(Vertaling – Versie September 2024)

Gegevensbeschermingsautoriteit

Algemeen Secretariaat

Artificiële-intelligentiesystemen en de AVG
Een benadering vanuit gegevensbescherming

Samenvatting

Deze informatiebrochure schetst de complexe wisselwerking tussen de algemene verordening gegevensbescherming (AVG)[i] en de verordening artificiële intelligentie (*AI act*)[ii] in de context van de ontwikkeling van AI-systemen. Het document wijst op het belang om AI-systemen af te stemmen op de beginselen van gegevensbescherming en daarbij rekening te houden met de unieke uitdagingen die AI-technologieën met zich meebrengen.

Belangrijke punten zijn onder meer:

- afstemming tussen AVG en *AI act*: de brochure onderstreept het complementaire karakter van de AVG en de *AI act* bij het waarborgen van de rechtmatige, behoorlijke en transparante verwerking van persoonsgegevens in AI-systemen;
- definitie van een AI-systeem: het document geeft een duidelijke definitie van AI-systemen en biedt illustratieve voorbeelden om het concept te verduidelijken;
- beginselen inzake gegevensbescherming: de brochure zoomt in op de belangrijkste AVG-beginselen, zoals rechtmatigheid, behoorlijkheid, transparantie, doelbinding, minimale gegevensverwerking, juistheid, opslagbeperking en de rechten van de betrokkenen in de context van AI-systemen;
- verantwoordingsplicht: het belang van verantwoording wordt benadrukt, met specifieke vereisten vanuit de AVG als vanuit de *AI act*;
- beveiliging: het document vestigt de aandacht op de noodzaak van robuuste technische en organisatorische maatregelen om persoonsgegevens die door AI-systemen worden verwerkt, te beschermen;
- menselijk toezicht: er wordt gewezen op de cruciale rol van menselijk toezicht bij de ontwikkeling en het gebruik van AI-systemen, met name voor AI-systemen met een hoog risico.

Door inzicht te geven in het juridische kader en praktische richtlijnen te bieden, wil deze informatiebrochure juridische professionals, functionarissen voor gegevensbescherming, informatica-technische profielen, en verwerkingsverantwoordelijken en verwerkers, in staat stellen om de vereisten van de AVG en de *AI act* te begrijpen en na te leven bij het ontwikkelen en inzetten van AI-systemen.

Doel van deze informatiebrochure

Het Algemeen Secretariaat van de Gegevensbeschermingsautoriteit ziet toe op de maatschappelijke, economische en technologische ontwikkelingen die een impact hebben op de bescherming van persoonsgegevens[iii].

In de afgelopen jaren hebben AI-technologieën een exponentiële groei gekend, waardoor verschillende industrieën ingrijpend veranderd zijn, en de manier waarop gegevens worden verzameld, verwerkt en gebruikt aanzienlijk is gewijzigd. Deze snelle vooruitgang heeft echter complexe uitdagingen met zich meegebracht op het gebied van gegevensbescherming, transparantie en verantwoordingsplicht.

In deze context publiceert het Algemeen Secretariaat van de Gegevensbeschermingsautoriteit deze informatiebrochure om inzicht te geven in gegevensbescherming en de ontwikkeling en implementatie van AI-systemen.

Het begrijpen en naleven van de AVG-beginselen en -bepalingen is van cruciaal belang om ervoor te zorgen dat AI-systemen ethisch verantwoord en in overeenstemming met de wettelijke normen werken. Deze informatiebrochure is bedoeld om de AVG-vereisten die specifiek van toepassing zijn op AI-systemen te verduidelijken en om nuttige inzichten te bieden aan belanghebbenden die betrokken zijn bij de ontwikkeling, implementatie en (interne) regulering van AI-technologieën.

Naast de AVG zal ook de verordening artificiële intelligentie (*AI act*), die op 1 augustus 2024 in werking is getreden, een belangrijke rol spelen bij het reguleren van de ontwikkeling en het gebruik van AI-systemen. Deze informatiebrochure gaat ook in op de vereisten van de *AI act*.

Doelpubliek van deze informatiebrochure

Deze informatiebrochure is bedoeld voor een uiteenlopend publiek van juridische professionals, functionarissen voor gegevensbescherming en personen met een technologische achtergrond, zoals business analisten, architecten en ontwikkelaars. De brochure is ook bedoeld voor verwerkingsverantwoordelijken en verwerkers die betrokken zijn bij de ontwikkeling en invoering van AI-systemen. Gezien het raakvlak van juridische en technische overwegingen die inherent zijn aan de toepassing van de AVG op AI-systemen, streeft deze informatiebrochure ernaar de kloof tussen wettelijke verplichtingen en technische implementatie te overbruggen.

Juridische professionals en DPO's spelen een cruciale rol bij het toezicht op de naleving van AVG-verplichtingen door organisaties, inclusief de verplichtingen die relevant zijn voor AI-systemen. Door inzicht te bieden in de vereisten van de AVG die specifiek van toepassing zijn op AI, voorziet deze informatiebrochure juridische professionals en DPO's van nuttige kennis om zich een weg te banen door de complexiteit van AI-gerelateerde gegevensverwerkingsactiviteiten, risico's te beoordelen, en passende beveiligings-maatregelen te treffen.

Tegelijkertijd vormen profielen met een informatica-technische achtergrond, zoals businessanalisten, IT-architecten en ontwikkelaars, een onmisbare schakel in het ontwerp, de ontwikkeling en de inzet van AI-systemen. Deze informatiebrochure erkent hun cruciale rol en wil de AVG-vereisten nader toelichten op een manier die toegankelijk is voor deze belanghebbenden met een informatica-technische achtergrond. De tekst bevat concrete voorbeelden uit de praktijk om te illustreren hoe AVG-beginselen zich laten vertalen naar praktische overwegingen tijdens de levenscyclus van AI-projecten. Door bruikbare inzichten te bieden, stelt deze informatiebrochure informatica-technische professionals in staat om AI-systemen te ontwerpen die voldoen aan de AVG-normen, waarin de beginselen van gegevensbescherming door ontwerp zijn ingebouwd en die potentiële juridische en ethische risico's beperken.

Wat is een AI-systeem?

De term "AI-systeem" kan op verschillende manieren worden geïnterpreteerd.

Deze informatiebrochure zoomt niet in op de details en nuances die de verschillende definities van elkaar onderscheiden.
In plaats daarvan bekijken we eerst de definitie van een AI-systeem zoals beschreven in de *AI act*[iv]:

Voor de toepassing van deze verordening wordt verstaan onder:
1) '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;

Met andere woorden:
Een AI-systeem is een computersysteem dat specifiek is ontworpen om data te analyseren, patronen te identificeren en die kennis te gebruiken om weloverwogen beslissingen te nemen of voorspellingen te doen.
In sommige gevallen kunnen AI-systemen leren van data en zich na verloop van tijd aanpassen. Dankzij dit leervermogen kunnen ze hun prestaties verbeteren, complexe patronen identificeren in verschillende datasets en meer nauwkeurige of genuanceerde beslissingen nemen.

Voorbeelden van AI-systemen in het dagelijkse leven:

Spamfilters in e-mail: spamfilters analyseren inkomende e-mails en herkennen patronen die spamberichten onderscheiden van echte e-mails. Na verloop van tijd, als mensen e-mails markeren als spam of geen spam, kan het AI-systeem daarvan leren en de nauwkeurigheid van de filtering verbeteren. Dit is een voorbeeld van een AI-systeem dat voldoet aan de criteria voor een AI-systeem:

- machinegebaseerd systeem: het is een computerprogramma;
- analyseert data: het analyseert de inhoud van e-mails;
- identificeert patronen: het identificeert patronen in e-mails die duiden op spam;

- neemt beslissingen: het beslist om een e-mail al dan niet als spam te categoriseren.

Aanbevelingssystemen voor streamingdiensten: streamingdiensten voor films, series of muziek gebruiken AI-systemen om aanbevelingen voor gebruikers te genereren. Deze systemen analyseren het vroegere kijk- of luistergedrag van een gebruiker en de gewoonten van soortgelijke gebruikers om content aan te bevelen waarin de gebruiker geïnteresseerd zou kunnen zijn. Dit is nog een voorbeeld van een AI-systeem:

- machinegebaseerd systeem: het is een computerprogramma;
- analyseert data: het analyseert de kijk-/luistergeschiedenis van een gebruiker;
- identificeert patronen: het identificeert patronen in de voorkeuren van de gebruiker en die van soortgelijke gebruikers;
- doet aanbevelingen: beveelt content aan op basis van de geïdentificeerde patronen.

Virtuele assistenten: virtuele assistenten reageren op spraakopdrachten en voeren taken uit zoals het instellen van alarmen, het afspelen van muziek of het bedienen van smart home-apparaten. Deze systemen maken gebruik van spraakherkenning en natuurlijke taalverwerking om verzoeken van gebruikers te begrijpen en actie te ondernemen. Dit is opnieuw een voorbeeld van een AI-systeem:

- machinegebaseerd systeem: het is een computerprogramma;
- analyseert data: het analyseert de spraakopdrachten van gebruikers;
- identificeert patronen: het identificeert patronen in spraak om verzoeken van gebruikers te begrijpen.
- neemt beslissingen: het beslist hoe te reageren op basis van zijn kennis.
- kan aanpassingsvermogen vertonen: sommige virtuele assistenten kunnen gebruikersvoorkeuren onthouden en hun reacties na verloop van tijd aanpassen.

AI-gestuurde analyse van medische beeldvorming: veel ziekenhuizen en zorgverleners gebruiken AI-systemen om artsen te helpen bij het analyseren van medische beelden, zoals röntgenfoto's, CT-scans en MRI's. Deze systemen zijn getraind op enorme datasets van gelabelde medische beelden, waardoor ze patronen en mogelijke afwijkingen kunnen identificeren.

- machinegebaseerd systeem: het is een computerprogramma;
- analyseert data: het analyseert de digitale medische beelden;
- identificeert patronen: het identificeert patronen in de beelden die kunnen wijzen op de aanwezigheid van een ziekte of afwijking;

- ondersteunt de besluitvorming: het systeem markeert mogelijke probleemgebieden in de beelden, waardoor artsen beter onderbouwde diagnoses kunnen stellen.

Vereisten van de AVG & AI act

Rechtmatige, behoorlijke en transparante verwerking

De AVG vereist een rechtmatige, behoorlijke en transparante verwerking van persoonsgegevens

AVG-rechtmatigheid van verwerkingen: de AVG stelt in artikel 6 zes rechtsgronden vast voor het verwerken van persoonsgegevens (toestemming, overeenkomst, wettelijke verplichting, vitale belangen, algemeen belang en gerechtvaardigd belang). Deze zelfde rechtsgronden blijven van toepassing op AI-systemen die persoonsgegevens verwerken onder de *AI act*.

Verboden AI-systemen: de *AI act* introduceert extra verbodsbepalingen bovenop de AVG voor bepaalde AI-systemen, nl. deze met een hoog risico. Terwijl de AVG zich richt op de bescherming van persoonsgegevens door middel van verschillende principes, verbiedt de AI act rechtstreeks specifieke vormen van AI-toepassingen met een hoog risico. Hier volgen enkele voorbeelden:

- Sociale score-systemen: deze systemen kennen een score toe aan individuen op basis van verschillende aspecten, wat mogelijk leidt tot discriminatie en beperking van hun kansen.
- AI-systemen voor gezichtsherkenning in realtime op openbare plaatsen (met beperkte uitzonderingen): deze systemen geven aanleiding tot vragen over bescherming van de privacy, bewegingsvrijheid en mogelijk misbruik voor grootschalige surveillance.

Behoorlijkheid:

- Hoewel de *AI act* geen specifieke sectie met de titel "behoorlijkheid" heeft, bouwt hij verder op het beginsel van behoorlijke verwerking van de AVG (art. 5.1.a) aangezien de *AI act* gericht is op het beperken van vooroordelen en discriminatie bij de ontwikkeling, de inzet en het gebruik van AI-systemen.

Transparantie:

- De *AI act* vereist een basisniveau van transparantie voor alle AI-systemen. Dit betekent dat gebruikers geïnformeerd moeten worden dat ze interageren met een AI-systeem. Een chatbot zou een interactie bijvoorbeeld kunnen beginnen met een bericht "Hallo, ik ben Nelson, **een chatbot**. Hoe kan ik u vandaag van dienst zijn?"
- De *AI act* vereist een hoger transparantieniveau voor AI-systemen met een hoog risico. Dit omvat het verstrekken van duidelijke en toegankelijke informatie over

hoe gegevens in deze systemen worden gebruikt, vooral met betrekking tot het besluitvormingsproces. Gebruikers moeten kunnen begrijpen welke factoren van invloed zijn op AI-beslissingen en hoe mogelijke vooringenomenheid wordt beperkt.

Doelbinding en minimale gegevensverwerking

De GDPR vereist doelbinding (art. 5.1.b) en minimale gegevensverwerking (art. 5.1.c). Dit betekent dat persoonsgegevens voor specifieke en gerechtvaardigde doeleinden moeten worden verzameld en beperkt moeten blijven tot wat noodzakelijk is voor die doeleinden. Deze beginselen zorgen ervoor dat AI-systemen gegevens niet gebruiken voor doeleinden waarvoor ze niet bedoeld zijn of dat ze niet buitensporig veel gegevens verzamelen.
De *AI act* versterkt het beginsel van doelbinding - uit de AVG - voor AI-systemen met een hoog risico door de noodzaak van een goed gedefinieerd en gedocumenteerd beoogd doel te benadrukken.

Voorbeeld: een AI-systeem voor het toekennen van leningen door een financiële instelling gebruikt naast standaard identificatiegegevens en kredietbureau-informatie ook geolocatiegegevens (bijv. in het verleden bezochte locaties) en social media-gegevens van een betrokkene (bijv. profielen van vrienden en hun interesses). Deze uitgebreide gegevensverzameling, met inbegrip van geolocatie en social media-gegevens, doet twijfels rijzen over de compliance van het systeem met de AVG.

Juistheid en actualiteit van de gegevens

De GDPR vereist dat persoonsgegevens correct zijn en, zo nodig, worden bijgewerkt (art. 5.1.d). Organisaties moeten redelijke stappen ondernemen om dit te waarborgen. De AI act bouwt verder op dit principe door te eisen dat AI-systemen met een hoog risico kwalitatieve en niet-vertekende gegevens gebruiken om discriminerende resultaten te voorkomen.

Voorbeeld: een financiële instelling ontwikkelt een AI-systeem om het goedkeuren van leningen te automatiseren. Het systeem analyseert verschillende datapunten van aanvragers van leningen, waaronder kredietgeschiedenis, inkomen en demografische gegevens (postcode). De trainingsgegevens van het AI-systeem weerspiegelen echter onbewust historische vooroordelen: de gegevens stammen uit een periode waarin leningen gemakkelijker werden verstrekt in rijkere buurten (met een hoger gemiddeld inkomen). Het AI-systeem houdt deze vooroordelen in stand omdat aanvragers van

leningen uit buurten met lagere inkomens systematisch leningen geweigerd worden, zelfs als ze daarvoor financieel in aanmerking komen. Dit resulteert in een discriminerende uitkomst en kan ernstige twijfel oproepen of het systeem wel voldoet aan de AI-wet.

Opslagbeperking

De AVG vereist dat persoonsgegevens niet langer worden bewaard dan nodig is om de doeleinden te bereiken waarvoor ze werden verzameld (art. 5.1.e). De *AI act* introduceert niet uitdrukkelijk een andere of extra vereiste met betrekking tot opslagbeperking voor AI-systemen.

Geautomatiseerde besluitvorming

De AVG en de *AI act* wijzen beide op het belang van menselijke betrokkenheid bij geautomatiseerde besluitvormingsprocessen die gevolgen hebben voor natuurlijke personen. Ze verschillen echter in focus:

- De AVG verleent natuurlijke personen het recht om niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking gebaseerd besluit waaraan voor hen rechtsgevolgen zijn verbonden (art. 22). Dit betekent dat betrokkenen het recht hebben om een heroverweging van een geautomatiseerd besluit door een menselijke besluitvormer te vragen. Het is een individueel recht om besluiten aan te vechten die als oneerlijk of onjuist worden ervaren.
- De *AI act* legt een grotere nadruk op menselijke betrokkenheid door zinvol menselijk toezicht verplicht te stellen tijdens de ontwikkeling, de inzet en het gebruik van AI-systemen met een hoog risico. Dit vormt een governancemaatregel om de ontwikkeling en het gebruik van verantwoorde AI te waarborgen. Menselijk toezicht onder de *AI act* omvat een breder scala aan activiteiten dan alleen de heroverweging van individuele besluiten. Het omvat bijvoorbeeld het controleren van de trainingsgegevens en algoritmen van het AI-systeem op mogelijke vooroordelen, het monitoren van de prestaties van het systeem en het ingrijpen in cruciale beslissingsmomenten van het AI-systeem

In essentie geeft de AVG natuurlijke personen de mogelijkheid om bezwaar te maken tegen uitsluitend geautomatiseerde besluiten, terwijl de *AI act* proactief menselijk toezicht vereist voor AI-systemen met een hoog risico om potentiële *bias* of vooroordelen te

voorkomen en een verantwoorde ontwikkeling en een verantwoord gebruik van dergelijke systemen te waarborgen.

Voorbeeld: een overheidsinstantie gebruikt een AI-systeem om te bepalen of iemand in aanmerking komt voor sociale uitkeringen op basis van inkomen, arbeidsstatus en gezinssituatie.
Volgens de AVG hebben personen het recht om niet te worden onderworpen aan uitsluitend geautomatiseerde verwerking om in aanmerking te komen voor sociale uitkeringen (art. 22). Dit betekent dat ze een heroverweging van het geautomatiseerde besluit door een menselijke besluitvormer kunnen vragen.
Volgens de *AI act* wordt dit AI-systeem geclassificeerd als een systeem met een hoog risico (aangezien het een aanzienlijke impact heeft op de bestaansmiddelen van personen). Dit vereist dat de overheidsinstantie menselijk toezicht inregelt tijdens de ontwikkeling, de inzet en het gebruik van het AI-systeem.

Beveiliging van de verwerking

Zowel de AVG als de *AI act* benadrukken het belang van de beveiliging van persoonsgegevens gedurende de levenscyclus van de verwerking. AI-systemen brengen echter specifieke risico's met zich mee waarvoor extra beveiligingsmaatregelen nodig zijn die verder gaan dan de traditionele praktijken voor gegevensbescherming.

De AVG verplicht organisaties om technische en organisatorische maatregelen (TOM's) te treffen die passen bij het risico dat gepaard gaat met hun gegevensverwerkingsactiviteiten. Hiervoor worden risicobeoordelingen uitgevoerd om potentiële bedreigingen en kwetsbaarheden te identificeren. De geselecteerde TOM's moeten deze risico's beperken en zorgen voor een basisbeveiligingsniveau voor persoonsgegevens.

De *AI act* bouwt verder op deze basis door robuuste beveiligingsmaatregelen voor AI-systemen met een hoog risico verplicht te stellen. AI-systemen introduceren namelijk specifieke risico's die verder gaan dan de traditionele gegevensverwerking, zoals:

- mogelijke vertekening van trainingsgegevens: vertekende trainingsgegevens kunnen leiden tot vooringenomen beslissingen door het AI-systeem, wat een oneerlijk effect heeft op individuen.;

- manipulatie door onbevoegde personen: een hacker zou bijvoorbeeld de trainingsgegevens van het AI-systeem kunnen manipuleren om de besluiten ervan op een nadelige manier te beïnvloeden. Stel je voor dat een systeem dat getraind is om kredietaanvragen goed te keuren, misleid wordt om geschikte aanvragers af te wijzen op basis van niet-relevante factoren.

Om deze unieke risico's aan te pakken, legt de *AI act* de nadruk op proactieve maatregelen zoals:

- mogelijke problemen identificeren en hierop anticiperen: dit omvat brainstormen over wat er mis zou kunnen gaan met het AI-systeem en hoe waarschijnlijk het is dat dit gebeurt (risicobeoordeling). Dit is een kernpraktijk in zowel de AVG als de *AI act*.
- voortdurend monitoren en testen: dit houdt in dat de prestaties van het AI-systeem regelmatig worden geëvalueerd op verschillende aspecten, waaronder:
    - veiligheidslekken: identificeren van zwakke plekken (in de code of in het ontwerp van het systeem) die door aanvallers kunnen worden misbruikt;
    - vertekening: controleren op mogelijke vertekening in de trainingsgegevens of besluitvormingsprocessen van het systeem.
- menselijk toezicht: de *AI act* benadrukt het belang van zinvol menselijk toezicht tijdens de ontwikkeling, de inzet en het gebruik van AI-systemen met een hoog risico. Dit zorgt ervoor dat mensen betrokken zijn bij belangrijke beslissingen inzake het AI-systeem en de kwetsbaarheden van het systeem begrijpen. Menselijk toezicht onder de *AI act* gaat verder dan alleen beveiligingsprocessen en omvat verschillende aspecten, zoals:
    - toetsen van trainingsgegevens en algoritmen op potentiële vertekeningen;
    - monitoren van de prestaties van het systeem op eerlijkheid, nauwkeurigheid en potentiële onbedoelde gevolgen;
    - tussenkomen op cruciale beslissingsmomenten, vooral wanneer deze aanzienlijke gevolgen kunnen hebben voor natuurlijke personen.

Voorbeeld: AI-gestuurd longkankerdiagnosesysteem.

Een AI-systeem dat door een ziekenhuis wordt gebruikt om longkanker te diagnosticeren is een voorbeeld van een AI-systeem met een hoog risico vanwege verschillende factoren:

- zeer gevoelige gegevens: het verwerkt zeer gevoelige persoonsgegevens, waaronder gezondheidsinformatie over patiënten (longen) en diagnoses (gegevens van bijzondere categorieën in artikel 9 van de AVG) ;

- gevolgen van gegevenslekken: een gegevenslek kan kritieke gezondheidsinformatie over patiënten blootleggen, wat kan leiden tot privacyschendingen en reputatieschade voor het ziekenhuis;
- levensbepalende beslissingen: de output van het systeem heeft een directe invloed op het leven van de patiënten. Een diagnose op basis van onjuiste of gecompromitteerde gegevens kan ernstige gevolgen hebben voor hun gezondheid en welzijn.

Zowel de AVG als de *AI act* benadrukken het belang van beveiligingsmaatregelen voor gegevensverwerkingsactiviteiten, vooral als het gaat om gevoelige gegevens.

- De AVG legt een basis voor gegevensbeveiliging: het verplicht organisaties om passende technische en organisatorische maatregelen (TOM's) te implementeren om persoonsgegevens te beschermen op basis van een risicobeoordeling. Voor gezondheidsgegevens moeten deze maatregelen bijzonder sterk zijn vanwege de gevoelige aard ervan. Voorbeelden in het kader van de AVG kunnen zijn:
  - encryptie van gegevens: versleutelen van patiëntgegevens in rust en in transit garandeert de vertrouwelijkheid ervan, zelfs als er een datalek plaatsvindt;
  - toegangscontrole: strikte toegangscontrole beperkt wie patiëntgegevens kan inzien en wijzigen;
  - penetratietesten: door regelmatig penetratietesten uit te voeren, kunnen zwakke plekken in de beveiliging van het systeem worden geïdentificeerd en aangepakt;
  - logging en auditing: het bijhouden van gedetailleerde logs van systeemactiviteiten maakt het mogelijk om eventueel verdacht gedrag te monitoren en te onderzoeken.
- De *AI act* bouwt verder op deze basis voor AI-systemen met een hoog risico: de *AI act* erkent de specifieke risico's van AI en schrijft robuuste beveiligingsmaatregelen voor. Deze kunnen aanvullende maatregelen omvatten die zijn afgestemd op de specifieke kwetsbaarheden van het AI-systeem, zoals gegevensvalidatie en kwaliteitsborging: de *AI act* benadrukt het belang van het waarborgen van de kwaliteit en integriteit van de gegevens die worden gebruikt om het AI-systeem te trainen en te bedienen. Dit kunnen technieken zijn voor:
  - de herkomst van gegevens: de herkomst van gegevens traceren om mogelijke bronnen van vertekening of manipulatie in de trainingsgegevens te identificeren, zoals onjuiste labeling van röntgenfoto's;
  - anomaliedetectie: het identificeren en signaleren van ongebruikelijke patronen in de trainingsgegevens die kunnen duiden op kwaadwillige

manipulatie, zoals een plotse toevloed van röntgenfoto's met onrealistische kenmerken;

- menselijke beoordeling van datapunten met een hoog risico: zorgverleners cruciale röntgenfoto's laten beoordelen voordat ze worden gebruikt om het AI-systeem te trainen, met name röntgenfoto's die ongebruikelijke kenmerken vertonen of die de resultaten voor de patiënt aanzienlijk kunnen beïnvloeden.

Door deze beveiligingsmaatregelen uit te voeren kan het ziekenhuis de risico's van het AI-gestuurde longkankerdiagnosesysteem beperken en de privacy van de patiënt, de gegevensbeveiliging en ten slotte de best mogelijke resultaten voor de patiënt garanderen.

Rechten van de betrokkene

De AVG kent natuurlijke personen rechten toe, zodat ze controle hebben over hun persoonsgegevens en hoe deze worden gebruikt. Deze rechten omvatten inzage (bekijken welke gegevens worden verwerkt, art. 15), rectificatie (onjuiste gegevens corrigeren en gegevens aanvullen, art. 16), wissing (verzoeken om gegevens te verwijderen, art. 17), beperking van de verwerking (beperken hoe gegevens worden gebruikt, art. 18) en gegevensoverdraagbaarheid (gegevens doorgeven aan een andere dienst, art. 20).
Om deze rechten doeltreffend te kunnen uitoefenen, moeten natuurlijke personen begrijpen hoe hun gegevens worden gebruikt. De *AI act* versterkt dit door het belang te benadrukken van een duidelijke uitleg over hoe de gegevens worden gebruikt in AI-systemen. Met deze transparantie kunnen natuurlijke personen geïnformeerd beslissingen nemen over hun gegevens, en effectiever gebruik maken van hun rechten als betrokkene.

Voorbeeld: een AI-systeem dat wordt gebruikt om premies voor autoverzekeringen te bepalen, kent een bepaalde klant (betrokkene) een relatief hoge premie toe. De *AI act* geeft deze klant recht op een duidelijke uitleg over hoe zijn premie wordt berekend. De verzekeraar (verwerkingsverantwoordelijke) zou bijvoorbeeld kunnen uitleggen dat er verschillende datapunten zijn gebruikt, zoals het aantal kilometers dat de klant jaarlijks rijdt, ongevallen in het verleden, en of de auto voor werkdoeleinden wordt gebruikt. Met deze informatie kan de klant op zijn beurt zijn AVG-rechten uitoefenen, zoals het recht op rectificatie (correctie van onjuiste persoonsgegevens of aanvulling van persoonsgegevens).

Verantwoordingsplicht

De AVG vereist (dat verwerkingsverantwoordelijken) verantwoording (afleggen) voor de verwerking van persoonsgegevens aan de hand van verschillende maatregelen zoals:

- Transparante verwerking; natuurlijke personen moeten begrijpen hoe hun gegevens worden verzameld, gebruikt, opgeslagen en gedeeld (bijv. door een duidelijke en beknopte gegevensbeschermingsverklaring, door rechten van betrokkenen, ...). Dankzij deze transparantie kunnen ze zien of er rechtmatig en behoorlijk met hun gegevens wordt omgegaan;
- Beleid en procedures voor het omgaan met persoonsgegevens: gedocumenteerd beleid zorgt voor consistente praktijken voor het omgaan met gegevens binnen de organisatie;
- Gedocumenteerde rechtsgrond voor de verwerking: voor elke gegevensverwerkende activiteit hebben organisaties aantoonbaar bewijs nodig van de rechtsgrond (toestemming, contract, gerechtvaardigd belang, etc.);
- Het bijhouden van verschillende registers (zoals het verwerkingsregister, verzoeken van betrokkenen, datalekken) is vereist: het bijhouden van een nauwkeurige administratie toont aan dat organisaties bereid zijn om verantwoording af te leggen en stelt hen in staat om tijdens audits of inspecties aan te tonen dat ze aan de regels voldoen;
- Beveiligingsmaatregelen: het implementeren en correct handhaven van passende technische en organisatorische maatregelen (TOM's) om persoonsgegevens te beschermen is cruciaal om verantwoording te kunnen afleggen;
- Een gegevensbeschermingeffectbeoordeling (*DPIA - Data Protection Impact Assessment*) is in sommige gevallen vereist: deze is verplicht bij het verwerken van gegevens met een hoog risico of het implementeren van nieuwe technologieën;
- In sommige gevallen is een functionaris voor gegevensbescherming (*DPO - Data Protection Officer*) vereist: overheidsorganisaties bijvoorbeeld, ongeacht hun kernactiviteiten, moeten een DPO hebben.

Hoewel de *AI act* geen specifieke sectie heeft over het afleggen van verantwoording, bouwt hij verder op de beginselen van de AVG. De *AI act* verplicht organisaties tot:

- een twee-stappen-benadering van risicobeheer voor AI-systemen. Een eerste classificatieproces categoriseert het risico van de AI voor natuurlijke personen (van minimaal tot hoog).

Voor systemen met een hoog risico is een meer grondige risicobeoordeling vereist. Deze gaat dieper in op de specifieke risico's en identificeert potentiële gevaren van het AI-systeem en wordt ook wel een FRIA (Fundamental Rights Impact Assessment - effectbeoordeling op het gebied van de fundamentele rechten) genoemd;

- duidelijke documentatie over het ontwerp en de implementatie van AI-systemen;
- processen voor menselijk toezicht op AI-systemen met een hoog risico. Dit kan menselijke tussenkomst of goedkeuring inhouden voor cruciale beslissingen die door het AI-systeem worden genomen;
- een formeel meldingsproces voor incidenten met betrekking tot AI-systeemstoringen of onbedoeld gedrag van het AI-systeem.

Compliance rechttoe rechtaan: user stories voor AI-systemen en de AVG- en AI act *requirements*

Het omzetten van regelgevende vereisten in technische specificaties voor AI-systemen brengt aanzienlijke uitdagingen met zich mee. Dit document wil aan de hand van user stories de kloof tussen wettelijke verplichtingen en systeemontwikkeling overbruggen.

User stories bieden een praktische benadering voor het begrijpen en aanpakken van regelgevende vereisten in de context van het ontwerp van AI-systemen. Door een gebruikersgericht perspectief te hanteren, kunnen organisaties wettelijke verplichtingen effectief omzetten in praktische stappen.

Ter illustratie van de toepassing van user stories op het gebied van AI wordt in dit document een systeem voor de berekening van autoverzekeringspremies als voorbeeld gebruikt.

Vereisten van rechtmatige, behoorlijke en transparante verwerking

User story: rechtmatigheid garanderen - juiste rechtsgrond
Als autoverzekeringsmaatschappij die een AI-systeem implementeert voor het berekenen van autopremies, moeten we een grondige beoordeling van de rechtsgrond uitvoeren om de meest geschikte juridische rechtvaardiging te bepalen voor het verzamelen en gebruiken van klantgegevens in ons AI-systeem. Dit is belangrijk om te voldoen aan het algemene AVG-beginsel van rechtmatigheid.

User story: rechtmatigheid garanderen - verboden gegevens
Als autoverzekeringsmaatschappij die een AI-systeem implementeert voor het berekenen van autopremies, moeten we ervoor zorgen dat ons systeem voldoet zowel aan de AVG- als aan de AI act-verbodsbepalingen voor het verwerken van bepaalde typen van persoonsgegevens. Hieronder vallen speciale categorieën van persoonsgegevens zoals ras of etnische afkomst, politieke opvattingen, religieuze overtuigingen, enz. Dit is belangrijk om te voldoen aan de bescherming van gevoelige persoonsgegevens in de AVG en de nadruk die de AI act legt op het voorkomen van discriminerende effecten.

User story: behoorlijkheid garanderen

Als autoverzekeringsmaatschappij die een AI-systeem implementeert voor het berekenen van autopremies, moeten we zorgen voor een behoorlijke en niet-discriminerende verwerking van klantgegevens. Dit is belangrijk om te voldoen aan het AVG-beginsel van behoorlijkheid enerzijds en om anderzijds tegemoet te komen aan de specifieke nadruk die de AI act legt op het voorkomen van vertekende uitkomsten die bepaalde groepen zouden kunnen benadelen.

De autoverzekeringsmaatschappij kan behoorlijkheid bereiken door middel van:

- review van de gegevensbronnen: de gegevensbronnen analyseren die worden gebruikt om het AI-systeem te trainen om mogelijke vertekening op basis van factoren zoals postcode, gender, leeftijd ... te identificeren en te beperken. Ervoor zorgen dat deze factoren worden gebruikt op een manier die relevant en noodzakelijk is voor premieberekeningen, zodat discriminerende uitkomsten worden vermeden;
- fairness testing: het AI-systeem regelmatig testen op potentiële vertekeningen in zijn output. Dit kan bijvoorbeeld door de autopremieberekeningen voor vergelijkbare klantprofielen te vergelijken om onverklaarbare verschillen op te sporen;
- menselijk toezicht: een menselijk beoordelingsproces implementeren voor beslissingen met grote gevolgen die door het AI-systeem worden genomen, zoals aanzienlijke verhogingen van autopremies of zelfs weigeringen van polissen.

User story: transparantie garanderen

Als autoverzekeringsmaatschappij die een AI-systeem implementeert voor het berekenen van autopremies, moeten we transparant zijn over hoe de gegevens van onze klanten worden gebruikt. Dit is belangrijk om te voldoen aan het algemene AVG-beginsel van transparantie en om tegemoet te komen aan de specifieke nadruk die de AI act legt op transparantie voor AI-systemen met een hoog risico.

De autoverzekeringsmaatschappij kan transparantie bereiken door middel van:

- een gegevensbeschermingsverklaring: leg in de gegevensbeschermingsverklaring van de verzekeringsmaatschappij duidelijk uit hoe klantgegevens worden verzameld, gebruikt en opgeslagen in het AI-systeem voor premieberekeningen.
- begrijpelijke uitleg: geef klantvriendelijke uitleg over het AI-premieberekeningsproces. Dit kan inhouden dat er eenvoudige taal, afbeeldingen of veelgestelde vragen worden gebruikt om de rol van de AI bij het bepalen van de premies voor autoverzekeringen te verduidelijken.

- recht op toegang tot informatie: implementeer mechanismen waarmee klanten eenvoudig toegang kunnen krijgen tot informatie over de datapunten die worden gebruikt in hun specifieke premieberekeningen.

Vereisten van doelbinding en minimale gegevensverwerking

User story: doelbinding garanderen

Als autoverzekeringsmaatschappij die een AI-systeem implementeert voor het berekenen van autopremies, moeten we ervoor zorgen dat de gegevens die we van onze klanten verzamelen beperkt blijven tot wat strikt noodzakelijk is voor de nauwkeurige berekening van de premies. Dit is belangrijk om te voldoen aan het beginsel van doelbinding onder de AVG.

User story: minimale gegevensverwerking garanderen

Als autoverzekeringsmaatschappij die een AI-systeem implementeert voor het berekenen van autopremies, moeten we een strategie van gegevensminimalisering hanteren om ervoor te zorgen dat we alleen de minimale hoeveelheid klantgegevens verzamelen en gebruiken die nodig is voor de nauwkeurige berekening van premies. Dit is belangrijk om te voldoen aan het beginsel van minimale gegevensverwerking onder de AVG.

Vereisten van juistheid en actualiteit van gegevens

User story: juistheid en actualiteit van gegevens garanderen

Als autoverzekeringsmaatschappij die een AI-systeem implementeert voor het berekenen van autopremies, moeten we processen ontwikkelen om de juistheid en up-to-dateheid van klantgegevens te garanderen die in het systeem worden gebruikt. Dit is belangrijk om te voldoen aan het beginsel van juistheid van gegevens onder de AVG.

De autoverzekeraar kan de juistheid en het up-to-date zijn van klantgegevens bereiken door:

- mechanismen voor gegevensverificatie: klanten gebruiksvriendelijke mechanismen aanbieden om hun persoonlijke gegevens in het autoverzekeringssysteem te verifiëren en bij te werken. Dit kan via een online portal, mobiele app of speciale telefoonlijn.
- regelmatige gegevensverversing: stel procedures op voor het regelmatig verversen van klantgegevens die in het AI-systeem worden gebruikt. Dit kan

inhouden dat klanten wordt gevraagd om hun informatie periodiek bij te werken of dat de gegevens worden geïntegreerd met externe gegevensbronnen (bijv. databanken met rijgegevens) om relevante datapunten automatisch bij te werken.

- waarschuwingen voor gegevenskwaliteit: implementeer waarschuwingen voor ontbrekende of mogelijk onnauwkeurige datapunten in klantprofielen. Hierdoor kan de verzekeringsmaatschappij proactief contact opnemen met klanten en om updates vragen.
- duidelijk communiceren aan klanten over hun recht op rectificatie onder de AVG. Dit recht geeft hen de mogelijkheid om correcties aan te vragen van onjuiste persoonsgegevens of om ontbrekende gegevens aan te vullen die worden gebruikt in het premieberekeningssysteem.

User story: gebruik van niet-vertekende gegevens garanderen

Als autoverzekeringsmaatschappij die een AI-systeem implementeert voor het berekenen van autopremies, moeten we ervoor zorgen dat de gegevens die worden gebruikt om het systeem te trainen en te laten functioneren geen vertekeningen vertonen. Dit is belangrijk om te voldoen aan de specifieke nadruk die de AI act legt op het voorkomen van vooringenomen uitkomsten die bepaalde groepen zouden kunnen benadelen.

De autoverzekeringsmaatschappij kan niet-vertekende gegevens verkrijgen voor eerlijke AI-premieberekeningen door middel van:

- evaluatie van gegevensbronnen: analyseer de gegevensbronnen die worden gebruikt om het AI-systeem te trainen. Identificeer in het proces van gegevensverzameling mogelijke vertekeningen of afwijkingen op basis van factoren zoals bijvoorbeeld sociaaleconomische afkomst.;
- regelmatige controles en bias-tests: controleer de prestaties van het AI-systeem voortdurend op mogelijke vertekeningen of afwijkingen in de output. Voer regelmatig bias-tests uit om discriminerende resultaten in premieberekeningen te identificeren en aan te pakken.;
- menselijk toezicht: implementeer een menselijk beoordelingsproces voor beslissingen met grote gevolgen die door het AI-systeem worden genomen, zoals aanzienlijke verhogingen van autopremies of zelfs polisweigeringen. Zo kunnen, door menselijke tussenkomst, vooringenomen beslissingen voorkomen worden.;
- transparantie tegenover klanten: informeer klanten via de gegevensbeschermingsverklaring over het streven van het bedrijf om niet-vertekende gegevens en gegevens van hoge kwaliteit te gebruiken in het AI-systeem..

Vereiste inzake beveiligde verwerking

User story: User story: passende beveiligingsmaatregelen implementeren voor AI in autoverzekeringen

Als autoverzekeringsmaatschappij die een AI-systeem implementeert voor het berekenen van autopremies, moeten we een grondige risicobeoordeling uitvoeren om potentiële bedreigingen en kwetsbaarheden te identificeren die van invloed kunnen zijn op onze klantgegevens. Bij deze beoordeling zal rekening worden gehouden met verschillende factoren, waaronder het type van gegevens (financiële gegevens van klanten versus basisinformatie over klanten), de verwerkingsactiviteiten en de mogelijke impact van een gegevenslek. Op basis van deze beoordeling implementeren we passende technische en organisatorische maatregelen (TOM's) om deze risico's te mitigeren en de bescherming van onze klantgegevens te garanderen. Dit is belangrijk om te voldoen aan de vereiste van beveiliging van de verwerking onder de AVG.

Voorbeelden van TOM's zijn onder meer:

- gegevensversleuteling: versleuteling van klantgegevens in rust en in transit om de vertrouwelijkheid ervan te beschermen ;
- toegangscontrole: het implementeren van strikte toegangscontrole om te beperken wie toegang heeft tot klantgegevens en wie deze kan wijzigen;
- regelmatige penetratietesten: uitvoeren van penetratietesten om zwakke plekken in de beveiliging van het systeem te identificeren en aan te pakken;
- logging en auditing: het bijhouden van gedetailleerde logs van systeemactiviteiten om eventueel verdacht gedrag te kunnen monitoren en onderzoeken.

User story: specifieke beveiligingsmaatregelen implementeren voor AI bij autoverzekeringen

Als autoverzekeringsmaatschappij die een AI-systeem implementeert voor het berekenen van autopremies, erkennen we dat AI-systemen specifieke risico's met zich meebrengen die verder gaan dan traditionele gegevensverwerking. Deze risico's kunnen onder meer bestaan uit potentiële vertekeningen of afwijkingen in de trainingsgegevens of manipulatie door onbevoegde partijen. Om deze specifieke risico's aan te pakken, zullen we aanvullende maatregelen implementeren in combinatie met de AVG-conforme TOM's. Dit is belangrijk om te voldoen aan de vereiste van beveiliging van de verwerking onder de AI act.

Voorbeelden van deze aanvullende maatregelen zijn onder meer:

- gegevensvalidatie en kwaliteitsborging: implementeren van processen om de kwaliteit en integriteit te waarborgen van de gegevens die worden gebruikt om het AI-systeem te trainen en te bedienen. Dit kan het natrekken van de herkomst van gegevens inhouden alsook het opsporen van afwijkingen in de output om mogelijke vertekeningen of pogingen tot manipulatie te identificeren.
- menselijk toezicht: opzetten van een raamwerk voor menselijk toezicht gedurende de levenscyclus van het AI-systeem. Dit kan inhouden dat datapunten met een hoog risico door de mens worden beoordeeld, dat de prestaties van het systeem door de mens worden gecontroleerd op eerlijkheid en nauwkeurigheid, en dat door de mens wordt tussengekomen op cruciale beslissingsmomenten.

Vereiste inzake (het kunnen aantonen van de) verantwoordingsplicht

User story: de rechtsgrond documenteren

Als autoverzekeringsmaatschappij die een AI-systeem implementeert voor het berekenen van autopremies, moeten we de rechtsgrond voor het verzamelen en gebruiken van klantgegevens in het AI-systeem duidelijk en beknopt vastleggen. Dit is belangrijk om te voldoen aan het AVG-beginsel inzake (het aantonen van) verantwoordingsplicht (ook in de context van audits of inspecties).

User story: een effectbeoordeling op het gebied van fundamentele rechten iuitvoeren (Fundamental Rights Impact Assessment, FRIA)

Als autoverzekeringsmaatschappij die een AI-systeem implementeert voor het berekenen van autopremies, moeten we een grondige FRIA (Fundamental Rights Impact Assessment) ontwikkelen en up-to-date houden om mogelijke risico's van dit AI-systeem proactief te identificeren en te mitigeren. Dit is belangrijk om te voldoen aan de vereisten van de AI act voor AI-systemen met een hoog risico en om eerlijke en niet-discriminerende premieberekeningen voor onze klanten te garanderen.

* * *

Referenties

[0] Voor de originele Engelse versie van dit document is gebruik gemaakt van spellingscontrole, grammaticacontrole en een groot taalmodel (Large Language Model) als hulpmiddel voor het corrigeren en verfijnen van de oorspronkelijke tekstgedeelten.

[i] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming), Publicatieblad van de Europese Unie L 119/1, 4.5.2016, p. 1–88.

[ii] Verordening (EU) 2024/1689 van het Europees Parlement en de Raad van 13 juni 2024 tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie (wet op de artificiële intelligentie), Publicatieblad van de Europese Unie L 199/1, 12.7.2024, p. 1–120.

[iii] Art. 20, § 1, 1°, van de wet tot oprichting van de Gegevensbeschermingsautoriteit van 3 december 2017, gewijzigd bij de wet van 25 december 2023.

[iv] Wet op de artificiële intelligentie, artikel 3 (1).