Het is tijd voor AI-beleid

Hoe snel de opkomst van Artificial Intelligence (AI) onze bedrijfsprocessen zal beïnvloeden is nog maar de vraag, maar dat AI niet alleen een hype zal zijn en op termijn blijvende impact gaat hebben op klantcontacten, backoffice processen, maar wellicht ook besluitvorming lijkt vrij zeker. Langzaam en zeker zien we dat AI onze organisaties binnenkomt bijvoorbeeld in de vorm van Microsoft's Copilot. De Europese AI-act is inmiddels ook van kracht en we moeten ons afvragen of wij (of onze ICT-uitbestedingspartners) 'high risk AI-systemen' gebruiken. Het wordt daarom 'tijd voor beleid'!

De belangrijke eerste vraag

De eerste vraag die wellicht op het bordje van een directie komt, zal vaak de vraag zijn: 'Mogen we gebruik gaan maken van Copilot, Chat of andere generative AI-tools?' Dat is op zichzelf een goede vraag, maar de scope is wellicht iets te beperkt. AI komt namelijk niet alleen voor in de vorm van deze bekende en krachtige tools. Het zit misschien ook al in de systemen die u gebruikt voor fraudedetectie en klantacceptatie. Misschien ook al heel diep technisch in de automatische patroonherkenning van uw firewalls. En vallen ingewikkelde (deterministische of stochastische) Excel-modellen wellicht ook onder de definitie van AI? En als u dan 's avonds thuiskomt en Netflix of Spotify aanzet of een reis boekt bij Booking.com: daar is AI weer. Misschien is het daarom beter om te beginnen met de vraag: 'Wat gebruiken we al en waarvoor zouden we AI willen inzetten?'

Artificial Intelligence is meer dan alleen generative AI

In november 2022 lanceerde OpenAI het publiek toegankelijke ChatGPT. De verbazing en bewondering over wat met dit tool allemaal mogelijk was, was enorm. Vooral omdat dit soort 'generatieve AI' zelf de creatieve processen die een mens uitvoert bijvoorbeeld bij het schrijven van tekst, kan nabootsen. Daarom hebben we soms de neiging om bij het gebruik van AI onze scope te beperken tot 'generative AI', maar het is veel meer dan dat. We noemden al Netflix en Spotify, maar denk ook aan de gezichtsherkenning op uw iPhone en de spraakassistenten. Als we naar de definitie van een AI-systeem kijken in de Europese AI-act dan lezen we (artikel 3, lid1).

Helaas, leuker kunnen we het niet maken en makkelijker ook niet. De belangrijkste boodschap die we willen meegeven is dat er wellicht al meer AI-systemen zijn te onderkennen dan waar u nu aan denkt.

Interne beheersing rondom het gebruik van AI

DORA vereist een 'raamwerk voor informatiebeveiliging' en daarvoor adviseren wij veelal om een aanpak te kiezen die in lijn is met de ISO27001 standaard. Dit is een standaard die 'goed te doen' is, al vraagt het wel het nodige aan vastleggingen en structuur. Een soortgelijke standaard is er inmiddels ook voor het beheer van AI-systemen, namelijk de ISO42001 standaard. Qua structuur en opbouw erg vergelijkbaar met de ISO27001. De eenvoudige aanpak is daarom om de interne beheersing rondom AI-systemen in eerste instantie te integreren in het bestaande raamwerk. Dan kom je ook vanzelf bij vragen rondom risicobeheersing: 'Hoe bewaken we de vertrouwelijkheid, integriteit en beschikbaarheid?' Specifiek voor AI-systemen komen hier ook strategische vragen bij zoals: 'Worden we niet te afhankelijk, kunnen we adequaat menselijk toezicht borgen?' Of omgekeerd: 'Wat als concurrenten hun backoffice-kosten enorm weten te verlagen en wij raken achterop?'.

Voorzichtig beginnen en geleidelijk leren

Als iemand in de organisatie enthousiast komt met de vraag: 'Mogen we Copilot gaan gebruiken?' En u concludeert dat er eerst beleid moet worden geformuleerd, en een strategie en een raamwerk van interne beheersing moet worden opgesteld, dan vermoed ik dat het enthousiasme om te innoveren snel wordt verstikt. Dat is ook niet wat we adviseren. Er is niets mis met 'voorzichtig beginnen, de mogelijkheden en de risico's beter leren kennen en aan de hand van de ervaringen een visie en strategie ontwikkelen'. Ook dat is beleid. Maar vergis u niet in de risico's. Als u bijvoorbeeld Copilot gaat gebruiken en dit pakket heeft toegang tot uw interne data (deze staan immers op de OneDrive, of in Sharepoint of Teams-mappen), bent u dan ook voorbereid op een medewerker die via Copilot gaat experimenteren (bijvoorbeeld: 'Geef me een overzicht van alle BSN-nummers en privéadressen van onze medewerkers?').

Definitie van een AI-systeem in de Europese AI-act (artikel 3, lid1):
'AI-systeem': een op een machine gebaseerd systeem dat is ontworpen om met verschillende niveaus van autonomie te werken en dat na het inzetten ervan aanpassingsvermogen kan vertonen, en dat, voor expliciete of impliciete doelstellingen, uit de ontvangen input afleidt hoe output te genereren zoals voorspellingen, inhoud, aanbevelingen of beslissingen die van invloed kunnen zijn op fysieke of virtuele omgevingen.

Wat zou je in het AI-beleid willen opnemen?

Binnen veel organisaties zien wij een toenemende behoefte aan richting en houvast bij de inzet van kunstmatige intelligentie. Hoewel organisaties doorgaans gebruikmaken van eigen formats voor beleidsdocumenten, komen er in een doordacht AI-beleid een aantal essentiële onderwerpen terug. In onze optiek zijn dat onder meer:

1. Doelstelling, definities en scope bepaling,
2. Governance, taken en verantwoordelijkheden,
3. Uitgangspunten, zoals principes en ethische richtlijnen,
4. AI-strategie ('wat willen we met AI'),
5. Het gebruik van AI binnen de organisatie ('wat mag wel, wat mag niet en wie keurt goed') om uiteindelijk toe te werken naar concrete afspraken en procedures.

In de praktijk zien we dat AI razendsnel zijn weg vindt in uiteenlopende applicaties en diensten. Tegelijkertijd is er sprake van een overvloed aan marketing en 'vage' beloften die nog lang niet waar gemaakt worden. In deze context is het van belang om te investeren in een zekere mate van AI-geletterdheid binnen de organisatie en dit ook onderdeel te maken van de AI-strategie. Zo kan uw team de werkelijke kansen van AI herkennen, maar ook kritischer omgaan met onrealistische verwachtingen of ongefundeerde beloften.

Welke procedures zijn nodig voor beheersing van AI?

Zonder heldere beleidskaders en procedures bestaat het risico op onbeheerste inzet van AI-toepassingen. Dit kan leiden tot inefficiënt gebruik van middelen, verspilling van tijd en budget, en in sommige gevallen zelfs tot problemen met regelgeving, zoals in het artikel van Ruben over AI-chatbots.

De paradox is dat ook succesvolle AI-initiatieven risico's met zich meebrengen wanneer ze buiten de beleidsstructuur om zijn ontwikkeld. Een toepassing die in eerste instantie goed functioneert, maar zonder duidelijke governance of risicobeheersing is opgezet, kan later lastig te corrigeren zijn of stop te zetten. Zeker wanneer gebruik is gemaakt van vertrouwelijke data of data met 'biases' in de trainingsfase, kan dit later tot aanzienlijke complicaties leiden.

Het bestuur moet verantwoordelijkheid kunnen dragen voor hetgeen binnen de organisatie wordt ontwikkeld en gedeeld en dus zullen goedkeuringsprocedures en wellicht ook 'tijdelijke waivers' onderdeel moeten zijn van het beleid.

Kortom: ruimte voor experimenteren is waardevol, maar dit moet altijd plaatsvinden binnen een gecontroleerde en veilige context. Dit vraagt om duidelijke procedures, heldere afspraken, en een structuur voor toezicht en handhaving. Niet alleen met het oog op wet- en regelgeving, maar vooral om te waarborgen dat investeringen in AI – zowel qua tijd als middelen – effectief en verantwoord worden ingezet.

Conclusie

Geen enkele organisatie kan om het gebruik van AI heen en mogelijk gebruikt u al meer dan u zich op dit moment realiseert. De Europese regelgeving verplicht u in elk geval om dit najaar AI-systemen met een hoog risico te registreren en te beheersen. Dus een eerste inventarisatie en analyse is wellicht wel verstandig. Sinds 2023 is de Autoriteit Persoonsgegevens toezichthouder op het gebruik van algoritmes en AI. Op de website is veel interessante informatie te vinden. Zelfs als u voorzichtig begint met algemene tools zoals Copilot of ChatGPT en als u dan ook nog heeft geborgd dat de gegevens niet worden gebruikt voor trainingsdoeleinden … dan nog loopt u een aantal operationele risico's. En om te voorkomen dat iedereen maar met van alles aan de slag gaat, is het ook gewoon verstandig om beleid op papier te zetten:
Het is tijd voor AI-beleid!

PS: Hoewel de verleiding wel aanwezig was om gebruik te maken van tools, al is het maar om de tekst, opbouw en spelling te controleren: dit artikel is nog volledig en uitsluitend met menselijke intelligentie tot stand gekomen!