Checklist Privacy Datagedreven Werken

Inleiding

Gemeenten beschikken als gevolg van hun taken over veel (digitale) gegevens. Vaak zijn deze gegevens ook persoonsgegevens. Gemeenten willen deze gegevens, op een slimmere gebruiken om hun primaire taken, beter uit te kunnen voeren. Dit slimmere gebruik bestaat onder andere uit:

- Het maken van rapportages om zo het management te kunnen informeren (trendanalyses);
- Het maken van beleidskeuzes om zo o.a. inwoners en bedrijven zo goed mogelijk van dienst te kunnen zijn. Voorbeelden hiervan zijn:
- Stadsbeheer: o.a. het verbeteren van het parkeerbeheer;
- Stadsontwikkeling: schone stad, strategische stedelijke planning, maatschappelijk vastgoed;
- Dienstverlening: klantsignaalmanagement, grip op werkvoorraden;
- Werk & inkomen: integraal klantbeeld, voorspellen in- en doorstroom van uitkeringsgerechtigden
- Maatschappelijke ontwikkeling: analyse wijkprogrammering, dashboard leerlingenstroom
- HR-analytics, personeelsbeleid, prognoses.

Dit zijn allemaal voorbeelden van datagedreven werken. Datagedreven werken kan op allerlei manieren, zoals met behulp van Excel, via SharePoint, of met behulp van een uitdraai uit een geautomatiseerd systeem.

Hoe zorg je er als privacy adviseur voor dat datagedreven werken met persoonsgegevens zo gebeurt dat de risico's voor de inwoner tot een aanvaardbaar minimum worden beperkt? In deze checklist zal de gemeentelijke werkgroep Datagedreven werken dit onderwerp vanuit het oogpunt van gegevens-bescherming gemeenten een kader meegeven voor datagedreven werken.

Deze checklist is voor de gemeentelijke privacy officer en functionaris voor de gegevensbescherming.

Wat is datagedreven werken?

Datagedreven werken is het realiseren van maatschappelijke waarde(n) door verantwoord datagebruik.[1] Dit met respect voor ethische en juridische kaders, in lijn met de publieke waarden die voorop zijn gezet. Dit betekent dat het eigenaarschap van datagedreven werken bij mensen ligt die bestuurlijke keuzes maken of deze controleren, en niet bij de ontwikkelaars.
Het gaat het hierbij om dat data worden gebruikt om betere dienstverlening te kunnen bieden, betere beleidsbeslissingen te kunnen nemen en gemakkelijker en sneller in te kunnen spelen op veranderende omstandigheden en om efficiëntere en effectievere bedrijfsvoering te kunnen realiseren. Datagedreven werken is op zich niet nieuw, maar door de toegenomen technische mogelijkheden van datagebruik en data-analyse is de wens ontstaan om van deze mogelijkheden gebruik te maken.

Zoals hiervoor al opgemerkt werken alle gemeenten al in meer of mindere mate datagedreven. Iedere gemeente kiest daarbij voor een eigen lokale oplossing. Dat kan door middel van een datapakhuis, het maken van een uitdraai in een geautomatiseerd systeem voor uitkeringen, excellijstjes, etc. Daarvoor zijn veel tools voorhanden.

Er is veel onduidelijkheid over de rechtmatigheid van datagedreven werken. Een zorgvuldige verwerking van de gebruikte persoonsgegevens en een goede bescherming van de gebruikte gegevens essentieel.

De werkgroep datagedreven werken, bestaande uit 10 deelnemers uit verschillende gemeenten en de VNG, heeft een checklist gegevensbescherming opgesteld die alle gemeenten kunnen gebruiken wanneer zij datagedreven (willen) werken. De werkgroep realiseert zich dat zij met deze checklist geen sluitende oplossing aandraagt. De in deze Checklist aangereikte werkwijze moet dan ook gezien worden als een voorgestelde 'best practice' op basis van gezamenlijk inzicht van de 10 betrokken gemeenten. Bij het (her)inrichten van de bestaande werkprocessen beveelt de werkgroep aan om de in deze Handreiking geschetste werkwijze over te nemen. Deze best practices bieden namelijk een relatief eenvoudige en beproefde manier om aan de bestaande wetgeving te voldoen.
Daarbij verwijst de werkgroep naar een aantal documenten, zoals die door de deelnemende gemeenten worden gebruikt. De werkgroep doet echter geen uitspraak over de juistheid van de documenten. Deze worden alleen als voorbeeld aangeboden.

Deze checklist is werk in uitvoering. Dat betekent dat de werkgroep de checklist kan aanpassen en/of aanvullen als gemeenten daar behoefte aan hebben. Voor tips/verbeterpunten: privacy@vng.nl

Datagedreven werken of vraagarticulatie?

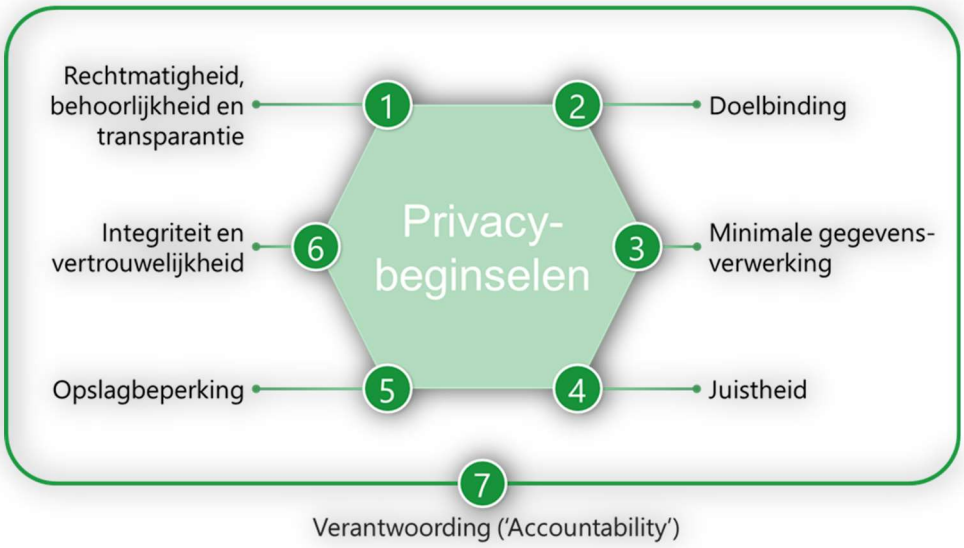
In de praktijk blijkt dat een maatschappelijke vraag vaak gesteld wordt vanuit een data- of een interactieperspectief ("Ik wil graag een dashboard/ kaart/ etc."). Vanuit gedrag is het goed verklaarbaar: je wilt een (snelle) oplossing. Bovendien denken mensen makkelijker visueel en het is nu eenmaal eenvoudiger een voorstelling te maken van het eindproduct en dit onder woorden te brengen dan te bedenken waarom je dit eindproduct maakt. De eerste stap in het proces van vraagarticulatie is dan ook om de maatschappelijke opgave uit het abstracte te halen en scherp en concreet te maken. Zo wordt de opgave het uitgangspunt van het vraagstuk, niet de data of de presentatievorm. (Vervolgens gaan we de fases in waarin de data en de keuze voor een oplossing verder worden verkend aan de hand van het bestaande landschap en (in ontwikkeling zijnde) kaders. In fase 3 wordt de keuze voor een richting gemaakt en onderbouwd. In fase 4 worden de vraag naar data en de vorm waarin deze gepresenteerd gaat worden tegelijk opgepakt in een ontwerpproces. Deze oplossing wordt getest en geëvalueerd in fase 5.) Het eindresultaat is dan niet een eindproduct, maar een besluit wat je in een proces hebt besproken en wilt laten onderzoeken en wilt laten maken. Dit voorkomt dat producten te snel ontwikkeld worden zonder de bruikbaarheid goed te testen. Vraagarticulatie is nog weliswaar nog niet een gebruikelijke benadering, maar het is toch goed gebruikers van deze checklist daar op te wijzen.

Juridisch kader

Het juridisch kader van datagedreven werken is in eerste instantie de desbetreffende materiewet (bv. Jeugdwet, Wet Ruimtelijke Ordening, Participatiewet). Daarnaast zijn de algemeen beginselen van de AVG van toepassing. Dat geldt temeer als de desbetreffende materie wet geen of weinig aanknopingspunten bevat over het (her)gebruik van persoonsgegevens voor datagedreven werken.

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 datagedreven werken. 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 datagedreven werken.

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[2].

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

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[3] kent zes grondslagen op grond waarvan persoonsgegevens mogen worden verwerkt. Daarvan is er eigenlijk maar één van toepassing voor de gemeente, te weten:
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 die aan de verwerkingsverantwoordelijke is opgedragen. De eis daarbij is dat die taak waarvoor de gemeente gegevens verwerkt, een basis[4] moet hebben in een nationale wet[5].
Als een gemeente een enquête uitvoert, zou de grondslag eventueel ook toestemming van de betrokkene kunnen zijn. Het moet dan wel helder zijn dat de gemeente niet optreedt als overheidsorgaan en voor de betrokken moet hel volstrekt helder zijn dat als hij niet meewerkt aan de enquête, dat geen enkel gevolg heeft in wat voor opzicht dan ook.

Doelbinding en grondslagen

Bovengenoemde uitgangspunten over doelbinding en grondslagen gelden altijd dus ook voor te ontwikkelen informatieproducten[6]. Het proces van aanvraag tot oplevering van een informatieproduct wordt daarbij als één onlosmakelijk proces van verwerking beschouwd. Dit geldt ook als er in dat proces gebruik gemaakt wordt van algoritmen.

Het informatieproduct kan[7]:

1. Hetzelfde doel en dezelfde grondslag hebben 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 die in het informatieproduct worden gebruikt, komen uit hetzelfde bronsysteem.

2. Een ander, maar verenigbaar, doel hebben als die op grond waarvan de gegevens oorspronkelijk zijn verzameld. Er is dan geen nieuwe grondslag nodig[8].
   Bij deze categorie informatieproducten gaat het uitsluitend om het doen van 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.[9] Dit wordt ook wel de “verdere verwerking van persoons-gegevens” 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.

3. Een ander en onverenigbaar doeleinde dan die waarvoor de persoonsgegevens oorspronkelijk zijn verzameld, mag enkel worden toegestaan als er een nieuwe geldige grondslag en doeleinde zijn.

Checklist Privacy Datagedreven Werken

Vragen die een privacy officer kan stellen/tips voor de privacy officer als deze wordt benaderd met de vraag of de gemeente voor een bepaald project datagedreven kan werken.

a. Richt ergens binnen de gemeente een centraal loket in voor de multidisciplinaire beoordeling van alle verzoeken rond gegevensleveringen.
b. Zorg dat een team (in ieder geval bestaand uit een PO/FG/CISO/Informatiebeheerder) de aanvraag checkt op gegevensbescherming, informatiebeveiliging, ethiek/haalbaarheid.
c. Vragen die moeten worden beantwoord:
   - Wat is het doel achter de vraag? Wat is de reden om deze vraag te stellen? Wat wil je bereiken?
   - Waarom voldoet de huidige situatie niet?
   - Is het noodzakelijk om voor dit verzoek persoonsgegevens te verwerken?
   - Nee? Dan is er geen belemmering t.a.v. de gegevensbescherming.
   - Ja? Is er een formele opdrachtgever van het verzoek (Dit moet een vakafdeling zijn!)? Gaat de opdrachtgever ook akkoord met deze vraag? Nee?
   - Zoek eerst een formele opdrachtgever.
   - Ja?
   - Gaat de opdrachtgever akkoord met de onderzoeksvraag?
   - Nee? Helaas, begin opnieuw.
   - Ja?
   - Is de onderzoeksvraag helder?
   - Nee?
   - Ga eerst de onderzoeksvraag helder krijgen.
   - Is de onderzoeksvraag wel helder, ga dan verder.
   - Is helder wat de gewenste opbrengst moet zijn?
   - Nee, zorg dat de gewenste opbrengst helder wordt.
   - Ja? Ga verder.
   - Weet je wat er met de uitkomsten gaat doen?
   - Nee? Ga daar eerst over nadenken.
   - Ja? Ga verder.
   - Valt de onderzoeksvraag binnen het gemeentelijke takenpakket?
   - Ja, ga verder
   - Nee, wat is de rol van de gemeente, waarom wil je dit?
d. Check of het antwoord op de gevraagde onderzoeksresultaten al ergens buiten de gemeente bekend zijn. Bijvoorbeeld bij het CBS, of waarstaatjegemeente.nl.
e. Is helder welke specifieke data nodig zijn?
f. Zijn de data al ergens beschikbaar (bv. via dataplatform)?
g. Zo nee, is het helder in welke databronnen de gevraagde gegevens zich bevinden en wie de eigenaar daarvan is?
   - Nee? Zoek dat uit.
   - Ja, ga verder.
h. Stel samen met de opdrachtgever, op basis van de bronnen, de haalbaarheid van de beantwoording van de vraag vast.
i. Is de onderzoeksvraag haalbaar? Zo ja, ga verder.
j. Zorg dat de (privacy)posities helder zijn: Wie is de bronhouder, wie is (intern) verwerkingsverantwoordelijke (verstrekker) voor de te ontvangen en te verwerken gegevens, wie is verwerkingsverantwoordelijke voor de verwerkte gegevens. Wie is de eventuele verwerker van de geleverde en te verwerken gegevens?

k. Is de wens een doorlopende geautomatiseerde verwerking?
   Zo ja: hoe vaak moet de data ververst worden?
l. Leg de gegevenslevering vast in een gegevensleveringsovereenkomst (GLO). In de GLO moet staan welke gegevens worden opgevraagd, wat het doel is, de grondslag (zowel levering als ontvangst) en wat er mee gebeurt. Het invullen van de GLO is gelijk aan een (pré-)DPIA: hieruit blijkt of er sprake is van een hoog (privacy) risico. Als er sprake is van een hoge risico's, neem dan maatregelen.
m. Zorg dat de verschillende inputgegevens altijd herleidbaar zijn.
n. Zorg dat de verschillende inputstromen altijd gescheiden blijven.
o. Zorg voor een authenticatie- en autorisatieproces (wie mag welke gegevens verwerken, inzien).
p. Zorg er voor dat de gebruikte gegevens volgens de geldende standaarden (BIO) zijn beveiligd.
q. Zorg voor heldere bewaartermijnen van het 'nieuwe' informatieproduct en zorg ervoor dat deze ook worden gehandhaafd. Bewaar na deze periode hooguit de anonieme trends.
r. Zorg dat de inwoner voldoende geïnformeerd is.
s. Zorg voor een duidelijke procedure voor eventueel hergebruik (verdere verwerking) van gegevens: is dit in overeenstemming met het oorspronkelijke gebruik? Zijn de gegevens die worden hergebruikt nog actueel?
t. Zorg er voor dat de verschillende dataleveringen ook worden geëvalueerd. Zo wordt voor de deelnemende partijen helder of een gegevenslevering in de toekomst beter kan, of dat een herhaling van de datalevering moet worden voorkomen.

***