen "exfiltreren". Microsoft's Insider Risk Management kan dit soort gedrag automatisch in de gaten houden en alert geven bij verdachte patronen.

- **Inzicht via Microsoft Sentinel** – Voor geavanceerdere monitoring en correlatie met andere beveiligingsgebeurtenissen is integratie met Microsoft Sentinel (SIEM) heel waardevol. Microsoft heeft een dataconnector ontwikkeld om Purview Information Protection events naar Sentinel te sturen. Je kunt hiermee in Sentinel een rijk overzicht krijgen van:

    - Welke labels worden hoe vaak gebruikt (label adoption over tijd).
    - Wanneer en door wie gevoelige documenten zijn geopend, van een ander label worden voorzien of verwijderd.
    - Correlaties met andere gebeurtenissen: bijvoorbeeld het detecteren dat kort na het downgraden van een label een bestand via e-mail naar buiten is gestuurd – dat zou kunnen wijzen op een bewuste omzeiling. Met Sentinel kun je zulke scenario's detecteren en automatisch een alert of zelfs een blokkade instellen.

Kortom, implementatie is niet het einde van de reis maar het begin. Door goed te **monitoren** kun je zien of het beleid werkt: Worden de beoogde documenten inderdaad gelabeld? Waar zit nog ongeclassificeerde gevoelige data? Zijn gebruikers geneigd om onnodig alles *Vertrouwelijk* te labelen, of juist niets? Met deze inzichten kun je trainingen bijsturen of je beleid verder aanscherpen. Labeling is dus geen "**set-and-forget**" oplossing, maar onderdeel van een continue verbeter-cyclus in je data governance.

Stapsgewijs aan de slag: voorbeeldscenario "Vertrouwelijk" label

Het is tijd om theorie om te zetten in praktijk. Hieronder bespreken we een concreet stappenplan om een nieuw label, bijvoorbeeld "Vertrouwelijk", in te voeren. Dit scenario laat zien hoe je gefaseerd te werk kunt gaan, van ontwerp tot uitrol en evaluatie. Mijn advies: begin klein met één of enkele labels en scenario's, en breid uit op basis van geleerde lessen.

Stap 1: Begrip & definitie

Bepaal wat 'Vertrouwelijk' betekent in jouw organisatie. Werk samen met *Data Stewards* en inhoudsdeskundigen om concreet te omschrijven welke informatie hieronder valt (bijv. klantcontracten, offertes, persoonsgegevens). Leg dit vast in heldere taal als basis voor je labelomschrijving.

Stap 2: Beveiligingsniveau kiezen

Kies de juiste bescherming voor 'Vertrouwelijk'. Beslis of je dit label gaat gebruiken met of zonder *encryptie*. - Optie A: Gebruiksvriendelijk (zonder encryptie) – Kies géén versleuteling, maar wél visuele markeringen (bijv. watermerk 'Vertrouwelijk'). Voordeel: iedereen kan de gelabelde documenten blijven openen en samenwerken zonder extra drempels. Nadeel: als het document uitlekt, is het weliswaar gemarkeerd als vertrouwelijk maar technisch niet beschermd. - Optie B: Strenger (met encryptie) – Koppel wel versleuteling aan het label, zodat alleen bepaalde groepen (bijv. directie, projectteam) de inhoud kunnen openen. Voordeel: sterkere beveiliging; ongeautoriseerde personen kunnen er niets mee. Nadeel: kan samenwerking bemoeilijken als iemand buiten de groep toegang nodig heeft (er is dan extra handeling vereist). Ons advies: hanteer encryptie **vooral voor de hoogst gevoelige data** (je *Geheim*-label) of streng vertrouwelijke subsets, en kies voor het algemene label 'Vertrouwelijk' in eerste instantie eventueel een gebruiksvriendelijkere aanpak zonder encryptie, tenzij regelgeving anders eist.

Stap 3: Label aanmaken & instellen

Creëer het label in de Purview portal. Ga naar *Information Protection* > *Labels* en voeg een nieuw label 'Vertrouwelijk' toe. Vul de naam in (of een naam die past bij jullie organisatiecultuur) én de **omschrijving** die je bij stap 1 hebt opgesteld – deze verschijnt als tooltip voor gebruikers en is enorm belangrijk voor begrip. Configureer vervolgens de instellingen: - Bij optie A: **Alleen visuele markeringen** instellen (bijv. header/footer tekst "Vertrouwelijk"). - Bij optie B: **Encryptie-instellingen** configureren (specificeer wie het mag openen: bijvoorbeeld enkel collega's binnen de afdeling, of individuen/groepen X en Y). Voeg eventueel ook hier een watermerk of header toe voor de duidelijkheid. *Pro-tip:* Schakel "require justification on downgrade" in voor dit label. Dan moeten gebruikers een reden opgeven als ze "Vertrouwelijk" proberen te verwijderen of te verlagen naar een lager label. Dit helpt misbruik voorkomen en geeft jou inzicht in mogelijke *valse positieven* of bewust misbruik.

Stap 4: Pilot-publicatie

Publiceer het label beperkt om te testen. Maak een nieuwe **Label Policy** aan voor je 'Vertrouwelijk' label, maar target deze in eerste instantie op een kleine *pilotgroep*. Bijvoorbeeld: alleen het IT-team en een paar enthousiaste eindgebruikers uit de business. Laat hen een paar weken met het nieuwe label werken en ervaringen terugkoppelen.
Beleid: Zet in de pilot-policy het label *niet* direct verplicht voor alle nieuwe documenten, en stel het ook niet als standaardlabel – je wilt eerst zien hoe mensen het vrijwillig toepassen. Gebruik de pilotfase om je uitleg, training en eventueel de labelinstellingen te verfijnen op basis van feedback.

Stap 5: Label ook locaties (containers)

Toepassen van het label op een Teams-site of SharePoint-site. Vergeet niet dat je het label **'Vertrouwelijk' ook kunt plakken op een volledige Microsoft 365-groep (Team/SharePoint). Doe dit bijvoorbeeld voor een projectsite waar vertrouwelijke info wordt gedeeld. Met een *site-label* kun je instellen dat de site privé is, dat extern delen uitstaat en dat alleen beheerde devices toegang hebben. Zo creëer je een veilige omgeving voor het project.
Let op: Het container-label beschermt de omgeving, niet automatisch alle bestanden erin. Als iemand een document met hogere classificatie (bijv. *Geheim*) in deze *Vertrouwelijk*-omgeving zet, logt Purview dat als afwijking zodat je actie kunt ondernemen.

Stap 6: Organisatiebreed uitrollen & trainen

Schaal na de pilot gefaseerd op. Als de pilot succesvol is, pas de label policy aan om 'Vertrouwelijk' nu **breder beschikbaar te maken** of voor iedereen verplicht te stellen, afhankelijk van de uitkomst. Communiceer duidelijk de lancering: leg nogmaals uit *wat* het label betekent en *hoe* men het moet gebruiken. Gebruik eventueel simpele beslisbomen of infographics op het intranet (bijv.: *"Bevat je document persoonsgegeven X of bedrijfsgevoelige info Y? Kies label Vertrouwelijk."*).
Zorg dat de IT-servicedesk op de hoogte is en klaarstaat voor vragen. En **blijf opleiden**: herhaal de boodschap in nieuwsbrieven, phishing-tests (met reminders over classificatie) en vervolgtrainingen.
Monitor het gebruik actief via Content/Activity Explorer en stuur bij waar nodig. Merk je bijv. dat iedereen opeens elk document als Vertrouwelijk labelt, dan is extra uitleg nodig – kennelijk durven mensen geen keuzes te maken. Zie je juist dat niemand het label gebruikt, dan moet je drempels wegnemen of meer promoten.

Stap 7: Test met Copilot

Voer real-life scenario's uit met AI. Heb je (pilot)toegang tot Microsoft 365 Copilot, test dan in een veilige setting hoe het samenspel werkt. Vraag bijvoorbeeld binnen een gelabelde Teams-omgeving aan Copilot om een samenvatting te maken van een *Vertrouwelijk* document. Controleer of de output ook als *Vertrouwelijk* gelabeld wordt (zou moeten, anders kloppen de instellingen niet). Laat een collega zonder toegang tot die content dezelfde vraag stellen – die zou als het goed is niets terugkrijgen van Copilot, wat betekent dat je labels en rechten hun werk doen.
Experimenteer ook met handmatige acties: download een gelabeld bestand en verwijder het label, kijk in Activity Explorer of de *Sensitivity label removed* gebeurtenis is vastgelegd. Dit soort tests geven vertrouwen dat je inrichting functioneert. Blijkt iets niet goed te werken, dan kun je vóór een brede Copilot-rollout nog bijstellen.

Na deze stappen heb je een robuust “Vertrouwelijk” label gerealiseerd en waardevolle ervaring opgedaan. Het principe is hetzelfde voor andere labels: werk per label of per gebruiksscenario een vergelijkbaar traject af. Zo houd je de implementatie behapbaar en kun je leren en aanpassen voordat je doorgaat naar de volgende fase of een extra label toevoegt.

Start klein, leer bij, en schaal op – dat is de kern van een succesvolle label-implementatie. In plaats van in één keer twintig labels en policies de organisatie in te slingeren, kies je een paar belangrijke scenario’s (bijv. bescherming van klantdata of interne financieel gevoelige info) als piloot. Breid daarna geleidelijk uit naar meer datatypes, strengere policies (zoals encryptie of verplichte labels) of nieuwe labels voor andere gevoelige categorieën. Zo ontwikkel je stap voor stap een volwassen Information Protection programma.

Conclusie: veilig op weg naar AI met een sterk datafundament

In deze gids hebben we gezien hoe **Microsoft Purview Information Protection** je helpt om de *basis voor betrouwbare AI* te leggen. **Gevoeligheidslabels zijn het fundament voor een veilige inzet van tools als Microsoft 365 Copilot**: ze zorgen ervoor dat AI alleen werkt met data die door jouw organisatie is getoetst en geclassificeerd. Met labeling kun je *met een gerust hart gas geven op het gebied van AI*, omdat je de risico’s beheerst.

Maar vergeet niet: het succesvol beschermen van informatie is niet enkel een technische exercitie. Het vergt ook een **cultuurverandering** en doorlopend aandacht voor gegevensbeheer. Labeling dwingt je om na te denken over de waarde van informatie en bevordert zo een bewuste omgang met data in de hele organisatie.

Microsoft Purview en Copilot ontwikkelen zich doorlopend. Nieuwe functies zoals Sensitivity Label Groups vereenvoudigen het beheer van veel labels, en DLP-integraties voor Copilot maken AI nog veiliger in gebruik. Houd Microsoft’s updates (via bijvoorbeeld de Microsoft 365 Roadmap en Microsoft Learn) goed in de gaten en plan regelmatig reviews van je labelbeleid om nieuwe opties te benutten.

Uiteindelijk is een investering in informatieclassificatie en -bescherming een investering in de toekomstbestendigheid van je organisatie. Met een schoon datahuis, helder gelabelde informatie en goed ingeregelde beveiligingsmaatregelen wordt Microsoft 365 Copilot van een potentiële risico-factor juist een vertrouwde copiloot. AI zal dan de gevoeligheidsetiketten respecteren, meewerken aan jullie beveiligingsbeleid en alleen de juiste informatie ontsluiten voor de juiste mensen.

Met Microsoft Purview Information Protection bouw je aan dat vertrouwen in data. Het is je veiligheidsriem in een wereld vol AI-innovatie, daarmee kun je vol gas geven op de

digitale snelweg, terwijl je organisatie veilig en compliant blijft. Kortom, als de basis op orde is, kun je met een gerust hart de vruchten plukken van Copilot en andere AI-toepassingen, wetende dat je gevoelige informatie onder controle is.

Ready for take-off?

Zet de stap naar een data-gedreven toekomst, met labeling als opstap naar nieuwe mogelijkheden.