yellow arrow

Data- en AI-governancebeleid

Klant: Template

Betreft: Data- en AI-governancebeleid

Datum: [dd-mm-jjjj]

Auteur: Remon Wieberdink

Versie: 1.0

Gids van de digitale vooruitgang

yellow arrow
Marconiweg 22c
8071 RA Nunspeet

Tel: 085 - 273 8313
hallo@yellowarrow.nl
https://yellowarrow.nl

IBAN: NL22 RABO 0158 4059 94
BTW: NL 8512.05.203.B01
KvK: 54167639

Inhoudsopgave

Inleiding

Dit document bevat ons data- en AI-governancebeleid. Het beschrijft hoe wij als organisatie omgaan met onze data en met de inzet van kunstmatige intelligentie (AI), en welke afspraken wij daarover hebben gemaakt.

Het beleid sluit aan op ons informatiebeveiligingsbeleid en gaat specifiek in op de onderwerpen die door de opkomst van AI extra aandacht vragen. Onderwerpen als algemene verantwoordelijkheden, training en bewustwording, en incidentafhandeling worden in ons informatiebeveiligingsbeleid behandeld en zijn hier niet herhaald.

Dit template is bedoeld als uitgangspunt en wordt aangepast aan de eigen situatie. Pas in elk geval de geel-gemarkeerde plekken aan en vul aan waar nodig.

Bij vragen over het document of als er hulp nodig is bij het toepassen binnen de organisatie helpen we je graag verder. Je kunt ons bereiken op hallo@yellowarrow.nl of via 085-273 83 13.

1. Doel en reikwijdte

Dit beleid beschrijft hoe wij als organisatie verantwoord omgaan met onze data en met de inzet van AI-toepassingen. Het is van toepassing op alle medewerkers, systemen, processen en leveranciers die data van onze organisatie verwerken of AI-toepassingen gebruiken in onze processen, ongeacht of die toepassingen door onszelf zijn ontwikkeld of via derden worden afgenomen (bijvoorbeeld als onderdeel van een SaaS-dienst).

Het doel is drieledig: onze data beschermen tegen ongewenst gebruik via AI, AI op een gecontroleerde manier inzetten en aantoonbaar voldoen aan relevante wet- en regelgeving.

2. Uitgangspunten voor het gebruik van data en AI

Bij de inzet van data en AI binnen onze organisatie hanteren wij de volgende uitgangspunten:

- Wij gebruiken AI om ons werk slimmer te maken; AI vervangt geen menselijke beslissingen die klanten of medewerkers raken;
- Belangrijke beslissingen worden niet uitsluitend door AI genomen, er is altijd een menselijke beoordelaar ("human in the loop");
- Wij gaan transparant om met de inzet van AI: voor betrokkenen is duidelijk wanneer zij met AI-output werken;
- Vertrouwelijke bedrijfsdata en persoonsgegevens worden alleen verwerkt in AI-toepassingen die daar expliciet voor zijn goedgekeurd;
- Wij gebruiken AI alleen voor doelen die passen bij onze bedrijfsvoering en bij onze waarden;
- De directie is eindverantwoordelijk voor data- en AI-governance en stelt hiervoor mandaat en middelen beschikbaar.

3. AI-register en toegestaan AI-gebruik

Wij houden een centraal overzicht bij van AI-toepassingen die binnen onze organisatie zijn toegestaan: het AI-register. Per toepassing leggen wij vast wat zij doet, welke data zij verwerkt, wie er eigenaar van is en op welke datum zij is goedgekeurd of laatst beoordeeld.

- Het gebruik van een nieuwe AI-toepassing met bedrijfsdata vereist voorafgaande goedkeuring;
- Het gebruik van publieke AI-tools (zoals gratis chatbots of consumenten-versies) met vertrouwelijke of persoonsgebonden data is niet toegestaan;
- AI-toepassing Microsoft Copilot welke in onze standaard Microsoft 365-werkomgeving is ingebouwd verwerkt alle data binnen onze eigen Microsoft omgeving en mag daarom wel bedrijfsdata bevatten;
- Het AI-register wordt minimaal jaarlijks opnieuw beoordeeld op volledigheid en actualiteit.

Het AI-register wordt bijgehouden op deze locatie: [...]

Tip

- Begin klein. Een eenvoudig AI-register in Excel of SharePoint met de kolommen tool, doel, eigenaar, risiconiveau, datum goedgekeurd en datum laatste evaluatie is genoeg om mee te starten.

- Inventariseer eerst wat er al wordt gebruikt voordat je nieuwe regels oplegt. Vaak zijn medewerkers al actief met AI-tools die de directie nog niet kent, dat geeft direct een realistisch beeld van waar het beleid op moet aansluiten.

4. Omgang met data in AI-toepassingen

Niet alle data mag in elke AI-toepassing terechtkomen. Wij hanteren drie dataniveaus en koppelen daar duidelijke regels aan:

- Openbaar – Dit is data dat openbaar gedeeld mag worden. Deze data mag in elke goedgekeurde AI-toepassing worden gebruikt;
- Intern – Dit zijn bedrijfsgegevens die niet publiekelijk beschikbaar zijn, maar niet voldoen aan de strengere eis van de vertrouwelijke data. Deze data is alleen toegestaan in AI-toepassingen waar een overeenkomst mee is en de data niet wordt gebuikt voor andere doeleinden zoals doorverkoop en/of het trainen van het AI-model;
- Vertrouwelijk – inclusief persoonsgegevens, klantdata, financiële data en intellectueel eigendom: alleen toegestaan in AI-toepassingen die hier expliciet voor zijn goedgekeurd, met passende contractuele afspraken (waaronder een verwerkersovereenkomst en uitsluiting van trainingsgebruik).

Persoonsgegevens worden uitsluitend verwerkt op basis van een rechtmatige grondslag onder de AVG. Prompts, AI-uitkomsten en eventuele tussenresultaten worden behandeld met dezelfde zorg als de onderliggende bedrijfsdata.

Tip

- Maak datacategorieën herkenbaar voor medewerkers. Een korte vuistregel zoals "alles wat je niet op LinkedIn zou plaatsen, gaat niet in een publieke AI-tool" werkt vaak beter dan een lange definitie.
- Controleer bij elke AI-leverancier of trainingsgebruik van eigen data uitstaat. Bij zakelijke abonnementen (zoals Microsoft 365 Copilot of ChatGPT Enterprise) is dat standaard, bij gratis of consumenten-versies vaak niet.

5. Risicobeoordeling van AI-toepassingen

Voor elke nieuwe of significant gewijzigde AI-toepassing en/of verwerking voorwaarde voeren wij een korte risicobeoordeling uit voordat zij in gebruik wordt genomen. In deze beoordeling kijken wij minimaal naar:

- Welke data de toepassing verwerkt en met welk doel;
- Welke beslissingen of acties op de uitkomsten worden gebaseerd, en hoeveel impact die hebben op personen of de bedrijfsvoering;
- Welke risico's er zijn op het gebied van privacy, beschikbaarheid, integriteit en uitlegbaarheid;
- Welke beheersmaatregelen nodig zijn om die risico's tot een aanvaardbaar niveau terug te brengen.

Toepassingen die meebeslissen over personen (bijvoorbeeld in HR, kredietwaardigheid of toegang) of over kritieke bedrijfsprocessen krijgen aanvullende waarborgen, waaronder een

gedocumenteerde validatie en een vaste menselijke controlestap. Acceptatie van rest-risico's gebeurt alleen met goedkeuring van de directie.

Tip

- Houd de beoordeling pragmatisch. Een halve A4 met de hierboven genoemde vragen is voor de meeste MKB-toepassingen voldoende. Diepere analyses zijn alleen nodig voor toepassingen met directe impact op klanten, medewerkers of compliance.
- Combineer de jaarlijkse herbeoordeling van het AI-register met de bestaande risicoanalyse uit het informatiebeveiligingsbeleid, dat scheelt aparte trajecten en zorgt voor één integraal overzicht.

6. Wet- en regelgeving

Wij voldoen aan de AVG en aan andere voor onze organisatie toepasselijke wet- en regelgeving op het gebied van privacy, data en AI. Voor AI-toepassingen volgen wij de uitgangspunten van de EU AI-verordening (AI Act): toepassingen die binnen de EU als verboden of hoog-risico worden aangemerkt, worden alleen ingezet wanneer wij aantoonbaar voldoen aan de bijbehorende eisen, of worden niet ingezet.

Dit onderwerp kan variëren per organisatie. Sectorspecifieke regelgeving (zoals NIS2, NEN 7510 in de zorg of DORA in de financiële sector) of klanteisen vanuit aanbestedingen kunnen aanvullende verplichtingen met zich meebrengen.