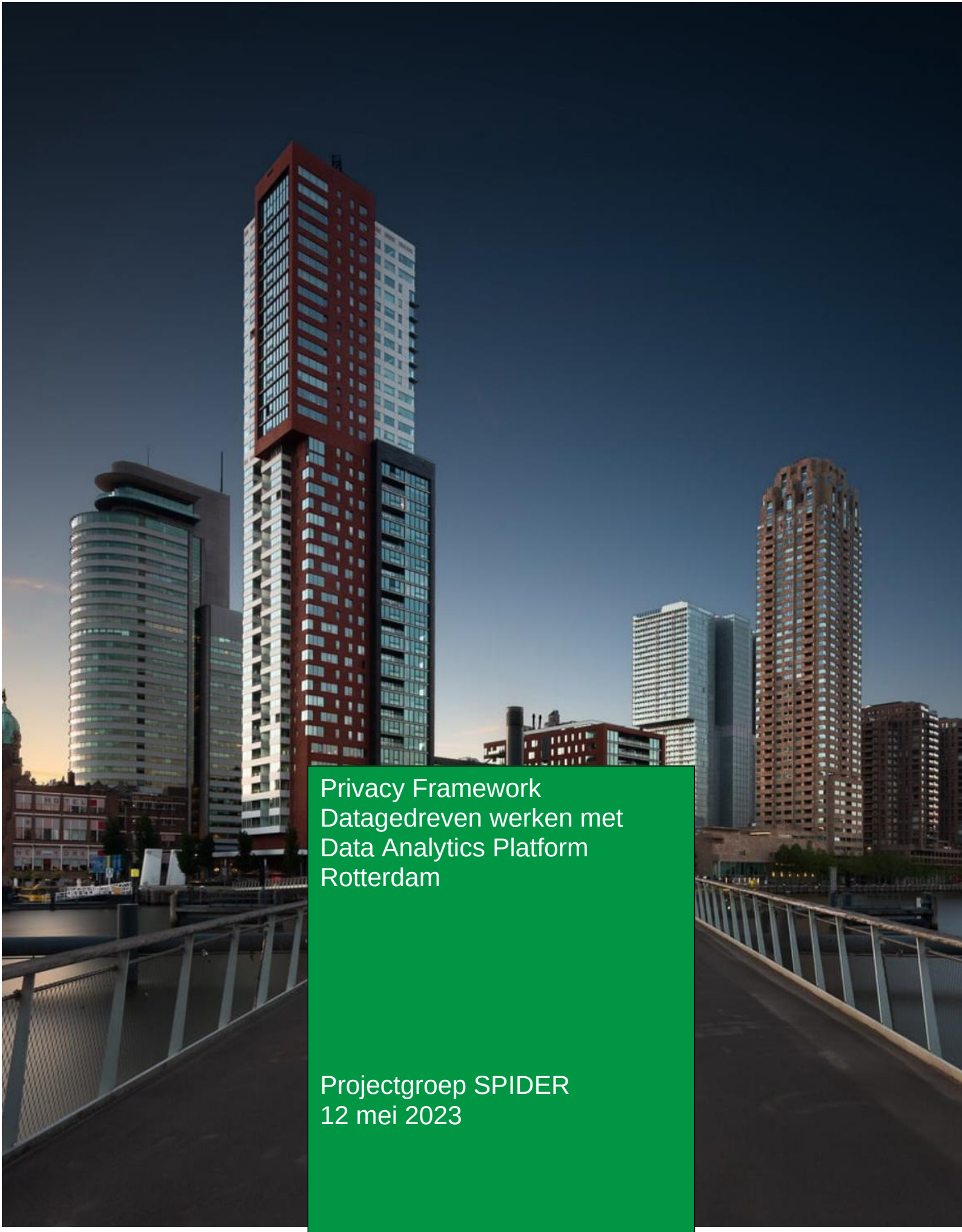


Privacy Framework Datagedreven werken met Data Analytics Platform Rotterdam

Projectgroep SPIDER
12 mei 2023

Gemeente Rotterdam

Voorblad

Gemeente Rotterdam, afdeling IIFO

Datum:	12 mei 2023
Versie:	1.0
Aan:	Concerndirectie
Auteur(s):	Projectgroep Spider (Security, Privacy, Informatiebeheer, Datamanagement, Ethiek, Rotterdam
Betreft:	Framework Privacy (beleidskader)
eigenaar:	Niels van Heezik, Afdelingshoofd

Inhoudsopgave

Inleiding Privacy Framework DGW

Rotterdam wil een netwerkstad zijn die optimaal gebruik maakt van data. Maar wel op een manier die past bij hoe Rotterdam zorgvuldig met haar burgers omgaat, op het gebied van privacy, informatiebeveiliging en ethiek *(bron: Digitaliseringsagenda)*

Scope
Daarom hierbij het *Privacy Framework DGW*, een beleidskader met spelregels voor datagedreven werken met persoonsgegevens op DAP'R, het Data en Analyse Platform Rotterdam. Het Framework is ook van toepassing op het huidige concern Datawarehouse, dat naar DAPR zal worden gemigreerd.[1]

Aanleiding
De gemeente beschikt over grote hoeveelheden gegevens. Die gegevens bevatten een schat aan informatie die waardevol zijn voor de verbetering van beleid en dienstverlening, zeker wanneer je deze samenbrengt, combineert en analyseert. Het ontsluiten en verzamelen op één plek, DAPR, verhoogt de efficiëntie en snelheid waarmee dataproducten tot stand komen. Maar daar liggen ook de risico's.

Een deel van die data zijn (gevoelige) persoonsgegevens. Van bijstandsuitkeringen tot cameratoezicht in de openbare ruimte, van wijkteams tot gemeentelijke heffingen, er zijn meer dan 500 processen waarbij de gemeente persoonsgegevens van burgers verwerkt. Veel datasets zullen dus meerdere soorten persoonsgegevens bevatten. Zeker wanneer gegevens met elkaar gecombineerd of verrijkt worden kan de informatie nog gevoeliger worden.

Risico's
Gevoelige data onderbrengen op één platform geeft risico's op datalekken en onrechtmatig gebruik. Bij het verwerken van data kunnen (onbedoelde) gevolgen optreden, zoals bias in algoritmes (bijv discriminatie). Deze schaden het vertrouwen van de burger in de overheid. Die gegevens moeten dan ook goed beschermd worden. En daarin voorziet de privacywetgeving AVG, de Algemene Verordening gegevensbescherming en andere wet- en regelgeving zoals de BIO, Baseline Informatiebeveiliging Overheid.

Privacy Framework
De AVG vereist dat organisaties veilig en verantwoord met persoonsgegevens van burgers en medewerkers omgaan. Vanuit verschillende invalshoeken wordt in dit Framework beschreven wat er voor nodig is om tot een informatieproduct te komen dat aan de AVG en andere wet- en regelgeving[2] voldoet. Het document beschrijft:

1. <u>Grondslag en doelbinding</u>
   Dit beschrijft welke grondslagen de AVG kent op grond waarvan per informatieproduct bepaald wordt welke persoonsgegevens mogen worden verwerkt, en onder welke voorwaarden.
2. <u>Governance</u>
   Hierin worden de rollen en verantwoordelijkheden in het proces beschreven. Daarin staat het DUB-proces[3] centraal.

[1] De scope van dit Framework is DAP'R/cDWH, maar uiteraard is de AVG ook van toepassing op het datagedreven werken vanuit andere applicaties.
[2] Ook andere wet- en regelgeving is van toepassing, zoals de BIO, de Archiefwet en de sectorale wetgeving. Denk aan de Wet op de BRP, de Jeugdwet maar ook de WOO.
[3] Data User Board, een adviserend orgaan waarin alle betrokkenen en disciplines zijn vertegenwoordigd met als doel een integraal privacy advies en een gebruiksovereenkomst (GLO) op te stellen.

3. Informatiebeheer
   De AVG vereist dat zo min mogelijk persoonsgegevens worden opgeslagen voor een zo kort mogelijke termijn. In dit hoofdstuk wordt dit principe in relatie tot de Archiefwet en bewaartermijnen beschreven.
4. Security
   Hierin wordt beschreven welke technische en organisatorische maatregelen nodig zijn om de gegevens te kunnen beschermen. Denk aan toegangsbeheer, logging, encryptie, ed.

Wat verstaan we onder informatieproducten?

1. Statistische analyses en onderzoek, dashboards of rapportages ten behoeve van beleid, dienstverlening of bedrijfsvoering. Deze bevatten geen persoonsgegevens in het eindproduct. Om het product te kunnen maken worden wel vaak persoonsgegevens gebruikt.
2. Informatieproducten waarin ook in het eindproduct persoonsgegevens voorkomen. Denk aan werklijsten of overzichten, met daarin gegevens van personen nodig voor werkvoorbereiding, workload, etc.
3. Algoritmes. Wanneer daar persoonsgegevens in worden gebruikt vallen deze onder de AVG en geldt dit kader ook voor algoritmes.

Doelgroep
Het Privacy Framework is bedoeld voor alle medewerkers die betrokken zijn bij datagedreven werken, voor afnemers van informatieproducten en bronhouders.

Tevens is dit kader de verantwoording waarmee het college naar de toezichthouders (FG, Autoriteit Persoonsgegevens, Rekenkamer) en desgevraagd de gemeenteraad kan aantonen dat de gemeente rechtmatig werkt.

Implementatie
Datagedreven werken is niet nieuw, de gemeente maakt al jaren gebruik van data voor beleidsprocessen en sturingsinformatie. De laatste jaren groeit dit exponentieel.
Dit Framework beschrijft op hoofdlijnen de spelregels, rollen en verantwoordelijkheden. Hiermee hebben we een stevig fundament gelegd. Daarmee is het document niet in beton gegoten, op basis van evaluaties en audits zal het doorontwikkeld worden, samen met de betrokken specialisten en adviseurs.

Privacyrisico's en -beginselen in de context van datagedreven werken

1.1 Algemeen

Het algemene wettelijk kader voor verwerking van persoonsgegevens binnen gemeente Rotterdam met behulp van het DAP'R wordt gevormd door de Algemene Verordening Gegevensbescherming ('AVG') en de Uitvoeringswet AVG ('UAVG'). Daarnaast zijn specifieke wetten en normenkaders van toepassing zoals de Gemeentewet, Archiefwet, BRP, Jeugdwet, WMO 2015, Baseline Informatiebeveiliging Overheid (BIO) en de Artificial Intelligence ACT, waarover nog dit jaar een akkoord wordt verwacht, en andere nog te ontwikkelen normenkaders rond Ethiek en Algoritmen. Al deze regels tezamen vormen op grond van de artikelen 5 en 6 AVG het algemene juridische kader van onderhavig Privacyframework.

Bijzondere vermelding verdient hier de Wet politiegegevens (Wpg). Deze wet regelt de verwerking van persoonsgegevens ter uitvoering van de politietaak, de zogenaamde politiegegevens.[4] De Wpg geldt niet naast, maar *in plaats van* de AVG. Omwille van de eenvoud wordt binnen dit framework gesproken van de AVG, maar daaronder wordt ook begrepen de Wpg, en de Wet Justitiele en strafvorderlijke gegevens (Wjsg) . Deze wetten vloeien voort uit de Richtlijn gegevensbescherming politie en justitie die in vergelijkbare bepalingen en waarborgen voorziet als de AVG. Het belangrijkste gevolg van het onderscheid tussen de AVG en de Wpg is dat de gegevens die onder de respectieve regelingen vallen, in beginsel strikt van elkaar gescheiden dienen te blijven, ook in het kader van datagedreven werken[5].

Wanneer is de AVG van toepassing?

De AVG is van toepassing wanneer er *persoonsgegevens* worden *verwerkt*.[6] Onder verwerking wordt o.a. verstaan het verzamelen, vastleggen, opslaan, wijzigen, opvragen, raadplegen, gebruiken, verstrekken, wissen en vernietigen van persoonsgegevens.
Een persoonsgegeven is ieder gegeven dat informatie bevat over een *natuurlijke persoon* (ofwel: betrokkene).

Soorten persoonsgegevens

De AVG maakt onderscheid tussen gewone en bijzondere categorieën van persoonsgegevens.

Gewone persoonsgegevens

Of een gegeven al of niet een persoonsgegeven is wordt ruim uitgelegd. Het gaat daarbij niet alleen om gegevens zoals naam, geboortedatum of adres, maar ook om subjectieve gegevens zoals meningen. Ook de vorm waarin of waarop de gegevens zich bevinden (zoals papier, vingerafdrukken, geluidsopnamen of camerabeelden) speelt geen rol[7].
Gegevens kunnen ook indirect herleidbaar zijn tot een persoon, zoals het kentekennummer en het IP-adres. Ook informatie die - in combinatie met andere gegevens - tot een bepaalde

[4] Artikel 1 sub a Wpg.
[5] Dit Framework geldt ook voor Ppg-gegevens. Voor Politiegegevens geldt een apart regime, niet de AVG. Dit neemt niet weg dat dit framework ook op Wpg-geg3evens van toepassing is. Denk aan Politiegegevens die verwerkt worden in het kader van Smart City toepassingen zoals mobiel cameratoezicht, Driehoek Burgemeester, OM en Politie.
[6] Daarnaast is van belang voor de toepasselijkheid van de AVG of de gegevens geheel of gedeeltelijk geautomatiseerd worden verwerkt en of ze zijn opgenomen in een bestand, dan wel bestemd om te worden opgenomen in een bestand. Binnen het kader van DGW is dit altijd het geval. Om deze reden zijn deze criteria hier niet opgenomen in de tekst.
[7] Zie ook advies 4/2007 van de artikel 29-werkgroep over "Persoonsgegevens"

persoon herleidbaar zijn worden beschouwd als persoonsgegevens. Dit is ook het geval bij gepseudonimiseerde gegevens die door gebruik van andere gegevens herleidbaar zijn tot een natuurlijke persoon. Anonieme gegevens vallen hier niet onder. Maar om persoonsgegevens werkelijk als anoniem te mogen beschouwen, moet worden gekeken naar alle middelen waarvan redelijkerwijs valt te verwachten dat zij kunnen worden gebruikt om de identiteit van betrokkene te achterhalen. Bij het beoordelen wat onder 'redelijkerwijs te verwachten' wordt verstaan moet rekening worden gehouden met alle objectieve factoren, zoals de kosten van en de tijd benodigd voor identificatie, met inachtneming van de beschikbare technologie of het tijdstip van verwerking en de technologische ontwikkelingen[8]. Door de snelle technologische ontwikkelingen zal het steeds moeilijker worden om te spreken van werkelijk anonieme gegevens.

Bijzondere persoonsgegevens
Dit zijn gegevens waaruit ras of etnische afkomst blijkt, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, het lidmaatschap van een vakbond, genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, gegevens over gezondheid en gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.
De verwerking, en dus ook de verwerking van deze persoonsgegevens met behulp van het DAP'R, is verboden, tenzij er een specifieke uitzondering van toepassing is (meer hierover in de paragrafen 1.2.1.5 en 1.2.1.6).

Strafrechtelijke gegevens
Naast bijzondere persoonsgegevens zijn ook *strafrechtelijke persoonsgegevens* dermate gevoelig dat daar een speciale regeling voor is. Deze persoonsgegevens mogen alleen worden verwerkt als dat gebeurt onder toezicht van de overheid, of als het specifiek bij wet is geregeld.

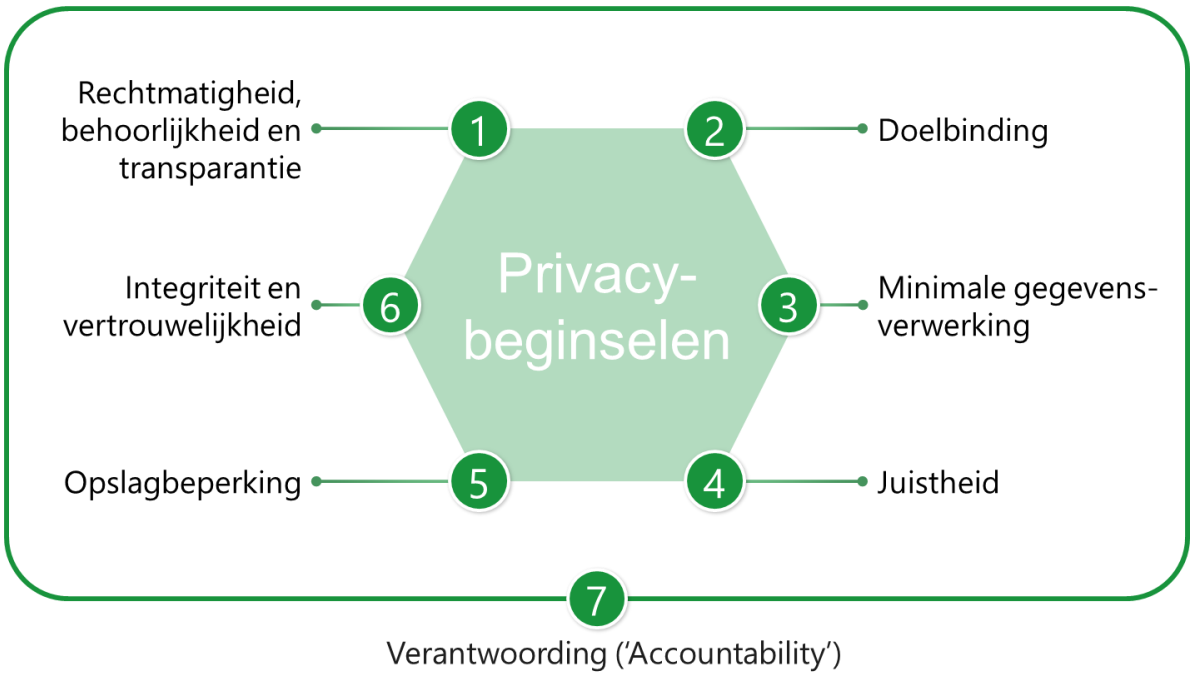
Gevoelige gegevens
Er zijn ook andere gegevens die niet 'bijzonder' zijn, maar wel gevoelig. Denk hierbij bijvoorbeeld aan financiële data of locatiegegevens. De maatregelen die genomen moeten worden om persoonsgegevens te beschermen zijn mede afhankelijk van de gevoeligheid van de gegevens en het risico dat zij kunnen vormen voor de betrokkene bij verkeerd gebruik of misbruik.

BSN
Het burgerservicenummer (BSN) is een bij wet vastgesteld nationaal identificatienummer. Dit mag alleen worden gebruikt voor bij wet voorgeschreven doelen. Die doelen zijn te vinden in de Wet algemene bepalingen burgerservicenummer, de Wet gebruik burgerservicenummer in de zorg en de Wet persoonsgebonden nummers in het onderwijs (meer hierover in paragraaf 1.2.1.4).

[8] Zie Overweging 26 bij AVG

1.2 Privacybeginselen

De AVG gaat ervan uit dat de gemeente privacyrisico's effectief beperkt en beheerst als zij door het treffen van maatregelen voldoet aan de zeven privacybeginselen die de AVG benoemt:



Deze zeven beginselen spelen een leidende rol bij het verantwoord omgaan en (datagedreven) werken met persoonsgegevens, en daarmee bij de inrichting van dit framework. Vanwege het eigen karakter van datagedreven werken, vergeleken met de verwerking van persoonsgegevens in de primaire processen, vraagt ieder beginsel om een doorvertaling naar de context van dit framework.

1.2.1 Rechtmatigheid, behoorlijkheid en transparantie

De verwerking van persoonsgegevens moet voldoen aan de beginselen van rechtmatigheid, behoorlijkheid en transparantie. Dit betekent dat gegevens voor gerechtvaardigde doelen rechtmatig en transparant verwerkt moeten worden. Maar ook dat gegevens op een rechtmatige manier zijn verkregen, dus bijvoorbeeld niet zonder dat betrokkene hiervan weet[9].

Bij elke verwerking van persoonsgegevens geldt dat uitsluitend noodzakelijke persoonsgegevens mogen verwerkt. Noodzakelijk wil zeggen dat het doel niet op andere, minder ingrijpende wijze kan worden bereikt (subsidiariteit) en dat de inbreuk in verhouding staat tot het doel dat men wil bereiken (proportionaliteit). Dit heeft tot gevolg dat er een

[9] Zo wil het feit dat informatie op social media te vinden is en daardoor voor iedereen beschikbaar is, bijvoorbeeld nog niet zeggen dat een gemeente deze gegevens van haar inwoners ook mag gebruiken. Dit mag alleen in uitzonderingsgevallen, bijvoorbeeld om signalen te controleren over onrechtmatig aanbod van woonruimte voor toeristische verhuur.

rechtstreeks verband moet zijn tussen de gegevens die worden verwerkt en het doel dat men wil bereiken. Dataminimalisatie maakt deel uit van deze toets.

1.2.2 Rechtmatigheid

Persoonsgegevens mogen slechts voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen worden verwerkt. Er mogen dus geen persoonsgegevens worden verwerkt zonder dat hiervoor een doel is bepaald. Gegevens verzamelen "omdat deze in de toekomst nog wel eens van pas kunnen komen" is dus niet toegestaan. Wel mogen persoonsgegevens voor meerdere doelen tegelijkertijd verwerkt worden. De verschillende doeleinden moeten dan wel duidelijk zijn omschreven. Duidelijk omschrijven wil zeggen dat, voordat met het verzamelen van persoonsgegevens wordt begonnen, duidelijk moet zijn vastgelegd waarvoor deze gegevens nodig zijn. De gegevens mogen (in principe) dan ook alleen voor dat specifieke doel worden gebruikt. Tenslotte moet het doel gerechtvaardigd zijn. Dit betekent dat de verwerking kan worden gebaseerd op een van de in de AVG (artikel 6) genoemde grondslagen.

Voor elke verwerking van gegevens is een rechtmatige grondslag (rechtvaardigingsgrond) nodig. De AVG[10] kent de volgende zes grondslagen, (waarvan er in de meeste gevallen 2 van toepassing zijn voor de gemeente):

1. de betrokkene heeft *toestemming* gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;
2. de verwerking is noodzakelijk voor de *uitvoering van een overeenkomst* waarbij de betrokkene partij is of om op verzoek van de betrokkene voor de sluiting van een overeenkomst maatregelen te nemen;
3. de verwerking is noodzakelijk om te *voldoen aan een wettelijke verplichting* die op de verwerkingsverantwoordelijke rust;
4. de verwerking is noodzakelijk om de *vitale belangen* van de betrokkene of van een andere natuurlijke persoon te beschermen;
5. de verwerking is noodzakelijk voor de vervulling van een *taak van algemeen belang* of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen;
6. de verwerking is noodzakelijk voor de behartiging van de *gerechtvaardigde belangen* van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene tot bescherming van persoonsgegevens, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.

Van de zes grondslagen die de AVG noemt, zijn er 2 het meest van toepassing voor de gemeente.
Grondslag 3: dit gaat over het moeten voldoen aan een wettelijke plicht waarbij het niet mogelijk is om hieraan te voldoen zonder persoonsgegevens te verwerken[11].
Grondslag 5: dit gaat over het verwerken van gegevens 'voor de vervulling van een taak van algemeen belang' of 'uitoefening van het openbaar gezag' waar de gemeente toe bevoegd is.

[10] Artikel 6, eerste lid, AVG
[11] Bijvoorbeeld: de verplichting (artikel 1.4 Wet BRP) voor het college van B&W om een basisregistratie personen bij te houden.

De eis op grond van artikel 6, derde lid, AVG„daarbij is dat die taak waarvoor de gemeente gegevens verwerkt, een basis[12] moet hebben in Unierecht of lidstatelijk recht[13].

De overige grondslagen mogen in principe niet worden gebruikt door de gemeente:

Grondslag 1: *toestemming van betrokkene'* kan in principe niet worden gebruikt vanwege de afhankelijkheidsrelatie tussen burger en overheid waardoor de burger zich in het algemeen niet vrij zal voelen om zijn toestemming te weigeren. De toestemming kan dan niet rechtsgeldig worden verleend.
Grondslag 2 *'uitvoering van een overeenkomst'* komt sporadisch voor in de verhouding overheid – burger en wordt dus zelden als grondslag gebruikt.
Grondslag 4 '*bescherming vitale belangen van betrokkene*' doet zich in principe niet voor in de verhouding overheid – burger en is dus niet bruikbaar als grondslag. Deze grondslag is voor hulpverleners van belang om acuut dringende noodzakelijke medische hulp aan betrokkene te verlenen.
Grondslag 6 '*gerechtvaardigd belang*' kan niet door de gemeente worden gebruikt bij de uitvoering van haar publieke taken, omdat de AVG deze expliciet voor de gemeente heeft uitgesloten[14]).

Een uitzondering op het niet mogen gebruiken van *toestemming* als grondslag, doet zich voor bij het verzamelen van persoonsgegevens rechtstreeks bij betrokkenen met behulp van een enquête, mits:

1. de toestemming vrij wordt gegeven. Dit houdt in dat betrokkene de keuze moet hebben om te weigeren, zonder dat hier negatieve consequenties aan verbonden zijn, zoals het uitnodigen van de burger voor deelname aan een enquête[15] voor het doen van onderzoek. Het verzoek om deelname kan zonder consequenties worden geweigerd. Toestemming is hier wel bruikbaar;
2. betrokkene vooraf specifiek wordt geïnformeerd over de redenen, de wijze waarop persoonsgegevens zullen worden verwerkt en hoe lang ze worden bewaard;
3. de toestemming ondubbelzinnig wordt gegeven. Er mag geen twijfel bestaan over het verlenen van de toestemming. Een actieve handeling (vinkje in vakje van akkoord aankruisen) is nodig.

1.2.3 Doelbinding en grondslagen en het DAP'R

Bovengenoemde uitgangspunten over doelbinding en grondslagen gelden vanzelfsprekend ook voor de verwerkingen in het kader van het DAP'R, waarin voor elk te ontwikkelen informatieproduct[16] een duidelijk omschreven doel met bijbehorende grondslag voor het gebruiken van persoonsgegevens moet worden vastgesteld. Het proces van aanvraag tot oplevering van een informatieproduct wordt daarbij als één onlosmakelijk proces van

[12] Overweging 41 AVG: hieruit blijkt dat het op grond van artikel 6, derde lid, AVG tot stand gekomen 'lid statelijk recht' niet per se een door een parlement vastgestelde of goedgekeurde wet hoeft te zijn. De rechtsgrond of wetgevingsmaatregel moet wel duidelijk en nauwkeurig zijn. In samenhang hiermee moet de toepassing daarvan voorspelbaar zijn voor degenen op wie deze van toepassing is.
[13] Bijvoorbeeld: het verwerken van persoonsgegevens in het kader van archivering in het algemeen belang, wetenschappelijk of historisch onderzoek, of statistische doeleinden
[14] Artikel 6, eerste lid, onder f, AVG en Overweging 47 AVG.
[15] Zoals Wijkonderzoek en Omnibus enquete.
[16] Onder informatieproducten wordt in het kader van dit framework verstaan: alle vormen van business information, analyse en statistische beleidsinformatie.

verwerking beschouwd. Dit geldt ook als er in dat proces gebruik gemaakt wordt van algoritmen.

Er kunnen globaal drie categorieën informatieproducten worden onderscheiden die met behulp van het DAP'R worden ontwikkeld[17]. Dit zijn informatieproducten waarvoor persoonsgegevens nodig zijn en die worden verwerkt voor:

1. hetzelfde doel en dezelfde grondslag als het primaire proces waarvoor de gegevens oorspronkelijk zijn verzameld
   Deze categorie informatieproducten ondersteunt het primaire proces, denk aan het creëren van werklijsten, overzichten ziekteverzuim medewerkers. Deze informatieproducten dienen hetzelfde doel als het doel waarvoor de gemeente de benodigde persoonsgegevens oorspronkelijk heeft verzameld. De verwerking behoort tot het primaire proces/taak van de gemeente. Deze informatieproducten kunnen persoonsgegevens bevatten. De grondslag blijft dezelfde als voor het primaire doel. De data komen uit hetzelfde bronsysteem.

2. een ander, maar verenigbaar, doel als die op grond waarvan de gegevens oorspronkelijk zijn verzameld. Er is dan geen nieuwe grondslag nodig[18].
   Bij deze categorie informatieproducten gaat het uitsluitend om het doen van wetenschappelijk en statistisch onderzoek ten behoeve van beleid. Daarbij worden persoonsgegevens verwerkt voor een ander doel dan het oorspronkelijke, maar dit is geen probleem want de AVG beschouwt dit andere doel als verenigbaar met het oorspronkelijke doel.[19]. Dit wordt ook wel de "verdere verwerking van persoonsgegevens" genoemd voor een ander, maar verenigbaar doel.
   Het spreekt voor zich dat de persoonsgegevens die hiervoor gebruikt worden rechtmatig dienen te zijn verzameld in het primaire proces om verder te mogen worden verwerkt. De eindproducten bevatten geen persoonsgegevens en worden niet gebruikt voor besluitvorming gericht op een individu. De eindproducten leiden tot beleidsinformatie, statistische en onderzoeksinformatie en worden niet gebruikt voor besluitvorming met rechtsgevolg voor een natuurlijke persoon. De beleidsinformatie kan wel leiden tot de totstandkoming van beleid.

3. Algoritmetoepassingen
   Dit zijn informatieproducten die - net als die genoemd onder categorie 1 en 2 - altijd het DUB-proces moeten doorlopen voordat zij worden ontwikkeld. Soms is hierbij sprake van de verdere verwerking van persoonsgegevens en soms van de verwerking van persoonsgegevens voor de uitoefening van een primaire taak. Ook kunnen er persoonsgegevens worden verwerkt zowel in de ontwikkelfase als in het eindproduct. Er kan bij de toepassing van algoritmen dus sprake zijn van zowel categorie 1 of 2. Bovendien kan het resultaat van het eindproduct leiden tot maatregelen of beslissingen die een bepaalde natuurlijke persoon betreffen. Om deze reden worden algoritmetoepassingen genoemd als afzonderlijke categorie.

[17] In de praktijk zal blijken of alle soorten informatieproducten kunnen worden ondergebracht in een van deze drie categorieën.
[18] Artikel 6, vierde lid, jo. Artikel; 5, eerste lid aanhef en onderdeel b, en artikel 89 van de AVG,
[19] Zie overweging 50 AVG

Deze informatieproducten worden ontwikkeld met behulp van 'Advanced analytics/business information' (BI) waarbij gebruik gemaakt kan worden van machine learning, een technologie waarbij door middel van berekeningen patronen uit sets met verschillende data kunnen worden ontdekt. Daarvoor worden vaak ook persoonsgegevens gebruikt, zowel in de ontwikkelfase als in het eindproduct.

Als voorbeelden hiervoor kunnen worden genoemd het gebruik van algoritmetoepassingen door de clusters Stadsbeheer en Stadsontwikkeling voor:

- Handhaving parkeerbeleid met behulp van scanauto's
- Toezicht en handhaving Vastgoedmisbruik (huisjesmelkers)
- Het gericht controleren van goed verhuurderschap op het naleven van de Woningwet,

en andere vormen van toezicht op de naleving van gemeentelijke regelgeving.

Het gebruik van algoritmes kent specifieke ethische risico's, zoals op bias in de uitkomsten (discriminatie). Naast de bepaling van doel en grondslag, zoals bij elk informatieproduct, wordt er ook een Algorithm Risk Assessment uitgevoerd om het risico van de algoritmetoepassing te duiden en eventuele aanvullende stappen voorschrijft. Juist vanwege die risicos bij algoritmes vooral de vraag over het middel zelf centraal staan: staan de risico's voor betrokkenen door het gebruik van het algoritme in verhouding tot het doel? Kan het doel ook op een andere manier bereikt worden? Etc. Ook wordt beoordeeld of het DUB-advies moet worden aangevuld met een IAMA (verplicht bij hoog-risico algoritmetoepassingen) of DEDA (optioneel bij laag-risico algoritmetoepassingen en andere informatieproducten). Om die reden wordt ook ethiek betrokken bij het DUB-proces net als een algoritme-expert.

Voor elk informatieproduct geldt dat – voorafgaand aan de ontwikkeling ervan – moet worden beoordeeld of dit is toegestaan op grond van de AVG. Deze afweging vindt plaats binnen het DUB-proces[20], eventueel aangevuld met een advies van het Algorithm Advisory Board. Meer over dit proces in hoofdstuk 4: Datamanagement.

1.2.4 Verdere verwerking van persoonsgegevens uit verschillende clusters/databronnen

Voor het ontwikkelen van informatieproducten is het vaak nodig om persoonsgegevens uit verschillende clusters/databronnen te combineren om tot een bruikbare analyse te komen. De combinatie van interne data uit een of meer clusters/databronnen is – onder voorwaarden – toegestaan. Deze voorwaarden zijn:

- de geselecteerde datasets zijn noodzakelijk zijn voor het onderzoeksdoel. Dit betekent dus niet dat datasets uit verschillende clusters/bronnen gekoppeld kunnen worden 'om te zien wat eruit komt'. Er moet altijd vooraf expliciet worden vastgesteld welk doel de verwerking (het informatieproduct) heeft. Alleen dan kan worden beoordeeld welke persoonsgegevens noodzakelijk zijn voor het specifieke doel van de verwerking en wat de grondslag is voor de koppeling; en
- voordat met de ontwikkeling wordt gestart – moet het DUB-proces zijn afgerond met een positief advies; en
- verdere passende organisatorische en technische maatregelen moeten zijn genomen.

20

Als passende maatregelen kunnen worden genoemd:

- het gescheiden opslaan van datasets afkomstig uit verschillende clusters/bronnen, en categorieën persoonsgegevens, om te voorkomen dat ongewenste koppelingen plaatsvinden (schotten ertussen);
- het autoriseren van een zeer beperkt aantal medewerkers met geheimhoudingsplicht die toegang hebben tot de betreffende datasets op basis van hun taken en verantwoordelijkheden;
- het combineren uitsluitend plaats te laten vinden nadat de datasets zijn gepseudonimiseerd en na koppeling direct worden ontdaan van hun herleidbaarheid tot personen, met verwijdering van de koppelsleutel.

Op deze wijze kan het privacyrisico voor betrokkenen tot een aanvaardbaar niveau worden beperkt.

1.2.5 Uitwisseling of delen van persoonsgegevens met andere clusters

Het koppelen van data in het kader van het DAP'R moet niet worden verward met de uitwisseling of het delen van persoonsgegevens tussen clusters onderling. Dit laatste kan alleen als de verdere verwerking (het delen met een ander cluster) verenigbaar is met het oorspronkelijke doel waarvoor de persoonsgegevens zijn verzameld (dat is vaak niet het geval).
In de praktijk betekent dit bijvoorbeeld dat datasets (met BSN) die een cluster nodig heeft voor zijn eigen primaire taak, niet met een ander cluster mag worden gedeeld. Indien een ander cluster BSN-gegevens nodig heeft voor zijn eigen primaire taak dan moet dit, conform de daarvoor geldende regels, worden overeengekomen met cluster DV. Gaat het om de uitwisseling van andere persoonsgegevens bijvoorbeeld in het kader van de bestuurlijke aanpak van ondermijning, dan moet daar eerst een DPIA voor worden uitgevoerd. De uitwisseling of delen van persoonsgegevens met andere clusters valt buiten de scope van dit framework.

1.2.6 Verdere verwerking van bijzondere persoonsgegevens

De AVG bevat een verbod op de verwerking van bijzondere persoonsgegevens, behalve als er beroep mogelijk is op een wettelijke uitzondering én op een van de grondslagen voor het verwerken van persoonsgegevens.
De voor het DAP'R belangrijkste uitzondering betreft de verwerking van bijzondere persoonsgegevens die noodzakelijk zijn met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden. De gedachte achter de uitzondering voor wetenschappelijk onderzoek en statistiek[21] is dat betrokkene in beginsel geen gevolgen ondervindt van de verwerking, zolang er maar passende maatregelen zijn genomen om herleidbaarheid te voorkomen.
Deze passende maatregelen zijn:

- securitymaatregelen zoals gescheiden opslag, geautoriseerde toegang en logging;
- maatregelen gericht op dataminimalisatie (afwegingen over nut en noodzaak), pseudonimisering en anonimisering van persoonsgegevens:

[21] Zie bijlage bij dit hoofdstuk voor meer toelichting over 'wetenschappelijk onderzoek of statistische doeleinden.

- bijzondere persoonsgegevens worden na uploaden in het DAP'R direct gepseudonimiseerd en na gebruik direct geanonimiseerd[22];
- onderzoekers van het bestand krijgen bij toepassing van deze techniek dus geen persoonsgegevens onder ogen.

Betrokkenen moeten voorafgaand aan de verwerking door middel van een specifiek op 'onderzoek voor wetenschappelijke en statistische doeleinden' gerichte privacyverklaring op de website van de gemeente te worden geïnformeerd over de verwerking en dat zij daartegen bezwaar kunnen maken.

1.2.7 Behoorlijkheid

Met behoorlijkheid doelt de AVG op het feit dat de verwerking van persoonsgegevens geen verrassing mag zijn voor degenen over wie die gegevens gaan. Omdat dit beginsel verder vorm krijgt bij het voldoen aan andere beginselen, zoals transparantie, doelbinding en dataminimalisatie, behoeft het hier geen verdere bespreking hoe de gemeente bij het datagedreven werken invulling geeft aan 'behoorlijkheid'.

1.2.8 Transparantie

Met transparantie bedoelt de AVG dat de gemeente open dient te zijn over de doelen waarvoor zij persoonsgegevens verwerkt, wélke gegevens zij daarvoor verwerkt, hoe lang zij die gegevens bewaart, etc. Dit beginsel wordt nader uitgewerkt in de artikelen 12, 13 en 14 van de AVG. De gemeentelijke privacyverklaring is bij uitstek het instrument om aan dit beginsel te voldoen. Daarom zal de privacyverklaring van de gemeente in algemene zin melding maken van het gebruik van persoonsgegevens voor onderzoek, statistische en analytische doeleinden. Daarnaast dient de proceseigenaar per informatieproduct te beoordelen of – specifiek voor dat informatieproduct – aanvullende communicatie richting betrokkenen noodzakelijk is om aan het beginsel van transparantie (en het daaraan gekoppeld beginsel van behoorlijkheid) te voldoen.

1.3 Minimale gegevensverwerking (dataminimalisatie).

Om tegemoet te komen aan het beginsel van dataminimalisatie, mag de gemeente niet meer gegevens verwerken dan nodig is voor het doel van de verwerking/het ontwikkelen van het informatieproduct. Dit moet voorafgaand aan elk te ontwikkelen informatieproduct worden vastgesteld.

Dataminimalisatie geldt niet alleen bij het selecteren van de persoonsgegevens die nodig zijn voor het kunnen ontwikkelen van het specifieke informatieproduct maar ook voor het mogen gebruiken van gegevens uit de verschillende bronsystemen die daarvoor nodig zijn. Het te ontwikkelen informatieproduct is bepalend daarvoor. De selectie vindt plaats in het DUB-proces. Gegevens die niet meer nodig zijn voor een of meer informatieproducten worden zo kort mogelijk bewaard met inachtneming van de wettelijke bewaartermijnen (zie hoofdstuk 3).

[22] Deze techniek komt verder aan de orde in hoofdstuk over PET.

Voor bijzondere persoonsgegevens geldt bovendien dat deze mogen pas worden ontsloten in het DAP'R als vaststaat dat zij voor tenminste één informatieproduct nodig zijn, én voor dat informatieproduct een uitzondering van toepassing is op het verbod om bijzondere persoonsgegevens te verwerken (artikel 9 AVG) en UAVG).

1.4 Juistheid

Het beginsel van juistheid houdt in dat de gemeente ervoor moet zorgen dat de door haar verwerkte persoonsgegevens zoveel mogelijk correct zijn. En dat de gemeente onjuiste gegevens – al dan niet op aangeven van de betrokkene – corrigeert. Vergeleken met de andere privacybeginselen heeft dit beginsel een beperkte betekenis binnen het DAP'R. Het corrigeren van gegevens gebeurt namelijk in de bronsystemen. Gecorrigeerde gegevens worden vervolgens automatisch opgenomen en vastgelegd in het DAP'R, zodat de gebruikers van het DAP'R – nadat de brongegevens zijn ververst – over de juiste gegevens beschikken. Zelfs als bij het gebruik van de op het DAP'R opgeslagen gegevens wordt geconstateerd dat gegevens niet correct zijn, dient verbetering in de bronsystemen plaats te vinden.[23]
In specifieke gevallen kan het voorkomen dat er privacyrisico's zijn verbonden aan het onjuist zijn van persoonsgegevens die via het DAP'R beschikbaar zijn gesteld. In die gevallen dient de (proces)eigenaar van het betreffende informatieproduct maatregelen te treffen om die risico's te mitigeren. Deze verantwoordelijkheid is vastgelegd in de governance, zie Hoofdstuk 2.2.4.

1.5 Opslagbeperking

Dit beginsel houdt in dat de gemeente persoonsgegevens niet langer mag bewaren dan nodig is voor het doel waarvoor zij die gegevens verwerkt. Hoe lang die bewaartermijn in een concreet geval is, wordt voor de gemeente nader ingevuld aan de hand van de Archiefwet. De Archiefwet schrijft, in combinatie met de selectielijst, immers voor hoelang de gemeente gegevens moet bewaren, en daarmee tevens de termijn waarmee zij de gegevens moet vernietigen. Uitgangspunt is dat persoonsgegevens in DAPR worden gepseudonimiseerd en waar mogelijk geanonimiseerd. Zie verder Hoofdstuk 3 Levenscyclusbeheer. en Hoofdstuk 4 Security.

1.6 Gegevensbescherming

Dit betreft de informatiebeveiligingsaspecten van het werken met het DAP'R. De Baseline Informatiebeveiliging Overheid (BIO) is leidend voor de maatregelen (controls) die de gemeente implementeert ten aanzien van dit onderwerp. Het betreft zaken als role-based access control, versleuteling en logging & monitoring. De nadere uitwerking hiervan is onderwerp van hoofdstuk **4**, Security. Uitgangspunt van het framework is dat, wanneer de gemeente voldoet aan de BIO, daarmee tevens wordt voldaan aan dit beginsel van de AVG.

[23] Het melden van datakwaliteitsissues bij de bronhouder maakt deel uit van gedegen datamanagement.

1.7 Verantwoording

Het beginsel van verantwoording verlangt van de gemeente dat zij kan uitleggen en aantonen hoe zij – ook bij het datagedreven werken met het DAP'R – voldoet aan de eerste zes privacybeginselen. Dit privacyframework, waarin de nodige beleidskeuzes zijn uitgewerkt en vastgelegd, is daar een onderdeel van. Maar ook zaken als de hierboven genoemde logging & monitoring, het uitvoeren van DPIA's en controles met behulp van audits spelen daar een belangrijke rol in. Er zijn dan ook DPIA's uitgevoerd op de systemen en applicaties waaruit DAPR is opgebouwd. Een aantal maatregelen die in de volgende hoofdstukken worden beschreven komen tegemoet aan de in de DPIA genoemde maatregelen

1.8 Rechten van betrokkenen

Naast het uitvoering geven aan deze beginselen, moet de gemeente burgers en medewerkers in staat stellen om hun AVG-rechten uit te oefenen. Dat heeft Gemeente Rotterdam centraal georganiseerd[24]. Deze rechten gelden ook op het werken met het DAP'R.

Sommige van die rechten vragen echter om specifieke aandacht in het kader van de op dit framework gebaseerde maatregelen:

- *Het recht op informatie* verlangt dat de gemeente een betrokkene informeert over de informatieproducten waarin diens persoonsgegevens worden verwerkt; hiervoor is nodig dat de gemeente inzichtelijk heeft uit welke bronnen gegevens afkomstig zijn, en in welke informatieproducten zij vervolgens worden verwerkt. Dit wordt ook wel datalineage genoemd. Betrokkenen worden geïnformeerd door middel van een specifieke privacyverklaring over datagedreven werken op de website van gemeente Rotterdam.
- *Recht op inzage* houdt in dat betrokkene recht heeft op inzage van de persoonsgegevens die de gemeente van hem/haar verwerkt.
- *Het recht op beperking* betekent dat de gemeente in staat moet zijn de gegevens van een specifieke betrokkene tijdelijk te onderbreken. Als dit zich voordoet betekent dat de gegevens van die betrokkene in geen enkel informatieproduct mogen worden verwerkt.
- *Het recht op bezwaar* houdt in dat een betrokkene bezwaar mag aantekenen tegen de verwerking van zijn/haar gegevens voor specifieke informatieproducten of analytische toepassingen. Als de gemeente besluit om het bezwaar te honoreren, dan mogen de gegevens van die betrokkene vanaf dat moment dus niet meer worden verwerkt in die informatieproducten / analytische toepassingen.
- *Het recht op verwijdering* betekent dat de gemeente op aanvraag van een betrokkene bepaalde gegevens moet verwijderen. Het recht op verwijdering is niet absoluut, maar moet gewogen worden tegen andere rechten en belangen en moet van geval tot geval worden beoordeeld.

Voor de uitoefening van AVG-rechten in het kader wetenschappelijk onderzoek en statistiek geldt een aantal uitzonderingen.

[24] Zie Privacybeleid gemeente Rotterdam, blz. 11-13

- Zo vindt aanpassing van gegevensbestanden op basis van verzoeken of klachten van burgers plaats bij het cluster/bronhouder of externe organisatie waar de gegevens oorspronkelijk zijn vastgelegd.
- Voorts kan het voorkomen dat in geval van het verder verwerken van interne gegevens van gemeente Rotterdam voor wetenschappelijk onderzoek en statistiek vanwege de anonimisering van gegevens niet aan verzoeken van burgers kan worden voldaan.
- Een verzoek tot gegevensaanpassing bij een bron waaraan al gegevens voor onderzoek zijn ontleend moet ook aan het DAP'R worden doorgegeven en daar worden verwerkt.
- Artikel 17, derde lid, onder d, AVG bepaalt dat het recht op verwijdering van persoonsgegevens niet geldt indien dit de doeleinden voor wetenschappelijk onderzoek onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen. In de praktijk kan dit het geval zijn als het onderzoeksbestand al is gegenereerd en het veel moeite zou kosten/of zelfs niet meer mogelijk zou zijn om de individuele gegevens weer op te sporen (bijvoorbeeld omdat ze al zijn gepseudonimiseerd/geanonimiseerd). Het kan ook zo zijn dat de bewuste gegevens van bijzonder belang zijn voor het onderzoeksresultaat. In alle gevallen wordt de betrokkene (of de externe organisatie als gegevens van derden afkomstig zijn, of het interne cluster die de oorspronkelijke data heeft verzameld) van het resultaat op de hoogte gebracht.
- Daarnaast kunnen instellingen voor wetenschappelijk onderzoek en statistiek meer rechten van de betrokkenen buiten toepassing laten[25]. De instelling moet in dat kader als een zodanige instelling of bij of krachtens de wet zijn aangewezen. Als onderdeel van de gemeente kan het DAP'R niet van deze uitzondering gebruik maken. De AVG-rechten van betrokkenen gelden dus altijd voor verwerkingen met behulp van het DAP'R, alleen zal het soms feitelijk niet mogelijk zijn hieraan te voldoen.
- Wanneer persoonsgegevens worden verwerkt op grond van een taak van algemeen belang (artikel 6, eerste lid, onder e, AVG) kan betrokkene daartegen bezwaar maken (artikel 21, eerste lid, AVG). Dit geldt niet in geval van gegevensverwerking voor wetenschappelijk onderzoek en statistiek voor een taak die noodzakelijk is voor een taak van algemeen belang. Die taak moet dan wel door een bestuursorgaan, zoals het college van B&W zijn aangewezen.

[25] Artikel 44 UAVG: het gaat om het recht op correctie, verwijdering en op beperking van de gegevensverwerking.

2 Privacygovernance datagedreven werken

Dit document[26] beschrijft de privacygovernance[27] rondom datagedreven werken met behulp van het Data & Analyse Platform Rotterdam (DAP'R). Met governance wordt in deze context bedoeld: de definitie van de betrokken rollen, de verdeling van hun verantwoordelijkheden, en – waar van toepassing – de procedures waarbinnen die verantwoordelijkheden worden uitgeoefend. De beschrijving van de governance vindt ook plaats in die volgorde:

1. de definitie van rollen;
2. de beschrijving van hun verantwoordelijkheden;
3. de procedures aan de hand waarvan de rollen hun verantwoordelijkheden uitoefenen.

De koppeling tussen rollen en verantwoordelijkheden is beschreven in de bijbehorende RACI-matrix.

2.1 Proces van verwerking data op DAP'R

Voor de verwerkingen in het kader van het DAP'R wordt het proces van aanvraag tot oplevering van een informatieproduct als één onlosmakelijk proces van verwerking beschouwd (zie hoofdstuk 1.2.1.2).
Voor de toepassing van de privacygovernance wordt in het proces van de verwerking van de data onderscheid gemaakt in de volgende fasering:

- In de eerste fase worden de gegevens verkregen uit de diverse aanleverende bronnen/bronsystemen naar DAP'R. Deze gegevens begeven zich via verschillende tussenstappen naar de opslaglaag,[28] waar ze beheerd worden..
- In de tweede fase worden de data in gebruik genomen door ze te bewerken tot een informatieproduct (onderzoek, dashboard, werkplanning, etc).
- In de derde fase is het product afgerond en worden de data die voor het product zijn gebruikt (versleuteld) bewaard of geanonimiseerd.

2.2 Doel en grondslag en het DAP'R

Van belang is dat voorafgaand aan de verwerking (en daarmee voor de start van de eerste fase) voor elk te ontwikkelen informatieproduct een duidelijk omschreven doel met bijbehorende grondslag voor het gebruik van persoonsgegevens moet worden vastgesteld.
Voorafgaand aan elk te ontwikkelen informatieproduct vindt in het DUB proces een beoordeling plaats van nut, noodzaak, doel, grondslag, dataminimalisatie, etc.
Dat betekent dat ook de afweging wordt gemaakt of het doel proportioneel is en of het voldoet aan het subsidiariteitsbeginsel.
Het proces van verkrijging tot oplevering van een informatieproduct wordt daarbij als één onlosmakelijk proces van verwerking beschouwd. Wanneer er een aanvraag is om bepaalde

[26] Dit hoofdstuk maakt onderdeel uit van het privacyframework voor datagedreven werken.
[27] Ook al bespreekt dit document de *privacy*governance voor datagedreven werken, de governance heeft ook betrekking heeft op het datagedreven werken met niet-persoonsgegevens.
[28] Het is mogelijk dat er technisch gezien sprake is van meerdere opslaglocaties. Dat neemt niet weg dat er logisch gezien één opslaglaag is, ook al kunnen de data zich fysiek verspreid over verschillende locaties, databases of platformen bevinden. Op het moment van vaststellen van deze governance zijn de belangrijkste opslaglocaties van het DAP'R het concern Datawarehouse en het Datalake.

gegevens op DAP'R voor een ander doel te gebruiken, wordt ook daarvoor eerst doel en grondslag bepaald. Ieder informatieproduct heeft dus een eigen doel en AVG-grondslag, zoals beschreven in hoofdstuk 1. <link naar pa

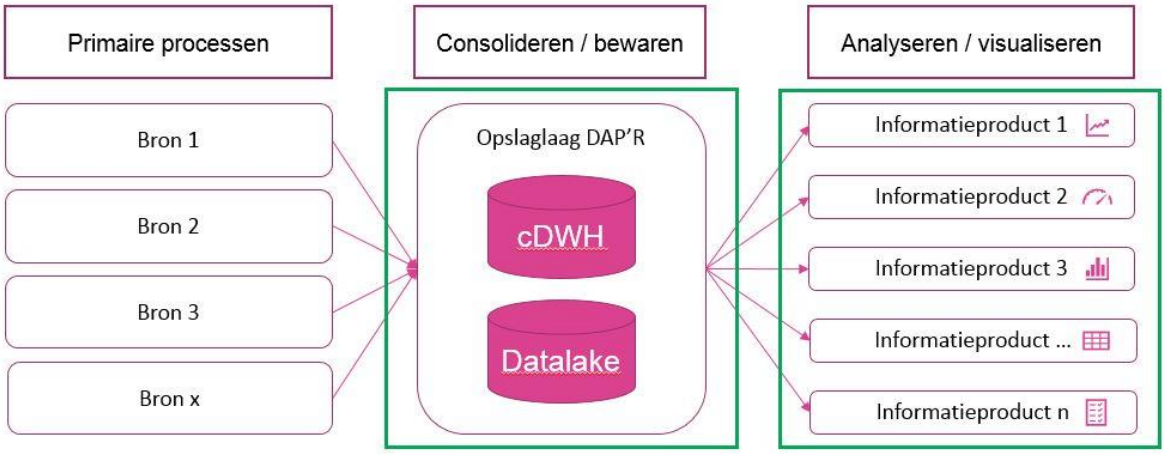
Dit geldt ook als er in dat proces gebruik gemaakt wordt van algoritmes met persoonsgegevens. Deze vallen ook onder het regime van de AVG en maken onderdeel uit van de hier beschreven governance. Aanvullend is er een algoritme governance, waaraan als adviserend orgaan de AAB (Algorithm Advisory Board) is toegevoegd. Tijdens het DUB proces worden in het DUB advies naast de privacy- en securityaspecten ook de informatiebeheer, datamanagement-, ethische aspecten en waar van toepassing ook algoritmegebruik meegenomen. In dat laatste geval wordt ook de algoritme expert betrokken bij het DUB proces.

2.2.1 Verantwoordelijkheden

Uit het bovenstaande volgt dat voorafgaand aan elk te ontwikkelen informatieproduct twee gegevensleveringsovereenkomsten (GLO) worden afgesloten, nl. die tussen bronhouder en hoofd OBI, en tussen Hoofd OBI en de producteigenaar, waarbij elk van de drie partijen zijn eigen bevoegdheden en verantwoordelijkheden heeft. Er is dus een knip in verantwoordelijkheden tussen verkrijging, beheer en gebruik.

- **Bronhouder** stemt door middel van ondertekenen van de GLO in om 'zijn' gegevens voor specifiek omschreven doelen en conform de eisen van de AVG (verder) te verwerken.
- **Hoofd OBI** stemt door middel van het ondertekenen van de GLO in om de ontvangen gegevens te beheren conform de eisen van de AVG en hetgeen is overeengekomen in de GLO.
- **De Producteigenaar** stemt door middel van het ondertekenen van de GLO in met de verantwoordelijkheid voor de inhoud van het te ontwikkelen informatieproduct (en niet met de technische en organisatorische aspecten daarvan, dat valt onder het beheer van hoofd OBI) en voor het verdere gebruik daarvan door de gebruikers van zijn informatieproduct.
  De proceseigenaar baseert zich hierbij op het advies dat uit het DUB proces volgt. Onderdeel daarvan is het advies van de privacyofficer(s) en het bindend advies van de bronhouder.

Dit leidt tot de volgende (versimpelde) weergave van hoe data vanuit verschillende bronnen, via de opslaglaag, naar specifieke informatieproducten / analytische toepassingen stromen:



2.2.2 Hergebruik

Zolang gegevens in de opslaglaag aanwezig zijn voor een bepaald informatieproduct kunnen deze ook beschikbaar worden gesteld voor andere informatieproducten. Hiervoor dient dan ook een DUB proces te zijn doorlopen.
Het bepalen van de inhoud van een dataset is een gezamenlijk inspanning van de product owner van het betreffende informatieproduct als afnemer, en OBI als leverancier. Uiteindelijk is de proceseigenaar die het informatieproduct afneemt eindverantwoordelijk voor het vaststellen van welke gegevens deel uitmaken van de dataset. De proceseigenaar baseert zich hierbij op het advies dat uit het DUB proces volgt. Onderdeel daarvan is het advies van de privacyofficer(s) en advies van de bronhouder. Zie hiervoor ook het DUB proces.
De specificatie daarvan maakt deel uit van de op te stellen gegevensleveringsovereenkomst.

2.2.3 Rapportagetools

Voor het daadwerkelijk omzetten van gegevens in inzichten met behulp van informatieproducten, maakt de gemeente gebruik van verschillende rapportagetools (bijvoorbeeld Cognos).
Alhoewel verschillend in functionaliteit en mogelijkheden om gegevens te visualiseren, hebben zij gemeen dat het gebruik van deze applicaties plaatsvindt in het kader van het gebruik van de data, waarbij ieder informatieproduct voor de AVG als eigenstandig verwerkingsproces wordt beschouwd. De verantwoordelijkheid voor het voldoen van dit proces aan de AVG ligt bij de proceseigenaar/ eigenaar van het informatieproduct.

2.2.4 Verantwoordelijkheden verzamelen, vastleggen en bewaren van gegevens

Van belang is dat de hier beschreven governance voornamelijk betrekking heeft op de totstandkoming, het gebruik en het uitfaseren van de diverse informatieproducten.

Voor de daaraan voorafgaande verkrijging – het verzamelen, vastleggen en bewaren van gegevens in het cDWH en het Datalake – geldt dat de verantwoordelijkheid voor het beheer en het voldoen aan wet- en regelgeving exclusief bij het hoofd OBI ligt. Oftewel: het hoofd OBI is de proceseigenaar en moet er dus voor zorgen dat de juiste maatregelen worden geïmplementeerd om te voldoen aan de AVG, de BIO en de Archiefwet. Dat wil zeggen dat op het moment dat de gegevens worden gedownload op DAP'R, Hoofd OBI verantwoordelijk is voor het beheer van de data op DAP'R. Zodra de GLO met de proceseigenaar/afnemer is

getekend komt de verantwoordelijkheid voor het opvolgen van de AVG daar te liggen. Dat wil zeggen dat deze verantwoordelijkheid draagt voor het eindproduct en de eventuele persoonsgegevens die daar in staan. In de GLO worden de afspraken daarover vastgelegd. Echter het (technische) beheer van de data op DAP'R blijft een verantwoordelijkheid van IIFO/Hoofd OBI. Hiermee kan ook het toezicht centraal belegd worden.
In geval van een datalek hangt het van de omstandigheden af waaronder deze heeft plaatsgevonden wie hiervoor verantwoordelijk is. Zodra het datalek ontdekt is moet daarvan melding worden gedaan en volgt dit het datalekkenprotocol.

2.2.5 Privacygovernance

Tot slot: de in dit hoofdstuk uitgewerkte governance sluit aan op de algemene privacygovernance van de gemeente, zoals vastgelegd in het gemeentelijk privacybeleid,[29] en hetgeen is beschreven in de Kadernota Sturen en Verantwoorden Rotterdam 2020[30] en het Besluit Mandaat, Volmacht en Machtiging Rotterdam 2021[31]

Het betreft dus niet een op zichzelf staande governance, maar een uitwerking daarvan specifiek voor datagedreven werken. Voor zover de hieronder beschreven rollen ook worden benoemd in de algemene privacygovernance hebben zij dezelfde betekenis. Voor het overige zijn de rollen zo veel mogelijk overgenomen uit de door de stuurgroep Datastrategie vastgestelde 'way of working' (WoW) voor data- & analyseprojecten. Deze WoW beschrijft in welke stappen een informatieproduct projectmatig tot stand komt binnen de Data en Analytics Competentie Centra van de gemeente.

Daarnaast is ook de aansluiting gezocht op de *datagovernance* binnen de gemeente. Datagovernance is gericht op het borgen van het definiëren, de beschikbaarheid en de kwaliteit van data, en heeft zijn eigen organisatorische inrichting:

Niveau	Verantwoordelijke voor gehele data levenscyclus	(Leveranciers)verantwoordelijk voor data (functionele en technische aspecten)
Bestuurlijk niveau	Vakwethouder (bestuurlijk opdrachtgever)	Wethouder Organisatie verantwoordelijk voor BCO/IIFO
Beleidsniveau	Directeur beleidsafdeling	Directeur IIFO
Uitvoeringsniveau	Proceseigenaar databron (alias Bronhouder, Data steward, Data-eigenaar): verantwoordelijk voor kwaliteit, definitie en gebruik databron. Proceseigenaar gebruiksverwerking (alias Eigenaar Informatieproduct, Klant, Afnemer, De Rotterdammer): verantwoordelijk voor gebruik van beschikbaar gestelde data binnen wet & regelgeving en vigerend beleid.	Generieke ICT voorzieningen: opslag, integratie, verwerking en distributie Beheer: Technisch en Functioneel beheerder
Controle en advies	Tweede lijn: Privacy, Security, Informatiebeheer, Algoritmes Data architectuur	Tweede lijn: CPO, CISO, PBI en BCO voor overkoepelende data governance Derde lijn: FG, Archiefinspectie, Concern Auditing

[29] Privacybeleid gemeente Rotterdam - RIO
[30] kadernota-sturen-en-verantwoorden-2020-def.pdf (rotterdam.nl)
[31] Besluit mandaat, volmacht en machtiging Rotterdam 2021 | Lokale wet- en regelgeving (overheid.nl)

De primaire verantwoordelijkheid voor data binnen de datagovernance ligt bij de Proceseigenaar databron (ook wel de bronhouder genoemd). De betrokkenheid van deze rol bij de compliance-aspecten van het datagedreven werken wordt hieronder besproken.

Tot slot: wanneer gebruik gemaakt wordt van algoritmetoepassingen is de algoritme governance aanvullend van kracht op de privacy- en de datagovernance zoals beschreven in dit Framework. Hiervoor kan ondersteuning gezocht worden bij de algoritme-experts van de gemeente en is een aanvullende derde lijn (AAB) ingericht, naast de derde lijn die voor alle vormen van datagedreven werken geldt (FG, Concern Auditing).

2.3 Rollen

2.3.1 Proceseigenaar gebruik (= eigenaar informatieproduct)

De proceseigenaar van de gebruiksverwerking is eindverantwoordelijk voor de compliance-aspecten van zijn/haar informatieproducten, waaronder het voldoen aan de AVG, BIO en Archiefwet. Dit heeft zowel betrekking op (de eigenschappen van) het informatieproduct zelf, het gebruik ervan door medewerkers van de gemeente en, voor zover van toepassing, het delen van het informatieproduct met externe partijen. Hij/zij bepaalt dus ook welke medewerkers toegang krijgen tot het informatieproduct, en wat hun toegangsrechten precies inhouden. Dit geldt wanneer het informatieproduct persoonsgegevens of naar personen herleidbare gegevens bevat. De toegangsrechten moeten gerelateerd zijn aan de functie.
De proceseigenaar / eigenaar van het informatieproduct is vaak ook degene die opdracht geeft tot het realiseren van dat informatieproduct, en daar het budget voor beschikbaar stelt. Meestal zal het een lijnmanager uit een van de clusters betreffen.
Om er zeker van te zijn dat te allen tijde iemand verantwoordelijk is voor het informatieproduct, zal OBI het informatieproduct slechts in beheer nemen, en de daarvoor benodigde data vanuit het cDWH en/of het Datalake beschikbaar stellen, als een lijnmanager zich over het proceseigenaarschap ontfermt en daarmee de betrokken (resterende) privacyrisico's aanvaardt. Die aanvaarding blijkt uit de ondertekening van een gegevensleveringsovereenkomst (GLO) tussen OBI en de proceseigenaar.[32]

Tot slot is het primair aan de eigenaar van het informatieproduct om ook toezicht te houden op de implementatie en effectiviteit van de compliancemaatregelen; de proceseigenaar vormt immers de 'first line of defense'.

2.3.2 Product owner

De product owner is een medewerker van de gemeente die namens de proceseigenaar optreedt bij het bepalen en prioriteren van de eigenschappen van het informatieproduct. De product owner heeft dus een leidende rol – maar niet de laatste stem – bij het bepalen van onder meer het doel van het informatieproduct, en hoe de output wordt gepresenteerd aan de gebruiker. Veel activiteiten die onder de eindverantwoordelijkheid van de proceseigenaar vallen, worden daarmee uitgevoerd door de product owner. Daarmee is de product owner als het ware gedelegeerd eigenaar van het informatieproduct.

2.3.3 Gebruiker informatieproduct

De gebruiker is degene die in de dagelijkse praktijk toegang heeft tot, en gebruik maakt van de output van het informatieproduct. Deze rol kan samenvallen met die van eigenaar of de

[32] Zie de paragraaf over het afsluiten van GLO's.

product owner, maar dat zal zeker niet altijd het geval zijn. Van de gebruiker wordt verlangd dat hij/zij het informatieproduct alleen gebruikt voor het doel waarvoor het is ontwikkeld, zodat het gebruik voldoet aan het doelbindingsvereiste van de AVG. Alhoewel de gebruiker daar geen formele rol in heeft, zal hij/zij in de praktijk ook betrokken kunnen worden bij het opstellen van user requirements ten aanzien van het informatieproduct, in het bijzonder met betrekking tot de benodigde datakwaliteit.

2.3.4 Proceseigenaar databron (alias bronhouder)

Het is aan de proceseigenaar van de databron[33] om te zorgen voor de definitie en kwalificatie van de data(objecten) waarvan hij/zij de bronhouder is, dat deze data beschikbaar zijn voor datagedreven werken, en dat de data voldoen aan de afgesproken kwaliteit. Deze rol staat ook wel bekend als de bronhouder. De bronhouder legt de definitie van de data vast in de datacatalogus.
Daarnaast geeft de bronhouder een bindend advies over het voorgenomen (her)gebruik van de gegevens waar hij/zij de bronhouder van is. Afspraken over kwaliteit en beschikbaarheid van data worden vastgelegd in een GLO tussen de bronhouder en OBI.
De aansprakelijkheid voor verantwoord gebruik ligt na ondertekening van de GLO bij Hoofd OBI voor het beheer van de data en later, na ondertekening van de GLO bij de afnemerproceseigenaar(s) van die informatieproducten.

2.3.5 Escalatie

Als de proceseigenaar databron / bronhouder het niet eens is met het beoogd gebruik van data waarvan hij/zij bronhouder is, en zijn/haar advies wordt niet opgevolgd dan kan hij/zij dit escaleren via het escalatiepad van de datagovernance:

- Als de bronhouder en de afnemer/eigenaar van het informatieproduct zich binnen hetzelfde cluster bevinden, wordt het verschil van inzicht voorgelegd aan de directie van het betreffende cluster.
- Als de bronhouder en de eigenaar van het informatieproduct zich binnen verschillende clusters bevinden, wordt het verschil van inzicht voorgelegd aan de Data Board.
  De Databoard bestaat uit een vertegenwoordiging van de clusterdirecties, en volgt de samenstelling van de stuurgroep datastrategie.

Als dit niet leidt tot een bevredigend resultaat, kan de zaak verder worden geëscaleerd naar de concerndirectie en uiteindelijk het College. Zolang de escalatieprocedure loopt, kan het informatieproduct niet in productie worden genomen, en zal geen structurele aanlevering van gegevens plaatsvinden vanuit de bron of vanuit de opslaglaag van het DAP'R.

2.3.6 Proceseigenaar verkrijging: Hoofd OBI

Naast de eindverantwoordelijkheid voor de compliance aspecten van de verkrijging van de data is de houder van deze rol ook verantwoordelijk voor het afsluiten van gegevensleveringsovereenkomsten:

- als afnemer van data ten behoeve van de verkrijging van data – in dat geval is de bronhouder de dataleverancier;
- als leverancier van data ten behoeve van gebruik in de diverse informatieproducten in dat geval is de eigenaar van het informatieproduct de data-afnemer.

[33] Dat wil zeggen: de proceseigenaar van het (primaire) proces waarin de data is 'ontstaan' (de AVG spreekt van verzamelen)

2.3.7 Beheerder DAP'R (OBI)

De beheerder van het DAP'R heeft een belangrijke faciliterende rol ten aanzien van het datagedreven werken. Die rol houdt onder meer in:

- het onderhouden en beschikbaar stellen van het Data & Analyse Platform Rotterdam voor het samenstellen van informatieproducten en het uitvoeren van analyses;
- het in opdracht van de verschillende clusters in beheer nemen/hebben van informatieproducten;
- het samenstellen van datasets op basis van de in de opslaglaag aanwezige data ten behoeve van self-service BI;
- het borgen van afspraken over de beschikbaarheid en kwaliteit van data;
- het op regelmatige basis rapporteren aan de verschillende proceseigenaren welke informatieproducten in beheer zijn, zodat zij geïnformeerd zijn over de informatieproducten waarvoor zij verantwoordelijk zijn;
- het adviseren van clusters en data- & analyseprojecten over de compliance-aspecten van datagedreven werken, waar onder de te implementeren privacybevorderende maatregelen;[34]
- het zorgen voor kennisdeling en bewustwording met betrekking tot de compliance-aspecten van datagedreven werken;
- het bijhouden van de datalineage.

Deze rol is – net als die van proceseigenaar van de verkrijgingsverwerking – belegd bij (het hoofd van) de afdeling OBI binnen het cluster BCO.

Manager DACC[35]

Per cluster is er een Data & Analytics Competence Center (DACC). Een DACC is een multidisciplinair team waarin IIFO en de clusters samenwerken om te voorzien in de informatiebehoefte van ieder cluster met behulp van informatieproducten. Ieder DACC wordt geleid door een DACC-manager. Namens de proceseigenaar zorgt de DACC-manager ervoor dat in het register van informatieproducten wordt bijgehouden welke informatieproducten in gebruik zijn.

Ook voor het ontwikkelen en testen van informatieproducten kan het nodig om te werken met (persoons)gegevens. Daarmee is de manager DACC ook eindverantwoordelijk voor de compliance-aspecten daarvan. De DACC-manager moet er dus voor zorgen dat degenen die zijn betrokken bij de ontwikkel- en testwerkzaamheden op de hoogte zijn van, en rekening houden met de eisen die wet- en regelgeving stellen aan het werken met (persoons)gegevens In principe wordt alleen gewerkt met versleutelde gegevens.
Voor informatieproducten die door een cluster in het kader van self-service BI worden ontwikkeld, ligt de verantwoordelijkheid voor bovengenoemde activiteiten bij het hoofd van de betreffende afdeling.

2.3.8 Business consultant

Ieder DACC heeft een business consultant. De business consultant werkt als adviseur en systeembewaker van het datagedreven werken. Hij/zij adviseert over de te maken stappen in volwassenheid rondom datagedreven werken en voert indien nodig uit. In relatie tot de compliance aspecten overziet de business consultant het geheel en adviseert aan zowel manager DACC als compliance specialisten.

[34] Ten behoeve van deze adviesfunctie beschikt OBI over een compliance officer, een privacyspecialist en een algoritme-expert.
[35] DACC staat voor **Data & Analytics Competence Center, een multidisciplinaire team waarin IIFO en de clusters samenwerken om te voorzien in de informatiebehoefte van de clusters. Per cluster is er een separaat DACC, die met behulp van scrumteams informatieproducten ontwikkelen.**

2.3.9 Functioneel beheerder

De functioneel beheerder van de applicaties binnen het DAP'R hebben een belangrijke uitvoerende rol bij het administreren van toegangsrechten. Zij zijn namelijk degenen die gebruikersrechten feitelijk invoeren, wijzigen en uiteindelijk weer verwijderen.[36] Ook rapporteren zij regelmatig aan de verschillende eigenaren van informatieproducten over de bestaande toegangsrechten tot hun informatieproducten, zodat de eigenaren kunnen beoordelen of de bestaande rechten correct zijn.

2.3.10 Informatie-analist / data-analist

De informatie-analist en/of data-analist is degene die voorziet in de vertaling van de business behoefte in wensen voor dataoplossingen, de oplevering van data en de uitvoering van activiteiten m.b.t. privacy, security en informatiebeheer. Zij hebben dus een belangrijke ondersteunende rol bij het specificeren van het doel en de AVG-grondslag van het informatieproduct / de gebruiksverwerking, het vaststellen van welke (persoons)gegevens daarvoor nodig zijn, en het vaststellen van privacybevorderende maatregelen. Ook zijn zij betrokken bij de implementatie en documentatie van de maatregelen, nadat de (toekomstig) proceseigenaar van het informatieproduct die maatregelen – al dan niet met behulp van een DPIA – heeft vastgesteld.

2.3.11 BI-specialist / data engineer / data scientist / poweruser

Dit zijn de medewerkers die zorgen voor het realiseren van informatieproducten c.q. het uitvoeren van analyses op datasets, en het technisch ontsluiten en prepareren van de benodigde data met behulp van de daarvoor beschikbare tooling – bijvoorbeeld applicaties als Cognos, Power BI en SAS Viya, programmeertalen als Pyhton en R, en ETL-tooling en ontwikkelomgevingen als Azure Databricks. Zij zorgen er dus voor dat (persoons)gegevens daadwerkelijk worden omgezet in de gewenste inzichten die een informatieproduct of analyse moet opleveren. Daarmee hebben zij een belangrijke rol bij het bepalen welke persoonsgegevens wel/niet nodig zijn, en dus het voldoen aan het beginsel van dataminimalisatie. Verder implementeren zij een belangrijk deel van de technische maatregelen voor het mitigeren van privacyrisico's.

Deze medewerkers werken voor een van de clusterspecifieke Data & Analytics Competence Centers, of in het geval van een poweruser (in het kader van self-service BI), elders binnen een cluster. Omdat zij bij het ontwikkelen en testen van het informatieproduct en het uitvoeren van analyses mogelijk met grote hoeveelheden persoonsgegevens werken, wordt van hen verwacht dat zij daar zeer zorgvuldig mee omgaan. Bovendien dienen de projectomgevingen waarin zij werken strikt van elkaar te zijn gescheiden. Op die manier hebben alleen de medewerkers die daadwerkelijk zijn betrokken bij het realiseren van het betreffende informatieproduct of het uitvoeren van een bepaalde analyse toegang tot de gegevens die daarvoor nodig zijn.

2.3.12 Privacy compliancespecialist

OBI ondersteunt de clusters ook door expertise te leveren op het gebied van privacy-/compliancevraagstukken bij datagedreven werken. De privacy compliancespecialist verzorgt de voorfase van het DUB-proces, samen met de gegevensmakelaar, op basis waarvan de leden van het DUB gericht hun adviezen kunnen uitbrengen. Voorts onderhoudt de privacycompliance specialist de richtlijnen voor de compliance-aspecten van datagedreven werken, waaronder dit privacyframework, adviseert in concrete gevallen bij het realiseren van

[36] Voor het concern Datawarehouse gebeurt dit door Wijzigingsbeheer van het team DWH van de afdeling OBI.

nieuwe informatieproducten, ondersteunt bij het uitvoeren van DPIA's, en houdt toezicht op de implementatie en effectiviteit van privacybevorderende maatregelen voor zowel de verkrijging als voor het (her)gebruik van de data.

2.3.13 Gegevensmakelaar

De belangrijkste taak van een gegevensmakelaar is het bij elkaar brengen van de vraag naar en het aanbod van data. Een gegevensmakelaar heeft dan ook bij uitstek zicht op welke data beschikbaar is om tot de door de opdrachtgever/proceseigenaar gewenste inzichten te komen. Op basis van die kennis kan een gegevensmakelaar goed inschatten welke (persoons)gegevens nodig zijn om te verwerken in het informatieproduct, en wat de kwaliteit van de daarvoor benodigde data is. Ook speelt de gegevensmakelaar een belangrijke rol bij de totstandkoming van de gegevensleveringsovereenkomst tussen dataleverancier en afnemer.

2.3.14 DISO / adviseur informatiebeheer / algoritme-expert

Deze functionarissen nemen – samen met de Privacy Officer – deel aan de Data Usage Board[37] (DUB) hebben een belangrijke adviserende taak richting de (toekomstig) proceseigenaar, omdat zij hem/haar adviseren over de te implementeren maatregelen uit hoofde van de AVG (en andere privacyregelgeving), de BIO en de Archiefwet. Ook adviseren zij waar van toepassing over de ethische aspecten van het informatieproduct,[38] zaken op het gebeid van datamanagement en het publiceren van data op grond van de Wet hergebruik overheidsinformatie. Dit doen de leden door vanuit hun expertise te adviseren over het te ontwikkelen informatieproduct.

2.3.15 Privacy Officer (PO)

De privacy officer neemt deel aan het DUB proces en adviseert daarin over de AVG aspecten van een bepaald informatieproduct. Hij/zij adviseert de proceseigenaar, waar nodig in samenspraak met de PO van de bronhouder en de security officer over de te nemen maatregelen. Het DUB proces leidt tot eén integraal advies waarin de Privacy officer het advies opstelt met input van de andere experts in het DUB proces.
Wanneer het DUB advies niet wordt overgenomen door de proceseigenaar kan de privacy officer of een ander lid van het DUB het advies voorleggen aan de FG,

2.3.16 Functionaris gegevensbescherming (FG)

De rol van de FG is niet anders dan bij de verwerkingen van persoonsgegevens in de primaire processen van de gemeente: Wanneer het DUB proces tot een advies leidt waarmee de proceseigenaar/afnemer het oneens is kan de FG om advies worden gevraagd. Zodoende is de FG onderdeel van de escalatieladder.
Wanneer het DUB proces leidt tot een DPIA wordt de DPIA altijd voorgelegd aan de FG, voorzien van advies door de PO'er, waarna de FG een advies geeft.
Tevens houdt de FG – als third line of defence – systeemtoezicht.

Interne auditor

De interne auditfunctie vormt – samen met de FG – de derde linie in het three lines of defense-model dat de gemeente hanteert. Interne auditors van Concern Auditing kunnen onafhankelijk de governance-, risicomanagement- en interne beheersingsprocessen van een organisatie beoordelen en geven aanvullende zekerheid over de kwaliteit ervan. Ze

[37] Zie hierover de paragraaf DUB-proces.
[38] In het bijzonder als de verwerking van gegevens plaatsvindt met behulp van een algoritme.

beantwoorden dus de volgende vraag: bestuurt de 1e lijn (management) de organisatie toereikend en worden ze hierin voldoende ondersteund door de 2e lijn?
Onderdeel van de governance is het controleren of de werkwijze en vastgestelde procedures ook daadwerkelijk worden gevolgd, en hierop te handhaven waar nodig. Daartoe zal de interne auditors (Concern Auditing) worden gevraagd een audit uit te voeren op de werking van dit kader in de praktijk. Daarnaast zal ook binnen OBI periodiek geëvalueerd worden, door een daarvoor aan te wijzen team. Waar nodig zal hoofd OBI opdracht geven de uitkomsten van audits en evaluaties door te voeren in het technische en organisatorische proces.

2.4 Procedures

Er zijn vele procedures die een rol spelen bij het werken met (persoons)gegevens. Denk aan autorisatieprocedures, de procedure voor het faciliteren van de (AVG-)rechten van betrokkenen en het melden/afhandelen van datalekken. De meeste procedures hebben een generiek karakter, en kunnen ook op het datagedreven werken worden toegepast.[39] Er zijn echter ook enkele procedures die specifiek voor datagedreven werken van belang zijn, en een belangrijke rol hebben bij het voldoen aan wet- en regelgeving. De voornaamste daarvan is het DUB-proces, als vast onderdeel van de way of working voor data- & analyseprojecten. Deze way of working geeft handvatten voor het realiseren van een informatieproduct, van eerste idee tot en met de in beheername en doorontwikkeling.[40] Maar ook als bij het realiseren of het doorontwikkelen van een informatieproduct niet volgens de way of working wordt gewerkt, is de proceseigenaar verplicht om advies te vragen aan de DUB.
Daarnaast speelt het GLO-proces een belangrijke rol bij het borgen van afspraken over het (door)leveren van data en de kwaliteit daarvan, maar ook bij het vastleggen van wie proceseigenaar is van – en dus verantwoordelijk is voor – welk informatieproduct.

2.4.1 DUB-proces

De Data Usage Board is een orgaan dat advies uitbrengt aan de toekomstige (proces)eigenaar van een te realiseren informatieproduct. Dit advies ziet onder meer opde volgende aspecten:

- Nut, noodzaak, doel, grondslag, dataminimalisatie en alle andere AVG principes.
- de te implementeren maatregelen voor het beperken en beheersen van privacyrisico's en informatiebeveiligingsrisico's;
- de te hanteren bewaartermijn;
- de toepassing van de FAIR-principes (Findable, Accessable, Interoperable, Reusable) op de outputdata;
- het verhogen van de data kwaliteit en daarmee de waarde van de data
- bepalen of uitvoering van een DPIA vereist is voor dataverwerkingen (waaronder algoritmes)
- de ethische aspecten van het informatieproduct, met name bij de inzet van algoritmes, waarbij naast een DPIA een ethische toets (DEDA bij laag risico of IAMA bij hoog risico), wordt uitgevoerd.

De samenstelling van de DUB is deels afhankelijk van het te ontwikkelen informatieproduct:

[39] Denk aan de procedures voor het bijwerken van het verwerkingsregister, het afsluiten van verwerkersovereenkomsten, het effectueren van de rechten van betrokkenen en het melden en afhandelen van potentiële datalekken.
[40] @@ Link opnemen naar beschrijving way of working op procesplein

- Als ten behoeve van het informatieproduct persoonsgegevens zullen worden verwerkt, neemt de Privacy officer van het opdrachtgevende cluster of afdeling plaats in de DUB. Zo nodig ook de privacy officer van de bronhouder(s).
- Als de verwerking plaatsvindt met behulp van een algoritme,[41] neemt ook een algoritme-expert deel aan het DUB.

Mede om te borgen dat *privacy by design* wordt toegepast, geeft de Data Usage Board twee keer advies over het te realiseren informatieproduct:

- Een advies aan het begin van het project, voordat het project start met de daadwerkelijke ontwikkelactiviteiten. Dit advies heeft onder meer betrekking op het te dienen doel en mogelijke grondslagen voor de verwerking, te implementeren beveiligingsmaatregelen, te hanteren bewaartermijnen en of het nodig is om een DPIA[42] en/of een ethische toets uit te voeren.
- Daarnaast vraagt de gegevensmakelaar die de DUB-bijeenkomst voorbereidt aan de Privacy Officer van het dataleverende cluster om schriftelijk advies uit te brengen. Dit advies heeft in het bijzonder betrekking op de verenigbaarheid van het gebruik van de brondata met de oorspronkelijke verwerkingsdoelen.
- Een advies aan het einde van het project, voordat OBI of het cluster het informatieproduct in beheer neemt. In het tweede advies beoordeelt de DUB in hoeverre de geïmplementeerde maatregelen een effectieve bijdrage leveren aan het beperken en beheersen van risico's en wordt een definitief Privacy advies gegeven.

Zie voor de nadere beschrijving en uitwerking van het DUB-proces en de daarbij behorende formulieren Data Governance (data hergebruik/ processen).

2.4.2 Gegevensleveringsovereenkomsten (GLO's)

Een GLO is een overeenkomst tussen twee partijen binnen de gemeente die betrekking heeft op het leveren van data: de dataleverancier en de afnemer. In een GLO maken leverancier en afnemer afspraken over om welke gegevens het precies gaat, en over de beschikbaarheid en kwaliteit van de betreffende gegevens. Zie datacontracten (GLO en DTA) voor de beschrijving van het proces voor het afsluiten van GLO's.

Parallel aan het onderscheid in verantwoordelijkheden tussen de verkrijging en de diverse gebruikstoepassingen is er een GLO voor:

- het ontsluiten van brongegevens en het bewaren daarvan in de opslaglaag van het DAP'R – de leverancier is dan de bronhouder, de afnemer is (het hoofd van) de afdeling OBI.
- het beschikbaar stellen van gegevens vanuit de opslaglaag ten behoeve van een specifiek informatieproduct – de leverancier is in dat geval (het hoofd van) de afdeling OBI, en de afnemer is de proceseigenaar van het informatieproduct.

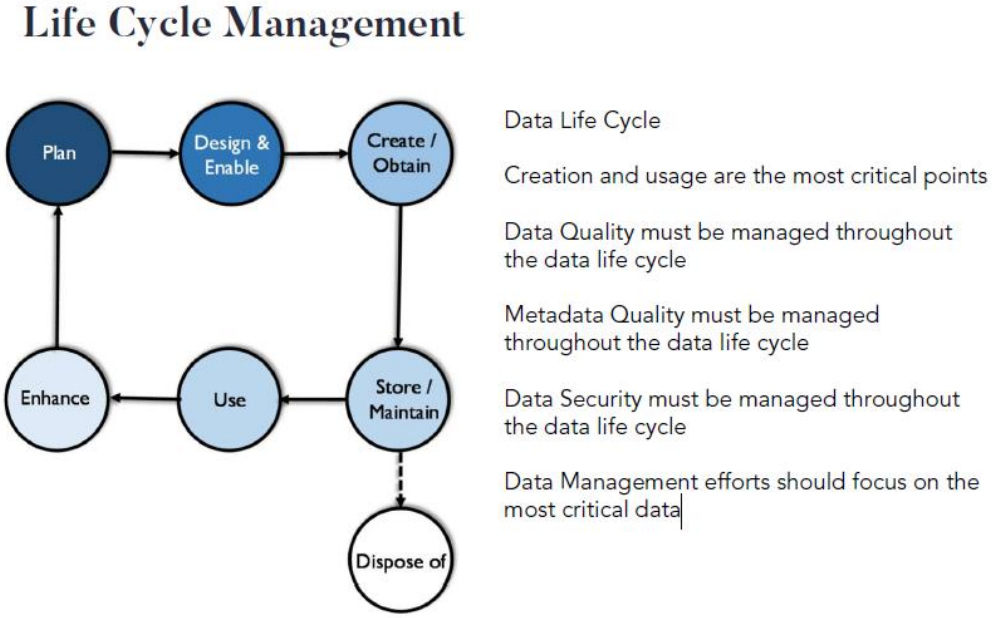
Zoals in de vorige paragraaf vermeld, zal de afdeling OBI data alleen structureel ter beschikking stellen aan de afnemer als er een GLO tot stand is gekomen tussen beide partijen. Door ondertekening van de GLO geeft de afnemer tevens aan dat hij/zij de risico's aanvaardt die voortvloeien uit het verwerken van de betreffende (persoons)gegevens.

[41] Zoals bedoeld in de algoritmegovernance van de gemeente; zie @@

[42] Onderdeel van dit framework is een aparte DPIA-template voor informatieproducten, opgenomen in annex III. Deze template beperkt zich tot de aspecten die voor ieder informatieproduct anders zijn, zoals doel, grondslag en benodigde persoonsgegevens. De aspecten van het gebruik van Cognos, Power BI en SAS Viya, die voor ieder informatieproduct hetzelfde zijn, zijn besproken in separate 'generieke DPIA's'.

3 Levenscyclusbeheer

Levenscyclusbeheer gaat over (de beheersprocessen rondom) het ontstaan, gebruiken, opslaan, wijzigen en uiteindelijk vernietigen van data en informatieproducten. Het beheren van de datalevenscyclus is een onderdeel van datamanagement. Het is niet de bedoeling dit onderwerp hier uit te werken; dit hoofdstuk gaat over de aspecten van de datalevenscyclus van belang voor het voldoen aan de AVG, de BIO en de Archiefwet bij het data gedreven werken met het DAP'R.



Figuur 1 De levencyclus van data volgens DAMA DMBOK

Data- en informatieproducten die wij binnen de gemeente Rotterdam ontwikkelen, vallen onder de regels van de Archiefwet en bijbehorende lagere regelgeving. Deze regels zijn er om:

- Transparant te maken hoe besluitvorming tot stand is gekomen en hoe de overheid heeft gehandeld (bijvoorbeeld voor de WOO);
- Goede dienstverlening en bedrijfsvoering mogelijk te maken;
- Bewijs van het handelen van de overheid te kunnen leveren, bijvoorbeeld bij bezwaar, beroep en geschillen.
- Behoud van informatie voor (historisch) onderzoek.

De Archiefwet, vertaald in de VNG Selectielijst, schrijft bewaartermijnen voor per proces en daar uit voortkomende informatie. Sommige categorieën informatie moeten we blijvend bewaren en binnen twintig jaar naar het Stadsarchief overgebrengen, andere moeten na een bewaartermijn vernietigd worden. Deze bewaartermijnen zijn een wettelijke grondslag om persoonsinformatie in de zin van de AVG verder te mogen
verwerken. De Archiefwettelijke maatregelen zijn op twee manieren ondersteunend aan de AVG:

- Door tijdig, volgens bewaartermijnen, te vernietigen, bewaren we persoonsgegevens niet onnodig lang (dataminimalisatie) en is helder voor alle betrokkenen hoe lang we hun gegevens bewaren.

- Transparantie richting burgers: door de data en documentatie over totstandkoming en werking van informatieproducten goed te bewaren, kunnen we betrokkenen makkelijk en betrouwbaar informeren over wat er met hun data is gebeurd en met welke data en algoritmen de gemeente een besluit heeft genomen.

De reikwijdte van de Archiefwet gaat verder dan de AVG. De regels gelden ook voor niet-persoonsgegevens.

Dit hoofdstuk beschrijft de werkwijze van levenscyclusbeheer *by design.* Maatregelen als functionaliteit in software, vastleggen van metadata en inrichting van het proces nemen we in het ontwerp mee. Hiermee lossen we niet het levenscyclusbeheer van bestaande informatieproducten en hun achterliggende data op. Dit vraagt om een eenmalige aanpak, waarbij we, bij ontbreken van metadata over bewaartermijnen, bestaande data en loggegevens gebruiken. Dit vraagt handwerk, met alle risico's van dien.
De datalevenscyclus (3.1) is verbonden met de levenscyclus van informatieproducten (3.2), omdat het doel en het bedrijfsproces van het informatieproduct in veel gevallen de bewaartermijn van de onderliggende data bepaalt.

3.1 Datalevenscyclus

3.1.1 Ontstaan en bewerken

De meeste gegevens in het DAP'R, zijn afkomstig uit bronsystemen, en bestonden voordat we het op het DAP'R ontsloten. Als nieuwe gegevens ontstaan op het DAP'R, is het een verrijking van gegevens. Als dit een generiek karakter heeft, voegen we de nieuw ontstane data toe aan de opslaglaag, en zijn deze beschikbaar voor hergebruik. In dat geval is het creëren van de gegevens onderdeel van de verwerking, en moeten we de nieuwe gegevens classificeren en toevoegen aan de datacatalogus.
Als de nieuwe data persoonsgegevens zijn, geldt dat we ze alleen creëren (en bewaren) als dat nodig is voor een of meer informatieproducten. Zolang dat het geval is, blijven zij bewaard in de opslaglaag, en passen we bewaartermijnen toe. Deze worden vastgesteld op basis van de VNG-selectielijst.

Data die we uit bronsystemen halen, moeten we bewerken. Data matchen, transformeren, integreren, standaardiseren en anonimiseren we, afhankelijk van het gebruik en autorisaties. Sommige bewerkingen zijn zo tijdrovend, dat we het resultaat moet opslaan zodat we deze 'snel' kunnen leveren. Om te voldoen aan dataminimalisatie doen we dit alleen als dit nodig is voor de gewenste performance. De lineage van deze bewerkingen moet transparant zijn en getoond kunnen worden, zodat gebruikers kunnen inzien hoe de data is ontstaan vanuit de brondata. De hierom opgeslagen data moeten we voorzien van een bewaartermijn en daarna vernietigen we ze. Bij BI is er een variant zonder tussenbewerkingen, namelijk Direct Query, dan is er geen tussentijdse gegevensopslag en wordt direct geput vanuit het Datawarehouse.

3.1.2 Gebruiken

Het gebruik van gegevens vindt – in geval van Business Intelligence en Analytics – plaats door verwerking ervan in de diverse informatieproducten. De meeste privacy risico's doen zich voor wanneer een informatieproduct persoonsgegevens bevat. Daarom toetsen we ieder voorgenomen gebruik (en opslag) vooraf door de Data Usage Board op compliance met onder meer de AVG, de BIO en de Archiefwet. Voor ieder gebruik van gegevens voor een informatieproduct, moet separaat worden beoordeeld of het mag en zo ja, welke maatregelen daarvoor nodig zijn. De proceseigenaar voert een PRA uit en een DPIA als dat nodig is.

Het gebruik van *persoons*gegevens begint met het bepalen van het doel van het informatieproduct en AVG-grondslag. Vervolgens moet de proceseigenaar vaststellen welke persoonsgegevens nodig zijn om dat doel te bereiken (dataminimalisatie). Dit gebeurt door eerst te bepalen welke dataobjecten nodig zijn, en vervolgens per dataobject welke attributen. Alleen *die* objecten en attributen worden vanuit de opslaglaag beschikbaar gesteld voor dat specifieke informatieproduct. Dataminimalisatie is ook het beoordelen of we:

- Gegevens uitsluitend geaggregeerd (geanonimiseerd indien daarna nog nodig); of
- Gegevens gepseudonimiseerd of (deels) gemaskeerd tonen aan de gebruiker van het informatieproduct. Anonimiseren of pseudonimiseren van *hergebruikte* gegevens is niet strijdig met de Archiefwet, omdat het nog steeds mogelijk is te reconstrueren hoe besluiten met het informatieproduct genomen zijn. Dit geldt niet voor informatie die we creëren in het oorspronkelijk bronproces. Bijvoorbeeld het verstrekken van een vergunning of uitkering. Daar gaat het vaak om een individueel persoon, die herkenbaar moet zijn voor de behandeling van de zaak en latere reconstructie.

Vervolgens stelt de proceseigenaar[43] vast hoe lang de gegevens bewaard moeten blijven voor het doel. Dit is onderdeel van het gesprek in de Data Usage Board (DUB) en vindt plaats in de ontwerpfase (*by design*). Zie hiervoor paragraaf 2.2.2. De cluster records manager[44] neemt hieraan deel. Deze stelt met de proceseigenaar vast welk IBP-proces[45] ondersteund wordt door het informatieproduct, of maakt een nieuw IBP-proces aan. Ieder IBP-proces is gekoppeld aan een categorie en vernietigingstermijn van de landelijke VNG Selectielijst. Zie verder onder 3.1.5 ‘Vernietigen’. Het is ook nodig in deze fase vast te stellen hoe ver je wilt terugkijken. Dan kun je in de software, of procesmatig de bewaartermijn starten. En tot slot welke specifieke toegangsrechten en overige beveiligingsmaatregelen we moeten toepassen. Een best practice is dat een informatieproduct de datum vermeldt van de onderliggende dataset, zodat de eindgebruiker weet hoe recent de gebruikte gegevens zijn.

Welke gegevens precies worden aangeleverd voor een specifiek informatieproduct en wat daar de beschikbaarheids- en kwaliteitscriteria voor zijn, leggen we vast in een gegevensleveringsovereenkomst tussen bronhouder en OBI, en de (proces)eigenaar van het informatieproduct. Bij data van een externe partij stel je een Data Transfer Agreement (DTA) op. Zie hiervoor hoofdstuk 4 over Datamanagement.

3.1.3 Opslaan

We slaan gegevens op in de opslaglaag van het DAP’R.
Het kan zijn dat de opslag in verschillende databases en verschillende fysieke locaties plaatsvindt, op eigen dataservers, of bij een externe hostingpartij. Logisch gezien is er één opslaglaag. Welke gegevens zijn opgenomen in de opslaglaag, en wat hun betekenis en eigenschappen zijn, leggen we vast in de datacatalogus.

De ‘opslaglaag’, is alleen voor het bewaren van gegevens, en het opbouwen van historie. Voordat we gegevens daadwerkelijk verwerken voor specifieke informatieproducten (zie hierna), laden we ze eerst in een aparte omgeving. Zo minimaliseren we het aantal medewerkers dat toegang heeft tot de opslaglaag. Zie hiervoor het hoofdstuk over Security (H4).

[43] of namens hem de product owner van het informatieproduct
[44] Contact Procesmanagement Beheer Informatiehuishouding - RIO (rotterdam.nl)
[45] Het Informatiebeheerplan (IBP) bevalt alle processen van de gemeente met bijbehorende informatieneerslag. Deze hebben een zogeheten P-nummer. Zie: Beleid, wetgeving en Informatiebeheerplan - RIO (rotterdam.nl)

Het beginsel van dataminimalisatie betekent dat de gemeente alleen gegevens bewaart in de opslaglaag die daadwerkelijk nodig zijn voor één of meer informatieproducten. Met datalineage bepalen we welke dataobjecten we opslaan door bij te houden welke dataobjecten nodig zijn voor welke informatieproducten.

Het exporteren van gegevens uit de opslaglaag en opslaan in excelsheets of PDF's mag alleen als dit niet strijdig is met de privacywetgeving, zoals vastgesteld in de DUB. Als dit nodig is voor het opleveren van een product, moeten we deze documenten in een beheerde omgeving opslaan, bij voorkeur DIVA. Zo waarborgen we de bewaartermijnen.

3.1.4 Wijzigen

Het wijzigen van de op het DAP'R aanwezige gegevens vindt in de bronsystemen plaats. De gewijzigde gegevens komen vervolgens via het ontsluitingsproces in de opslaglaag terecht, waarbij de verouderde/gecorrigeerde gegevens als historie bewaard blijven tot hun bewaartermijn verstrijkt. Het recht op correctie heeft dus geen rechtstreekse impact op het DAP'R, en hoeven we geen maatregelen te treffen op het DAP'R. Het is van belang dat alleen een zeer beperkte groep ontwikkelaars toegang heeft tot het wijzigen van de business rules die de de bron naar de opslaglaag vertalen in het DAP'R.

3.1.5 Vernietigen

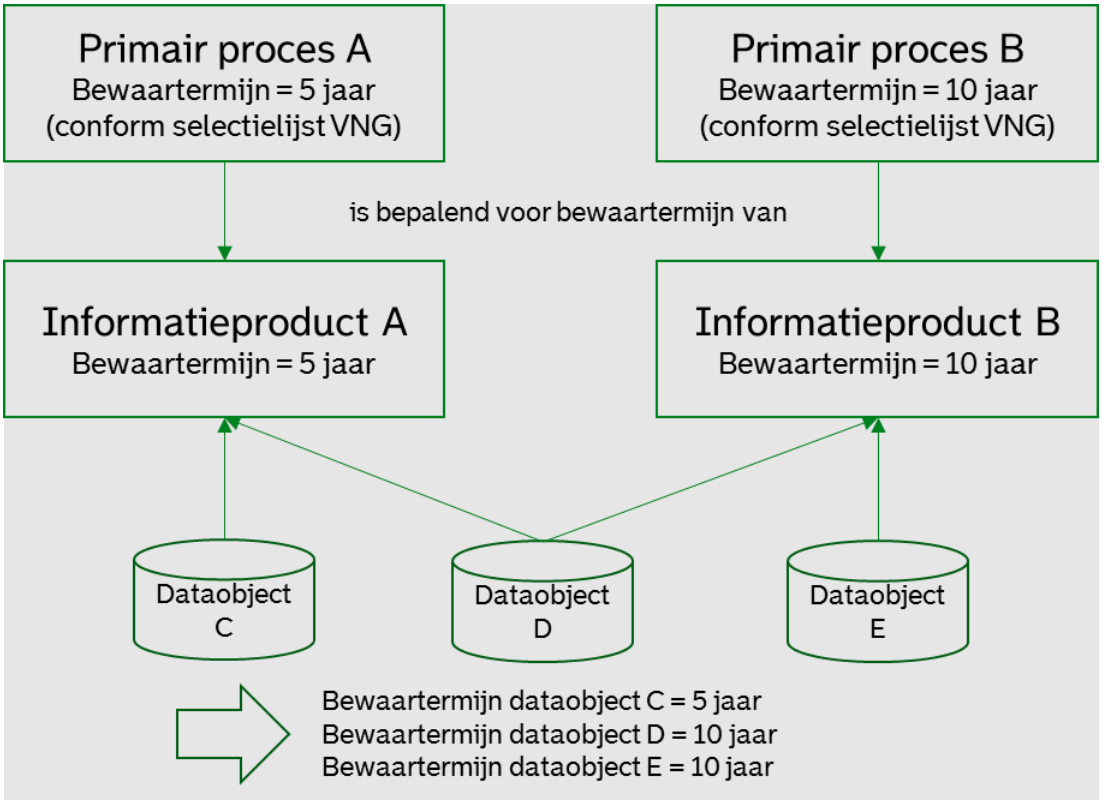
Op grond van de Archiefwettelijke VNG Selectielijst voor gemeenten[46] moet de gemeente per proces bepalen hoelang de daarin verwerkte gegevens bewaard moeten blijven. Zo moet de proceseigenaar ook voor ieder informatieproduct vaststellen wat de bewaartermijn is. Omdat een informatieproduct altijd een bedrijfsproces ondersteunt, is de bewaartermijn voor het informatieproduct gelijk aan de bewaartermijn van dat bedrijfsproces. Als een informatieproduct meerdere bedrijfsprocessen ondersteunt, geldt de langste termijn. Het informatieproduct dat het proces met kortste bewaartermijn ondersteunt, heeft dan geen toegang meer.

Deze bewaartermijn geldt voor:

- De definitie van het informatieproduct, oftewel de regels aan de hand waarvan de gegevens worden verwerkt en getoond aan de gebruiker;
- Een eventueel 'hardcopy' rapport van het informatieproduct;
- De data die in het informatieproduct worden verwerkt

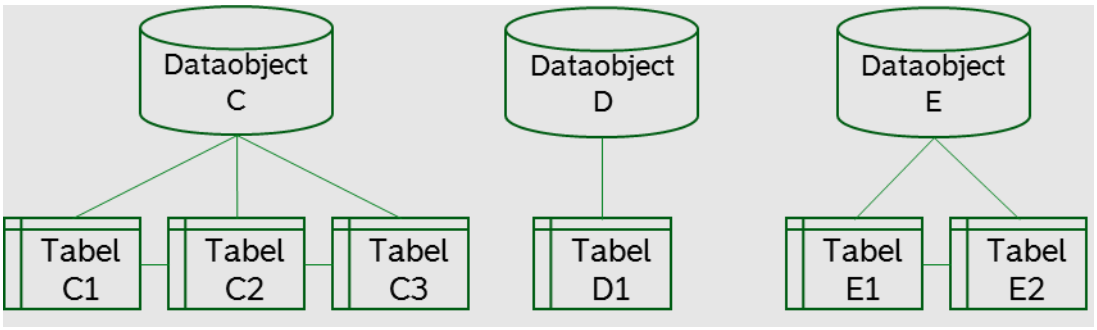
NB: de bewaartermijn van de data wordt dus *niet* afgeleid van de bron van de data.
De definitie kan simpelweg worden gearchiveerd in de daarvoor beschikbaar gestelde infrastructuur (bij voorkeur een register van definities), terwijl de data wordt bewaard in de opslaglaag van het DAP'R. Daartoe moet eerst worden vastgesteld welke dataobjecten precies nodig zijn voor dat informatieproduct, om vervolgens per dataobject de bewaartermijn te bepalen:

[46] Selectielijst 2020 vastgesteld | VNG



Als een dataobject in meerdere informatieproducten wordt verwerkt – zoals bij dataobject D het geval is – geldt de langste termijn.

Een dataobject is op zijn beurt opgebouwd uit een of meerdere tabellen. Als op bovenstaande manier per dataobject de bewaartermijn is bepaald, moet die vervolgens worden toegepast op alle onderliggende tabellen:



Het toepassen van bewaartermijnen op de onderliggende tabellen, gebeurt door voor ieder record binnen een tabel te bepalen wanneer de bewaartermijn begint. Na het verstrijken van deze termijn, wordt het record definitief verwijderd uit de opslaglaag.
Wanneer de bewaartermijn begint, wordt bepaald aan de hand van business rules. Voor ieder informatieproduct wordt per dataobject de business rule bepaald. Omdat een dataobject in meerdere informatieproducten verwerkt kan worden (zoals dataobject D in het voorbeeld hierboven), leidt dit mogelijk tot meerdere business rules voor ieder dataobject in de

opslaglaag. In dat geval wordt de business rule toegepast die tot de langste bewaartermijn leidt.

In sommige gevallen is een dataobject niet opgebouwd uit tabellen, maar uit andere soorten bestanden. Het gaat dan bijvoorbeeld om afbeeldingen en documenten. Dit soort bestanden bevatten geen records zoals tabellen die hebben. Bewaartermijnen kunnen dan ook niet op recordniveau worden bepaald, maar zullen in plaats daarvan op bestands-niveau worden toegepast.

Naast dat voor de in dataobjecten aanwezige gegevens bewaartermijnen gelden, geldt dat ook voor de dataobjecten. Zoals in paragraaf gezegd, bevat de opslaglaag van het DAP'R alleen dataobjecten nodig voor een of meer informatieproducten. Dat betekent dat, als een informatieproduct komt te vervallen, moet worden bekeken of de daarin gebruikte dataobjecten nog nodig zijn voor andere informatieproducten. Als dat niet het geval is, dan start de bewaartermijn voor het dataobject als geheel:

- Het ontsluiten van brongegevens voor dit dataobject wordt gestopt;
- Dan gaat de bewaartermijn in;
- Na afloop van de bewaartermijn wordt het gehele dataobject, inclusief alle onderliggende tabellen/bestanden, verwijderd.[47]
- Eventuele ruwe gegevens, tijdelijk ingeladen gegevens in analysetools, de inhoud van de datamart worden als dubbele gegevens beschouwd en kunnen meteen na het afsluiten van het informatieproduct worden vernietigd. De laatste twee worden periodiek ververst, waarbij de oude (kopie)gegevens worden overschreven.
- Tijdens de levensduur van het informatieproduct moeten periodiek data die buiten de scope van de historie vallen worden opgeschoond/op bewaartermijn afgesteld, handmatig, of softwarematig.

De boven beschreven werkwijze is gebaseerd op de VNG Selectielijst 2020 en de Handreiking[48]. Het is raadzaam om een discussie op landelijk/VNG niveau te starten over de vraag tot op welk detailniveau de data van een informatieproduct bewaard moeten blijven gedurende de periode dat het informatieproduct in gebruik is, plus de bewaartermijn. Dit vanuit oogpunt van dataminimalisatie op grond van de AVG. In 2023 zal de huidige selectielijst geëvalueerd worden en zal dit punt vanuit Rotterdam ingebracht worden.

Daarbij moet worden afgewogen of het bewaren van *alle* data die ten grondslag liggen aan een informatieproduct niet in tegenspraak is met het principe van dataminimalisatie uit de AVG. Dataminimalisatie houdt in dat bij het verzamelen en verwerken van persoonsgegevens niet meer gegevens mogen worden gebruikt dan nodig is om het doel waarvoor ze gebruikt zullen worden te bereiken. Het langdurig bewaren van grote hoeveelheden data met persoonsgegevens leidt echter tot privacyrisico's. Door beveiligingsincidenten kunnen data bijvoorbeeld in handen komen van of zichtbaar worden voor onbevoegden. Hier gaat het echter om het bewaren van gegevens die al getoetst zijn in het licht van dataminimalisatie. Zij zouden anders niet voor het informatieproduct gebruikt mogen worden. In ieder geval geldt: als er wettelijke termijnen zijn, dan moet de organisatie die in acht nemen. Dit in het belang van de reconstrueerbaarheid van besluitvorming. Om die risico's zo klein mogelijk te houden worden de data in een zo vroeg mogelijk stadium gepseudonimiseerd en waar mogelijk

[47] Als op grond van de Archiefwet de betreffende gegevens niet voor vernietiging in aanmerking komen, dan worden het dataobject direct verwijderd van het DAP'R, en de onderliggende gegevens ondergebracht in de archiefbewaarplaats van de gemeente.
[48] handreiking-gebruik-selectielijst_20200506.pdf (vng.nl) par, 5.17

geanonimiseerd. Naast de beveiligingsmaatregelen die in H4 worden besproken worden privacyrisico's op die manier zo klein mogelijk gehouden..

3.2 Levenscyclus van informatieproducten

3.2.1 Ontstaan

Informatieproducten worden ontwikkeld en getest door de BI-teams van de afdeling OBI, en door BI-specialisten binnen de clusters (self-service BI). Hierbij kan het nodig zijn met persoonsgegevens te werken. Als dat het geval is, is er sprake van een verwerking van persoonsgegevens, en is de AVG van toepassing. Dat betekent dat de gemeente het ontwikkelen en testen van informatieproducten moet voorzien van de benodigde waarborgen, en dat de eigenaar van het ontwikkel- en testproces daarvoor verantwoordelijk is. Het proces waar het hier om gaat, is de way of working voor data- en analyseprojecten – zie ook de inleiding van hoofdstuk 0. De proceseigenaar is het hoofd van de afdeling OBI.

Om bij het ontwikkelen en testen van informatieproducten privacyrisico's te beperken, nemen we de volgende maatregelen:

- We gebruiken als regel gepseudonimiseerde of geanonimiseerde persoonsgegevens, waarbij uitzonderingen getoetst moeten worden door de DUB.
- Bijzondere gegevens (gegevens over gezondheid, religie, etniciteit, ed.) worden geanonimiseerd. Waar mogelijk vooraf, en altijd na afronding van het informatieproduct. Ook hier worden uitzonderingen getoetst in de DUB.
- We bewaren de gegevens in een aparte projectomgeving; alleen de medewerkers die zijn betrokken bij de ontwikkel- en testwerkzaamheden voor dat specifieke informatieproduct hebben toegang tot deze projectomgeving.
- Na afloop van het project zorgt de projectleider ervoor dat de gegevens uit de projectomgeving voorzien worden van een bewaartermijn, waar mogelijk direct gepseudonimiseerd of geanonimiseerd worden en na afloop daarvan worden verwijderd. Projectdocumentatie wordt gearchiveerd in DIVA.
- Regelmatig controleert de functioneel beheerder welke projectomgevingen bestaan, en of zij nog in gebruik zijn. Zo niet, dan zorgt de eindverantwoordelijke voor de ontwikkel- en testwerkzaamheden ervoor dat de niet meer in gebruik zijnde omgevingen worden verwijderd.
- De bewaartermijn voor data in ontwikkel- en testomgevingen is 5 jaar (cat. 19.1 VNG Selectielijst).

Als het informatieproduct klaar is om in productie/beheer te nemen, werken we de datalineage en de benodigde registers bij. Dit is een cyclisch proces dat zich bij iedere wijziging herhaalt. Afhankelijk van het informatieproduct kan het gaan om het register informatieproducten, het verwerkingsregister en het algoritmeregister. In die fase is ook de het IBP-proces vastgesteld en daarmee de bewaartermijn, de technische en procesmatige maatregelen voor inregelen en toepassen van de bewaartermijn zijn getroffen en eventuele restrisico's zijn geaccordeerd. De afspraken worden na advies van de Data Usage Board vastgelegd in een GLO.

3.2.2 Gebruiken

Waarvoor en door wie een informatieproduct precies wordt gebruikt, is aan de proceseigenaar/afnemer om te bepalen. In zijn algemeenheid is daar slechts over te zeggen dat het gebruik in lijn moet zijn met het vooraf vastgestelde doel van het informatieproduct. De proceseigenaar informeert de gebruikers die toegang hebben over dit doel, en over het feit dat zij het informatieproduct niet voor andere doelen mogen gebruiken.

De proceseigenaar bepaalt ook met wie *buiten de gemeente* het informatieproduct wordt gedeeld. Ook daar is het beginsel van doelbinding op van toepassing: het extern delen moet noodzakelijk zijn om het doel van het informatieproduct te realiseren.

3.2.3 Opslaan

Nadat het informatieproduct is samengesteld, is het technisch mogelijk om het op te slaan buiten de applicatie waarin het informatieproduct is samengesteld, bijvoorbeeld in pdf-formaat. Alhoewel het wenselijk kan zijn dat gebruikers dat kunnen, kleven daar ook privacy- en andere compliancerisico's aan, voor zover het informatieproduct persoonsgegevens bevat. Die nadelen zijn:

- Het is lastiger om te borgen dat het informatieproduct niet voor andere doelen wordt gebruikt, omdat er geen zicht meer is op wie op welk moment toegang had tot de gegevens.
- Het is lastiger om aan het beginsel van opslagbeperking en de Archiefwet te voldoen, omdat er geen zicht is op waar het informatieproduct wordt opgeslagen.
- Het is lastiger om gevolg te geven aan de rechten van betrokkenen – in het bijzonder het recht op verwijdering – omdat er geen zicht is op waar het informatieproduct wordt opgeslagen.
- Het is lastiger om te borgen dat blijvend wordt voldaan aan de BIO als er geen zicht is op waar het informatieproduct wordt opgeslagen, en wie er op die plaats toegang hebben tot de daarin besloten gegevens.

Het aan de proceseigenaar gebruiksverwerking om te besluiten of het opslaan door gebruikers is toegelaten. Voor informatieproducten die persoonsgegevens bevatten dient deze keuze expliciet te worden gemaakt en onderbouwd worden gedocumenteerd. De Data Usage Board zal hierover worden geïnformeerd, zodat de leden daar advies over uit kunnen brengen aan de (toekomstig) proceseigenaar.

3.2.4 Wijzigen

Net als de totstandkoming van nieuwe informatieproducten, loopt het wijzigen ervan volgens de gebruikelijke change- en releasemanagementprocessen van OBI en de DACC's. Voor grote wijzigingen kan de Way of Working voor data- & analyseprojecten worden gebruikt, waarin ook het DUB-advies, addendum op het GLO en het uitvoeren van een eventuele DPIA als belangrijke privacy waarborgen deel van uitmaken. Mocht de wijziging daar aanleiding toe geven, dan dienen (waar van toepassing) het register informatieproducten, de datalineage, het verwerkingsregister en het algoritmeregister te worden bijgewerkt.

3.2.5 Verwijderen

Ook informatieproducten komen aan het einde van hun levenscyclus. Niet alleen om systeemcapaciteit te sparen, maar ook vanuit compliance perspectief is het nodig om het informatieproduct te verwijderen, of over te brengen naar het Stadsarchief (wanneer het blijvend bewaard moet worden).[49] Om aan de Archiefwet te voldoen, moet de definitie van het informatieproduct worden gearchiveerd in DIVA volgens de geldende bewaartermijn. De data die nodig zijn om het informatieproduct later nogmaals te kunnen samenstellen, worden bewaard in de opslaglaag van het DAP'R, totdat zij conform de bewaartermijn vernietigd moeten worden, of overgebracht naar het Stadsarchief.

[49] Zo is het samenstellen van een informatieproduct dat niet meer in gebruik is, strijdig met de AVG, omdat er onnodig persoonsgegevens worden verwerkt.

Om te signaleren welke informatieproducten voor verwijdering in aanmerking komen, moet er, procesmatig en/of geautomatiseerd, een overzicht bijgehouden worden, met een instelbaar signaleringsmechanisme wanneer informatieproducten langer dan bijvoorbeeld een jaar niet gebruikt zijn. De ‘niet gebruik’-meldingen worden gedeeld met de betreffende proceseigenaars van de daarop vermelde informatieproducten, zodat zij op basis van het overzicht kunnen aangeven welke informatieproducten kunnen komen te vervallen.

Zodra een eigenaar aangeeft dat een informatieproduct kan vervallen, wordt het op de bewaartermijn afgesteld, zoals hierboven beschreven. Het verladen van gegevens vanuit de opslaglaag voor het betreffende informatieproduct stopt, en er wordt beoordeeld of de onderliggende dataobjecten ook voor archivering/verwijdering in aanmerking komen. Tot slot dienen (waar van toepassing) het register informatieproducten, het GLO-register, de Gegevenscatalogus, de datalineage, het verwerkingsregister en het algoritmeregister te worden bijgewerkt. Er is functionaliteit nodig om het vervallen van bewaartermijnen te signaleren, te controleren of de data nog door andere informatieproducten wordt gebruikt en zo niet, de vernietiging, of overbrenging te effectueren.

4 Security

Dit hoofdstuk beschrijft op hoofdlijnen welke keuzes zijn gemaakt met betrekking tot de inrichting van informatiebeveiliging binnen het DAP'R. Het gaat daarbij specifiek om de volgende applicaties:

- het concern Datawarehouse
- het Datake
- IBM Cognos
- Microsoft Power BI
- SAS Viya
- Azure Databricks, Azure Synapse en Azure Machine Learning

Al deze applicaties zijn geclassificeerd op Basisbeveiligingsniveau (BBN) 2+. Uitgangspunt voor de hierna volgende beschrijving is dan ook dat alle controls[50] behorend bij dit BBN niveau zijn geïmplementeerd, of nog zullen worden geïmplementeerd, om volledig aan de Baseline Informatiebeveiliging Overheid BIO) te voldoen. Voor een meer gedetailleerde beschrijving van geïmplementeerde en te implementeren controls wordt verwezen naar de zelfassessments behorende bij deze applicaties.

4.1 Prioritering maatregelen

Er is een risicoanalyse uitgevoerd door de DISO BCO, welke een aantal hoofdrisico's heeft gedefinieerd. Dit zijn de volgende risico's:

- Toegang tot data
- Misbruik van data
- Leveranciersmanagement
- Assurance dienstverlening OBI
- Gebruik Shadow IT

Als gevolg van deze risico's zijn er een aantal hoofdmaatregelen geadviseerd:

- Adequate toegangsbeveiliging
- Loggen van gebruikersactiviteiten
- Afspraken met externe leveranciers
- Programmatuurgerichte maatregelen
- Mensgerichte maatregelen

Het is uiteindelijk van belang dat alle BIO controls worden geïmplementeerd, maar hoofdzakelijk dient er een focus te liggen op het vijftal geadviseerde hoofdmaatregelen. De controls zullen zoveel mogelijk worden geïmplementeerd met relevante risico's in het achterhoofd.

[50] In AVG-termen: technische en organisatorische maatregelen

4.2 Toegangsbeveiliging

Een van de grootste risico's is ongeautoriseerde toegang tot data. Dit kan zowel van buitenaf als binnenaf gebeuren. Om ongeautoriseerde toegang door medewerkers te voorkomen is het de bedoeling dat toegangsbeveiliging zo goed mogelijk is ingericht.

Een aantal maatregelen dient getroffen te worden.

4.2.1 Reguliere accounts

- Bepaal waar en op welke wijze functiescheiding wordt toegepast, zodat gebruikers alleen informatie kunnen inzien en verwerken die ze nodig hebben voor het uitoefenen van hun taak. Dit is het principe van least privilege.
  - Pas functiescheiding toe op medewerkers die gegevens inladen en medewerkers die gegevens gebruiken. Dit zijn verschillende belangen die zoveel mogelijk gescheiden dienen te blijven.
- Het verlenen van toegangsrechten dan wel functieprofielen binnen de tools en opslagfaciliteiten wordt uitsluitend verleend na autorisatie door een bevoegde functionaris die staat genoteerd in een mandaatregister.
  - Zorg dat het toewijzen van rechten via een traceerbaar proces verloopt, bijvoorbeeld via SARA. Zorg ook dat er met profielen wordt gewerkt, vermijd het kopiëren van rechten van andere gebruikers naar een nieuwe gebruiker.
  - Het verlenen van toegangsrechten gaat met behulp van een autorisatiematrix. Voor ieder proces/applicatie dient er een autorisatiematrix te zijn. Deze autorisatiematrix bevat minimaal welke rollen er aanwezig zijn en welke rechten deze rollen hebben. Er wordt gewerkt met rollen/functies, er vindt geen toegang plaats zonder toewijzing van een rol.
- Er is een formele registratie- en afmeldprocedure voor het beheren van gebruikersidentificaties.
  - Handelingen en afwegingen in het proces dienen opgeschreven te zijn.
- Toegangsrechten van gebruikers behoren bij beëindiging van dienstverband te worden verwijderd en bij wijzigingen behoren ze te worden aangepast.
- Alle uitgegeven toegangsrechten worden minimaal eenmaal per halfjaar beoordeeld. De eigenaren van de tools en opslagfaciliteiten horen deze beoordeling uit te (laten) voeren.
  - Functioneel Beheer ondersteunt in dit proces door het te initiëren, voortgang te bewaken etc. Daadwerkelijke controle dient plaats te vinden door verantwoordelijk managers.

Toegangsbeveiliging is veelal een menselijk proces, er kunnen dus fouten insluipen. Het is daarom aan te raden zoveel mogelijk van de toegangsbeveiliging te automatiseren. Denk hierbij bijvoorbeeld aan het automatisch verlopen van toegangsrechten.

4.2.2 Beheeraccounts

Maatregelen:

- De uitgegeven speciale bevoegdheden worden minimaal ieder kwartaal beoordeeld.
- Alleen bevoegd personeel heeft toegang tot systeemhulpmiddelen, zoals beheertools.
  - Zorg dat aantallen beheerders zoveel mogelijk beperkt zijn, maar wel met oog voor een praktisch werkbare situatie. Het is niet aan te raden slechts één beheerder aan te stellen voor een applicatie.

4.3 Loggen gebruikersactiviteiten

Maatregelen:

- De logregels bevatten minimaal de gebeurtenis; de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon; het gebruikte apparaat; het resultaat van de handeling; een datum en tijdstip van de gebeurtenis. Log ook het gebruik van systeemhulpmiddelen, zoals beheertools.
- Bepaal de bewaarperiode van de logging. Binnen deze periode is de beschikbaarheid van de loginformatie gewaarborgd.
  - Bij logging van systeemhulpmiddelen betreft dit minimaal een halfjaar.
  - De gelogde informatie omtrent een (vermoedelijk) beveiligingsincident wordt minimaal drie jaar bewaard.
- Zorg dat toegang tot logging beperkt is, en waar mogelijk onmogelijk te manipuleren is. Indien logging wordt getransporteerd naar een andere applicatie, zorg dat dit zo veilig mogelijk gebeurt.

4.4 Afspraken met externe leveranciers

Maatregelen:

- Zorg ervoor dat de leveranciers voldoen aan het programma van eisen (PvE) van de gemeente Rotterdam. De eisen rondom informatiebeveiliging uit het PvE zijn in bijlage B te vinden.
- Blijf periodiek monitoren of leveranciers blijvend aan de eisen voldoen. Dit kan bijvoorbeeld door het beoordelen van verklaringen, rapportages en andere teksten.
- Een ISAE3402 verklaring of SOC2 verklaringen hebben de voorkeur boven certificeringen zoals ISO27001.

4.5 Programmatuurgerichte maatregelen

Maatregelen:

- Toegang gebeurt altijd op basis van tweefactor-/ multifactorauthenticatie. Dit geldt dus voor alle toegang, waaronder gebruikers- beheerders- service- en machine-to-machine accounts.
- Initiële/ geresette wachtwoorden hebben een maximale geldigheidsduur van een werkdag en moeten bij het eerste gebruik worden gewijzigd.
- Wachtwoorden voldoen aan complexiteitseisen. Ze hebben minimaal een wachtwoordlengte van 10 posities en bestaan uit minstens een getal, letter en teken (@#! etc.)

4.6 Governance

Governance van informatiebeveiliging bij DAP’R volgt het algemene informatiebeveiligingsbeleid van de gemeente Rotterdam.