



Governance voor de verantwoorde toepassing van hoog-risico-algoritmen in de gemeente Rotterdam

Van

Wubbo Wierenga, Wouter Verbeek & Mariam Al-Saqaff (Berenschot)

Datum

26 juli 2021



Inhoudsopgave

1	Inleiding	4
1.1	Doel en uitgangspunten van de governance voor de verantwoorde toepassing van hoog-risico-algoritmen in de gemeente Rotterdam	4
1.2	Definities	5
1.2.1	Definitie algoritmetoepassing	5
1.2.2	Definitie governance	5
1.2.3	Verantwoorde toepassing (ethiek)	6
1.3	De beschrijving van de governance voor de verantwoorde toepassing van hoog-risico-algoritmen in de gemeente Rotterdam	6
2	Het selecteren van de hoog-risico-algoritmetoepassingen met de Algorithm Risk Assessment (ARA)	8
2.1	Inleiding: de ARA als selectiemethode voor hoog-risico-algoritmetoepassingen	8
2.2	Aansluiten bij het Europese systeem van risicoclassificatie	8
2.3	De selectie van hoog-risico-algoritmetoepassingen door de beantwoording van drie vragen	10
3	Beschrijving governance voor risicovolle algoritmetoepassingen in de gemeente Rotterdam	11
3.1	Inleiding	11
3.2	De inhoudelijke elementen van de governance voor hoog-risico-algoritmetoepassingen in de gemeente Rotterdam	11
3.2.1	Het opstellen van een AIA (algoritmeregister en DEDA)	12
3.2.2	Het uitvoeren van de AIA: de algoritme-governance-cyclus	12
3.2.3	Algorithm Advisory Board (AAB)	13
3.3	Taken en verantwoordelijkheden	13
3.3.1	Het onderscheid tussen organisatieniveaus en verantwoordelijkheden	13
3.3.2	Taak- en verantwoordelijkheidsverdeling op uitvoerings- en communicatieniveau	14
3.3.3	Taak- en verantwoordelijkheidsverdeling op bestuurlijk- en beleidsniveau	15
3.3.4	Taak- en verantwoordelijkheidsverdeling op controleniveau	16
3.3.5	Een samenvattend overzicht van taken en verantwoordelijkheden	17
4	Implementatie van de governance voor risicovolle algoritmetoepassingen in de	



	gemeente Rotterdam	18
4.1	Personeel en expertise	18
4.1.1	Het aannemen van een algoritme-expert (profiel)	18
4.1.2	Het uitbreiden van de taken van de Privacy Officer (PO)	18
4.1.3	Samenstellen Algorithm Advisory Board (AAB)	19
4.2	Verdere uitwerking governance (standaardiseren AIA, integratie in DPIA en verdere integratie met aanpalende governance)	19
4.3	Communicatie en cultuur	19



1 Inleiding

In het rapport 'Gekleurde technologie' beschrijft de Rekenkamer van Rotterdam dat de opkomst van algoritmen niet altijd zichtbaar is, maar wel onstuitbaar en veelomvattend. De gemeente Rotterdam zet steeds vaker complexe algoritmen in. Deze toenemende inzet van algoritmen is in de kern positief: het stelt de gemeente in staat om beleidsdoelen op een effectieve en efficiënte manier te bereiken en is ook nodig om bij te blijven bij de ontwikkelingen in de rest van de samenleving.

Het is belangrijk dat deze toenemende inzet van algoritmen op een verantwoorde en legitieme manier gebeurt. Daarin zijn algoritmen in de kern niet bijzonder. Of de gemeente nu algoritmen inzet of niet, ze moet altijd verantwoord handelen. Wel zijn er algoritmetoepassingen die vanwege hun aard of impact speciale aandacht vragen. Om de verantwoorde en legitieme inzet van deze hoog-risico-algoritmetoepassingen te garanderen, is daarom een aanvulling op de bestaande governancestructuren binnen de gemeente Rotterdam noodzakelijk. Het is deze aanvulling die in dit document beschreven wordt.

1.1 Doel en uitgangspunten van de governance voor de verantwoorde toepassing van hoog-risico-algoritmen in de gemeente Rotterdam

Het doel van deze aanvullende governance is:

Een governance voor de verantwoorde toepassing van hoog-risico-algoritmen in de gemeente Rotterdam

Daarbij gelden de volgende uitgangspunten:

- *Aanvullend karakter.* Binnen de gemeente Rotterdam zijn verschillende governance-structuren actief om verantwoord handelen van de gemeente te bevorderen. De belangrijkste staat beschreven in de kadernota *Sturen en verantwoorden*. Verder zijn de AVG-governance, datagovernance en de governance voor informatiebeveiliging (BIO) relevant. De governance voor de verantwoorde toepassing van hoog-risico-algoritmen moet aanvullend zijn op deze bestaande governance.
- *De algemene beginselen van behoorlijk bestuur (Abbb).* De governance is gericht op de verantwoorde toepassing van hoog-risico-algoritmen. Er is sprake van verantwoorde toepassing wanneer de inzet van het algoritme voldoet aan het toepasselijke recht en de algemene beginselen van behoorlijk bestuur. Daarbij is de uitdaging om de tijdloze Abbb te vertalen naar de specifieke eigenschappen van (de toepassing van) algoritmen.
- *Aansluiten bij Europese en nationale ontwikkelingen.* Binnen de Europese Unie en de Rijksoverheid zijn beleids- en wetgevingsprocessen gaande die raken aan de (governance van) verantwoorde toepassing van algoritmen binnen overheidsorganisaties. Om de governance toekomstvast te maken, wordt in dit document daarom zoveel mogelijk op deze ontwikkelingen aangesloten. Een belangrijke ontwikkeling binnen de Europese Unie is de risicobenadering. In deze benadering worden de eisen aan de toepassing van een algoritme gekoppeld aan het risico dat de inzet van een algoritme onverantwoorde resultaten of effecten heeft.

- *De aanbevelingen van 'Gekleurde technologie'*. Een belangrijke aanleiding voor deze governance is het rapport 'Gekleurde technologie' van de rekenkamer van de gemeente Rotterdam. Uit het rapport volgt een aantal aanbevelingen, waarvan de belangrijkste is om een heldere governance in te richten voor de verantwoorde toepassing van algoritmen. Er ontbreekt vooral een overkoepelende structuur. De governance beschreven in dit document werkt daarom de rollen, verantwoordelijkheden en processen voor de ontwikkeling en beheersing van algoritmen uit.

1.2 Definities

Dit document bevat de aanvullende governance voor de verantwoorde toepassing van hoog-risico-algoritmen in de gemeente Rotterdam. Om tot een heldere beschrijving te komen, worden in deze paragraaf drie kernbegrippen gedefinieerd. Het gaat om:

- 1 algoritmetoepassing
- 2 governance
- 3 verantwoorde toepassing (ethiek).

In de governance is 'hoog risico' ook een kernbegrip. Dit kernbegrip wordt in hoofdstuk 2 verder uitgewerkt.

1.2.1 Definitie algoritmetoepassing

Een algoritmetoepassing bestaat uit vier onderdelen:



- 1) Gegevens: voor de toepassing van een algoritme zijn gegevens noodzakelijk. De gegevens zijn de input van het algoritme.
- 2) Algoritme: een algoritme is software en kan variëren van een simpele keuzeboom tot niet-lineaire modellen die doen denken aan neurale netwerken. Het algoritme zelf is de throughput.
- 3) Resultaten: dit is de output van het algoritme. De resultaten kunnen gebruikt worden om een voorspelling te doen, besluiten te nemen, adviezen te geven.
- 4) Impact: dit is de publieke waarde die de toepassing van het algoritme voor de Rotterdammers beoogd te genereren. Deze precieze waarde varieert per onderwerp. Een algoritmetoepassing kan bijvoorbeeld resulteren in betere besluiten over het kappen van bomen (resultaat) waardoor de kwaliteit van de openbare ruimte toeneemt (impact).

1.2.2 Definitie governance

Om de governance op de toepassing van algoritmen adequaat te beschrijven, maken we een onderscheid tussen drie typen governance:

- a. Ontwikkelgovernance. Dit is de governance op het proces van idee, intake, opstart, lab en opschaling van een algoritmetoepassing.¹

¹ Dit overzicht komt uit Data & Analyse: Way of working, van DGW (versie 17-12-2020).



- b. Beheersgovernance. Dit betreft de governance op het gebruik, beheer en doorontwikkeling van het algoritme.
- c. Overkoepelende governance. De governance die gericht is op het duurzaam laten functioneren van de gehele governance op algoritmen. Hieronder valt ook de controlefunctie.

De ontwikkel- en beheersgovernance worden gekoppeld aan de ontwikkel- en de beheerfase van algoritmetoepassingen. De overkoepelende governance is relevant voor beide fasen.

1.2.3 Verantwoorde toepassing (ethiek)

Er is sprake van verantwoorde toepassing wanneer de inzet van het algoritme voldoet aan de eisen die het recht aan overheidshandelen stelt. Binnen de gemeente (en alle andere bestuursorganen in Nederland) volgen deze eisen uit de Algemene beginselen van behoorlijk bestuur (Abbb) uit de Algemene wet bestuursrecht (Awb). Op grond van de Awb zijn deze beginselen van toepassing op al het gemeentelijk handelen: of de gemeente nu een bankje in het Vroesepark plaatst, een kapvergunning afgeeft of een algoritme inzet, de Abbb zijn van toepassing.

De algemene beginselen van behoorlijk bestuur werken vaak ongemerkt door in het overheidshandelen omdat ze meestal zijn uitgewerkt in wet- en regelgeving. Bijvoorbeeld, wanneer de gemeente een aanvraag voor een kapvergunning behandelt, past de betreffende medewerker de wet- en regelgeving toe, die vaak in werkprocessen nader zijn geconcretiseerd. Door deze werkprocessen op een juiste manier te volgen, voldoet de gemeente (meestal) 'automatisch' ook aan de Abbb bij het beoordelen van een aanvraag.

Bij nieuwe ontwikkelingen – zoals algoritmen – zijn deze beginselen nog niet (helemaal) uitgewerkt in de wet- en regelgeving. Dit betekent dat de Abbb direct het gemeentelijk handelen inkaderen. Dit stelt de gemeente voor de uitdaging om de tijdloze Abbb te vertalen naar de specifieke eigenschappen van algoritmen. De Rijksoverheid heeft hiervoor zeer recent (maart 2021) een aanzet gedaan: de Richtlijnen voor het toepassen van algoritmen door overheden en publieksvoorlichting over data-analyses. Deze richtlijnen zijn zeker nog niet helemaal uitgewerkt, maar geven richting aan de toekomstige invulling van de Abbb voor algoritmen.

1.3 De beschrijving van de governance voor de verantwoorde toepassing van hoog-risico-algoritmen in de gemeente Rotterdam

Om tot een gestructureerde beschrijving van de governance te komen, wordt in drie hoofdstukken de governance beschreven.



Het selecteren van de hoog-risico-algoritmetoepassingen met de Algorithm Risk Assessment (ARA) (hoofdstuk 2)

Op basis van de hiervoor beschreven uitgangspunten moet de aanvullende governance voor de verantwoorde toepassing van algoritmen alleen gericht zijn op hoog-risico (high risk)-algoritmetoepassingen. Voor deze algoritmetoepassingen is de bestaande governance ontoereikend en is aanvullende governance noodzakelijk voor de verantwoorde toepassing van algoritmen.



Om van de aanwezige algoritmen binnen de gemeente een eerste, grofmazige selectie te maken van de hoog-risico-algoritmen is de Algorithm Risk Assessment (ARA) ontwikkeld. De ARA wordt beschreven in hoofdstuk 2.

Inrichting van de aanvullende governance voor hoog-risico-algoritmetoepassingen (hoofdstuk 3)

Nadat we in hoofdstuk 2 hebben beschreven hoe de hoog risico algoritmetoepassingen te selecteren, wordt in hoofdstuk 3 de governance op deze algoritmetoepassingen beschreven. Wanneer uit de ARA blijkt dat een algoritmetoepassing een laag of beperkt risico heeft, geldt de standaard governance van de gemeente Rotterdam. Er is geen specifieke aanvullende governance noodzakelijk. Wanneer uit de ARA blijkt dat een algoritmetoepassing (in potentie) een hoog risico vormt, is de aanvullende governance noodzakelijk als kader voor een verantwoorde toepassing van deze algoritmen.

De kern van deze aanvullende governance vormt de Algoritme Impact Assessment (AIA). De AIA bevat, in lijn met de Data Protection Impact Assessment (DPIA), een analyse van de risico's van een algoritmetoepassing en een overzicht van concrete maatregelen (inclusief rollen en verantwoordelijkheden) om deze risico's te mitigeren. In hoofdstuk 3 wordt deze aanvullende governance verder uitgewerkt.

Het implementeren van de aanvullende governance voor hoog-risico-algoritmetoepassingen (hoofdstuk 4)

In hoofdstuk 4 worden de eerste stappen beschreven voor de implementatie van de aanvullende governance voor hoog-risico-algoritmetoepassingen binnen de gemeente Rotterdam.

2 Het selecteren van de hoog-risico-algoritmetoepassingen met de Algorithm Risk Assessment (ARA)

2.1 Inleiding: de ARA als selectiemethode voor hoog-risico-algoritmetoepassingen

De eerdergenoemde definitie van algoritmetoepassingen is zeer breed. Veel eenvoudige en risicoloze processen (denk aan Excel-berekeningen) vallen onder deze definitie van algoritmetoepassing. Voor deze eenvoudige en risicoloze algoritmetoepassingen is geen aanvullende governance noodzakelijk, maar is de standaard governance binnen de gemeente (bijvoorbeeld uit de kadernota *Sturen en verantwoorden*) voldoende. Voor hoog-risico-algoritmen is deze bestaande governance niet voldoende en is aanvullende governance noodzakelijk.

Met de Algorithm Risk Assessment (ARA) worden uit alle algoritmetoepassingen binnen de gemeente Rotterdam de hoog risico varianten geselecteerd. In dit hoofdstuk wordt de ARA beschreven. De aan hoog risico gekoppelde aanvullende governance wordt in het volgende hoofdstuk beschreven.



2.2 Aansluiten bij het Europese systeem van risicoclassificatie

In mei 2021 heeft de Europese Commissie (EC) een voorstel 'ter bevordering van een Europese benadering van AI' naar buiten gebracht. Dit voorstel bevat twee verordeningen en een gecoördineerd plan om niet alleen de kansen, maar ook de risico's van AI te adresseren. Vooruitlopend op de besluitvorming over dit voorstel wordt in lijn met de Europese aanpak een risicobenadering gekozen in de governance voor algoritmetoepassingen in de gemeente Rotterdam.

Op hoofdlijnen (toegepast op algoritmetoepassingen) valt de Europese risicoclassificatie in drie groepen uiteen. De eerste groep bestaat uit verboden algoritmetoepassingen die een onaanvaardbaar risico vormen omdat het gebruik ervan fundamentele rechten schendt. Als voorbeeld noemt het commissievoorstel systemen die kwetsbaarheden bij specifieke groepen personen proberen uit te nutten, social credit-achtige systemen en bepaalde vormen van biometrische identificatie.



De tweede groep vormen de hoog-risico-algoritmetoepassingen. In het commissievoorstel gaat het daarbij om toepassingen die 'aanzienlijke risico's' kunnen opleveren voor de gezondheid, veiligheid, of grondrechten van personen. Een voorbeeld zijn algoritmen die bedoeld zijn om door of namens overheidsinstanties te worden gebruikt om te beoordelen of natuurlijke personen in aanmerking komen voor overheidsuitkeringen en -diensten, evenals voor het verlenen, beperken, intrekken of terugvorderen van dergelijke uitkeringen en diensten. Deze toepassingen zijn niet verboden, maar moeten aan strikte eisen voldoen. Om te bepalen of een algoritmetoepassing een hoog risico is, wordt in het commissievoorstel een uitputtende lijst met type algoritmetoepassingen gegeven.

De derde groep bestaat uit beperkt en minimaal risico-algoritmetoepassingen. In het commissievoorstel vallen spamfilters en chatbots in de categorie 'beperkt risico'. Deze algoritmetoepassingen kunnen manipulerend werken, maar door een eenvoudige transparantieplichting is deze mogelijke manipulatie inzichtelijk te maken. Voor dit type risico's is geen aanvullende governance noodzakelijk.

Het doel van de ARA is de selectie van hoog-risico-algoritmetoepassingen uit alle werkzame gemeentelijke algoritmetoepassingen. De selectie van deze hoog-risico-algoritmetoepassingen moet er ook toe leiden dat eventuele verboden algoritmetoepassingen in beeld komen.

In het EC-voorstel worden algoritmes in onder andere spamfilters e.d. als laag of beperkt risico geclassificeerd. Ook voor de gemeente Rotterdam geldt dat dit laag-risico-algoritmes zijn waarop de aanvullende algoritmegovernance niet van toepassing is. Concreet gaat het binnen Rotterdam om de volgende onderdelen waarop de governance niet van toepassing is en waarvoor geen ARA hoeft te worden uitgevoerd:



- Algoritmes ingebouwd in IT for IT software, zoals spamfilters, intrusion detection e.d..
- Het gebruik van algoritmes in kantoorsoftware die vanuit de fabrikant zijn ingebouwd (bijvoorbeeld Office-applicaties die automatische suggesties doen). Let op: een algoritme dat door iemand wordt ontwikkeld in een dergelijk programma is wél aan een ARA en mogelijk aan de specifieke algoritmegovernance onderworpen.

2.3 De selectie van hoog-risico-algoritmetoepassingen door de beantwoording van drie vragen

De Algorithm Risk Assessment (ARA) bestaat uit de beantwoording van drie vragen. Door deze vragen te beantwoorden, wordt inzichtelijk welke algoritmetoepassingen een hoog risico hebben of verboden zijn. De aanpak met drie vragen wijkt deels af van het commissievoorstel. Waar de EC kiest voor een beoordeling op basis van een uitputtende lijst met type algoritmetoepassingen, bestaat de ARA uit een drietal simpele vragen die door proceseigenaren kunnen worden beantwoord. Het voordeel van deze aanpak is tweeledig. In de eerste plaats zijn de vragen toekomstbestendiger, terwijl een uitputtende lijst tijdens het Europese wetgevingsproces nog aangepast gaat worden en ook in de toekomst (vanwege technologische ontwikkeling) steeds aanpassing en verbetering behoeft. In de tweede plaats leidt het stellen van vragen ertoe dat medewerkers van de gemeente zelf nadenken over de verantwoorde toepassing van algoritmen.

De ARA bestaat uit drie vragen, die zijn gekoppeld aan drie onderdelen van een algoritmetoepassing:

- *Algoritme:* is de werking van het algoritme niet volledig én beknopt uit te leggen aan een gemiddelde Rotterdammer?
- *Resultaat:* ontbreekt er een menselijke beoordeling voordat de uitkomst van het algoritme in de praktijk wordt gebracht doormiddel van een concrete handeling van de gemeente?
- *Impact:* is het voorstelbaar dat de algoritmetoepassing uitmondt in een onrechtvaardige handeling van de gemeente tegen burgers of bedrijven?

Er is geen vraag opgenomen over de gegevens, omdat betreffende vragen in de Privacy Risk Assessment zijn opgenomen.

Wanneer het antwoord op één van deze vragen 'ja' luidt (of bij twijfel daarover), is er sprake van een hoog-risico-algoritmetoepassing. Dit betekent dat de gemeente Rotterdam moet nagaan welke aanvullende governance noodzakelijk is om tot een verantwoorde toepassing van deze algoritmen te komen. Deze aanvullende governance verschilt per algoritmetoepassing en is afhankelijk van de specifieke risico's van de algoritmetoepassing.

3 Beschrijving governance voor risicovolle algoritmetoepassingen in de gemeente Rotterdam

3.1 Inleiding

Op basis van de ARA krijgt een algoritmetoepassing een risicoclassificatie. Als blijkt dat de algoritmetoepassing een laag of minimaal risico heeft, is de standaard governance binnen de gemeente (bijvoorbeeld uit de kadernota *Sturen en verantwoorden*) voldoende. Er is geen aanvullende governance noodzakelijk. Als op basis van de ARA de conclusie is dat een algoritmetoepassing een hoog risico heeft, is aanvullende governance noodzakelijk.



In dit hoofdstuk wordt deze aanvullende governance beschreven. De kern van deze aanvullende governance vormt de Algoritme Impact Assessment (AIA). De AIA bevat, in lijn met de DPIA, een analyse van de risico's van een algoritmetoepassing en een overzicht van concrete maatregelen (inclusief rollen en verantwoordelijkheden) om deze risico's te mitigeren. Als hulpmiddel hierbij wordt de ethische data assistent (DEDA) ingezet. De AIA wordt opgenomen in het algoritmeregister, waarin alle hoog-risico-algoritmen binnen de gemeente Rotterdam worden geregistreerd.

Om de aanvullende governance voor algoritmen onder te brengen binnen de gemeente Rotterdam, worden in dit hoofdstuk de rollen en verantwoordelijkheden beschreven voor de ontwikkelfase (ontwikkelgovernance), de beheerfase (beheersgovernance) en het toezicht op het geheel (overkoepelende governance).

3.2 De inhoudelijke elementen van de governance voor hoog-risico-algoritmetoepassingen in de gemeente Rotterdam

Wanneer op basis van de ARA is vastgesteld dat een algoritmetoepassing een hoog risico heeft, is aanvullende governance noodzakelijk. Een centrale rol in de aanvullende governance speelt de Algorithm Impact Assessment (AIA). Deze wordt opgesteld voor ieder hoog risico algoritmetoepassing. Verder wordt ter versterking van de governance van algoritmetoepassing een Algorithm Advisory Board (AAB) ingericht.



3.2.1 Het opstellen van een AIA (algoritmeregister en DEDA)

Een van de hoofdconclusies van 'Gekleurde Technologie' is dat er een algoritmeregister moet zijn waaruit blijkt wat de risico's van een algoritmetoepassing zijn en welke bijpassende beheersmaatregelen getroffen dienen te worden. Het zijn deze risico's en beheersmaatregelen die de kern vormen van de AIA. Door de AIA en het algoritmeregister aan elkaar te koppelen, wordt tegemoet gekomen aan deze hoofdconclusie uit het rekenkamerrapport.

De opzet van een AIA

Op dit moment heeft de gemeente Rotterdam geen AIA. Idealiter komt er een standaardformulier (zoals bij DPIA), zodat de AIA steeds op een vergelijkbare manier wordt uitgevoerd. Voor nu geldt dat een AIA tenminste uit de volgende onderdelen bestaat (opzet in lijn met DPIA):

1. Een omschrijving van de algoritmetoepassing aan de hand van het onderscheid tussen gegevens, algoritme, resultaat en impact.
2. Een omschrijving van de precieze risico's aan de hand van het onderscheid tussen gegevens, algoritme, resultaat en impact (een verdieping van de ARA).
3. Een overzicht van beheersmaatregelen op basis van de risico's.
4. Een planning van de maatregelen.

Wel of geen onderdeel van DPIA

Voor de precieze rol en invulling van de AIA is van belang of de algoritmetoepassing persoonsgegevens verwerkt of niet. Indien er sprake is van de verwerking van persoonsgegevens, wordt een DPIA opgesteld en is de AIA onderdeel van de DPIA. Wanneer er geen sprake is van de verwerking van persoonsgegevens wordt de AIA een zelfstandig document.

Het onderscheid tussen ontwikkel en beheerfase

Voor de ontwikkel- en beheerfase wordt een aparte AIA opgesteld. De reden is dat (in de meeste gevallen) tijdens de ontwikkelfase van een algoritme-toepassing zich andere risico's voordoen en daardoor andere beheersmaatregelen passend zijn, ten opzicht van de beheerfase. Dus wanneer de ontwikkeling en de beheersing van de algoritmetoepassing intern binnen de gemeente plaatsvinden, wordt tweemaal een AIA ingevuld.

3.2.2 Het uitvoeren van de AIA: de algoritme-governance-cyclus

De AIA vormt de kern van de aanvullende governance voor hoog-risico-algoritmietoepassingen. Belangrijk is dat de AIA voor iedere hoog-risico-algoritmietoepassing een eigen risicoanalyse en beheersmaatregelen bevat. Daarmee wordt de AIA gericht op de specifieke risico's van een algoritmetoepassing. De aanvullende governance van hoog-risico-algoritmietoepassing is daarmee nooit een 'one size fits all'-benadering, maar steeds gericht op de specifieke risico's van een toepassing.

Een belangrijk kenmerk van de beheersmaatregelen in de AIA is dat ze een cyclisch karakter hebben, waardoor een algoritme-governance-cyclus ontstaat. Voor de hand ligt om op basis van de risico's en beheersmaatregelen het controlestelsel van de gemeente Rotterdam te hanteren (pagina 32 van de kadernota *Sturen en Verantwoorden 2020*). In het algoritmeregister wordt geregeld dat er automatisch een signaal uitgaat wanneer een algoritmetoepassing opnieuw beoordeeld moet worden.



3.2.3 Algorithm Advisory Board (AAB)

Naast de AIA is de instelling van een Algorithm Advisory Board (AAB) een andere belangrijke aanvulling voor de governance van algoritmetoepassingen binnen de gemeente Rotterdam. De AAB is een externe adviescommissie die de gemeentelijke organisatie scherp houdt en zorgt dat veranderende maatschappelijke ontwikkelingen hun weerslag vinden in de governancestructuur van de gemeente Rotterdam.

De AAB-experts van buiten de gemeente als derde line of defense. Te denken valt aan governance experts, ethici, juristen en algoritme-experts. In het bijzonder valt natuurlijk te denken aan wetenschappers die onderzoek doen naar ethiek van algoritmen. AAB stuurt de adviezen aan de directeur Bestuurs- en Concernondersteuning (BCO).

De Algorithm Advisory Board voert één of twee keer per jaar een analyse uit, waarbij ze bepaalde algoritmetoepassingen onder de loep nemen en daarbij controleren:

1. of de governanceprocessen zijn gevolgd
2. wat de kwaliteit van de AIA's zijn
3. in hoeverre er witte vlekken zijn en wat er aan de governanceprocessen moet worden aangepast.

De AAB kan zelf scope, reikwijdte en onderzoeksmethoden bepalen. De AAB kan worden gevoed door de Ombudsman en de voorzitter van de bezwaarschriftencommissie. De werking van het AAB wordt na vier jaar geëvalueerd.

3.3 Taken en verantwoordelijkheden

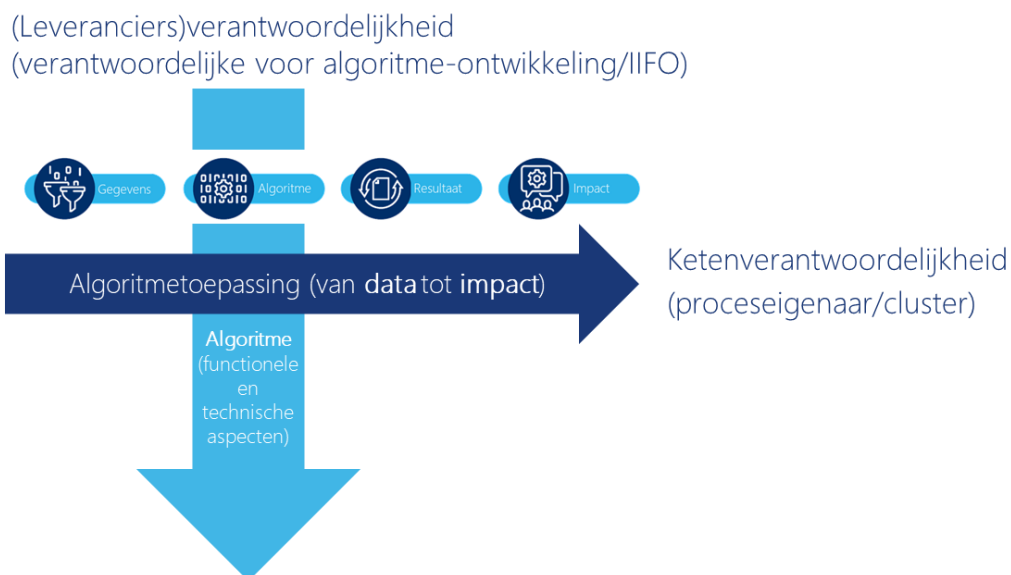
De ARA, AIA en AAB vormen de inhoudelijke aanvullingen aan de bestaande governance van de gemeente Rotterdam. De AIA wordt uitgevoerd als uit de ARA blijkt dat een algoritmetoepassing een hoog risico heeft. De AIA, ARA en AAB zijn hiervoor in dit rapport verder uitgewerkt. In deze paragraaf staat de vraag centraal: wie heeft welke verantwoordelijkheid voor deze aanvullende governance?

3.3.1 Het onderscheid tussen organisatieniveaus en verantwoordelijkheden

Om deze vraag te beantwoorden, wordt in deze paragraaf het volgende onderscheid gemaakt: Daarbij wordt een onderscheid gemaakt tussen vijf niveaus binnen de organisatie:

- **Bestuurlijk niveau** waar de verantwoordelijkheid ligt voor de besluitvorming en verantwoording over de inzet van algoritmen en voor het proces.
- **Beleidsniveau** waar de afweging en vertaling van beleid naar uitvoering via de inzet van algoritmen plaatsvindt.
- **Uitvoeringsniveau** waar het ontwerpen, maken, gebruiken en onderhouden van algoritmen plaatsvindt.
- **Controleniveau** dat toetst of algoritmen doelmatig, doeltreffend en rechtmatig worden ingezet. Denk aan de functionaris gegevensbescherming, de interne controller of externe auditor.
- **Communicatieniveau** dat met de burger communiceert over organisatieprocessen of individuele beslissingen. Dit zijn rollen die door communicatie- en beslismedewerkers worden vervuld.

Op het controleniveau is de overkoepelende governance belegd. De ontwikkel- en beheersgovernance lopen door alle organisatieniveaus heen. Verder is relevant om het onderscheid te maken tussen de verantwoordelijkheid voor de algoritmetoepassing als geheel en de verantwoordelijkheid voor (de kwaliteit van) het algoritme zelf. Dit laatste ziet toe op de functionele en technische aspecten van het algoritme. De verantwoordelijkheid voor de toepassing wordt samengevat onder de noemer procesverantwoordelijkheid en de verantwoordelijkheid voor de kwaliteit van het algoritme onder de noemer leveranciersverantwoordelijkheid. Binnen de Rotterdamse context, leidt dit tot de onderstaande taak- en verantwoordelijkheidsverdeling:



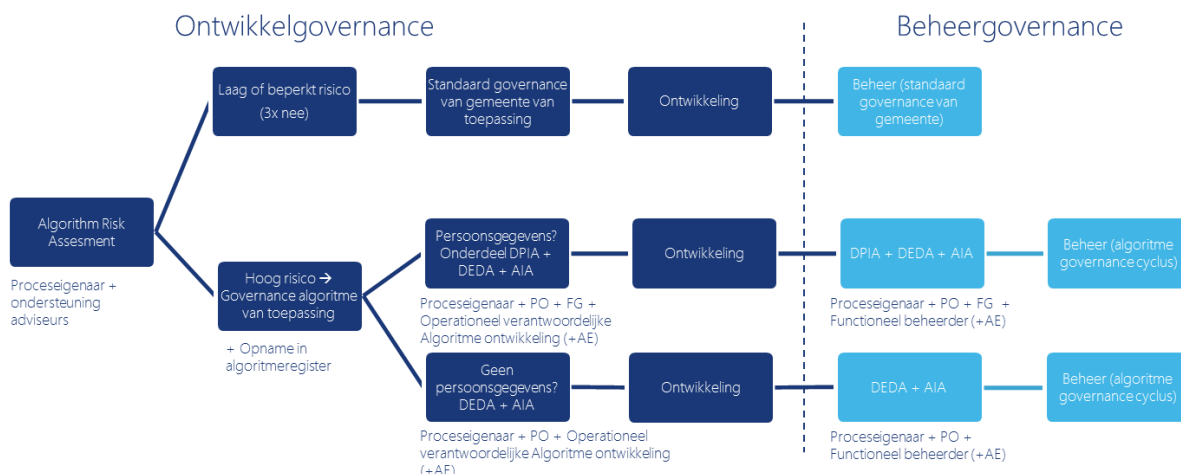
Deze verdeling van verantwoordelijkheden is ook van toepassing indien er meerdere data-eigenaren zijn. In dat geval blijft de proceseigenaar die het algoritme toepast/gebruikt ketenverantwoordelijk.

De beschrijving van taken en verantwoordelijkheden start op uitvoeringsniveau. Daar heeft deze aanvullende governance de meeste gevolgen met het oog op de inzet van mensen en middelen. Daarna wordt het bestuurlijk- en beleidsniveau beschreven. Als afsluiting wordt het controleniveau beschreven.

3.3.2 Taak- en verantwoordelijkheidsverdeling op uitvoerings- en communicatieniveau

De proceseigenaar is verantwoordelijk

Op uitvoeringsniveau staat de proceseigenaar centraal. Hij of zij is verantwoordelijk voor het uitvoeren van de ARA en de AIA (en het communiceren hierover binnen en buiten de organisatie). Het invullen van deze assessments vereist specialistische kennis, die een proceseigenaar niet heeft. Hij of zij ontvangt daarom ondersteuning van toegewijde specialisten van BCO. In hoofdlijn is de taakverdeling op uitvoeringsniveau als volgt te illustreren.



De inzet van privacy officer en algoritme-expert

Zeker wanneer een DPIA moet worden opgesteld (omdat sprake is van de verwerking van persoonsgegevens) is de privacy officer (PO) een belangrijke speler bij het opstellen van de ARA en de AIA. Omdat een PO doorgaans niet is opgeleid in de (technische) werking van algoritmetoepassingen, kan de PO een beroep doen op een algoritme-expert. Deze persoon (die tevens fungeert als secretaris van de AAB) heeft bij voorkeur een technisch achtergrond en kan de werking van de hele algoritmetoepassing (van gegevens tot impact) overzien. Ook wanneer er geen DPIA wordt opgesteld (omdat er geen persoonsgegevens worden verwerkt), zijn de PO en de algoritme-expert beschikbaar om de proceseigenaar met advies te ondersteunen bij het opstellen van de ARA en AIA. Daarmee wordt de rol van de PO iets ruimer dan op dit moment.

De leveranciersverantwoordelijkheid

De proceseigenaar is verantwoordelijk voor de algoritmetoepassing als geheel (procesverantwoordelijkheid). De leveranciersverantwoordelijkheid valt op uitvoeringsniveau uiteen in functioneel beheer in de beheerfase en het de operationele verantwoordelijkheid voor de algoritme-ontwikkeling binnen Innovatie, Informatievoorziening, Facilitair en Onderzoek (IIFO) tijdens de ontwikkelfase. Deze leveranciersverantwoordelijkheid geldt overigens niet voor het communicatieniveau.

3.3.3 Taak- en verantwoordelijkheidsverdeling op bestuurlijk- en beleidsniveau

Op bestuurlijk- en beleidsniveau is vooral het onderscheid in leveranciersverantwoordelijkheid en procesverantwoordelijkheid relevant. Procesverantwoordelijk op bestuurlijk niveau is de wethouder die verantwoordelijk is voor de beleidsinhoud. Dus als de algoritmetoepassing wordt ingezet voor Werk & Inkomen, dan is de wethouder verantwoordelijk voor Werk & Inkomen verantwoordelijk. Op beleidsniveau geldt hetzelfde voor de directeur van de betreffende beleidsafdeling. De leveranciersverantwoordelijkheid op bestuurlijk- en beleidsniveau is belegd bij de wethouder verantwoordelijk voor BCO / IIFO, respectievelijk de directeur IIFO.



3.3.4 Taak- en verantwoordelijkheidsverdeling op controleniveau

Inhoud van de taak- en verantwoordelijkheidsverdeling op controleniveau

De taak- en verantwoordelijkheidsverdeling op controleniveau is gericht op het duurzaam laten functioneren van de gehele governance op algoritmen. Dit betekent dat de governance van algoritmen gemonitord, onderzocht en geëvalueerd wordt en dat er duidelijkheid is over *lines of defense* (zie p. 8 en 9 kadernota *Sturen en Verantwoorden*).

De lines of defense

De eerste *line of defense* wordt gevormd door de alle functionarissen die hiërarchisch of functioneel medewerkers aansturen. Voor de toepassing van algoritmetoepassingen geldt hetzelfde. Daarbij moet worden aangetekend dat de precieze invulling van deze *line of defense* sterk afhangt van de manier waarop een cluster het proceseigenaarschap belegd heeft (en dus waar in de hiërarchische structuur de proceseigenaar geplaatst is).

De tweede *line of defense* wordt gevormd door functionarissen die, onafhankelijk van de eerste lijn, verantwoordelijk zijn voor advisering en het verstrekken en vaststellen van concernbrede kaders. Zoals hiervoor is beschreven, is deze taak belegd bij de PO en de algoritme-expert voor de procesverantwoordelijkheid. Voor de leveranciersverantwoordelijkheid is deze taak belegd bij de CPO.

De derde *lines of defense* wordt gevormd door de financial audit. Deze heeft tot taak om vast te stellen of de eerste en tweede lijn gezamenlijk zodanig hebben gefunctioneerd dat doelstellingen zijn gerealiseerd (doelmatig en doeltreffend) en dat er sprake is van betrouwbare en rechtmatige informatie. Daarnaast is de Algorithm Advisory Board (AAB) een extra onderdeel van deze *lines of defense*.

Het monitoren, onderzoeken en evalueren van de governance op hoog-risico-algoritmetoepassingen (“overkoepelende governance”)

Als specifiek onderdeel van de tweede *lines of defense* is BCO verantwoordelijk voor het regelmatig monitoren, onderzoeken en evalueren van de governance op algoritmetoepassingen. Als blijkt dat er een probleem is, doet BCO een voorstel om de governance aan te passen of om de condities (financiën of deskundigheidsbevordering) aan te passen waaronder de uitvoering van de governance plaatsvindt. De concerndirectie besluit over eventuele voorstellen voor aanpassing van de (uitvoering van de) governance van algoritmen binnen de gemeente.



3.3.5 Een samenvattend overzicht van taken en verantwoordelijkheden

Niveau	Verantwoordelijk voor gehele keten van toepassing algoritme	(Leveranciers)verantwoordelijk voor algoritme (functionele en technische aspecten)
Bestuurlijk niveau	Wethouder inhoudelijk (bestuurlijk opdrachtgever)	Wethouder verantwoordelijk voor BCO/IIFO
Beleidsniveau	Directeur beleidsafdeling	Directeur IIFO
Uitvoeringsniveau	Proceseigenaar (opdrachtgever)	Ontwikkelfase: operationeel verantwoordelijke voor algoritme ontwikkeling binnen de gemeente (ook bij externe leverancier) Beheerfase: Functioneel beheerder
Controlniveau	Tweede lijn: PO (uitbreiding indien AVG n.v.t.) en BCO voor overkoepelende governance Derde lijn: Financial Audit en Algorithm Advisory Board (AAB)	Tweede lijn: CPO (uitbreiding indien AVG n.v.t.) en BCO voor overkoepelende governance Derde lijn: Financial Audit en Algorithm Advisory Board (AAB)
Communicatieniveau	Proceseigenaar	Proceseigenaar

4 Implementatie van de governance voor risicovolle algoritmetoepassingen in de gemeente Rotterdam

In dit hoofdstuk worden, op basis van de voorgaande hoofdstukken, op hoofdlijnen de eerste stappen beschreven om de governance voor risicovolle algoritmetoepassing in de gemeente Rotterdam te implementeren.



4.1 Personeel en expertise

De implementatie van de bovenstaande governance heeft personele consequenties. Deze zien toe op het aannemen van een algoritme-expert en het uitbreiden van de taken van de PO en CPO. Ook moeten er leden worden gezocht voor Algorithm Advisory Board (AAB).

4.1.1 Het aannemen van een algoritme-expert (profiel)

In de voorgaande governance is een algoritme-expert die de PO en de CPO ondersteunt bij zijn of haar taken en die als secretaris van het Algorithm Advisory Board fungeert. Deze persoon moet in staat zijn om ethische en juridische principes door te vertalen naar algoritmen. Dit vereist enerzijds het goed kennen en begrijpen van ethische principes (zoals de algemene beginselen van behoorlijk bestuur) en anderzijds diepgaande kennis van hoe algoritmen werken en waar risico's zitten. Een voorbeeld daarvan is dat het niet opnemen van een bepaald kenmerk in een model niet automatisch leidt tot het niet maken van onderscheid op basis van zo'n variabele.

Momenteel beschikt de gemeente Rotterdam zowel over ethisch- en juridisch onderlegde experts, als over algoritme-experts (vaak ontwikkelaars). Wat echter ontbreekt is iemand die beide werelden aan elkaar kan verbinden. Daarom stellen we voor een nieuwe rol binnen de gemeente Rotterdam te introduceren die in staat is die verbinding te leggen. Deze algoritme-expertrol komt onder IIFO te vallen en gaat concernbreed ondersteunen met advies over de ethisch verantwoorde toepassing van algoritmen. Deze expert kan worden ingeroepen bij het uitvoeren van een DEDA of kan om advies worden gevraagd door bijvoorbeeld ontwikkelaars (tweedelijns). Deze persoon dient een wiskundige achtergrond te hebben en ervaring met juridische ethische thema's.

4.1.2 Het uitbreiden van de taken van de Privacy Officer (PO)

Als er sprake is van een hoog-risico-algoritmetoepassing hebben de PO's de taak om hiermee rekening te houden bij het opstellen van de DPIA of, als er geen persoonsgegevens verwerkt worden, bij het opstellen van de AIA. Beide taken vereisen inzicht in de werking en (mogelijke) ontwikkeling van een algoritmen. De meeste PO's hebben een juridisch profiel. Het is daarom noodzakelijk om de PO's die dat nodig hebben, aanvullende training te bieden.



4.1.3 Samenstellen Algorithm Advisory Board (AAB)

Zoals eerder werd beschreven, bestaat de AAB uit experts van buiten de gemeente. Te denken valt aan governance-experts, -ethici, -juristen en algoritme-experts. In het bijzonder valt natuurlijk te denken aan wetenschappers die onderzoek doen naar ethiek van algoritmen. Deze moeten worden benaderd voor deze rol. De leden van ABB krijgen een vergoeding (vergelijkbaar met de rekenkamer) voor hun werkzaamheden en worden voor vier jaar benoemd door de gemeente. Een lid van de ABB kan één keer herbenoemd worden.

4.2 Verdere uitwerking governance (standaardiseren AIA, integratie in DPIA en verdere integratie met aanpalende governance)

De uitwerking van de governance wordt gericht op het standaardiseren van de AIA en eventuele integratie van de AIA in de DPIA. Voor de hand ligt het maken van een smart standaardformulier dat, nadat een ARA is uitgevoerd, een bijpassende DPIA (persoonsgegevens) of AIA (wanneer geen persoonsgegevens) genereert. Verder is een uitwerking van deze governance gebaat bij een verdere integratie met andere governance structuren zoals AVG governance, de governance voor informatiebeveiliging (BIO) en de ontwikkelingen om te komen tot een datagovernance.

4.3 Communicatie en cultuur

Van belang is dat binnen de gemeente steeds meer medewerkers een 'antenne' hebben voor de verantwoorde toepassing van algoritmen. De drie vragen in de Algorithm Risk Assessment (ARA) bieden daarvoor een goed uitgangspunt. Het verspreiden van de ARA (en daarmee de redeneerlijn binnen de governance) binnen de organisatie is van groot belang voor het implementeren van deze governance. Aanvullend hierop kan een programma voor de bewustwording over algoritmen en risico's worden opgezet. Dit programma wordt concernbreed uitgezet met een focus op clusters, aangezien zij proceseigenaar zijn en de procesverantwoordelijkheid dragen.



Verklarende afkortingenlijst

Afkorting	Verklaring
AAB	Algorithm Advisory Board (Nederlands: Algoritme Adviesraad)
Abbb	De algemene beginselen van behoorlijk bestuur
AIA	Algorithm Impact Assessment (Nederlands: Algoritme Impactbeoordeling)
ARA	Algorithm Risk Assessment (Nederlands: Algoritme Risicobeoordeling)
AVG	Algemene verordening gegevensbescherming
Awb	Algemene wet bestuursrecht
BCO	Bestuurs- en Concernondersteuning
BIO	Baseline Informatiebeveiliging Overheid
CPO	Concern Privacy Officer
DEDA	De Ethische Data Assistent
DPIA	Data Protection Impact Assessment
EC	Europese Commissie
IIFO	Innovatie, Informatievoorziening, Facilitair en Onderzoek
PO	Privacy Officer