Sigra

Verslag

Sigra

AI in bestaande software: ben je erop voorbereid?

AI komt steeds vaker via bestaande software naar binnen. Is uw leveranciers-management daarop voorbereid?

Veel organisaties in zorg en welzijn besteden aandacht aan generatieve AI, zoals chatbots of tekstassistenten. Tegelijkertijd gebeurt er iets dat minstens zo relevant is en minder opvalt: AI-functionaliteiten worden steeds vaker toegevoegd aan software die organisaties al jarenlang gebruiken. Denk aan HR-systemen die sollicitaties analyseren, planningssoftware die voorspellingen doet over personeelsinzet of applicaties die automatisch aanbevelingen genereren - vaak geïntroduceerd als een nieuwe module of een extra knop in bestaande software.

Tijdens een recent intercollegiaal overleg binnen het netwerk Privacy, Informatieveiligheid en Ethiek van Sigra stond daarom de vraag centraal: **hoe voorkom je dat AI ongemerkt wordt geïntroduceerd zonder dat duidelijk is welke verantwoordelijkheden daarbij horen?**

AI-functionaliteit is niet hetzelfde als een gewone software-update

Bij traditionele software-updates ligt de nadruk vaak op functionaliteit, beveiliging en continuïteit. Bij AI-functionaliteiten komen daar nieuwe vragen bij.

Welke rol vervult de leverancier precies? Is sprake van een AI-systeem in de zin van de AI Act? Hoe wordt het systeem getraind? Welke gegevens worden verwerkt? Welke risico's bestaan er op fouten, discriminatie of ongewenste uitkomsten? En welke documentatie hoort daarbij beschikbaar te zijn?

Juist omdat AI vaak wordt toegevoegd aan reeds bestaande applicaties, ontstaat het risico dat organisaties een nieuwe functionaliteit activeren zonder stil te staan bij deze vragen. Dat raakt niet alleen aan juridische compliance, maar ook aan de ethische verantwoordelijkheid die zorg- en welzijnsorganisaties dragen ten opzichte van cliënten, medewerkers en andere betrokkenen.

De AI Act legt verantwoordelijkheden niet alleen bij gebruikers

De discussie werd mede ingegeven door toepassingen op het gebied van werving en selectie. De AI Act noemt AI-systemen die worden ingezet voor het analyseren of filteren van sollicitaties en het beoordelen van kandidaten expliciet als hoog-risico toepassing (Bijlage III). Voor dergelijke systemen gelden vergaande verplichtingen: een conformiteitsbeoordeling, technische documentatie, een register, aantoonbaar menselijk toezicht en transparantie naar betrokkenen. Die verplichtingen gelden vóórdat een systeem in gebruik wordt genomen - niet pas daarna.

Tegelijkertijd zien we in de markt dat leveranciers en afnemers soms verschillend kijken naar de vraag wie precies welke verantwoordelijkheden draagt. Daarbij ontstaat regelmatig discussie over de rol van aanbieder, gebruiksverantwoordelijke (deployer) en eventuele andere partijen in de waardeketen.

Voor organisaties in zorg en welzijn is het niet altijd eenvoudig om te beoordelen of een leverancier zijn verplichtingen voldoende heeft ingevuld. Juist daarom is het belangrijk om hierover kritische vragen te stellen voordat nieuwe AI-functionaliteiten in gebruik worden genomen.

Een contract is niet hetzelfde als compliance

Een leverancier kan verantwoordelijkheden contractueel beschrijven of verdelen - maar daarmee staat de juridische rolverdeling nog niet vast. De AI Act kent eigen definities voor aanbieder en gebruiksverantwoordelijke (deployer), en die definities volgen de feiten, niet de contracttekst. Een bepaling in een SLA die stelt dat de afnemer 'aanbieder wordt' zodra hij een module activeert, heft de verplichtingen van de leverancier niet op als die leverancier functioneel als aanbieder kwalificeert.

Voor organisaties in zorg en welzijn betekent dit dat het verstandig is om zelfstandig te beoordelen:

- welke AI-functionaliteit wordt geleverd;
- welk doel die functionaliteit heeft;
- welke rol de leverancier vervult;
- welke rol de eigen organisatie vervult;
- welke documentatie beschikbaar moet zijn;
- welke risico's daarmee samenhangen.

Van privacymanagement naar AI-leveranciersmanagement

Veel organisaties in zorg en welzijn hebben inmiddels processen ingericht voor AVG-compliance en leveranciersmanagement. Denk aan verwerkersovereenkomsten, Dpia's en informatiebeveiligingsbeoordelingen. Vraagstukken rondom privacy, Informatieveiligheid en ethiek zijn voor veel leden van Sigra dan ook geen onbekend terrein.

De opkomst van AI vraagt echter om een uitbreiding van deze werkwijze. AI-leveranciersmanagement gaat niet alleen over privacy en Informatieveiligheid, maar voegt daar een extra dimensie aan toe: transparantie, menselijk toezicht, risico-classificatie, uitlegbaarheid en ethische governance

Binnen zorg en welzijn speelt dit extra sterk. Organisaties werken met kwetsbare doelgroepen, verwerken gevoelige gegevens en dragen een maatschappelijke verantwoordelijkheid die verder gaat dan louter juridische compliance. AI-systemen die beslissingen ondersteunen of beïnvloeden - ook in HR of planning - raken daarmee aan de kern van wat het betekent om een betrouwbare zorg- of welzijnsorganisatie te zijn.

Zes vragen die iedere organisatie aan leveranciers kan stellen

Een praktische uitkomst van de discussie is dat organisaties bij nieuwe AI-functionaliteiten in ieder geval de volgende vragen zouden kunnen stellen:

1. Is sprake van een AI-systeem in de zin van de AI Act?
2. Welke juridische rol ziet de leverancier voor zichzelf en waarom?
3. Heeft de leverancier een beoordeling uitgevoerd van de AI Act-classificatie van de toepassing?
4. Welke technische en organisatorische documentatie is beschikbaar?
5. Welke wijzigingen in functionaliteit of gebruik kunnen gevolgen hebben voor de verantwoordelijkheden van de organisatie?
6. Worden wijzigingen in de AI-functionaliteit tijdig en actief gecommuniceerd, en op welke manier?

Vaak levert het gesprek over deze vragen al veel waardevolle informatie op - en geeft het antwoord op de vraag of een leverancier zijn zaken op orde heeft.

Blijf kritisch, ook als AI via vertrouwde software wordt geleverd

De belangrijkste conclusie van het intercollegiaal overleg was misschien wel dat AI niet alleen binnenkomt via nieuwe leveranciers of experimentele toepassingen. Steeds vaker

wordt AI onderdeel van software die al jarenlang in gebruik is bij organisaties in zorg en welzijn.

Dat maakt goed leveranciersmanagement belangrijker dan ooit. Niet omdat iedere AI-functionaliteit direct problematisch zou zijn, maar omdat organisaties moeten begrijpen wat zij precies inzetten, welke risico's daarbij horen en welke verantwoordelijkheden - juridisch én ethisch - daarmee gepaard gaan.

Wie nu goede afspraken maakt en de juiste vragen stelt, legt ook de basis voor verantwoorde AI-governance in de toekomst.

AI-governance begint daarom niet bij de technologie, maar bij het stellen van de juiste vragen.