Gemeente Amsterdam

20 januari 2022

Instrumenten voor publieke controle op algoritmes

- Governance
- Contractvoorwaarden
- Handreiking bezwaarbehandelaars algoritmes
- Mensenrechten-impactassesment
- [redacted]-analyse

GOVERNANCE

Taken en verantwoordelijkheden bij het gebruik van Algoritmen door de gemeente Amsterdam

Digitale Strategie en Informatie / CIO Office
20 januari 2022



Inhoud



1. Inleiding
2. Levenscyclus van een algoritme
3. Wie doet wat?
4. Verantwoordelijkheden
5. Contactpersonen

Inleiding



Voor wie is deze notitie bestemd?

- Het college van Amsterdam heeft ambitie om aan een vrije, creatieve, en inclusieve stad te werken. Amsterdam geeft daarmee prioriteit aan investeringen in en beleid op (digitale) ontwikkeling.
- Met als doel het zorgen voor interventies die het leven van Amsterdammers verbeteren; door de negatieve effecten van digitalisering te beperken en de positieve effecten te versterken.
- Deze notitie is bestemd voor alle medewerkers van de gemeente Amsterdam die betrokken zijn bij de ontwikkeling van nieuwe technologie.



Waarom algoritmen?

- Nieuwe technologie wordt toegepast bij de diensten van de gemeente Amsterdam, met als doel slimme oplossingen te verkrijgen voor stedelijke vraagstukken.
- De meeste activiteiten van de gemeente hebben directe of indirecte impact: als we een boete opleggen of belasting heffen heeft dat natuurlijk impact, maar ook als we vuilnis ophalen of bomen kappen.
- Daarnaast ontwikkelen we soms ook algoritmen met als doel daarvan te leren; een innovatie kan leiden tot nieuwe inzichten of nieuwe toepassingen voor de stad.
- Algoritmen die impact hebben op burgers of bedrijven, worden opgenomen in het Algoritmeregister.



Wat is een algoritme?

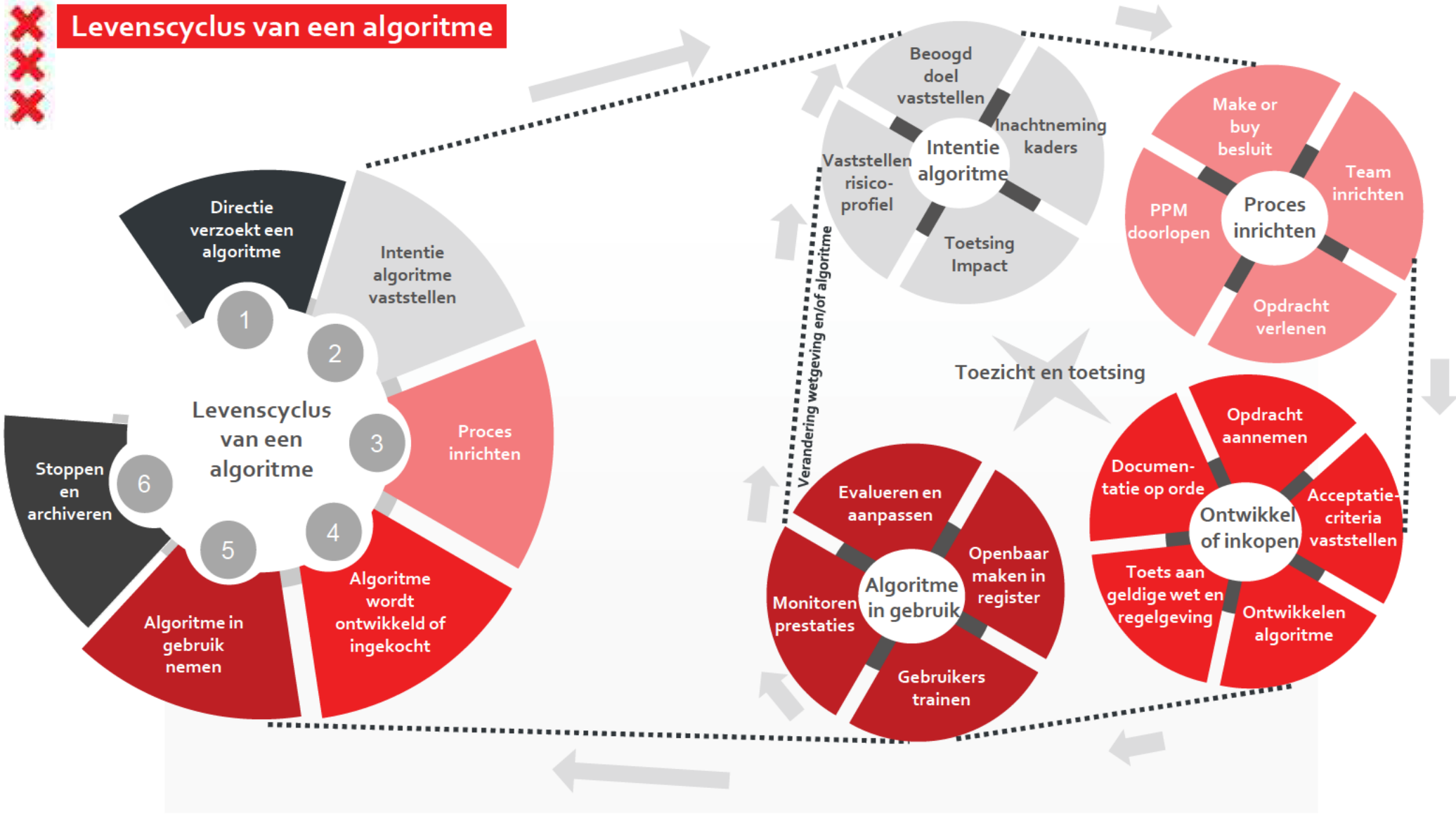
- De definitie die de gemeente hanteert is:
  Software die - door gebruik van data-analyse, statistiek of zelflerende logica - geautomatiseerd voorspellingen doet, beslissingen neemt of adviezen geeft die leiden tot beslissingen van de gemeente die bestuursrechtelijk, privaatrechtelijk en/of feitelijk van aard zijn en die direct of indirect één of meer burgers van de gemeente, bezoekers van de gemeente of bedrijven of andersoortige instellingen in aanmerkelijke mate treffen.
- Binnen deze definitie passen zowel simpele rekenmodellen als 'machine-learning-modellen' en andere vormen van kunstmatige intelligentie (ook wel 'Artificial Intelligence' of AI genoemd).



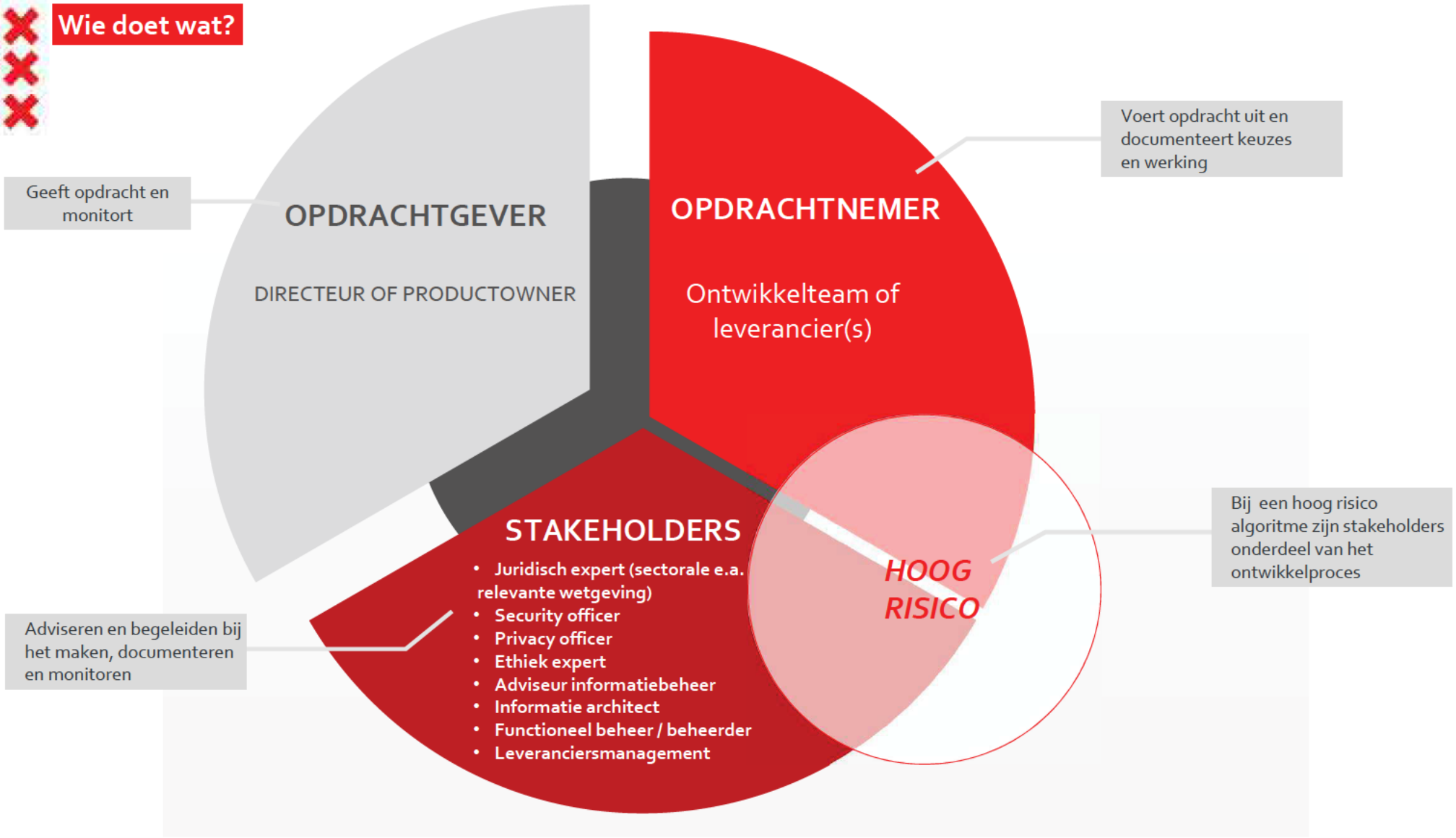
Waar gaat deze notitie over?

- Deze notitie is bedoeld om innovatie door middel van slimme technologie te stimuleren.
- Deze notitie is bedoeld om de mogelijk negatieve effecten te beperken door het beheersen van risico's.
- Deze notitie geeft richting aan de in de EU proposal for Regulation on artificial intelligence opgenomen vereisten voor de ontwikkeling en het gebruik van algoritmen.

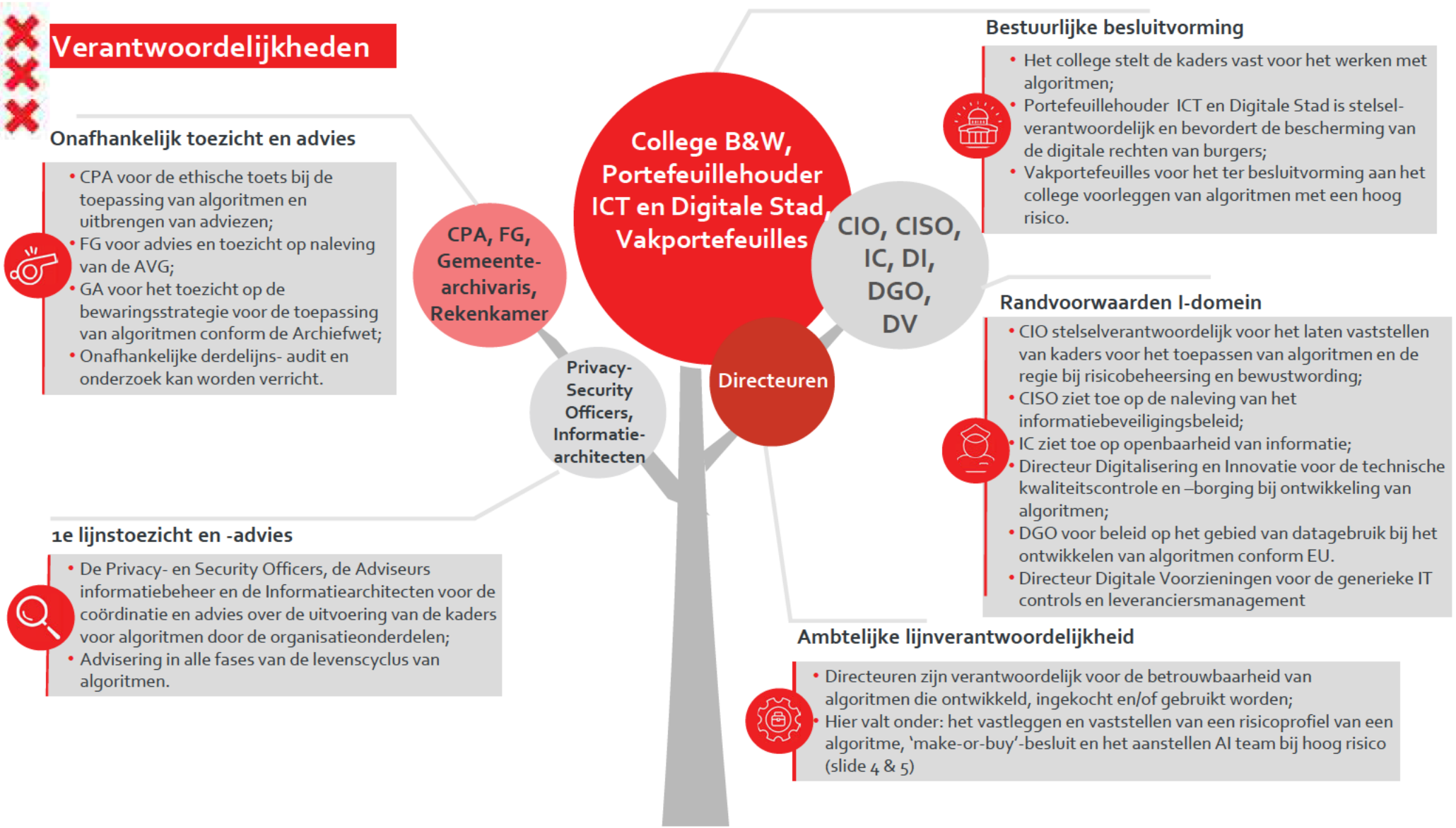
Levenscyclus van een algoritme



Wie doet wat?


Geeft opdracht en monitort
OPDRACHTGEVER
DIRECTEUR OF PRODUCTOWNER
Voert opdracht uit en documenteert keuzes en werking
OPDRACHTNEMER
Ontwikkelteam of leverancier(s)
Bij een hoog risico algoritme zijn stakeholders onderdeel van het ontwikkelproces
HOOG RISICO
STAKEHOLDERS
• Juridisch expert (sectorale e.a. relevante wetgeving)
• Security officer
• Privacy officer
• Ethiek expert
• Adviseur informatiebeheer
• Informatie architect
• Functioneel beheer / beheerder
• Leveranciersmanagement
Adviseren en begeleiden bij het maken, documenteren en monitoren

Verantwoordelijkheden



Onafhankelijk toezicht en advies

- CPA voor de ethische toets bij de toepassing van algoritmen en uitbrengen van adviezen;
- FG voor advies en toezicht op naleving van de AVG;
- GA voor het toezicht op de bewaringsstrategie voor de toepassing van algoritmen conform de Archiefwet;
- Onafhankelijke derdelijns- audit en onderzoek kan worden verricht.

Bestuurlijke besluitvorming

- Het college stelt de kaders vast voor het werken met algoritmen;
- Portefeuillehouder ICT en Digitale Stad is stelsel-verantwoordelijk en bevordert de bescherming van de digitale rechten van burgers;
- Vakportefeuilles voor het ter besluitvorming aan het college voorleggen van algoritmen met een hoog risico.

Randvoorwaarden I-domein

- CIO stelselverantwoordelijk voor het laten vaststellen van kaders voor het toepassen van algoritmen en de regie bij risicobeheersing en bewustwording;
- CISO ziet toe op de naleving van het informatiebeveiligingsbeleid;
- IC ziet toe op openbaarheid van informatie;
- Directeur Digitalisering en Innovatie voor de technische kwaliteitscontrole en –borging bij ontwikkeling van algoritmen;
- DGO voor beleid op het gebied van datagebruik bij het ontwikkelen van algoritmen conform EU.
- Directeur Digitale Voorzieningen voor de generieke IT controls en leveranciersmanagement

1e lijnstoezicht en -advies

- De Privacy- en Security Officers, de Adviseurs informatiebeheer en de Informatiearchitecten voor de coördinatie en advies over de uitvoering van de kaders voor algoritmen door de organisatieonderdelen;
- Advisering in alle fases van de levenscyclus van algoritmen.

Ambtelijke lijnverantwoordelijkheid

- Directeuren zijn verantwoordelijk voor de betrouwbaarheid van algoritmen die ontwikkeld, ingekocht en/of gebruikt worden;
- Hier valt onder: het vastleggen en vaststellen van een risicoprofiel van een algoritme, 'make-or-buy'-besluit en het aanstellen AI team bij hoog risico (slide 4 & 5)

Contactpersonen

Contact

- Voor vragen over de governance algoritme, neem contact op met CIOoffice@amsterdam.nl
- Heb je een algoritme die je openbaar wilt maken, neem contact op met CIOoffice@amsterdam.nl

Gemeente Amsterdam

Taken en verantwoordelijkheden bij het gebruik van Algoritmen door de gemeente Amsterdam

CONCEPTVERSIE 0.14

Innovaties met behulp van technologie

Het college van Amsterdam heeft haar ambitie om aan een vrije, creatieve, en inclusieve stad te werken. Amsterdam geeft daarmee prioriteit aan investeringen in en beleid op (digitale) ontwikkeling. Met als doel het zorgen voor interventies die het leven van Amsterdammers verbeteren; door de negatieve effecten van digitalisering te beperken en de positieve effecten te versterken. Maar hoe laten we de technologie werken voor Amsterdammers?

Nieuwe technologie wordt toegepast in diensten van de gemeente Amsterdam, met als doel slimme oplossingen te verkrijgen voor stedelijke vraagstukken. De meeste activiteiten van de gemeente hebben directe of indirecte impact: als we een boete opleggen of belasting heffen heeft dat natuurlijk impact, maar ook als we vuilnis ophalen of bomen kappen. Daarnaast ontwikkelen we soms ook algoritmen met als doel daarvan te leren; een innovatie kan leiden tot nieuwe inzichten of nieuwe toepassingen voor de stad.

Deze notitie *Taken en verantwoordelijkheden bij het gebruik van Algoritmen door de gemeente Amsterdam* is bedoeld om innovatie door middel van slimme technologie te stimuleren én om de mogelijk negatieve effecten te beperken door het beheersen van risico's. Het geeft richting aan de vereisten voor de ontwikkeling en het gebruik van algoritmen in de voorgestelde EU AI verordening.[1]

Definitie van algoritme en hoog risico

We hanteren bij deze afspraken de volgende definitie om te bepalen of een door de gemeente gebruikt algoritmisch systeem (hierna: algoritme) onder dit kader valt:

> *software die - door gebruik van data-analyse, statistiek of zelflerende logica - geautomatiseerd voorspellingen doet, beslissingen neemt of adviezen geeft die leiden tot beslissingen van de gemeente die bestuursrechtelijk, privaatrechtelijk en/of feitelijk van aard zijn en die direct of indirect één of meer burgers van de gemeente, bezoekers van de gemeente of bedrijven of andersoortige instellingen in aanmerkelijke mate treffen.*

Er zijn op dit moment verschillende definities voor 'algoritme' of 'algoritmische toepassing'. Vanuit de Rijksoverheid wordt gewerkt aan bruikbare en heldere definities. Tot die tijd hanteren we bovenstaande definitie. Deze definitie is overigens grotendeels in lijn met de definitie die is voorgesteld door de Europese Commissie in hun voorstel tot regulering van AI[2].

De definitie is breed en tegelijk precies. Binnen deze definitie passen zowel simpele rekenmodellen als 'machine-learning-modellen' en andere vormen van kunstmatige intelligentie (ook wel 'Artificial Intelligence' of AI genoemd). Als zo'n algoritme gebruikt wordt bij een activiteit met impact op burgers of bedrijven, dan nemen we het algoritme op in het Algoritmeregister en gelden ook de andere instrumenten voor het beheersen van risico's van gebruik van algoritmen. Bij een hoog risico op negatieve impact gelden aanvullende maatregelen voor besluitvorming en betrokken expertisen.[3]

---

[1] Voorstel voor een VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD TOT VASTSTELLING VAN GEHARMONISEERDE REGELS BETREFFENDE ARTIFICIËLE INTELLIGENTIE (WET OP DE ARTIFICIËLE INTELLIGENTIE) EN TOT WIJZIGING VAN BEPAALDE WETGEVINGSHANDELINGEN VAN DE UNIE, d.d. 21 april 2021; hierna: 'voorgestelde EU AI verordening'.

[2] Voorgestelde EU AI verordening, artikel 3 (1): '"artificiële-intelligentiesysteem" (AI-systeem): software die is ontwikkeld aan de hand van een of meer van de technieken en benaderingen die zijn opgenomen in de lijst van bijlage I en die voor een bepaalde reeks door mensen gedefinieerde doelstellingen output kan genereren, zoals inhoud, voorspellingen, aanbevelingen of beslissingen die van invloed zijn op de omgeving waarmee wordt geïnterageerd.'

[3] Volgens de classificatie in de voorgestelde EU AI verordening artikel 6 en 7.

Taken en verantwoordelijkheden

Organisatorisch kader
Het organisatorisch kader voor de taken en verantwoordelijkheden maakt duidelijk wat de rol, taken en verantwoordelijkheden zijn van de betrokken bestuurlijke en ambtelijke actoren op het gebied van het gebruik van algoritmen en rekenmodellen in de gemeente Amsterdam.

Deze notitie beschrijft de verantwoordelijkheden en daarbij horende taken op verschillende niveaus:

Bestuurlijke verantwoordelijkheid:
- Het college van B&W en/of Burgemeester als vakportefeuillehouder
- Stelselverantwoordelijkheid (vakportefeuillehouder ICT en Digitale Stad)

Ambtelijke verantwoordelijkheid:
- Lijnverantwoordelijkheid (eerste lijn)
- Advies (eerste lijn)
- Stelselverantwoordelijkheid (tweede lijn)
- Toezicht en advies (derde lijn, onafhankelijk)

Bestuurlijk

De verantwoordelijkheden en taken van de bestuurders:

College B&W, Burgemeester,
Het college van Burgemeester en Wethouders, dan wel de Burgemeester, ieder vanuit hun eigen taak en bevoegdheid, is verantwoordelijk voor de toepassing van algoritmen die door of namens de gemeente worden uitgevoerd.

Portefeuillehouder ICT
De portefeuillehouder ICT en Digitale Stad heeft de stelselverantwoordelijkheid voor het gebruik van algoritmen en is verantwoordelijk voor:
- het door het college laten vaststellen van kaders voor het werken met algoritmen;
- het initiëren van flankerende activiteiten om de bescherming van persoonsgegevens en digitale rechten van burgers binnen de organisatie te bevorderen, zoals een communicatieplan, training en bewustwording van medewerkers, risicomanagement en de informatie aan Amsterdammers over de wijze waarop de gemeente Amsterdam omgaat met algoritmen en de wijze waarop deze gebruik kan maken van zijn/ haar rechten ingevolge de wet.

Vakportefeuilles
De vakportefeuillehouders zijn -politiek- verantwoordelijk voor:
- De betrouwbaarheid[4] van de algoritmen die worden toegepast door de directies of stadsdelen die binnen zijn/haar eigen vakportefeuille vallen, zoals Dienstverlening, Jeugd, Onderwijs, Zorg,

[4] Deze moeten wettig zijn door te voldoen aan alle toepasselijke wet-en regelgeving, ethisch zijn, door naleving van ethische beginselen en waarden te waarborgen en robuust, zowel vanuit technisch als sociaal oogpunt, zoals omschreven in de Ethische richtsnoeren voor betrouwbare KI van de Onafhankelijke Deskundigengroep op hoog niveau inzake kunstmatige intelligentie opgericht door de Europese Commissie in juni 2018.

Werk, Inkomen en Participatie, Handhaving, Basisinformatie, Onderzoek, Informatie en Statistiek, Wonen;
- Het ter besluitvorming aan het college voorleggen van algoritmen met een hoog risico.

Daar waar de Burgemeester portefeuillehouder is op een domein en het een toepassing is waarvoor het college verantwoordelijk is, is de burgemeester te beschouwen als een vakportefeuillehouder

Ambtelijk, stelselverantwoordelijkheid

De verantwoordelijkheden en taken binnen het I-domein voor de randvoorwaarden voor het werken met algoritmen: het vaststellen van kwalitatieve kaders en het voeren van regie zoals controles, risicomanagement en bewustwording.

Chief Information Officer (CIO)

De Chief Information Officer (CIO) is verantwoordelijk voor het laten vaststellen van kaders voor het toepassen van algoritmen en de regie als het gaat om het beheersen van risico's.

De Chief Information Officer (CIO) heeft de volgende taken:
- In opdracht van de Wethouder ICT en Digitale Stad formuleren en beheren van kaderstellende afspraken en uitgangspunten voor het toepassen van algoritmen, ter bescherming van rechten van burgers en bedrijven, waaronder[5]:
  - Beleid voor het gebruik van algoritmen met definities en verwerkingseisen om de betrouwbaarheid te waarborgen, de definitie van algemene uitgangspunten voor toepassingen met behulp van algoritmen voor de stad en een overzicht van wet- en regelgeving voor de generieke toepassing van algoritmen[6];
  - Een standaard voor het vaststellen van een risicoprofiel;
  - Een verantwoordingsstrategie met betrekking tot input, output, gebruikte technologie en documentatie voor verantwoording;
  - Een referentiearchitectuur voor algoritmen;
  - Vastgestelde ethische principes voor ethisch en verantwoord gebruik van data en algoritmen;
  - Het vaststellen van standaarden voor technische documentatie over de werking van het algoritme[7]
- Bewustwording en opleiding van medewerkers van de gemeente Amsterdam op het gebied van het gebruik van algoritmen, waaronder opleidingen van alle medewerkers werkzaam in het I-domein en kennisontwikkeling en competenties op het gebied van ethiek, beleid voor algoritmen en use cases.
- Het inrichten van risicomanagement ten aanzien van het gebruik van algoritmen, waaronder een jaarlijkse controle op de naleving van de vastgestelde uitgangspunten voor algoritmen en de controle van de naleving van de Taken en verantwoordelijkheden voor het gebruik van algoritmen. Dit gebeurt via het bewaken van de i-portfolio's en het opstellen van concern-rapportages daarover

De CIO zoekt hier bij de samenhang en samenwerking met de Data Governance Office als het gaat om databeleid en dataproducten.

Chief Information Security Officer (CISO)

De CISO ziet toe op de ontwikkeling en naleving van het informatiebeveiligingsbeleid bij de toepassing van algoritmen.

---

[5] Conform artikel 17 van de voorgestelde EU AI verordening.

[6] De kaders en standaarden worden op intranet gepubliceerd op een centrale en toegankelijke plaats.

[7] Conform artikel 11 van de voorgestelde EU AI verordening.

Informatiecommissaris (IC)
De Informatiecommissaris ziet toe op openbaarheid van informatie. Openbaarheid van informatie is het uitgangspunt, tenzij een van de weigeringsgronden op grond van de Wet Openbaarheid van bestuur van toepassing zijn. Deze wetgeving moet ervoor zorgen dat overheidsinformatie beter vindbaar, uitwisselbaar, eenvoudig te ontsluiten en goed te archiveren is. Op het gebied van algoritmen gaat openbaarheid van informatie in het bijzonder over vastleggen in transparantie over het doel en de werking van het algoritme, hoe risico's worden voorkomen en welke factoren belangrijk zijn voor de uitkomst van het algoritme.

Directeur Digitalisering en Innovatie
De Directeur Digitalisering en Innovatie is verantwoordelijk voor juiste registratie van alle vereiste informatie en documentatie over het algoritmische systeem in het i-portfolio.

Directeur Digitale voorzieningen
De Directeur Digitale voorzieningen is verantwoordelijk voor de technische kwaliteitscontrole en -borging bij de begripsvorming, ontwikkeling, modellering, evaluatie en monitoring van de algoritmen, borgt de naleving van technische kwaliteitsvereisten en toetst de documentatie van het Ontwikkelteam. Deze controle vindt in ieder geval plaats voor het in productie nemen van algoritmen met een hoog risico.

Directeur Data
Data en datasets in Amsterdam worden via een centrale functie benaderbaar en worden zo veel mogelijk voor hergebruik beschikbaar gesteld. Uitgangspunt is daarbij, 'Open data, tenzij'. Daarbij wordt gewerkt aan (nieuwe) dataproducten, en het beschikbaar stellen van dataspecialisten.

De taken van directeur de Directeur Data zijn:
- Het signaleren van de toepassing van algoritmen bij data-analyses, met als doel de verantwoordelijke partij daarvan op de hoogte te stellen;
- Het bevorderen van de naleving van taken en verantwoordelijkheden bij het gebruik van algoritmen;
- Beleid op het gebied van datagebruik bij het ontwikkelen van algoritmen.[8]

Ambtelijk, lijnverantwoordelijkheid
De verantwoordelijkheden en taken van de ambtelijke organisatie bij het gebruik van algoritmen. De precieze uitvoering van de taken zal per proces of per algoritme anders ingevuld worden, en is onder meer afhankelijk van de werkwijze in de verschillende stadia van de levenscyclus van het algoritme. Welke taken uitgevoerd dienen te worden is afhankelijk van het risicoprofiel van het algoritme.

Stedelijk directeur
Indien een algoritme directie-overstijgend binnen een bepaald domein toegepast wordt in het kader van de uitvoering van een of meerdere processen bij die directies, is de stedelijk directeur verantwoordelijk voor de betrouwbaarheid van het algoritme, inclusief bijbehorende taken (zie 'Directeuren van de directie/en dagelijks bestuur van het stadsdeel'). Indien het algoritme initieel

[8] Conform artikel 10 van de voorgestelde EU AI verordening.

onder verantwoordelijkheid van een directeur toegepast werd, maar vervolgens opgeschaald wordt binnen het gehele domein, draagt de directeur van de betrokken directie de verantwoordelijkheid over aan de stedelijk directeur.

Directeuren en dagelijks bestuur van het stadsdeel
De betrokken directeur van de directie (namens de Wethouder(s)), directeur OOV (namens de Burgemeester), de Directeur Digitalisering en Innovatie in geval van technische innovatie als doel, dan wel het dagelijks bestuur van het stadsdeel is verantwoordelijk voor de betrouwbaarheid van algoritmen die ontwikkeld, ingekocht en/of gebruikt worden. Daarbij hoort de uitvoering van specifieke taken. De volgorde van deze taken kan per keer verschillen. Als het gaat om een opgave of een programma waarbij algoritmen worden ingezet, is de opdrachtnemer voor de opgave of de programmadirecteur verantwoordelijk voor de uitvoering van deze taken. De directeur dan wel het dagelijks bestuur van een stadsdeel kan ook een productowner opdracht geven om deze taken namens hem uit te voeren. De directeur dan wel het dagelijks bestuur van het stadsdeel blijft altijd eindverantwoordelijk.

De taken zullen zowel bij nieuwe algoritmen als bij (grote) wijzigingen uitgevoerd moeten worden:

<u>Doelen, risico's en besluiten vastleggen</u>
- Het vaststellen en vastleggen van het beoogde doel; hiertoe moet voor alle betrokkenen documentatie beschikbaar zijn waaruit minimaal blijkt wat het beleidsdoel of de wettelijke taak is waaraan het algoritme een bijdrage moet leveren, wat het specifieke probleem of vraagstuk is waar algoritmische ondersteuning bij gewenst is en wat het gewenste maatschappelijk nut is;
- Het vastleggen van het risicoprofiel[9] van het algoritme voordat een beslissing wordt genomen over het ontwikkelen of inkopen ervan. Hierbij wordt de benodigde technische en juridische expertise betrokken;
- Het vastleggen en het nemen van een besluiten om wel of geen algoritme te gebruiken, inclusief de overwegingen daartoe, waaronder het besluit om te ontwikkelen, testen en te implementeren in de bedrijfsvoering;
- Het besluit over de toepassing van algoritmen wordt genomen met inachtneming van de vastgestelde kaders en het gemeentelijk beleid op het gebied van algoritmen, principes voor ethisch en verantwoord gebruik van data en algoritmen en de kaders voor gegevensbescherming, openbaarheid van informatie en informatiebeveiliging en archivering;
- Het voorleggen van risicovolle of politiek gevoelige algoritmes aan de vakportefeuillehouder die het voorstel over de inzet van het algoritme vervolgens voorlegt aan het college.

<u>Procesvoorbereiding</u>
- Het Project Portfolio Management-proces of vergelijkbaar proces bij nieuwe toepassingen van algoritmen doorlopen en borgen dat het project in lijn blijft met de doelstelling, risico-inschatting en het besluit;
- Het toetsen van de impact van het beoogde algoritme bij inwoners en ondernemers van de stad, zoals gesteld in de Datastrategie data van de stad, voor de stad.
- Onderzoeken en besluiten of een algoritme hergebruikt, ontwikkeld of ingekocht moet worden (make-or-buy-besluit);
- Indien algoritme in eigen beheer ontwikkeld wordt: een opdracht verlenen aan een ontwikkel-team en het beschikbaar stellen van de benodigde capaciteit en de samenstelling van het ontwikkel-team uitgaande van het vastgestelde beoogde doel; onderstaande taken voor het 'ontwikkel-team' zijn onderdeel van die opdracht.

[9] Tot een hoog risico behoren algoritmen als zodanig geclassificeerd in de voorgestelde EU AI verordening artikel 6 en 7.

- Indien het algoritme ingekocht wordt: een opdracht verlenen aan een opdrachtnemer en het beschikbaar stellen van de benodigde capaciteit voor de begeleiding van de opdracht;
- Zorgt ervoor dat er gebruikersinstructies zijn opgesteld en dat menselijk toezicht op het algoritme effectief kan worden uitgevoerd[10];
- Een akkoord op de door het ontwikkel-team of opdrachtnemer opgestelde acceptatiecriteria (ofwel 'definition of done') volgens de vastgestelde standaard voor de start van het ontwikkelproces (zie: 'Ontwikkel-team').

<u>Ontwikkelen of inkopen</u>

- Het betrekken van stakeholders en eindgebruikers van het algoritme in het ontwikkelproces;
- Het inwinnen van advies en begeleiding bij het ontwerp, het modelleren en monitoren van de toepassing op basis van het risicoprofiel:
  - Bij algoritmen zonder hoog risico wordt technische expertise, juridische expertise, ethische expertise, de security- en de privacy-officer en de expertpool architectuur- en recordmanagement geraadpleegd;
  - Bij hoog-risico-algoritmen moet voorgaande expertise onderdeel zijn van het ontwikkelproces als stakeholders (bij een scrum/agile-aanpak) of geïntegreerd in het team (bij een watervalaanpak);
- Bij hoge risico's wordt aangetoond door middel van een Kunstmatige Intelligentie Impact Assessment -of een vergelijkbaar instrument- en aanvullende analyses dat de betrouwbaarheid van het algoritme voldoende is gewaarborgd en ook worden de te nemen maatregelen gemotiveerd;
- Een toets van het algoritme aan de referentiearchitectuur voor algoritmen;
- Het borgen van privacy by design, security by design, archivering by design, het gebruik van basisregistraties in het ontwerp en ethics bij design op basis van input, output, gebruikte technologie en documentatie voor verantwoording, waaronder de verplichtingen op grond van de Algemene verordening gegevensbescherming (zoals inschrijving in het Avg-register, het verrichten van een privacy impact assessment en een privacyverklaring), de Baseline Informatiebeveiliging Overheid (BIO),de Archiefwet (documentatieplichten) en de toepassing van verschillende wetten over de Basisregistraties;
- Het (periodiek) consulteren van een expert met kennis van relevante sectorale wet- en regelgeving en de algemene beginselen van behoorlijk bestuur als deze geen onderdeel is van het ontwikkel-team en het vastleggen en actueel houden van specifieke wet- en regelgeving die van toepassing is: het gaat dan om een toets of de logica, de werking en gebruikte data met betrekking tot het algoritme rechtmatig zijn;
- Het consulteren van eerstelijns adviseurs op het gebied van gegevensbescherming (privacy officers), informatiebeveiliging (security officers), en informatiebeheer (adviseurs informatiebeheer en architectuur als deze geen onderdeel zijn van het ontwikkel-team;
- Het treffen van passende technische en organisatorische maatregelen die noodzakelijk zijn voor betrouwbare algoritmen, het gaat dan om robuustheid, nauwkeurigheid en cyberbeveiliging;
- Bij de uitvoering door of inkoop bij derde partijen: de controle van de kwaliteit en volledigheid van de in het kader van de standaardclausules voor de inkoop van algoritmen geleverde informatie over de kwaliteit van de data en over de transparantie, kwaliteit, risicomanagementstrategieën en beheer van de algoritmische toepassing;
- Bij hoog-risico-algoritmen: indien er sprake is van afwijking van de ethische standaard voor de toepassing van data of algoritmen, de regelgeving omtrent de verwerking van persoonsgegevens of algoritmen met een hoog risico, zal de directeur/dagelijks bestuur voordat een beslissing wordt genomen over nieuwe of wijzigingen van bestaande

[10] Conform artikel 13 en 14 van de voorgestelde EU AI verordening.

toepassingen van algoritmen tevens advies inwinnen bij de Commissie Persoonsgegevens Amsterdam.

Transparante communicatie

- Het maken van een expliciete afweging ten aanzien van de openbaarheid van informatie over het gebruik van algoritmen voor burgers;
- Het inschrijven van algoritmen in het register voor algoritmen en het bijhouden van wijzigingen;
- Communicatie in heldere taal aan burgers over de toepassing en de werking van algoritmen, waaronder in elk geval vermelding van de noodzakelijke informatie in begrijpelijke taal in een besluit waarbij in de voorbereiding een algoritme is gebruikt, zodat betrokken burgers daartegen kunnen opkomen in bezwaar of beroep;
- Bij hoog risico algoritmen wordt in overleg met woordvoering besloten of actieve communicatie nodig is om burgers en bedrijven goed te informeren (persbericht).

Gebruik, monitoring en evaluatie

- Garanderen dat voldoende kennis en competenties beschikbaar zijn bij gebruikers van het algoritme om de output van het algoritme juist te kunnen interpreteren; hiervoor wordt een beheerplan opgesteld;
- De controle of aan de prestatiecriteria (zie ook 'acceptatiecriteria') blijvend is voldaan, documentatie en validaties daarvan door middel van het laten uitvoeren en beoordelen van tests voordat de nieuwe of gewijzigde algoritme toepassing in de productieomgeving wordt geïmplementeerd;
- Bij de uitvoering door derde partijen: de periodieke controle van afgesproken contractvoorwaarden, servicelevels en assurancerapportages van de leverancier;
- Het rapporteren over de naleving van het kader voor algoritmen aan de CIO, de Functionaris gegevensbescherming en de Gemeentearchivaris;
- Dat er een proces is ingericht om de prestaties van de algoritme te monitoren gedurende de levenscyclus;
- Het vastleggen van gevallen waarin van de uitkomst van een algoritme expliciet is afgeweken, en de redenen waarom, om deze input vervolgens het algoritme te evalueren;
- Het sturen op bewustzijn en naleving van het beleid bij medewerkers van het organisatieonderdeel.

Overige taken

- Het -indien aan de orde- opstellen en via de vakwethouder aan het college ter besluitvorming aanbieden van uitwerkingen van het kader voor de toepassing voor algoritmen.

Ontwikkel-team en stakeholders

Onderstaande taken zijn onderdeel van de opdracht van de directeur of dagelijks bestuur van het stadsdeel en vallen daarmee onder de verantwoordelijkheid van die directeur of dagelijks bestuur van het stadsdeel. De taken worden uitgevoerd door een divers en multidisciplinair ontwikkel-team, waarvan de samenstelling afhankelijk is van het risicoprofiel van het te ontwikkelen algoritme:

- Bij algoritmen zonder hoog risico wordt technische expertise, juridische expertise, ethische expertise, de security- en de privacy-officer en de expertpool architectuur- en recordmanagement geraadpleegd wanneer dat noodzakelijk is;
- Bij hoog-risico-algoritmen moet deze expertise onderdeel zijn van het ontwikkelproces als stakeholders (bij een scrum/agile- of DevOps-aanpak) of geïntegreerd in het team (bij een watervalaanpak).

De medewerkers van het ontwikkelteam hebben de volgende taken:

- Het verhelderen van de opdracht van de directeur middels een intake, met als doel om gelijke verwachtingen te creëren tussen opdrachtgever en opdrachtnemer over het beoogde doel, het maatschappelijk nut en de omvang van de opdracht;
- Het uitvoeren van een toets aan de referentiearchitectuur voor algoritmen;
- Een toets aan artikel 1 uit de Grondwet (GW)/artikel 14 Europees Verdrag voor de Rechten van de Mens (EVRM) en toepassing van de algemene beginselen van behoorlijk bestuur: het gaat dan om een toets of de logica, de werking en gebruikte data met betrekking tot het algoritme rechtmatig zijn en er geen sprake is van vooringenomenheid [redacted]
- Het laten opstellen van een overzicht van relevante sectorale wet- en regelgeving en het vastleggen en actueel houden van specifieke wet- en regelgeving die van toepassing is: het gaat dan om een toets of de logica, de werking en gebruikte data met betrekking tot het algoritme rechtmatig zijn en er geen sprake is van vooringenomenheid [redacted]
- Een toets op geldende wet- en regelgeving met betrekking tot automatische besluitvorming[11] en menselijk toezicht[12] door een stakeholder of teamlid met de benodigde expertise;
- De uitvoering van de taken die door het ontwikkel-team worden uitgevoerd op het gebied van begripsvorming, ontwerp, modelleren, trainen, testen, valideren, evalueren, accepteren en implementeren, monitoren en door ontwikkelen van algoritmen, een en ander volgens het in de gemeente Amsterdam ontwikkelde standaard ontwikkelproces voor algoritmes en de vastgestelde borgende maatregelen tijdens de fases in dit proces, waaronder een verplichte analyse op overfitting en underfitting en/of [redacted] en de controle op de juistheid en volledigheid van de verwerking;
- Het testen van het algoritme in de loop van het ontwikkelingsproces en in ieder geval voordat het systeem in gebruik wordt genomen aan de hand van vooraf vastgestelde standaarden en probabilistische drempels die passend zijn voor het beoogde doel;
- Ondersteuning en advies bij het opstellen en onderhouden van Kunstmatige Intelligentie Impact Assessments of soortgelijke verplichte ethische toetsen en het bepalen van aanvullende risicobeheersingsmaatregelen in het ontwerp van de algoritme naar aanleiding, zoals dat het algoritme tijdens de levensduur kan omgaan met fouten en dat er een 'stop-knop' is;
- Het daarmee vaststellen en analyseren van de bekende en te voorziene risico's inclusief gevolgen voor mensenrechten en de afweging van ethische principes, het evalueren en monitoren daarvan gedurende de levenscyclus van het algoritme;
- De risico's worden zo veel mogelijk uitgesloten of beperkt door middel van een adequaat ontwerp en adequate ontwikkeling:
  - waar passend worden adequate maatregelen voor beperking en controle genomen in verband met risico's die niet kunnen worden uitgesloten;
  - er wordt toereikende informatie verstrekt aan opdrachtgever over bedoelde risico's;
  - er wordt waar passend voorzien in een voorstel voor de opleidingen van gebruikers.
- Het vastleggen van de acceptatiecriteria (ofwel: 'definition of done') waarin is bepaald aan welke eisen de oplossing moet voldoen (inclusief juridische, ethische en technische vereisten) en een relatie wordt gelegd met de omschrijving van het beoogde doel volgens de daarvoor vastgestelde standaard, en deze laten goedkeuren door de opdrachtgever;
- Het aangetoond scheiden van training-, test- en validatiedata;
- Voor de databronnen zo veel mogelijk borgen dat er geen beperkingen zijn ten aanzien van de rechten op de data;
- Het gebruik van data en databeheer voor het trainen en modelleren van het algoritme gebeurt in overeenstemming met passende praktijken voor databeheer[13]

[11] Als bedoeld in artikel 22 Algemene Verordening Gegevensbescherming
[12] Conform de eisen in artikel 14 van de voorgestelde EU AI verordening.
[13] Onder verwijzing naar de criteria van artikel 10 van het voorstel van de voorgestelde EU AI verordening.

- Een toets aan dataminimalisatie en een expliciete afweging met betrekking tot proportionaliteit door een stakeholder of teamlid met de benodigde expertise;
- Het borgen van de nauwkeurigheid, robuustheid en cyberbeveiliging van de toepassing [14]
- Een toets op uitlegbaarheid en een expliciete afweging tussen de uitlegbaarheid van het model en de prestatie van het model die wordt voorgelegd aan de opdrachtgever door een stakeholder of teamlid met de benodigde expertise; de werking ervan moet in elk geval voldoende transparant zijn om gebruikers in staat te stellen de output van het systeem te interpreteren en op passende wijze te gebruiken;
- Ervoor zorgen dat algoritmen vergezeld gaan van gebruiksinstructies in een passend digitaal of ander formaat dat beknopte, volledige, juiste en duidelijke informatie bevat die relevant, toegankelijk en begrijpelijk is voor gebruikers/opdrachtgever;
- Het documenteren van verantwoordingsstukken die vereist zijn volgens de door de CIO vastgestelde verantwoordingsstrategie op basis van het risicoprofiel van het algoritme. Daaronder valt bij een hoog-risico-algoritme in ieder geval:
  - het geven van inzicht in de gemaakte keuzes en de gehanteerde aannames;
  - de categorieën van data die zijn gebruikt bij het ontwikkelen van het algoritme;
  - de wijze waarop in menselijke tussenkomst is voorzien;
  - de gebruikte methode(n) om risico's te identificeren;
  - de geïdentificeerde risico's en de maatregelen die zijn genomen om de risico's te mitigeren, waaronder wat eventuele bekende of te voorziene omstandigheden zijn in verband met het gebruik van het algoritme in overeenstemming met het beoogde doel ervan of in een situatie van redelijkerwijs te voorzien misbruik;
  - een beschrijving van de maatregelen die zijn getroffen om minimaal de volgende zaken in de data te voorkomen: sociaal geconstrueerde vertekening; onnauwkeurigheden; fouten; vergissingen; [redacted] (ongewenste vooringenomenheid);
  - de partijen die betrokken zijn geweest als opdrachtgever en bij het ontwikkelen van het algoritme en hun rol en taken;
  - de noodzakelijke technische documentatie[15];
  - de noodzakelijke logging[16].
- Het openbaar (laten) publiceren van het model (code en werking), tenzij er gegronde redenen zijn om daarvan af te zien, zoals de uitzonderingsgronden van de Wet openbaarheid van bestuur of een beperking in de eigendoms- of gebruiksrechten inclusief een expliciete afweging over het licentiëren van gebruiksrechten.

Directeur Digitale voorzieningen
De directeur Digitale voorzieningen is verantwoordelijk voor de uitvoering van alle generieke IT controls die worden uitgevoerd, waaronder maar niet beperkt tot:

- Het vaststellen van een security management-strategie die uitgaat van security by design.
- Het beschikbaar stellen van aparte omgevingen en middelen voor ontwikkeling, QA / test en productie, zodat het testen wordt uitgevoerd met een due diligence in de omgeving identiek aan productie en een maandelijkse controle van de IT- omgeving en vastleggen dat deze omgevingen identiek zijn aan elkaar;
- Het inrichten van de noodzakelijke logging[17];
- Het maandelijks monitoren van de prestaties van de algoritmen in relatie tot de beschikbaarheid en capaciteit van de IT-omgeving;

[14] Conform artikel 15 van de voorgestelde EU AI verordening.

[15] Conform artikel 11, lid 1 en bijlage IV van de voorgestelde EU AI verordening.
[16] Conform artikel 12 van de voorgestelde EU AI verordening.
[17] Conform artikel 12 van de voorgestelde EU AI verordening.

- Gebruikmaking van twee-factor authenticatie bij hoog-risico-zones, periodiek wijzigen van wachtwoorden, vergrendelen van accounts bij inactiviteit, en blokkeren na een vooraf ingesteld aantal foutieve inlogpogingen;
- Generieke beheeraccounts zijn geblokkeerd of alleen te gebruiken onder registratie en toezicht;
- Controle of het wachtwoordbeheer actief is en zijn de wachtwoorden van geschikte kwaliteit zijn;
- Voor het inrichten van toegangsrechten gelden naamgevingsconventies en een systematiek van toegangsrechten per gebruikersgroep en/of rol ter bevordering van de onderhoudbaarheid van het beheer.

Leveranciersmanagement
Leveranciersmanagement is verantwoordelijk voor:

- Het onderwerpen van de toepassingen die worden ingekocht aan eisen op het gebied van beheersing op het gebied van architectuur, informatiebeveiliging, privacy en informatiebeheer, gebruikersrechten, wijzigingen, continuïteit en capaciteit.
- Borgen dat de overeenkomst met derde partijen clausules bevat voor:
    a. de eigendom van IE (dat wil zeggen intellectueel eigendom van gegevens, code, modellen en 'leren');
    b. overeenkomsten die zorgen voor toegang tot de code wanneer dit zou moeten;
    c. overeenkomsten die zorgen voor toegang tot de data wanneer dit zou moeten ondersteuningseisen en de garanties;
    d. het van toepassing verklaren van standaardclausules van de gemeente Amsterdam voor de inkoop van algoritmen.
- Het bijhouden van een overzicht van alle algoritmen die zijn ingekocht bij derde partijen.
- Het treffen van waarborgen dat dezelfde beheersingsniveaus worden toegepast als bij algoritmen die in eigen beheer worden ontwikkeld, door voorafgaand te eisen dat
    a. per leverancier de afhankelijkheidsrisico's in kaart zijn gebracht, en waar van toepassing bijpassende beheersingsmaatregelen zijn getroffen om die risico's te mitigeren;
    b. per leverancier een contract is opgesteld, inclusief periodieke rapportageverplichting door middel van een service level agreement, en bijpassende rapportages.

Functioneel beheer/keteninformatiemanager
Tot de taken van de functioneel beheerders behoren in ieder geval:

Stedelijke standaardprocessen voor functioneel beheer:

1. Meldingenproces via het Servicepunt (vragen gebruikers; gebruiksondersteuning, incidenten, aanvragen voor autorisatie, klachten en complimenten)
2. Het wijzigingenproces (standaard-, eenvoudige en uitgebreide wijzigingen);
3. Adviseren in projecten over het in beheer name proces.

En:

4. Dat gebruikerstoegang tot het platform en/of de oplossing, met inbegrip van de opslagplaatsen van de relevante gegevens, logboekbestanden en andere relevante bestanddelen is ingeregeld en toegewezen op basis van 'need to have';
5. Verificatiecontroles op gebruikers accounts, waarbij functiewijzigingen en uitdiensttredingen worden bewaakt voor aanpassen van de toegangsrechten en voor intrekken van de identiteits- en authenticatiemiddelen;
6. De monitoring en beoordeling van de prestaties van algoritmen die in beheer zijn genomen;

7. Onderhoud en beheer van de toepassing, waaronder versiebeheer, het bewaren van loginformatie over de werking van het algoritme en toegankelijk maken totdat de bewaartermijnen zijn verstreken.
8. Toegangsbeveiliging is geïmplementeerd volgens het principe 'niets mag, tenzij nodig' op alle IT-middelen;
9. Controleren of wijzigingen in de code van het algoritme op een gecontroleerde wijze worden uitgevoerd, door het testen en autoriseren van wijzigingen. Er vindt periodieke monitoring plaats op de verwerkte wijzigingen;
10. In geval van grote wijzigingen: het documenteren van verantwoordingsstukken over het proces dat is gevolgd bij de wijziging van het algoritme en de in dat kader gebruikte data. Daaronder valt bij een hoog-risico-algoritme in ieder geval: zie taken 'ontwikkel-team ';
11. Toets of gebruikers op applicatieniveau en daarbuiten dezelfde rechten en beperkingen hebben;
12. Indien gekozen wordt voor een Devops- methode, deelname aan het Devops-team.
13. Dat voldoende kennis en competenties beschikbaar zijn om algoritmes in productie te beheren.

Tot de taken van de keteninformatiemanagers behoren in ieder geval:
1. Operationeel leveranciers- en contractmanagement waaronder opdrachten aan ICT en leveranciers,
2. Dat er een actuele DAP (Dossier Afspraken en Procedures) en Service Level Agreement is van de toepassing en het bewaken van de afspraken;
3. Financieel management, behoefte-management en planning en control.

Eerstelijnstoezicht en -advies

De Privacy- en security officers, de Adviseurs informatiebeheer en de Informatiearchitecten zijn belast met de coördinatie en advies over de uitvoering van de kaders voor algoritmen door de organisatieonderdelen. Zij leveren een actieve bijdrage bij de ontwikkeling van bewustzijn en kennis van het beleid bij medewerkers op het gebied van algoritmen en de advisering in alle fases van de levenscyclus van algoritmen.
Ook rapporteren zij over de naleving van wet- en regelgeving en het kader algoritmen desgevraagd aan de CIO FG/Gemeentearchivaris.

Tot de taken van de Privacy officer behoren in ieder geval:
- Het adviseren over nieuwe of aangepaste toepassingen in het licht van wettelijke verplichtingen in de Avg en de naleving van het kader algoritmen;
- Een toets aan artikel 22 Algemene verordening gegevensbescherming en artikel 9 Algemene verordening gegevensbescherming; geen automatische besluitvorming of documentatie waarom het is toegestaan,
- Hanteren van het recht om niet onderworpen te zijn aan geautomatiseerde besluitvorming (indien van toepassing), en een vastgelegde en met betrokkenen gecommuniceerde procedure als dat wel is toegestaan.
- Vaststellen wie de verwerkingsverantwoordelijke en verwerker is van de persoonsgegevens met betrekking tot het algoritme en de daarbij gebruikte data en het vaststellen van de rechtmatige grondslag voor het verwerken van persoonsgegevens door het algoritme;
- Adviseren over data protection impact assessments/ risicoanalyses van de beveiliging;
- Toets of profilering wordt toegepast in de zin van artikel 4 Avg en benoemen van de risico's;

- Eerstelijns toezicht op de verwerking van persoonsgegevens bij de toepassing van algoritmen;
- Advies over de verplichting om de Autoriteit Persoonsgegevens voorafgaand te raadplegen over risico's indien de AVG dit vereist.

Tot de taken van de Security officer behoren in ieder geval:
- Het adviseren over de beveiliging van nieuwe of aangepaste toepassingen aan de hand van de Baseline Informatiebeveiliging Overheid (BIO);
- Toets of er een functiescheiding tussen aanvragen, autoriseren en verwerken van wijzigingen in gebruikersaccounts en toegangsrechten is, toets of functiewijzigingen en uitdiensttredingen worden bewaakt voor aanpassen van de toegangsrechten en voor intrekken van de identiteits- en authenticatiemiddelen;
- Toetsen of het algoritme is beveiligd, zodat er geen risico is op ongeautoriseerde toegang, wijziging, beschadiging en/of dataverlies;
- Toetsen of er back-ups van het algoritme gemaakt en het algoritme en de data hersteld kunnen worden;
- Toepassen van security by design;
- Het uitoefenen van het eerstelijns toezicht op de beveiligingsmaatregelen bij de toepassing van algoritmen, waaronder maar niet beperkt tot controle op malwaredetectie, patchbeleid en het beoordelen van penetratietesten;
- Adviseren over risicoanalyses van de beveiliging;
- Jaarlijkse controle of de beveiligingsparameters voldoen aan de security eisen.

Tot de taken van de Adviseur informatiebeheer behoren in ieder geval:
- Advies over bewaartermijnen en toepassing verantwoordingsstrategie: de bewaartermijn is afgestemd op de eisen van wet- en regelgeving en op de controle- en auditcyclus van de betreffende gegevens en geïmplementeerd.
- Onder de taken van de Adviseur informatiebeheer valt in elk geval het vernietigen, overbrengen en beschikbaar stellen van informatie over algoritmes, waaronder gebruikte input en outputdata.

Tot de taken van de Informatiearchitect behoren in ieder geval:
- Advies en begeleiding bij de toets aan de referentiearchitectuur voor algoritmen, en het opstellen van een algemene- en doelbeschrijving voor de toepassing.

Onafhankelijk advies en toezicht

Commissie Persoonsgegevens Amsterdam (CPA)
Het college van Burgemeester en Wethouders heeft de Commissie Persoonsgegevens Amsterdam ingesteld. Deze commissie adviseert het college omtrent de gegevensverwerking in breedste zin. Daaronder wordt ook begrepen de ethische toets bij de toepassing van algoritmen. De werkwijze van de commissie en met name het houden van -in beginsel- openbare vergaderingen en uitbrengen van adviezen, draagt bij aan de transparantie rondom de verwerking van persoonsgegevens bij de toepassing van algoritmen door de gemeente.

De CPA heeft de volgende taak:

Bij afwijking van de ethische principes voor data en algoritmen of bij vragen over de toepassing van algoritmen adviseert de CPA over de toepassing met inachtneming van de wet- en regelgeving, de maatschappelijke en ethische inzichten en technologische ontwikkelingen. Indien de FG en de CPA conflicterende adviezen of verschillen van inzicht hebben met betrekking tot de bescherming van persoonsgegevens bij de toepassing van algoritmen, is het advies van de FG leidend. In dat geval wordt het besluit over de toepassing van het algoritme door de betrokken directeur dan wel het dagelijks bestuur van het stadsdeel voorgelegd aan de verantwoordelijke bestuurlijke portefeuillehouder conform deze notitie.

Functionaris Gegevensbescherming
De Functionaris Gegevensbescherming (FG) is de interne toezichthouder voor de naleving van de Algemene verordening gegevensbescherming en brengt advies uit over de naleving van het stedelijk kader verwerken persoonsgegevens en verplichtingen ingevolge de wet.

De Functionaris Gegevensbescherming heeft onder meer de volgende taken met betrekking tot algoritmen:

1. Advies over verplichtingen uit hoofde van de AVG en andere gegevensbeschermingsbepalingen;
2. Toezien op het naleven van de AVG en andere gegevensbeschermingsbepalingen en van het beleid m.b.t. de bescherming van persoonsgegevens (i.c. het stedelijk kader);
3. Desgevraagd advies verstrekken m.b.t. de gegevensbeschermingseffectbeoordeling (data protection impact assessment) en toezien op de uitvoering daarvan;
4. Met de toezichthoudende autoriteit (Autoriteit Persoonsgegevens) samenwerken;
5. Optreden als contactpunt voor de toezichthoudende autoriteit inzake met verwerking van persoonsgegevens verband houdende aangelegenheden.

Gemeentearchivaris
De Gemeentearchivaris is verantwoordelijk voor het toezicht op de bewaringsstrategie voor de toepassing van algoritmen conform de Archiefwet. Het gaat daarbij om het documenteren van input, output, gebruikte technologie en documentatie voor verantwoording en bewaring/vastlegging.

Auditor en Rekenkamer
Onafhankelijke derdelijns- audits en onderzoek worden verricht dan wel in opdracht van de gemeente Amsterdam, door een onafhankelijke auditor, om vast te stellen of voldaan is aan alle vereisten dan wel eigenstandig door de Rekenkamer Metropool Amsterdam.

Rapportage en escalatielijn is als volgt:
De rapportage en escalatielijn is als volgt: Algoritme-team/Security Officer -> CTIO/CISO/IC/->GMT->verantwoordelijk bestuurlijk portefeuillehouder én
Adviseur informatiebeheer->Gemeentearchivaris_>verantwoordelijk bestuurlijk portefeuillehouder:
Privacy Officer->FG->Gemeentesecretaris >verantwoordelijk bestuurlijk portefeuillehouder
Jaarlijks brengt de CIO verslag uit aan het college en de raad.

CONTRACT-VOORWAARDEN

Contractbepalingen in aanvulling op de GIBIT voor het rechtvaardig gebruik van Algoritmische toepassingen

Definities

Algoritmische toepassing: "software waarmee op geautomatiseerde wijze voorspellingen worden gedaan, beslissingen worden genomen en/of adviezen worden gegeven door gebruik te maken van data-analyse, statistiek en/of zelflerende logica."

Audit: de in artikel 8 van deze Contractbepalingen bedoelde audit.

Beoogde gebruik: "het oplossen van de door de Opdrachtgever voorafgaand aan het gebruik van de Algoritmische toepassing gedefinieerde probleem of problemen."

Besluiten: "besluiten van de gemeente die bestuursrechtelijk, privaatrechtelijk en/of feitelijk van aard zijn en die direct of indirect één of meer burgers van de gemeente, bezoekers van de gemeente of bedrijven of andersoortige instellingen die in de gemeente zijn gevestigd in aanmerkelijke mate treffen."

Contractbepalingen: "deze onderhavige bepalingen voor Opdrachtgevers voor het rechtvaardig gebruik van Algoritmische toepassingen."

GIBIT: "de Gemeentelijke inkoopvoorwaarden bij IT van de gemeente Amsterdam (geregistreerd bij de KvK d.d. 04 september 2017, KvK nr. 34366966)."

ICT-prestatie: "alle door Leverancier op grond van de Overeenkomst te leveren goederen (waaronder begrepen Gebruiksrechten) en diensten."

Leverancier: "de partij waarmee Opdrachtgever een Overeenkomst gesloten heeft."

Opdrachtgever: "de partij ten behoeve waarvan de Overeenkomst wordt gesloten."

Overeenkomst: "de afspraken tussen Opdrachtgever en Leverancier met betrekking tot de levering van de ICT Prestatie, waarvan de GIBIT onderdeel uitmaakt. Overeenkomsten die worden gesloten onder een mantel- of raamovereenkomst worden voor deze Contractbepalingen steeds als afzonderlijke Overeenkomst beschouwd."

Dit document is een concept, opgesteld in het kader van het traject 'Grip op algor tmes', gein tieerd door Gemeente Amsterdam. Samen met experts, betrokkenen en andere overheden wil Gemeente Amsterdam contractvoorwaarden en inkoopvoorwaarden voor eerlijke en transparante algor tmes te ontwikkelen. Neem voor meer informatie contact op met [redacted]

Procedurele transparantie: "het verstrekken van informatie over het doel van de Algoritmische toepassing en het proces dat is gevolgd bij de ontwikkeling en toepassing van de Algoritmische toepassing en de in dat kader gebruikte data, waaronder in ieder geval moet worden begrepen het geven van inzicht in de gemaakte keuzes en de gehanteerde aannames, de categorieën van data die zijn gebruikt bij het ontwikkelen van de Algoritmische toepassing, de wijze waarop in menselijke tussenkomst is voorzien in de Algoritmische toepassing, de gebruikte methode om risico's te identificeren, de geïdentificeerde risico's en de maatregelen die zijn genomen om de risico's te mitigeren en de partijen die betrokken zijn geweest bij het ontwikkelen van de Algoritmische toepassing en hun rol."

Rapport: een rapport als bedoeld in artikel 8.2 van deze Contractbepalingen

Technische transparantie: "het verstrekken van informatie aan de hand waarvan de Opdrachtgever inzicht kan krijgen in de technische werking van de Algoritmische toepassing, waaronder in ieder geval kan worden begrepen het verstrekken van de broncode van de Algoritmische toepassing, de technische specificaties die zijn gebruikt bij de ontwikkeling van de Algoritmische toepassing, de bij de ontwikkeling van de Algoritmische toepassing gebruikte data, technische informatie over de wijze waarop de bij de ontwikkeling van de Algoritmische toepassing gebruikte data zijn verkregen en bewerkt, informatie over de gehanteerde ontwikkelmethode en het doorlopen ontwikkelproces, motivatie van de keuze voor een bepaald model en bijbehorende parameters en informatie over de prestaties van de Algoritmische toepassing."

Uitlegbaar(heid): "Het op individueel niveau kunnen uitleggen waarom een Algoritmische toepassing tot een bepaalde beslissing of uitkomst komt. Tenzij Partijen uitdrukkelijk anders overeenkomen, vormt daar in ieder geval onderdeel van dat duidelijk is wat de belangrijkste factoren zijn op basis waarvan een Algoritmische toepassing tot een bepaalde uitkomst is gekomen en welke wijzigingen in de input moeten worden doorgevoerd om tot een andere uitkomst te komen. Onder het Uitlegbaar maken van een Algoritmische toepassing valt mede het verstrekken van alle (technische) informatie die nodig is om in een bezwaarprocedure, een beroepsprocedure of een andere juridische procedure de totstandkoming van een Besluit toe te lichten en om de wederpartij en eventuele andere belanghebbenden de gelegenheid te bieden de totstandkoming van een Besluit te toetsen zodat de wederpartij reële rechtsbescherming wordt geboden."

Contractbepalingen

Artikel 1 Toepasselijkheid

1.1. Deze Contractbepalingen zijn van toepassing indien Leverancier aan de Opdrachtgever een Algoritmische toepassing levert die door de Opdrachtgever

wordt gebruikt bij het nemen van Besluiten, het voorbereiden van Besluiten of in het kader van handhavings- of fraudeonderzoek.

1.2. Deze Contractbepalingen zijn eveneens van toepassing indien Leverancier aan de Opdrachtgever een Algoritmische toepassing levert die wordt ingezet voor het nemen van beslissingen of het voorbereiden van beslissingen over medewerkers van de Opdrachtgever.

1.3. Deze Contractbepalingen zijn van toepassing indien Leverancier de Algoritmische toepassing als onderdeel van een afgesproken ICT-prestatie aan de Opdrachtgever levert.

1.4. Indien de Algoritmische toepassing onderdeel uitmaakt een afgesproken ICT-prestatie die door Leverancier aan de Opdrachtgever worden geleverd, dan zijn deze Contractbepalingen van toepassing op die ICT-prestatie in aanvulling op de GIBIT.

1.5. Indien deze Contractbepalingen strijdig zijn met de bepalingen in de GIBIT, dan gelden deze Contractbepalingen.

Artikel 2 Kwaliteit van de data

2.1. Indien en voor zover de Algoritmische toepassing in het kader van de te leveren ICT-prestatie wordt ontwikkeld op basis van data die door de Opdrachtgever aan Leverancier worden aangeleverd, zal Leverancier de redelijkerwijs van hem te verwachten maatregelen nemen om ervoor te zorgen dat de bij het ontwikkelen van de Algoritmische toepassing gebruikte data worden geanalyseerd, gestructureerd en/of bewerkt:

a. volgens een gemotiveerde aanpak die onder meer, maar niet uitsluitend, tot doel heeft om sociaal geconstrueerde vertekening, onnauwkeurigheden, fouten, vergissingen en "[redacted] (ongewenste vooringenomenheid) in deze data zoveel als redelijkerwijs mogelijk te voorkomen;

b. op een wijze die in overeenstemming is met toepasselijke wet- en regelgeving.

2.2. Indien en voor zover de Algoritmische toepassing wordt ontwikkeld op basis van data die niet door de Opdrachtgever aan Leverancier worden aangeleverd, zal Leverancier ervoor zorgen dat de bij het ontwikkelen van de Algoritmische toepassing gebruikte data worden verzameld, geanalyseerd, gestructureerd en/of bewerkt:

a. volgens een gemotiveerde aanpak die onder meer, maar niet uitsluitend, tot doel heeft om sociaal geconstrueerde vertekening,

onnauwkeurigheden, fouten, vergissingen en "[redacted] (ongewenste vooringenomenheid) in deze data zoveel als redelijkerwijs mogelijk te voorkomen;

b. op een wijze die in overeenstemming is met toepasselijke wet- en regelgeving.

2.3. Indien en voor zover Leverancier de Algoritmische toepassing voorafgaand aan het sluiten van de Overeenkomst heeft ontwikkeld, staat Leverancier ervoor in dat de in artikel 2.2 van deze Contractbepalingen beschreven maatregelen reeds zijn genomen.

Artikel 3 Rechten op de data

3.1. Alle rechten met betrekking tot de data die in het kader van de Overeenkomst door de Opdrachtgever aan Leverancier worden verstrekt, komen toe aan de Opdrachtgever. Leverancier heeft niet het recht deze data te gebruiken voor andere doeleinden dan het uitvoeren van de Overeenkomst. Leverancier zal deze data op eerste verzoek van de Opdrachtgever vernietigen en/of tot afgifte van de data aan de Opdrachtgever overgaan.

3.2. Alle rechten met betrekking tot de data die in het kader van de uitvoering van de Overeenkomst worden gecreëerd of verzameld, komen toe aan de Opdrachtgever. Tenzij Partijen anders overeenkomen, heeft Leverancier niet het recht deze data te gebruiken voor andere doeleinden dan het uitvoeren van de Overeenkomst. Leverancier zal deze data op eerste verzoek van de Opdrachtgever vernietigen en/of tot afgifte van de data aan de Opdrachtgever overgaan.

3.3. Afgifte van de in artikel 3.1 en 3.2 van deze Contractbepalingen bedoelde data vindt plaats in een door de Opdrachtgever aan te wijzen gangbaar bestandsformaat. Indien Leverancier voor het omzetten van de data naar het door de Opdrachtgever gewenste bestandsformaat aanvullende werkzaamheden dient te verrichten, zal de Opdrachtgever Leverancier hiervoor een redelijke vergoeding betalen. Een geschil over de hoogte van de door Opdrachtgever aan Leverancier te betalen vergoeding, kan voor Leverancier geen reden zijn om zijn verplichtingen uit deze Contractbepalingen op te schorten.

3.4. Op eerste verzoek van de Opdrachtgever zal Leverancier bewijs van vernietiging van de data verstrekken.

Artikel 4 Kwaliteit van de Algoritmische toepassing

4.1. Leverancier verklaart dat de Algoritmische toepassing is of zal worden ontwikkeld en functioneert op een wijze die in overeenstemming is met wet- en regelgeving.

4.2. Leverancier verklaart dat de Algoritmische toepassing volgens een gemotiveerde aanpak is of zal worden ontwikkeld.

4.3. Leverancier verklaart dat de Algoritmische toepassing nauwkeurig en correct functioneert of zal functioneren.

4.4. Leverancier verklaart dat de Algoritmische toepassing geschikt is of geschikt zal zijn voor het Beoogde gebruik.

Artikel 5 Transparantie over de Algoritmische toepassing

5.1. Leverancier zal op eerste verzoek van de Opdrachtgever aan de Opdrachtgever Procedurele transparantie verschaffen. De Opdrachtgever heeft het recht om de in dat kader door Leverancier verstrekte informatie met derden te delen en openbaar te maken. Op verzoek van de Opdrachtgever zal Leverancier een door de Opdrachtgever aan te wijzen register voor Algoritmische toepassingen invullen.

5.2. Leverancier zal op eerste verzoek van de Opdrachtgever aan de Opdrachtgever Technische transparantie verschaffen om de Opdrachtgever in staat te stellen een Audit uit te voeren als bedoeld in artikel 8 van deze Contractbepalingen. De Opdrachtgever zal dergelijke informatie uitsluitend opvragen en gebruiken indien en voor zover dat noodzakelijk is voor de toepassing van artikel 8 van deze Contractbepalingen. De Opdrachtgever zal op grond van artikel 5.2 van deze Contractbepalingen aan haar verstrekte bedrijfsvertrouwelijke informatie geheimhouden en na afloop van een Audit als bedoeld in artikel 8 van deze Contractbepalingen vernietigen, tenzij een op de Opdrachtgever rustende wettelijke verplichting zich tegen geheimhouding of vernietiging verzet of de Opdrachtgever de informatie nodig heeft in het kader van een geschil met Leverancier of een derde.

5.3. Bij de toepassing van artikel 5.2 van deze Contractbepalingen kan Leverancier ervoor kiezen om de broncode van de Algoritmische toepassing niet af te geven aan de Opdrachtgever, maar aan een door de Opdrachtgever aan te wijzen en in te schakelen onafhankelijke derde die namens de Opdrachtgever de in artikel 8 van deze Contractbepalingen bedoelde Audit zal uitvoeren. Eventuele meerkosten die daaruit voortvloeien komen voor rekening van Leverancier. De Opdrachtgever kan van Leverancier eisen dat een voorschot wordt betaald in verband met de kosten van de onafhankelijke derde.

5.4. De Opdrachtgever dient te allen tijde de mogelijkheid te hebben om de werking van de Algoritmische toepassing uit te leggen (Uitlegbaarheid). Leverancier is verplicht aan het Uitlegbaar maken van de Algoritmische toepassing zijn volledige medewerking te geven en alle daarvoor benodigde informatie aan de Opdrachtgever te verstrekken. De Opdrachtgever heeft het recht om de in dat kader door Leverancier verstrekte informatie met derden te delen en openbaar te maken.

5.5. Gedurende de looptijd van de Overeenkomst vormen de in artikel 5 van deze Contractbepalingen beschreven verplichtingen resultaatsverplichtingen en is de Opdrachtgever, tenzij Partijen anders overeenkomen, voor het nakomen van deze verplichtingen geen aanvullende vergoeding verschuldigd aan Leverancier. Na de looptijd van de Overeenkomst vormen de in artikel 5 van deze Contractbepalingen beschreven verplichtingen inspanningsverbintenissen en is de Opdrachtgever voor de in dat kader door Leverancier te verrichtten werkzaamheden een redelijke vergoeding verschuldigd.

5.6 Indien sprake is van een overlap tussen de informatie die wordt verstrekt op basis van de verschillende leden van artikel 5 van deze Contractbepalingen, staat het de Opdrachtgever steeds vrij om te kiezen welk lid van artikel 5 van deze Contractbepalingen Opdrachtgever zal toepassen.

Artikel 6 Risicomanagementstrategie bij ontwikkeling van de Algoritmische toepassing

6.1. Bij de ontwikkeling van de Algoritmische toepassing zal Leverancier een gangbare en up-to-date risicomanagementstrategie hanteren die passend is voor de aard van de Algoritmische toepassing. Bij het toepassen van deze risicomanagementstrategie zal Leverancier de belangrijkste risico's identificeren die zich kunnen voordoen bij het gebruik van de Algoritmische toepassing door de Opdrachtgever en maatregelen treffen teneinde de geïdentificeerde risico's beheersbaar te maken. Bij het identificeren van de risico's zal Leverancier indien relevant in ieder geval aandacht besteden aan het risico dat niet wordt voldaan aan één of meer van de verplichtingen genoemd in artikel 2 en artikel 4 van deze Contractbepalingen, risico's die verband houden met discriminatie, de mogelijkheid voor de Opdrachtgever om controle te houden over de Algoritmische toepassing en gegevensbescherming.

6.2. Leverancier zal de in artikel 6.1 van deze Contractbepalingen beschreven risicomanagementstrategie op dusdanige wijze uitvoeren en documenteren dat de tijdens de in artikel 8 van deze Contractbepalingen bedoelde Audit kan controleren of Leverancier aan de in artikel 6.1 van deze Contractbepalingen beschreven verplichting heeft voldaan.

6.3. Indien en voor zover Leverancier de Algoritmische toepassing voorafgaand aan het sluiten van de Overeenkomst heeft ontwikkeld, staat Leverancier ervoor in dat de in artikel 6.1 en artikel 6.2 van deze Contractbepalingen beschreven handelingen reeds hebben plaatsgevonden. Op eerste verzoek van de Opdrachtgever zal Leverancier daarvan bewijs aanleveren.

Artikel 7 Beheer van de Algoritmische toepassing

7.1. Indien de ICT-prestatie als een dienst wordt geleverd en het beheer en onderhoud van de Algoritmische toepassing onderdeel uitmaakt van die ICT-prestatie, staat Leverancier ervoor in dat de Algoritmische toepassing en de daarbij behorende documentatie gedurende de looptijd van de Overeenkomst aan de in artikel 4 van deze Contractbepalingen genoemde Contractbepalingen blijft voldoen.

7.2. Indien de ICT-prestatie als een dienst wordt geleverd en het beheer en onderhoud van de Algoritmische toepassing onderdeel uitmaakt van die ICT-prestatie, maakt onderdeel van de door Leverancier te leveren ICT-prestatie uit dat Leverancier gedurende de looptijd van de Overeenkomst continue zal monitoren of de in artikel 6.1 van deze Contractbepalingen bedoelde risico's nog actueel zijn en of de in artikel 6.1 van deze Contractbepalingen bedoelde maatregelen effectief zijn. Indien dat niet het geval blijkt te zijn, zal Leverancier aanvullende maatregelen treffen.

7.3. Onderdeel van de in artikel 7.2 van deze Contractbepalingen bedoelde verplichting is dat Leverancier zal informeren indien nieuwe risico's bekend worden of de in artikel 6.1 van deze Contractbepalingen bedoelde maatregelen niet effectief blijken te zijn.

Artikel 8 Audit of andersoortige controle

8.1. Leverancier is te allen tijde verplicht om mee te werken aan een door of namens de Opdrachtgever uit de voeren Audit of andersoortige controle waarin wordt beoordeeld of Leverancier de in deze Contractbepalingen afgesproken Contractbepalingen naleeft. Deze medewerking ziet onder meer op het geven van Technische transparantie, het geven van Procedurele transparantie, het inzicht geven in de uitgevoerde risicomanagementstrategie, het beschikbaar stellen van personeel van Leverancier voor het houden van interviews en het geven van toegang tot de locaties van Leverancier.

8.2. De Opdrachtgever zal een Rapport op (laten) stellen waarin de conclusies van de Audit worden vastgelegd. In het Rapport zal de Opdrachtgever vastleggen

in hoeverre Leverancier de verplichtingen uit deze Contractbepalingen naleeft. Indien de Opdrachtgever vaststelt dat Leverancier de verplichtingen van deze Contractbepalingen niet juist naleeft, is Leverancier verplicht om binnen de door de Opdrachtgever Rapport vastgestelde redelijke termijn de in het Rapport constateerde gebreken te verhelpen. Herstelt Leverancier de in het Rapport geconstateerde gebreken niet binnen de door de Opdrachtgever gestelde hersteltermijn, dan verkeert Leverancier van rechtswege in verzuim.

8.3. De Opdrachtgever heeft het recht de conclusies van het in artikel 8.2 bedoelde Rapport openbaar te maken. Bij strijdigheid tussen artikel 5.2 en artikel 8.3 heeft artikel 8.3 voorrang.

8.4. De Opdrachtgever heeft het recht om maximaal één keer per kalenderjaar een Audit uit te (laten) voeren.

8.5. De Opdrachtgever kan besluiten de Audit (gedeeltelijk) te laten uitvoeren door een onafhankelijke auditor.

8.6. De kosten van de eventueel door de Opdrachtgever in te schakelen auditor komen voor rekening van de Opdrachtgever. Voor eventuele kosten die Leverancier in het kader van de Audit zal maken voor andere werkzaamheden dan het verstrekken van Technische transparantie of Procedurele transparantie, zal de Opdrachtgever Leverancier een redelijke vergoeding betalen. Een geschil over de hoogte van een dergelijke vergoeding kan voor Leverancier nooit reden zijn om zijn verplichtingen uit deze Contractbepalingen op te schorten. Een dergelijke vergoeding hoeft de Opdrachtgever niet te betalen indien uit de het Rapport blijkt dat Leverancier deze Contractbepalingen op wezenlijke punten niet naleeft of heeft nageleefd.

Artikel 9 Kosten

Tenzij Partijen anders overeenkomen of in Contractbepalingen uitdrukkelijk anders is bepaald, is de Opdrachtgever voor de werkzaamheden die voortvloeiden geen aanvullende vergoeding verschuldigd aan Leverancier.

HANDREIKING BEZWAAR-BEHANDELAARS

Handreiking ‘Effectieve en efficiënte rechtsbescherming tegen het gebruik van algoritmen door de overheid’

Context en inleiding

Soms wordt bij een besluit, of de voorbereiding daarvan, een algoritme gebruikt. Dat kan zijn direct – bijvoorbeeld het scannen van kentekens om te controleren of parkeergeld is betaald – of indirect – bijvoorbeeld bij een risico-inschatting die wel of geen aanleiding geeft om nader onderzoek naar een persoon te doen. Omdat een algoritme vaak technisch complex is, is voor bezwaarmakers of behandelend ambtenaren niet altijd duidelijk welke invloed het algoritme heeft gehad op het besluit en of dit van belang is voor de beoordeling van een bezwaar. Dit kan gevolgen hebben voor de rechtsbescherming bij het gebruik van algoritmen in een bestuursrechtelijke context.

Deze handreiking bevat aanbevelingen voor behandelaars van een bezwaar waarbij een algoritme ten grondslag ligt aan het genomen primair besluit. Met deze handreiking willen we zorgen voor een toegankelijke, structurele en effectieve bezwaarprocedure. Zodat het voor burgers duidelijker is hoe zij tegen een besluit op basis van een algoritme bezwaar kunnen maken, waar zij informatie over het algoritme kunnen vinden én hoe een zorgvuldige heroverweging plaatsvindt. Deze handreiking draagt bij aan de betrouwbaarheid van het algoritme en de controle hierop. Dit zal een belangrijke rol spelen bij de eventuele rechterlijk toetsing in beroep.

Juridische achtergrond

Het is essentieel dat een bestuursorgaan besluiten waarin algoritmen zijn verwerkt in de bezwaarfase heroverweegt, zodat de rechter dat besluit daarna kan toetsen. Het bestuursorgaan moet daarbij ambtshalve onderzoeken of een bezwaarschrift een probleem zichtbaar maakt als algoritmen bij de voorbereiding van besluiten worden gebruikt. Daarbij moet bijvoorbeeld gekeken worden naar menselijke tussenkomst. Maar ook het besluit anders was geweest, als er geen algoritme was gebruikt. Daarnaast moet het bestuursorgaan de algemene beginselen van behoorlijk bestuur toetsen, in het bijzonder het zorgvuldigheidsbeginsel, het gelijkheidsbeginsel en het motiveringsbeginsel. Voor een uitgebreide juridische analyse, zie bijlage 1.

Aanbevelingen voor bezwaarbehandelaars

Instellen bezwaar

- Sluit aan bij de bestaande bezwaarprocedure van het bestuursorgaan voor bezwaarschriften tegen besluiten ingevolge de Algemene wet Bestuursrecht (hierna: Awb). Met andere woorden: het algoritme kan binnen de reguliere bezwaarprocedure worden getoetst.

Eerste beoordeling ingediend bezwaarschrift

Uitgangspunt is dat de behandelend ambtenaar de werking van het algoritme begrijpt, de uitkomst ervan kan duiden en begrijpt welke informatie de indiener van het bezwaarschrift nodig heeft om te begrijpen wat de uitkomst en de impact van het algoritme op zijn situatie is.

- Controleer of (in de voorbereiding) gebruik gemaakt is van een algoritme.
    - Hanteer daarbij de volgende definitie:
        - *Software;*
        - *die door gebruik van data-analyse, statistiek of zelflerende logica;*
        - *geautomatiseerd voorspellingen doet, beslissingen neemt of adviezen geeft;*
        - *die leiden tot directe of indirecte impact op de bezwaarmaker.*
    - Neem bij twijfel contact op met de opsteller van het primair besluit of experts in de organisatie.

- De beoordeling van het bezwaarschrift vindt plaats op basis van de gronden van bezwaar: wees echter altijd alert op de mogelijke betrokkenheid van een algoritme, ook als het bezwaarschrift daar niet specifiek op ingaat. Bijvoorbeeld als de bezwaarmaker aangeeft dat het besluit in strijd is met:
    - 'de algemene beginselen van behoorlijk bestuur';
    - 'het zorgvuldigheidsbeginsel';
    - 'het motiveringsbeginsel' of
    - 'het gelijkheidsbeginsel'.

- Stel op basis van de grondslag van het bezwaar vervolgens vast of het algoritme, de rechtmatigheid van de achterliggende algoritmische beslisregel en de (menselijke) belangenafweging die aan het besluit ten grondslag ligt, moet worden getoetst.

Verzoek om aanleveren relevante stukken

Bovenop de standaardprocedure zijn voor de beoordeling van algoritmen meestal aanvullende stukken nodig.

- In bijlage 2 vind je een voorbeeld van een standaard checklist voor de stukken die het organisatieonderdeel voor de beoordeling van het algoritme moet overleggen.

- Maak daarbij onderscheid tussen maatwerkgegevens die ingevoerd zijn en standaardgegevens die door het algoritme gebruikt worden.
    - Het bestuursorgaan moet individuele gegevens uit eigen beweging op papier of anderszins waarneembaar beschikbaar stellen als stukken die op de zaak betrekking hebben. Dit betekent niet dat tabellen in of met het besluit moeten worden overgelegd of ter beschikking moeten worden gesteld. Het is voldoende

als duidelijk wordt gemaakt welke keuzes bij de invoer zijn gemaakt ten aanzien van de 'maatwerk' invoergegevens.
    - De plicht om uit eigen beweging gegevens over te leggen geldt niet zonder meer voor de gebruikte standaardinvoergegevens die onafhankelijk zijn van het concrete geval. Hier moet de bezwaarmaker zelf om verzoeken.

Ter inzage leggen van de stukken

- Houd er bij het ter inzage leggen rekening mee dat eventuele datasets met persoonsgegevens van de bezwaarmaker daarvan uitgezonderd moeten worden vanwege de persoonlijke levenssfeer (grondslag: artikel 7:4 lid 6 en 8 Algemene wet bestuursrecht).

Verweerschrift

- Neem (op basis van de informatie in de stukken in de checklist in bijlage 2) in ieder geval de volgende informatie op:
    - een begrijpelijke uitleg van het doel van het algoritme of het proces waarvan het algoritme onderdeel uitmaakt;
    - een begrijpelijke uitleg van de werking van het algoritme;
    - de belangrijkste factoren op basis waarvan het algoritme tot een bepaalde uitkomst is gekomen en;
    - (indien mogelijk:) welke wijzigingen in de input van het algoritme zouden moeten worden doorgevoerd om tot een andere uitkomst te komen.

- Laat de juristen of behandelend ambtenaren van de afdeling die geregeld deze bezwaarzaken behandelen regelmatig een training volgen zodat hun kennis over algoritmen actueel blijft.

Samenstelling hoorcommissie

Bij de beoordeling van algoritmen is specifieke kennis vereist. Houd daarmee rekening bij de samenstelling van de hoorcommissie.

- Overweeg om een kamer of poule te maken voor leden van de bezwaarcommissie met expertise op het gebied van algoritmen en geautomatiseerde besluitvorming, ethiek en privacybescherming.

- Overweeg de benoeming van een expert als lid.

- Zorg voor opleidingen voor de secretaris, voorzitter en commissieleden.

Hoorzitting en advies

- Aandachtspunten bij de uitwerking van het advies bij een bezwaar tegen algoritmische besluitvorming zijn in ieder geval:
    - het zorgvuldigheidsbeginsel;
    - de vergewisplicht en het motiveringsbeginsel;
    - de rechtmatigheid van de achterliggende algoritmische beslisregel;
    - de (menselijke) belangenafweging die aan het besluit ten grondslag ligt.

- Beoordeel of de uitkomst van het algoritme een [redacted] heeft, dat wil zeggen:
    - of er een vertekening van onderzoeksresultaten is;

- of er een vooroordeel of vooringenomenheid is die een objectieve waarneming of beoordeling van de feiten in de weg staat; en/of
- of het besluit anders zou zijn geweest, als het besluit niet gebaseerd zou zijn op een algoritme in de voorbereiding.

Beslissing op bezwaar

- Zorg dat de behandelend ambtenaar de benodigde kennis heeft om het advies van de commissie te beoordelen en uit te leggen aan het bestuursorgaan dat beslist op bezwaar. Neem bij twijfel contact op met een expert in de organisatie.

- Zorg, als dat relevant is, weer voor een duidelijke uitleg van het algoritme in de beslissing op bezwaar (voor enkele handvatten, zie 'verweerschrift').

Beroep

- Zorg dat de afdeling die het bezwaar als verwerende partij heeft behandeld, de zaak ook bij de rechter behandelt. Dit is een vuistregel die extra belangrijk is, gelet op de expertise die nodig is voor het voeren van verweer bij beroep tegen beslissingen op bezwaar waarbij de werking van een algoritme is beoordeeld.

Bijlage 1 – Juridische achtergrond

In het openbaar bestuur wordt steeds meer gebruik gemaakt van algoritmische besluitvormingsprocedures. Vooral bij grootschalige en routinematige (financiële) besluiten. Besluiten in de zin van artikel 1:3, eerste lid, van de Awb komen hierbij zonder *directe* menselijke tussenkomst tot stand. Het gaat om besluiten die uit computers rollen omdat ze daartoe door mensen zijn geïnstrueerd.

Aanleiding

Dergelijke procedures worden complex en ondoorzichtig gevonden. Voor een burger is het niet gemakkelijk om te achterhalen op welke gronden algoritmische besluitvorming heeft plaatsgevonden. Dit heeft ook consequenties voor een eventuele bezwaar- en/of beroepsprocedure. De Afdeling bestuursrechtspraak van de Raad van State heeft in de AERIUS-uitspraak van 17 mei 2017 geoordeeld dat bij het gebruik van algoritmen een gebrek aan inzicht in de gemaakte keuzes en gebruikte gegevens en aannames kan ontstaan, wat ertoe kan leiden dat partijen een ongelijkwaardige procespositie hebben. Voor de burger kan het bovendien moeilijk zijn om te achterhalen op welke gronden bezwaar kan worden aangetekend tegen een dergelijk besluit.

Hieronder geven we in het kort de stand van zaken weer met betrekking tot het bestuursrechtelijk toetsingskader voor geautomatiseerde besluitvorming.

Toetsingskader geautomatiseerde besluitvorming
De Afdeling advisering RvS
De Afdeling advisering van de Raad van State beveelt aan om voor de normering van geautomatiseerde besluitvorming aansluiting te zoeken bij algemene beginselen van behoorlijk bestuur, in het bijzonder bij het **motiveringsbeginsel** en het **zorgvuldigheidsbeginsel**. Deze beginselen kunnen compensatie bieden als wetgeving de rechtspositie van burgers onvoldoende bepaalt.

<u>Het motiveringsbeginsel:</u>
De overheid moet haar besluiten begrijpelijk, deugdelijk en volledig motiveren. Het motiveringsbeginsel verreist enerzijds de juiste vaststelling van de feiten en anderzijds het gegeven dat de vaststelling van de feiten moet leiden (althans mag leiden) tot de genomen beslissing.

<u>Het zorgvuldigheidbeginsel:</u>
Op grond van het zorgvuldigheidbeginsel moet een bestuursorgaan een besluit zorgvuldig voorbereiden en nemen. Bij de voorbereiding vergaart het bestuursorgaan de benodigde kennis over de relevante feiten en de af te wegen belangen. De belangen die rechtstreeks bij het besluit betrokken zijn, worden afgewogen.

SyRi-uitspraak
Op 5 februari 2020 heeft de rechtbank Den Haag uitspraak gedaan over SyRI (Systeem Risico Indicatie), een systeem van de overheid dat burgergegevens aan elkaar koppelt om fraude met sociale voorzieningen op te sporen. De rechter noemde in de uitspraak risico's op discriminatie en

stigmatisering en aantasting van de privacy. Gebrekkige transparantie van het gebruikte algoritme speelde de hoofdrol.[1]

De wetgeving is over de inzet van SyRI volgens de uitspraak van de rechtbank onvoldoende inzichtelijk en controleerbaar, wat ten koste is gegaan van het transparantiebeginsel dat door de privacywetgeving is voorgeschreven. De inbreuk op het privéleven is voor burgers niet te voorzien en zij kunnen zich er niet tegen verweren. Door het gebrek aan transparantie kan ook niet gegarandeerd worden dat de beginselen van doelbinding en dataminimalisatie worden nageleefd.

De rechtbank had geen inzicht gekregen in de volgende zaken:
- de feitelijke gegevensverwerking;
- het gehanteerde algoritme;
- de ingezette methode van gegevensverwerking.

De Afdeling bestuursrechtspraak
In de AERIUS-uitspraak (AERIUS I) heeft de Afdeling bestuursrechtspraak de aanzet gegeven voor een algemeen toetsingskader voor geautomatiseerde besluitvorming. In haar uitspraak van 18 juli 2018 over de Blankenburgverbinding (AERIUS II) heeft de Afdeling dit toetsingskader voor geautomatiseerde besluitvorming verfijnd.

Om de eerder genoemde ongelijkwaardige procespositie te voorkomen en om reële rechtsbescherming mogelijk te maken, heeft de Afdeling in AERIUS I de norm geformuleerd dat het bestuursorgaan verplicht is om uit eigen beweging **de gemaakte keuzes** en **de gebruikte gegevens** en **aannames** bij het gebruik van algoritmes volledig, tijdig en op een passende wijze beschikbaar te stellen.

> *'Ter voorkoming van deze ongelijkwaardige procespositie rust in dit geval op genoemde ministers en de staatssecretaris de verplichting om de gemaakte keuzes en de gebruikte gegevens en aannames volledig, tijdig en uit eigen beweging openbaar te maken op een passende wijze zodat deze keuzes, gegevens en aannames voor derden toegankelijk zijn. Deze volledige, tijdige en adequate beschikbaarstelling moet het mogelijk maken de gemaakte keuzes en de gebruikte gegevens en aannames te beoordelen of te laten beoordelen en zo nodig gemotiveerd te betwisten, zodat reële rechtsbescherming tegen besluiten die op deze keuzes, gegevens en aannames zijn gebaseerd mogelijk is, waarbij de rechter aan de hand hiervan in staat is de rechtmatigheid van deze besluiten te toetsen.'*[2]

In de AERIUS II-uitspraak brengt de Afdeling een nuancering aan in haar toetsingskader voor geautomatiseerde besluitvorming door een expliciet onderscheid te maken tussen *maatwerk-invoergegevens* en *standaard-invoergegevens*. Het bestuursorgaan moet maatwerk-invoergegevens, individuele gegevens die de gebruiker zelf invoert, uit eigen beweging op papier

---

[1] Nederlands Juristenblad – 20-12-2019 – afl. 44: *Gebrek aan transparantie is drieledig . Het is (a) een bewuste ondoorzichtigheid gericht op de bescherming van intellectuele eigendomsrechten, (b) een ondoorzichtigheid wegens een gebrek aan deskundigheid van rechter en bestuur en (c) een intrinsieke ondoorzichtigheid van voor het menselijk brein moeilijk te doorgronden algoritmische systemen. De inzet van algoritmen in overheidsbesluitvormingsprocedures roept vanuit juridisch perspectief allerhande vragen op die te maken hebben met de juistheid en representativiteit van invoergegevens, technische transparantie en uitlegbaarheid van gebruikte modellen in de 'black box', gegevensbescherming en andere grondrechtelijke kwesties. Dit belemmert de effectieve rechtsbescherming van burgers tegen besluiten waarbij algoritmen zijn gebruikt.*
[2] Overwegingen 14.3 en 14.4

of anderszins waarneembaar beschikbaar stellen als stukken die op de zaak betrekking hebben (zoals bedoeld in de artikelen 7:2, tweede lid en 8:42 Awb). Dit betekent volgens de Afdeling niet dat alle kaarten en tabellen met gegevens per wegvak in of met het besluit moeten worden overgelegd of ter beschikking worden gesteld. Het is voldoende dat in of met het besluit duidelijk is gemaakt welke keuzen bij de invoer zijn gemaakt ten aanzien van de 'maatwerk'-invoergegevens.

De plicht om gegevens uit eigen beweging over te leggen geldt niet zonder meer voor de gebruikte standaard-invoergegevens die onafhankelijk zijn van het concrete geval. Hier moet de bezwaarmaker zelf om verzoeken.

De Hoge Raad (bijvoorbeeld in zaken over WOZ-beschikkingen) en de CRvB hebben zich inmiddels bij deze lijn van de Afdeling aangesloten.

Resumerend: als een bestuursorgaan zijn beslissingen baseert op een computerprogramma/algoritme moet het op grond van de AERIUS-uitspraken:

1. volledig en tijdig
2. de gemaakte keuzes en de gebruikte gegevens en aannames
3. uit eigen beweging openbaar te maken
4. op een passende wijze zodat deze keuzes, gegevens en aannames voor derden toegankelijk zijn.

Toetsingskader binnen de Algemene Verordening Gegevensbescherming (AVG)

Artikel 22 van de AVG stelt dat een betrokkene het recht heeft niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft. Op grond van artikel 40 van de Uitvoeringswet AVG geldt het verbod op geautomatiseerde individuele besluitvorming, anders dan op basis van profilering, niet als deze besluitvorming noodzakelijk is om te voldoen aan een wettelijke plicht of als het noodzakelijk is om een taak van algemeen belang uit te voeren.

Wel moet de verwerkingsverantwoordelijke dan passende maatregelen treffen om het gerechtvaardigd belang van de betrokkene te beschermen.

Conclusie:

De besluiten die tot stand komen met behulp van geavanceerde systemen zijn moeilijk te beoordelen en te controleren. De algoritmes waarop deze systemen zijn gebaseerd worden complex en nauwelijks transparant gevonden.

Bij de toetsing van dergelijke besluiten in bezwaar en beroep kan dan ook moeilijk worden nagegaan of er een zorgvuldige afweging heeft plaatsgevonden tussen de nadelige gevolgen van het gebruik van algoritmes en het algemene belang dat hiermee gediend is.

In bovenstaande jurisprudentie vormt transparantie de kern van maatregelen om grip te krijgen op algoritmische besluitvorming. Bij het bepalen van deze transparantie kan worden aangesloten bij het motiverings- en het zorgvuldigheidsbeginsel.

Een bestuursorgaan moet inzichtelijk maken:

1. dat een besluit tot stand is gekomen met behulp van een algoritme;
2. van welke feiten het is uitgegaan en welke gegevens van de burger gebruikt c.q. verwerkt zijn;
3. welke relevante belangen tegen elkaar zijn afgewogen en hoe die afweging is verlopen (bijvoorbeeld het gewicht dat wordt toegekend aan elk afgewogen kenmerk; welke analytische technieken gebruikt zijn; welke specifieke voorspellende data; wat de belangrijkste policy-keuzes waren; een uitleg van het voorspellende algoritme);
4. hoe het algoritme werkt (niet de techniek, maar hoe de uitkomsten van het algoritme tot stand komen).

Ofwel, zoals de Afdeling het verwoordt: welke keuzes en aannames zijn gemaakt en welke invoergegevens zijn gebruikt.

Geraadpleegde literatuur:

https://marliesvaneck.wordpress.com/tag/aerius/
http://www.stibbe.com/en/news/2017/august/afdeling-bestuursrechtspraak-formuleert-toetsingskader-voor-geautomatiseerde-besluitvormingsproces
https://pure.uvt.nl/ws/portalfiles/portal/31738610/AA20190776.pdf
Effectieve rechtsbescherming bij algoritmische besluitvorming in het bestuursrecht, de Poorter, Jurgen; Goossens, Jurgen Published in: Nederlands Juristenblad 2019.
Betekenisvolle transparantie voor algoritmische besluitvorming, C. Adriaansz, 9-3-2020, Computerrecht 2020/43.

Bijlage 2 – Checklist bewijsstukken

De gemeente moet op een individueel niveau aan een burger kunnen uitleggen waarom een algoritme tot een bepaalde beslissing of uitkomst komt en moet de burger de gelegenheid bieden om daar, zo nodig in een juridische procedure, bezwaar tegen te maken.

Hiervoor moet de ontwikkelaar (intern of leverancier) in ieder geval de volgende informatie aanleveren:

- wat zijn de belangrijkste factoren op basis waarvan het algoritme tot een bepaalde uitkomst is gekomen en;
- welke wijzigingen in de input zouden moeten worden doorgevoerd om tot een andere uitkomst te komen. (Achterliggende gedachte daarbij is dat de gemeente aan een burger wil kunnen uitleggen wat ze moet veranderen om ervoor te zorgen dat een besluit wordt genomen, dat wel door de burger wordt gewenst.)

Als dit onvoldoende blijkt te zijn, vraag dan bij de ontwikkelaar informatie op over het doel van het algoritme en het proces dat is gevolgd bij het ontwikkelen en toepassen van het algoritme en de in dat kader gebruikte data. Daaronder valt in ieder geval:

- documentatie die inzicht geeft in de gemaakte keuzes en de gehanteerde aannames;
- de categorieën van data die zijn gebruikt bij het ontwikkelen van het algoritme;
- de wijze waarop in menselijke tussenkomst is voorzien;
- de gebruikte methode(n) om risico's te identificeren;
- de geïdentificeerde risico's en de maatregelen die zijn genomen om de risico's te beperken;
- de partijen die betrokken zijn geweest bij het ontwikkelen van het algoritme en hun rol;
- een 'gemotiveerde aanpak' die beschrijft welke maatregelen zijn getroffen om minimaal de volgende zaken in de data te voorkomen:
    - sociaal geconstrueerde vertekening;
    - onnauwkeurigheden;
    - fouten;
    - vergissingen;
    - '[redacted] (ongewenste vooringenomenheid).
- een beschrijving van de wijze waarop de data in overeenstemming zijn met wet- en regelgeving.

MENSENRECHTEN-IMPACTANALYSE

INCLUSIEF

[redacted]-ANALYSE

Gemeente Amsterdam

Template Kunstmatige Intelligentie Impact Assessment

V1. Gemeente Amsterdam

Kunstmatige Intelligentie (hierna KI) :
Directie:
Verwerkings-
verantwoordelijke:
Leverings-
verantwoordelijke:
Afdeling:
Afdelingshoofd:
Werkproces:
Proceseigenaar:
Opgesteld door:
Datum:
Versie:

Bijlagen:

1) DPIA werkproces;
2) Excelbestand met overzichten van:
    - Verwerkte data (met doelbinding, relevantie voor ontwikkeling KI);
    - Opgestelde features;
    - Business rules betreffende werkproces;
    - Verwijderde features;
3) Excelbestand met weging betrokken (grond)rechten en waarden inzet KI;
4) Baselinetoets / DRA
5) Rapport [redacted] analyse;
6) Auditrapport;
7) CPA/ FG advies/ adviezen;
8) Collegebesluit;
9) Gebruikersinstructie
10) Beheerplan

Inhoudsopgave:

1. Inleiding p.
2. Bepalen noodzaak uitvoeren Kunstmatige Intelligentie Impact Assessment. p.
3. KI-toepassing, verantwoordelijkheden en werkproces p.
4. Beschrijf de baten van de KI-toepassing toepassing p
5. Architectuur p.
6. Data en data governance
7. Wettige en ethische toepassing p.
8. [redacted] analyse p.
9. Technische documentatie p.
10. Risicomanagement p.
11. Informatiebeveiliging p
12. Beheer p
13. Communicatie p.
14. Verantwoording p.
15. Afweging en beoordeling p.

1. Inleiding

2. Bepalen noodzaak voor het doen van een kunstmatige intelligentie impact assessment

2.1 ***Wordt de kunstmatige intelligentie (hierna: KI) toegepast in een nieuw (maatschappelijk) domein?***

2.2 ***Wordt gebruik gemaakt van een nieuwe vorm van KI-technologie?***

2.3 ***Is er sprake van een verboden KI-toepassing zoals beschreven in art. 5 van de (concept) regelgeving European Approach for AI van de Europese Commissie?***

2.4 ***Heeft de KI een hoge mate van autonomie?***

2.5 ***Wordt de KI toegepast in een complexe omgeving?***

2.6 ***Wordt de KI toegepast binnen een 'gevoelig' werkproces?***

2.7 ***Heeft de KI eerder schade toegebracht aan fundamentele rechten van natuurlijke personen of groepen?***

2.8 ***Zijn er zorgen over de KI en de potentiële schade en impact?***

2.9 ***Wordt gebruik gemaakt van gevoelige gegevens over personen?***

2.10 ***Wordt een voorspelling gegenereerd op persoonlijke niveau op basis van persoonlijke kenmerken?***

2.11 ***Neemt de KI-beslissingen die natuurlijke of rechtspersonen in aanzienlijke mate treffen dan wel rechtsgevolgen voor hen hebben?***

2.12 ***In hoeverre is de output van de KI van invloed op het besluitvormingsproces binnen de organisatie?***

2.13 ***Is er, mede bezien vanuit de geconstateerde en voorzienbare risico's, sprake van een hoge risico KI-systeem?***

2.14 ***Indien er sprake is van een (potentiële) hoge risico KI-toepassing, is de Autoriteit Persoonsgegevens geïnformeerd over de intentie om de KI-toepassing te ontwerpen en te ontwikkelen?***

2.15 ***Conclusie (uitvoeren KI-assessment of niet?)***

Ja? Ga door naar 3. Nee? Sla de afwegingen hierboven inclusief conclusie op.

3. KI-toepassing, verantwoordelijkheden en betreffende werkproces

3.1 ***Beschrijf de toepassing en het doel van de toepassing.***

3.2 ***Beschrijf het werkproces (BPMn uitwerking en toelichting).***

3.3 ***Welke processtap/ taak wordt ondersteund met de KI?***

3.4 ***Worden bij deze processtap/ taak beslisregels toegepast door medewerkers of systemen?***

3.5 ***Welke verantwoordelijkheden zijn er als het gaat om het verwerken van de gegevens?***
Zie document 'taken en verantwoordelijkheden bij het gebruik van Algoritmen en rekenmodellen door de gemeente Amsterdam'.

3.6 ***Wie zijn betrokken bij de ontwikkeling van de KI?***

3.7 ***Welke verantwoordelijkheid heeft ieder rol?***

3.8 ***Beschrijf welke actoren een rol spelen in de toepassing.***

3.9 ***Beschrijf welke KI-technologie wordt ingezet om het doel te bereiken.***

3.10 ***Beschrijf of er is nagedacht over manieren om het KI-systeem te ontwikkelen of de KI te trainen zonder of met zo weinig mogelijk gebruik van potentieel gevoelige gegevens of persoonsgegevens?***

3.11 ***Wie zorgt ervoor dat de KI operationeel (beheer) blijft en wordt gemonitord?***

4. Beschrijf de baten van de KI-toepassing

4.1 Wat zijn de baten voor de organisatie?

4.2 Wat zijn de baten voor het individu?

4.3 Wat zijn de baten voor de maatschappij als geheel?

5. Architectuur

5.1 Hoe ziet de huidige architectuur eruit voor het gebruik van de KI?

5.2 Hoe zit de toekomstige architectuur eruit voor het gebruik van de KI?

6. Data en data governance

6.1 ***Beschrijf welke brondata worden gebruikt binnen het werkproces en in het kader van de toepassing.***

6.2 ***Beschrijf of de brondata voor de KI is aangevuld met afgeleide data?***

6.3 ***Heeft de gemeentelijke organisatie volledige controle en beheersing (eigenaarschap) over de gebruikte data voor de KI?***

6.4 ***Beschrijf de reikwijdte van de gegevens in uw gegevenssets die worden onderzocht (bijv. of ze persoonsgegevens bevatten)?***

6.5 ***Wat is de bewaartermijn van de gegevens en voor verwerking ten behoeve van de KI-toepassing?***

6.6 ***Hoe is de data geleverd en verzameld?***

6.7 ***Welke afspraken zijn er gemaakt over de levering en verzameling van de data?***

6.8 ***Wat is de kwaliteit en kwantiteit van de beschikbare data?***

6.9 ***Is de data passend voor de KI-toepassing? Zo ja, waarom?***

6.10 ***De data heeft passende 'statistische' eigenschappen. Dit geldt zowel voor de individuele dataset als ook voor een combinatie van datasets***

6.11 ***Zijn er relevante aannames, met betrekking tot de informatie die de gegevens geacht worden te meten en te duiden?***

6.12 ***Zijn er 'data gaps' of tekortkoming in de data? Zo ja, kunnen er maatregelen worden troffen om dit te corrigeren? Welke maatregelen zijn dit?***

6.13 ***Zijn passende maatregelen genomen om categorieën persoonlijke data te beschermen? Zo ja, welke maatregelen zijn die (bv: encryptie, pseudonimisatie, aggregatie, anonimisatie)***

6.14 ***Welke datavoorbereiding- en verwerkingsmethodieken zijn toegepast (annotatie, labelling, cleaning, aggregatie)***

6.15 ***Zijn er afspraken gemaakt over de bewaartermijnen van de verwerkte data en de verwijdering/ archivering van de data als de termijn is verlopen of de data niet meer noodzakelijk is voor de ontwikkeling van de KI? Zo ja, wat zijn deze afspreken?***

6.16 ***Is de training-, validatie- en testdata relevant, representatief, foutloos en compleet?***

6.17 ***Zijn er duidelijke criteria/ parameters vastgesteld voor het correct functioneren van de KI?***

6.18 ***Welke methoden worden gebruikt om te verifiëren of de KI binnen de gestelde parameters blijft?***

6.19 ***Is de output van de KI consequent?***

6.20 ***Welke out-put data genereert de KI?***

6.21 ***Welke relevante designkeuzes voor de KI-toepassing zijn gemaakt?***

6.22 ***Is er onderzoek gedaan naar onbewuste vooringenomenheid in de dataset en de KI-toepassing? Zo ja, wat zijn de uitkomsten hiervan en welke maatregelen zijn getroffen?***

7. Wettige en ethische toepassing

7.1 ***Wat is de wettelijke grondslag voor de beoogde verwerking van de gegevens ten behoeve van het ontwikkelen, trainen en inzetten van de KI?***

7.2 ***Welke waarden en belangen spelen een rol in de context van de KI-toepassing?***
Invullen template 'weging betrokken (grond)rechten en waarden bij inzet KI

7.3 ***Hoe worden de waarden en belangen van betrokken actoren geborgd?***

7.4 ***Zijn de waarden en belangen geconcretiseerd in wet- en regelgeving?***
Invullen template 'weging betrokken (grond)rechten en waarden bij inzet KI

7.5 ***Hoe wordt gedurende het ontwikkelproces getoetst aan deze waarden en belangen?***

7.6 ***Is er, in de gebruikssituaties waarin er mogelijk sprake kan zijn van negatieve gevolgen voor de grondrechten, een effectbeoordeling op het gebied van grondrechten uitgevoerd?***

7.7 ***In hoeverre hebben betrokkene een kwetsbare positie ten opzichte van de gebruiker van de KI (bezien vanuit macht, kennis, economische en sociale omstandigheden of leeftijd).***

7.8 ***Wordt door de KI bepaalde personen of groepen schade toegebracht of ongunstig behandeld wat niet gerechtvaardigd is en in verhouding staat tot hun sociale gedrag of de ernst ervan?***

7.9 ***Wordt door keuze architectuur of de gebruikersinterface van de KI menselijk gedrag, meningen of beslissingen beïnvloed?***

7.10 ***Versterkt of vergroot het KI-systeem menselijke capaciteiten?***

7.11 ***Wie is de "human in control" en wat zijn de momenten of hulpmiddelen voor menselijke interventie?***

7.12 ***In hoeverre is het mogelijk om een persoon 'uit' de KI te halen (opt-out?)***

7.13 ***Zijn er voorzorgsmaatregelen genomen om overmatig vertrouwen in of op het KI-systeem bij werkprocessen te voorkomen?***

7.14 ***In hoeverre kan de output van de KI worden teruggedraaid, gecorrigeerd of buiten beschouwing worden gelaten?***

7.15 ***Is er getoetst in hoeverre er sprake is van profilering en in hoeverre dat is toegestaan?***

7.16 ***Is er een menselijke toezichthouder aangewezen om de werking van de KI te monitoren en om effectieve maatregelen als de KI niet naar behoren presteert?***

7.17 ***Is de onderliggende logica in de KI-toepassing passend bij de wettelijke taak die moet worden uitgevoerd met de inzet hiervan?***

7.22 ***Is de KI-toepassing voldoende transparant en controleerbaar? Zo ja, waarom?***

7.23 ***Is de ontwikkelde KI-toepassing wettig en ethisch verantwoord? Zo ja, waarom?***

8. [redacted] analyse

De [redacted] analyse omvat de volgende onderdelen:

1. Te onderzoeken ("gevoelige") groepen bepalen
2. Hypotheses opstellen over features die tot indirecte [redacted] leiden
3. Metrics selecteren passend bij het project
4. Directe [redacted] analyseren
5. Indirecte [redacted] analyseren
6. [redacted] op niet meetbare variabelen analyseren
7. Gevonden [redacted] wegen en beoordelen met verantwoordelijke directie
8. [redacted] waar nodig mitigeren
9. Conclusies opstellen

Deze onderdelen hoeven niet exact in de weergegeven volgorde uitgevoerd te worden en hebben bovendien een iteratief karakter: uitkomsten van één onderdeel kunnen ertoe leiden dat een ander onderdeel nogmaals uitgevoerd of aangepast wordt. Dit herhaalt zich totdat alle onderdelen naar tevredenheid zijn afgerond. De onderdelen worden hieronder in detail toegelicht.

8.1 Te onderzoeken ("gevoelige") groepen bepalen

Het kernprincipe wat we toepassen om [redacted] te achterhalen is om de uitkomsten van de KI te vergelijken voor verschillende groepen. De *punten* waarop wordt vergeleken (de metrics) worden beschreven in onderdeel 2. De *groepen* die worden vergeleken zijn gebaseerd op kenmerken waarop we geen ongerechtvaardigd onderscheid mogen en/of willen maken. We hebben de volgende kenmerken geïdentificeerd waarvoor dit het geval is:

- Nationaliteit*
- Geboorteland*
- Postcode*
- Huidskleur
- Etniciteit
- Geslacht*
- Leeftijd*
- Burgerlijke staat*
- Seksuele geaardheid
- Religie
- Politieke opvatting
- Verblijfsstatus*
- Zwangerschap
- Gezondheid
- Sociale klasse
- Genetica

De met een asterisk gemarkeerde kenmerken zijn bij de gemeente bekend over de mensen die, doordat zij wonen op een adres in de dataset, opgenomen zijn in de dataset.

8.2 Metrics selecteren passend bij het project

De KI kan op verschillende manieren beoordeeld worden, bijvoorbeeld:

- *Accuracy*: Percentage KI voorspellingen wat juist is.
- *Selection rate*: Percentage zaken wat door de KI aangewezen wordt als fraude.
- *False positive rate (FPR)*: Percentage van alle niet-fraudezaken dat (ten onrechte) door de KI als fraude wordt aangewezen. Zegt iets over de kans dat een zaak onnodig wordt onderzocht, daarom hoe lager, hoe beter.
- *True positive rate (TPR)*: Percentage van alle fraudezaken dat (terecht) door de KI als fraude wordt aangewezen. Zegt iets over de pakkans, daarom hoe hoger, hoe beter.
- *False negative rate (FNR)*: Percentage van alle fraudezaken dat (ten onrechte) door de KI niet als fraude wordt aangewezen. Complementair aan de TPR.
- *False discovery rate (FDR)*: Percentage van alle fraudevoorspellingen wat onjuist is.

Zulke cijfers noemen we *metrics*. Een metric kan worden uitgerekend voor de hele dataset of juist per groep, waarna we kunnen vergelijken of bepaalde groepen door de KI anders behandeld worden, waardoor zij mogelijk benadeeld worden. Het is doorgaans niet mogelijk om alle metrics tegelijkertijd te verbeteren, waardoor er met de specifieke projectcontext in gedachten keuzes gemaakt moeten worden. Zo zijn in medische toepassingen *false negatives* doorgaans ongewenst, omdat dat betekent dat er een ziekte over het hoofd wordt gezien, terwijl in andere gevallen *false positives* meer nadelen met zich meebrengen.

Om een beeld te geven van de hoeveelheid [redacted] in de KI zijn de volgende metrics gekozen:

- *Disparate impact*: Verhouding tussen de selection rate van twee groepen.
- *Average odds difference*: Gemiddelde van het verschil tussen twee groepen in FPR en het verschil in TPR.
- *False discovery rate difference*: Verschil in FDR tussen twee groepen.
- *False positive rate difference*: Verschil in FPR tussen twee groepen.
- *Generalized entropy index*: Oorspronkelijk afkomstig uit onderzoek naar inkomensongelijkheid; geeft uitdrukking aan de ongelijkheid tussen groepen én binnen een groep.

8.3 Hypotheses opstellen over features die tot indirecte [redacted] leiden

Dat een bepaald kenmerk niet als feature in de KI zit, betekent niet dat de KI hier geen [redacted] tegen kan hebben. Een bekend voorbeeld is dat KI zonder nationaliteit als feature alsnog een [redacted] op nationaliteit kan hebben doordat postcode *wel* in de KI zit en sterk samenhangt met nationaliteit. Voor alle features in de KI zijn daarom hypotheses opgesteld over mogelijke relaties met de gevoelige kenmerken. Als zo'n samenhang leidt tot een [redacted] op het gevoelige kenmerk noemen we dat indirecte [redacted]

8.4 Directe [redacted] en controlevariabelen analyseren

Met directe [redacted] wordt bedoeld een [redacted] veroorzaakt door het direct meenemen van een gevoelig kenmerk als feature in de KI. De gevoelige kenmerken die zijn overwogen voor de KI zijn geslacht en leeftijd. De exacte features die hieruit zijn afgeleid, zijn te vinden in VERWIJZING NAAR TEMPLATE

Gevoelige kenmerken die niet worden ingezet als feature kunnen worden gebruikt als controlevariabele. Dit betekent dat het gevoelige kenmerk *niet* in de KI wordt meegenomen, maar dat we er *wel* groepen mee maken om te zien of de metrics verschillen tussen deze groepen.

Het analyseren gebeurt als volgt:

1. Deel de dataset op in twee groepen op basis van een gevoelig kenmerk.
2. Bereken de bovengenoemde metrics voor beide groepen.
3. Bekijk of de metrics verschillen tussen de groepen.

Als de metrics niet (substantieel) van elkaar verschillen tussen groepen op basis van kenmerk X, dan kunnen we concluderen dat de KI geen (substantieel) verschil maakt op basis van kenmerk X. Is dit het geval, dan kunnen ook de hypotheses over indirecte [redacted] betreffende dit kenmerk van de lijst worden gehaald.

Als de metrics wel (substantieel) van elkaar verschillen, dan is er mogelijk sprake van een ongerechtvaardigde [redacted] Deze resultaten worden verzameld en meegenomen naar onderdeel 7.

8.5 Indirecte [redacted] analyseren

Met indirecte [redacted] wordt bedoeld een [redacted] veroorzaakt door het meenemen van een op het eerste gezicht onschadelijke feature die samenhangt met een gevoelig kenmerk.

Onderdeel 3 heeft geleid tot hypotheses over de features die indirecte [redacted] zouden kunnen veroorzaken. Onderdeel 4 heeft deze lijst mogelijk verkleind, als al geconcludeerd kon worden dat de KI geen verschil maakt op basis van een gevoelig kenmerk.

Het analyseren gebeurt op de manier zoals in onderdeel 4 beschreven, met als enige aanpassing dat de groepen nu niet gebaseerd zijn op een gevoelig kenmerk, maar op een van de features die voorkomt op de lijst met indirecte-[redacted]-hypotheses.

Als de metrics niet (substantieel) van elkaar verschillen tussen groepen op basis van feature X, dan kunnen we alle indirecte-[redacted]-hypotheses voor feature X ontkrachten. Als de metrics wel (substantieel) van elkaar verschillen, dan is de hypothese mogelijk waar en is er mogelijk sprake van een ongerechtvaardigde [redacted] Deze resultaten worden verzameld en meegenomen naar onderdeel 7.

8.6 [redacted] op niet meetbare variabelen analyseren

Lang niet alle gevoelige kenmerken op de lijst in onderdeel 1 worden geregistreerd door de gemeente of zelfs de overheid in het algemeen.

8.7 Gevonden [redacted] wegen en beoordelen met verantwoordelijke directie

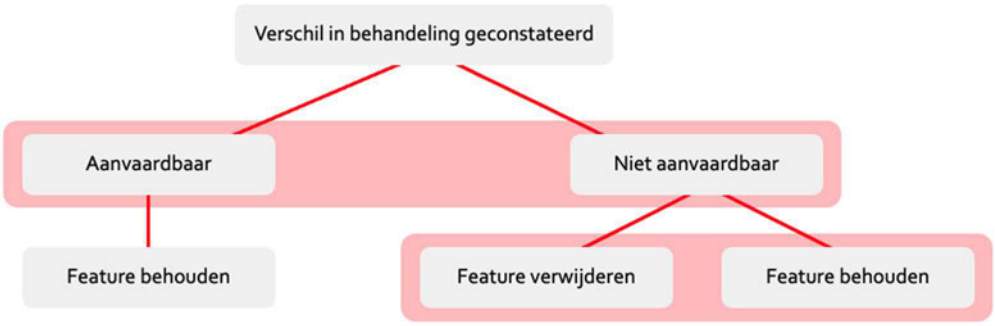
Het uitvoeren van de voorgaande stappen resulteert in een lijst van features met een indicatie van de mate waarin deze features [redacted] veroorzaken tegen bepaalde groepen, uitgedrukt in de metrics. Vervolgens wordt iedere feature voorgelegd aan de verantwoordelijke directie.

Wanneer een verschil in behandeling is geconstateerd (oftewel: de metrics verschillen substantieel tussen twee groepen), is de eerste vraag of dit verschil aanvaardbaar is of onaanvaardbaar. Een verschil zou bijvoorbeeld aanvaardbaar kunnen zijn als er een achterliggend verband is tussen een derde kenmerk en de uitkomsten van de KI, dat het verschil verklaart, en dit achterliggende verband is niet problematisch. Bij het nemen van deze beslissingen zijn meerdere invalshoeken relevant, hieronder weergegeven. Het is daarom van belang dat er mensen vanuit verschillende rollen en achtergronden betrokken zijn bij het wegen van de uitkomsten van de [redacted] analyse.



Wanneer een verschil aanvaardbaar wordt geacht, kan de feature behouden blijven. Wanneer een verschil niet aanvaardbaar wordt geacht, kan ervoor gekozen worden om de feature volledig uit de KI te verwijderen, of om te proberen de feature te behouden, waarover meer in onderdeel 8.

De overwegingen die gemaakt moeten worden zijn hieronder schematisch weergegeven.



8.8 [redacted] waar nodig mitigeren

De [redacted] die niet aanvaardbaar worden geacht, worden in dit onderdeel aangepakt. De ene aanpak is het weglaten van features. De andere is om de [redacted] te proberen te verminderen door het doen van aanpassingen in de KI (bv. de loss function of postprocessing) of de data (bv. herwegen voor een gebalanceerdere dataset).

Na dit onderdeel worden de onderdelen 4 t/m 7 altijd herhaald, omdat aanpassingen aan de KI invloed kunnen hebben op de uitkomsten van de [redacted] analyse voor andere features. Bovendien is noch het weglaten van features noch het aanpassen van data of de KI een waterdichte oplossing (respectievelijk door indirecte [redacted] en imperfecties in de methodes), dus ook de [redacted] van de feature/gevoelige groep die is aangepast moet opnieuw bekeken worden.

8.9 Conclusies opstellen

Nadat alle onderdelen zijn doorlopen en in onderdeel 7 uiteindelijk alle overgebleven verschillen als aanvaardbaar beoordeeld worden, worden de conclusies van de [redacted] analyse vastgelegd in en Rapport [redacted] Analyse. Dit omvat de oorspronkelijk gevonden en uiteindelijke [redacted] eventuele maatregelen die genomen zijn, en de overwegingen uit onderdeel 7.

8.10 Samenvatting rapport

Nader in te vullen

9. Technische documentatie[1]

9.1 Wat zijn de interacties tussen de KI-toepassing met hard- en software dat geen onderdeel uitmaakt van de KI-toepassing zelf?

9.2 Wat zijn de revelante soft- of firmware versies?

9.3 Op welke manier is het KI-systeem in gebruik genomen en door wie?

9.4 Op welke hardware functioneert of zou de KI-toepassing moeten functioneren?

9.5 Is er een gebruikersinstructie en (indien nodig) installatie instructie opgesteld? De gebruikersinstructie bevat de volgende informatie:

- *Een gedetailleerde beschrijving van de KI-toepassing en het ontwikkelproces bestaande uit (aanvullend op KIIA);*
- *De methodiek en de uitgevoerde stappen voor het ontwikkelen van de KI-toepassing;*
- *De ontwerpspecificaties van het systeem;*
- *De belangrijkste ontwerpkeuzes inclusief afwegingen en aannames die zijn gedaan, ook met betrekking tot personen, groepen of gebruikers;*
- *De belangrijkste classificatie keuzes*
- *Waar de KI-toepassing is ontworpen en de verschillende parameters;*
- *De beslissingen over eventuele afwegingen met betrekking tot technische oplossingen die zijn gekozen om te kunnen voldoen aan de requirements;*
- *Een beschrijving van de architectuur van het systeem waaruit blijkt hoe de softwarecomponenten zijn gebouwd of zijn gekoppeld/ geïntegreerd met elkaar.*
- *De rekenmiddelen die worden gebruikt om de KI-toepassing te ontwikkelen, trainen, testen en te valideren;*

9.6 Wat zijn, indien van toepassing, de vooraf bepaalde (toekomstige) wijzigingen in de KI-toepassing en diens prestaties?

9.7 Hoe wordt omgegaan met de onvoorspelbaarheid van het handelen van de KI?

9.8 Welke maatregelen zijn genomen om de verklaarbaarheid te borgen?

9.9 Is er een overzicht van alle veranderingen die aan de KI-toepassing zijn aangebracht gedurende de levenscyclus?

[1] Zie Richtlijn European Approach for AI voor alle documentatievereisten.

9.10 Is er een beheerplan opgesteld?

10. Risicomanagement

10.1 ***Welke risicomanagement systeem wordt toegepast en welke instrumenten worden daarbij ingezet?***

10.2 ***Is er een risicoanalyse uitgevoerd over de toepassing van de KI?***

10.3 ***Is er een overzicht van de geïdentificeerde risico's?***

10.4 ***Kunnen deze risico's worden geëlimineerd of worden gereduceerd?***

10.5 ***Is er een overzicht opgesteld van de getroffen of nog te treffen maatregelen?***

10.6 ***Zijn potentiële veiligheidsrisico's vastgesteld van (andere) voorzienbare toepassingen van de technologie, met inbegrip van onbedoeld of kwaadwillig misbruik ervan? Is er een plan om deze risico's te beperken of te beheren?***

10.7 ***Is het acceptabel, gezien de risico's en de beoogde maatregelen, om de KI-toepassing in gebruik te nemen?***

10.8 ***Wordt het risicomanagementsysteem gedurende de levenscyclus van de KI-toepassing toegepast?***

10.9 ***Wordt het risicomanagementsysteem periodiek geëvalueerd?***

11. Informatiebeveiliging

11.1 Is er sprake van security by design? Zo ja, hoe wordt dit toegepast?

11.2 Is een Diepgaande Risico Analyse uitgevoerd?

11.3 Welke maatregelen zijn genomen om de betrouwbaarheid van het handelen van de KI te borgen?

11.4 Welke maatregelen zijn genomen om de veiligheid van de KI te borgen?

11.5 Welke maatregelen zijn genomen om de vertrouwelijkheid te borgen?

11.6 Welke maatregelen zijn genomen om de integriteit te borgen?

11.7 Welke maatregelen zijn genomen om de beschikbaarheid te borgen?

11.8 Welke maatregelen zijn er genomen om de traceerbaarheid te borgen?

11.9 Welke maatregelen zijn genomen om de verklaarbaarheid te borgen?

11.10 Wordt loginformatie over de werking van de KI (geautomatiseerd) gegeneerd, bewaard en toegankelijk gemaakt? Deze logs bevatten minimaal:

- *Startdatum, tijd, eind data en tijd van elk gebruik*
- *De referentiedatabase waarin de data wordt gecontroleerd door de KI-toepassing*
- *De inputdata waarop de 'match' is gemaakt*
- *De indentificatie van de natuurlijke personen die betrokken zijn bij de verificatie van de resultaten.*

11.11 Door wie worden de logs bewaard?

11.12 Wordt gecontroleerd of toegangsrechten up-to-date zijn met betrekking tot de omgeving waarin de KI functioneert?

11.13 Worden toegangsrechten aangepast zodra er een uitdiensttreding of functiewijziging van een werknemer plaatsvindt?

11.14 Worden toegangsrechten uitgegeven door daarvoor bevoegde personen?

11.15 Wordt functievermenging voorkomen bij de toegang van gebruikers tot de KI?

11.16 Wordt er gebruikgemaakt van generieke beheeraccounts? Staat het aantal beheeraccounts in logische verhouding tot de beheerders?

11.17 Wordt er bij het inrichten van toegangsrechten van verschillende gebruikersgroepen/rollen gebruikgemaakt van naamgevingsconventies en systematiek?

11.18 Worden er naamgevingsconventies gebruikt voor gebruikers en beheerders, zodat zij geïdentificeerd kunnen worden?

11.19 Voeren beheerders werkzaamheden als beheerder en werkzaamheden als gewone gebruiker uit onder 2 verschillende gebruikersnamen?

11.20 Hebben gebruikersaccounts (geen) directe toegang tot onderliggende componenten?

11.21 Bestaat er een functiescheiding tussen aanvragen, autoriseren en verwerken van wijzigingen in gebruikersaccounts en toegangsrechten?

11.22 Is het wachtwoordbeheer interactief en zijn de wachtwoorden van geschikte kwaliteit?

11.23 Worden wijzigingen in de code van de KI op een gecontroleerde wijze uitgevoerd? Denk aan het testen en accorderen/autoriseren van wijzigingen

11.24 Is de KI beveiligd, zodat er geen risico is op ongeautoriseerde toegang, wijziging, beschadiging en/of dataverlies?

11.25 Worden er back-ups van de KI gemaakt en kan de KI en de data hersteld worden?

12. Beheer

12.1 Is er een beheerplan opgesteld?

12.2 Is er voldoende capaciteit om de KI-toepassing operationeel te houden en wijzigingen door te voeren?

12.3 Is er voldoende kennis aanwezig om de KI-toepassing operationeel te houden en wijzigingen door te voeren?

12.4 Worden de werking van de KI-toepassing periodiek geëvalueerd?

13. Communicatie

13.1 ***Is er een gebruikersinstructie opgesteld?***

13.2 ***Zijn mechanismen ingesteld om gebruikers in kennis te stellen van de redenen en criteria achter de resultaten van het KI-systeem?***

13.3 ***Is duidelijk gemaakt richting gebruikers en betrokkenen wat het doel van het KI-systeem is en wie of wat er profijt kan hebben van het product of de dienst?***

13.4 ***Is inzichtelijk gemaakt welke kenmerken, beperkingen en potentiële tekortkomingen van het KI-systeem duidelijk kenbaar gemaakt.***

14. Verantwoording

14.1 ***Hebt u mechanismen ingesteld die de controleerbaarheid van het systeem door interne en/of externe onafhankelijke actoren mogelijk maken, bijvoorbeeld in de vorm van waarborging van de traceerbaarheid en het bijhouden van de processen en resultaten van het KI-systeem?***

14.2 ***Is er, naast de interne initiatieven of kaders voor het toezicht op ethiek en verantwoording, ook sprake van een vorm van externe begeleiding of zijn er ook controleprocessen ingesteld?***

14.3 ***Hebt u een mechanisme ingesteld om relevante belangen en waarden die door het KI-systeem in het gedrang komen, alsook potentiële afwegingen daartussen, vast te stellen?***

15. Afwegingen en conclusie

15.1 Is de toepassing proportioneel?

15.2 Is met minder ingrijpende middelen hetzelfde doel te verwezenlijken?

15.3 Gaat het om positive sum in plaats van zero sum?

15.4 Zijn er rest-risico's?

15.5 Hoe wordt verantwoordelijkheid genomen voor verder gebruik?

TEMPLATE

Weging betrokken (grond)rechten

#	Betrokken (grond)rechten / waarden	Wettelijke bepaling(en):	Zwaartebepaling potentiële aantasting rechten bij gebruik van het model zonder getroffen	Risico	Kans (1,2,3; hoog, middel, laag)	Impact (1,2,3; hoog, middel, laag)	Risico (1-3 = laag; 4-6 = middel 7-9=hoog)	In hoeverre van toepassing	#	Getroffen maatregelen voor eerbiediging betrokken (grond)recht en waarden:	Status maatregel	Resultaat (geëlimineerd of gereduceerd)	Bron:
1													
									101				
									102				
									103				
									104				
2													
									101				
									102				
									103				
									104				
3													
									101				
									102				
									103				
									104				

TEMPLATE

Overzicht verwerkte data, business rules en features

Bron	Kenmerk/dataveld	Doelbinding voor het verwerken van het kenmerk in proces rechtmatigheid (basis in DPIA werkproces)	Toelichting waarom relevant voor ontwikkeling KI	Hoe is dit kenmerk verwerkt? (verwijzen naar features of koppelkenmerk)

BR ID	Als situatie X	Dan situatie Y	Onderbouwing van de business rule: waarop is het gebaseerd? Objectieve rechtvaardiging (redelijke en proportionele tot beoogde doel)
BR1			
BR2			
BR3			
BR4			
BR5			
BR6			
BR7			
BR8			
BR9			
BR10			

Feature #	Feature	Uitleg betekenis feature	Sensit viteit feature (laag, m dden, hoog)	Wordt deze feature (variabele) al toegepast n het werkproces?	Op bas s waarvan kan deze features worden toegepast (bv. web- an regelgeving of beleidsregels)?	Te onderzoeken voor bias?	In geval van ind rect tot welke groep/kenmerk/	Reas tast b as analyse	Conclusie en onderbouwing voor het gebruik van de feature in de KI (hierin wordt de juridische en ethische afweging gemaakt).	Is het gebruik van de feature vastgesteld door de verwerkingsverantwoordelijke(n)?

Feature #	Feature	U tleg betekenis feature	Sens tiv teit feature (laag, midden, hoog)	Wordt deze feature (variabele) al toegepast in het werkproces?	Op bas s waarvan kan deze features worden toegepast (bv. wet- en regelgeving of beleidsregels)?	Te onderzoeken voor bias?	In geval van indirect tot welke groep/kenmerk/	Resultaat bias analyse	Conclus e en onderbouw ng voor het gebru k van de feature n de KI (hier n wordt de jurid sche en eth sche afweging gemaakt).	Is het gebruik van de feature vastgesteld door de verwerkingsverantwoordel jke(n)?