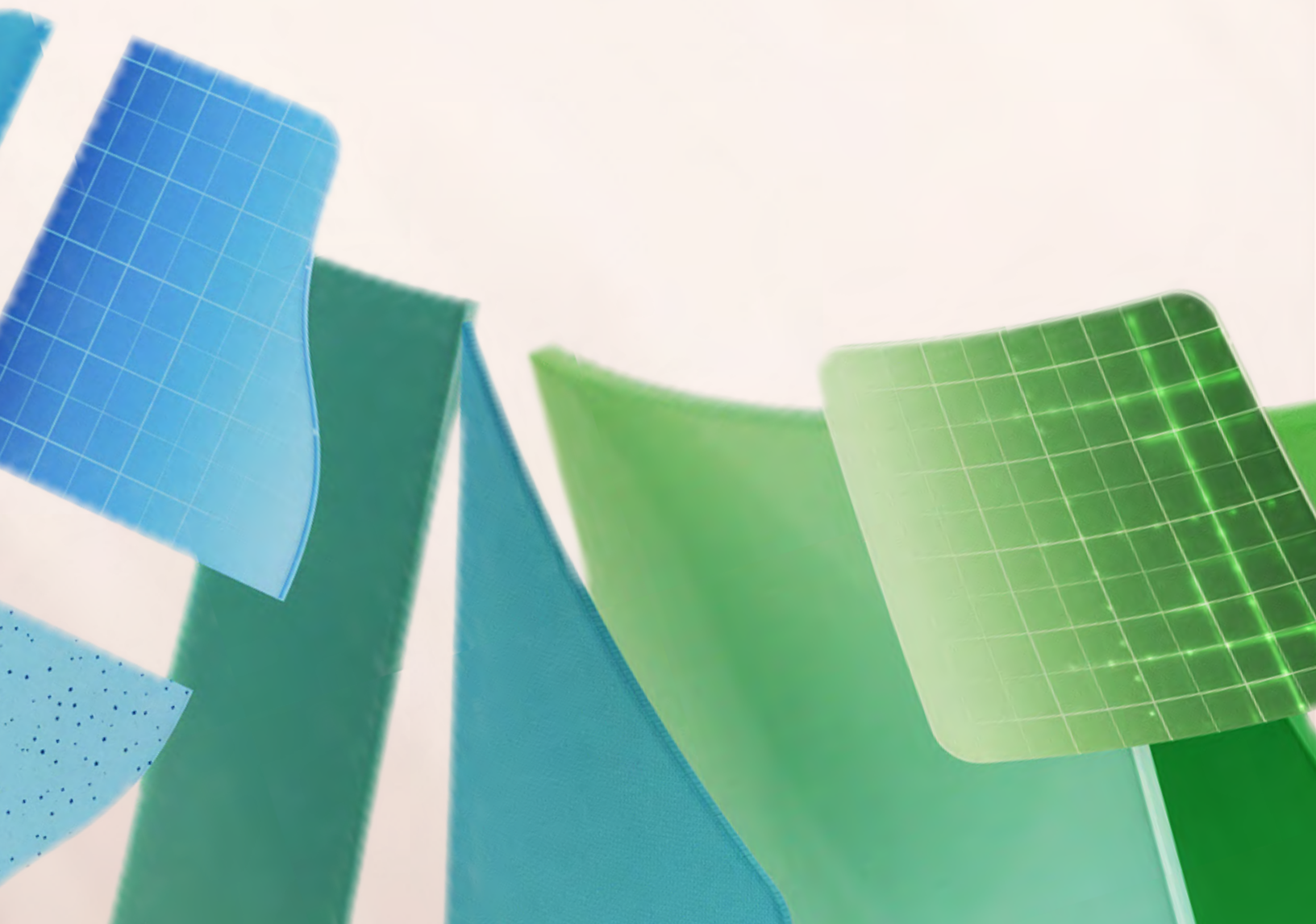


Data onder controle

Het belang van data governance voor
succes met AI



Inhoud

Inleiding

Data governance vormt de ruggengraat van een veilige AI-adoptie

Generatieve AI kan een bedrijf transformeren, maar het realiseren van dat potentieel hangt af van de kwaliteit en beschikbaarheid van je bedrijfsdata.

Organisaties met een sterke data governance kunnen de concurrentie een stap vóór blijven met AI. Data governance zorgt ervoor dat data die door AI wordt opgevraagd en gegenereerd, juist, veilig, gecontroleerd en compliant is.

Kwaliteit en beschikbaarheid van data:

AI-systemen hebben grote, hoogwaardige datasets nodig om de best mogelijke respons te bieden met de juiste context uit de unieke workflows van je organisatie. Een hogere datakwaliteit leidt tot effectievere AI-inzichten en -voorspellingen.

Compliance: Een sterke data governance zorgt voor naleving van de regelgeving, waardoor het risico op juridische problemen en boetes wordt verkleind.

Security: Door data op de juiste manier te labelen en te beheren wordt gevoelige informatie beschermd tegen ongeautoriseerde toegang, onbevoegd delen en datalekken.

Vertrouwen: Een betrouwbare data governance vergroot het vertrouwen van stakeholders in de uitvoer van AI, wat de adoptie en ondersteuning voor AI-initiatieven bevordert.

Dit eBook introduceert essentiële data governance-praktijken voor een organisatie die klaar is voor AI. Hierin wordt besproken hoe je robuuste normen voor datakwaliteit instelt, naleving van wettelijke vereisten waarborgt en maatregelen implementeert voor de bescherming van persoonsgegevens en de beveiliging. Je leert strategieën om het vertrouwen in AI-systemen te vergroten en data direct beschikbaar te maken om praktische inzichten te genereren, of het nu gaat om te voorkomen dat gevoelige inhoud van meetings extern wordt gedeeld of om de organisatie te beschermen tegen datalekken. Door deze praktijken toe te passen, kan je organisatie het volledige potentieel van AI benutten om te blijven innoveren en de concurrentie een stap vóór te blijven.

Gebruiksscenario's voor generatieve AI

Communicatie versnellen: Maak sneller gepersonaliseerde content, zodat je meer tijd overhoudt om relaties op te bouwen en samen te werken.

De efficiëntie verbeteren: besteed minder tijd aan routinetaken, verhoog de productiviteit en verlaag de kosten.

Innovatie mogelijk maken: help ideeën en voorstellen te genereren voor nieuwe producten en diensten.

Klantervaringen personaliseren: pas content en aanbevelingen aan om de loyaliteit en betrokkenheid te stimuleren.

1 Versterking van data governance voor AI-transformatie

Elke onderneming heeft zijn eigen beleid en processen voor datagebruik. De maturiteit en volledigheid van frameworks voor data governance varieert, maar er zijn er nog maar weinig die echt geoptimaliseerd zijn voor AI. Veel best practices voor data governance blijven hetzelfde, zoals het waarborgen van de nauwkeurigheid en de consistentie van data. Andere aspecten moeten echter worden bijgewerkt om alles uit de AI-investeringen te halen.

Laten we eens naar enkele belangrijke gebieden kijken:

Zichtbaarheid van data

Gedetailleerde kennis van de datastroom binnen AI-systemen maakt het mogelijk om ongeautoriseerd of oneigenlijk gebruik op te sporen en te beperken. Dit inzicht ondersteunt de security en compliance, zodat gevoelige data kunnen worden beschermd om de AI-waarde te maximaliseren.

Bij traditionele data governance gaat het er vooral om te weten waar data zich bevindt en de toegang te beheren. Naarmate AI echter meer geïntegreerd wordt in de bedrijfsvoering, moet de data governance gelijke tred houden met de veranderende beveiligingsbehoeften. Bij een zeer gevoelige productlancering

moet bijvoorbeeld ook door AI gegenereerde content worden beheerd, zodat alle door AI geproduceerde documenten, communicaties en inzichten met betrekking tot het project veilig zijn. Dit betekent dat er beveiligingsmaatregelen moeten worden geïmplementeerd, zodat alleen bevoegde teamleden toegang hebben tot AI en dit kunnen gebruiken om projectinformatie te analyseren of samen te vatten.

Bovendien kunnen organisaties de operationele kosten in verband met AI beter beheersen door het beheren van dataverwerking en opslagvolumes.

Datakwaliteit

De kwaliteit van data is extra belangrijk bij AI, omdat een slechte datakwaliteit rechtstreeks van invloed is op de resultaten van AI. Wanneer je AI-tools gebruikt voor query's op je bedrijfsdata, is het belangrijk dat die data actueel en betrouwbaar is. Ook moet je weten wat de herkomst en kwaliteit is van de data die je teams gebruikt om hun eigen AI-modellen en -apps te bouwen. Regelmatige data-audits, strenge validatieprocessen en proactief beheer helpen de data-integriteit te waarborgen. Door zich op deze gebieden te concentreren, kunnen organisaties betrouwbare AI-resultaten behalen die tot betere besluitvorming en innovatie leiden.

Gebruikersbeheer

Met AI kunnen gebruikers op geavanceerde manieren met data werken. Ze communiceren door middel van prompts in natuurlijke taal met AI-systemen zoals Microsoft 365 Copilot. Met de juiste machtigingen en beveiligingen kan AI een reactie genereren via toegang tot relevante datacontext, zoals bestanden, chats en e-mails, en via plug-ins met externe bronnen.

Het is van cruciaal belang om de data die in deze processen wordt gebruikt, te monitoren om ervoor te zorgen dat de AI juiste, gegronde antwoorden biedt. Het bieden van transparantie door middel van voetnoten of links naar originele bronnen helpt gebruikers de informatie te verifiëren. Het risico op misbruik van data wordt zo verkleind en naleving van de regelgeving wordt gewaarborgd.

Compliance en eDiscovery

De opkomst van AI brengt nieuwe uitdagingen met zich mee op het gebied van compliance en eDiscovery (de verwerking van data voor rechtszaken). Het gaat dan met name om het beheer van door AI gegenereerde data en de aanpassing aan veranderende wettelijke vereisten. Om deze uitdagingen aan te pakken, moeten de frameworks voor data governance worden bijgewerkt. Er moet beleid worden ontwikkeld voor content die door AI wordt gegenereerd, bijvoorbeeld om ervoor te zorgen dat door AI geproduceerde documenten of communicaties worden gevolgd, gecategoriseerd en veilig worden opgeslagen. Zo moet het beleid bijvoorbeeld worden bijgewerkt zodat door AI gegenereerde e-mails of rapporten correct worden getagd en gearhiveerd voor toekomstig gebruik.

Om eDiscovery-mogelijkheden te verbeteren moeten er AI-tools worden geïntegreerd die door AI gegenereerde content op verschillende platforms kunnen zoeken en identificeren. Tijdens een juridisch onderzoek moeten eDiscovery-tools bijvoorbeeld in staat zijn om specifieke, door AI gegenereerde documenten te vinden en op te halen, relevante communicatie samen te vatten en duidelijke controletrajecten te bieden om compliance te bewijzen. Door deze mogelijkheden bij te werken, kunnen organisaties data beter beheren tijdens juridische audits of onderzoeken, zodat alle relevante door AI gegenereerde informatie toegankelijk en verdedigbaar is voor de rechtbank.

Datasecurity

Voor de beveiliging van AI-gestuurde activiteiten moeten Zero Trust-principes op identiteitsniveau worden toegepast om het risico van ongeautoriseerde toegang tot een minimum te beperken. Regelmatige updates van endpoints, zowel apparaten als applicaties, verminderen zwakke plekken die kunnen worden misbruikt. Bewustzijn van de tools voor generatieve AI die binnen de organisatie worden gebruikt, maakt het mogelijk om niet-goedgekeurde of onveilige applicaties te blokkeren, waardoor beveiligingslekken kunnen worden voorkomen. Door de toegang tot AI-tools en -data te beperken tot alleen vertrouwd personeel, kunnen organisaties de data-integriteit verbeteren en hun AI-activiteiten beschermen tegen potentiële bedreigingen.



Wat is Zero Trust?

Zero Trust is een beveiligingsmodel waarin elke aanvraag wordt geverifieerd alsof die afkomstig is van een niet-vertrouwd netwerk. In plaats van ervan uit te gaan dat alles binnen de bedrijfsfirewall veilig is, wordt bij deze aanpak het principe van 'nooit vertrouwen, altijd verifiëren' gehanteerd.

Zero Trust-principes

Expliciet verifiëren: voer verificatie en autorisatie altijd uit op basis van alle beschikbare datapunten.

Toegang geven met zo min mogelijk bevoegdheden: beperk de toegang van gebruikers met behulp van Just-In-Time en Just-Enough Access (JIT/JEA), adaptief beleid op basis van risico en bescherming van persoonsgegevens.

Ga uit van een inbreuk: beperk de schade, beheer de toegang, zorg voor encryptie en gebruik data om bedreigingen te herkennen en de verdediging te versterken.

De rol van hoofddatabeheer in de AI-transformatie: oorsprong, kwaliteit en betrouwbaarheid

Nu organisaties AI als hulpmiddel gebruiken bij zakelijke beslissingen, moeten ze ervoor zorgen dat deze systemen correcte en betrouwbare resultaten opleveren. De data die ten grondslag ligt aan AI-reacties moet beschikbaar, consistent en goed gedocumenteerd zijn.

Hoofddatabeheer ondersteunt betrouwbare AI door governancebeleid te implementeren dat bijhoudt waar data vandaan komt, de kwaliteit ervan controleert en de betrouwbaarheid en nauwkeurigheid waarborgt. Deze praktijken vormen het fundament voor AI-systemen die betrouwbare inzichten leveren, op basis waarvan met vertrouwen geïnformeerde beslissingen kunnen worden genomen.

Dataherkomst: inzicht in de oorsprong en wijzigingen van informatie

Bij dataherkomst wordt de reis van data door een organisatie gevolgd. De oorsprong, transformaties en bestemmingen van de data worden gedocumenteerd. Voor bedrijven die werken op basis van AI, is inzicht in de herkomst van data om verschillende redenen essentieel:

- **Transparantie:** weten waar data vandaan komt en hoe deze verandert, helpt de nauwkeurigheid van door AI gegenereerde uitvoer te bevestigen en zorgt voor naleving van de regelgeving door duidelijk inzicht te bieden in de geschiedenis van de data.
- **Traceerbaarheid:** met dataherkomst kunnen organisaties fouten of inconsistenties herleiden tot de bron, wat het oplossen van problemen en de correctie van data vereenvoudigt.
- **Impactanalyse:** inzicht in hoe data wordt gebruikt door generatieve AI-tools helpt bij het beoordelen van de potentiële impact van wijzigingen in databronnen of verwerkingsmethoden op de nauwkeurigheid van de uitvoer en de bedrijfsresultaten.

Datakwaliteit: de kwaliteit bepaalt de waarde van AI-reacties

Datakwaliteit is rechtstreeks van invloed op de betrouwbaarheid van AI-uitvoer. Met data van hoge kwaliteit kunnen AI-modellen correcte en waardevolle reacties geven op invoer van gebruikers. Belangrijke aspecten van datakwaliteit zijn:

- **Nauwkeurigheid:** data moet de condities in de praktijk correct weergeven.
- **Volledigheid:** alle benodigde data moet aanwezig en verantwoord zijn.
- **Consistentie:** data moet consistent zijn in verschillende systemen en in de loop van de tijd.
- **Tijdigheid:** data moet up-to-date zijn en beschikbaar zijn wanneer dat nodig is.

Betrouwbaarheid van data: data moet betrouwbaar zijn

Betrouwbaarheid betekent dat de data consistent voldoet aan de kwaliteitsnormen en beschikbaar is wanneer dat nodig is. Voor bedrijven die werken op basis van AI, is betrouwbare data cruciaal om het vertrouwen te bevorderen in de AI-tools en de beslissingen waarvoor deze de informatie aanleveren.

Om de betrouwbaarheid van data te waarborgen, is het volgende nodig:

- **Dataredundantie:** implementeer back-upsystemen die verlies voorkomen en de beschikbaarheid verhogen.
- **Regelmatige back-ups:** voer vaak back-ups uit als bescherming tegen beschadiging of verlies van data.
- **Bewaking en waarschuwingen:** zet bewakingssystemen op om problemen met data in real time te detecteren en stakeholders meteen te waarschuwen.
- **Plannen voor noodherstel:** ontwikkel en test plannen om data te herstellen en de activiteiten snel te hervatten na een verstoring.

De relatie tussen governance, security en verantwoordelijke kunstmatige intelligentie

Data governance en security vormen samen de ruggengraat voor een verantwoordelijk gebruik van AI. Veilige data van hoge kwaliteit zorgt ervoor dat AI ethisch en effectief werkt. Belangrijke gebieden om rekening mee te houden zijn dataclassificatie, toegangsbeheer, encryptie, incidentrespons en naleving van regelgeving.

Dataclassificatie

Het classificeren van data is een essentieel onderdeel om te beheren hoe AI-tools omgaan met gevoelige informatie. Data en meetings worden doorgaans geclassificeerd als algemeen, vertrouwelijk of zeer vertrouwelijk. Een juiste classificatie zorgt ervoor dat AI alleen toegang krijgt tot relevante informatie, waardoor het risico op blootstelling van gevoelige data aan onbevoegde gebruikers wordt verkleind.

Verkeerde classificatie daarentegen kan ertoe leiden dat AI data verwerkt die moet worden beperkt, wat kan leiden tot beveiligingslekken of problemen met compliance. Effectieve data governance, via geautomatiseerde tools of beleid voor eindgebruikers, zorgt ervoor dat data correct wordt geclassificeerd. Daardoor wordt gevoelige informatie beschermd en kan AI beter betrouwbare uitvoer leveren die aan de regelgeving voldoet.

Toegangsbeheer

Met toegangsbeheercontroles wordt geregeld wie toegang heeft tot data die relevant is voor AI en welke applicaties of identiteiten bevoegd zijn om die data te gebruiken. Zwakke toegangscontroles kunnen leiden tot blootstelling van gevoelige informatie, waardoor het risico op inbreuk en misbruik wordt vergroot.

Data governance speelt een belangrijke rol bij het afdwingen van deze controles door de toegang tot data te beperken tot geautoriseerd personeel en specifieke applicaties, zodat gevoelige data correct wordt verwerkt. Op die manier wordt niet alleen de integriteit van de data beschermd, maar zorg je er ook voor dat AI-systemen werken met veilige, vertrouwde datasets, waardoor de betrouwbaarheid en compliance worden verbeterd.

Encryptie

Door encryptie te gebruiken om te voorkomen dat data wordt onderschept of gemanipuleerd, kun je ervoor zorgen dat generatieve AI-tools hun reacties op de juiste context baseren, zoals werkgerelateerde data, bestanden, chats en e-mails, zonder het risico op datalekken.

Data governance-beleid kan robuuste versleutelingspraktijken vereisen, zodat data gedurende de hele levenscyclus beschermd blijft. Deze aanpak zorgt ervoor dat AI-tools betrouwbare antwoorden kunnen leveren, terwijl je data veilig blijft en het vertrouwen behouden blijft.

Incidentafhandeling

Gevoelige organisatiedata kunnen op straat komen te liggen door incidenten waarbij generatieve AI-tools onbevoegde toegang verlenen tot bestanden, e-mails of andere bedrijfsdata die systemen gebruiken om reacties te genereren.

Een proactief incidentresponsplan is cruciaal in dergelijke gevallen. Zonder een dergelijk plan loopt de organisatie niet alleen het risico dat gevoelige data op straat komen te liggen, maar ook dat de AI-uitvoer gecompromitteerd is. Data governance houdt ook in dat je beschikt over gedetailleerde responsprotocollen om een inbreuk snel aan te pakken, de impact ervan tot een minimum te beperken en ervoor te zorgen dat AI-systemen betrouwbaar blijven.

Naleving van wet- en regelgeving

AI-applicaties moeten voldoen aan wet- en regelgeving op het gebied van bescherming van persoonsgegevens en privacy, zoals de AVG of CCPA. Non-compliance kan tot hoge boetes leiden en het vertrouwen aantasten. Het is ook cruciaal om te begrijpen waar AI-tools data verwerken, omdat veel gratis tools data wereldwijd of buiten de gebruikelijke opslaglocaties van je bedrijf kunnen verwerken. Data governance zorgt er niet alleen voor dat AI-applicaties binnen wettelijke kaders worden uitgevoerd, maar ook dat data binnen de juiste servicegrenzen blijft, conform de compliancienormen van je organisatie. Deze aanpak ondersteunt ethisch AI-gebruik en helpt het vertrouwen in AI-technologie te vergroten.



4

Het framework voor data governance bijwerken om AI-adoptie te ondersteunen

In het veranderende AI-landschap is het belangrijk om specifieke gebieden van je bestaande framework voor data governance te identificeren die mogelijk extra aandacht vereisen. In plaats van het hele framework te herzien, kun je je beperken tot die gebieden die waarschijnlijk het meest zullen veranderen. Je kunt je dan vooral richten op waar de waarde van AI het meest wordt vergroot en er tegelijkertijd voor zorgen dat je data beschermd en veilig blijft. Hier zijn enkele belangrijke zaken om rekening mee te houden:

Beleid en procedures aanpassen

Voor AI moet data op nieuwe manieren worden verzameld, verwerkt en gebruikt. Door het databeleid bij te werken kun je relevante behoeften aanpakken op het gebied van dataprivacy, naleving van wet- en regelgeving en ethisch gebruik. Je kunt bijvoorbeeld persoonsgegevens beschermen door te vereisen dat data in specifieke gevallen wordt geanonimiseerd. De gegevens kunnen dan in de hele AI-levenscyclus veiliger worden gebruikt.

Rollen en verantwoordelijkheden

Het is essentieel om AI-gereedheid op te nemen in alle rollen die betrokken zijn bij data governance. Medewerkers die bekend zijn met AI-datavereisten kunnen als stewards fungeren om de datakwaliteit en compliance te ondersteunen. Multifunctionele samenwerking tussen juridische, IT- en data science-teams kan helpen AI-specifieke uitdagingen effectiever aan te pakken.

Datanormen en -definities aanpassen

Standaardisering van data-indelingen, definities en meetwaarden voor datakwaliteit maakt de implementatie van beleid voor het gebruik van AI-tools binnen een organisatie eenvoudiger. Met duidelijke datanormen wordt het makkelijker om te beslissen welke datasets AI-tools kunnen gebruiken om zakelijke context te bieden en welke data gebruikers kunnen uploaden voor analyse. AI-applicaties gebruiken dan altijd de meest relevante en vertrouwde data, waardoor ze effectiever worden en naleving van het organisatiebeleid wordt ondersteund.

Continue verbetering

Data governance is een doorlopend proces, zeker met AI. Regelmatige audits en updates van je governancekader kunnen helpen bij de aanpassing aan nieuwe AI-ontwikkelingen en wijzigingen in de regelgeving. AI zelf kan worden gebruikt om governancepraktijken te controleren en te verbeteren, bijvoorbeeld om hiaten op te sporen en verbeteringen voor te stellen. Deze proactieve aanpak verbetert de compliance en efficiëntie naarmate AI-technologieën zich verder ontwikkelen.

Tools en technieken voor effectieve data governance

Afstemmen op bedrijfsdoelen:

zorg dat je data governance-strategie doelen van de organisatie ondersteunt om de besluitvorming en efficiëntie te verbeteren.

Routinematige taken automatiseren:

automatiseer terugkerende taken zoals dataclassificatie en toegangsbeheer om handmatige fouten te verminderen en de beveiliging te verbeteren.

Zorgen voor hoge

nauwkeurigheidsnormen: gebruik validatie- en opschoningstools om de integriteit van data na verloop van tijd te ondersteunen.

Gebruikers trainen: bied training aan op het gebied van tools en procedures voor data governance om wanbeheer te voorkomen en naleving van het beleid te waarborgen.

Regelmatig audits uitvoeren: evalueer datapraktijken regelmatig om ervoor te zorgen dat ze meegaan met de veranderingen in de regelgeving en de organisatie.

Conclusie

Effectieve data governance voor AI met Microsoft 365

Robuuste data governance is een voorwaarde voor een verantwoordelijk gebruik van AI. Een effectieve data governance zorgt voor beschikbaarheid, nauwkeurigheid en beveiliging van data, zodat AI betrouwbare inzichten kan leveren en innovatie kan bevorderen. Door datakwaliteit, compliance en security een hoge prioriteit te geven, krijg je meer mogelijkheden met AI, waardoor de besluitvorming verbetert en je een voorsprong behoudt op de concurrentie.

Microsoft 365: meer mogelijkheden voor AI

Microsoft 365 biedt eersteklas productiviteitsapps met ingebouwde tools voor classificatie, beheer en bescherming van data. Deze functies ondersteunen je framework voor data governance en maken een zorgeloze adoptie van AI mogelijk wanneer je er klaar voor bent. Microsoft 365 helpt je bij het volgende:

- **Datakwaliteit:** ondersteuning van nauwkeurigheid en betrouwbaarheid voor AI-uitvoer.
- **Compliance:** naleving van wettelijke vereisten, waardoor juridische risico's worden teruggedrongen.
- **Zero Trust Security:** bescherming van gevoelige informatie tegen onbevoegde toegang, inbreuken en cyberdreigingen.

Ontdek uitgebreide productiviteitstools met AI-opties en robuuste bescherming om je organisatie te helpen efficiënt en veilig te werken.



Verken Microsoft 365