
Implementatie- document AI-verordening



Leeswijzer / Inleiding

Het Europees Parlement keurde in december 2023 de AI-Verordening goed. Deze trad op 1 augustus 2024 in werking. De verordening richt zich op het reguleren van AI-systemen binnen de Europese Unie. Het doel is om potentiële risico's voor de gezondheid, veiligheid en grondrechten van burgers zo veel mogelijk te minimaliseren. De AI-Verordening is opgesteld volgens een risicogebaseerde benadering. Dit betekent dat AI-systemen worden ingedeeld op basis van het risico dat zij kunnen vormen voor individuen en de samenleving. Afhankelijk van het risiconiveau gelden specifieke verplichtingen en vereisten voor ontwikkelaars, aanbieders en gebruikers van AI-systemen.

De verplichtingen uit de verordening treden niet allemaal tegelijk in werking, maar worden gefaseerd ingevoerd. De eerste verplichtingen gingen in februari 2025 in. Dit betreft het verbod op het gebruik van verboden AI-systemen en de verplichting om actief te investeren in AI-geletterdheid. In augustus 2025 start het toezicht op de eisen voor AI voor algemeen gebruik. Een jaar later – in 2026 – houdt de toezichthouder toezicht op hoogrisico-AI-systemen en de transparantieplichting. Tot slot treedt de AI-Verordening in augustus 2027 volledig in werking. In 2030 komt er een einde aan het verlengde overgangsregime voor bestaande AI bij overheidsorganisaties.

De implementatie van de AI-Verordening brengt voor de waterschappen veel werk mee. Om meer duidelijkheid rondom de AI-Verordening te scheppen, licht deze handreiking verschillende aspecten van de verordening uit.

Dit document is samengesteld door de Unie van Waterschappen, in samenwerking met de waterschappen en het Waterschapshuis. Het heeft als doel om de waterschappen inzicht te geven in de verplichtingen die voortvloeien uit de AI-Verordening, wat deze voor hen betekenen en hoe zij hieraan kunnen voldoen. Elk hoofdstuk beschrijft (een deel van) de verplichtingen en geeft daarbij een toelichting.

Geschreven door:

Waterschappen:

Juliëtte Pelamonia (Vallei en Veluwe)
Janny Planting (Fryslan)
Marchien Brandsma (Noorderzijlvest)
Thijs Cuppen (Limburg)
Sophie Chaouat (Rijnland)
Monique van Gruisen-Deckers (Rivierenland)
Sam Baartmans (Delfland)
Maxime Visser (Delfland)
Ramon Snippe (Drents Overijsselse Delta)
Leonie Smit (Noorderzijlvest)
Hilde Klok (Hunze en Aa's)
Esther van Laarhoven (Aa en Maas)
Eddie Jacobs (Brabantse Delta)
Bas Slaats (Schieland en Krimpenerwaard)
Heidi Eijsberg (Scheldestromen)
Ronald Groeneweg (Waternet)

Unie van Waterschappen:

Medina Gasjimova
Lise Adriaensen
Lazora Bernardus

Het Waterschapshuis:

Katja van Beem
Besime Aydin

Begrippenlijst

AI-systeem: door mensen ontworpen technologieën die autonoom en zelfstandig inputgegevens verwerken en beslissingen of voorspellingen genereren, vaak met behulp van machinaal leren. Kenmerkend voor AI-systemen zijn het inferentievermogen (het vermogen om op basis van data output te creëren die de fysieke of virtuele omgeving beïnvloedt) en het zelflerend vermogen (het vermogen om zich aan te passen en te verbeteren zonder menselijke tussenkomst).

Gebruiksverantwoordelijke: natuurlijke- of rechtspersonen, inclusief overheidsinstanties en agentschappen, die een AI-systeem onder eigen verantwoordelijkheid gebruiken. Dit geldt niet voor AI-systemen die worden gebruikt in een persoonlijke en/of niet-professionele context. Het waterschap wordt gezien als een overheidsinstantie.

Onrechtmatig gebruik: een situatie waarin een AI-systeem wordt gebruikt op een manier die in strijd is met de wet of de rechten van anderen schendt.

Contractuele aansprakelijkheid: verwijst naar de verplichtingen die voortvloeien uit contracten tussen partijen. In het geval van AI-systemen kunnen contracten tussen fabrikanten, leveranciers en gebruikers specifieke bepalingen bevatten over aansprakelijkheid.

1. AI-Verordening

Het Europees Parlement en de Raad namen de AI-Verordening (EU 2024/1689) op 21 mei 2024 aan. Op 1 augustus 2024 trad de verordening in werking. Verordeningen zijn rechtstreeks van toepassing in de lidstaten en hoeven niet te worden omgezet in nationale wetgeving. Wel zullen bepaalde onderdelen, zoals het toezicht, nog verder worden uitgewerkt.

De AI-Verordening treedt stapsgewijs in werking en op 2 augustus 2027 is de verordening volledig van toepassing. Verboden AI-praktijken zijn al vanaf 2 februari 2025 verboden en vanaf 2 augustus 2026 gelden een groot deel van de vereisten voor hoogrisico- en andere AI-systemen. Figuur 1 toont een schematische weergave van de toepassingen uit de verordening.

Waarden

De AI-Verordening moet worden toegepast in overeenstemming met de waarden van de Europese Unie (EU), zoals vastgelegd in het Handvest. De grondrechten uit het Handvest van de Grondrechten van de Europese Unie vormen de kern van de verordening en zorgen ervoor dat AI-technologieën op een ethische en verantwoorde manier worden ontwikkeld en gebruikt binnen de EU. Het doel van de verordening is om uniforme regels te stellen zodat AI-toepassingen niet alleen worden gestimuleerd, maar ook gereguleerd.

Onderling afwijkende nationale regels kunnen leiden tot versnippering van de interne markt en tot vermindering van de rechtszekerheid. Daarom moet in de hele EU een consistent en hoog beschermingsniveau worden gewaarborgd, zodat AI-systemen betrouwbaar zijn. De uniforme verplichtingen zorgen ervoor dat belangrijke belangen worden gerespecteerd en dat de grondrechten worden nageleefd. Om dit te bereiken heeft de verordening een aantal specifieke doelen vastgesteld:

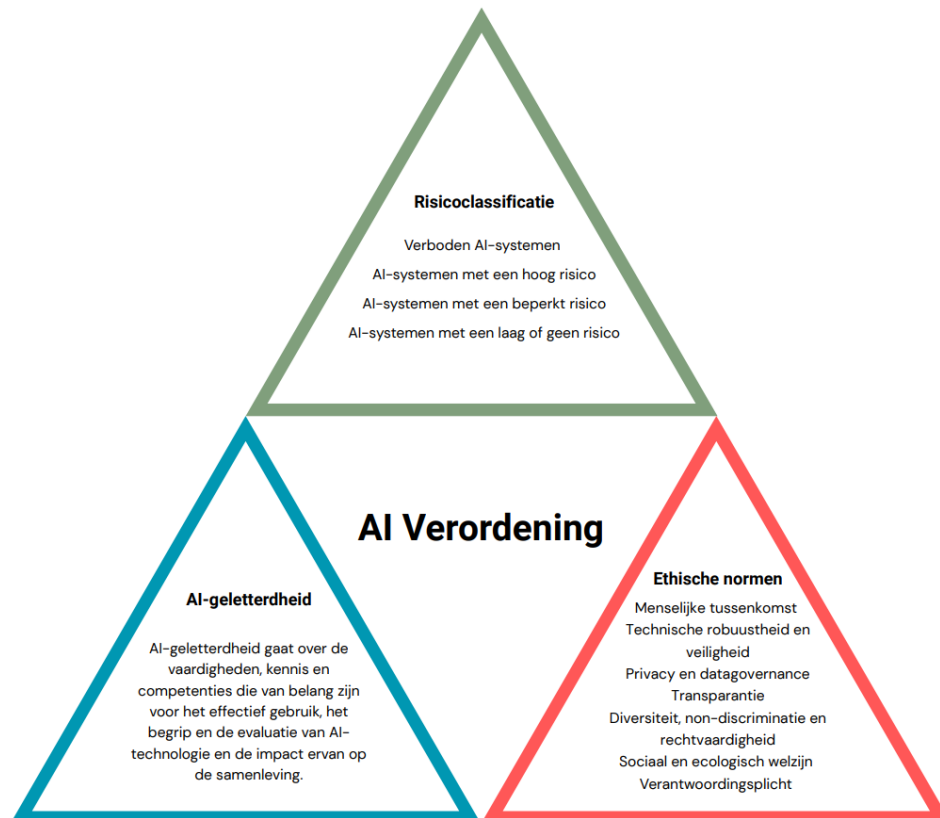
1. **Bescherming van de grondrechten:** het beschermen van fundamentele rechten van EU-burgers, zoals privacy, veiligheid en non-discriminatie bij het gebruik van AI-systemen. Deze grondrechten liggen op verschillende plaatsen vast. Het gaat om het recht op privacy en gegevensbescherming, het recht op non-discriminatie, het recht op een eerlijk proces, de vrijheid van meningsuiting en informatie, en het recht op waardigheid.
2. **Bevordering van innovatie:** het stimuleren door duidelijke en voorspelbare regels rondom AI-technologieën.
3. **Risicobeheer:** een risicogebaseerde aanpak waarbij AI-systemen worden geclassificeerd op basis van hun risiconiveau. Voor elk niveau gelden specifieke regels om risico's voor gezondheid, veiligheid en grondrechten te beperken.
4. **Transparantie en verantwoordelijkheid:** de nadruk ligt op transparantie en verantwoordelijkheid. Dit vereist duidelijke gebruikersinformatie, menselijk toezicht en de mogelijkheid voor burgers/gebruikers om beslissingen te begrijpen en te betwisten.
5. **Uniform kader:** een samenhangende aanpak van AI-regulering binnen de EU zodat er een gelijk speelveld ontstaat voor bedrijven in verschillende lidstaten.

Toepassingsbereik

AI-systemen die worden ingezet voor militaire, defensie- of nationale veiligheidsdoeleinden vallen buiten het toepassingsgebied van de AI-Verordening. Zodra dezelfde systemen voor civiele of openbare doeleinden worden gebruikt, is de verordening wél van toepassing en moeten alle regels worden nageleefd. De verordening is ook van toepassing op aanbieders buiten de EU als hun AI-systemen output leveren die binnen de EU wordt gebruikt. Daarom is het belangrijk om in

de hele dataketen inzicht te hebben in de herkomst, het gebruik en de toepassing van data om de regels goed te kunnen naleven.

Ook bestaan er niet-bindende ethische normen die ondersteuning bieden bij het maken van verantwoorde keuzes rond de ontwikkelingen en het gebruik van AI. Ze helpen om AI-systemen betrouwbaar en ethisch verantwoord te maken en omvatten zeven kernprincipes: menselijke tussenkomst, technische robuustheid en veiligheid, privacy en data governance, transparantie, diversiteit, non-discriminatie en rechtvaardigheid, sociaal en ecologisch welzijn en verantwoordingsplicht.



Figuur 1: opzet Verordening

2. AI-geletterdheid

Met de komst van de Europese AI-Verordening is de term AI-geletterdheid geïntroduceerd. Vanaf 2 februari 2025 moeten aanbieders (leveranciers van AI-systemen) en gebruiksverantwoordelijken (degenen die een AI-systeem inzetten) zorgen dat medewerkers en andere personen die namens hen AI-systemen gebruiken, AI-geletterd zijn.

Het begrip

AI-geletterdheid gaat over de vaardigheden, kennis en competenties die van belang zijn voor het effectief gebruik, het begrip en de evaluatie van AI-technologie en de impact ervan op de samenleving. Het gaat daarbij niet alleen om technische expertise, het omvat ook juridische, ethische, sociale en praktische aspecten. Dat betekent dat AI-geletterdheid verder gaat dan basiskennis van de technologie; het vereist inzicht in zowel de kansen (de voordelen) van AI, maar ook de risico's voor de gebruiker en de personen of groep personen (de burgers) waarop je AI toepast en wat daar eventueel de gevolgen van kan zijn.

Wanneer is een medewerker AI geletterd?

Dit bepaal je aan de hand van de functie van een medewerker, de kennis die een medewerker al heeft van AI, hoe vaak AI door diegene wordt ingezet en kennis over de gevolgen en impact van AI voor andere mensen.

Vanuit het Europese AI-bureau en de Europese Commissie zijn er (nog) geen richtlijnen over AI-geletterdheid waarvan gebruik gemaakt kan worden. Tot die tijd zal het dus aan de nationale toezichthouders zijn om concrete invulling te geven aan het begrip AI-geletterdheid en aan de maatregelen die door aanbieders en gebruikers van AI-systemen in dat kader moeten worden genomen. De Autoriteit Persoonsgegevens (AP) heeft in februari 2025 een document opgesteld "Aan de slag met AI-geletterdheid" dat richtsnoeren biedt bij het concreet oppakken van dit onderwerp (zie Aan de slag met AI-geletterdheid | Autoriteit Persoonsgegevens).

In het AI-kompas van de waterschappen (deel I: het bestuurlijk kader) is AI-geletterdheid ook opgenomen (hoewel niet met deze exacte term). Dit kompas, dat onderdeel is van de Vaarkaart Digitaal op koers, bevat vijf uitgangspunten voor AI-gebruik. Bij vier van de vijf uitgangspunten 'Kansengericht', 'Toekomstgericht', 'Uitlegbaar' en 'Ethisch afgewogen' komt het aspect AI-geletterdheid terug.

Wat moeten de waterschappen doen?

Gesteld kan worden dat AI-geletterdheid toeziet op twee aspecten: enerzijds gaat het om de bewustwording, anderzijds om kennisontwikkeling. De Verordening geeft niet aan op welke wijze je invulling moet geven aan AI-geletterdheid. Dit betekent dat de mate van AI-geletterdheid per organisatie kan verschillen. Van belang is om in ieder geval rekening te houden met de volgende stappen:

Stap 1: Inventariseren van AI-systemen en competentieniveau

Medewerkers die met een AI-systeem werken of mogelijk gaan werken, moeten daar geïnformeerd over worden. Dit betekent dat er een inventarisatie gedaan moet worden of er AI-systemen toegepast worden binnen de organisatie. Indien er wel AI-systemen toegepast worden, moet een classificatie bepaald worden. Ook is het van belang om het competentieniveau vast te stellen. Het toepassen van en werken met een AI-systeem betekent ook dat er met data gewerkt wordt. Het is daarom ook van belang om vast te stellen om welke data het gaat.

Stap 2: Richtlijnen opstellen voor het gebruik

Na de inventarisatie is het van belang om vast te stellen welke AI-systemen gebruikt mogen worden binnen de organisatie. Naast het vast leggen van welke systemen er gebruikt mogen worden, is het van belang om te bepalen voor welke handelingen deze systemen gebruikt mogen worden. Denk hierbij ook aan het vaststellen van databeveiliging, privacy en ethische aspecten.

Stap 3: Borg het kennisniveau en creëer bewustwording

Het is van groot belang om alle organisatielagen bewust te maken van de kansen die het werken met een AI-systeem met zich meebrengt. Daarnaast dienen de medewerkers kennis te ontwikkelen over wat deze kansen zijn en hoe ze goed benut kunnen worden. Door het creëren van bewustwording en ontwikkelen van kennis, weten de medewerkers waar ze aan toe zijn. Dit zorgt ervoor dat men bewust omgaat met de toepassingen en kennis heeft van de kansen die het met zich meebrengt. Dit kan gerealiseerd worden door het aanbieden van cursussen, leerlijnen en trainingen, afhankelijk van de organisatie laag en het kennisniveau.

Stap 4: Integreer AI-geletterdheid in de bedrijfsprocessen

De implementatie van AI-geletterdheid is geen eindpunt, maar een continu proces. De AI-Verordening en AI-toepassingen zijn dynamisch. De technologie gaat in een veel sneller tempo dan dat deze ingebed kan worden in de organisatie. Dit betekent ook dat het kennisniveau altijd op peil moet blijven. Door AI-geletterdheid onderdeel te maken van het organisatieproces, kan dit geborgd worden. Gedacht kan worden aan het opnemen in een PDCA-cyclus.

Hulpmiddelen

- o AP: <https://www.autoriteitpersoonsgegevens.nl/documenten/aan-de-slag-met-ai-geletterdheid>
- o Europa Decentraal: [Publicatiereeks digitale vaardigheden. Deel II: AI-geletterdheid en decentrale overheden - Europa decentraal](#)
- o Digitale Overheid: [Wat je moet weten over AI-geletterdheid - Digitale Overheid](#)
- o Digital Europe: [EU-Fondsenwijzer - Europa decentraal](#) (mogelijkheid subsidie aanvragen decentrale overheden om AI-geletterdheid te verbeteren)

3. Risicoclassificatie

3.0 Risicocategorieën

AI-systemen kunnen uiteenlopende effecten hebben op mensen en de samenleving. Sommige toepassingen hebben minder toereikende gevolgen, terwijl andere diep kunnen ingrijpen in mensenrechten, veiligheid of democratische processen. Om doeltreffende en evenwichtige regels voor AI-systemen in te voeren, is een duidelijke, risico gebaseerde aanpak noodzakelijk. Deze aanpak moet de regels afstemmen op de aard en ernst van de risico's die AI-systemen kunnen veroorzaken. Daarom zijn in de verordening vier categorieën opgenomen. Door risico's te classificeren, kunnen maatwerkregels opgesteld worden. Het gaat om de volgende vier (risico) categorieën:

1. Verboden AI-systemen.
2. Hoog risico AI-systemen.
3. Beperkt risico AI-systemen.
4. AI-systemen met een minimale risico.

De vier risico's worden hieronder nader toegelicht en uitgewerkt.

3.1. Verboden AI-systemen

Naast de verplichting om medewerkers AI-geletterd te maken, treden per 2 februari 2025 ook de eerste verboden in werking. Welke AI-systemen verboden zijn, is opgenomen in artikel 5 van de Verordening.

Bij de beoordeling of er binnen de waterschappen verboden AI-systemen gebruikt worden, is gekeken naar de primaire taken van een waterschap. Vervolgens is er een inventarisatie gedaan naar de mogelijke gebruikte AI-systemen die wellicht als verboden aangemerkt zouden kunnen worden. Uit de inventarisatie is het gebruik van verboden AI-systeem bij de waterschappen niet naar voren gekomen. Dit neemt echter niet weg dat er alsnog wel met een AI-systeem gewerkt wordt waarbij sprake zou kunnen zijn van een verboden systeem. Dit houdt in dat er altijd een classificatie moet plaatsvinden bij het in gebruik nemen van een (nieuw) AI-systeem.

Wat moeten de waterschappen doen?

Bepaalde begrippen uit artikel 5 behoeven een nadere uitleg om een duidelijker beeld te geven wat er onder wordt verstaan. Verboden die op voorhand uitgesloten kunnen worden, dus waarbij al bekend is en verondersteld mag worden dat een waterschap daar niet mee te maken heeft en niet mee te maken zal hebben, zal verder niet nader worden uitgewerkt. Het gaat hierbij om sub b en sub e tot en met f. Dit betekent dat er een korte uiteenzetting volgt van sub a, c, g en h.

Sub a: AI-systeem dat gebruikmaakt van manipulatieve technieken

AI-systemen die subliminale of misleidende technieken gebruiken om het gedrag van een persoon aanzienlijk te veranderen, waardoor hun vermogen om geïnformeerde beslissingen te nemen wordt aangetast en mogelijk aanzienlijke schade kan veroorzaken.

Sub c: AI-systeem dat gebruik maakt van social scoring

Het gaat hierbij om een AI-systeem dat individuen beoordeelt op basis van hun sociaal gedrag of persoonlijke kenmerken en daar (negatieve) gevolgen aan verbindt. Dit kan discriminerende gevolgen hebben of dat bepaalde groepen of mensen uitgesloten worden. Dit kan een gevoel van een oneerlijke behandeling en ongerechtvaardigd handelen met zich meebrengen. Bij een dergelijk AI-systeem kan gedacht worden aan biometrische identificatie bij de grenscontroles

waarbij personen met bepaalde uiterlijke kenmerken of sociaal gedrag, benadeeld kunnen worden.

Sub g: Categorisering o.b.v. biometrische gegevens

Deze verbodsbepaling heeft betrekking op het gebruik van een AI-systeem dat mensen categoriseert. Concreet betreft dit een verbod om een AI-systeem te gebruiken dat natuurlijke personen en individuen in categorieën indeelt, op basis van biometrische gegevens. Denk daarbij aan gegevens die betrekking hebben op ras, politieke opvattingen, het lid zijn van een vakbond, religieuze opvattingen of informatie over het seksleven en/of seksuele gerichtheid.

In de AI-Verordening worden biometrische gegevens geduid als persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedrag gerelateerde kenmerken van een natuurlijk persoon, zoals gezichtsafbeeldingen of vingerafdrukgegevens. Waterschappen maken voor hun taakuitoefening géén gebruik van biometrische gegevens van burgers.

Een voorbeeld hiervan is een (AI-)systeem dat door banken en/of financiële instellingen wordt gebruikt om bepaalde mensen (groepen) aan verscherpt toezicht te onderwerpen, aan de hand van bepaalde geloofsovertuigingen. Bijvoorbeeld donaties aan een moskee die meer gescreend worden dan donaties aan de christelijke kerk. De bestuurder van de moskee werd in een automatisch systeem 'geflagd' als meer risicovol.

Sub h: Gebruik van biometrische gegevens, realtime, in de openbare ruimte, vanwege rechtshandhaving

Hier aan de orde is het gebruik van biometrische gegevens in de openbare ruimte ten behoeve van de rechtshandhaving (opsporing en vervolging). Rechtshandhaving is in Nederland opgedragen aan de opsporingsbevoegde instantie (OM). Gebruik van biometrische gegevens door een AI-systeem is verboden, tenzij een legitiem doel zoals genoemd in de AI-Verordening wordt nagestreefd. Dit zijn:

- i. het gericht zoeken naar specifieke slachtoffers van ontvoering, mensenhandel of seksuele uitbuiting van mensen, alsook het zoeken naar vermiste personen;
- ii. het voorkomen van een specifieke, aanzienlijke en imminente dreiging voor het leven of de fysieke veiligheid van natuurlijke personen of een reële en actuele of reële en voorspelbare dreiging van een terroristische aanslag;
- iii. de lokalisatie of identificatie van een persoon die ervan wordt verdacht een strafbaar feit te hebben gepleegd, ten behoeve van een strafrechtelijk onderzoek of vervolging of tenuitvoerlegging van een straf voor in bijlage II genoemde strafbare feiten waarop in de betrokken lidstaat een vrijheidsstraf of een tot vrijheidsbeneming strekkende maatregel staat met een maximumduur van ten minste vier jaar.

Wat als iets toch onder verboden AI-systeem valt en wie houdt toezicht daarop?

Het is op dit moment niet duidelijk wie toezicht gaat houden. Autoriteit Persoonsgegevens (AP) is op dit moment de coördinerende toezichthouder, maar een definitieve toezichthouder is op dit moment nog niet aangewezen.

Dit neemt niet weg dat we verantwoord om moeten gaan met AI-systemen en ervoor moeten zorgen dat we geen verboden AI-systemen in onze organisatie gebruiken. Het gebruik van verboden AI-systemen kan namelijk ernstige gevolgen hebben voor de organisatie. Op het moment dat het definitief bekend is wie de toezichthouder zal zijn, kunnen overtredingen resulteren in boetes. Het belangrijkste gevolg is dat je als waterschap, een publiek orgaan,

reputatieschade kunt oplopen.

3.2. Hoog risico AI-systemen

Een AI-systeem met hoog risico is een systeem dat een aanzienlijke kans heeft om schade te veroorzaken aan de gezondheid, veiligheid of grondrechten van mensen. Dit kan bijvoorbeeld zo zijn als het systeem beslissingen neemt die grote gevolgen hebben voor mensen, zoals bij het stellen van een medische diagnose of het doen van juridische uitspraken. Als het AI-systeem slechts eenvoudige taken uitvoert of alleen suggesties geeft, zonder de uiteindelijke beslissing te beïnvloeden, wordt het niet als een hoog risico beschouwd.

Risicoclassificatie	Uitleg	Verwijzing verordening
AI-systemen met een hoog risico	Een AI-systeem met hoog risico is een systeem dat een aanzienlijke kans heeft om schade te veroorzaken aan de gezondheid, veiligheid of grondrechten van mensen. Dit kan bijvoorbeeld gebeuren als het systeem beslissingen neemt die grote gevolgen hebben voor mensen, zoals bij medische diagnoses of juridische uitspraken. Als het AI-systeem echter slechts eenvoudige taken uitvoert of alleen suggesties geeft zonder de uiteindelijke beslissing te beïnvloeden, wordt het niet als een hoog risico beschouwd. Specifieke gevallen van hoog-risico AI-systemen: • AI-systemen die de toegang bepalen tot het onderwijs. • AI-systemen voor werving, selectie, promotie, taaktoewijzing en monitoring van werknemers. • AI-systemen voor het bepalen van toegang tot gezondheidszorg, sociale diensten en uitkeringen. • AI-systemen voor het evalueren van kredietscores en financiële risico's. • AI-systemen voor de triage van noodoproepen en het sturen van hulpdiensten. • AI-systemen voor risicobeoordeling, bewijsmateriaalanalyse, en profilering bij misdaadopsporing. • AI-systemen voor risicobeoordeling en ondersteuning bij visum- en asielaanvragen. • AI-systemen ter ondersteuning van gerechtelijke autoriteiten en alternatieve geschillenbeslechting.	• Overweging 46 t/m 69. • Hoofdstuk 3 vanaf artikel 6.

	Er is geen sprake van een hoog risico AI systeem indien aan één van de volgende voorwaarden is voldaan: • het AI-systeem is bedoeld om een beperkte procedurele taak uit te voeren; • het AI-systeem is bedoeld om het resultaat van een eerder voltooide menselijke activiteit te verbeteren; • het AI-systeem is bedoeld om besluitvormingspatronen of afwijkingen van eerdere besluitvormingspatronen op te sporen en is niet bedoeld om de eerder voltooide menselijke beoordeling zonder behoorlijke menselijke toetsing te vervangen of te beïnvloeden, of • het AI-systeem is bedoeld om een voorbereidende taak uit te voeren voor een beoordeling die relevant is voor de in bijlage III van de AI Verordening vermelde gebruiksgevallen. Let op: een in bijlage III bedoeld AI-systeem wordt altijd als een AI-systeem met een hoog risico beschouwd indien het AI-systeem profilering van natuurlijke personen uitvoert.	
--	---	--

Praktische voorbeelden

Enkele praktische voorbeelden hiervan zijn:

- o *Overstromingsvoorspelling:* AI-systemen die voorspellen waar en wanneer overstromingen kunnen optreden. Fouten in deze systemen kunnen leiden tot gebrekkige voorbereidingen of schade.
- o *Waterkwaliteitsbewaking:* Technologieën die afwijkingen in de waterkwaliteit analyseren en signaleren. Onjuiste analyses kunnen gevolgen hebben voor de volksgezondheid en het milieu.
- o *Infrastructuurmonitoring:* AI-algoritmen die de staat van dijken, sluizen en dammen evalueren. Een verkeerde risico-inschatting kan ernstige gevolgen hebben.
- o *Energiemanagement:* Systemen die het gebruik van pompen en sluizen optimaliseren. Als deze verkeerd functioneren, kunnen zowel operationele als veiligheidsproblemen ontstaan.
- o *Handhaving:* Een AI-systeem dat gebruikt wordt bij het automatisch detecteren van overtredingen, bijvoorbeeld via dronebeelden. Foutieve interpretaties kunnen onterechte boetes of misbruik van bevoegdheden tot gevolg hebben.

- o *Contracten*: Een AI-systeem dat automatisch contracten opstelt en analyseert, waarbij beslissingen worden genomen over juridische implicaties zonder menselijke verificatie. Dit kan leiden tot juridische conflicten als het systeem fouten maakt of nuances niet goed begrijpt.
- o *Personeelszaken*: het inzetten van een urenregistratiesysteem waarbij wijzigingen worden doorgevoerd zonder menselijke tussenkomst en waarbij het voor de medewerker niet meer traceerbaar is.

Wat moeten waterschappen doen?

AI-systemen met een hoog risico in de context van een waterschap zijn toepassingen die voldoen aan artikel 6 van de AI-Verordening (behoudens de uitzonderingen uit het derde lid). Hierbij is van essentieel belang of sprake is van menselijke tussenkomst of niet. Door menselijke tussenkomst is er minder risico bij het gebruik van AI, omdat menselijke controle en supervisie ervoor zorgen dat AI-systemen worden gemonitord en gecorrigeerd wanneer nodig. Het is daarom van belang om in kaart te krijgen of er gewerkt wordt met hoog risico AI-systemen en hier menselijke tussenkomst op toe te passen.

Aan de hand van artikel 6 van de AI-Verordening kan worden getoetst of sprake is van een hoog risico AI-systeem. In het eerste lid staat de definitie, deze is onderverdeeld in twee onderdelen, namelijk sub a en b. Aan beide moet worden voldaan. Verder staat in het tweede lid een verwijzing naar bijlage III, als een AI-systeem op deze lijst staat dan betreft het in ieder geval een hoog risico AI-systeem. In het derde lid zijn uitzonderingen genoemd op het tweede lid.

De volgende gevallen wijzen op een hoog risico AI-systeem:

1. *Mogelijke gevolgen voor grondrechten*: het AI-systeem kan de privacy, vrijheid van meningsuiting, en andere fundamentele rechten van individuen beïnvloeden.
2. *Veiligheid*: het AI-systeem kan risico's vormen voor de fysieke en digitale veiligheid.
3. *Menselijke tussenkomst*: Het ontbreken van menselijke supervisie kan leiden tot ongecontroleerde en potentieel schadelijke beslissingen door het AI-systeem.
4. *Mogelijke gevolgen voor gezondheid en omgeving*: het AI-systeem kan negatieve effecten hebben op de gezondheid van individuen en de natuurlijke omgeving.
5. *Belemmering van wettelijke taken*: het AI-systeem kan de uitvoering van wettelijke en regulerende taken hinderen.
6. *Veiligheidscomponent in kritieke infrastructuur*: een AI-systeem dat een veiligheidscomponent vormt in kritieke infrastructuren kan aanzienlijke risico's met zich meebrengen.

Het advies bij één of meer van deze indicatoren is om altijd een risicobeoordeling uit te voeren.

3.3. Beperkt risico AI-systemen

Een AI-systeem wordt als beperkt risico beschouwd wanneer het een beperkte kans heeft om schade te veroorzaken aan de gezondheid, veiligheid of grondrechten van mensen. Hiervan is sprake als het AI-systeem slechts eenvoudige taken uitvoert of alleen suggesties geeft zonder de

uiteindelijke beslissing te beïnvloeden.

Wat er onder een beperkt risico AI-systeem valt, is opgenomen in artikel 50 van de AI-Verordening. Aanbieders en gebruikers van dergelijke AI-systemen moeten aan transparantieplichtingen voldoen. Een AI-systeem brengt een beperkt risico met zich mee als het menselijke handelen niet wezenlijk wordt beïnvloed. Waterschappen zijn over het algemeen gebruikers.

Risicoclassificatie	Uitleg	Verwijzing verordening
AI-systemen met een beperkt risico	Een AI-systeem wordt als beperkt risico beschouwd wanneer het niet direct invloed heeft op de rechten en vrijheden van individuen, maar toch transparantie en duidelijke richtlijnen vereist om het vertrouwen en de veiligheid in het gebruik ervan te waarborgen. • Klantenservice chatbots: Deze AI-systemen beantwoorden standaardvragen zonder gevoelige informatie te verwerken, waardoor ze een beperkt risico vormen. • Spellings- en grammaticacontrole software: AI-systemen die tekst analyseren en corrigeren voor spellings- en grammaticafouten zonder diepgaande persoonlijke gegevens te verwerken. • Voorspellende tekstinvoermethoden: AI-gebaseerde voorspellende tekstinvoermethoden op smartphones die suggesties geven op basis van eerder getypte woorden. • Automatische aanbevelingssystemen: Deze systemen doen productaanbevelingen op e-commerce websites op basis van gebruikersgedrag zonder gevoelige persoonlijke gegevens te gebruiken.	• Overweging 52 t/m 53.

Hieronder enkele voorbeelden van AI-systemen met een beperkt risico en de daarbij horende transparantieplichtingen:

- o *Interactie met natuurlijke personen:* AI-systemen die direct met mensen interageren moeten gebruikers informeren dat ze met een AI-systeem te maken hebben, tenzij dit al

duidelijk is voor een redelijk geïnformeerde persoon.

- o *Synthetische inhoud*: AI-systemen die synthetische audio-, beeld-, video- of tekstinhoud genereren, moeten ervoor zorgen dat deze inhoud duidelijk gemarkeerd is als kunstmatig gegenereerd.
- o *Emotieherkenning en biometrische categorisering*: Gebruikers moeten geïnformeerd worden wanneer AI-systemen emotieherkenning of biometrische categorisering gebruiken. Dit geldt vooral voor systemen die gevoelige gegevens verwerken.
- o *De transparantieplichting* is bedoeld om de transparantie en het vertrouwen in AI-systemen te vergroten, en om ervoor te zorgen dat ze op een verantwoorde en ethische manier worden ingezet.

Praktische voorbeelden

Binnen de werkgroep AI-Verordening is een inventarisatie gedaan naar AI-systemen die mogelijk een beperkt risico hebben. De volgende toepassingen zijn geïnventariseerd:

- o *Voorspellende tekstinvoermethoden*: AI-gebaseerde voorspellende tekstinvoermethoden (zoals in Teams bijvoorbeeld) die suggesties geven op basis van eerder getypte woorden.
- o *Chatbots*: Deze AI-systemen beantwoorden standaardvragen zonder gevoelige informatie te verwerken, waardoor ze een beperkt risico vormen.
- o *Geautomatiseerde rapportagesystemen*: Deze systemen kunnen gegevens verzamelen en analyseren om rapporten te genereren over bijvoorbeeld waterkwaliteit.

Wat moeten de waterschappen doen?

In hoofdstuk twee is een uitleg gegeven van de verplichtingen van waterschappen met betrekking tot AI-geletterdheid. AI-geletterdheid is belangrijk wanneer het gaat om werken met beperkt risico AI-systemen. Werknemers moeten zich bewust zijn dat ze werken met AI-systemen en hoe ze hier mee moeten omgaan.

3.4. Laag risico AI-systemen

Laag risico AI-systemen worden onderworpen aan minimale vereisten, zoals transparantieplichtingen. Dit betekent dat de gebruikersverantwoordelijke de menselijke gebruiker duidelijk moet maken dat het systeem gebruik maakt van AI.

Risicoclassificatie	Uitleg	Verwijzing verordening
AI-systemen met een laag of geen risico	Als laatste zijn er toepassingen van AI waarin zowel de kans op schade als de eventuele impact hiervan zo klein zijn, dat er geen bijzondere regels zijn. Het enige wat vereist is, is dat de technische documentatie van het model up-to-date blijft. Deze categorie AI is al veel in gebruik, hoewel er lange tijd geen bewustzijn was om dit als AI te herkennen. Denk bijvoorbeeld aan spamfilters in je e-	

	mail of adblockers in je browser. Deze toepassingen maken het leven gemakkelijker, kunnen weinig schade aanrichten en de kans dat ze überhaupt schade veroorzaken, is relatief klein.	
--	---	--

Praktische voorbeelden

Enkele praktische voorbeelden van AI-systemen met een laag risico zijn:

- o Spamfilter e-mail;
- o Spelling- en grammaticacorrectie;
- o Slimme thermostaat;
- o Virtuele assistent (Siri, Alexa, etc.);
- o Navigatie-apps.

Wat moeten waterschappen doen?

Aan de hand van de algehele inventarisatie naar het gebruik van AI-systemen in de organisatie en de daaropvolgende classificatie wordt ook deze categorie inzichtelijk. Voor AI-systemen die als laag risico worden gekwalificeerd, kunnen waterschappen de onderstaande stappen nemen:

- o Gebruikers/medewerkers informeren dat ze gebruik maken van (laag-risico) AI-systemen en de mogelijke risico's daarvan schetsen (transparantie)
- o Benoem in de privacyverklaring dat gebruik wordt gemaakt van laag-risico AI-systemen, zodat burgers (externen) en medewerkers (intern) geïnformeerd zijn over het gebruik van AI;
- o Zorg ervoor dat gebruikers weten dat ze met een AI-systeem te maken hebben. Dit kan door duidelijke meldingen te geven wanneer AI wordt gebruikt, bijvoorbeeld als het mailcontact betreft, dit vermelden in de mail.
- o Neem (de laag-risico) AI-systemen op in het (landelijk) algoritmeregister, zodat je transparant en open bent over de gebruikte AI-modellen en het doel hiervan.
- o Stel interne richtlijnen op voor het gebruik van AI, gericht op ethiek en privacy.

Toezicht

De Autoriteit Persoonsgegevens (AP) en Rijksinspectie Digitale Infrastructuur (RDI) adviseren om AI-toezicht in verschillende sectoren zoveel mogelijk te laten aansluiten bij het bestaande toezicht. AI-producten met een hoog risico (die nu al een CE-markering vereisen) kunnen hetzelfde blijven. De externe toezichthouder voor bescherming van persoonsgegevens blijft dan ook waarschijnlijk de AP. Ook relevant voor de waterschappen: de toezichthouder op AI-toepassingen bij kritieke infrastructuur wordt de RDI, samen met de Inspectie voor Leefomgeving en Transport (ILT).

Aansprakelijkheid van de gebruiker

Onrechtmatig gebruik van AI-systemen is een overtreding van de AI-Verordening. Het is daarom belangrijk om de aansprakelijkheidsrisico's in kaart te brengen. Dit kan je doen door de volgende stappen te doorlopen:

1. Inventariseer wat voor soort type contract het is.
2. Maakt de ontwikkelaar/leverancier gebruik van een AI-oplossing?
3. Zo ja, breng in kaart welke risico-classificatie verbonden is aan deze AI-oplossing?

4. Gebruikt het waterschap deze AI-oplossing voor de kritieke activiteiten die betrekking hebben op onze kerntaken?
5. Stel vast welke eisen de AI-Verordening stelt aan de risico-classificatie. Controleer in een aparte risicobeoordeling van het voorgestelde AI-systeem of aan de wettelijke eisen is voldaan?
6. Breng specifiek in kaart of de ontwikkelaar/leverancier kan voldoen aan de eisen die de AI-Verordening stelt voor toezicht?
7. Stel vast welk kwaliteitsmanagementsysteem de ontwikkelaar/leverancier gebruikt en controleer of dit voldoet aan de AI-Verordening?
8. Controleer of het waterschap de gebruikersvoorschriften van de ontwikkelaar/leverancier kan naleven en of er technische aanpassingen nodig zijn.
9. Zijn alle gebruikers zich bewust van de gebruikersvoorschriften en de daaraan gekoppelde risico's?
10. Inventariseer of de cybersecurityregelgeving van toepassing is.
11. Onderzoek of de programmatuur aan de stand van de techniek, Europese en internationale normen en certificeringen voldoet.
12. Zijn de AWBIT 2023 van toepassing verklaard? Zijn er aanvullende maatregelen nodig?
13. Is er een exit-strategie overeengekomen?
14. In welke mate is het waterschap afhankelijk van een leverancier? Wat is het alternatief?
15. Contracten moeten voorzien in regelmatige audits en beoordelingen om ervoor te zorgen dat alle partijen voldoen aan de vastgestelde normen en verplichtingen.
16. Is in de overeenkomst een medewerkingsplicht opgenomen, zodat het waterschap kan voldoen aan alle eisen van de AI-Verordening? Zo nee, is het nodig om de contracten daarop aan te passen?
17. Kom overeen dat cyberincidenten niet kwalificeren als een situatie van overmacht (6:75 BW). Is dat contractueel goed vastgelegd?

Het is van belang dat alle betrokken partijen, van ontwikkelaars tot eindgebruikers, zich bewust zijn van hun verantwoordelijkheden en verplichtingen.

Bij het beoordelen van een AI-systeem moeten we niet alleen kijken naar de technische specificaties en prestaties, maar ook naar de bredere juridische en ethische implicaties. Dit omvat het naleven van de relevante Europese en internationale normen en certificeringen, evenals de lokale regelgeving en de specifieke eisen van de AI-Verordening. Een grondige risicobeoordeling en het implementeren van beheersmaatregelen zijn onmisbare stappen om de integriteit en veiligheid van het AI-systeem te waarborgen.

Daarnaast speelt de contractuele vastlegging een cruciale rol in het beheer van de toeleveranciersketen. Contracten moeten duidelijke afspraken bevatten over regelmatige audits, medewerkingsplicht en hoe om wordt gegaan met cyberincidenten. Het is ook belangrijk om een exit-strategie te hebben die de continuïteit van de dienstverlening waarborgt in geval van beëindiging van de samenwerking met een leverancier.

4. Samenhang wetgeving

AI-systemen raken uiteenlopende rechtsgebieden, van gegevensbescherming tot cyberveiligheid. Het is daarom belangrijk om te begrijpen hoe de AI-Verordening zich verhoudt tot andere rechtskaders.

4.1. Privacy

AVG

De Algemene Verordening Gegevensbescherming (AVG) geldt sinds 25 mei 2018 in de hele Europese Unie (EU). Deze verordening bevat gedetailleerde voorschriften voor bedrijven en organisaties over het verzamelen, opslaan en beheren van persoonsgegevens.

Verhouding met AI-Verordening

In overweging 10 van de AI-Verordening staat dat de bestaande Uniewetgeving over de verwerking van persoonsgegevens van toepassing blijft op het gebruik van AI-systemen en de aanbieders en gebruikers van deze systemen. Dit is niet alleen de AVG, maar ook de onder andere nu geldende Richtlijn 2022/58/EG. Ook de nationale toezichthouders behouden hun bevoegdheden uit de AVG. Overweging nummer 38 vermeldt uitdrukkelijk dat de AI-Verordening niet bedoeld is als rechtsgrondslag voor biometrische identificatie op afstand (handhaving openbare orde).

Persoonsgegevens mogen volgens artikel 59 van de AI-Verordening wel gebruikt worden voor een ander doel dan waarvoor ze verzameld zijn, namelijk voor het trainen en testen van AI-systemen die bedoeld zijn om een aanzienlijk openbaar belang te waarborgen. Deze belangen omvatten openbare veiligheid en volksgezondheid, bescherming van het milieu, groene transitie en klimaatverandering, energieduurzaamheid, veiligheid van vervoerssystemen, kritieke infrastructuur en het verbeteren van de doeltreffendheid en kwaliteit van het openbaar bestuur en openbare diensten (artikel 59, lid 1, sub a). Het artikel somt daarnaast de voorwaarden op waaraan voldaan moet worden.

In overweging nummer 67 wordt uitdrukkelijk vermeld dat verwerking van persoonsgegevens in datasets bij AI-systemen moet voldoen aan de beginselen en voorschriften van de AVG.

Het recht op privacy en bescherming van persoonsgegevens moet gedurende de hele levenscyclus van het AI-systeem worden gewaarborgd. Dit volgt uit overweging 69 van de AI-Verordening. In dit verband zijn bij de verwerking van persoonsgegevens de beginselen van minimale gegevensverwerking en van gegevensbescherming door ontwerp en door standaardinstellingen, zoals vastgelegd in het Unierecht inzake gegevensbescherming, van toepassing. De maatregelen die aanbieders nemen om deze beginselen na te leven, moeten niet alleen anonimisering en versleuteling omvatten. Ze moeten ook technologie gebruiken die de toepassing van algoritmen op gegevens en de training van AI-systemen mogelijk maakt zonder de uitwisseling of het kopiëren van de ruwe of gestructureerde gegevens zelf tussen partijen. Hierbij worden de eisen inzake datagovernance waarin de AI-Verordening voorziet, in acht genomen.

Samenvattend, de AI-Verordening waarborgt dat het recht op privacy en bescherming van persoonsgegevens centraal blijft staan bij de verwerking en het gebruik van AI-systemen, terwijl tegelijkertijd wordt gezorgd voor een aanzienlijk openbaar belang.

4.2. Cyberbeveiligingswet

De Cyberbeveiligingswet (hierna: Cbw) is de naam van de Nederlandse implementatie van de NIS2-richtlijn. De NIS2-richtlijn dient om kwetsbaarheden van de voorloper, de NIS1-richtlijn, te verhelpen. Het doel van de richtlijn is om de netwerk- en informatiebeveiliging in Europa te uniformeren, de digitale paraat- en alertheid te vergroten en om de gevolgen van cyberincidenten te verkleinen.

Verhouding met AI-Verordening

Artikel 2 bevat het juridisch kader van de Cbw. De Cbw is erop gericht om risico's voor de beveiliging van netwerk- en informatiesystemen te beheersen (a), incidenten te voorkomen en eventueel de gevolgen daarvan te beperken (b en c) informatie te verkrijgen over incidenten, dreigingen en kwetsbaarheden.

AI is door mensen ontworpen software. Deze software kan bij gebrekkig, onduidelijk of onvoldoende functioneren (aanzienlijke) risico's met zich meebrengen voor de veiligheid van netwerk- en informatiesystemen. Een AI-systeem raakt daarom ook potentieel netwerk- en informatiesystemen, zodat de Cbw en de AI-Verordening naast elkaar van toepassing zijn.

Aanwijzing als essentiële of belangrijke entiteit

De Cbw is alleen van toepassing op essentiële of belangrijke entiteiten die in Nederland zijn gevestigd en hun diensten in de EU verlenen. De Cbw wijst deze entiteiten aan. In de wet zelf of door middel van aanwijzing via bijvoorbeeld de Wwke. De waterschappen zijn aangewezen als een essentiële entiteit.

4.3. Wet weerbaarheid kritieke entiteiten

De Wet weerbaarheid kritieke entiteiten (hierna: Wwke) is een implementatie van de Europese CER-richtlijn. Deze richtlijn dient om vitale maatschappelijke functies van economische activiteiten te borgen. In de Wwke worden fysieke (beschermings)maatregelen opgelegd aan onder andere de waterschappen.

Verhouding met de AI-Verordening

De waterschappen zijn kritieke entiteiten althans vervullen essentiële diensten ten behoeve van alle Nederlanders. Gebruik van AI kan potentieel het leveren van deze essentiële diensten in gevaar brengen. De AI-verordening is naast de Wwke van toepassing wanneer AI-systemen worden gebruikt in of behulpzaam zijn bij de uitvoering van essentiële diensten.

Aanwijzing als kritieke entiteit

De minister van I&W moet het waterschap bij besluit, door middel van een ministeriële regeling, aanwijzen als kritieke entiteit (hierna: KE). Activiteiten van het waterschap, bijvoorbeeld zuivering van afvalwater, moet door de minister als kritieke infrastructuur worden bestempeld. Als dat het geval is, dan is de Wwke van toepassing op het waterschap en/of de kritieke activiteiten/essentiële diensten.

4.4. Algoritmeregister

Nagenoeg alle overheidsinstellingen maken gebruik van algoritmes. Het inzetten en gebruiken van een AI-toepassing is onlosmakelijk verbonden met algoritmes. Overheidsinstanties hebben op dit moment de mogelijkheid om de algoritmes waar ze gebruik van maken, te publiceren in het algoritmeregister. Dit is op dit moment niet wettelijk verankerd. Het kabinet wil, om de algoritmes te kunnen reguleren, dit wel verplichten in een wettelijke kader.

4.5 Uitvoeringswet AI

Nederland is als lidstaat verplicht om ervoor te zorgen dat de bepalingen uit de AI-Verordening nageleefd worden. Hoe ze dit zal doen, zal worden opgenomen in de Uitvoeringswet AI. Het zal vooral toezien op toezicht. Op dit moment is er nog geen zicht op wanneer de wet in werking zal treden. De verwachting is dat het pas eind 2025 zal zijn.

4.6. Data act

De Data Act verplicht organisaties om gebruikers toegang te geven tot de data die zij zelf genereren via digitale producten of diensten. Daarnaast is de wet bedoeld om de toegang tot data eerlijker, transparanter en veiliger te maken. De Data Act zal per 11 september 2025 van toepassing zijn in Nederland.

Op basis van de wet kan, in sommige, bijzondere, gevallen de waterschappen toegang vragen/worden gevraagd tot gegevens van private partijen. Gedacht kan worden aan gevallen waarbij er sprake is van een cyberaanval of een noodsituatie. Indien een externe, derde private partij, over gegevens beschikt, kan het waterschap om verschaffing van deze gegevens vragen.

Verhouding AI-Verordening

Waterschappen moeten in kaart brengen welke data zij verzamelen, wie eigenaar is van de data en wie toegang heeft. Dit geldt ook voor data die voortkomt uit slimme sensoren, meetapparatuur of digitale diensten. Het is belangrijk om vast te leggen onder welke voorwaarden deze data gedeeld mag worden.

Bij het gebruiken of maken van een AI-systeem, wordt simpelweg gebruik gemaakt van data. Daarom is het belangrijk om ook vast te leggen welke data er verzameld wordt, maar ook aan wie het versterkt wordt.

4.7. Data governance act

Om het beheer en de toegankelijkheid van data binnen de Europese Unie te verbeteren, is de Data Governance Act (DGA) in werking getreden. In de wet zijn eisen opgenomen over de manier waarop data wordt verzameld, beheerd en gedeeld tussen organisaties en individuen. De DGA is van toepassing op alle organisaties die data verzamelen en verwerken, waaronder de waterschappen.

Verhouding AI-Verordening

Aankomende jaren zal data en de uitwisseling van data tussen de verschillende overheidsorganisaties steeds een belangrijkere rol gaan spelen. Dit zal nog meer van belang zijn als een waterschap een AI-systeem als gebruiker in gebruik gaat nemen. Om de uitwisseling van data tussen verschillende systemen en organisaties te vergemakkelijken, moeten data toegankelijk en interoperabel zijn. Dit betekent dat data in gestandaardiseerde formaten moet worden opgeslagen en dat er gebruik moet worden gemaakt van open standaarden en protocollen. Hierdoor kunnen verschillende systemen en applicaties eenvoudig met elkaar communiceren en data uitwisselen.

Deze data kan ook gevoelige informatie bevatten. Het is daarom van belang om te zorgen voor een goede beveiliging van deze informatie. De DGA stelt strenge eisen aan de beveiliging en bescherming van persoonsgegevens.

5. Inrichting governance & compliance

Governance verwijst naar het geheel van regels, processen en controles waarmee organisaties worden bestuurd. In de context van AI is governance cruciaal voor transparantie, verantwoordingsplicht en naleving van wet- en regelgeving. Door duidelijke regels en processen in te stellen, kunnen we de impact van AI op de samenleving beter beheersen en ervoor zorgen dat AI-systemen eerlijk en rechtvaardig worden ingezet.

5.1 Technische specificaties

AI-systemen moeten duidelijk gedefinieerde technische specificaties hebben om hun prestaties en betrouwbaarheid te waarborgen. Dit omvat specificaties voor de hardware waarop het systeem draait, de software-architectuur, de algoritmen die worden gebruikt en de datasets die worden verwerkt. Het is essentieel dat deze specificaties regelmatig worden bijgewerkt om te voldoen aan de nieuwste technologische ontwikkelingen en veiligheidsnormen.

5.2 Kwaliteitsbeheer

Kwaliteitsbeheer is een cruciaal onderdeel van governance voor AI-systemen. Dit omvat het vaststellen van normen en procedures om de kwaliteit van AI-modellen te waarborgen. Regelmatige evaluaties en bijstellingen zijn noodzakelijk om ervoor te zorgen dat AI-systemen blijven voldoen aan de gestelde verwachtingen en wettelijke vereisten.

5.3 Interne en externe controles

Interne controles zijn processen en mechanismen binnen een organisatie die ervoor zorgen dat de activiteiten voldoen aan de vastgestelde beleidslijnen en normen. Beide soorten controles zijn essentieel om vertrouwen te creëren in AI-systemen, doordat ze transparantie en verantwoordelijkheid bevorderen en helpen bij het opsporen en corrigeren van eventuele tekortkomingen.

Voor de validatie van AI-systemen zijn er specifieke strategieën en procedures nodig om ervoor te zorgen dat ze naar behoren functioneren en voldoen aan de gestelde eisen. Deze processen omvatten:

- o Definiëren van duidelijke validatiecriteria gebaseerd op technische specificaties en gebruiksscenario's.
- o Uitvoeren van grondige testen en simulaties om de prestaties en betrouwbaarheid van het systeem te evalueren.
- o Regelmatige reviews en audits van het systeem om continue naleving en aanpassing aan nieuwe eisen te waarborgen.

5.4 Bewaring van documentatie en logbestanden

Artikel 18 en 19 van de AI-Verordening richt zich op de bewaring van documentatie. Het stelt dat alle relevante documentatie met betrekking tot de ontwikkeling, implementatie en werking van AI-systemen zorgvuldig moet worden bewaard. Dit is essentieel voor het waarborgen van transparantie en naleving van de regelgeving.

6. Samenhang interne activiteiten

De AI-Verordening raakt ook uiteenlopende interne sector brede activiteiten. Het is daarom belangrijk om de samenhang tussen deze activiteiten en de AI-Verordening te begrijpen.

6.1 De Vaarkaat

De ambitie van de gezamenlijke waterschappen voor de digitale transformatie is in 2023 vastgesteld door het bestuur van de Unie van Waterschappen. De uitdagingen en mogelijkheden die op de sector afkomen worden vertaald in vijf thema's, zoals "de meerwaarde van data" en "uniforme sector naar een hoger niveau". De Vaarkaat is voor veel waterschappen de aanleiding om samenhang aan te brengen bij bestaande en nieuwe activiteiten op het gebied van de digitale transformatie. Uitwerkingen die nu sector breed worden opgepakt zijn onder andere het AI-kompas, een datastrategie voor de sector en digitale ethiek. De Vaarkaat helpt ons ook om de ontwikkelingen op het gebied van wet- en regelgeving een logische plek te geven bij de digitale transformatie.

AI is een belangrijke technologie, die bij de uitwerking van de Vaarkaat op veel plekken een rol zal spelen. De implementatie van de AI-Verordening draagt bij aan een verantwoord en wettelijk gebruik van AI en vormt dus de basis voor andere uitwerkingen van de Vaarkaat.

6.2 AI-kompas

Het AI-kompas is één van de uitwerkingen van de Vaarkaat en beschikt over een bestuurlijk kader dat moet helpen bij het maken van de juiste afwegingen bij het toepassen van AI. Het AI-kompas beschrijft hoe AI zorgvuldig, onderbouwd en transparant ingezet kan worden in lijn met de geldende wet- en regelgeving. Het bestuurlijk deel bevat vijf uitgangspunten voor AI-gebruik binnen de waterschappen: kansengericht, toekomstgericht, solidariteit, uitlegbaar en ethisch afgewogen. Onder het onderdeel uitlegbaar valt het 'vertrouwen, verantwoordelijkheid en naleving van wet- en regelgeving'. Als waterschappen dragen we de verantwoordelijkheid om ervoor te zorgen dat technologische innovaties, zoals AI, ten goede komen aan de samenleving zonder onbedoelde negatieve gevolgen. Duidelijke uitleg over AI-uitkomsten draagt bij aan het opbouwen van vertrouwen en de naleving van wet- en regelgeving.

6.3 Themagroep Data en ethiek

Eén van de uitwerkingen van de Vaarkaat is de Strategienota voor het Waterschapshuis, waarin de ambitie vertaald is naar een concreet plan voor de komende jaren voor de activiteiten van het Waterschapshuis. De Strategienota is in het begin van 2024 vastgesteld. Bij de Strategienota hoort ook een nieuwe governance van het Waterschapshuis, en worden een viertal thema's uitgewerkt in themaplannen. Dit zijn bijvoorbeeld themaplan "wet- en regelgeving" en het themaplan "data en ethiek". De themaplannen worden uitgevoerd door de bijbehorende themagroepen, die in 2025 gestart moeten zijn. De themagroepen brengen samenhang aan in de projecten van het Waterschapshuis door op hun thema richtlijnen, collectieve standpunten en uitvoeringsprincipes vast te stellen. Ze kunnen ook geraadpleegd worden als er vraagstukken op hun gebied uitgewerkt moeten worden.

In de themagroep Data en ethiek worden alle zaken rond dit thema behandeld. In het themaplan is het als volgt geformuleerd: "Het is de ambitie van de waterschappen om alle informatie die over de grens van een individueel waterschap uitgewisseld moet worden (wettelijke grondslag, bestuurlijke opdracht, etc.), op uniforme wijze via gemeenschappelijke voorzieningen beschikbaar te maken. Ethisch handelen is hierbij een belangrijke voorwaarde. Het thema data & ethiek versterkt de 'kracht van samen' doordat het Waterschapshuis (hWh), de Unie van

Waterschappen en de waterschappen zelf samenwerken aan toepassing van standaarden, modellen en voorzieningen, waarbij hWh voor kennis, expertise en coördinatie als spil functioneert ten dienste van de waterschappen.”

6.4 Themagroep Wet- en regelgeving

Er komt een groot volume aan (veelal Europese) wet- en regelgeving op de waterschappen af die impact heeft op de inrichting van de organisatie op bedrijfsvoering en IT-vlak. Een aantal impactvolle wetten zijn nog nauwelijks geïmplementeerd bij de waterschappen of een volgende tranche komt er alweer aan. Het bundelen van krachten (kennis en capaciteit) ligt hierdoor voor de hand.

Het themaplan Wet- en regelgeving faciliteert de waterschappen in het voldoen aan wet- en regelgeving in de brede context van informatie, digitalisering en dienstverlening. Wet- en regelgeving raakt alle onderdelen van de organisatie. Vaak is er behoefte aan samenwerking op de meeste onderdelen, de wettelijke bepalingen zijn immers voor alle waterschappen even relevant en passend. Door een gestructureerde wijze van samenwerking tussen de waterschappen, het Waterschapshuis en de Unie van Waterschappen kunnen aandachtspunten eerder gesignaleerd worden. Hierdoor kunnen de waterschappen eerder compliant zijn op het terrein van wet- en regelgeving. Analyseren van relevante wet- en regelgeving op samenhang en het relateren aan processen binnen waterschappen maakt daar een onderdeel van uit. Daarnaast kunnen kaders geformuleerd worden voor projectuitvoering van projecten binnen het Waterschapshuis.

De Unie van Waterschappen heeft van waterschappen input nodig om de belangen van de waterschappen bij de ontwikkeling van nieuwe wet- en regelgeving te behartigen. Ook hier kunnen waterschappen hun krachten bundelen.

6.5 Datastrategie

Momenteel wordt er een uniforme datastrategie opgezet door middel van een projectgroep. Een datastrategie is cruciaal om snel en accuraat toegang te hebben tot betrouwbare en actuele data omdat het de basis legt voor een efficiëntere en effectievere uitvoering van de primaire processen van de waterschappen. Door datagedreven werken te integreren in de processen, kunnen waterschappen niet alleen hun operationele efficiëntie verbeteren, maar ook de betrouwbaarheid en transparantie van hun diensten vergroten. Dit is essentieel om het vertrouwen van de samenleving te winnen en te behouden, en om de opgaven op het gebied van waterbeheer duurzaam aan te pakken. Daarbij moeten de waterschappen voldoen aan diverse wet- en regelgeving rondom digitalisering, zoals de AI-Verordening. Het is daarom van belang om deze regelgeving te verankeren in de datastrategie, zodat datagedreven werken op een verantwoorde en juridisch juiste manier plaatsvindt.