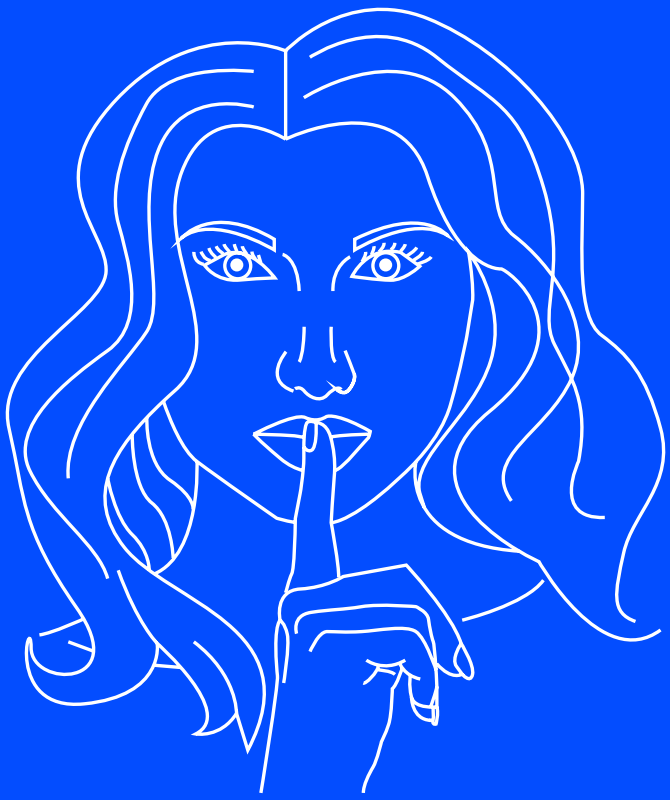
SSST ... NIET AAN DE GBA VERTELLEN.

Hoe je rekening houdt met gegevensbescherming door ontwerp- en standaardinstellingen van je AI-toepassing.



Kenniscentrum Data & Maatschappij

Deze brochure, een afgeleide van het rapport 'Artificiële intelligentie en gegevensbescherming: een verkennende gids', is een uitgave van het Kenniscentrum Data & Maatschappij.

Onderzoeksgroep CiTiP (KU Leuven) verzorgde inhoudelijk deze brochure. Onderzoeksgroep imec-SMIT, Vrije Universiteit Brussel focuste op de tekstredactie, de vormgeving en vertaalde de inhoud op maat van de lezer.

Kenniscentrum
Data & Maatschappij

Wanneer je een AI-toepassing ontwikkelt, ben je verplicht de persoonsgegevens te beschermen die worden verzameld. De **Algemene Verordening Gegevensbescherming** (AVG - beter bekend als GDPR) bevat regels voor de **verwerking van persoonsgegevens** voor particuliere bedrijven en overheidsinstanties. De AVG is opgebouwd rond **zeven principes** waarmee je moet rekening houden bij de verwerking van persoonsgegevens. Maar hoe pas je deze principes toe in de praktijk?

Deze brochure geeft per principe aan hoe je hiermee kan rekening houden door het **ontwerp of als standaardinstelling van jouw AI-toepassing**. Zo vind je per principe het volgende terug:

- een **korte uitleg** van het principe;
- een **fictieve bekentenis** van een bedrijf dat het principe niet toepaste zoals het hoort en op de vingers werd getikt door klanten of de Gegevensbeschermingsautoriteit (GBA). Deze autoriteit ziet toe op de correcte naleving van de bescherming van persoonsgegevens in België;
- een **aantal maatregelen** die de overtreder had kunnen nemen door middel van het ontwerp (O) of als standaardinstelling (S) van de AI-toepassing.

Aan de hand van deze bekentenissen geven we praktische tips mee over hoe je de AVG wel kan **toepassen in de praktijk** én dit door middel van het ontwerp en/of als standaardinstelling van jouw AI-toepassing.

Wil je graag **meer informatie** over gegevensbescherming door ontwerp en standaardinstellingen? Dan verwijzen we je graag naar het rapport 'Artificiële intelligentie en gegevensbescherming: een verkennende gids' (hoofdstuk 4.1).

VERWERK RECHTVAARDIG, WEES GOEDAARDIG

Elke verwerking van persoonsgegevens moet op een toepasselijke rechtsgrond gebaseerd zijn en de betrokkene moet op correcte wijze over de verwerking worden geïnformeerd (AVG-principe: rechtmatigheid, behoorlijkheid, transparantie).

Een fictieve bekentenis

Bij WainingAllDai ontwikkelen we een **app** die op basis van AI een **passende wijn bij elke stemming of gelegenheid** voorstelt. Om onze suggesties zo nauwkeurig mogelijk te maken, krijgt de app bij installatie **toegang tot de microfoon** van de smartphone. Zo kan onze app op basis van de microfoongegevens de omstandigheden analyseren en begrijpen in wat voor situatie de gebruiker zich bevindt. Omdat we niet zeker wisten of dit wel toegestaan is, vermeldden we dat **niet in** onze **privacyverklaring**. Niet lang na de lancering kregen we een brief van een advocaat: zijn cliënt had ontdekt dat onze app toegang had tot de microfoon. Ze zouden **klacht** neerleggen bij de GBA voor deze ongeoorloofde verwerking en opslag van persoonsgegevens. Die liet er geen gras over groeien en beboette ons stevig. Eind goed, al goed: onze app heeft geen toegang meer tot de microfoon en de resultaten zijn even goed. Prachtig toch?

Welke maatregelen had de overtreder moeten nemen?

- De app-ontwikkelaar moet in de ontwerpfase nadenken of het verzamelen van omgevingsgeluiden (inclusief persoonsgegevens) **noodzakelijk** is **voor de functionaliteit** van de app. Zo ja, kan de ontwikkelaar zich beroepen op de noodzakelijkheid voor de uitvoering van de gebruiksovereenkomst met de gebruiker. Zo nee (zoals in dit scenario), moet er afzonderlijk toestemming gevraagd worden indien de functionaliteit toch wordt aangeboden.
- In beide gevallen moet de betrokkene op afdoende wijze worden geïnformeerd over de beoogde verwerking. Dit kan door bij het eerste gebruik van de app de gebruiker een interactief en stapsgewijs **overzicht** te geven van de **belangrijkste verwerkingen**, zeker indien er toegang wordt verleend tot de microfoon.

GEGEVENS NIET RECYCLEREN, MAAR PRIVACY RESPECTEREN

Persoonsgegevens mogen slechts worden verzameld en verwerkt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Een bijkomende verwerking mag enkel plaatsvinden indien die verwerking gebeurt voor een doeleinde dat verenigbaar is met de initiële doeleinden (AVG-principe: doelbinding).

Een fictieve bekentenis

Wij gebruiken in onze productielijn **robots** die de **arbeiders helpen** bij de assemblage van onze producten. Deze robots zijn uitgerust met een **camera en bewegingssensoren**. Op voorstel van onze HR-directeur Mr. O'Brien zijn we die gegevens ook beginnen gebruiken bij de **evaluatie van onze medewerkers**, zonder hen dat te zeggen. Blijkt dat de arbeiders nauwelijks bewogen en voortdurend stilstonden! We concludeerden dat er niets anders opzat dan hen in verschillende golven te **ontslaan**. Toen de **vakbond** meer vernam over onze methodes, klaagden ze ons aan bij de GBA. En die autoriteit gaf hen gelijk. Later bleek ook nog eens dat de medewerkers wel degelijk nodig waren in het productieproces. We konden niet anders dan opnieuw onervaren mensen aanwerven omdat de robots het niet alleen kunnen.

Welke maatregelen had de overtreder moeten nemen?

› Voor over te gaan tot de **bijkomende verwerking** van de persoonsgegevens had het bedrijf zich moeten afvragen of het **nieuwe doel** (evaluatie van medewerkers) wel **verenigbaar** is **met het eerste doel** (productie). Dit kan gebeuren door gepaste **interne richtlijnen en procedures** op te stellen die bepalen welke gegevens worden verwerkt en wie toegang tot deze gegevens heeft. Alle medewerkers moeten van deze richtlijnen op de hoogte worden gebracht, ook bv. HR-medewerkers. Ook kan je doelbinding in dit geval bevorderen door de toegang tot de gegevens die de robot verzamelt, technisch te reserveren voor degenen die hier echt toegang toe moeten hebben. Persoonsgegevens moet je dus automatisch afschermen, zodat bv. in dit geval de HR-medewerker er geen gebruik van kan maken.

HOU JE GEGEVENS MINIMAAL, DAT IS GENIAAL

Organisaties mogen slechts de persoonsgegevens verzamelen en verwerken die noodzakelijk zijn voor het doel dat ze beogen (AVG-principe: minimale gegevensverwerking).

Een fictieve bekentenis

Ons bedrijf Kwebbel en Kwabbel is gespecialiseerd in de ontwikkeling van **chatbots voor online verkoopplatformen**. We vonden het belangrijk dat gebruikers altijd een versie van onze chatbot te zien krijgen die op vlak van **gender** bij hen aansluit. Daarom is de eerste vraag op elke site 'Identificeert u zich als man, vrouw of LGBTQ?'. Vervolgens verandert onze chatbot van kleur: blauw voor mannen, roze voor vrouwen en regenboogkleuren voor LGBTQ-gebruikers. Bovendien kunnen we zo ook **genderspecifieke productaanbevelingen** doen. Maar dat wordt niet door iedereen goed onthaald… onze inbox zit vol met klachtenbrieven van klanten die vinden dat we genderneutraal moeten zijn of die vinden dat wij helemaal geen zaken hebben met hun genderidentiteit.

O Welke maatregelen had de overtreder moeten nemen?

› Bij het ontwerpen van chatbots moet dit bedrijf zich afvragen of genderinformatie echt **nodig** is voor wat ze willen bereiken (**gepersonaliseerde productaanbevelingen**). Daarbij mag niet vergeten worden dat seksuele geaardheid een 'gevoelig' gegeven is dat slechts in **beperkte omstandigheden** verwerkt mag worden. De verwerking daarvan moet dus noodzakelijk zijn om gebruikers te verplichten deze informatie te geven. In dit geval lijkt dat niet zo te zijn, aangezien productaanbevelingen ook op basis van andere criteria dan gender of seksuele geaardheid gepersonaliseerd kunnen worden.

S Welke maatregelen had de overtreder moeten nemen?

› Mocht het bedrijf deze functionaliteit toch willen aanbieden aan gebruikers, moet het de vraagstelling aanpassen. De **eerste twee vragen** moeten dan zijn: 'Wenst u een genderspecifieke versie van de chatbot op deze site te gebruiken?' en 'Wenst u genderspecifieke productaanbevelingen te ontvangen?'. Als er geen of een negatief antwoord is op één van beide vragen, moet een **genderneutrale chatbot en/of productaanbevelingen** aangeboden worden. Alleen bij een positief antwoord kan de chatbot vragen naar het gender van de gebruiker. Ook kan de chatbot meegeven dat de bezoeker andere productaanbevelingen krijgt als die deze informatie deelt. Om ook de seksuele geaardheid in aanmerking te nemen, is een afzonderlijke, uitdrukkelijke toestemming van de gebruiker nodig.

VOOR EEN TOPRESULTAAT, HOU JE GEGEVENS ACCURAAT

De verwerkte persoonsgegevens moeten altijd juist en accuraat zijn. Indien nodig, moeten gebruikers de gegevens kunnen corrigeren, bijwerken of verwijderen (AVG-principe: juistheid).

Een fictieve bekentenis

Wij ontwikkelen AI-software die gebruikt kan worden voor **rekruteringsdoeleinden**. Deze software analyseert het **CV** dat de gebruiker invoerde, en stelt dan wekelijks of maandelijks de **meest gepaste vacatures** voor. Maar een gebruiker kan geen wijzigingen aanbrengen eenmaal zijn CV is ingevoerd. Dat zou onze software ontregelen en resulteren in weinig relevante aanbevelingen. Als de gebruiker toch wijzigingen wil aanbrengen, moet die een nieuw profiel aanmaken. Voor trainingsdoeleinden bewaren we trouwens al de eerder ingevoerde CV's voor onbepaalde duur. Ondertussen krijgen we meer en meer klachten van, voornamelijk, professionele gebruikers omdat ze te veel profielen moeten aanmaken en het overzicht niet meer kunnen bewaren.

Welke maatregelen had de overtreder moeten nemen?

› Het bedrijf moet in het ontwerp van de AI-toepassing mogelijk maken dat een gebruiker **wijzigingen of correcties** aanbrengt **in het initiële CV**.

Bovendien moet het verouderde CV's verwijderen en kan het die niet voor onbepaalde duur bewaren.

VERMIJD EEN AANVARING DOOR CORRECTE BEWARING

Persoonsgegevens mogen maar worden bewaard zolang dat noodzakelijk is voor de doeleinden van de verwerking - met uitzondering van een aantal situaties (AVG-principe: opslagbeperking).

Een fictieve bekentenis

Mijn bedrijf hAIppyMeal levert **slimme schermen** aan fastfoodrestaurants die op basis van het **gezicht van klanten** een **menu voorstellen**. Uit onderzoek blijkt namelijk dat vrouwen vaker kip- of veggiegerechten eten en mannen vaker rundvleesgerechten. Bovendien stelt de software ook een menu op maat voor als het jou denkt te herkennen van een eerder bezoek. Zo wordt het bestellingsproces nog verkort! Een paar maanden na de installatie van onze eerste schermen in een restaurant kregen we plots allerlei **klachten** van klanten die het niet vonden kunnen dat hun foto werd bewaard en verscheen bij klanten met dezelfde gelaatskenmerken. Waarom geven mensen in dit geval wel om hun privacy, maar niet als ze foto's van zichzelf delen met onbekenden op sociale media?

S Welke maatregelen had de overtreder moeten nemen?

› Het bedrijf kan best **automatische bewaringstermijnen** voor de verschillende types persoonsgegevens (gezicht, menukeuze,...) in zijn software inbouwen. Zodra de termijn is overschreden, moet het bedrijf de gerelateerde gegevens verwijderen. Zo kan in dit geval het ingescande gezicht best onmiddellijk na de bestelling worden verwijderd, én zeker niet worden getoond aan derden. Los van het principe van opslagbeperking, kunnen hier uiteraard ook vragen worden gesteld omtrent de **proportionaliteit en de rechtvaardigheid van de verwerking**. Zo is het duidelijk dat het bedrijf verschillende toestemmingen had moeten vragen voor de beoogde verwerkingen van de gezichtsgegevens van klanten.

LAAT JE NIET HACKEN, VOORKOM GEGEVENSLEKKEN

Organisaties moeten technische en organisatorische maatregelen nemen om verwerkte persoonsgegevens te beveiligen tegen externe en interne risico's - zoals ongeoorloofde verwerking, onopzettelijke vernietiging... (AVG-principe: integriteit en vertrouwelijkheid).

Een fictieve bekentenis

Met mijn bedrijf FAIce kregen we onlangs de opportuniteit om **gezichtsherkenningscamera's** te plaatsen aan de **in- en uitgang** van restaurant Bon AppetAIt. Op die manier kon het restaurant nagaan hoeveel klanten er in realtime dineren én wanneer het **keukenpersoneel** het best een **pauze** neemt en wanneer zeker niet. Maar een van de obers heeft alle gegevens, inclusief beelden van de gezichten van de klanten, **geëxporteerd en gepubliceerd op het internet** omdat Bon AppetAIt zijn arbeidscontract niet wou verlengen. Mensen konden zien wie er allemaal in het restaurant dineerde en wat zij aten. Ik had nochtans tegen de eigenaar van het restaurant gezegd dat die het standaardwachtwoord (123456) voor de database moest veranderen!

O/S Welke maatregelen had de overtreder moeten nemen?

› In dit geval had FAIce ervoor kunnen zorgen dat de **database beter beschermd** was dan met een gemakkelijk te achterhalen wachtwoord. Verder had het er ook voor kunnen zorgen dat gegevens in **versleutelde**/**geanonimiseerde vorm** worden opgeslagen. Het restaurant had op zijn beurt maatregelen kunnen nemen zoals: de toegang tot persoonsgegevens **registreren**, enkel medewerkers toegang tot de database geven voor wie dit nodig is voor de functie, en dat met **geïndividualiseerde accounts en rolbepaling**. Dit staat los van de vraag of het gebruik van camerabeelden voor deze doeleinden wel **proportioneel en gerechtvaardigd** is.

DOCUMENTEER JE DADEN, HET ZAL JE NIET SCHADEN

Organisaties die persoonsgegevens verwerken moeten de maatregelen die zij nemen om de AVG na te leven kunnen aantonen en moeten daarom hun gerelateerde acties en documenteren (AVG-principe: verantwoordingsplicht).

Een fictieve bekentenis

Bij DeliverAI gebruiken we **autonome drones** om **pakketjes** af te leveren. Onze drones gebruiken **camera's** en filmen zo bijvoorbeeld ook de daken van huizen. Een van onze businessmanagers kwam een jaar geleden met het idee om gegevens over onze klanten die een huis zonder zonnepanelen bewonen, te delen met leveranciers van **zonnepanelen**. Zo kunnen zij hen persoonlijk contacteren met een aanbod. Een koppel dat zo een aanbod voor zonnepanelen kreeg, vroeg de installateur waarom zij ongevraagd dat aanbod ontvingen. Die verwees hen door naar ons. Nu hebben we een **klacht bij de GBA** aan onze broek!

Welke maatregelen had de overtreder moeten nemen?

› Voor het bedrijf overging tot de verdere verwerking van de persoonsgegevens (de doorgifte aan de zonnepanelenleverancier) had DeliverAI best een **gegevens-beschermingseffectbeoordeling** (GEB) uitgevoerd. Als er een **functionaris** voor gegevensbescherming (of data protection officer - DPO) is aangesteld, zou het bedrijf deze ook moeten consulteren. In ieder geval moet het bedrijf potentiële klanten over deze verzameling én doorgifte van gegevens **informeren**. Dit zijn verplichtingen waar medewerkers goed van op de hoogte moeten zijn. Het is aangeraden om in het proces van het bedenken en uitwerken van nieuwe bedrijfsactiviteiten altijd een stap in te bouwen waarbij wordt nagedacht over de **mogelijke juridische verplichtingen**, en dit **proces** te **documenteren**. (NB: Een cruciaal aspect in de GEB zou de vraag over doelbinding zijn, waarbij het bedrijf zich moet afvragen of het deze gegevens wel verder mag verwerken voor doeleinden anders dan de bezorging van pakketjes. Bovendien moet het ook terdege bewust zijn van andere mogelijk toepasselijke wettelijke vereisten.)

Disclaimer

Het Kenniscentrum Data en Maatschappij wenst bij te dragen aan het debat en het creëren van een maatschappelijk draagvlak voor AI en data-gedreven toepassingen. Onze juridische informatie is algemeen en kan niet beschouwd worden als individueel juridisch advies. Ze kan niet worden gebruikt ter vervanging van advies door een juridisch expert. Hoewel we ernaar streven om onze documenten correct en accuraat op te stellen, is het mogelijk dat de daarin vervatte positie niet toepasbaar is op uw specifieke situatie, niet volledig, juist of actueel is, of niet overeenkomt met de positie die een rechtbank of toezichthoudende autoriteit zou kunnen innemen. Het Kenniscentrum draagt dan ook geen enkele verantwoordelijkheid voor de naleving van de toepasselijke wettelijke voorschriften door jouw organisatie.

Kenniscentrum
Data & Maatschappij

“GIJ ZULT DE ALGEMENE VERORDENING GEGEVENSBESCHERMING TOEPASSEN DOOR ONTWERP- EN STANDAARDINSTELLINGEN.”

Kenniscentrum -
Data & Maatschappij