



# INZICHTEN 2024

VERVOLGPUBLICATIE OP *AI BEELDHERKENNING MET DRONES IN DE OPENBARE RUIJME, MARKTVISIE EN INKOOPSTRATEGIE (JANUARI 2024)*  
DOOR HET LEERNETWERK AI BEELDHERKENNING

JANUARI 2025

**Deze publicatie is tot stand gekomen als onderdeel van het Leernetwerk AI Beeldherkenning, een initiatief van de Nederlandse AI Coalitie en PIANOo Expertisecentrum Aanbesteden, in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.**



Auteurs: Céline van Dooren (PIANOo), Joris Krüse (Studio Kidman & Nicholson) en Martin Jansen (Mens, Merk & Ruimte).

Met bijdragen van: de deelnemende overheden van het Leernetwerk AI beeldherkenning, Hans Nouwens (gemeente Breda), Laurens Samson (gemeente Amsterdam), Rob de Lange (Provincie Overijssel), Jessica Maes (Nationaal Cyber Security Centrum (NCSC)), Bram van Aggelen (Nationaal Cyber Security Centrum (NCSC)), Mark Loos (Netherlands Space Office (NSO)), Peter Verkoulen (Centre of Excellence for Data Sharing & Cloud), Evelien Zengerink (gemeente Amsterdam), Peter Stoop (gemeente Amsterdam), Marieke Peeters (Hogeschool Utrecht), Muriel Jobst-de Boer (PIANOo).

Ontwerp en productie: Studio Kidman & Nicholson, PIANOo, Xerox

Ben je enthousiast over de inhoud, wil je van gedachten wisselen of verbeteringen aandragen? Neem dan contact op via [info@pianoo.nl](mailto:info@pianoo.nl).

PIANOo Expertisecentrum Aanbesteden  
Rijksdienst voor Ondernemend Nederland  
[www.pianoo.nl](http://www.pianoo.nl)



# INHOUDSOPGAVE

Introductie	4
1 Borgen van kwaliteit	5
2 Cybersecurity	7
3 Delen van data, AI en informatie	9
4 Ethiek en publieke acceptatie	12
5 Het inkopen van oplossingen met AI beeldherkenning	15

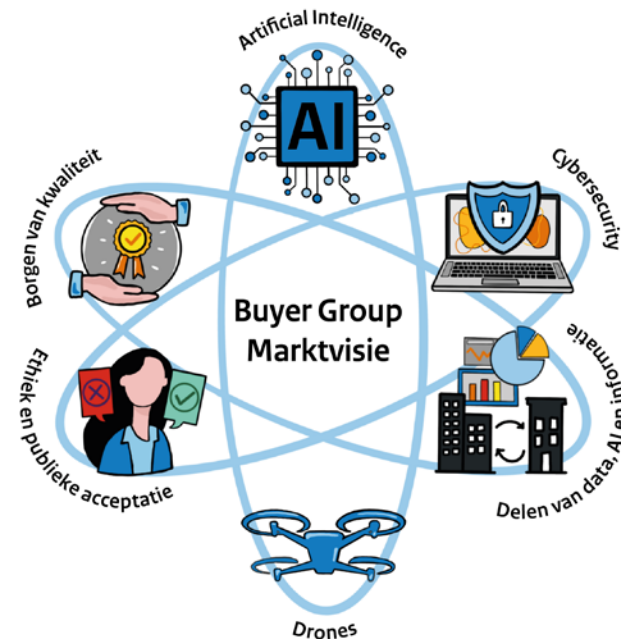
# INTRODUCTIE

Een verantwoorde inkoop van AI-oplossingen, bijvoorbeeld oplossingen met beeldherkenning, vereist een zorgvuldig proces. Overheden moeten algoritmes begrijpen, onderhouden en verantwoorden zolang ze in gebruik zijn, zeker bij directe impact op burgers. In het inkoopproces komen complexe behoeften zoals technologische eisen en maatschappelijke acceptatie samen. Daarom speelt inkoop een cruciale rol.

In januari 2024 is de [marktvisie 'AI beeldherkenning in de publieke ruimte, marktvisie en inkoopstrategie'](#) gepubliceerd als resultaat van de Buyer Group AI beeldherkenning met drones. Deze marktvisie biedt houvast bij het inkopen van AI beeldherkenning met o.a. drones en informeert aanbestedende diensten en marktpartijen over relevante thema's en aandachtspunten. Doel van de marktvisie is een verantwoorde en toekomstbestendige inzet van AI beeldherkenning op 4 kernthema's:

- Borgen van kwaliteit
- Cybersecurity
- Delen van data, AI en informatie
- Ethiek en publieke acceptatie

In 2024 is de Buyer Group verder gegaan als [Leernetwerk AI beeldherkenning](#) om deze thema's te verdiepen. In 4 themasessies zijn praktijkvoorbeelden gedeeld en ervaringen uit het onderzoeksveld behandeld. De inzichten en praktische inkooptips die hieruit volgden, zijn in deze vervolgpublishatie gebundeld.



Elk thema begint met een casus uit de praktijk, gevolgd door de daarin opgedane inzichten en de inhoudelijke bijdrage uit de themasessie. Daarna geven we tips voor de inkoop van oplossingen met AI beeldherkenning. Tot slot volgt een vertaling naar het inkoopproces van (de ontwikkeling van) algoritmes zoals AI-beeldherkenning in de vorm van de Leidraad 'Het kopen of laten ontwikkelen van algoritmes en AI: het inkopersperspectief'.

De terugblikken van de 4 themasessies zijn terug te lezen op de [website van PIANOo](#).

# 1 BORGEN VAN KWALITEIT



## Casus: Bredata's droneproject voor veilige bedrijventerreinen

Met het project [Inzet Drones voor Veilige Bedrijventerreinen](#) onderzoekt de gemeente Breda hoe innovatieve technologieën bedrijventerreinen veiliger en aantrekkelijker kunnen maken. Onder leiding van Hans Nouwens, Programmamanager Bredata, test de gemeente in een proeftuin de inzet van een drone met camera voor toepassingen zoals handhaving, detectie van zwerfvuil, ondermijning, surveillance en assetmanagement. De drone observeert bijvoorbeeld foutgeparkeerde vrachtwagens en zwerfvuil met behulp van AI-beeldherkenning, gebaseerd op een bestaand algoritme dat is geregistreerd in het Algoritmeregister van de Rijksoverheid.

### Levenscyclus van een algoritme als uitgangspunt

Laurens Samson, Lead van het Computer Vision-team van gemeente Amsterdam, benadrukt dat geen enkel algoritme compleet foutloos is. Door alle fasen van de levenscyclus van een algoritme zorgvuldig te doorlopen, zijn fouten wel te detecteren en corrigeren voordat ze problemen veroorzaken. De Bredata-casus laat zien hoe de verschillende fasen van de levenscyclus van een algoritme zijn doorlopen en welke inzichten dat heeft opgeleverd.

In de beginfase draait alles om het scherpstellen van de probleemstelling en het verkennen van mogelijke oplossingen. In deze casus was de uitdaging helder: hoe kan het monitoren van zwerfvuil, criminaliteit en parkeeroverlast effectiever met behulp van een drone?

De realistische setting van de proeftuin dient als een laboratorium om de technologie in te testen. Samenwerkend met diverse stakeholders verzamelt Bredata feedback vanuit verschillende perspectieven. Dit helpt om verwachtingen te managen en legt een basis voor de verdere ontwikkeling van het algoritme.

Zodra het concept staat, begint de fase van ontwikkelen en trainen. De keuzes die hierbij worden gemaakt, bepalen hoe robuust en schaalbaar de oplossing is. Bredata gebruikt een bestaand algoritme van een andere aanbestedende dienst dat is geregistreerd in het Algoritmeregister van de Rijksoverheid. Het algoritme is bedoeld voor objectherkenning op straatniveau, maar werd in de proeftuin aangepast om ook beelden vanuit een droneperspectief te verwerken – bijvoorbeeld voor de detectie van zwerfvuil en foutgeparkeerde voertuigen. Het projectteam streeft naar een infrastructuur om continu dronebeelden te kunnen analyseren. Ter voorkoming van een wildgroei aan drones is gekozen voor 1 gedeelde drone die meerdere gebruikers kunnen inzetten.

Inzichten in de nauwkeurigheid van de beeldherkenning kwamen vooral voort uit de gebruik- en beheerfase van het algoritme. Samson benadrukte dat data-invoer met de tijd verandert (zogenoemde 'datadrift') waardoor regelmatige her-training is vereist. Zo bleek het algoritme uit het Bredata-project in staat om kentekens te herkennen met een nauwkeurigheid van 93%. Onder bepaalde omstandigheden – bijvoorbeeld bij slecht zicht op trailers en nachtelijke omstandigheden bleek de herkenning lastiger. Ook variaties in de omgeving zoals weersomstandigheden kunnen de prestaties negatief beïnvloeden. Al deze bevindingen hebben geholpen bij de verdere verfijning van het model.

Zodra het algoritme zijn grenzen heeft bereikt of als de technologie nieuwe mogelijkheden biedt, breekt de uitfaseringsfase aan. Bredata hanteerde een Agile-aanpak, waarbij de AI-oplossing als een Minimum Viable Product (MVP) functioneert. De data werden in dit project alleen gebruikt voor testdoeleinden en niet langdurig opgeslagen. Dit vergemakkelijkt het afbouwproces en beperkt privacy-risico's.

### **Opgedane tips en inzichten voor inkoop**

- Specificeer wat de oplossing moet kunnen, inclusief technische details zoals herkenningssnauwkeurigheid, AVG-compliance en robuustheid.
- Vraag om proefprojecten in de vorm van een proeftuin of pilot om de praktische toepasbaarheid van een concept te verkennen.
- Overweeg een analyse van de beschikbare datasets en ga na of ze representatief en van voldoende kwaliteit zijn om het algoritme te trainen.
- Vraag om het gebruik van bewezen algoritmes die aan te passen zijn aan de specifieke context.
- Borg dat de oplossing schaalbaar is en bestaande processen en systemen integreert.
- Vraag hoe de leverancier omgaat met datadrift, zoals veranderende omstandigheden of datasets.
- Vereis systemen voor continue monitoring van prestaties.
- Laat jaarlijkse evaluaties uitvoeren om te bepalen of het algoritme her-training of aanpassingen nodig heeft.
- Stel eisen aan het opslaan, verwijderen en overgedragen van data na uitfasering om privacy te borgen.
- Werk samen met andere overheden of organisaties die ervaring hebben met soortgelijke projecten en deel eigen opgedane kennis en inzichten via bijvoorbeeld het Algoritmeregister.
- Overweeg open source-oplossingen voor meer transparantie en hergebruik van technologie.



## 2 CYBERSECURITY



### Casus: Crowd control bij evenementen in de provincie Overijssel

De provincie Overijssel wilde AI beeldherkenning inzetten voor crowd control bij evenementen zoals het Bevrijdingsfestival in Zwolle. Het idee was om camera's en sensoren te gebruiken om drukte te monitoren en verkeersstromen te sturen. Rob de Lange, CISO bij de provincie Overijssel, stelde dat de risico's daarvan groter waren dan aanvankelijk gedacht. Belangrijke uitdagingen betroffen privacy (hoe zorg je dat mensen niet te identificeren zijn in datasets?), manipulatie (wat als camera's worden omgebogen of beelden worden vervalst?) en een kosten-batenafweging (zijn er eenvoudigere en effectievere alternatieven?). De uiteindelijke oplossing was pragmatisch: mensen gebruiken camera's puur voor real-time observatie zonder dat data wordt opgeslagen of geanalyseerd door AI.

### Cybersecurity als ketengerichte en multidisciplinaire benadering

Jessica Maes, Coördinator Advies en Kennisproducten van het [Nationaal Cyber Security Centrum \(NCSC\)](#) reageerde op de casus van de provincie Overijssel. Volgens het NCSC is cybersecurity gebaat bij een ketengerichte en multidisciplinaire benadering. Veiligheid is geen geïsoleerde inspanning: elke schakel in de keten – van dataverzameling tot opslag en verwerking – vereist zorgvuldige bescherming. Kwetsbaarheden kunnen op elk niveau ontstaan. De Overijsselse casus liet zien dat zelfs een klein zwak punt een heel

systeem kan ondermijnen. Van een verkeerd geplaatste camera en een onversleutelde verbinding tot slecht beheerde toegangsrechten. *Tooling*, zoals een Software Bill of Materials (SBOM), kan helpen bij het identificeren van kwetsbaarheden in softwarecomponenten. De Plan-Do-Check-Act (PDCA) cyclus is een gestructureerde manier om beveiligingsmaatregelen continu te evalueren en aan te passen aan nieuwe bedreigingen. Beveiliging is immers geen eenmalige actie, maar een voortdurend proces.

Het NCSC ziet kennisdeling als een belangrijke pijler van cyberweerbaarheid. Organisaties zouden incidenten niet in stilte moeten oplossen maar actief hun aanpak moeten delen om zo andere organisaties te waarschuwen en versterken. Transparantie en samenwerking zijn daarmee wapens tegen cyberdreigingen. Rob verwees naar de luchtvaartindustrie, waar incidenten altijd worden gemeld, gedeeld en onderzocht zodat men ervan leert. Opdrachtgevers en opdrachtnemers zouden zo ook samen moeten leren van 'cyber leaks' en 'cyber hacks'.

Ook menselijke betrokkenheid is van belang. Het NCSC stelde dat technologie slechts zo effectief is als de mensen die ermee werken en benadrukte het belang van bewustwording en training. Gebruikers inzicht geven in risico's en trainen in veilig gedrag legt de basis voor een duurzame cyberveilige cultuur. Simulaties zoals phishing-tests en ransomware-oefeningen helpen om benodigde vaardigheden te versterken. Bij de Overijsselse casus bleek menselijke observatie de oplossing voor het signaleren van kwetsbaarheden.



## Opgedane inzichten en tips voor inkoop

- Betrek interne experts vanaf het begin. Door het samenstellen van een multidisciplinair team met o.a. een inkoopadviseur, IT-specialist, jurist, CISO, etc. zijn technische, juridische en ethische aspecten van een project te beoordelen.
  - Overweeg om al in de inkoopfase ethische hackers te betrekken. Door hen de geplande systemen te laten beoordelen vóóordat ze worden geïmplementeerd, zijn potentiële risico's die ontwikkelaars en inkoopers mogelijk missen alsnog te identificeren.
  - Besteed ook aandacht aan kleine onverwachte kwetsbaarheden die vaak over het hoofd worden gezien, zoals fysieke manipulatie van hardware (e.g. ombuigen van camera's) of het vervangen van sensoren. Laat een team van experts bijvoorbeeld proberen de AI-oplossing te manipuleren of te hacken. Dit helpt bij het blootleggen van onverwachte kwetsbaarheden en het versterken van je beveiligingsstrategie.
  - Stimuleer scenario-denken bij opdrachtnemers om meerdere risicoscenario's en bijbehorende risicobeperkende strategieën in de offertefase te beschrijven. Dit laat zien hoe ze voorbereid zijn op onverwachte gebeurtenissen.
  - Overweeg het gebruik van *tooling* zoals Software Bill of Materials (SBOM) door opdrachtnemers te vragen om een gedetailleerde lijst te leveren van alle softwarecomponenten en -versies. Dit helpt kwetsbaarheden sneller te identificeren en risico's beter te beheersen.
- Overweeg het toevoegen van een testperiode aan het contract. Zo is de AI-oplossing onder gecontroleerde omstandigheden te beoordelen voordat hij volledig operationeel wordt.
  - Overweeg het simuleren van dreigingen binnen de specifieke context. Pas dreigingsscenario's ook aan op de unieke gebruikssituaties van jouw organisatie, zoals manipulatie van drones bij kritieke infrastructuur of interferentie met dataverbindingen.
  - Overweeg het implementeren van een PDCA-cyclus (continu verbeterproces) om beveiligingsmaatregelen periodiek te evalueren en aan te passen aan nieuwe dreigingen.
  - Beveilig systemen tegen typisch menselijke fouten zoals verkeerd gebruik van software of slecht beheerde toegangsrechten. Ook simpele fouten kunnen tot grote kwetsbaarheden leiden.
  - Overweeg het ontwikkelen van een 'Cyber Incident Response Playbook' en een duidelijk stappenplan specifiek voor cyberincidenten met AI-oplossing. Dit vergemakkelijkt snelle en gecoördineerde actie in geval van een aanval.



## 3 DELEN VAN DATA, AI EN INFORMATIE

### Casus: NSO's satellietdataportaal als voorbeeld van datadelen

Het [satellietdataportaal van het Netherlands Space Office \(NSO\)](#) biedt gratis toegang tot satellietdata voor Nederlandse gebruikers. Mark Loos, Adviseur bij NSO, verstelde dat NSO de data centraal inkoop en ze op een veilige manier beschikbaar stelt, waarmee publieke én private partijen laagdrempelig toegang krijgen tot waardevolle gegevens. Door de data op toegankelijke en waardevolle wijze beschikbaar te stellen, kan de data door diverse gebruikers en voor diverse doeleinden worden gebruikt, zoals het aanpakken van maatschappelijke opgaven, het creëren van economische waarde en het bevorderen van wetenschappelijk onderzoek.

Het satellietdataportaal onderstreept het belang om bij de inkoop (van de ontwikkeling) van toepassingen met AI beeldherkenning rekening te houden met zaken als robuuste dataregulering, samenwerking binnen vertrouwde ecosystemen, het gebruik van beschikbare veilige (sectorale) datadelingsplatforms en interoperabiliteit en portabiliteit van de data.

### Openheid en ontwikkelingen ter bevordering van datadelen

Data is waardevol en hergebruik van bestaande data is efficiënt. Peter Verkoulen, Programmadirecteur van het Centre of Excellence for Data Sharing & Cloud (CoE-DSC), gaf aan dat organisaties nu naar schatting slechts 2% van hun data delen vanwege de uitdagingen die de effectiviteit van datadeling beïnvloeden. Belangrijke obstakels

zijn een gebrek aan vertrouwen over de controle op en veiligheid van data en de technologische en juridische complexiteit bij het bouwen van interoperabele systemen tussen sectoren. Dit doet niets af aan de noodzaak van interoperabiliteit en cloudportabiliteit voor eenvoudig datadelen tussen verschillende cloudomgevingen.

Interoperabiliteit en cloudportabiliteit zijn belangrijke aspecten bij de ontwikkeling van oplossingen met AI beeldherkenning met gebruik van bestaande of gegenereerde data en informatie. Het NSO stelt bijvoorbeeld verschillende dataformaten beschikbaar op het satellietportaal en biedt gebruiksvriendelijke toegangsmogelijkheden waardoor data overdraagbaar is naar andere processen, systemen (interoperabiliteit) en organisaties (cloudportabiliteit). Ook stimuleert NSO door middel van open source licenties het gebruik van de gedeelde data, waardoor gebruikers veilig afgeleide producten kunnen delen zonder de brondata vrij te geven. Dit versterkt datasoevereiniteit en minimaliseert privacyrisico's.

Om organisaties en mensen controle over hun eigen data te laten houden en waarde uit de eigen data te kunnen halen, werkt de Europese Unie (EU) aan verplichte maatregelen en stimulerende initiatieven om gewenst gedrag zoals veilig datadelen te bevorderen. Voorbeelden van verplichtende maatregelen zijn de General Data Protection Regulation (GDPR, 2016), Open Data Directive (2019), Data Governance Act (DGA, 2022) en de Data Act (2024). De Data Act geeft organisaties en mensen meer controle over hun data en regelt onder andere de portabiliteit van data tussen cloudomgevingen.

Stimulerende initiatieven moeten gecontroleerde en gedecentraliseerde datadeling mogelijk maken, zodat datadelen binnen en tussen sectoren en landen eenvoudiger wordt. Een voorbeeld is [Gaia-X](#), een ecosysteem dat de digitale soevereiniteit van Europa moet bevorderen door een federatief systeem te creëren waarin data op een veilig en betrouwbare manier kan worden gedeeld tussen organisaties en cloud serviceproviders. Het systeem richt zich op het ontwikkelen van een netwerk van vertrouwde partijen die op een interoperabele manier data met elkaar kunnen delen. Het Gaia-X Trust Framework geldt als een belangrijk instrument om vertrouwen te kweken door verschillende niveaus van certificering en labeling. Een ander voorbeeld is [SIMPL](#), een software-infrastructuur die als basis dient voor de Common European Data Spaces. Het initiatief faciliteert gestandaardiseerd datadelen tussen sectoren en landen, waarbij deelnemers volledige controle houden over externe toegang tot hun data. SIMPL is gebaseerd op federatieve principes. Dit betekent dat data bij de bron kan blijven, terwijl het toegankelijk wordt gemaakt voor andere partijen.

Het [CoE-DSC](#) helpt in Nederland bij het bevorderen van datadelen door het ontwikkelen van bouwstenen, gereedschappen en kennis om datadelen in verschillende sectoren te faciliteren. De verwachting is dat de samenwerking tussen sectoren en landen zowel nationaal als internationaal toeneemt en dat dit leidt tot nieuwe en schaalbare data-ecosystemen. Ook is de verwachting dat grote Europese bedrijven binnenkort Gaia-X-labels gaan uitvragen bij hun leveranciers. Dit zal een belangrijke impuls geven aan de adoptie van Gaia-X en het creëren van een markt voor datadelen. Ook zal EU-wetgeving de markt voor datadelen de komende jaren fundamenteel gaan veranderen. Allemaal veranderingen die tijd kosten, en toch is de verwachting dat de wetgeving een onomkeerbare verschuiving in gang zet naar meer gecontroleerd en soeverein datadelen.



## Opgedane inzichten en tips voor inkoop

- De naleving van Europese en nationale wetgeving is essentieel. Zorg dus dat je goed op de hoogte bent van relevante wetgeving. Contracten moeten borgen dat datadeling veilig en conform geldende wetgeving gebeurt. Voeg compliance-eisen toe aan aanbestedingsdocumenten om veiligheid en privacy te garanderen.
  - Stel interoperabiliteitseisen op door in aanbestedingen te vereisen dat data tussen cloudomgevingen uitwisselbaar is. Zo bevorder je de interoperabiliteit en verklein je de kans op een *vendor lock-in*. Zo zijn organisaties niet afhankelijk van 1 leverancier en kunnen ze eenvoudiger wisselen tussen cloudaanbieders zonder verlies van controle over hun data.
  - Overweeg het werken met gecertificeerde data-ecosystemen en het selecteren van leveranciers die voldoen aan de Europese standaarden voor datasoevereiniteit, bijvoorbeeld door het gebruik van Gaia-X-certificeringen, decentrale data-architecturen of soortgelijke standaarden. Dit versterkt datasoevereiniteit en betrouwbare datadeling.
  - Overweeg het integreren van data-altruïsme in je strategie. Zo moedig je leveranciers aan om data beschikbaar te stellen voor maatschappelijk nut, bijvoorbeeld stedelijke ontwikkeling of milieumonitoring.
  - Overweeg om gebruik te maken van sectorale initiatieven door aan te sluiten bij bestaande platforms in sectoren waar data-uitwisseling van belang is, zoals landbouw of infrastructuurbeheer. Deze initiatieven ondersteunen veilige en gedeelde datatoegang.
- Overweeg het gebruik van bestaande data-infrastructuren zoals SIMPL voor gestandaardiseerde en veilige data-uitwisseling en een betere samenwerking met andere publieke of private partijen.
  - Overweeg het toevoegen van datagebruiksvoorwaarden. Formuleer datagebruiksrechten en verantwoordelijkheden duidelijk in overeenkomsten met leveranciers zodat alle partijen weten wie welke data onder welke voorwaarden kan gebruiken.
  - Zorg voor proactieve databeveiligingseisen, bijvoorbeeld door het vereisen van geavanceerde beveiligingsprotocollen zoals data-encryptie en Privacy Enhancing Technologies (PET) die het risico's op datalekken minimaliseren.
  - Bouw kennis over technologische complexiteit op binnen de organisatie, bijvoorbeeld door het organiseren van trainingen over data-interoperabiliteit en cloudportabiliteit voor het inkoopteam en andere relevante interne stakeholders. Zo kun je effectief technologische uitdagingen aanpakken en het gesprek voeren met leveranciers.
  - Evalueer regelmatig of aanbestedingen en contracten nog voldoen aan actuele Europese en nationale wet- en regelgeving en pas je processen daarop aan.

## 4 ETHIEK EN PUBLIEKE ACCEPTATIE



### Casus: Computer Vision in de openbare ruimte van Amsterdam

De gemeente Amsterdam gebruikte voor haar project 'computer vision in de openbare ruimte' een burgerpanel van 11 personen met uiteenlopende meningen over AI en beeldherkenning in de openbare ruimte. Het panel werd betrokken bij de ontwikkeling van containerherkenning in Agile en Design Thinking werkvormen.

Dataminimalisatie bleek een belangrijk punt volgens Evelien Zengerink en Peter Stoop, Projectmanager, respectievelijk Productowner en Projectmanager bij de gemeente Amsterdam. Samen met het burgerpanel werden 4 scenario's voor dataminimalisatie ontwikkeld, van het opslaan van beeld met een container tot het vervagen van de omgeving op dit beeld, het opslaan van alleen de container zonder context en alleen het opslaan van de containerlocatiecoördinaten. Op basis van praktijktests werden de scenario's verder uitgewerkt tot een werkbare oplossing. De input van het burgerpanel werd opgenomen in de stukken voor de bestuurlijke besluitvorming, zodat het college van B&W en de gemeenteraad konden meekijken met de dialoog met en binnen het panel.

### Het ethisch perspectief als dynamisch en iteratief proces

Door ethiek te beschouwen als een continu proces en publieke acceptatie als actieve samenwerking, transparantie te waarborgen

en te werken vanuit een lerende aanpak, kunnen overheden technologieën ontwikkelen die voldoen aan technische vereisten én aansluiten bij waarden en verwachtingen in de samenleving. Zo luidde de reflectie van Marieke Peeters, Onderzoeker op het gebied van verantwoorde AI aan de Hogeschool Utrecht.

Ethiek is geen statisch kader om 'het goede' te kunnen doen. Ethiek is dynamisch en moet iteratief meegroeien met maatschappelijke normen en waarden. Het is een voortdurend proces van reflectie en aanpassing. In de praktijk betekent dit dat ethiek voortdurend moet worden geëvalueerd en ingebed in technologische en beleidsmatige keuzes. Het continu betrekken van het burgerpanel uit de casus gaf directe feedback in een fase waarin aanpassingen van de oplossing goed mogelijk waren. Dit resulteerde in een gedragen oplossing.

Marieke legde uit waarom zij vindt dat de term publieke acceptatie te beperkt is geformuleerd. Publieke acceptatie zou namelijk niet beperkt moeten blijven tot het 'informereren' van burgers. Het gaat om het opbouwen van een actieve en wederkerige relatie, waarin burgers niet alleen worden gehoord maar ook daadwerkelijk invloed kunnen uitoefenen. Dat burgers bijvoorbeeld in burgerpanels en workshops actief kunnen meedenken over ethische keuzes is goed, maar daarbij moeten ze ook zien hoe hun input wordt verwerkt en invloed heeft op de uiteindelijke beslissingen. Deze aanpak maakt publieke acceptatie meer een proces van actieve samenwerking tussen burgers en overheid dan de eenzijdige verwachting dat burgers technologie zonder meer accepteren.

Transparantie is een cruciale factor in ethiek die verder gaat dan alleen technische uitleg. Het gaat om inzicht in besluitvormingsprocessen en het zichtbaar maken van de afweging van een ethisch dilemma. Transparantie is te bereiken door input van burgers direct te integreren in beleidsstukken en bestuurlijke processen. Zo wordt de stem van burgers gehoord én weegt deze ook daadwerkelijk mee in de besluitvorming. De gevoerde dialoog in het Amsterdamse burgerpanel werd bijvoorbeeld opgenomen in de bestuurlijke stukken. (Technische) documentatie en algoritmische keuzes zijn ook inzichtelijk te maken op platforms zoals het Algoritmeregister.

Ethiek is een dynamisch proces, want technologieën en maatschappelijke normen veranderen continu. AI-projecten moeten met deze ontwikkelingen meebewegen. Dit vereist een lerende organisatie die kan inspelen op nieuwe inzichten en kan reageren op feedback van burgers en andere stakeholders. In de praktijk gebeurt dit bijvoorbeeld door het inbouwen van regelmatige evaluaties en feedbackloops. Dit houdt in dat ethische risico's en maatschappelijke reacties voortdurend worden gemonitord en technologieën en processen waar nodig worden aangepast. Ook kennisdeling binnen en tussen organisaties is essentieel om blinde vlekken te identificeren en *best practices* te verspreiden.

## Opgedane inzichten en tips voor inkoop

- Overweeg om leveranciers te verplichten om een ethische impact assessment (EIA) uit te voeren en de resultaten daarvan op te leveren. Dit helpt bij het identificeren van potentiële risico's en garandeert dat ethiek al vroeg in het proces wordt meegenomen. Laat de EIA meewegen in de uiteindelijke beoordeling. Je kunt ook evalueren hoe leveranciers rekening houden met dataminimalisatie, bias en maatschappelijke acceptatie.
- Overweeg de verplichtstelling van externe audits om objectief te laten beoordelen hoe goed een technologie voldoet aan ethische normen. Neem bijvoorbeeld in de aanbesteding de verplichting op dat periodieke ethische audits zijn uitgevoerd door onafhankelijke partijen. Of verbind sancties aan het niet naleven van ethische richtlijnen.
- Overweeg de inrichting van verplichtingen voor participatieprocessen, zoals workshops of burgerpanels. Je kunt de participatieverplichtingen opnemen in de aanbesteding inclusief deliverables, zoals rapportages over burgerinput en hoe die te verwerken. Of stel als eis dat leveranciers publieke marktconsultaties of demonstraties organiseren als onderdeel van de implementatiefase.
- Verplicht leveranciers om transparant te zijn over hoe hun AI-systemen werken en welke data worden gebruikt. Vereis heldere documentatie over de werking van algoritmes en besluitvormingsprocessen afgestemd op een breed publiek. Laat leveranciers datasets documenteren inclusief herkomst, selectiecriteria en maatregelen om *bias* te voorkomen. Verplicht publicatie van deze gegevens op relevante platforms, zoals het Algoritmeregister van de Nederlandse overheid.
- AI-technologie evolueert snel terwijl maatschappelijke normen veranderen. Contracten moeten daarom flexibel zijn voor aanpassingen en updates. Overweeg bijvoorbeeld om clausules op te nemen die leveranciers verplichten om systemen aan te



passen op basis van nieuwe inzichten, feedback of veranderende regelgeving. Of eis een monitoringsplan inclusief tussentijdse evaluaties en mogelijkheden voor bijsturing.

- Overweeg om prototypes van AI-systemen te laten ontwikkelen en testen specifiek voor ethische dilemma's en publieke acceptatie via pre-commerciële inkoop (PCP). Vraag leveranciers bijvoorbeeld om scenario's te ontwikkelen en testen, zoals dataminimalisatie of alternatieve gebruiksvormen. Of organiseer proeftuinen waarin burgers direct feedback kunnen geven op een prototype.
- AI-systemen moeten inclusief en toegankelijk zijn voor alle burgers. Vereis daarom dat leveranciers technologieën ontwikkelen die eenvoudig te begrijpen en gebruiken zijn. Vraag om testen met diverse groepen gebruikers.
- Het gebruik van open standaarden is gewenst om afhankelijkheid van leveranciers (vendor lock-in) te vermijden en publieke controle te versterken. Overweeg waar mogelijk het gebruik van open standaarden en interoperabiliteit met andere systemen te verplichten. Laat leveranciers aantonen hoe zij bijdragen aan transparantie en samenwerking binnen bredere ecosystemen.

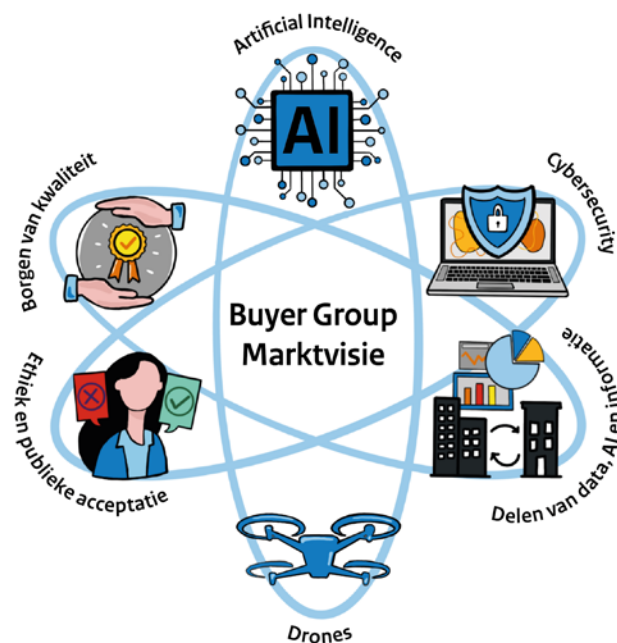
- Leveranciers moeten technologie op toegankelijke manieren demonstreren aan burgers en gemeenschappen. Dit bevordert vertrouwen en geeft direct inzicht in de publieke perceptie. Laat leveranciers bijvoorbeeld publieksdemo's organiseren waarin technologie in begrijpelijke termen wordt uitgelegd. Verplicht leveranciers om input uit deze sessies te documenteren en waar nodig te verwerken in updates van AI-systemen.
- Training is essentieel ter voorbereiding op complexe ethische vraagstukken. Organiseer daartoe workshops over ethiek en AI gericht op het herkennen en mitigeren van ethische risico's. Zorg dat inkoopteams basiskennis hebben van AI-technologieën zodat ze interne opdrachtgevers en leveranciers kritisch kunnen bevragen. Creëer een cultuur waarin lessen uit eerdere aanbestedingen worden vastgelegd en gedeeld binnen en tussen organisaties. Eis bijvoorbeeld van leveranciers dat ze ethische evaluaties documenteren en delen. Verrijk bestaande kennisplatforms waarin overheden *best practices* en uitdagingen uitwisselen.

## 5 HET INKOPEN VAN OPLOSSINGEN MET AI BEELDHERKENNING

Algoritmes, waaronder AI beeldherkenning, raken steeds meer verweven in allerlei IT-toepassingen. Ook overheden gebruiken in dienstverlening steeds meer toepassingen waarin algoritmes zijn verwerkt. Overheden moeten in staat zijn om toepassingen met algoritmes, die gebruikt worden in de dienstverlening, te begrijpen, onderhouden en uit te leggen aan de maatschappij gedurende de gehele levenscyclus van een algoritme. Zeker wanneer een algoritme impact heeft op burgers.

Het inkopen van (de ontwikkeling van) een oplossing met AI beeldherkenning vereist onder meer aandacht vanwege de snelle ontwikkelingen in technologie en regelgeving. Het inkoopproces is belangrijk omdat verschillende behoeften en complexiteit rondom algoritmes, zoals AI beeldherkenning, hier bij elkaar (moeten) komen. Een gedegen inkoopproces levert een bijdrage aan het voorkomen van negatieve en ongewenste effecten bij de inzet van algoritmes. Voor de inzet van algoritmes moeten bijzonderheden en specifieke complexe aspecten in het inkoopproces worden samengebracht. De inkoopadviseur zal daarom samen met de interne opdrachtgever en overige leden van het multidisciplinaire inkoopteam de vertaling moeten maken naar een overheidsopdracht voor verantwoorde ontwikkeling en inzet van algoritmes in samenwerking met private partijen.

Voor een overzicht van de aandachtspunten voor inkoopadviseurs van overheidsorganisaties bij het kopen of laten ontwikkelen van een algoritme, zoals AI beeldherkenning, heeft PIANOo in het kader van de Community of Practice Digitale Innovaties de leidraad 'Het kopen of laten ontwikkelen van algoritmes en AI: het inkoopersperspectief' ontwikkeld.





PIANOo Expertisecentrum Aanbesteden

Rijksdienst voor Ondernemend Nederland  
[www.pianoo.nl](http://www.pianoo.nl)