AI, de AI-verordening en de AVG

De impact op de veilige verwerking van persoonsgegevens en de onderlinge verhouding van beide kaders

Erik Steijn
FG / CAICO

AI-toepassingen worden in hoog tempo geïntegreerd in bedrijfsprocessen, dienstverlening en besluitvorming. Tegelijkertijd verwerken die toepassingen vaak persoonsgegevens, soms expliciet, vaak impliciet via prompts, logbestanden of trainingsdata[1]. De inzet van AI raakt daarmee onmiddellijk aan het grondrecht op gegevensbescherming en aan de AVG.

Vanaf 1 augustus 2024 geldt daarnaast een tweede, productgericht kader: de AI-verordening. Beide kaders gelden naast elkaar en grijpen op verschillende momenten in de levenscyclus van een AI-systeem in. Voor verwerkingsverantwoordelijken, aanbieders en gebruiksverantwoordelijken is het van belang te begrijpen hoe de kaders zich tot elkaar verhouden en welke verplichtingen wanneer ontstaan.

Dit whitepaper is opgesteld vanuit mijn adviespraktijk en de gecombineerde rollen van Functionaris Gegevensbescherming (FG) en Certified AI Compliance Officer (CAICO). Het whitepaper is bedoeld als helder, hanteerbaar overzicht voor privacy- en compliancefuncties. Juridische verwijzingen zijn met opzet expliciet opgenomen, zodat het document tevens als referentie kan dienen bij interne besluitvorming.

[1] *Trainingsdata wordt o.a. opgebouwd uit de ingevoerde prompts en bevatten daarmee persoonsgegevens van de 'prompter' en mogelijk ingevoerde persoonsgegevens.*

1. Inleiding

Sinds 1 augustus 2024 is de AI-verordening (Verordening (EU) 2024/1689) in werking. De verordening introduceert een Europees, risicogebaseerd kader voor het ontwikkelen, in de handel brengen en gebruiken van AI-systemen. De verplichtingen gaan in fasen in: de bepalingen over verboden AI-praktijken en AI-geletterdheid gelden sinds 2 februari 2025, de verplichtingen voor AI-modellen voor algemene doeleinden sinds 2 augustus 2025 en de kern van de verplichtingen voor AI-systemen met een hoog risico vanaf 2 augustus 2026.

De AI-verordening laat de AVG nadrukkelijk onverlet: artikel 2, lid 7, AI-verordening bepaalt dat de verordening de Uniewetgeving inzake gegevensbescherming, waaronder de AVG, onverkort van toepassing laat. Beide kaders vullen elkaar aan: de AVG beschermt het grondrecht op gegevensbescherming en richt zich op de rechtmatigheid van verwerkingen, terwijl de AI-verordening AI-systemen behandelt als product en eisen stelt aan veiligheid, kwaliteit en grondrechtenbescherming gedurende de hele levenscyclus.

Voor organisaties betekent dit dat AVG-verplichtingen (rechtmatige grondslag, doelbinding, dataminimalisatie, transparantie, DPIA) blijven gelden bovenop nieuwe verplichtingen uit de AI-verordening (AI-geletterdheid, risicoclassificatie, gebruik volgens gebruiksaanwijzing, menselijk toezicht, logging, registratie in de EU-databank en -voor bepaalde gebruiksverantwoordelijken- een grondrechteneffectbeoordeling, ook wel FRIA genoemd).

Dit whitepaper biedt een zakelijk en juridisch nauwkeurig overzicht van (1) de impact van AI en de AI-verordening op de veilige verwerking van persoonsgegevens, en (2) de verhouding tussen de AI-verordening en de AVG. Het whitepaper sluit af met praktische aanbevelingen en de toezichtcontext in Nederland.

2. De AI-verordening in vogelvlucht

2.1 Doel en juridische basis

De AI-verordening, Verordening (EU) 2024/1689, is op 12 juli 2024 gepubliceerd in het Publicatieblad van de EU en op 1 augustus 2024 in werking getreden. Het is een horizontale productverordening die geharmoniseerde regels stelt voor het in de handel brengen, in gebruik stellen en gebruiken van AI-systemen in de Europese Unie. De verordening is rechtstreeks van toepassing in alle lidstaten en hoeft niet eerst in nationaal recht te worden omgezet.

De verordening hanteert een productveiligheidslogica: AI-systemen worden gereguleerd op basis van het risico dat zij vormen voor gezondheid, veiligheid en grondrechten. Daarmee verschilt het kader fundamenteel van de AVG, die uitgaat van het grondrecht op gegevensbescherming en rechten van betrokkenen.

2.2 Risicogebaseerde benadering

De AI-verordening maakt onderscheid in vier risiconiveaus:

- **Onaanvaardbaar risico**: verboden AI-praktijken op grond van artikel 5 AI-verordening (zoals social scoring door overheden, manipulatieve technieken die schade veroorzaken en biometrische identificatie op afstand in real time door rechtshandhaving);
- **Hoog risico**: AI-systemen die vallen onder artikel 6 en bijlage III AI-verordening (onder meer toepassingen in werving en selectie, kredietverlening, toegang tot publieke diensten en uitkeringen, onderwijsbeoordeling, en bepaalde toepassingen in rechtshandhaving en migratie). Voor deze systemen gelden uitgebreide verplichtingen voor aanbieder en gebruiksverantwoordelijke;
- **Beperkt risico**: AI-systemen waarvoor transparantieverplichtingen gelden op grond van artikel 50 AI-verordening (zoals chatbots, emotieherkenning, biometrische categorisering en deepfakes);
- **Minimaal of geen risico**: overige AI-systemen, waarvoor geen specifieke verplichtingen gelden buiten de algemene bepalingen (waaronder artikel 4 over AI-geletterdheid).

In de literatuur en in toelichtingen wordt soms gesproken over drie in plaats van vier risiconiveaus, doordat *beperkt risico* en *transparantieverplichtingen* als één categorie worden behandeld en *minimaal risico* als restcategorie zonder verplichtingen buiten beschouwing wordt gelaten. Beide stellingen zijn op zichzelf niet onjuist, maar voor de praktijk hanteren wij consequent de vierdeling. Deze sluit aan op de officiële communicatie van de Europese Commissie, op de voorlichting van de Autoriteit Persoonsgegevens (AP) en op het gangbare gebruik in DPIA- en FRIA-trajecten. Daarbij is van belang dat *minimaal risico* sinds 2 februari 2025 niet langer een geheel verplichtingenvrije categorie is: artikel 4 AI-verordening (AI-geletterdheid) is van toepassing op aanbieders en gebruiksverantwoordelijken van álle AI-systemen, ongeacht het risiconiveau.

Naast deze vier risiconiveaus voor AI-systemen kent de verordening een afzonderlijk spoor voor AI-modellen voor algemene doeleinden (general purpose AI, GPAI of GenAI), geregeld in hoofdstuk V. Daarin wordt aanvullend onderscheid gemaakt tussen GPAI-modellen mét en zónder systeemrisico. Dit GPAI-regime staat naast de risicoclassificatie van AI-systemen en moet bij de beoordeling van een concrete toepassing afzonderlijk worden meegewogen wanneer een GPAI-model wordt geïntegreerd in een eigen AI-toepassing.

2.3 Rollen onder de AI-verordening

De AI-verordening kent verschillende actoren met eigen verplichtingen. De twee meest voorkomende in de praktijk zijn:

- **Aanbieder (provider)**: de partij die een AI-systeem onder eigen naam of merk ontwikkelt en in de handel brengt of in gebruik stelt;
- **Gebruiksverantwoordelijke (deployer)**: iedere natuurlijke of rechtspersoon, overheidsinstantie of ander orgaan die een AI-systeem onder eigen verantwoordelijkheid gebruikt voor professionele doeleinden. Organisaties die AI-tools inkopen en inzetten, zijn doorgaans gebruiksverantwoordelijke.

Daarnaast zijn er importeurs en distributeurs. *Onder bepaalde omstandigheden, bijvoorbeeld substantiële wijzigingen aan een hoog risico-AI-systeem of het op de markt brengen onder eigen naam, kan een* ***gebruiksverantwoordelijke alsnog als aanbieder worden aangemerkt*** *(artikel 25 AI-verordening), met de daarbij behorende, uitgebreidere verplichtingen.*

2.4 Fasering en sancties

De verordening kent een gefaseerde inwerkingtreding:

Datum	Wat gaat in
1 augustus 2024	Inwerkingtreding van de verordening (artikel 113 AI-verordening).
2 februari 2025	Verboden AI-praktijken (artikel 5) en de verplichting tot AI-geletterdheid (artikel 4) zijn van toepassing.
2 augustus 2025	Verplichtingen voor aanbieders van AI-modellen voor algemene doeleinden, de governance- en sanctiebepalingen en de aanwijzing van bevoegde nationale autoriteiten worden van toepassing.
2 augustus 2026	De kern van de verordening, onder meer de verplichtingen voor hoog risico-AI-systemen uit bijlage III, en de overige transparantieverplichtingen worden van toepassing.
2 december 2026	Watermerkverplichtingen voor AI-gegenereerde inhoud (artikel 50, lid 2) worden van toepassing.
2 augustus 2027	Verplichtingen voor AI-systemen die zijn ingebouwd in producten, die onder bestaande EU-productwetgeving vallen (bijlage I). *NB: het Digital Omnibus-akkoord beoogt deze datum te verschuiven naar 2 augustus 2028 (zie hoofdstuk 7).*

De in deze tabel genoemde data weerspiegelen de op dit moment geldende verordeningstekst. Na goedkeuring door het EP op 16 juni 2026jl. wordt deze datum - zodra de Raad formeel heeft bekrachtigd[2] - verschoven naar 2 december 2027 (zie hoofdstuk 7). Tot dat akkoord formeel is vastgesteld en in het Publicatieblad van de EU is gepubliceerd, blijven de hier genoemde data juridisch leidend.

[2] *De EP-stemming van 16 juni 2026 (423 voor, 57 tegen, 174 onthoudingen) is een cruciale stap: het EP heeft zijn definitieve goedkeuring gegeven. De Raad moet nog formeel bekrachtigen, maar dat is een technische stap.*

De sancties zijn aanzienlijk en cumuleren mogelijk met sancties onder de AVG. Op grond van artikel 99 AI-verordening kunnen boetes oplopen tot:

- €35 miljoen of 7% van de wereldwijde jaaromzet voor overtredingen van het verbod op AI-praktijken;
- €15 miljoen of 3% van de wereldwijde jaaromzet voor overige overtredingen, waaronder schendingen van de verplichtingen voor hoog risico-AI;
- €7,5 miljoen of 1% (voor MKB: 1,5%) van de wereldwijde jaaromzet bij het verstrekken van onjuiste of misleidende informatie aan toezichthouders.

Ter vergelijking: het boeteplafond onder de AVG (artikel 83 AVG) bedraagt €20 miljoen of 4% van de wereldwijde jaaromzet. Een AI-incident waarbij zowel de AI-verordening als de AVG worden geschonden, kan dus tot meerdere, gestapelde sancties leiden.

3. Impact van AI op de veilige verwerking van persoonsgegevens

AI-systemen zijn geen neutrale technologie. Het gebruik van AI raakt de kern van de AVG-beginselen en stelt nieuwe eisen aan de wijze waarop persoonsgegevens worden verwerkt, beveiligd en verantwoord.

3.1 Druk op de AVG-beginselen (artikel 5 AVG)

De beginselen van artikel 5 AVG komen in een AI-context onder bijzondere druk te staan:

- **Rechtmatigheid, behoorlijkheid en transparantie.** Generatieve AI-modellen, die op grote schaal openbare en publieke data verwerken, roepen vragen op over de grondslag voor verwerking. De European Data Protection Board (EDPB) heeft in Advies 28/2024 verduidelijkt dat gerechtvaardigd belang (artikel 6, lid 1, onder f, AVG) als grondslag kan dienen voor training en inzet, echter dat per geval een driestappentoets[3] nodig is en dat passende waarborgen en transparantie cruciaal zijn;
- **Doelbinding.** Gegevens, die voor een afgebakend doel zijn verzameld, mogen niet zonder meer worden gebruikt om een AI-model te trainen of fijn te slijpen. Vergelijkbaarheid van doelen moet worden getoetst aan artikel 6, lid 4, AVG;
- **Minimale gegevensverwerking.** AI-systemen vragen vaak om grote, breed gedefinieerde datasets. Dit staat op gespannen voet met de eis dat gegevens *'toereikend, ter zake dienend en beperkt tot wat noodzakelijk is'* moeten zijn;
- **Juistheid.** Grote taalmodellen kunnen onjuiste uitspraken doen over personen (hallucinaties). De plicht tot juistheid van gegevens en de rechten op rectificatie (artikel 16 AVG) raken hierdoor in beeld bij iedere output die over een natuurlijke persoon gaat;
- **Opslagbeperking**. Bewaartermijnen voor prompts, logs en modelartefacten verdienen expliciete vastlegging, ook bij externe AI-leveranciers;

[3] *De driestappentoets bestaat uit:*
1. *Er is daadwerkelijk sprake van een gerechtvaardigd belang (identificatie van het gerechtvaardigd belang);*
2. *De verwerking is noodzakelijk om dit belang te behartigen(de noodzakelijkheidstoets);*
3. *En er is een afweging gemaakt tussen de organisatiebelangen en die van de betrokkenen (belangenafweging).*

- **Integriteit en vertrouwelijkheid.** De inzet van cloud-gebaseerde AI-diensten brengt nieuwe beveiligingsrisico's met zich mee: ongewenste prompt-ingave, model lekkage, onbedoelde doorgifte naar derde landen en hergebruik van prompts voor modeltraining.

3.2 De anonimiteitsvraag: wanneer bevat een AI-model persoonsgegevens?

Een kernvraag voor de FG-praktijk is of een AI-model zélf persoonsgegevens ***bevat***. De EDPB heeft hierover op 17 december 2024 Advies 28/2024 vastgesteld, op verzoek van de Ierse toezichthouder. De kernpunten:

- *AI-modellen die zijn getraind met persoonsgegevens kunnen niet zonder meer als anoniem worden beschouwd.* Anonimiteit moet per geval worden beoordeeld;
- Een model kan als anoniem worden aangemerkt wanneer de kans dat persoonsgegevens direct of via gerichte queries uit het model kunnen worden geëxtraheerd, verwaarloosbaar is voor iedere betrokkene van wie de gegevens in de training van het model zijn gebruikt;
- Voor de inzetfase blijft de AVG van toepassing wanneer met het model persoonsgegevens worden verwerkt, bijvoorbeeld via prompts, outputs of in interactie met andere systemen;
- Onrechtmatige verwerking in de ontwikkelfase kan doorwerken in de rechtmatigheid van het latere gebruik van het model. Of die doorwerking zich voordoet, moet eveneens per geval worden beoordeeld.

Voor organisaties die AI inkopen, betekent dit dat de stelling *het model is anoniem, dus de AVG is niet van toepassing*, zelden zonder onderbouwing houdbaar is.

Praktijkimplicatie voor de FG-rol
Bij iedere AI-implementatie, waarbij persoonsgegevens worden verwerkt of zouden kunnen worden gereproduceerd uit een model, hoort een gedocumenteerde beoordeling van: (a) de grondslag in de ontwikkelfase, (b) de grondslag in de inzetfase, (c) een onderbouwing van eventueel beweerde anonimiteit, en (d) een beoordeling van eventuele doorwerking van onrechtmatige trainingsdata.

3.3 Bijzondere categorieën en geautomatiseerde besluitvorming

AI-systemen die worden ingezet voor profilering of besluitvorming over personen, raken aan artikel 22 AVG. Dat artikel beperkt zich -behoudens uitzonderingen- uitsluitend op geautomatiseerde verwerking gebaseerde besluiten met rechtsgevolgen of vergelijkbaar aanmerkelijke gevolgen voor de betrokkene. *Voor hoog risico-AI-systemen onder de AI-verordening is menselijk toezicht expliciet voorgeschreven (artikel 14 AI-verordening)*. Dat sluit aan op de AVG, echter vervangt deze niet.

Verwerking van bijzondere categorieën persoonsgegevens (artikel 9 AVG) blijft slechts mogelijk op basis van een van de uitzonderingsgronden uit artikel 9, lid 2, AVG. Artikel 10, lid 5, AI-verordening kent één bijzondere bepaling: aanbieders van hoog risico-AI-systemen mogen *onder strikte voorwaarden* en *uitsluitend voor het opsporen en corrigeren van bias* bijzondere categorieën persoonsgegevens verwerken. Deze bepaling vormt géén vrijbrief; zij voorziet in passende waarborgen waaronder pseudonimisering en beperkte toegang.

3.4 Verwerkers, ketens en internationale doorgifte

De meeste organisaties zetten geen eigen AI-modellen in, maar maken gebruik van diensten van externe leveranciers (bijvoorbeeld Microsoft, OpenAI, Google, Amazon, Anthropic en hun resellers). Dit roept onder de AVG onverminderd vraagstukken op rond:

- De verwerkersovereenkomst (artikel 28 AVG), inclusief afspraken over sub-verwerkers, retentie van prompts en logs en het uitsluiten van hergebruik voor modeltraining;
- Doorgifte naar landen buiten de EER (hoofdstuk V AVG), waarbij het EU-VS Data Privacy Framework, Standard Contractual Clauses en aanvullende waarborgen aandacht vragen;
- De positie van de leverancier onder de AI-verordening: leveranciers zijn doorgaans ***aanbieder*** van het AI-systeem en moeten technische documentatie en gebruiksinstructies leveren (artikelen 11 en 13 AI-verordening) die de gebruiksverantwoordelijke nodig heeft om zelf aan de verordening en aan de AVG te voldoen.

3.5 Transparantie en informatieplicht

Transparantie is in beide kaders een terugkerend thema, maar met verschillende invalshoeken:

- Onder de AVG gelden de informatieplichten van de artikelen 13 en 14 ten aanzien van de betrokkene wiens persoonsgegevens worden verwerkt;
- Onder de AI-verordening verplicht artikel 50 dat gebruikers worden geïnformeerd wanneer zij interacteren met een AI-systeem (zoals een chatbot), dat AI-gegenereerde content als zodanig herkenbaar is en dat deepfakes worden gemarkeerd;
- Artikel 26, lid 11, AI-verordening verplicht gebruiksverantwoordelijken van hoog risico-AI bovendien om natuurlijke personen te informeren wanneer zij worden onderworpen aan een dergelijk systeem.

Voor de praktijk betekent dit dat privacyverklaringen, gebruiksvoorwaarden en interfaces in samenhang moeten worden ingericht: een AVG-informatieplicht en een AI-transparantieverplichting kunnen elkaar overlappen, ze dekken echter niet altijd hetzelfde af.

Let op:
de *transparantieverplichtingen van artikel 50*, m.u.v. de watermerkverplichting, treden in werking op ***2 augustus 2026***! De watermerkverplichting verschuift naar 2 december 2026.

4. De verhouding tussen de AI-verordening en de AVG

4.1 Twee verschillende uitgangspunten

De AI-verordening en de AVG hebben een verschillende grondslag en een verschillend perspectief. De AVG is een grondrechtenverordening: zij beschermt het in artikel 8 van het Handvest van de grondrechten van de EU vastgelegde recht op de bescherming van persoonsgegevens. Zij richt zich op de gehele verwerkingscyclus en geeft betrokkenen rechten.

De AI-verordening is in de kern een productverordening. Zij stelt eisen aan AI-systemen als product en aan de actoren in de waardeketen, vergelijkbaar met productveiligheidswetgeving die ook geldt voor liften, speelgoed of medische hulpmiddelen. Zij verleent in beginsel geen individuele rechten aan natuurlijke personen, met uitzondering van bepaalde transparantieverplichtingen en het klachtrecht uit artikel 85 AI-verordening.

4.2 De "without prejudice"-clausule (artikel 2, lid 7, AI-verordening)

De verhouding is uitdrukkelijk geregeld. Artikel 2, lid 7, AI-verordening bepaalt dat de verordening de Uniewetgeving inzake de bescherming van persoonsgegevens en privacy (uitdrukkelijk genoemd worden de AVG, Verordening (EU) 2018/1725, Richtlijn 2002/58/EG (e-Privacy) en de Richtlijn gegevensbescherming opsporing en vervolging (EU) 2016/680) onverlet laat. De AVG blijft dus *integraal van toepassing op iedere verwerking van persoonsgegevens, óók binnen een AI-context.*

Dit betekent dat de AI-verordening geen lex specialis is ten opzichte van de AVG. Beide kaders gelden naast elkaar. Waar zich overlap voordoet, geldt het strengste regime. Bij twijfel over een grondslag voor de verwerking van persoonsgegevens biedt de AI-verordening op zichzelf géén legitimatie; daarvoor blijft de AVG bepalend.

Kerngedachte
De AI-verordening regelt of een AI-systeem op de markt mag, in welke vorm en onder welke productvereisten. De AVG regelt of en hoe persoonsgegevens in en rond dat systeem mogen worden verwerkt. Beide vragen moeten afzonderlijk worden beantwoord; positieve naleving van het ene kader bevrijdt niet van het andere.

4.3 Complementaire en overlappende verplichtingen

Op tal van plaatsen verwijst de AI-verordening uitdrukkelijk naar de AVG of bouwt zij erop voort. Een aantal voorbeelden:

Onderwerp	AVG	AI-verordening
Effectbeoordeling	DPIA - artikel 35	FRIA - artikel 27 (voor bepaalde gebruiksverantwoordelijken van hoog risico-AI)
Transparantie	Artikelen 12-14 (informatieplicht)	Artikel 50 (transparantie naar gebruiker) en artikel 26, lid 11 (informatie aan betrokken personen)
Menselijk toezicht	Artikel 22 (geautomatiseerde besluitvorming)	Artikel 14 (menselijke betrokkenheid bij hoog risico-AI)
Bijzondere persoonsgegevens	Artikel 9	Artikel10, lid 5 (uitsluitend voor bias-detectie en -correctie, met aanvullende waarborgen)
Documentatie en verantwoording	Artikel 5, lid 2 en artikel 30 (register van verwerkingen)	Artikelen 11 en 18 (technische documentatie en logging)
Toezichthouder	AVG-toezichthouders (in Nederland: AP)	Markttoezichtautoriteiten; de AP wordt in Nederland een centrale rol toebedeeld (zie hoofdstuk 6)

Artikel 26, lid 9, AI-verordening verplicht gebruiksverantwoordelijken van hoog risico-AI bovendien om de door de aanbieder verstrekte informatie (op grond van artikel 13) te benutten bij de DPIA onder artikel 35 AVG. De DPIA en de FRIA kunnen daarom in één gecombineerd traject worden uitgevoerd, mits beide kaders volledig en aantoonbaar zijn afgedekt.

4.4 DPIA en FRIA: complementair, niet uitwisselbaar

De DPIA [artikel 35 AVG] en de grondrechteneffectbeoordeling, de Fundamental Rights Impact Assessment (FRIA) [artikel 27 AI-verordening] lijken op elkaar, maar hebben een verschillende reikwijdte.

De DPIA is verplicht wanneer een verwerking waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Zij richt zich primair op risico's voor persoonsgegevens en privacy. De FRIA is verplicht voor een specifieke groep gebruiksverantwoordelijken van hoog risico-AI-systemen uit bijlage III, te weten:

- Publiekrechtelijke organen;
- Particuliere entiteiten die openbare diensten verlenen;
- Alle gebruiksverantwoordelijken van AI-systemen die worden ingezet voor kredietwaardigheidsbeoordeling of voor risicobeoordeling en prijsstelling bij levens- en ziektekostenverzekeringen.

De FRIA bestrijkt het volledige spectrum van grondrechten uit het Handvest, naast gegevensbescherming ook bijvoorbeeld non-discriminatie, het recht op een eerlijk proces en het recht op effectieve rechtsbescherming. Zij omvat ten minste een beschrijving van het gebruik, de betrokken personen, de specifieke risico's op schade, de getroffen menselijke toezichtmaatregelen en de procedures bij intreden van risico's, inclusief klachtmechanismen. Artikel 27, lid 4, AI-verordening bepaalt expliciet dat de FRIA de DPIA op het terrein van grondrechten aanvult.

In Nederland kan aan de FRIA-verplichting praktisch invulling worden gegeven met het Impact Assessment Mensenrechten en Algoritmes (IAMA). Het IAMA is een Nederlands methodisch instrument dat sinds februari 2026 *uitdrukkelijk* in lijn is gebracht met artikel 27 AI-verordening. De inhoudelijke bespreking én het advies om ***de IAMA breder in te zetten dan strikt verplicht***, zijn opgenomen in paragraaf 5.4 van dit whitepaper.

4.5 Verschillende rollen, deels parallel

De AVG kent verwerkingsverantwoordelijke en verwerker. De AI-verordening kent aanbieder, gebruiksverantwoordelijke, importeur en distributeur. Deze rollen lopen niet één-op-één parallel, staan echter vaak wel in een logische verhouding tot elkaar:

- Een externe AI-leverancier is doorgaans aanbieder *onder de AI-verordening én verwerker onder de AVG;*
- Een organisatie, die een AI-systeem inkoopt en gebruikt voor eigen processen, is doorgaans *gebruiksverantwoordelijke onder de AI-verordening én verwerkingsverantwoordelijke onder de AVG*;
- Wanneer beide partijen daadwerkelijk gezamenlijk doel en middelen bepalen, kan een gezamenlijke verwerkingsverantwoordelijkheid (artikel 26 AVG) ontstaan.

Voor de praktijk is het verstandig de rolverdeling per kader expliciet vast te leggen, zowel in interne documentatie als in contracten met leveranciers.

5. Praktische implicaties voor organisaties

De gelaagde toepassing van de AI-verordening en de AVG vraagt om een gestructureerde aanpak. Onderstaande zeven elementen vormen de minimaal noodzakelijke basis.

5.1 AI-geletterdheid (artikel 4 AI-verordening) - al van toepassing

Sinds 2 februari 2025 zijn aanbieders en gebruiksverantwoordelijken *verplicht* ervoor te zorgen dat hun personeel en de personen, die namens hen AI-systemen gebruiken, een toereikend niveau van AI-geletterdheid hebben. De verplichting geldt voor ***alle*** AI-systemen, ongeacht het risiconiveau en is breder dan zuiver technische scholing: zij omvat het begrijpen van kansen, risico's en juridische context, afgestemd op de rol en de toepassing.

Voor opdrachtgevers van Parell BV betekent dit concreet: een vastgesteld en gedocumenteerd opleidingsprogramma, gericht op de relevante doelgroepen en met passende registratie.

5.2 Inventarisatie en risicoclassificatie

Een actueel overzicht van ingezette en voorgenomen AI-systemen is een randvoorwaarde voor compliance. Dit overzicht bevat per systeem ten minste: doelstelling, leverancier, betrokken gegevensstromen, risicoclassificatie onder de AI-verordening (verboden, hoog, beperkt of minimaal) en de positie van de organisatie (aanbieder, gebruiksverantwoordelijke of beide).

5.3 DPIA en FRIA in één geïntegreerd traject

Waar zowel DPIA als FRIA verplicht zijn, is een geïntegreerd traject doelmatig. Beide instrumenten moeten echter inhoudelijk volledig zijn afgedekt; de FRIA mag de DPIA niet vervangen. De informatieverstrekking door de aanbieder (artikelen 13 en 11 AI-verordening) moet expliciet in het assessment worden verwerkt.

5.4 IAMA: aanbevolen breed beoordelingskader

Naast de DPIA en de FRIA bestaat in Nederland het ***Impact Assessment Mensenrechten en Algoritmes (IAMA)***; ontwikkeld door Universiteit Utrecht in opdracht van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Het IAMA is breder dan de FRIA: het is toepasbaar op zowel AI-systemen als andere algoritmes en het bestrijkt het volledige spectrum van mensenrechten.
In februari 2026 is het IAMA geactualiseerd, verkort en *uitdrukkelijk in lijn gebracht met artikel 27 AI-verordening*: vragen, die rechtstreeks samenhangen met de FRIA-verplichting, zijn in de nieuwe versie afzonderlijk gemarkeerd. Het IAMA kan daarmee worden gebruikt om -voor zover van toepassing- invulling te geven aan de FRIA-verplichting.

Het IAMA is binnen de Rijksoverheid in feite het primaire instrument: op grond van een aangenomen motie van de Tweede Kamer (maart 2022) is gebruik van het IAMA voorgeschreven wanneer algoritmes worden ingezet om beslissingen over mensen te maken. Voor private organisaties geldt deze verplichting niet. Het IAMA wordt echter ook buiten de overheid breed als best practice toegepast.

Dringend advies:

Formeel-juridisch is de FRIA, en daarmee een IAMA als invulling daarvan, ***alleen verplicht bij hoog risico-AI-systemen*** *en, binnen die categorie, alleen voor de in artikel 27 AI-verordening aangewezen gebruiksverantwoordelijken. Vanuit mijn praktijk als FG en CAICO adviseer ik organisaties die de eerste stappen zetten met AI echter om* ***standaard****, dus ook bij ogenschijnlijk niet-hoog risico-systemen,* ***ten minste een verkorte IAMA uit te voeren****. De achtergrond van dit advies is dat de risicoclassificatie onder de AI-verordening niet alleen wordt bepaald door het AI-systeem als zodanig, echter in belangrijke mate ook door de context en het beoogde doel waarvoor het wordt ingezet. Een generiek AI-systeem dat op zichzelf geen hoog risicotoepassing is, kan* ***door inbedding in een specifiek bedrijfsproces*** *(bijvoorbeeld werving en selectie, prestatiebeoordeling van werknemers, kredietverlening of toegang tot voorzieningen)* ***alsnog kwalificeren als hoog risico*** *onder bijlage III AI-verordening, met alle bijbehorende verplichtingen. Een vroegtijdige IAMA helpt om deze drempel tijdig in beeld te brengen en voorkomt dat een organisatie achteraf moet vaststellen dat de toepassing in een zwaarder regime valt dan aanvankelijk gedacht.*

Een aanvullend voordeel is dat een IAMA, door zijn dialogische karakter, bijdraagt aan interne bewustwording, eigenaarschap en governance. Voor organisaties, die de AI-volwassenheid van hun teams en processen nog opbouwen, is dat een waardevolle uitkomst op zichzelf, los van de juridische verplichting.

5.5 Transparantie en interface-ontwerp

Transparantieverplichtingen onder beide kaders moeten worden vertaald naar concrete teksten en interfaces: privacyverklaring, voorwaarden bij chatbots en virtuele assistenten, watermerken op AI-gegenereerde content en informatie aan personen die met of door een hoog risico-AI-systeem worden beoordeeld.

5.6 Contracten met leveranciers

Verwerkersovereenkomsten, AI-specifieke addenda en DVO's/SLA's[4] verdienen actualisering, in het bijzonder op de volgende punten:

- Uitsluiting van gebruik van prompts en outputs voor modeltraining, tenzij dit uitdrukkelijk is overeengekomen;
- Vastleggen retentietermijnen voor prompts, logs en modelartefacten;
- Expliciete beschikbaarstelling van de in artikelen 11 en 13 AI-verordening genoemde documentatie en gebruiksaanwijzingen;
- Regelingen voor incidenten en datalekken, die zowel onder artikel 33-34 AVG als artikel 73 AI-verordening (ernstige incidenten) vallen;
- Aansprakelijkheid en -bij voorkeur- een carve-out voor bestuurlijke boetes en schade uit hoofde van schending van de verwerkersovereenkomst.

[4] *DVO: dienstverleningsovereenkomst; SLA: Service Level Agreement.*

5.7 Documentatie, logging en monitoring

De AI-verordening kent een sterke verantwoordingscomponent. Voor hoog risico-AI-systemen schrijven de artikelen 12 en 19 logging-verplichtingen voor aanbieders voor; artikel 26, lid 6, AI-verordening verplicht gebruiksverantwoordelijken om logbestanden, die onder hun controle vallen, ten minste zes maanden te bewaren, tenzij specifiek Unierecht of nationaal recht anders bepaalt. Voor overheidsinstanties geldt aanvullend de registratieplicht in de EU-databank voor hoog risico-AI (artikel 71 AI-verordening). Eén en ander komt boven op het register van verwerkingen onder artikel 30 AVG.

6. Toezicht in Nederland

Nederland kiest in beginsel voor een sectoraal model: bestaande toezichthouders houden binnen hun eigen domein toezicht op AI en werken samen waar systemen meerdere domeinen raken. De Autoriteit Persoonsgegevens (AP) is sinds 2023 coördinerend toezichthouder op algoritmes en AI en regisseur van de Algoritme- en AI-kamer (AAK).

Op 20 april 2026 is het wetsvoorstel Uitvoeringswet AI-verordening in internetconsultatie gebracht. Het voorstel stond van 20 april tot en met 1 juni 2026 open voor internetconsultatie. Na sluiting bekijken de ministeries alle reacties en passen zij het wetsvoorstel waar nodig aan, waarna een verslag met uitkomsten volgt. Onder meer de AFM en de Nederlandse Orde van Advocaten hebben een consultatiereactie ingediend.

De AFM heeft een uitvoeringstoets ingediend en oordeelt dat het wetsvoorstel in de basis uitvoerbaar is, maar dat gerichte aanpassingen nodig zijn, met name voldoende capaciteit, heldere bevoegdheden en een duidelijke taakverdeling, in het bijzonder tussen de AFM en DNB.

Het voorstel bevat onder meer:

- De aanwijzing van tien organisaties als markttoezichtautoriteit, aansluitend op bestaande sectorale toezichthouders (waaronder DNB, AFM, NVWA, IGJ en de Nederlandse Arbeidsinspectie);
- De AP als coördinerend toezichthouder en 'vangnet' voor gebieden zonder duidelijke sectorale toezichthouder, met een afzonderlijke AI-bestuurder;
- De AP en de Rijksinspectie Digitale Infrastructuur (RDI) in een centrale en coördinerende rol.

Daarnaast richten AP en RDI vanaf 2026 een AI regulatory sandbox in waar organisaties hun AI-systemen onder begeleiding van toezichthouders kunnen toetsen.

Cumulatief toezicht en cumulatieve sancties

Eén AI-incident kan tegelijk een AVG-overtreding en een AI-verordening overtreding zijn. Toezichthouders zijn gehouden om samen te werken en bevoegdheden af te stemmen, maar sancties kunnen daadwerkelijk cumuleren. Voor opdrachtgevers betekent dit dat zowel het in lijn werken met de AVG- als de AI-verordening aantoonbaar moet zijn op het moment dat een incident zich voordoet.

Tot slot één belangrijk punt: het kabinet erkent zelf dat de nationale uitvoeringswet *mogelijk niet gereed zal zijn vóór de inwerkingtreding van de verordening* in augustus 2026, echter benadrukt dat dit de rechtstreekse werking van de AI-verordening onverlet laat, verplichtingen voor aanbieders en gebruiksverantwoordelijken gelden ook zonder uitvoeringswet.

7. De Digital Omnibus: een dossier in beweging

Op 19 november 2025 heeft de Europese Commissie het zogenoemde Digital Omnibus-pakket gepresenteerd. Het pakket bestaat uit twee samenhangende voorstellen: een digitale omnibusverordening die onder meer de AVG, de Data Act, de e-Privacyrichtlijn, de NIS2-richtlijn en de eIDAS-verordening raakt en een afzonderlijke omnibusverordening voor de AI-verordening. Het pakket maakt onderdeel uit van de bredere Commissie-inzet om Europese digitale wetgeving te vereenvoudigen en de regeldruk voor ondernemingen te verlichten.

Het Digital Omnibus-pakket is op dit moment geen *geldend recht*; het bevindt zich in de gewone wetgevingsprocedure.
Voor het AI-deel heeft het Comité van Permanente Vertegenwoordigers van de lidstaten bij de Europese Unie (Coreper[5]) op 13 mei 2026 het op 7 mei 2026 bereikte voorlopige politieke akkoord tussen Raad en Europees Parlement (EP) bevestigd. Het akkoord vereist nog formele bekrachtiging door beide medewetgevers voordat het in het Publicatieblad kan worden gepubliceerd.
Het AVG-deel bevindt zich nog in onderhandeling. Het pakket wordt daarom in dit whitepaper bewust afzonderlijk behandeld: het is van direct strategisch belang, wijzigt echter het in voorgaande hoofdstukken geschetste juridische kader nog *niet*.

7.1 Belangrijkste voorgestelde wijzigingen op hoofdlijnen

Voor de AVG zijn onder meer de volgende voorstellen relevant:

- **Begrip persoonsgegevens.** De Digitale Omnibus legt vast dat per ontvanger kan verschillen of bepaalde informatie als persoonsgegeven moet worden gezien. Bepalend is of díe partij redelijkerwijs over de middelen beschikt om de persoon achter de gegevens te achterhalen. Dezelfde dataset kan dus voor de ene organisatie wél persoonsgegevens bevatten en voor een andere niet, bijvoorbeeld wanneer alleen de eerste over de sleutel beschikt om gepseudonimiseerde gegevens te herleiden tot personen. Deze benadering sluit aan bij de rechtspraak van het Hof van Justitie van de EU, onder meer in de zaak van de Single Resolution Board (SRB);
- **Gerechtvaardigd belang en AI-training.** De Digitale Omnibus wil expliciete erkenning van gerechtvaardigd belang (artikel 6, lid 1, onder f, AVG) als grondslag voor het trainen en inzetten van AI-systemen, *onder voorwaarden en mét waarborgen*.
- **Bijzondere categorieën in trainingsdata.** De Digitale Omnibus wil een beperkte uitzondering voor situaties waarin bijzondere categorieën persoonsgegevens onbedoeld in trainingsdatasets terechtkomen en verwijdering onevenredige inspanning zou vergen, *mits passende waarborgen worden getroffen*.
- **Meldplicht datalekken.** Een voorstel om de *meldplicht bij datalekken* te beperken tot incidenten met een *waarschijnlijk hoog risico* voor betrokkenen, en de meldtermijn te verlengen van 72 naar 96 uur, met een centraal Europees meldloket.

[5] Coreper: Comité des Représentants Permanents

Voor de AI-verordening worden onder meer wijzigingen voorgesteld in de verplichting tot AI-geletterdheid (artikel 4), die in de huidige Commissietekst meer als stimuleringsverplichting voor de Commissie en lidstaten wordt geformuleerd en, het meest in het oog springend, een uitstel van de toepassingsdata voor hoog risico-AI.

Op 7 mei 2026 hebben de Raad en het Europees Parlement een voorlopig politiek akkoord bereikt over de Omnibus AI. Daarin worden de toepassingsdata voor hoog risico-AI als volgt verschoven:

- ***Stand-alone hoog risico systemen uit bijlage III*** (zoals werving en selectie, kredietbeoordeling, onderwijs en rechtshandhaving): van *2 augustus 2026* naar *2 december 2027*, een uitstel van ruim zestien maanden;
- ***Hoog risico-AI ingebouwd in gereguleerde producten uit bijlage I*** (zoals medische hulpmiddelen, machines en voertuigen): van *2 augustus 2027* naar *2 augustus 2028*.

Daarnaast verschuift de termijn waarbinnen lidstaten ten minste één nationale AI regulatory sandbox moeten inrichten naar 2 augustus 2027 en gaan de transparantie- en watermerkverplichtingen voor al op de markt zijnde systemen (artikel 50, lid 2) over naar 2 december 2026. De overige transparantieverplichtingen blijven van toepassing vanaf 2 augustus 2026.

De definitief aangenomen tekst door het EP op 16 juni jl. brengt o.a. de volgende aanpassingen met zich mee:

- *Verbod op nudifier-apps en CSAM*. De definitief aangenomen tekst verbiedt AI-systemen die materiaal van seksueel misbruik van kinderen (CSAM) genereren, of die afbeeldingen, video's en audio maken die de intieme delen of seksueel expliciete activiteiten van een identificeerbare persoon weergeven zonder diens toestemming. Aanbieders mogen deze systemen niet in de EU in de handel brengen tenzij zij over passende technische waarborgen beschikken. Bedrijven hebben tot ***2 december 2026*** de tijd om hun systemen in lijn te brengen;
- De definitie '*veiligheidscomponent*' is aangescherpt. De definitief aangenomen tekst verduidelijkt wat als een 'veiligheidscomponent' kan worden aangemerkt: producten met AI-functies die alleen gebruikers helpen of prestaties optimaliseren, vallen niet automatisch onder hoog-risico-verplichtingen *als het falen ervan geen gezondheids- of veiligheidsrisico's meebrengt;*
- *Uitbreiding vrijstelling voor klein en middelgrote ondernemingen (kmo) naar kleine midcap.* Vrijstellingen voor kmo's van bepaalde regels worden uitgebreid tot kleine midcap-ondernemingen;
- Gestroomlijnde handhaving GPAI binnen het AI-bureau. De handhaving van bepaalde AI-systemen voor algemene doeleinden wordt gestroomlijnd binnen het AI-bureau van de EU;
- Bias-detectie is ook van toepassing voor niet-hoog-risico AI. De mogelijkheid om persoonsgegevens te verwerken voor bias-opsporing en -correctie met passende waarborgen geldt nu ook voor AI-systemen zonder hoog risico, niet enkel voor hoog-risico-systemen zoals artikel 10 lid 5 AI-verordening nu bepaalt.

Het is van belang te benadrukken dat dit *door het EP is goedgekeurd*; het wachten is nu nog op bekrachtiging door de Raad. De wijzigingen krijgen pas juridische werking na formele vaststelling door beide medewetgevers en publicatie in het Publicatieblad van de EU, naar verwachting vóór 2 augustus 2026. Tot dat moment blijft 2 augustus 2026 formeel de geldende toepassingsdatum voor hoog risico-AI en blijft dit dus een actieve nalevingsdatum

> *De Europese Commissie en toezichthouders benadrukken dat organisaties hun voorbereidingen niet mogen uitstellen: het uitstel is bedoeld om voldoende tijd te bieden voor de benodigde standaarden en compliance-instrumenten, niet als aanleiding om de implementatie stil te leggen.*

7.2 Positie van de Autoriteit Persoonsgegevens

De AP heeft direct na publicatie kritisch gereageerd en haar standpunt later uitgewerkt in een position paper over Omnibus Digitaal en Omnibus AI. De kernboodschap is dat vereenvoudiging niet ten koste mag gaan van mensenrechten, rechtszekerheid en effectief toezicht. De AP onderschrijft dat de Commissie de gevolgen van het voorstel onvoldoende heeft onderzocht.

De voornaamste zorgen van de AP betreffen:

- De voorgestelde wijziging van het begrip persoonsgegevens: de AP pleit voor behoud van de huidige definitie, omdat onduidelijkheid zowel bescherming als toezicht verzwakt;
- Voorgestelde versoepelingen van transparantie- en verantwoordingsverplichtingen, die volgens de AP het toezicht ondermijnen;
- De verschuiving van de verantwoordelijkheid voor AI-geletterdheid van organisaties naar overheden: organisaties moeten zelf verantwoordelijk blijven voor de kennis en vaardigheden van hun medewerkers;
- De algemene onduidelijkheid van een aantal voorgestelde bepalingen, die volgens de AP de gesignaleerde problemen niet oplossen.

De AP signaleert ook positieve elementen, met name daar waar het pakket toezicht versterkt of definities op Europees niveau uniformeert.

7.3 Positie van het Nederlandse kabinet

Het kabinet heeft zijn standpunt vastgelegd in het BNC-fiche van 12 december 2025. De hoofdlijn is gemengd: het kabinet verwelkomt de Commissie-inzet om digitale wetgeving te vereenvoudigen en de regeldruk te verminderen, omdat dat aansluit bij de eigen doelstellingen. Tegelijk plaatst het kabinet 'grote zorgen' bij de voorgestelde fundamentele wijzigingen in de AVG. De Eerste Kamer heeft op 24 februari 2026 ingestemd met het plaatsen van een parlementair behandelvoorbehoud, mede vanwege de impact op grondrechten. Dit behandelvoorbehoud is op 24 maart 2026 weer opgeheven.

Het College voor de Rechten van de Mens heeft het voorstel betiteld als een 'zorgwekkende afzwakking' van de bescherming van grondrechten, in het bijzonder het recht op gegevensbescherming en non-discriminatie. Het College is sinds 2024 in Nederland aangewezen als toezichthouder op grondrechten bij AI-systemen.

Wat betekent dit voor uw organisatie?
Het Digital Omnibus-pakket wijzigt het geldende recht (nog) niet. Tot het pakket is aangenomen en gepubliceerd, blijven de AVG en de AI-verordening onverkort van toepassing in hun huidige vorm. Het is niet verstandig om DPIA's, FRIA's, beleid of contracten nu reeds aan te passen aan voorgestelde tekst die nog kan wijzigen of sneuvelen. Wel is het verstandig om het dossier actief te volgen en het ontwerp van uw compliancehuis zo in te richten dat het flexibel is voor toekomstige wijzigingen, bijvoorbeeld door grondslagkeuzes en bewaartermijnen modulair vast te leggen.

8. Aanbevelingen

Op basis van het voorgaande adviseer ik organisaties die AI inzetten of overwegen om in 2026 ten minste de volgende stappen te zetten:

Nr.	Aanbeveling
1	Stel een actueel AI-register op met risicoclassificatie en rolaanduiding per systeem.
2	Implementeer en documenteer een AI-geletterdheidsprogramma op grond van artikel 4 AI-verordening.
3	Combineer DPIA en -waar verplicht- FRIA in één assessment, waarin de informatie uit artikelen 11 en 13 AI-verordening wordt verwerkt.
4	Overweeg, zeker bij de eerste stappen met AI, om standaard ook bij ogenschijnlijk niet-hoog risico-systemen een (verkorte) IAMA uit te voeren; de inzet in een specifiek proces kan een systeem alsnog tot hoog risico maken.
5	Actualiseer verwerkersovereenkomsten en AI-addenda: hergebruik voor modeltraining, retentie, sub-verwerkers, doorgifte, aansprakelijkheid.
6	Beleg menselijk toezicht aantoonbaar in het werkproces; documenteer rollen, bevoegdheden en escalatieroutes.
7	Vertaal transparantieverplichtingen (AVG én AI-verordening) naar privacyverklaring, gebruikersinterfaces en interne werkinstructies.
8	Richt incident- en datalekprocedures zo in dat zij zowel artikel 33-34 AVG als artikel 73 AI-verordening (ernstige incidenten) afdekken.
9	Plan een periodieke herijking: AI-systemen, modellen en hun gebruiksdoelen veranderen, en daarmee de juridische beoordeling.
10	Volg het Digital Omnibus-dossier actief en richt beleid, DPIA's en contracten modulair in, zodat aanpassing aan toekomstige wijzigingen in AVG en AI-verordening met beperkte inspanning mogelijk is.

9. Tot slot

De inzet van AI is geen voorbijgaande ontwikkeling en de AI-verordening is een blijvend kader naast de AVG. Voor organisaties betekent dit een dubbele opgave: bestaande AVG-praktijken moeten worden doorontwikkeld en tegelijk moet een nieuw, productgericht compliancekader worden ingebed in inkoop, projectmanagement en bestuurlijke besluitvorming.

Het samenspel van AVG en AI-verordening vraagt om begeleiding die beide kaders in samenhang behandelt: van inventarisatie en risicoclassificatie tot DPIA, FRIA, contractuele afspraken en governance op bestuursniveau. Parell BV biedt die begeleiding vanuit de gecombineerde expertise van Functionaris Gegevensbescherming (FG) en Certified AI Compliance Officer (CAICO).

Over Parell

Ons motto is "Leuke dingen doen met leuke mensen met een maatschappelijke relevantie" en dit beschrijft ook precies wie wij zijn. Parell is een club van professionals met hart voor de publieke zaak. We houden ons bezig met uiteenlopende onderwerpen, zoals organisatieontwikkeling, cybersecurity, datagedreven werken, pentesten en AI en dit doen we vooral in de zorg, het onderwijs, de overheid en semi-overheid.
We stellen de mens centraal, niet het systeem. We luisteren, stellen prikkelende vragen en sluiten aan bij wat er al in jouw organisatie aanwezig is. Zo maken we verandering duurzaam.

Over de auteur

Erik Steijn is een ervaren, mensgerichte FG/DPO en CAICO die op het snijvlak van privacy, security en verantwoord datagebruik opereert, met een duidelijke focus op overheid en zorg.
Hij combineert zijn juridische privacy-expertise met praktijkervaring, waar hij organisaties helpt om AVG- en AI-compliance duurzaam te verankeren in bestuur, processen en gedrag.

Vragen of behoefte aan ondersteuning?

Heeft u naar aanleiding van dit whitepaper vragen, of wilt u sparren over de toepassing in uw eigen organisatie? Neem dan gerust contact op met Parell BV of rechtstreeks met mij. Wij denken graag mee, zowel op strategisch niveau als bij de concrete inrichting van DPIA- en FRIA-trajecten, contracten, beleid en werkinstructies.
Erik Steijn - FG / CAICO

Contact
Velperweg 28A
6824 BJ Arnhem
085 4011 274
info@parell.nl

Bijlage: geraadpleegde bronnen

Onderstaande bronnen zijn gebruikt bij het opstellen van dit whitepaper. Verwijzingen zijn waar relevant gemarkeerd met het bijbehorende artikelnummer in de tekst.

Wet- en regelgeving

- Verordening (EU) 2024/1689 van het Europees Parlement en de Raad van 13 juni 2024 tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie (AI-verordening), PB L, 2024/1689, 12 juli 2024;
- Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 (Algemene Verordening Gegevensbescherming, AVG);
- Uitvoeringswet AI-verordening, internetconsultatie 20 april 2026 - 1 juni 2026 (Rijksoverheid).

Toezichthouders en EU-organen

- European Data Protection Board, Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models, vastgesteld 17 december 2024;
- European Data Protection Board, Statement on the role of Data Protection Authorities in the AI Act framework, 16 juli 2024;
- Autoriteit Persoonsgegevens, Toezicht op AI en algoritmes — visiedocument en publicaties op autoriteitpersoonsgegevens.nl;
- Autoriteit Persoonsgegevens, Bericht "Toezicht op AI wordt concreet: sleutelrol voor de AP en de RDI", april 2026;
- Europese Commissie, AI Act - overzicht en implementatietijdlijn, digital-strategy.ec.europa.eu.
- Europees Parlement, persbericht 16 juni 2026, AI-wet: EP keurt vereenvoudigingsmaatregelen en verbod op "nudifier"-app goed;
- Persbericht Europees Parlement; aangenomen teksten EP, 16 juni 2026 (plenaire vergadering);
- AFM, Uitvoeringstoets Verordening Artificiële Intelligentie, 12 juni 2026;
- Nederlandse Orde van Advocaten, Advies Uitvoeringswet AI-verordening, 1 juni 2026.

Jurisprudentie

- Hof van Justitie van de EU, arrest van 4 september 2025, zaak C-413/23 P (EDPS / GAR) (EDPS t. SRB), ECLI:EU:C:2025:571.

Dit whitepaper is opgesteld met zorg op basis van openbare bronnen en de geldende wet- en regelgeving op het moment van opstellen. Hij vormt geen juridisch advies in een concrete casus. Voor een op uw situatie toegesneden advies is een afzonderlijke consultatie met de FG en/of een AI-compliancespecialist de aangewezen route.