Gemeente Amsterdam

Handreiking i-kaders voor verbonden partijen

1 mei 2023

Inhoud

1. Kaders voor verbonden partijen 3
1.1 Inleiding 3
1.2 Leeswijzer 3
2. Grondslag in Nota beleidskader verbonden partijen 4
2.1 Oprichting van een verbonden partij 4
2.2 Beheer van verbonden partijen 4
2.3 Samenvattend overzicht 5
3. Uitgangspunten in het I-domein 5
3.1 Voorwaarden op gebied van dataverwerking en informatiebeveiliging 5
3.2 Voorwaarden ten behoeve van de bescherming van persoonsgegevens 7
3.3 Gebruik maken van nieuwe technologie (algoritmen) 8
3.4 Voorwaarden duurzame toegankelijkheid van informatie 9
3.5 Voorwaarden openbaarheid van informatie 9
3.6 Analyse kaders I-domein op basis van een Quick Scan 10
3.7 Samenvattend overzicht 13

Bijlage 1: Checklist vragen bij oprichting en beheer voor dataverwerking en informatiebeveiliging ... 14
Bijlage 2: Checklist vragen bij oprichting en beheer voor bescherming persoonsgegevens 15
Bijlage 3: Checklist voor algoritme gebruik 16
Bijlage 4: Checklist voor duurzame toegankelijkheid van informatie 19
Bijlage 5: Proces gegevensdeling inclusief vragen 21
Bijlage 6: Concept Informatieovereenkomst voor uit Amsterdam gemandateerde taken 24

1. Kaders voor verbonden partijen

1.1 Inleiding

De gemeente Amsterdam voert haar taken uit op basis van wet- en regelgeving. Zij stelt waar nodig eigen kaders waaraan de eigen organisatie moet voldoen. Binnen het I-domein zijn kaders opgesteld die gericht zijn op informatievoorziening, we noemen dit de i-kaders. Deze kaders gaan over datadeling, gegevensbescherming, informatiebeveiliging, duurzame toegankelijkheid, openbaarheid en ethische afwegingen bij datagebruik. De gemeentelijke kaders zijn direct van kracht als de gemeente een taak of dienst zelf uitvoert of laat uitvoeren. Wanneer de gemeente ertoe besluit of verplicht is om deze taak via een verbonden partij uit te voeren zijn deze kaders ook van toepassing. Verbonden partijen zijn rechtspersonen waarin de gemeente een financieel én bestuurlijk belang heeft. Het gaat hierbij om privaatrechtelijke rechtspersonen (vennootschappen, stichtingen, verenigingen, coöperaties), gemeenschappelijke regelingen en ook om Europese groeperingen voor territoriale samenwerking (EGTS).

Financieel belang
De gemeente heeft een financieel belang als middelen beschikbaar zijn gesteld die ze kwijt is wanneer de verbonden partij failliet gaat. Een ander kenmerk van een financieel belang is dat de gemeente aansprakelijk is als de verbonden partij haar verplichtingen niet nakomt. Van financieel belang is sprake als de gemeente bijvoorbeeld aandeelhouder is, aan een gemeenschappelijke regeling deelneemt, een lening heeft verstrekt en/of een garantie heeft afgegeven.

Bestuurlijk belang
Een bestuurlijk belang houdt in dat de gemeente zeggenschap over de rechtspersoon heeft. Dat kan via vertegenwoordiging in het bestuur zijn of via stemrecht. Er is een bestuurlijk belang als een wethouder, raadslid of ambtenaar namens de gemeente in het bestuur van de verbonden partij plaatsneemt of namens de gemeente stemt. Bij zitting in een toezichthoudend orgaan is alleen een bestuurlijk belang als de gemeente in dit toezichthoudend orgaan een besluitvormende stem heeft.

1.2 Leeswijzer

In deze handreiking wordt verder uitgewerkt op welke wijze de gemeente uitvoering geeft aan de (gemeentelijke) i-kaders bij de oprichting en het beheer van verbonden partijen. De handreiking is bedoeld voor organisatieonderdelen die een verbonden partij gaan oprichten of gaan verlengen.

Het doel van deze handreiking is om ambtenaren die betrokken zijn bij de oprichting en het beheer van verbonden partijen een beeld te geven op welke wijze de kaders in het I-domein van invloed kunnen zijn op hun werkzaamheden enerzijds en anderzijds voor de ambtenaren die betrokken zijn in het I-domein om inzicht te geven in welke rol zij hebben als adviseur bij de oprichting en het beheer van verbonden partijen. Op basis van deze kaders kan de gemeente sturen op het voldoen aan de gestelde kaders als taken worden gemandateerd/ overgedragen aan externe partijen. Het toepassen van de kaders zal altijd op maat gemaakt moeten worden, hiervoor is betrokkenheid nodig uit het I-

domein. Vooralsnog wordt de handreiking gebruikt bij een startgesprek met de verbonden partij. Vervolgens zal de inzet vanuit het I-domein vooral gericht zijn op toezicht.

Deze notitie gaat eerst kort in op de onderliggende beleidskaders bij Directie Middelen en Control en bij de informatievoorziening. Vervolgens schetst het in de bijlagen de praktische vragen die beantwoord moeten worden bij inrichting of beheer van een verbonden partij.

2. Grondslag in Nota beleidskader verbonden partijen

In de Nota beleidskader verbonden partijen (Nota) is vastgelegd dat bij het oprichten van een verbonden partij en het beheer van bestaande verbonden partijen wet- en regelgeving met betrekking tot informatievoorziening en digitalisering van toepassing is.

2.1 Oprichting van een verbonden partij

Aan het oprichten van een verbonden partij gaat een denkproces en een besluitvormingsproces vooraf zoals beschreven staat in de Nota. Het bestaansrecht van een verbonden partij is (primair) gelegen in het borgen van het publiek belang. Bij de oprichting van een verbonden partij ligt het zwaartepunt vanuit het perspectief van het I-domein op de zogenaamde onderzoeksfase. In deze fase wordt nader onderzocht of de beoogde rechtsvorm het meest passend is voor het gestelde publiek belang. De randvoorwaarden en uitgangspunten op het gebied van beleids- en bedrijfsvoering, personeel, (good) governance, financiën en voldoen aan wet- en regelgeving, waaronder dataverwerking worden benoemd.

In deze fase wordt bedacht welke bevoegdheden van de gemeente eventueel overgaan naar de verbonden partij, welke contracten moeten worden afgesloten en welk toezicht de gemeente wil houden op de uitvoering van de activiteit van de verbonden partijen. Elk van deze onderwerpen heeft mogelijk een effect op de afspraken die moeten worden gemaakt met een verbonden partij in het kader van het I-domein. Voor aanvullende afspraken met de verbonden partij over onderstaande onderwerpen kan gebruik worden gemaakt van de informatieovereenkomst uit bijlage 6. Het vastleggen en concretiseren van de afspraken rondom digitalisering en informatievoorziening in bijvoorbeeld samenwerkingsovereenkomsten vindt plaats in de beheerfase.

Toetsing van de impact van kaders uit het I-domein vindt plaats in de onderzoeksfase van de oprichting van een verbonden partij door middel van een startgesprek.

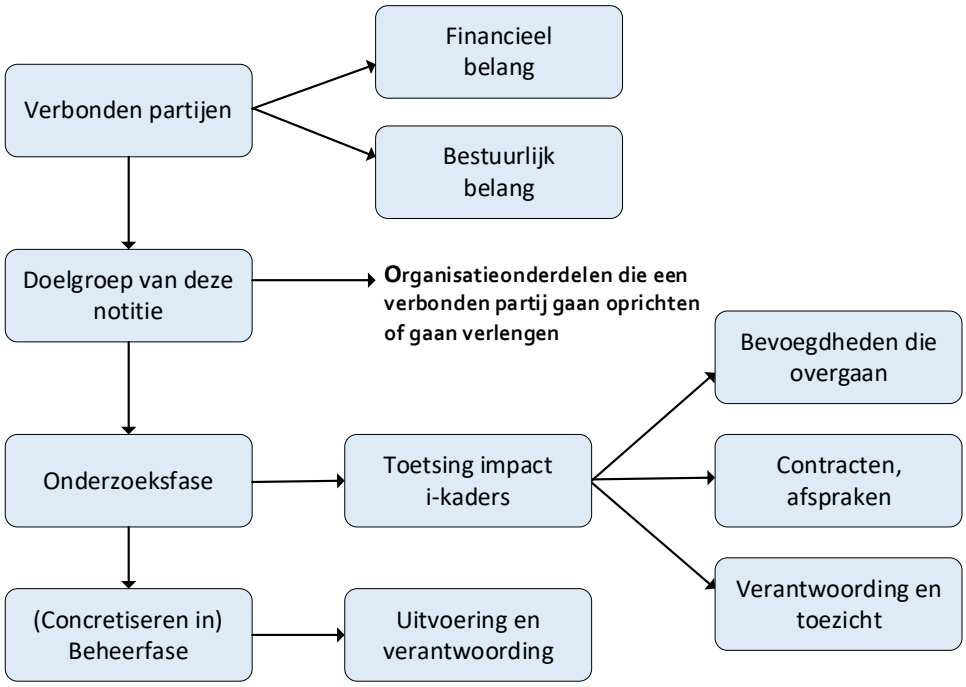
2.2 Beheer van verbonden partijen

Op het moment dat een verbonden partij is opgericht gaat deze over in de beheerfase. Op dat moment wordt vanuit de gemeente gemonitord of en hoe taken/opdrachten die de verbonden partij uitvoert ook daadwerkelijk worden uitgevoerd en of de verbonden partij ook op een maatschappelijk verantwoorde wijze uitvoering geeft.

In de beheerfase ligt de nadruk op de uitvoering van de kaders door de verbonden partij en het voldoen aan de kaders. Dit is de verantwoordelijkheid van de betreffende verbonden partij. Het I-domein van de gemeente houdt daarop toezicht.

De gemeente hecht veel belang aan goed beleid ten aanzien van maatschappelijk verantwoord ondernemen (MVO). Als publiek aandeelhouder verwacht de gemeente van haar deelnemingen en overige verbonden partijen dat ze oog hebben voor bredere publieke belangen, zoals duurzaamheid, inclusiviteit, goed werkgeverschap en de maatschappelijke impact van digitalisering en informatievoorziening. Bij het beheer van de verbonden partijen moet rekening worden gehouden met de kaders vanuit het I-domein. Ook blijft de gemeente in de meeste gevallen een formeel toezicht houden met betrekking tot de taak die een verbonden partij voor de gemeente uitvoert.

2.3 Samenvattend overzicht



3. Uitgangspunten in het I-domein

Het I-domein kent regels en gemeentelijke uitgangspunten die moeten worden nageleefd en gemonitord, op het gebied van data, bescherming persoonsgegevens, informatiebeveiliging, duurzame toegankelijkheid van informatie en openbaarheid. Deze regels en uitgangspunten spelen ook een rol bij de oprichting en het beheer van een deelneming of een verbonden partij. De meeste van de genoemde regels en uitgangspunten zijn onderdeel van de Gemeentelijke Inkoop bij IT Toolbox (GIBIT). Deze uniforme voorwaarden helpen gemeenten bij het professionaliseren van de inkoop van ICT-diensten en –producten. Hieronder wordt per discipline uit het I-domein een kort overzicht gegeven van de belangrijkste gemeentelijke regels en kaders die van invloed zijn bij verbonden partijen. Voor de betrokken ambtenaar is het nuttig om eerst de quickscan uit te voeren en vervolgens de risicogebieden nader te onderzoeken.

3.1 Voorwaarden op gebied van dataverwerking en informatiebeveiliging

Bij de oprichting moet worden nagedacht over datagovernance in de verbonden partij. In de datagovernance is opgenomen hoe wordt omgegaan met data en welke rollen en

verantwoordelijkheden hierbij van belang zijn. Afhankelijk van of de dataverwerking een onderdeel van de uitvoering van het publiek belang is of niet kan de gemeente hier verder gaande eisen aan stellen bij de oprichting.

Indien dataverwerking een onderdeel is van de uitvoering van het publiek belang dan moet op basis van de Amsterdamse datagovernance een datastrategie[1] worden opgesteld. In de datastrategie staat centraal dat de Amsterdammers zeggenschap krijgen over hun data. Deze zeggenschap kan beperkt worden op basis van wet- en regelgeving[2]. Daarnaast wordt vastgelegd dat data over de stad beschikbaar gesteld moeten worden voor de stad. Dit moet zonder onevenredige inspanning of kosten mogelijk zijn. Daarnaast zijn er uitzonderingen op de data die beschikbaar kunnen worden gesteld, bijvoorbeeld persoonsgegevens, economische of financiële belangen, opsporing en vervolging van strafbare feiten, inspectie, controle en toezicht door bestuursorganen[3]. Deze twee uitgangspunten worden vormgegeven via de Tada-waarden.[4]

Datastrategie

1. Amsterdammer heeft zeggenschap over zijn gegevens;
2. Data over de stad is beschikbaar voor de stad.

Als de verbonden partij een gegeven dat als authentiek gegeven in een basis- of kernregistratie beschikbaar is, nodig heeft bij het vervullen van een gemeentelijke taak, moet deze partij dit gegeven gebruiken. Als deze partij een onjuistheid of het ontbreken van een authentiek gegeven in een basis- of kernregistratie meent te zien, moet deze hierover onderbouwd terug melden aan de stelselbeheerder[5]. Ten slotte moeten de rechten op de data die in het kader van het publiek belang worden verzameld of gecreëerd toekomen aan de gemeente. Hierbij hoeft de gemeente niet gebruik te maken van de wet- en regelgeving die dergelijke rechten al vast heeft gelegd[6]. De afspraken hierover moeten worden vastgelegd in een oprichtingsakte of beheerafspraak.

Authentieke gegevens moeten uit de basis- of kernregistraties worden afgenomen.
Als de verbonden partij constateert dat dit authentieke gegeven onjuist is of ontbreekt is terug melden aan de stelselbeheerder verplicht.
De rechten op de data komen aan de gemeente toe als de data in het kader van publiek belang zijn verzameld of gecreëerd.

Een specifiek onderdeel van de dataverwerking is de informatiebeveiliging. Het doel van informatiebeveiliging is het waarborgen van: de beschikbaarheid van gegevens en systemen (zijn de gegevens continue beschikbaar), de integriteit van gegevens (zijn de gegevens juist, actueel en volledig) en de vertrouwelijkheid van gegevens (zijn de gegevens alleen beschikbaar voor bevoegden). Voor de informatiebeveiliging wordt de Baseline Informatiebeveiliging Overheid (BIO) toegepast, die is geconcretiseerd in een beleidskader informatiebeveiliging.

---

[1] Collegebesluit 12-1-2021
https://amsterdam.raadsinformatie.nl/document/9648497/1/Datastrategie%20gemeente%20Amsterdam%202021-2022
[2] art. 2.54 lid 3 Wet brp; art. 41 Uitvoeringswet Algemene verordening gegevensbescherming
[3] Arti. 3.1 lid 1 en 3 Wet open overheid (Woo)
[4] Gebaseerd op het Tada-Manifest https://tada.city/
[5] Terugmelding.Basisinformatie@amsterdam.nl (artikel 9-10 van het Reglement basisinformatie 2018).
[6] art. 1 lid 2 Richtlijn hergebruik overheidsinformatie; art. 2 lid 1 onder b Wet hergebruik van overheidsinformatie; art. 5.1 lid 1 onder c en lid 2 onder f Woo

In het kader van het voeren van beheer hangt het af van wat bij de oprichting van de verbonden partij is afgesproken. Op het moment dat er bij de oprichting afspraken zijn gemaakt over de dataverwerking en informatiebeveiliging zal bij het beheer van de verbonden partij moeten worden vastgesteld of deze ook daadwerkelijk worden nageleefd. De verbonden partij legt hierover periodiek verantwoording af aan Amsterdam. Via de jaarlijkse verantwoording in bijvoorbeeld een jaarverslag kan worden vastgesteld of wordt voldaan aan de eisen. Voor verbonden partijen waarbij geen afspraken zijn gemaakt over dataverwerking is dit een onderwerp waarover de gemeente als publiek aandeelhouder in algemene zin vragen kan stellen of de organisatie voldoet aan de eisen van informatieveiligheid. De gemeente heeft als ambitie om zorgvuldig om te gaan met de verwerking van data. Zij vraagt als aandeelhouder op basis van deze ambities aandacht voor de gemeentelijke kaders. Zie bijlage 1 voor meer informatie over dataverwerking en informatiebeveiliging.

3.2 Voorwaarden ten behoeve van de bescherming van persoonsgegevens

Wanneer in het kader van het publieke belang persoonsgegevens worden verwerkt moeten er bij de oprichting van de verbonden partij afspraken worden vastgelegd over de afbakening van rol, taken en verantwoordelijkheden van verbonden partijen en de gemeente Amsterdam. Per verbonden partij moet worden vastgesteld wie de verwerkingsverantwoordelijke, gezamenlijke verwerkingsverantwoordelijken of verwerkers van persoonsgegevens zijn om te borgen dat deze persoonsgegevens worden beschermd en het voor burgers duidelijk is tot wie zij zich kunnen wenden voor bijvoorbeeld uitoefening van hun rechten op grond van de Algemene verordening gegevensbescherming (Avg). Om dit vast te stellen kan de bijgevoegde checklist (bijlage 2) gebruikt worden.

Bij verbonden partijen die in het kader van het publieke belang persoonsgegevens verwerken geldt naast de Avg tevens het Stedelijk Kader verwerking persoonsgegevens Amsterdam[7]. Daarin staan onder meer de rollen en verantwoordelijkheden beschreven. Bij het overdragen van processen en/ of systemen waarin persoonsgegevens worden opgeslagen dient in samenwerking met de Privacy Officer van het betreffende cluster een pre-DPIA/quickscan te worden uitgevoerd. Als hieruit een verhoogd risico wordt geconstateerd, dient er een Data Protection Impact Assessment (DPIA) te worden uitgevoerd.[8]

In het kader van het voeren van beheer hangt het af van wat in bij de oprichting van de verbonden partij is afgesproken. Op het moment dat er bij de oprichting afspraken zijn gemaakt over de borging van gegevensbescherming zal in het beheer moeten worden gecontroleerd of deze ook daadwerkelijk worden nageleefd. Voor verbonden partijen waarbij geen afspraken zijn gemaakt over de borging van gegevensbescherming is dit een onderwerp waarover de aandeelhouder in algemene zin vragen kan stellen in het kader van het voldoen aan de eisen van de Avg. De gemeente streeft naar zorgvuldige omgang met persoonsgegevens. Zij vraagt als aandeelhouder daarom ook aandacht voor de gemeentelijke kaders en stelt hierover verwachtingen op. Zie bijlage 2 voor meer informatie over borging van persoonsgegevens bij een verbonden partij.

[7] Zie: https://intranet.amsterdam.nl/kennis-beleid/bedrijfsvoering/informatie/privacy/taken-verantwoordelijkheden/
[8] Zie: https://intranet.amsterdam.nl/kennis-beleid/bedrijfsvoering/informatie/privacy/

Als afspraken over borging van gegevensbescherming zijn vastgelegd bij de oprichting, dan wordt in de beheerfase getoetst of deze afspraken worden nageleefd.
Als er geen afspraken zijn vastgelegd bij de oprichting, dan wordt door de gemeente de borging van gegevensbescherming als onderwerp meegegeven om vragen over te stellen als aandeelhouder.

3.3 Gebruik maken van nieuwe technologie (algoritmen)

De gemeente Amsterdam heeft kaders voor het gebruik van algoritmische toepassingen. Er zijn op dit moment verschillende definities voor 'algoritme' of 'algoritmische toepassing'. Vanuit de Rijksoverheid en de Europese Commissie wordt gewerkt aan bruikbare en heldere definities. Tot die tijd hanteren we 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 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."*[9]

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 en als het gebruik valt onder de verantwoordelijkheid van de gemeente Amsterdam, dan nemen we het algoritme op in het Algoritmeregister en dient de verbonden partij passende instrumenten in te zetten voor het beheersen van risico's van het gebruik van algoritmen.

Artificial Intelligence
Hieronder vallen zowel simpele rekenmodellen (bijvoorbeeld berekeningen van uitkeringen) als 'machine-learning-modellen' (bijvoorbeeld camera's die afval herkennen).
De gebruikte algoritmen worden bij impact voor de Amsterdammer of bedrijven en als het gebruik valt onder de verantwoordelijkheid van de gemeente Amsterdam opgenomen in het Algoritmeregister van Amsterdam.

Het gebruik van algoritmen is maatschappelijk gezien omstreden vanwege de mogelijke discriminatie of uitsluiting van personen. De gemeente wil voorkomen dat met het gebruik hiervan inbreuk wordt gemaakt op de bescherming van persoonsgegevens en stelt daarom extra eisen bij het inkopen van Artificial Intelligence (AI) diensten.

Het gebruik van algoritmen en AI is niet een onderwerp waarover bij de oprichting van de deelneming altijd specifiek afspraken worden gemaakt. Bij de oprichting is nog niet (altijd) duidelijk of de verbonden partij gebruik gaat maken van algoritmen of AI. Wel kan, ook als inzet algoritme nog niet duidelijk is, in het kader van het beheer van verbonden partijen worden gewezen op de verantwoordelijkheid die de verbonden partij heeft gezien het maatschappelijke debat en kan worden opgeroepen om eisen die gelijk zijn aan die van Amsterdam te hanteren voor de inkoop en het gebruik ervan. Is bij oprichting reeds duidelijk dat algoritmen zullen worden ingezet, dan dient gebruik te worden gemaakt van de eigen inkoopeisen voor algoritmen van de gemeente Amsterdam. Zie bijlage 3 voor meer informatie over de vereisten en vragen rondom algoritmen en verbonden partijen.

[9] Zie: raadsinformatiebrief Algoritme Lifecycle Programma d.d. 9 juli 2021

De gemeente Amsterdam heeft eigen inkoopeisen voor algoritmen opgesteld. Verbonden partijen worden opgeroepen om deze inkoopeisen toe te passen bij het gebruik van algoritmen.

3.4 Voorwaarden duurzame toegankelijkheid van informatie[10]

De gemeente Amsterdam moet voldoen aan de wettelijke kaders die gaan over de duurzame toegankelijkheid van informatie. Daarnaast zijn ook in de Amsterdamse Archiefverordening en het Besluit Informatiebeheer afspraken vastgelegd over de bestuurlijke verantwoordelijkheid en het ambtelijke beheer van informatie. Deze regels borgen dat de gemeente transparant kan zijn over haar handelen. De duurzame bewaring van informatie is hiervoor van essentiële waarde. De Gemeentearchivaris houdt toezicht op de duurzame bewaring van informatie. Het bestuur is verantwoordelijk voor de duurzame bewaring van informatie.

De keuze om in een samenwerkingsverband of andere vorm van verbondenheid taken/ bevoegdheden te mandateren, delegeren of toekennen heeft consequenties voor de verantwoordelijkheid en de inrichting van informatiebeheer. Bij de oprichting van een verbonden partij dienen er afspraken gemaakt te worden over de borging van duurzame toegankelijkheid en toezicht. Wanneer een taak wordt gemandateerd, blijft de gemeente bestuurlijk verantwoordelijk en blijft de Gemeentearchivaris toezicht houden op deze taak. Daarom dienen er bij de oprichting van een verbonden partij meteen afspraken gemaakt te worden over het organiseren van toezicht, wat de verbonden partij wel en niet met de informatie mag doen en over momenten waarop de informatie weer terug dient te worden gebracht naar de gemeente. In bijlage 5 staat hierover meer informatie.

In de beheerfase moeten afspraken gemaakt worden over de bewaring, beschikbaarstelling en vernietiging van informatie. Hierbij dient ook aandacht worden geschonken aan de openbaarheid van informatie. Duurzame toegankelijkheid van informatie is namelijk essentieel voor openbaarheid van publieke informatie. Zie bijlage 4 voor meer informatie.

3.5 Voorwaarden openbaarheid van informatie

Toegang tot publieke informatie is een recht van de burger. Dit recht is vastgelegd in de Wet open overheid (Woo). De Woo geeft regels voor actieve - en passieve openbaarheid, waarbij het uitgangspunt is dat informatie openbaar wordt gemaakt tenzij er een zwaarwegende wettelijke reden is om dit (nog) niet te doen. Het college van B&W is verantwoordelijk voor openbaarheid, ook als de gemeentelijke taak door een derde wordt uitgevoerd. De informatie die ontstaat bij het uitvoeren van die taak valt onder de Woo en de verplichtingen die de gemeente in dat kader heeft. In de onderzoeksfase dienen er afspraken te worden gemaakt over de afhandeling van Woo-verzoeken en over actief openbaar te maken informatie. Deze afspraken moeten in afstemming met de informatiecommissaris worden gemaakt.

Passieve openbaarheid
Iedereen mag een verzoek indienen om publieke informatie openbaar te maken: een Woo-verzoek. Bij de oprichting van de verbonden partij en wanneer er een verzoek wordt ingediend moet er onder andere rekening worden gehouden met de volgende onderdelen:

- Afronding van het verzoek binnen de wettelijke termijnen.

[10] Zie: https://www.amsterdam.nl/stadsarchief/organisatie/toezicht/toezicht-wettelijk/

- Afwegen openbaarheid per alinea: wettelijke weigeringsgronden.
- Alle informatie verzamelen die onder de reikwijdte van het verzoek valt: gaat om gemeentelijke informatie, waar die ook ligt binnen de gemeente of bij de verbonden partij.
- Een zienswijze kan gevraagd worden bij belanghebbenden als we denken dat er bezwaar op openbaarmaking kan zijn.
- Hanteren van het openbaar maken van alle beleidsopvattingen van figuren met een publieke functie. Bij alle andere wordt deze informatie geanonimiseerd openbaar gemaakt.

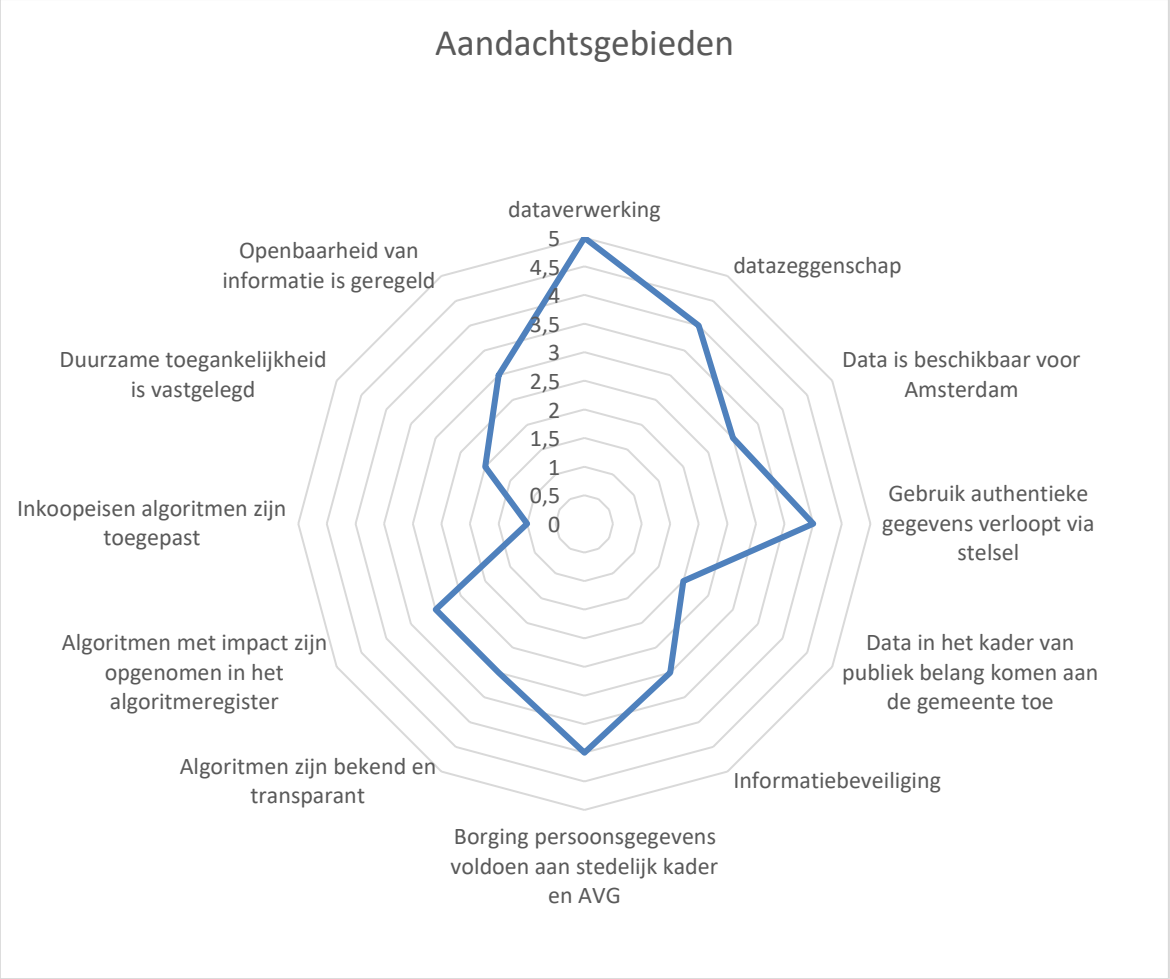
Actieve openbaarheid
De Woo verplicht ons uit eigen beweging informatie openbaar te maken: actieve openbaarheid. Er zijn 11 informatie-categorieën die verplicht actief openbaar gemaakt moeten worden. Daarnaast is er een inspanningsverplichting om meer (beleids)informatie actief openbaar te maken. Informatie wordt openbaar gemaakt via het publicatiekanaal van het Stadsarchief Amsterdam en op termijn via het landelijke platform PLOOI. In de beheerfase dienen er afspraken gemaakt te worden over het organiseren van toezicht, welke informatie wel of niet openbaar wordt gemaakt, waar informatie wordt gepubliceerd en hoe wij dat in samenspraak organiseren.

3.6 Analyse kaders I-domein op basis van een quickscan

Om te bepalen welke kaders nadere afspraken nodig hebben is het van belang om de verschillende onderwerpen te wegen. Dit kan door het uitvoeren van een quickscan. Deze quickscan wordt uitgevoerd door de betrokken directie en ondersteund door het I-domein voorafgaand aan de oprichting van een verbonden partij. Op basis van de quickscan wordt duidelijk op welke onderwerpen nader onderzoek nodig is.

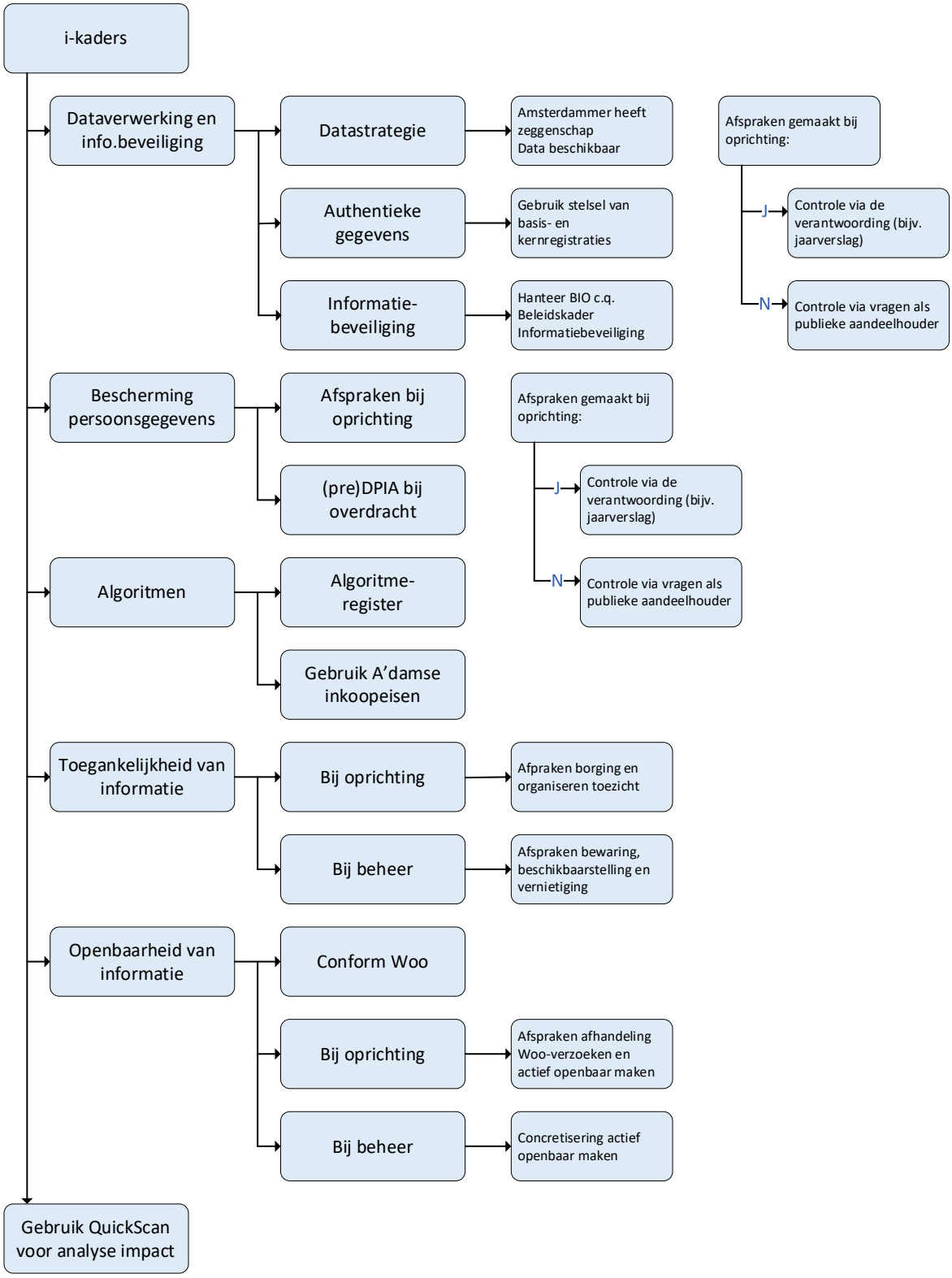
Hieronder is ter illustratie een afbeelding opgenomen van een mogelijke quickscan. Door middel van de score op een vijfpuntsschaal wordt het risico/ aanwezigheid van het aandachtsgebied bepaald.

	Score (range) van mate van risico					score
Aandachtsgebied	Laag 1	2	3	4	Hoog 5	
dataverwerking	zonder persoonsgegevens				complex	5
datazeggenschap	Amsterdammer heeft zeggenschap				niet ingeregeld	4
Data is beschikbaar voor Amsterdam	Ja				Nee	3
Gebruik authentieke gegevens verloopt via stelsel	ja				niet vastgelegd	4
Data in het kader van publiek belang komen aan de gemeente toe	ja				nee	2
Informatiebeveiliging	basis ingericht					3
Borging persoonsgegevens voldoen aan stedelijk kader en AVG	ja				niet vastgelegd	4
Algoritmen zijn bekend en transparant	ja				nee	3
Algoritmen met impact zijn opgenomen in het algoritmeregister	ja				nee	3
Inkoopeisen algoritmen zijn toegepast	ja				nee	1
Duurzame toegankelijkheid is vastgelegd	ja				nee	2
Openbaarheid van informatie is geregeld	ja				nee	3



De hoogste risico's in dit voorbeeld betreffen dus Dataverwerking, Datazeggenschap, Gebruik authentieke gegevens verloopt via stelsel, en Borging persoonsgegevens voldoen aan stedelijk kader en AVG. Dat zijn dus de (eerste) aandachtsgebieden die nadere aandacht vergen.

3.7 Samenvattend overzicht



Bijlage 1: Checklist vragen bij oprichting en beheer voor dataverwerking en informatiebeveiliging

Vragen/onderwerpen bij oprichting

- Worden gegevens buiten het eigen inhoudsdomein gedeeld en hergebruikt voor zover wet- en regelgeving dat toestaan?
- Gegevens worden op verantwoorde wijze beschikbaar gesteld?
- Gegevens worden op transparante, verantwoorde en controleerbare wijze gebruikt
- Is sprake van inzet van algoritmen?
- Bepaal welke algemene (ISO 27001/2) en sector/branche specifieke regelgeving op het gebied van informatiebeveiliging van toepassing is.
- Bepaal hoe de governance op het gebied van informatiebeveiliging wordt ingericht (directie, rol van een CISO, bestuur, toezicht).
- Maak afspraken over de verantwoording op het gebied van informatiebeveiliging, zowel richting directie en bestuur als richting de gemeente (inhoud, diepgang, frequentie, tijdstip, periodieke of incidentele audits). Bepaal welke (vertrouwelijke) rapportages beschikbaar worden gesteld aan de gemeente Amsterdam.
- Maak afspraken over het onderhouden van contacten op het niveau van de CISO van de verbonden partijen met de gemeente Amsterdam
- Bepaal hoe en wanneer informatie wordt uitgewisseld inzake incidenten en datalekken.

Vragen/onderwerpen bij beheer:

- Op welke wijze geeft de verbonden partij invulling aan de bewustwording van informatiebeveiliging en dataverwerking?

Monitoringsmogelijkheden:

- Jaarverslag.
- ISO 27000 certificering
- Jaarlijks rapportage over het voldoen aan afgesproken beveiligingskaders, inclusief eventuele auditrapportages

Bijlage 2: Checklist vragen bij oprichting en beheer voor bescherming persoonsgegevens

Vragen/onderwerpen bij oprichting

- Wil de verbonden partij persoonsgegevens verwerken in het kader van het publieke belang?
- Is de verbonden partij verantwoordelijke voor de verwerking van de persoonsgegevens of is er een gezamenlijke verantwoordelijkheid?
    - Hoe is de formeel-juridische bevoegdheid om het doel en de middelen van de gegevensverwerking vast te stellen geregeld. Hierbij geldt: hoe minder vrijheid er is bij de uitoefening van de opdracht, hoe eerder sprake er is van een verwerker in plaats van een (gezamenlijke) verwerkingsverantwoordelijke. De vraag is eerder is er sprake van een wettelijke taak. Deze wettelijke taak kan worden gemandateerd naar een partij. Deze partij is in dat geval een verwerker.
- Is deze formeel-juridische bevoegdheid afwijkend van de feitelijke invloed die de verbonden partij heeft?
    - Wie bepaalt dan feitelijk het doel en de middelen van de gegevensverwerking?
    - Wie beslist bijvoorbeeld over doelbinding, de opslag van persoonsgegevens en bewaartermijnen?
    - Wie draagt er zorg voor de ontwikkeling van de informatievoorziening en het uitvoeren van eventuele wijzigingen daarin of changes/update?
- Bij wie moet het toezicht liggen op de verwerking van de persoonsgegevens?
    - Wie stelt het informatiebeveiligingsbeleid vast en houdt daar toezicht op?
    - Wie stelt het privacybeleid vast voor de gegevensverwerking en houdt daar toezicht op?
    - Wie meldt en handelt datalekken af?
- Het beeld dat de verbonden partij bij betrokkenen geeft en de verwachtingen van betrokkenen op grond daarvan.
    - Wie stelt de privacyverklaring op?
    - Waar is het loket voor de rechten van betrokkenen? Bepaal hoe de governance op het gebied van gegevensbescherming wordt ingericht (directie, rol van de FG, bestuur, toezicht).
    - Maak afspraken over de verantwoording op het gebied van gegevensbescherming, zowel richting directie en bestuur als richting de gemeente (inhoud, diepgang, frequentie, tijdstip, periodieke of incidentele audits). Bepaal welke (vertrouwelijke) rapportages beschikbaar worden gesteld aan de gemeente Amsterdam.
    - Maak afspraken over het onderhouden van contacten op het niveau van de FG van de verbonden partij met de gemeente Amsterdam
- Is sprake van inzet van algoritmen?

Vragen/onderwerpen bij beheer:

Monitoringsmogelijkheden:

- Jaarverslag. Wanneer een verbonden partij de verwerker is van persoonsgegevens, staat er iets over de uitvoering hiervan in het jaarverslag.

Bijlage 3: Checklist voor algoritme gebruik

Vragen/onderwerpen bij oprichting (vragen uit de risicotool)

- Gebruikt verbonden partij een algoritmische toepassing?[11]
    - Er is hier sprake van software waarin gebruik gemaakt wordt van data- analyse, statistiek en/ of zelflerende logica?
    - De software komt deels of volledig op geautomatiseerde wijze tot een uitkomst (bijv. een advies of voorspelling)
- Hebben die algoritmes die besluit nemen wezenlijke impact op burgers?
    - Het systeem neemt beslissingen of geeft informatie die door de organisatie wordt gebruikt om een beslissing te nemen (bijv. een advies, prioritering, monitoring, categorisering, analyse, signalering, voorspelling, profiel, etc.)
    - Deze beslissingen treffen direct of indirect één of meer Amsterdammers, bezoekers, bedrijven of organisaties in de gemeente.
      Bijvoorbeeld omdat de beslissing rechtsgevolgen heeft, of helpt bepalen wie welke dienstverlening krijgt of omdat de beslissing gebruikt wordt bij de inrichting van de publieke ruimte. Of omdat als er een fout gemaakt wordt door het systeem dit vervelende gevolgen heeft voor betrokkenen.
- Of ze vallen in één van de categorieën die door de Europese Commissie als hoog risico wordt aanduid
    - Biometrische identificatie en categorisering van natuurlijke personen
    - Beheer en exploitatie van kritische infrastructuur
    - Onderwijs en beroepsopleiding
    - Werkgelegenheid, personeelsbeheer en toegang tot zelfstandige arbeid
    - Toegang tot dienstverlening en uitkeringen (beoordelen of personen in aanmerking komen voor overheidsuitkeringen en- diensten of het verlenen, beperken, intrekken of terugvorderen van uitkeringen en diensten)
    - Rechtshandhaving
    - Migratie, asiel en beheer van grenscontroles
    - Rechtsbedeling en democratische processen
- Zitten er aan deze algoritmische toepassingen risico's? voorbeelden risicostellingen:
    - De gemeente is onvoldoende transparant over dit algoritmisch systeem, waardoor Amsterdammers onvoldoende vertrouwen in de gemeente kunnen hebben, of Amsterdammers of toezichthouders het handelen van de gemeente onvoldoende kunnen controleren
    - Minderheden of groepen Amsterdammers met specifieke kenmerken kunnen onbedoeld buitengesloten worden of schade lijden door dit algoritmische systeem
    - Het is onduidelijk waar de benodigde data voor dit systeem te verkrijgen zijn
    - Het is onduidelijk hoe de integriteit van de data te waarborgen en te controleren is, alsmede wie hiervoor verantwoordelijk is
    - De beschikbare data voor dit systeem kunnen in de toekomst wijzigen waardoor het functioneren van het systeem onder druk wordt gezet
    - De uitkomsten van dit algoritmisch systeem kunnen onduidelijk zijn en daarmee tot verkeerde interpretatie door betrokken ambtenaren leiden

[11] Definitie algoritme: Een algoritme of systeem moet in het register als het aan de volgende definitie voldoet:
Software die - door gebruik van data-analyse, statistiek of zelflerende logica - geautomatiseerd voorspellingen doet, besluiten neemt of adviezen geeft, die leiden tot directe of indirecte impact op burgers of bedrijven

    - Voor sommige gegevens die door deze algoritmische toepassing worden gebruikt, heeft de gemeente geen inhoudelijke of juridische argumenten
    - De gemeente kan niet garanderen dat de cybersecurity, van de gehele keten waarbinnen de algoritmen worden gebruikt, in orde is.
    - Het is mogelijk dat Amsterdammers of ambtenaren dit systeem manipuleren of gebruiken voor andere, ongewenste of onverwachte doeleinden
    - Er wordt voor dit algoritmische systeem gebruik gemaakt van profilering van Amsterdammers
    - Het is bij deze algoritmische toepassing wellicht niet mogelijk om de factoren die leiden tot uitkomsten over Amsterdammers te achterhalen, evenals welke aanpassingen in gedrag tot een andere uitkomst hadden geleid
    - Het is niet uit te sluiten dat het algoritmische systeem ongewenste vooringenomenheid (bias) bevat
    - Betrokken ambtenaren kunnen niet afwijken van de uitkomst van het algoritmische systeem, of kunnen het systeem niet tijdelijk stilzetten, op momenten dat zij dit wel zouden willen
    - Sommige data die voor dit systeem worden gebruikt, zijn verkeren in andere toepassingscontexten dan die van het algoritmische systeem zelf
    - Het is onduidelijk hoe de prestaties van het algoritme het best gemeten kunnen worden, of wat de minimale prestatie- eisen zijn
    - Het is mogelijk dat uitkomsten van het algoritmische systeem niet zinvol- door een ambtenaar- kunnen worden gecontroleerd of geïnterpreteerd voordat de gemeente actie onderneemt
    - De gemeente werkt voor dit algoritmische systeem samen met een externe leverancier, waardoor wij de betrouwbaarheid van het systeem mogelijk niet kunnen garanderen
- Mocht er in de toekomst een taak deel of geheel geautomatiseerd worden neem dan contact op met Bestuurszaken.DII@Amsterdam.nl voor juiste afwegingskaders.

Vragen/onderwerpen bij beheer:

- Zie vragen/ onderwerpen bij oprichting
- Bij elke grote of wezenlijke wijziging in gebruikte data of beleidswijziging of wet- en regelgeving of in het algoritme zelf moet men dit opnieuw beoordelen en de vragen onder het kopje oprichting doornemen.
- Een paar voorbeelden voor het herkennen van 'wezenlijke wijziging':
    - Er worden wezenlijk andere gegevens gebruikt in de algoritmetoepassing;
    - De code van het algoritme wordt complexer en wordt meer zelflerend;
    - De status van de resultaten van de algoritmetoepassing wijzigt van een nuttige suggestie voor een besluit naar een geautomatiseerd besluit;
    - Het wordt duidelijk dat de algoritmetoepassing onverwachte neveneffecten heeft die de impact van de algoritmetoepassing in een ander licht stellen, bijvoorbeeld wanneer een algoritmetoepassing gericht op handhaving van regels, vooral bepaalde groepen binnen de samenleving raakt.
    - Er komt een nieuwe volksvertegenwoordiging of bestuur van de overheidsorganisatie die in meerderheid tegen de inzet van de algoritmetoepassing is. Dit wijzigt de politieke legitimering van de algoritmetoepassing en kan ertoe leiden dat de algoritmetoepassing moet worden beëindigd;

- De wettelijke grondslag voor het gebruik van gegevens wordt verruimd, waardoor nieuwe gegevens beschikbaar zijn voor de algoritmetoepassing en de voorwaarden voor de juridische legitimiteit van de algoritmetoepassing veranderen;
- Er ontstaat onrust in de samenleving over de inzet van een algoritmetoepassing, waardoor de maatschappelijke legitimiteit van de algoritmetoepassing afbrokkelt

Monitoringsmogelijkheden:

- Algoritme van verbonden partijen ook in register of andere manier van documenteren publiceren
- Audit
- Richt een evaluatiestructuur/periodiek controlemoment in om te controleren of er wezenlijke wijzigingen zijn

Bijlage 4: Checklist voor duurzame toegankelijkheid van informatie

- Certificering van het verplichte normenstelsel en verklaring van toepasselijkheid (VVT)
- Een assurance-rapport (TPM, bijvoorbeeld ISAE3402 of SOC type 2) van een onafhankelijke derde/auditor die ter zake aantoonbaar deskundig is;

Vragen/onderwerpen bij oprichting

- De keuze om in een samenwerkingsverband taken/bevoegdheden te mandateren, delegeren of attribueren heeft consequenties voor de verantwoordelijkheden en de inrichting van het informatiebeheer.
- Bij mandatering moet er een overeenkomst worden getekend waarin afspraken worden gemaakt over: het beheren van deze informatie conform archiefwet en lokale Amsterdamse verordeningen en regels, hoe informatie over de taak van andere informatie kan worden gescheiden, afhandelen van wob verzoeken, het overbrengen van informatie naar de archiefbewaarplaats, hoe het toezicht wordt vormgegeven, het delen van informatie met derde partijen, etc. hiervoor wordt een standaard overeenkomst opgesteld waarin ook andere i-disciplines zijn vertegenwoordigd. Betrek in een dergelijke situatie altijd de gemeentearchivaris, Afdeling Toezicht.
- Bij mandaat blijft Amsterdam bestuurlijk verantwoordelijk, zal de informatie terug moeten komen naar de Stad en houdt de Gemeentearchivaris van Amsterdam toezicht op de informatie die de betreffende gemandateerde taak aangaat.
- Bij overige rechtsvormen zoals delegatie, gaat ook de verantwoordelijkheid over naar het samenwerkingsverband. Formeel gezien heeft Amsterdam dan op het gebeid van de Archiefwet minder te organiseren, echter in de praktijk is Amsterdam vaak vertegenwoordigd in het bestuur en kan het zinvol of wenselijk zijn dat de gemeentearchivaris van Amsterdam wordt aangesteld als toezichthouder en archiefbewaarplaats voor het samenwerkingsverband. (Voor elke overheidsorganisatie, ook gemeenschappelijke regelingen geldt de Archiefwet en moet er een toezichthouder en archiefbewaarplaats worden aangewezen door het bestuur). Voor vragen, neem contact op met de gemeentearchivaris, team Toezicht.
- Bij de inrichting van een verbonden partij is het betrokken bestuursorgaan (in het geval van gemeente is dat de raad, B&W of de burgemeester) verantwoordelijk voor:
    - het aanwijzen van een archiefbewaarplaats
    - het maken van afspraken m.b.t. de lokale regelgeving (Archiefverordening en Besluit Informatiebeheer) die word gevolgd
    - het maken van afspraken over de uitoefening van het toezicht
    - het maken van afspraken over de financiële aspecten van bovenstaande punten.

Vragen/onderwerpen bij beheer:

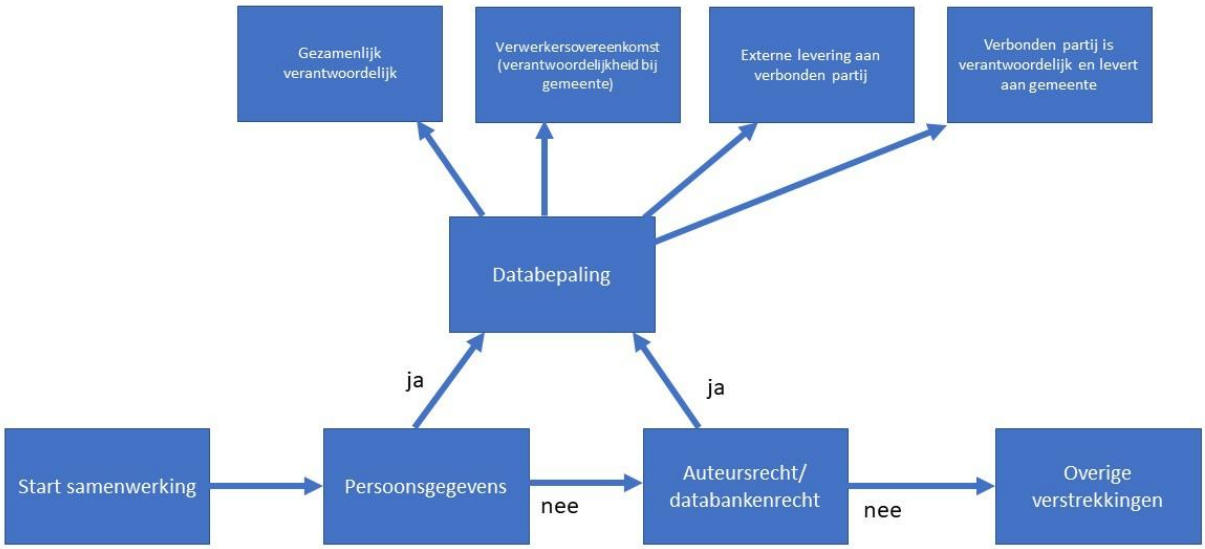
- De proceseigenaar (verbonden partij) is verantwoordelijk voor het informatiebeheer van het proces/project volgens de Archiefverordening 2008.
- Informatiebeheer moet in samenwerkingsverbanden zo veel mogelijk worden ingericht binnen dezelfde (IB) kaders die we binnengemeentelijk stellen (informatie moet compleet, up-to-date, betrouwbaar en authentiek zijn, informatiebeheer vindt volledig digitaal plaats en Informatiebeheer begint voor in het proces):

- De verbonden partij dient informatie voortkomend uit taken die namens de gemeente Amsterdam worden uitgevoerd te beheren conform het meest actuele Besluit Informatiebeheer van Amsterdam
- De verbonden partij dient informatie voortkomend uit taken die namens de gemeente Amsterdam worden uitgevoerd van andere informatie makkelijk te kunnen scheiden.
- De verbonden partij moet informatie overbrengen naar de Archiefbewaarplaats van Amsterdam

Monitoringsmogelijkheden:

De gemeentearchivaris blijft bij gemandateerde taken de toezichthouder van deze gemandateerde taken. Daarvoor kunnen archiefinspecties worden ingezet.

Bijlage 5: Proces gegevensdeling inclusief vragen



Toelichting

Algemeen
De gemeente kan taken uitbesteden. Als de verbonden partij daarbij persoonsgegevens van Amsterdammers verwerkt is het nodig om afspraken te maken over de verantwoordelijkheden en taken bij het beschermen van deze gegevens. Hiervoor wordt gebruik gemaakt van de Databepaling zoals opgenomen in bijlage 6 (artikel 6).
Wat voor soort afspraken nodig zijn is afhankelijk van de vraag of de gemeente alleen of samen met de verbonden partij verantwoordelijk is voor de taak. Standaarden kunnen daarbij een handvat bieden. Databepaling geldt voor gegevens waarop auteurs- of databankenrecht rust (onafhankelijk of het om persoonsgegevens gaat) zoals die uit de Basisregistratie (BRK) en het Handelsregister (HR).

Vragen bij proces in afbeelding hierboven. Worden er persoonsgegevens verstrekt? Als dat het geval is moet er een databepaling worden opgesteld. Deze kent verschillende verschijningsvormen op basis van verantwoordelijkheid.

Als eerste die van gezamenlijke verwerkingsverantwoordelijkheid, waarbij de gemeente én de verbonden partij gezamenlijk verantwoordelijk zijn voor de verwerkingen in de applicatie (en dus hoofdelijk aansprakelijk; art. 6:166 BW). In een dergelijke situatie moeten de gemeente en de aanbieder onderling afspraken maken over hoe zij uitvoering geven aan hun onderlinge verantwoordelijkheden die voortvloeien uit de Avg. Dergelijke afspraken worden vastgelegd in een 'onderlinge regeling' als bedoeld in artikel 26 AVG.

Een tweede vorm is als de gemeente verantwoordelijk blijft over de verstrekte gegevens. Dan moet er een verwerkersovereenkomst worden gesloten als een verbonden partij persoonsgegevens verwerkt of gebruikt in opdracht van de gemeente (art. 28 AVG). De verwerker moet de instructies van de gemeente opvolgen. De gemeente blijft verwerkingsverantwoordelijke. In de standaard

verwerkersovereenkomst (model VNG en aanvullende bepalingen) worden afspraken gemaakt over hoe er met deze persoonsgegevens wordt omgegaan.

De derde verschijningsvorm is die van levering aan de verbonden partij. Een externe leveringsovereenkomst wordt gebruikt om aan verbonden partijen - binnen de kaders van de privacyregelgeving - persoonsgegevens te verstrekken en hierover afspraken vast te leggen.
Bij de externe levering gaat het om een incidentele of terugkerende gegevenslevering van de gemeente aan of externe partij.

De laatste vorm gaat in op de situatie dat de gemeente informatie ontvangt van de verbonden partij. Als de gemeente persoonsgegevens verwerft van een verbonden partij, en deze partij stelt zelf het doel en de middelen van de verwerking vast en dus zelf verantwoordelijk is voor de verwerking van persoonsgegevens, zijn er andere afspraken nodig. Hiervoor kunnen de bepalingen worden gebruikt die van toepassing zijn op een inkoopclausule.

Dus: zelfstandige verwerkingsverantwoordelijkheid aan de zijde van de verbonden partij. In deze situatie is de gebruiker van de applicatie zelfstandig gebonden aan de regels van de AVG. De gemeente heeft geen zeggenschap over de wijze waarop de gebruiker persoonsgegevens verwerkt. De gemeente zou via een inkoopclausule echter wel de gebruiker contractueel kunnen verplichten om zorgvuldig en op een specifieke wijze persoonsgegevens te verwerken.

Bijzondere situatie met betrekking tot persoonsgegevens.
In deze situatie zijn de gemeente en de externe gebruiker ieder verantwoordelijk voor zijn eigen (deel)verwerking. Ook in dat geval kan de gemeente slechts invloed uitoefenen op de wijze van verwerking van persoonsgegevens door met de gebruiker een 'overeenkomst zorgvuldige verwerking' te sluiten. NB hiervoor kunnen de bepalingen voor een zelfstandige verantwoordelijkheid als voorbeeld gebruikt worden. Deze kunnen worden gebruikt als uitgangspunt.
Van een gedeelde verwerkingsverantwoordelijkheid is sprake in de situatie dat verschillende verwerkingen min of meer zijn geïntegreerd zonder dat er sprake is van een gezamenlijke verwerkingsverantwoordelijkheid . Er is sprake van afzonderlijke verwerkingsverantwoordelijkheid per (deel-)verwerking. De betrokkene kan slechts één van de afzonderlijke verantwoordelijken aanspreken. Zie Kamerstukken II 1997-1998, 25892, nr. 3, p. 58. Hier zal de artikel 26 regeling op onderdelen aangepast kunnen worden, bepaalde onderdelen kunnen dan worden gewijzigd of geschrapt.

De databepaling (auteursrecht/ databankenrecht)
De Databepaling geldt in alle gevallen dat er gebruik wordt gemaakt van informatie waarop auteurs- of databankenrecht rust (onafhankelijk of het om persoonsgegevens gaat) zoals die uit de Basisregistratie (BRK) en het Handelsregister (HR). Daarnaast zijn er in specifieke gevallen nog nadere afspraken mogelijk. Data en technologie: geen persoonsgegevens. Dan gelden de formats voor de afspraken die onder deze punten vallen. Dat zijn specifieke afspraken over de rechten op data (auteursrecht, databankenrecht), afspraken bij de inkoop van algoritmen. Is er toch sprake van indirecte of directe persoonsgegevens (NB hier is al snel sprake van, zeker bij het combineren van data)? Dan kunnen deze afspraken gecombineerd worden met de formats die voor de verwerking van persoonsgegevens zijn opgesteld of kan er gekeken worden of in die formats bepalingen/ vergelijkbare items staan die gebruikt moeten worden. Er gelden bij deze type van derde partijen wel algemene eisen en regels voor onder andere archivering, informatiebeveiliging en openbaarheid. Daarvoor worden aanvullende eisen opgenomen in het convenant.

Voorwaarden verstrekkingen door gemeente
In een aantal gevallen zal de gemeente de verbonden partij voorzien van data. Zodra deze data afkomstig is uit basis- of kernregistraties[12] gelden daarvoor specifieke wet- en regelgeving. Bijvoorbeeld is de verstrekking vanuit de Basisregistratie Personen (BRP) gebonden door specifieke regels. Aan deze aanvullende eisen moeten de verbonden partij voldoen voordat een verstrekking mogelijk is.

De gemeente kent verstrekkingen uit basis-, kern- en bronregistraties[13]. De verstrekkingen verlopen via het I-domein door de gemeentelijke verstrekker.[14] Voor de verstrekking van basisgegevens worden de landelijke en gemeentelijke regels en werkwijzen toegepast. Voor de verstrekking van brongegevens (proces-specifiek) gelden de Amsterdamse kaders.

[12] artikelen 9, 10 en 11 van het Reglement basisinformatie 2018
[13] Proces-specifieke gegevens
[14] Vierentwintigste wijzigingsbesluit Bevoegdhedenbesluit ambtelijke organisatie Amsterdam. Vastgesteld 23 november 2021

Bijlage 6: Concept Informatieovereenkomst voor uit Amsterdam gemandateerde taken

Voor u ligt de standaard voor een informatieovereenkomst van de gemeente Amsterdam.

De gemeente Amsterdam heeft de standaard voor een informatieovereenkomst, versie 0.1, bijgewerkt op 28 september 2021.

Deze overeenkomst heeft ten doel contractuele afspraken te maken over het verwerken van informatie in opdracht van de gemeente Amsterdam door <organisatie> in het kader van de aan <organisatie> gemandateerde taken. Het gaat daarbij over het beheren, delen, openbaren, beveiligen en verwerken van informatie.

Informatieovereenkomst uitvoering <naam hoofdovereenkomst>

Gemeente <naam gemeente>, gevestigd te Amsterdam, in deze rechtsgeldig vertegenwoordigd door <heer of mevrouw> <persoonsnaam>, <functie>, hierna te noemen: de Gemeente Amsterdam

Partijen,

{organisatie} gevestigd te <plaatsnaam>, KVK-nummer <nummer> in deze rechtsgeldig vertegenwoordigd door <de heer of mevrouw>, <persoonsnaam> , <functie>, hierna te noemen: <organisatie>

hierna afzonderlijk te noemen "Partij", of gezamenlijk "Partijen"

Overwegen het volgende:

a. <INDIEN VAN TOEPASSING> Partijen hebben op <datum> de <titel hoofdovereenkomst>, hierna Hoofdovereenkomst, afgesloten, op grond waarvan <organisatie> de volgende dienst(en) levert <specificatie dienst(en)>;
b. {organisatie} met ingang van {datum} {ten behoeve van de Hoofdovereenkomst, of andere regeling zoals een opdracht, of gemeenschappelijke regeling} in mandaat taken uitvoert op het gebied van {gemandateerde taken} voor college en uit dien hoofde informatie ontvangt, creëert en (persoonsgegevens) verwerkt;
c. Partijen over het beheer van deze informatie afspraken wensen te maken om te borgen dat aan verplichtingen op grond van de Archiefwet 1995, het Archiefbesluit 1995, de Archiefregeling en de Archiefverordening van de gemeente Amsterdam wordt voldaan;
d. Partijen over het openbaar maken van informatie afspraken wensen te maken om te borgen dat aan verplichtingen op grond van de Wet open overheid (Woo) en de uitgangspunten rondom openbaarheid van de gemeente Amsterdam wordt voldaan;
e. Partijen in het kader van de vervulling van rechten en plichten uit hoofde van de Algemene verordening gegevensbescherming (AVG) afspraken wensen te maken over het verwerken van persoonsgegevens bij de uitoefening van de gemandateerde taken;
f. Partijen ter uitvoering van de Baseline Informatiebeveiliging Overheid (BIO) en het stedelijk kader informatiebeveiliging afspraken wensen te maken, om te borgen dat de informatie op het juiste niveau wordt beveiligd;

g. Partijen overige afspraken wensen vast te leggen, waaronder over de rechten op data, geautomatiseerde besluitvorming, profilering en algoritmen.
h. Gelet op de omstandigheid dat onderwerpen niet {in de Hoofdovereenkomst, mandaat of andere regeling zoals een gemeenschappelijke regeling} zijn vastgelegd, Partijen daarom de volgende afspraken over de verwerking van informatie vastleggen in deze informatieovereenkomst (hierna: de Informatieovereenkomst);

En komen het volgende overeen:

Artikel 1 Definities
Deze overeenkomst verstaat onder:
1.1 college: burgemeester en wethouders van de Gemeente Amsterdam;
1.2 Woo: Wet open overheid15;
1.3 Informatie: alle gegevens die worden gedeeld, gecreëerd en verwerkt ter uitvoering van de door college in mandaat gegeven taken (hieronder vallen onder andere, maar niet beperkt tot, archiefbescheiden in de zin van de Archiefwet 1995 en persoonsgegevens in de zin van de AVG).
1.4 Archiefbewaarplaats: de door college overeenkomstig artikel 31 van de Archiefwet 1995 aangewezen Archiefbewaarplaats.
1.5 Bijlagen: aanhangsels die onlosmakelijk deel uitmaken van deze Informatieovereenkomst.

Artikel 2 Ingangsdatum en duur
2.1 Deze Informatieovereenkomst gaat in op <DATUM> en eindigt op het moment dat het mandaat aan <organisatie> wordt ingetrokken {of de opdracht, machtiging, gemeenschappelijke regeling eindigt}.
2.2 Ten aanzien van de bepalingen betreffende de verwerking van persoonsgegevens eindigt deze overeenkomst op het moment dat {organisatie} de verwerking van persoonsgegevens heeft beëindigd en de afspraken over het teruggeven en/of wissen van persoonsgegevens zijn nagekomen.
2.3 Na beëindiging van de overeenkomst stelt {organisatie} binnen <TERMIJN> alle informatie die in het kader van de uitvoering van de aan {organisatie} gemandateerde gemeentelijke taken zijn ontstaan en welke nog niet zijn overgebracht naar de Archiefbewaarplaats, binnen {termijn} ter beschikking aan college.
2.4 De geheimhoudingsverplichting geldt ook nog na beëindiging van deze overeenkomst.

Artikel 3 Geschillen
3.1 In het geval van een geschil zullen Partijen onverwijld met elkaar in overleg treden om tot een oplossing te komen.
3.2 Partijen zullen zich tot het uiterste inspannen om tot een oplossing te komen. Als Partijen niet tot een oplossing komen, zal het geschil worden voorgelegd aan de bevoegde rechter te Amsterdam.
3.3 Op deze Overeenkomst is Nederlands recht van toepassing.
3.4 Partijen kiezen domicilie te Amsterdam.

Artikel 4. Verantwoordelijkheden {organisatie} ten aanzien van de informatie
4.1 {organisatie} verplicht zich tot het vormen en beheren van een archief van alle informatie die {organisatie} na ingangsdatum vanwege de gemandateerde taken

[15] Tot 1-5-2022 wordt de Wet openbaarheid van bestuur toegepast.

ontvangt, opmaakt, genereert en verwerkt. Dit archief dient te worden gevormd en beheerd conform de Archiefwet 1995 en daarop gebaseerde regelingen en voorschriften waaronder de Archiefverordening en het Besluit Informatiebeheer van de gemeente Amsterdam.

4.2 {organisatie} draagt zorg dat de informatie behorende tot de in mandaat gegeven taken, als zodanig herkenbaar zijn en in de informatiesystemen van {organisatie} van andere informatie kan worden gescheiden.

4.3 {organisatie} stelt alle informatie beschikbaar <kosteloos of tegen een vergoeding> binnen (termijn) na een verzoek van de Gemeente Amsterdam.
Onder de werking van deze bepaling vallen tevens complexere informatiebronnen zoals real-time data, het gebruik van algoritmen en kopieën en bewerkingen van persoonsgegevens,

4.4 <Als de organisatie persoonsgegevens verwerkt voor de in mandaat gegeven taken:> {organisatie} zal bij overdracht van persoonsgegevens waarborgen dat er geen sprake is van verlies van functionaliteit of (delen van) de persoonsgegevens en dat de continuïteit van de dienstverlening maximaal gewaarborgd blijft.

4.5 De Gemeente Amsterdam kan eisen stellen aan de wijze van beschikbaarstelling van de informatie, waaronder eisen aan het bestandsformaat.

4.6 Ten aanzien van de informatie verplicht {organisatie} zich, voor zo lang het mandaat loopt of tot de informatie is overgebracht naar de Archiefbewaarplaats tot:

- het in goede, geordende en toegankelijke staat brengen, houden en bewaren van de informatie met inachtneming van alle wettelijke voorschriften en gemeentelijke aanwijzingen;
- het toekennen van de bewaar- en vernietigingstermijnen aan de hand van de geldende gemeentelijke selectielijst;
- het vernietigen van informatie en persoonsgegevens na afloop van de geldende bewaartermijnen en na goedkeuring door de gemeentearchivaris van Amsterdam;
- het overbrengen van informatie naar de Archiefbewaarplaats.

4.7 <Als de organisatie persoonsgegevens verwerkt voor de in mandaat gegeven taken:> {organisatie} verwerkt persoonsgegevens die worden ontvangen, gecreëerd en verwerkt ter uitvoering van in mandaat gegeven taken uitsluitend voor de uitvoering van deze gemandateerde taken en uitsluitend overeenkomstig schriftelijke instructies, tenzij een op {organisatie} van toepassing zijnde Unierechtelijke of lidstaatrechtelijke wettelijke bepaling hem tot verwerking verplicht. In dat geval zal {organisatie} de gemeente Amsterdam, voorafgaand aan de verwerking, daarvan zonder onredelijke vertraging in kennis stellen, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.

4.8 <Als de organisatie persoonsgegevens verwerkt voor de in mandaat gegeven taken:> De {organisatie} is aan te merken als verwerker in de zin van de AVG van de Gemeente Amsterdam {organisatie} en vanuit die hoedanigheid verplicht om medewerking te verlenen aan het sluiten van (de meest actuele) verwerkersovereenkomst (bijlage XXX). De verwerkersovereenkomst is een onlosmakelijk deel van deze overeenkomst.

4.9 <Als de organisatie persoonsgegevens verwerkt voor de in mandaat gegeven taken:> Als een betrokkene een beroep doet op zijn rechten zoals genoemd in artikel 12 t/m 22 AVG, faciliteert {organisatie} de Gemeente Amsterdam om daarop binnen de wettelijke termijnen een beslissing te nemen.

4.10 Op verzoek van de Gemeente Amsterdam werkt {organisatie} mee aan of <organisatie> voorziet in de uitvoering van een gegevensbeschermingseffectbeoordeling (DPIA) en een voorafgaande raadpleging als bedoeld in artikel 35 en 36 AVG.

4.11 De {organisatie} verleent medewerking aan het opstellen van een verklaring over bescherming persoonsgegevens door de gemeente Amsterdam en de publicatie ervan.

4.12 De {organisatie} is verplicht volgens de volgende algemeen erkende normen voor informatiebeveiliging te werken: (ISO27001 / NEN7510 en/of Baseline Informatiebeveiliging Overheid (BIO)) om te zorgen voor technische robuustheid van de ICT-infrastructuur, organisatorische en digitale weerbaarheid van de informatievoorziening en het voorkomen van schade.
Op verzoek van de Gemeente Amsterdam werkt {organisatie} mee aan of voorziet {organisatie} in de uitvoering van een risicoanalyse, kwetsbaarheidsanalyse of IT-audit voor informatiebeveiliging om de risico's om de risico's in verband met het verlies van vertrouwelijkheid, integriteit, en beschikbaarheid van informatie voor informatiebeveiliging te identificeren*;*

Of een aan bovenstaande normen gelijkwaardig normenstelsel, waarbij het bewijs voor gelijkwaardigheid aan de norm wordt geleverd door een onafhankelijke derde/auditor als bedoeld in het ISO-systeem.

Artikel 5. Verstrekken van informatie door Amsterdam aan {organisatie}

5.1 De gemeente Amsterdam verstrekt aan {organisatie} de voor de taakoefening benodigde informatie uit de door haar gevormde archieven en systemen. De informatie wordt {digitaal en/of in kopie vorm verstrekt}.

5.2 De leveringstermijn van deze informatie wordt bepaald per soort informatie. Omvangrijke aanvragen worden in overleg behandeld en in dat geval kan de levertermijn langer zijn.

Artikel 6. Databepaling

6.1 In de zin van deze bepaling wordt met data bedoeld alle –zowel analoge als digitale - gegevens, waaronder begrepen zowel ruwe/onbewerkte als bewerkte gegevens en ongeacht in welke vorm en/of op welke informatiedrager deze gegevens zich bevinden.

6.2 Alle rechten met betrekking tot de data die in het kader van deze Informatieovereenkomst door de Gemeente Amsterdam aan {organisatie} worden verstrekt, komen toe aan de Gemeente Amsterdam. {organisatie} heeft, tenzij het open data betreft, niet het recht deze data te gebruiken voor andere doeleinden dan het uitvoeren van deze overeenkomst. <meer informatie in de toelichting>

6.3 Als bij het vervullen van een gemeentelijke taak een gegeven nodig is dat als authentiek gegeven in een basis- en kernregistratie beschikbaar is, gebruikt {organisatie} dit gegeven als bedoeld in artikel 9 van het Reglement basisinformatie 2018.

6.4 Als {organisatie} gerede twijfel heeft over de juistheid of het ontbreken van een authentiek gegeven in een basis- of kernregistratie, meldt {organisatie} dit aan de stelselbeheerder onder opgaaf van redenen als bedoeld in artikel 10 van het Reglement basisinformatie 2018.

Artikel 7.Geautomatiseerde beslissingen en profilering

7.1 De {organisatie} verklaart dat ter uitvoering van de gemandateerde taken geen sprake is van geautomatiseerde beslissingen en/of profilering.

[wettelijk toegestane uitzonderingen en waarborgen benoemen]

[uitzonderingen benoemen]

7.2 De {organisatie} verklaart:

- dat de Algoritmische toepassing is of zal worden ontwikkeld en functioneert op een wijze die in overeenstemming is met wet- en regelgeving, waaronder -

maar daartoe niet beperkt- de Algemene beginselen van behoorlijk bestuur, mensenrechten en wet- en regelgeving en richtlijnen voor betrouwbare (wettig, ethisch en robuuste) AI;
- dat de Algoritmische toepassing volgens een gemotiveerde aanpak is of zal worden ontwikkeld.
- dat de Algoritmische toepassing nauwkeurig en correct functioneert of zal functioneren.
- dat de Algoritmische toepassing geschikt is of geschikt zal zijn voor het beoogde gebruik.

7.3 [Aanvullende afspraken over transparantie over algoritmen e.d.]
Op eerste verzoek verschaft de {organisatie} procedurele transparantie over de algoritmen die zij ten behoeve van de gemandateerde taken inzetten. De gemeente Amsterdam heeft het recht om de in dat kader verstrekte informatie met derden te delen en openbaar te maken. Op verzoek van de gemeente Amsterdam zal de {organisatie} een aan te wijzen register voor Algoritmische toepassingen invullen.

Artikel 8. Delen van informatie tussen {organisatie} en overige (overheids)organisaties

8.1 Indien {organisatie} informatie wil delen met andere (overheids)organisaties en/of subverwerkers wordt toestemming gevraagd aan de gemeente Amsterdam. Indien er toestemming is verleend is {organisatie} verantwoordelijk dat alle wet- en regelgeving – zowel nationaal als lokaal – met betrekking tot overheidsinformatie wordt voldaan. Daarnaast gelden de afspraken van deze overeenkomst ten aanzien van de informatie, ook voor de aanvullende partij.

8.2 {organisatie} mag geen persoonsgegevens verwerken buiten de Europese Economische Ruimte (EER), tenzij college daar uitdrukkelijke, schriftelijke toestemming voor geven. Na toestemming, al dan niet onder voorwaarden, is {organisatie} verantwoordelijk dat de doorgifte voldoet en blijft voldoen aan de AVG.

8.3 Bij een doorgifte als bedoeld in het derde lid maakt {organisatie} (termijn) een analyse van het beschermingsniveau van het land of landen waar de persoonsgegevens worden verwerkt. De Gemeente Amsterdam kan op ieder moment besluiten om de toestemming in te trekken. In een dergelijk geval zal {organisatie} de doorgifte beëindigen (termijn) en de verwerking verplaatsen naar een locatie binnen de EER.

Artikel 9. Openbaarheid

9.1 {organisatie} stelt alle informatie beschikbaar die college uit het door {organisatie} beheerde archief nodig achten voor de behandeling van Wob verzoeken uiterlijk binnen {X} werkdagen nadat daarom is verzocht.

9.2 {organisatie} maakt informatie actief openbaar na toestemming van de Gemeente Amsterdam.

Artikel 10. Uitvoering audits

10.1 De gemeente Amsterdam is gerechtigd te verzoeken om de verwerking van informatie door <organisatie> te doen laten controleren door middel van een audit.

10.2 <organisatie> is verplicht de Gemeente Amsterdam of de -in opdracht van de Gemeente Amsterdam- controlerende instantie toe te laten en alle medewerking te verlenen, waaronder het verlenen van de verlangde informatie, zodat de controle daadwerkelijk uitgevoerd kan worden. De Gemeente Amsterdam zal de audit slechts (laten) uitvoeren na een voorafgaande melding aan <organisatie> en met inachtneming van een redelijke termijn.

10.3 De kosten van de hiervoor genoemde audit wordt gedragen door de Gemeente Amsterdam tenzij de auditor een of meer tekortkomingen van niet ondergeschikte aard van <organisatie> constateert, die ten nadele zijn van de Gemeente Amsterdam.

10.4 De kosten voor eventuele hertesten, herstelwerkzaamheden en het oplossen van de bevindingen worden gedragen door <organisatie>, tenzij Partijen in overleg anders overeenkomen.

10.5 Indien <organisatie> niet beschikt over een geldige certificering als rapporteert <organisatie> jaarlijks over de opzet, bestaan en werking van het stelsel van maatregelen en procedures, gericht op naleving van het bepaalde in artikel 4.13. Deze rapportage betreft ook, indien van toepassing, de werkzaamheden van door hem ingeschakelde derden. <organisatie> zal minimaal eens per jaar kosteloos een TPM c.q. een verklaring van een onafhankelijke externe deskundige aan de Gemeente Amsterdam verstrekken over de naleving van de overeengekomen technische en organisatorische beveiligingsmaatregelen.

Artikel 11. Toezicht

11.1 De gemeente Amsterdam is eindverantwoordelijk voor de informatie en houdt toezicht op:

- Naleving van de Archiefwet door de Gemeentearchivaris van Amsterdam
- Naleving van de Algemene Verordening Persoonsgegevens door de Functionaris Gegevensbescherming van Amsterdam
- Naleving van informatiebeveiligingseisen door de CISO van Amsterdam
- Naleving van de Wet open overheid door de Informatiecommissaris van Amsterdam
- Naleving van het Reglement basisinformatie 2018 door de Chief Data Officer/ Stelselregisseur van Amsterdam

11.2 {organisatie} verstrekt op eerste verzoek alle informatie aan de Gemeente Amsterdam en aan de functionarissen van de Gemeente Amsterdam die zijn belast met het toezicht, die nodig wordt geacht om de het toezicht te kunnen uitvoeren. De leveringstermijn van deze informatie is <AANTAL> werkdagen. Bij omvangrijke aanvragen kan in overleg de levertermijn langer zijn dan <AANTAL> werkdagen.

11.3 {organisatie} rapporteert jaarlijks aan de gemeente Amsterdam over het voldoen aan de afspraken in deze overeenkomst. Hierover worden nadere afspraken uitgewerkt.

11.3 {organisatie} biedt jaarlijks aan de functionarissen die namens college zijn belast met het toezicht een verslag aan waarin verantwoording wordt afgelegd over de wijze waarop invulling wordt gegeven aan de naleving van de in artikel 11.1 genoemde wet- en regelgeving ten aanzien van de informatie behorende tot de uit Amsterdam gemandateerde taken.

11.4 Functionarissen die namens Gemeente Amsterdam zijn belast met het toezicht beoordelen jaarlijks de door {organisatie} opgeleverde rapportage als bedoeld in artikel 11.3 en deze beoordeling maakt onderdeel uit van jaarlijkse bestuurlijke verslaglegging van de gemeente Amsterdam.

Artikel 12 Informatiebeveiligingsincidenten en datalekken

12.1 {organisatie} informeert Gemeente Amsterdam zonder onredelijke vertraging, maar uiterlijk binnen 24 uur na vaststelling van een (vermoedelijke) ernstig informatiebeveiligingsincident, inbreuk in verband met persoonsgegevens of een datalek en beschrijft de aard van het informatiebeveiligingsincident, de (vermoedelijke) inbreuk of datalek en de categorie persoonsgegevens, de categorie betrokkenen en het aantal betrokkenen.

12.2 {organisatie} treft in geval van een ernstig informatiebeveiligingsincident, inbreuk of datalek zonder onredelijke vertraging alle maatregelen om de inbreuk of het datalek te herstellen, de gevolgen daarvan te beperken en nieuwe gevallen te voorkomen.
12.3 {organisatie} heeft een gedetailleerd logboek van de informatiebeveiligingsincidenten inbreuken en datalekken waarin de maatregelen die zijn opgenomen. De Gemeente Amsterdam mag dat inzien, wanneer deze daarom vraagt.
12.4 De Gemeente Amsterdam beslist of de inbreuk moet worden gemeld bij de toezichthoudende autoriteit en/of Betrokkene. {organisatie} ondersteunt de Gemeente Amsterdam waar nodig bij de melding aan de toezichthoudende autoriteit en/of Betrokkene.

Artikel 13 Financiële afspraken

13.1 De kosten van het beheer van de informatie, inclusief de kosten van bewaring, vernietiging en het overbrengen naar de Archiefbewaarplaats, maken onderdeel uit van de jaarlijkse gemeentelijke bijdrage aan {organisatie} en worden niet afzonderlijk gefactureerd;
13.2 De kosten voor hardware en software die nodig zijn voor de uitvoering van het archiefproces komen ten laste van {organisatie};
13.3 De kosten van het in digitale kopie-vorm ter beschikking stellen van informatie uit dossiers die zich bevinden bij de Gemeente Amsterdam en waarover {organisatie} moet beschikken als gevolg van de taken die college aan {organisatie} hebben opgedragen, komen voor rekening van college.
13.4 De kosten voor het voldoen aan regelgeving op het gebied van informatiebeveiliging en gegevensbescherming worden gezien als reguliere bedrijfsvoeringskosten die voor rekening komen van de organisatie.
13.5 Over de kosten voor toezichtsactiviteiten door functionarissen van de Gemeente Amsterdam worden apart afspraken gemaakt.
13.6 Er worden apart afspraken gemaakt over de kosten bij de toepassing van artikel 4.3 van deze overeenkomst.

Artikel 14. Aansprakelijkheid [UITSLUITEND INDIEN NIET GEREGELD IN HOOFDOVEREENKOMST]

14.1 De partij die toerekenbaar tekortschiet in de nakoming van zijn verplichtingen, is tegenover de andere partij aansprakelijk voor de door deze geleden en/of te lijden schade.
14.2 De aansprakelijkheid voor schade, uit welke hoofde dan ook, is – tenzij anders overeengekomen – beperkt tot vier maal de hoogte van de Vergoeding per gebeurtenis, met dien verstande dat de aansprakelijkheid nooit meer zal bedragen dan € 5.000.000,-- per gebeurtenis. Samenhangende gebeurtenissen worden daarbij aangemerkt als één gebeurtenis.

Artikel 15. Geheimhoudingsplicht en boetebeding

15.1 {organisatie} is verplicht om de informatie die {organisatie} verwerkt in de uitoefening van gemandateerde taken geheim te houden, tenzij het om open data gaat of om informatie die op grond van de Wet open overheid wordt openbaargemaakt.
15.2 Indien {organisatie} zijn verplichtingen uit hoofde van artikel 15.1 .niet nakomt, zal deze onmiddellijk, zonder dat enige verdere actie of formaliteit is vereist, jegens de Gemeente Amsterdam een onmiddellijk opeisbare boete verbeuren ten bedrage van € 25.000,- (vijfentwintigduizend euro) voor iedere dergelijke inbreuk, zonder dat de Gemeente Amsterdam enig verlies of schade behoeft te bewijzen en onverminderd het recht van de Gemeente Amsterdam om aanvullende schadevergoeding te vorderen als daarvoor gronden zijn, behoudens rechterlijke matiging.

15.3 De gemeente Amsterdam zal zorgvuldig omgaan met vertrouwelijk informatie die aan de gemeente ter beschikking worden gesteld door de verbonden partij. Bijvoorbeeld bij de melding van informatiebeveiligingsincidenten of datalekken.

Aldus overeengekomen en in tweevoud ondertekend,
datum: <.....>

Gemeente Amsterdam	<Naam bedrijf /organisatie>
namens deze: <naam, functie>	namens deze: <naam, functie>
plaats: <.....>	plaats: <.....>
datum: <.....>	datum: <.....>

Toelichting op de databepaling in artikel 4

Afwegen en keuze maken of alleen de gemeente de data exclusief mag gebruiken of dat <organisatie> de data ook beperkt dan wel onbeperkt mag gebruiken.

Uitgangspunt is dat <organisatie> alleen de verzamelde data mag gebruiken voor het uitvoeren van de overeenkomst (optie 1). Het is voorstelbaar is dat zich situaties voordoen waarin het gezien de aard van de gemaakte afspraken en de vertrouwelijkheid van de verzamelde data, redelijk en toelaatbaar is dat <organisatie> de verzamelde data ook beperkt mag gebruiken voor eigen productontwikkeling (optie 2) of ook andere doeleinden (optie 3).
Voor de keuze voor optie 1,2 en 3 is mede de classificatie van data van belang.
Bij geheime en vertrouwelijke data >> keuze tussen optie 1 en 2
Bij open data >> optie 3

Optie 1 (geheime en vertrouwelijke data)
Alle rechten met betrekking tot de data die in het kader van de uitvoering van deze overeenkomst door <organisatie> worden gecreëerd of verzameld komen toe aan de Gemeente Amsterdam. Het betreft zowel data, die behoren tot de kern van de gemandateerde taken als data, die een nevenproduct zijn bij de uitvoering van de gemandateerde taken. <organisatie> heeft niet het recht deze data te gebruiken voor andere doeleinden dan het uitvoeren van deze overeenkomst. <organisatie> zal deze data op eerste verzoek van de Gemeente Amsterdam vernietigen en/of tot afgifte van de data aan de Gemeente Amsterdam overgaan.

Optie 2 (geheime en vertrouwelijke data)
Alle rechten met betrekking tot de data die in het kader van de uitvoering van deze vereenkomst door worden <organisatie> gecreëerd of verzameld komen toe aan de Gemeente Amsterdam. Het betreft zowel data, die behoren tot de kern van de gemandateerde taken als data, die een nevenproduct zijn bij de uitvoering van de gemandateerde taken. <organisatie> heeft niet het recht deze data te gebruiken voor andere doeleinden dan het uitvoeren van deze vereenkomst en voor zover noodzakelijk voor de eigen productontwikkeling, doch mits geanonimiseerd (uitsluitend in een vorm waarin de data direct noch indirect te herleiden is tot individuele personen, groepen van individuele personen of de Gemeente Amsterdam). <organisatie> zal deze data op eerste verzoek van de Gemeente Amsterdam vernietigen en/of tot afgifte van de data aan de Gemeente Amsterdam overgaan.

Optie 3 (in geval van open data)
Partijen komen overeen dat rechten op de data worden uitgesloten. Zo niet, dan begrenst de Gemeente Amsterdam de uitoefening van rechten op de data, zodanig dat hergebruik vóór de uitoefening van rechten gaat (art. 8 en 11 Hergebruikrichtlijn (PbEU 2019, L 172/56); art. 15b Auteurswet; art. 8 lid 2 Databankenwet; bijv. via de Creative Commons-zeroverklaring (CC0) of Creative Commons-naamsvermeldinglicentie).Het betreft zowel data, die behoren tot de kern van de gemandateerde taken als data, die een nevenproduct zijn bij de uitvoering van de gemandateerde taken. Dat betekent dat zowel <organisatie> en de Gemeente Amsterdam de data vrij kunnen gebruiken, ook voor doeleinden anders dan de uitvoering van deze overeenkomst. Indien en voor zover de Gemeente Amsterdam niet zelf de beschikking heeft over een kopie van de data, zal <organisatie> de data op eerste verzoek van de Gemeente Amsterdam aan de Gemeente Amsterdam verstrekken.