(Nederlandse versie – April 2026)

Gegevensbeschermingsautoriteit

De impact van artificiële intelligentie op privacy

Inhoudsopgave

Doel van deze informatiebrochure

De Gegevensbeschermingsautoriteit (GBA) houdt voortdurend toezicht op de maatschappelijke, economische en technologische ontwikkelingen die een impact hebben op de bescherming van persoonsgegevens.

Een van deze zich snel ontwikkelende trends is dat het gebruik van artificiële-intelligentiesystemen (AI) niet meer beperkt blijft tot de industrie en de academische wereld, maar ook steeds meer deel uitmaakt van het dagelijkse leven van burgers. Van virtuele hulpmiddelen tot medische diagnoses met behulp van AI: mensen komen steeds vaker in aanraking met AI-systemen. Sommige van deze systemen zijn getraind op basis van persoonsgegevens[1] die uit verschillende bronnen zijn verzameld, waaronder feeds van sociale media, zoekopdrachten op internet, invoer in chatbots of online aankopen. De complexiteit en ondoorzichtigheid van AI-systemen maken het echter moeilijk om te begrijpen welke persoonsgegevens worden verzameld, wat het doel van de verwerking[2] is en hoe beslissingen worden genomen. Deze kenmerken hebben gevolgen voor burgers bij de uitoefening van hun recht op gegevensbescherming, omdat zij hierdoor de controle over hun persoonsgegevens verliezen en minder goed in staat zijn om oneerlijke resultaten aan te vechten.

Het recht op privacy en gegevensbescherming, verankerd in het Handvest van de grondrechten van de Europese Unie en de Algemene Verordening Gegevensbescherming (AVG), voorziet in objectieve rechten die tot doel hebben mensen controle te geven over hun persoonsgegevens. Daarnaast voorziet de verordening artificiële intelligentie (AI-wet) in een regelgevingskader voor de ontwikkeling en het inzetten van AI-systemen dat gericht is op het bevorderen van een innovatief klimaat, met inachtneming van de veiligheid, gezondheid en grondrechten van burgers.

In deze context is deze informatiebrochure opgesteld, om mensen te helpen begrijpen hoe AI-systemen van invloed kunnen zijn op hun privacy en de bescherming van hun persoonsgegevens. De brochure biedt ook praktische aanbevelingen om mensen te helpen de controle over hun gegevens te behouden in een omgeving die steeds meer door AI wordt gestuurd.

---

[1] Artikel 4.1 AVG: "*'persoonsgegevens': alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ('de betrokkene'); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;*"
Opmerking: er gelden strengere beschermingsmaatregelen voor de verwerking van bijzondere categorieën van gegevens (bijv. gezondheid, ras, religie) op grond van artikel 9 van de AVG.

[2] Artikel 4.2 AVG: "*'verwerking': een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;*"

Op basis van de brochure "Artificiële-intelligentiesystemen en de AVG: een benadering vanuit gegevensbescherming" van december 2024 wil het Algemeen Secretariaat dieper ingaan op specifieke onderwerpen om burgers bewuster te maken, de kennis over AI te vergroten en praktische adviezen te geven aan de industrie via een reeks publicaties over AI en gegevensbescherming. U vindt de volledige reeks **hier**.

Publiek voor deze informatiebrochure

Deze informatiebrochure is bedoeld voor personen die in hun dagelijkse leven gebruikmaken van of interactie hebben met AI-systemen, hetzij via onlineplatforms, mobiele applicaties, verbonden apparaten of andere digitale diensten.

Hij is voor lezers die willen begrijpen hoe AI-systemen hun persoonsgegevens gebruiken en hoe dit hun privéleven kan beïnvloeden, zonder dat hiervoor technische of juridische achtergrondkennis nodig is.

Aan de hand van duidelijke uitleg en concrete voorbeelden biedt de brochure een beknopt overzicht van wat AI-systemen zijn, hoe ze werken, welke soorten persoonsgegevens ze verzamelen en verwerken, welke potentiële risico's voor de privacy ze met zich meebrengen en welke rechten mensen hebben op grond van de wetgeving inzake gegevensbescherming – met eenvoudige stappen om die rechten uit te oefenen.

De impact van artificiële intelligentie op privacy

1. AI-systeem

1.1. Begrip en kenmerken

De AI-wet definieert een AI-systeem als: *'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[3], 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"* [4].

Deze definitie hanteert een op de levenscyclus gebaseerd perspectief, waarbij een onderscheid wordt gemaakt tussen de ontwikkelingsfase van AI-systemen en het inzetten ervan. In dat verband erkent ze dat hun kenmerken in de ene fase kunnen voorkomen zonder dat deze naar de andere fase worden overgedragen.[i]

In wezen zijn AI-systemen computergebaseerde systemen die beslissingen kunnen nemen door gegevens te analyseren en patronen te identificeren. Door hun autonomie kunnen ze van die gegevens leren om hun prestaties aan te passen en te verbeteren, zodat nauwkeurigere of genuanceerdere resultaten worden gegenereerd, soms door toekomstig gedrag af te leiden.[ii]

1.2. AI-systeem & AI-model

Wat AI-systemen onderscheidt van traditionele automatiseringssystemen – zoals vooraf gedefinieerde klantsegmentatie (gebruikers gegroepeerd op basis van vooraf gedefinieerde kenmerken) of tools voor het maskeren van gegevens volgens vaste regels (namen of ID's worden vervangen door pseudoniemen volgens vaste patronen) – is hun inferentievermogen op basis van gegevens of kennis.[iii] AI-systemen maken gebruik van geavanceerde gegevensverwerkingstechnieken[5] om te infereren uit gegevens en, in sommige gevallen, om te leren of zich aan te passen.[iv]

Deze gegevensverwerkingstechnieken worden uitgevoerd door een of meer AI-modellen binnen een AI-systeem. Een AI-model is een algoritme dat is getraind op een dataset om een aantal vooraf gedefinieerde of door training aangeleerde taken uit te voeren. AI-

[3] Expliciete doelstellingen zijn doelstellingen die door de ontwikkelaar bewust in het systeem zijn gecodeerd (bijv. fouten minimaliseren, klikfrequentie maximaliseren, ziekterisico voorspellen). Impliciete doelstellingen worden afgeleid uit het gedrag van het systeem of onderliggende veronderstellingen (bijv. het bij voorkeur weergeven van emotioneel provocerende berichten, het versterken van polariserende inhoud of het prioriteren van inhoud van zeer actieve gebruikers kan wijzen op een verborgen doel om betrokkenheid te vergroten).

[4] Artikel 3.1 van de AI-wet.

[5] Er kunnen twee belangrijke benaderingen van gegevensverwerking worden onderscheiden. Enerzijds een benadering op basis van machinaal leren waarbij het AI-systeem aan de hand van gegevens leert hoe bepaalde doelstellingen kunnen worden bereikt. Anderzijds een benadering op basis van logica en kennis waarbij AI-systemen informatie kunnen afleiden uit de gecodeerde kennis of de symbolische weergave van de taken in kwestie.

systemen integreren AI-modellen met andere systeemcomponenten (monitoringtools, applicatieprogramma-interfaces (API's), enz.).[v]

De analogie met koken helpt om het verschil te begrijpen. Het trainen van een AI-model is het bedenken van een recept voor een cake, terwijl het AI-systeem de cake bakt. De gebakken cake (de output) hangt af van de kwaliteit van de ingrediënten (de data), de betrouwbaarheid van het recept (de AI-modelarchitectuur) en de te volgen stappen (het algoritme). Door het model in het AI-systeem te integreren, kan de cake worden gebakken volgens het recept, met de juiste ingrediënten, door de stappen in de juiste volgorde uit te voeren en door de oven, cakevorm, mengkommen, enz. te gebruiken (de infrastructuur, API's, interfaces, enz.) om het proces uit te voeren.

1.3. Toepassingsgebied van het AI-systeem

AI-systemen kunnen op veel manieren worden gebruikt[6]. Daarom kunnen AI-systemen, afhankelijk van hun doel, in een of meer van de volgende categorieën worden ingedeeld. Het doel waarvoor een AI-systeem bedoeld is, helpt ook om te bepalen welke categorieën gegevens nodig zijn voor de training en het inzetten ervan.

Expertsystemen simuleren het besluitvormingsvermogen van een menselijke expert op specifieke gebieden (bijv. door geautomatiseerde klinische diagnostische opmerkingen te geven bij medische verslagen). Ze hebben vaak gestructureerde persoonsgegevens nodig, zoals medische dossiers, juridische casussen of diagnostische informatie.

Autonome systemen kunnen onafhankelijk functioneren in dynamische omgevingen (bijv. zelfrijdende auto's, drones). Ze kunnen locatiegegevens, sensorgegevens of biometrische identificatiegegevens verwerken.

Cognitive computing bootst menselijke denkprocessen na om ongestructureerde gegevens te interpreteren en besluitvorming te ondersteunen (bijv. systemen die worden gebruikt voor het evalueren van patiëntgegevens). Deze systemen maken vaak gebruik van diverse persoonsgegevens, zoals e-mails, spraakopnames, documenten en chatlogs.

Computer vision interpreteert visuele input, zoals afbeeldingen of video's, voor herkenning, tracking of analyse (bijv. systemen die worden gebruikt om de bewegingen van patiënten te monitoren). Een dergelijk systeem kan gezichtsbeelden, looppatronen en videobeelden verwerken.

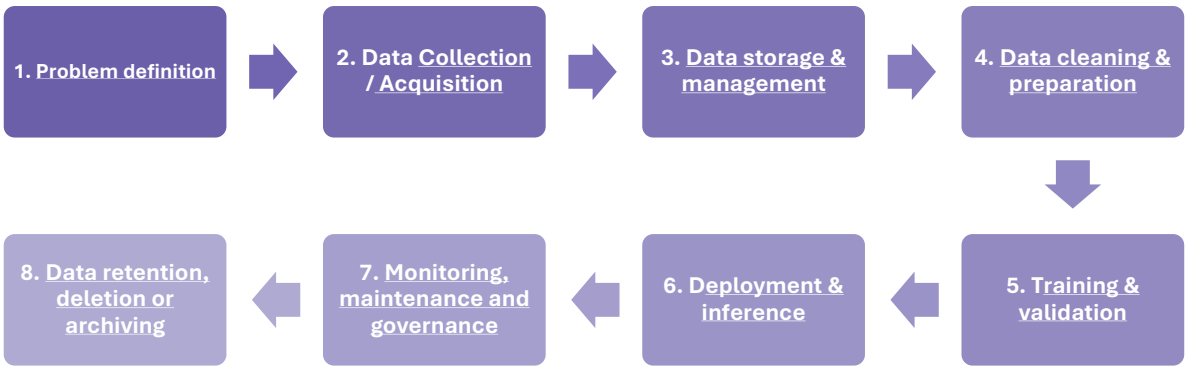
AI-aangedreven robots hebben betrekking op machines die complexe taken uitvoeren door interactie met hun omgeving (bijv. autonome robotstofzuigers). Afhankelijk van hun toepassing kunnen ze gebruikmaken van audiovisuele gegevens en locatiegegevens.

AI-systemen voor natuurlijke taalverwerking zijn ontworpen om menselijke taal in tekst- of spraakvorm te begrijpen, te interpreteren en te genereren (bijv. chatbots). Deze systemen verwerken vaak chatgeschiedenissen en spraakopdrachten.

[6] Zie de brochure 'Artificiële-intelligentiesystemen en de AVG: een benadering vanuit gegevensbescherming, pagina's 6-7, uitgegeven door de Gegevensbeschermingsautoriteit.

1.4. Levenscyclus van het AI-systeem en daarmee verband houdende gegevensverwerkingsactiviteiten

Ongeacht hun doeleinde volgen AI-systemen tijdens hun levenscyclus doorgaans vergelijkbare gegevensverwerkingsactiviteiten. De onderstaande afbeelding toont de gegevensverwerkingsactiviteiten die gewoonlijk worden uitgevoerd gedurende de levenscyclus van een AI-systeem.



vi

1. Probleemdefiniëring: De eerste stap is het identificeren van het doeleinde van het AI-systeem. Dit doeleinde moet duidelijk worden gedefinieerd en omvat doorgaans doelstellingen, succescriteria en wettelijke verplichtingen.

2. Dataverzameling/-verwerving: De tweede stap is het verzamelen of verwerven van ruwe data, waaronder persoonsgegevens, uit verschillende bronnen. Dergelijke bronnen omvatten, maar zijn niet beperkt tot:

- Activiteit op sociale media: online berichten, 'likes', reacties, connecties, enz.
- Klantendatabanken: namen, e-mailadressen, telefoonnummers,
- aankoopgeschiedenis, enz.
- Transactiegegevens: creditcardbetalingen, facturen, loyaliteitskaartgegevens, enz.
- Browsegeschiedenis: bezochte websites, zoekopdrachten, klikpatronen, enz.
- Openbare registers: bedrijfsregisters, eigendomsakten, forumberichten, enz.
- Slimme apparaten: spraakopdrachten, gps-locatie, fitnesstrackergegevens, enz.

3. Opslag en beheer van data: De derde stap is gericht op het veilig opslaan en beheren van de gegevens die in de vorige stap zijn verzameld of verworven. Dit omvat het toepassen van passende opslagvoorwaarden en beveiligingsmaatregelen, zoals versleuteling, toegangscontroles en mechanismen ter bescherming van de privacy.

4. Opschoning en voorbereiding van data: In de vierde stap worden de ruwe data voorverwerkt om de kwaliteit en de consistentie te verbeteren en tegelijkertijd de privacy te waarborgen. Deze voorverwerkingsactiviteiten kunnen bestaan uit het corrigeren van fouten in de data (bijv. over- of ondervertegenwoordiging van bepaalde demografische groepen), het standaardiseren van de data (bijv. alle datums worden in dit formaat

vastgelegd: DD/MM/JJJJ; alle gegevens over geslacht worden in dit formaat geregistreerd: man/vrouw), en indien mogelijk, de pseudonimisering of anonimisering van de persoonsgegevens. Zodra de gegevens zijn opgeschoond, worden ze meestal opgesplitst in drie verschillende datasets met elk hun eigen doel in de vijfde stap (trainingsdataset, validatiedataset en testdataset).

5. Training en validatie: In deze stap worden de datasets gebruikt om een AI-systeem te trainen, te valideren en te testen om de nauwkeurige werking van het AI-systeem te verzekeren. Validatiedata helpen bij het aanpassen van het systeem tijdens de training, terwijl testdata worden gebruikt om belangrijke prestatiemaatstaven te beoordelen, zoals nauwkeurigheid, rechtvaardigheid en veralgemeenbaarheid. Trainingsdata worden gebruikt om het AI-systeem te trainen voordat het wordt ingezet.

6. Inzet en inferentie: Na een succesvolle validatie wordt een getraind AI-systeem ingezet en begint het inputdata te ontvangen (bijv. gebruikersprompts of door het systeem gegenereerde vragen) en output te genereren. Er kunnen filtermechanismen worden toegepast om ongewenste inputs of verboden outputs te voorkomen.

7. Monitoring, onderhoud en governance: Nadat een AI-systeem is ingezet, wordt het gemonitord om ervoor te zorgen dat het naar verwachting presteert. Feedback en systeemdata kunnen worden gebruikt voor het verfijnen of hertrainen van het model. Governanceprocessen zorgen voor naleving, controleerbaarheid en verantwoording gedurende de hele levenscyclus van AI.

8. Behoud, verwijdering of archivering van data: Persoonsgegevens mogen niet langer worden bewaard dan nodig is. Zodra gegevens niet langer nodig zijn, moeten ze veilig worden verwijderd, geanonimiseerd of gearchiveerd in overeenstemming met de toepasselijke wetgeving inzake gegevensbescherming en het beleid van de organisatie.

Opgemerkt moet worden dat de zevende en achtste stap tegelijkertijd kunnen worden uitgevoerd en een continu proces vormen. Tijdens de levenscyclus van een AI-systeem is voortdurende monitoring noodzakelijk om onrechtvaardige of onnauwkeurige resultaten te identificeren. Deze monitoring maakt het mogelijk om het AI-systeem aan te passen om de prestaties te verbeteren en onnauwkeurigheden te corrigeren – of deze nu voortkomen uit de trainings- of validatiegegevens, of uit de onderliggende broncode.

2. Privacyrisico's

AI-systemen zorgen voor nieuwe dimensies in privacyrisico's door de uitgebreide verzameling en verwerking van gegevens. Deze risico's vloeien voort uit het onrechtmatig of ongeoorloofd verzamelen, verwerken of delen van persoonsgegevens. Maar zelfs rechtmatige gegevensverwerkingen kunnen privacyproblemen opleveren, vooral als ze niet voldoende transparant, rechtvaardig of evenredig zijn. Voorbeelden hiervan zijn buitensporige bewaking, profilering of onvoorzien secundair gebruik van gegevens.

AI-systemen kunnen privacyrisico's vergroten – zoals het risico van buitensporige of onevenredige gegevensverzameling en mogelijke schendingen van het beginsel van minimale gegevensverwerking (artikel 5.1.c) AVG) – vanwege hun vermogen om vaak in

real time enorme hoeveelheden persoonsgegevens te verwerken. Risico's die vroeger geïsoleerd waren – zoals handmatige profilering[7], beperkte bewaking of gerichte reclame – kunnen nu systemische problemen worden. AI-systemen kunnen worden gebruikt om miljoenen gebruikers te profileren, gezichtsherkenning toe te passen in openbare ruimtes en zeer gepersonaliseerde en gerichte advertenties te leveren.[vii] De snelheid, schaal en ondoorzichtigheid van de geautomatiseerde besluitvorming van AI-systemen maken het moeilijk om schendingen van privacy en gegevensbescherming te voorkomen.

AI-gestuurde automatisering heeft het potentieel om menselijk toezicht op geautomatiseerde, op data gebaseerde beslissingen op te heffen of te verminderen. Dergelijke geautomatiseerde beoordelingen worden in alledaagse scenario's gebruikt, zoals bij het inschatten van kredietwaardigheid, het evalueren van veiligheidsrisico's en bij wervings- of selectieprocessen. Deze automatische besluitvorming roept vragen op over transparantie en menselijke betrokkenheid, wat rechtvaardige resultaten kan ondermijnen en de mogelijkheid van personen om genoegdoening te krijgen kan beperken.[viii] Hoewel artikel 22 van de AVG besluiten verbiedt die uitsluitend op geautomatiseerde verwerking zijn gebaseerd en aanzienlijke gevolgen hebben (zie punt 3.2.h)), zijn er onder specifieke voorwaarden en waarborgen uitzonderingen mogelijk.

Het vermogen van AI om gevoelige persoonsgegevens te infereren kan leiden tot illegale verwerkingsactiviteiten of het categoriseren en profileren van burgers.[ix] Met behulp van technieken op basis van machinaal leren kunnen AI-systemen kenmerken zoals seksuele geaardheid, religieuze overtuigingen, gezondheidstoestand of emotionele toestand afleiden uit indirecte bronnen zoals browsegeschiedenis, online aankoopgeschiedenis of stemgeluid – vaak zonder medeweten of toestemming van de betrokkene. Bovendien kunnen inferenties onnauwkeurig of misleidend zijn vanwege hun probabilistische[x] karakter (statistische schattingen in plaats van geverifieerde feiten).

3. Bescherming van uw persoonsgegevens

De AVG heeft een breed toepassingsgebied en heeft betrekking op activiteiten waarbij persoonsgegevens binnen de EU worden verwerkt.[8] AI-systemen kunnen persoonsgegevens in verschillende fasen van hun levenscyclus[xi] verwerken, soms niet doelbewust. In feite moeten AI-systemen die niet bedoeld zijn om persoonsgegevens te verwerken, worden getraind om deze gegevens te herkennen. In dat geval worden persoonsgegevens opgenomen in de trainings-, validatie- en testdatasets, en worden ze verwerkt in de ontwikkelingsfase.

Artikel 5 van de AVG somt de beginselen op die bij alle verwerkingen van persoonsgegevens in acht moeten worden genomen. Deze beginselen vereisen dat persoonsgegevens: op rechtmatige, behoorlijke en transparante wijze worden verwerkt;

[7] Artikel 4.4 van de AVG: "*'profilering': elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen;*"
[8] Artikelen 2 en 3 van de AVG.

worden verzameld voor een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doeleinde; toereikend, ter zake dienend en noodzakelijk zijn om dat doel te verwezenlijken; juist en geactualiseerd zijn; niet langer worden bewaard dan nodig is voor de verwerking; en op passende wijze worden beveiligd. Bovendien moeten verwerkingsverantwoordelijken[9] kunnen aantonen dat zij deze beginselen naleven.

Op grond van het transparantiebeginsel zijn verwerkingsverantwoordelijken verplicht om personen op een duidelijke en toegankelijke manier te informeren over de verwerkingsactiviteiten. Meer specifiek kunnen verwerkingsverantwoordelijken, indien van toepassing, worden gevraagd om de logica achter geautomatiseerde besluiten, zoals die van AI-systemen, toe te lichten.

In de volgende punten worden belangrijke aspecten behandeld waarop mensen moeten letten wanneer ze online actief zijn. Deze aanbevelingen zijn bedoeld om hen bewust te maken van de verwerkingsactiviteiten die worden uitgevoerd en van de manieren waarop zij hun rechten kunnen uitoefenen.

3.1. Belangrijke aandachtspunten

3.1.1. Controleren van privacybeleid, algemene voorwaarden en standaardprivacyinstellingen

Als u akkoord gaat met het privacybeleid, kunnen verwerkingsverantwoordelijken de daarin beschreven persoonsgegevens verwerken. Personen hebben het recht om niet in te stemmen met privacybeleid zonder dat dit hen belet toegang te krijgen tot websites, diensten, enz., tenzij er een gegronde reden is (bijv. cookies die nodig zijn voor het functioneren van de website). Het intrekken van toestemming moet net zo eenvoudig zijn als het geven ervan.

Door het privacybeleid en de algemene voorwaarden te lezen en te controleren, krijgen betrokkenen inzicht in hoe hun persoonsgegevens worden verzameld, verwerkt en gedeeld. Dit bevordert het nemen van weloverwogen beslissingen en vergemakkelijkt de effectieve uitoefening van gegevensbeschermingsrechten.

Het is raadzaam om de standaardprivacyinstellingen te controleren, zoals die met betrekking tot chatgeschiedenis, zoekgeschiedenis, AI-training, gepersonaliseerde advertenties, het delen van analyses en automatische cloudback-ups. Deze instellingen zijn vaak standaard ingeschakeld en kunnen worden aangepast aan individuele voorkeuren.

Bovendien is het voor mensen die thuis slimme apparaten gebruiken verstandig om standaardwachtwoorden te wijzigen en na te gaan hoe deze apparaten hun persoonsgegevens verwerken. Slimme apparaten in huis verzamelen informatie over de huishoudelijke activiteiten van personen, waaronder mogelijk gevoelige gegevens of

[9] Artikel 4.7 AVG: "*'verwerkingsverantwoordelijke': een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen;*"

gedragsgegevens. Door te begrijpen hoe dergelijke apparaten informatie verzamelen, verwerken en delen, kunnen potentiële risico's worden vastgesteld en beperkt, waardoor onnodige of buitensporige gegevensuitwisseling in de thuisomgeving wordt verminderd.

3.1.2. Voorzichtig zijn met het delen van persoonsgegevens

Voordat ze gevoelige informatie – zoals medische gegevens, financiële gegevens of persoonlijke afbeeldingen – in chatbots, applicaties of online platforms invoeren, moeten betrokkenen voorzichtigheid aan de dag leggen. Waar mogelijk kan het gebruik van pseudoniemen of het bewerken van persoonlijk identificeerbare informatie (bijv. namen, adressen of leeftijd) helpen om de identiteit van een persoon te beschermen.

Door de bekendmaking van persoonlijke informatie te beperken, wordt het risico op misbruik, profilering of ongeoorloofde toegang verminderd, en wordt de controle over persoonsgegevens versterkt.

Voordat mensen met AI-systemen communiceren, moeten ze nadenken over de gevoeligheid van de informatie die ze verstrekken. Een nuttige vraag, die als leidraad kan dienen, is: “Als ik tijdens een diner bij onbekende mensen zou zitten, zou ik dan deze informatie over mezelf of iemand anders met anderen delen?”

3.1.3. Up-to-date houden van software en apparaten

Het regelmatig updaten van software en firmware helpt veiligheidsrisico's te beperken, zodat de kans op datalekken of ongeoorloofde toegang tot persoonsgegevens kleiner wordt.

3.1.4. Beheren van applicatie- en apparaatrechten

Het is raadzaam om regelmatig applicaties te controleren die toegang hebben tot de microfoon, camera, locatiegegevens, contacten en bestanden van een apparaat. Wanneer bepaalde toestemmingen niet essentieel zijn, kan de betrokkene ervoor kiezen om deze uit te schakelen of alleen in te schakelen wanneer dat nodig is, bijv. door de toegang tot foto's te beperken of deze selectief te delen met specifieke applicaties. Door toestemmingen op deze manier aan te passen, wordt onnodige toegang tot persoonsgegevens beperkt, zodat alleen essentiële informatie wordt verwerkt.

3.2. Rechten van de betrokkene

Wie de aanbevelingen uit het vorige punt opvolgt, zou al moeten begrijpen welk soort persoonsgegevens verwerkingsverantwoordelijken in hun bezit hebben en gebruiken. Daarnaast verleent de AVG personen rechten die kunnen worden uitgeoefend door contact op te nemen met de genoemde verwerkingsverantwoordelijken. Als om de uitoefening van deze rechten wordt verzocht, moeten verwerkingsverantwoordelijken binnen een maand antwoorden. Deze termijn kan met maximaal twee maanden worden verlengd, indien dit gerechtvaardigd is.

3.2.1. Recht op informatie

De artikelen 13 en 14 van de AVG voorzien in een recht op informatie, waarbij verwerkingsverantwoordelijken verplicht zijn om personen te informeren over de verwerkingsactiviteiten die worden uitgevoerd. Deze informatie moet personen in staat stellen weloverwogen beslissingen te nemen en hun rechten op het gebied van

gegevensbescherming uit te oefenen. De informatie moet in duidelijke en toegankelijke taal worden aangeboden en staat meestal in het privacybeleid.

De AVG maakt onderscheid tussen situaties waarin persoonsgegevens rechtstreeks bij de betrokkene worden verzameld (toestemmingsformulieren, website-abonnementen, enz.) en situaties waarin deze gegevens onrechtstreeks worden verzameld (webscraping, licentieovereenkomsten, enz.). Wanneer persoonsgegevens onrechtstreeks worden verzameld, verplicht artikel 14 van de AVG de verwerkingsverantwoordelijken om de betrokkene binnen een maand na de verzameling te informeren.

Verwerkingsverantwoordelijken moeten de volgende informatie verstrekken: identiteit en contactgegevens van de verwerkingsverantwoordelijke; doel(en) van en rechtsgrond(en) voor de verwerking; bewaartermijnen van de gegevens; rechten van de betrokkene; details over gegevensdoorgifte; en informatie over geautomatiseerde besluitvorming. Op grond van artikel 14 van de AVG zijn verwerkingsverantwoordelijken ook verplicht om de gegevensbronnen en categorieën van verzamelde persoonsgegevens bekend te maken.

3.2.2. Recht van inzage

Op grond van artikel 15 van de AVG hebben betrokkenen het recht om uitsluitsel te verkrijgen over het al dan niet verwerken van hen betreffende persoonsgegevens. Wanneer dit recht wordt uitgeoefend, moeten verwerkingsverantwoordelijken toegang verlenen tot gegevens zoals het doel en de categorieën van de verwerkte gegevens, de ontvangers van de gegevens (indien van toepassing), de bewaartermijn, de rechten inzake gegevensbescherming, het recht om een klacht in te dienen bij een toezichthoudende autoriteit, de bron van de gegevens wanneer deze niet rechtstreeks van de betrokkene zijn verkregen, en elke geautomatiseerde besluitvorming, met inbegrip van profilering, met nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.

Bovendien hebben betrokkenen het recht om kosteloos een kopie te verkrijgen van de persoonsgegevens die worden verwerkt, indien die kopie nodig is om inzicht te krijgen in de context waarin de gegevensverwerking plaatsvindt.[10]

3.2.3. Recht op gegevenswissing

Op grond van artikel 17 van de AVG kunnen betrokkenen verzoeken om hun persoonsgegevens zonder onredelijke vertraging te laten verwijderen als aan bepaalde voorwaarden is voldaan, namelijk wanneer:

- de persoonsgegevens niet langer nodig zijn voor het oorspronkelijke doeleinde van de verwerking;
- de betrokkene zijn toestemming intrekt en er geen andere rechtsgrond voor de verwerking is;

[10] Volgens het HvJ-EU in de zaak C-487/21 (Österreichische Datenschutzbehörde en CRIF) kan een “kopie” delen van originele documenten of volledige documenten omvatten, indien dit nodig is om de doeltreffendheid van het recht van inzage te waarborgen, met inachtneming van de rechten en vrijheden van anderen. Het formaat moet de betrokkene in staat stellen de gegevens te bewaren en te raadplegen, en in sommige gevallen (bijv. handgeschreven notities of geluidsopnames) kan het formaat zelf integraal deel uitmaken van de persoonsgegevens.

- de betrokkene overeenkomstig artikel 21, lid 1, van de AVG bezwaar maakt tegen de verwerking en er geen prevalerende dwingende gerechtvaardigde gronden voor de verwerking zijn;
- de persoonsgegevens onrechtmatig zijn verwerkt;
- de persoonsgegevens moeten worden gewist om te voldoen aan een wettelijke verplichting; of
- de persoonsgegevens zijn verzameld in verband met een aanbod van diensten van de informatiemaatschappij.

In situaties waarin de verwerkingsverantwoordelijke de persoonsgegevens aan derde ontvangers heeft doorgegeven of openbaar heeft gemaakt, moet hij passende maatregelen treffen om ervoor te zorgen dat deze persoonsgegevens worden gewist.[11]

3.2.4. Recht van bezwaar

Artikel 21 van de AVG geeft betrokkenen het recht om bezwaar te maken tegen de verwerking van hun persoonsgegevens. Zodra bezwaar wordt gemaakt, moet de verwerkingsverantwoordelijke de verwerking stopzetten, tenzij hij dwingende gerechtvaardigde gronden voor de verwerking aanvoert.

Wanneer de verwerking ten behoeve van direct marketing plaatsvindt, is het recht van bezwaar absoluut en is geen rechtvaardiging nodig.

Zowel de Belgische als de Franse gegevensbeschermingsautoriteit hebben overigens richtlijnen gepubliceerd waarin wordt uiteengezet welke stappen mensen kunnen ondernemen om te voorkomen dat technologiebedrijven (zoals Meta, TikTok, Microsoft, X) hun persoonsgegevens gebruiken om hun AI-systemen te trainen. Deze stappen zijn **hier** en **hier** beschikbaar.

3.2.5. Recht op beperking van de verwerking

Op grond van artikel 18 van de AVG hebben betrokkenen het recht de beperking van de verwerking van gegevens te vragen wanneer:

- de juistheid van de persoonsgegevens wordt betwist door de betrokkene;
- de verwerking onrechtmatig is;
- de verwerkingsverantwoordelijke de gegevens niet meer nodig heeft voor het oorspronkelijke doeleinde, maar de betrokkene deze nodig heeft voor de instelling, uitoefening of onderbouwing van een rechtsvordering;
- de betrokkene bezwaar heeft gemaakt tegen de verwerking (artikel 21 van de AVG), terwijl de afweging tussen het belang van de verwerkingsverantwoordelijke en dat van de betrokkene wordt uitgevoerd.

Tijdens een dergelijke beperking mogen persoonsgegevens alleen worden verwerkt (met uitzondering van de opslag ervan) met toestemming van de betrokkene of voor de

[11] Artikel 19 AVG: "*De verwerkingsverantwoordelijke stelt iedere ontvanger aan wie persoonsgegevens zijn verstrekt, in kennis van elke rectificatie of wissing van persoonsgegevens of beperking van de verwerking overeenkomstig artikel 16, artikel 17, lid 1, en artikel 18, tenzij dit onmogelijk blijkt of onevenredig veel inspanning vergt. De verwerkingsverantwoordelijke verstrekt de betrokkene informatie over deze ontvangers indien de betrokkene hierom verzoekt.*"

instelling, uitoefening of onderbouwing van een rechtsvordering of ter bescherming van de rechten van een andere natuurlijke persoon of rechtspersoon of om gewichtige redenen van algemeen belang voor de Unie of voor een lidstaat. De betrokkene wordt op de hoogte gebracht voordat de beperking wordt opgeheven.

Het recht op beperking van de verwerking verschilt van het recht van bezwaar, omdat het resulteert in een pauze voor alle verwerkingsactiviteiten, in plaats van alleen voor specifieke doeleinden.

3.2.6. Recht op rectificatie[11]

Artikel 16 van de AVG geeft betrokkenen het recht om te verzoeken onjuiste persoonsgegevens te corrigeren en onvolledige gegevens te vervolledigen (ook door middel van een aanvullende verklaring).

Indien de gegevens aan derden zijn verstrekt, moet de verwerkingsverantwoordelijke hen op de hoogte brengen van de rectificatie, tenzij dit onmogelijk blijkt of onevenredig veel inspanning vergt.

3.2.7. Recht op overdraagbaarheid van gegevens

Op grond van artikel 20 van de AVG hebben betrokkenen het recht om hun persoonsgegevens in een gestructureerde, gangbare en machineleesbare vorm te verkrijgen. Zij hebben ook het recht om deze aan een andere verwerkingsverantwoordelijke over te dragen indien de verwerking: berust op de toestemming van de betrokkene; noodzakelijk is voor de uitvoering van een overeenkomst; of via geautomatiseerde procedés wordt verricht. Indien dit technisch mogelijk is moeten gegevens rechtstreeks naar de nieuwe verwerkingsverantwoordelijke worden doorgezonden.

3.2.8. Recht om niet te worden onderworpen aan geautomatiseerde besluitvorming

Artikel 22 van de AVG geeft betrokkenen het recht om niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor hen rechtsgevolgen zijn verbonden of dat hen anderszins in aanmerkelijke mate treft[12].

Een verwerking is niet uitsluitend op automatische verwerking gebaseerd wanneer er sprake is van een relevante menselijke betrokkenheid. Dit veronderstelt de betrokkenheid van een persoon met voldoende bevoegdheid om de uitkomst van de verwerkingsactiviteit te wijzigen.[xii]

Geautomatiseerde besluitvorming is toegestaan wanneer dit noodzakelijk is voor de uitvoering van een overeenkomst, met de uitdrukkelijke toestemming van de betrokkene of indien dit wettelijk is toegestaan. In dergelijke gevallen moeten

[12] Volgens de WP29-richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering (2018) kunnen besluiten worden beschouwd als besluiten die de betrokkenen anderszins in aanmerkelijke mate treffen indien zij: de omstandigheden, het gedrag of de keuzes van de betrokkenen wezenlijk kunnen treffen; een langdurig of blijvend effect op de betrokkene kunnen hebben; of kunnen leiden tot uitsluiting of discriminatie van personen.

verwerkingsverantwoordelijken ervoor zorgen dat de betrokkenen het recht hebben om menselijke tussenkomst[13] van de verwerkingsverantwoordelijke te verkrijgen, hun standpunt kenbaar te maken en het besluit te betwisten.

Bovendien hebben betrokkenen op grond van artikel 15.1.h) van de AVG recht op uitleg over de werking van het mechanisme dat wordt gebruikt bij geautomatiseerde besluitvorming[14] [15]. Dit houdt in dat de procedures en principes die worden toegepast om inzicht te krijgen in hoe persoonsgegevens zijn gebruikt bij geautomatiseerde besluitvorming, duidelijk moeten worden gecommuniceerd[16].

3.3. Uitoefening van de rechten van de betrokkene

Wanneer een verwerkingsverantwoordelijke wordt verdacht van misbruik van persoonsgegevens, of wanneer het nodig is om te controleren welke gegevens worden verwerkt, kunnen betrokkenen hun gegevensbeschermingsrechten uitoefenen.

3.3.1. Rechtstreeks contact opnemen met de verwerkingsverantwoordelijke

Betrokkenen kunnen hun rechten uitoefenen door contact op te nemen met de verwerkingsverantwoordelijke.

- Gebruik van een standaardbrief: De GBA heeft **hier** standaardbrieven op maat samengesteld. Ze bieden gestandaardiseerde formats om te helpen bij het formuleren van dergelijke verzoeken. In de brief moet duidelijk worden aangegeven wat de aard van het verzoek is en op welke rechtsgrond het is gebaseerd.
- Identificatie van de contactgegevens van de verwerkingsverantwoordelijke: Indien beschikbaar, dient het verzoek te worden gericht aan de aangewezen functionaris voor gegevensbescherming (DPO), wiens contactgegevens in het privacybeleid worden vermeld. Als er geen DPO is opgegeven, kan het verzoek worden verzonden naar het algemene contactadres van de verwerkingsverantwoordelijke.
- Bewaring van bewijsmateriaal: De betrokkene moet altijd een kopie van het verzoek bewaren. Dit geldt als bewijs voor het geval dat verdere maatregelen, met inbegrip van een regelgevende interventie, noodzakelijk worden.
- Tijd geven om te reageren: Volgens de wetgeving inzake gegevensbescherming zijn verwerkingsverantwoordelijken verplicht om binnen een maand na ontvangst van het verzoek te reageren. In uitzonderlijke gevallen kan deze termijn met maximaal twee maanden worden verlengd, met opgave van redenen.

[13] Wat AI-systemen met een hoog risico betreft (hoofdstuk III van de AI-wet), moeten gebruiksverantwoordelijken het menselijk toezicht opdragen aan natuurlijke personen die over de nodige bekwaamheid, opleiding en bevoegdheid beschikken en de nodige ondersteuning krijgen (artikel 26.2 van de AI-wet). Artikel 14 van de AI-wet stelt de vereisten en doelstellingen vast voor menselijk toezicht op AI-systemen met een hoog risico.
[14] *Dun & Bradstreet*, § 57.
[15] Bovendien bepaalt artikel 86 van de AI-wet als algemene regel dat personen het recht hebben op een duidelijke uitleg over de rol die het AI-systeem met een hoog risico heeft gespeeld in het besluitvormingsproces, indien het besluit aanzienlijke gevolgen heeft voor hun gezondheid, veiligheid of grondrechten.
[16] *Dun & Bradstreet*, § 61.

3.3.2. De GBA inschakelen

Als de verwerkingsverantwoordelijke niet reageert of als het antwoord als ontoereikend wordt beschouwd, kan de betrokkene de zaak doorverwijzen naar de bevoegde toezichthoudende autoriteit (**via het contactformulier**):

- Een bemiddeling aanvragen: Bemiddeling is vaak de meest efficiënte methode om geschillen op te lossen. De GBA kan de verwerkingsverantwoordelijke verzoeken om de rechten van de betrokkene op passende wijze aan te pakken.
- Een klacht indienen: Wanneer bemiddeling niet tot een oplossing leidt, kan een formele klacht worden ingediend bij de GBA. Dit kan aanleiding geven tot handhavingsmaatregelen, met inbegrip van maar niet beperkt tot een waarschuwing, een administratieve geldboete of een onmiddellijk bevel om bepaalde verwerkingsactiviteiten te staken.

Referenties:

- Andreas Krause, Jonas Hübotter. *Probabilistic Artificial Intelligence* (2025). Beschikbaar via deze link: https://arxiv.org/pdf/2502.05244.
- Bart Custers, Helena Vrabec. Tell me something new: data subject rights applied to inferred data and profiles, Computer Law & Security Review, Volume 52, 2024, 105956, ISSN 2212-473X, https://doi.org/10.1016/j.clsr.2024.105956. (https://www.sciencedirect.com/science/Article/pii/S0267364924000232).
- Bygrave, in Kuner, Bygrave, Docksey. *The EU General Data Protection Regulation (GDPR): A Commentary, Article 22 GDPR*, (Oxford University Press 2020) p. 533.
- Daniel J. Solove. Artificial Intelligence and Privacy, 77 Fla. L. Rev. 1 (2025). Beschikbaar via deze link: https://scholarship.law.ufl.edu/flr/vol77/iss1/1.
- Enrico Glerean. *Fundamentals of Secure AI Systems with Personal Data* (2024). EDPB.
- Europese Commissie. Richtsnoeren betreffende de definitie van een artificiële-intelligentiesysteem zoals vastgesteld bij Verordening (EU) 20241689 (AI-verordening), https://digital-strategy.ec.europa.eu/nl/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application.
- Europees Comité voor gegevensbescherming (European Data Protection Board – EDPB). *Respecteer de rechten van individuen* ("SME Guide"). Beschikbaar via deze link: https://www.edpb.europa.eu/sme-data-protection-guide/respect-individuals-rights_nl.
- Europees Toezichthouder voor gegevensbescherming (European Data Protection Supervisor - EDPS). Guidelines on the protection of personal data processed by mobile applications (2016). Beschikbaar via deze link: https://www.edps.europa.eu/sites/default/files/publication/16-11-07_guidelines_mobile_apps_en.pdf (enkel beschikbaar in het Engels).
- Europees Toezichthouder voor gegevensbescherming (European Data Protection Supervisor - EDPS). *Guidelines on the Rights of Individuals with regard to the Processing of Personal Data* (2014). Beschikbaar via deze link: https://www.edps.europa.eu/sites/default/files/publication/14-02-25_gl_ds_rights_en.pdf (niet beschikbaar in het Nederlands).
- Europees Toezichthouder voor gegevensbescherming (European Data Protection Supervisor - EDPS). *Tech Dispatch #2/2023 - Explainable Artificial Intelligence (XAI)*. Beschikbaar via deze link: https://www.edps.europa.eu/system/files/2023-11/23-11-16_techdispatch_xai_en.pdf (enkel beschikbaar in het Engels).
- Marco Almada. *Law & Compliance in AI Security & Data Protection* (2024). EDPB.
- OECD (2024) "*Explanatory memorandum on the updated OECD definition of an AI system*", OECD Artificial Intelligence Papers, No. 8, OECD Publishing, Paris, beschikbaar via deze link: https://doi.org/10.1787/623da898-en (enkel beschikbaar in het Engels).
- Richtlijn 2016/679/EG 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.

- Verordening (EU) 2024/1689 van het Europees Parlement en de Raad van 13 juni *2024 tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie en tot wijziging van de Verordeningen (EG) nr. 300/2008, (EU) nr. 167/2013, (EU) nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 en (EU) 2019/2144, en de Richtlijnen 2014/90/EU, (EU) 2016/797 en (EU) 2020/1828*.
- Groep artikel 29 (WP29), *Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening 2016/679*, 17/NL WP251 rev.01, 6 februari 2018.

[i] *Richtsnoeren betreffende de definitie van een artificiële-intelligentiesysteem zoals vastgesteld bij Verordening (EU) 20241689 (AI-verordening)*, p. 2.
[ii] Voor meer informatie: overweging 12 AI-wet.
[iii] *Richtsnoeren betreffende de definitie van een artificiële-intelligentiesysteem zoals vastgesteld bij Verordening (EU) 20241689 (AI-verordening)*, p. 5.
[iv] Overweging 12 AI-wet.
[v] Marco Almada - *Law & Compliance in AI Security & Data Protection*, p. 22-24.
[vi] Enrico Glerean - *Fundamentals of Secure AI Systems with Personal Data*, p. 40-44.
[vii] Daniel J. Solove, *Artificial Intelligence and Privacy*, 77 Fla. L. Rev. 1 (2025). Beschikbaar via deze link: https://scholarship.law.ufl.edu/flr/vol77/iss1/1, p. 59-62.
[viii] Daniel J. Solove, *Artificial Intelligence and Privacy*, p. 6, 55-66.
[ix] Daniel J. Solove, *Artificial Intelligence and Privacy*, p. 16-18, 36-37, 39-40.
[x] Andreas Krause, Jonas Hübotter (2025) - *Probabilistic Artificial Intelligence*. Beschikbaar via deze link: https://arxiv.org/pdf/2502.05244 p.1-2, 37-38.
[xi] Marco Almada - *Law & Compliance in AI Security & Data Protection*, p. 25-26.
[xii] WP29, *Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening 2016/679*, 17/NL WP251 rev.01, 6 februari 2018, p. 24-25.
Bygrave, in Kuner, Bygrave, Docksey, *The EU General Data Protection Regulation (GDPR): A Commentary, Article 22 GDPR*, (Oxford University Press 2020) p. 533.