



Van Adviescommissie Digitale Ethiek
Aan College van Burgemeester en Wethouders
Onderwerp Advies casus datawarehouse
Datum 1 augustus 2023
Bijlagen Brief werkwijze commissie en verzoek ambitiestelling 2023-2024

Commissieleden

contact@ade-nijmegen.nl

5.1.2e

5.1.2e (commissielid heeft niet deelgenomen aan het schrijven van dit advies)

5.1.2e

5.1.2e

5.1.2e

Ambtelijk secretaris

5.1.2e @nijmegen.nl

5.1.2e

Inleidende samenvatting

De Adviescommissie Digitale Ethiek is in februari 2023 gevraagd om advies uit te brengen over het datawarehouse van de Gemeente Nijmegen. De vraagstelling over deze casus is in goede samenwerking met de ambtelijke organisatie opgesteld, en in bijzonder met de Functionaris Gegevensbescherming. Het datawarehouse is reeds vanuit andere perspectieven belicht, maar nog niet vanuit het maatschappelijk-ethische perspectief van de Adviescommissie. Daarmee is dit advies complementair aan de eerder uitgebrachte adviezen en beoordelingen.

Tevens is dit de eerste behandelde casus van de in januari 2023 gestarte Adviescommissie. Tijdens het adviestraject is er daarom extra tijd uitgetrokken om al doende kennis op te bouwen, een werkwijze vast te stellen, en de ambities en behoeften voor de periode 2023-2024 te inventariseren. Daarmee beschikt de Adviescommissie voortaan over een vaste procedure om zowel gevraagd als ongevraagd advies uit te kunnen brengen. Een nadere toelichting is te vinden in de bijgevoegde brief van de Adviescommissie aan het College van Burgemeester & Wethouders.

Omschrijving casus

De Gemeente Nijmegen heeft zich als doel gesteld om haar beleidsvorming en -uitvoering te verbeteren met behulp van informatie-gedreven inzichten. Om dit te bereiken, heeft zij eerder besloten een datawarehouse in te richten waarin gegevens (m.a.w. data) uit verschillende interne en externe bronsystemen kunnen worden gekopieerd en gecombineerd voor beleidsrelevante analyses. Hierdoor hoeven de bronsystemen niet telkens apart te worden geraadpleegd voor het uitvoeren van analyses, wat kostenintensief, technisch complex, en hoogdrempelig is. Hoewel de juridische onderbouwing voor deze analyses voldoende is, is dit niet het geval voor het importeren naar, combineren in, en exporteren uit het datawarehouse. Juridisch gezien bevindt het datawarehouse zich in grijs gebied, waardoor er een 'restrisico' bestaat bij het inrichten en gebruiken ervan.

Specifiek gaat het hierbij om het onderscheid tussen de zogeheten 'load 1' en 'load 2' van het datawarehouse. Load 1 omvat de complete set data die in het datawarehouse wordt gecombineerd, ongeacht uit welk bronsysteem de gegevens zijn gekopieerd. Een deel van de dataset betreft (bijzondere) persoonsgegevens. In load 2 worden alleen specifieke gegevens verwerkt voor gebruik in een analyse, waarbij van tevoren moet worden vastgelegd wat het doel en de noodzaak is van de analyse. De gemeente heeft besloten dat er geen analyses mogen worden uitgevoerd ten behoeve van geautomatiseerde besluitvorming of analyses die herleidbaar zijn naar individuele personen. Daarmee is load 2 niet wezenlijk anders dan het uitvoeren van analyses zonder datawarehouse.

Er is geen juridische grondslag voor load 1 omdat het kopiëren, importeren, en combineren van deze gegevens op zichzelf geen doelbinding heeft; de gemeente kan niet voor elk specifiek gegeven van tevoren onderbouwen waarom zij die verwerkt voor gebruik in het datawarehouse. Ook kan er niet worden gegarandeerd dat de in het datawarehouse opgenomen gegevens met hetzelfde doel worden gebruikt als het doel waarvoor de gegevens oorspronkelijk zijn verzameld in het bronsysteem. Daarnaast is het de commissie niet duidelijk geworden hoe deze verzameling in alle gevallen aan het beginsel van dataminimalisatie voldoet. De gemeente geeft aan dat er alleen gegevens in het datawarehouse opgenomen worden die daadwerkelijk gebruikt worden voor analyses, maar het is voor de commissie niet inzichtelijk geworden hoe wordt voorkomen dat er zonder nut of noodzaak gegevens worden toegevoegd aan het datawarehouse.

Daarmee schendt het concept van een datawarehouse in beginsel meerdere basisprincipes van de Algemene verordening gegevensbescherming (AVG). Tegelijkertijd laat de praktijk zien dat vele Nederlandse overheden datahuizen gebruiken om hun dienstverlening en processen te verbeteren, daar er vaak geen realistisch alternatief voor handen is. Ook het Nijmeegse datawarehouse is inmiddels al enkele jaren in gebruik en is stapsgewijs uitgebreid.

Na het 'restrisico' meermaals vanuit juridisch perspectief te hebben belicht door zowel de Functionaris Gegevensbescherming als een extern onderzoeksbureau, is de Adviescommissie gevraagd om vanuit een maatschappelijk perspectief en aan de hand van een digitaal-ethische invalshoek te reflecteren op deze casus. Het advies van de commissie is bedoeld ter aanvulling van de juridische overwegingen, om zodoende een breder beeld te krijgen van het gebruik van een datawarehouse door de gemeente.

Advies

De Adviescommissie heeft vanuit maatschappelijk en digitaal-ethisch perspectief het datawarehouse overwogen. Zij heeft hierbij geconstateerd dat de maatschappelijke wenselijkheid van de met behulp van het datawarehouse uit te voeren analyses op zichzelf voldoende is onderbouwd. Daarnaast zijn alternatieve oplossingen onhaalbaar, en is het hoogst onwaarschijnlijk dat het datawarehouse in de komende jaren overbodig zal worden. Zodoende is een datawarehouse een permanente, duurzame, en kosteneffectieve oplossing. De noodzaak van het datawarehouse als middel is daarmee volgens de Adviescommissie geloofwaardig aangetoond.

Echter, zij is van mening dat er onnodige risico's worden genomen in de huidige opzet en gebruik van het datawarehouse. Voorzorgsmaatregelen om deze risico's te adresseren zijn sinds 2017 herhaaldelijk voorgesteld, maar slechts gedeeltelijk geïmplementeerd. Daarmee

is het restrisico er nog steeds. Naast vraagtekens over de juridische houdbaarheid van de huidige situatie – een afweging die bij de Functionaris Gegevensbescherming is belegd – uit de Adviescommissie haar zorgen over de veiligheid van de in het datawarehouse gecombineerde gegevens; het rechtmatig en integer gebruik van deze gegevens voor analyses; de controleerbaarheid van het gebruik; het waarborgen van digitale burgerrechten; en de mogelijkheid van adequaat toezicht en verantwoording.

Het datawarehouse bevat mogelijk (bijzondere) persoonsgegevens waarvan niet duidelijk is in hoeverre deze relevant zijn voor de analyses die de gemeente wenst uit te voeren. Ook is het onvoldoende duidelijk en controleerbaar hoe (onbedoelde) schade aan de individuen van wie deze gegevens zijn wordt voorkomen, bijvoorbeeld in de vorm van discriminatoire analyses of *de facto* geautomatiseerde besluitvorming. Tevens is er mogelijk onvoldoende bescherming tegen datalekken en onrechtmatige toegang tot en bewerking van gegevens. Tot slot is het de commissie onduidelijk hoeverre de gemeente met betrekking tot het datawarehouse aan haar (wettelijke) verplichtingen kan voldoen, waaronder verzoeken van burgers en het gemeentebestuur.

De Adviescommissie ziet de huidige ethische afwegingen van de gemeente ten aanzien van het datawarehouse als niet voldoende transparant en ontoereikend vastgelegd. De ethische en maatschappelijk risico's, en de mogelijk daaruit volgende vormen van schade, zijn in potentie groot. Met behulp van de eerder geadviseerde en de door de Adviescommissie voorgestelde maatregelen kunnen deze risico's tot een minimum worden beperkt. Zij adviseert deze maatregelen op een zo kort mogelijke termijn alsnog te implementeren.

Zie voor een meer gedetailleerde beschrijving van de overwegingen van de Adviescommissie de bevindingen op de volgende pagina's.

Bevindingen

Hierna volgen de bevindingen opgesplitst per thema in de Code Goed Digitaal Openbaar Bestuur (CODIO), namelijk *Democratie*, *Rechtstaat*, en *Bestuurskracht*. Deze bevindingen zijn uitsluitend beschreven zoals deze van toepassing zijn op de casus, aangevuld met eventuele overwegingen van de Adviescommissie. Een gedetailleerde beschrijving van de betekenis van de drie thema's en de verzameling van onderliggende subthema's en 30 waarden zijn te raadplegen in het oorspronkelijke CODIO-rapport¹. Omwille van de leesbaarheid van de tekst wordt er niet naar de volledige set waarden verwezen, maar de Adviescommissie past deze waarden wel toe in haar werkwijze².

De Adviescommissie vindt het waardevol om eventuele minderheidsopvattingen van haar leden te vermelden. Het wordt aangegeven indien er sprake is van een opvatting waarover binnen de commissie geen consensus is bereikt.

Democratie

De belangrijkste waarden binnen dit thema die relevant zijn bevonden door de Adviescommissie betreffen transparantie, duurzaamheid, het voorkomen van schade, en bescherming.

Transparantie: Burgers hebben naar alle waarschijnlijkheid geen kennis van het bestaan van het datawarehouse van de Gemeente Nijmegen. Er bestaat volgens de gemeente een mogelijkheid om in te zien welke data in het datawarehouse opgeslagen is van een bepaald persoon. Dit is volgens de commissie echter onvoldoende gecommuniceerd en te hoogdrempelig van aard. Ook is het de commissie onduidelijk of hierin aan te geven is door burgers met welk doel de gegevens verwerkt mogen worden. Dit is in theorie wel te implementeren. Dit niveau van openheid en transparantie is ook het uitgangspunt van de Wet open overheid (Woo).

Duurzaamheid: Er is geen ecologisch duurzaam en kosteneffectief alternatief voorhanden om de data beschikbaar te maken dan de datawarehouse oplossing waar momenteel voor gekozen is. Andere manieren om de data t.b.v. de doelen die worden gesteld binnen 'load 2' beschikbaar te maken, brengen andere en meer overhead-, veiligheids-, privacy-, en performance issues met zich mee.

Voorkomen van schade: De Adviescommissie is van mening dat er meer voorzorgsmaatregelen genomen zouden moeten worden ter voorkoming van mogelijke

¹ Meijer, A., & Ruijter, E. (2021). *Code Goed Digitaal Openbaar Bestuur (CODIO): Borgen van waarden bij de digitalisering van het openbaar bestuur*. USBO Advies, Universiteit Utrecht.

² Zie ook de bijlage "Brief werkwijze commissie en verzoek ambitiestelling 2023-2024"

schade. Denk hierbij aan preventie van ongeoorloofde combinaties van gegevens; betere beveiliging van de gegevens en levering; implementatie van rollen- en rechtenbeheer voor personen met toegang tot het datawarehouse; screening van personen met toegang; betere opsplitsing (compartimentalisatie) van de gegevens; periodieke externe (technische) audits; certificering (bijv. ISO27001); en betrokkenheid van de Chief Information Security Officer en de Chief Data Officer van de gemeente.

Bescherming: In die zin is het voor de Adviescommissie momenteel onvoldoende duidelijk, met het oog op bescherming, in hoeverre er maatregelen zijn genomen om te voorkomen dat bijvoorbeeld bijzondere persoonsgegevens of medische gegevens beschikbaar worden gesteld en welke conclusies hieraan verbonden worden op een mogelijk ongewenste of oneerlijke manier. Betere classificatie van de gegevens zou hier in de basis bij kunnen helpen.

Rechtstaat

De belangrijkste waarden binnen dit thema die relevant zijn bevonden door de Adviescommissie betreffen de waarden privacy, menselijke autonomie, non-discriminatie, en aanvechtbaarheid.

Privacy: Binnen het datawarehouse zijn te weinig maatregelen getroffen om technisch te voorkomen dat er bepaalde data gecombineerd wordt waardoor de privacy niet (toekomstbestendig) gewaarborgd is. Technische maatregelen, zoals de eerder genoemde compartimentalisatie en pseudonimisering, kunnen de bescherming van de privacy verhogen.

Menselijke autonomie: In de huidige opzet is zelfbeschikking over data in theorie mogelijk, maar te hoogdrempelig voor inwoners. Gebrekkige synchronisatie van mutatie- en verwijderingsverzoeken is een inbreuk op de menselijke autonomie. Deze verzoeken moeten daarom binnen de geldende wettelijke termijnen worden verwerkt in het datawarehouse; daar is nu geen proces voor. Het is volgens de Adviescommissie technisch mogelijk menselijke autonomie in een datawarehouse goed in te regelen en burgers hierover te informeren.

Non-discriminatie: Het risico op het uitvoeren discriminatoire analyses kan niet uitgesloten worden en het is onduidelijk welke maatregelen de gemeente genomen heeft om dit te voorkomen. De criteria voor en wijze van beoordeling van aanvragen om analyses uit te voeren met de in het datawarehouse aanwezige data zijn voor de commissie onvoldoende helder. Deze controle vervult echter een cruciale rol in het voorkomen van analyses die (onbedoeld) discriminerende gevolgen teweeg kunnen brengen.

Aanvechtbaarheid: Volgens de gemeente is het mogelijk voor inwoners om de opname van hun persoonsgegevens in het datawarehouse te weigeren voor die onderdelen waarvan de

gegevens wettelijk gezien ook uit het bronbestand verwijderd mogen worden. Voor de commissie is dit proces onduidelijk, en onvoldoende transparant ingericht wat de aanvechtbaarheid belemmert.

Bestuurskracht

De belangrijkste waarden binnen dit thema die relevant zijn bevonden door de Adviescommissie betreffen de volgende zeven waarden.

Wendbaarheid: Via een datawarehouse is de opslag en verwerking van gegevens vele malen wendbaarder dan met aparte gegevensverzameling. Hier ligt de cruciale meerwaarde van een datawarehouse. De Adviescommissie is van mening dat alternatieve oplossingen dermate minder wendbaar zijn dat een datawarehouse de enige haalbare oplossing is om de door de gemeente beoogde doelstellingen te bereiken. Op de zeer lange termijn zou er (mogelijk) kunnen worden gewerkt aan de integratie en synchronisatie van alle bronsystemen van de in het datawarehouse verzamelde gegevens, waardoor het datawarehouse uiteindelijk overbodig wordt en kan worden uit gefaseerd.

Risicobewustzijn: De Adviescommissie verkeert in de veronderstelling dat de gemeente de informatieveiligheid van het datawarehouse kan verbeteren door de risico's in de reeds uitgevoerde *Data Protection Impact Assessments* (DPIA's) uit 2017 en 2022 te adresseren. Uit de gesprekken die de commissie heeft gevoerd werd duidelijk dat de bij de uitvoering betrokken personen zich bewust waren van deze risico's. Het is voor de Adviescommissie des te meer onduidelijk waarom de in de DPIA's voorgestelde maatregelen nog niet volledig zijn geïmplementeerd. Daarmee is bewustzijn onvoldoende vertaald naar daadwerkelijk handelen, en worden er mogelijk onnodige risico's genomen bij het gebruik van het datawarehouse.

Veiligheid: Gegevens worden deels handmatig geïmporteerd, en vanuit sommige organisaties worden gegevens per e-mail aangeleverd. Het is voor de Adviescommissie onduidelijk of hier de juiste veiligheidsmaatregelen worden genomen, en zelfs als dit het geval is leiden deze mogelijkheden tot een aanzienlijk risico op menselijke fouten. De gemeente zou kunnen overwegen dit verder te automatiseren, teneinde een datalek of onrechtmatig gebruik van gegevens te voorkomen.

Doelmatigheid: Het datawarehouse is doelmatig in die zin dat dit een duurzamere en financieel prudentere oplossing is dan het alternatief van aparte databases. Dit moet echter niet worden verward met doelmatigheid in de zin van gegevensverzameling en -gebruik, wat nadrukkelijk in strijd is met het uitgangspunt van een datawarehouse.

Verantwoording: Het College van Burgemeester & Wethouders legt niet actief verantwoording af over het datawarehouse. Dit wordt verder gecompliceerd door het feit dat het beheer van het datawarehouse deels is belegd bij een samenwerkingsverband in

plaats van bij de gemeentelijke organisatie zelf. Ook is bij de inrichting van het datawarehouse aangegeven dat het datawarehouse een tijdelijke oplossing betreft totdat er alternatieven mogelijkheden beschikbaar komen, maar dit is zowel in de ogen van de uitvoerende personen als de Adviescommissie onrealistisch. Het is technisch onhaalbaar, duurder, en minder duurzaam om in plaats van een datawarehouse de bronsystemen direct met load 2 te verbinden. Omdat de tijdelijkheid van deze oplossing daarmee hoogst onwaarschijnlijk is, is het maatschappelijk wenselijk een jaarlijkse verantwoording over het gebruik en de noodzaak van het datawarehouse te organiseren. Deze verantwoording kan niet worden belegd bij de Functionaris Gegevensbescherming, gezien deze als toezichthouder een andersoortige rol heeft.

Controleerbaarheid: Het datawarehouse is, buiten de huidige zes systeembeheerders, onvoldoende controleerbaar door interne en externe partijen. Zo is er geen mogelijkheid tot inzage voor burgers of andere belanghebbenden, en is het onduidelijk of er aan eventuele informatieverzoeken op basis van relevante wet- en regelgeving en individuele gerechtelijke uitspraken kan worden voldaan. De gegevensleveringsovereenkomsten zijn bovendien te weinig inzichtelijk over welke data er worden aangeleverd en naar het datawarehouse worden geïmporteerd. Er is in het bijbehorende formulier geen inhoudelijke beschrijving opgenomen over wat een specifiek gegeven in de praktijk meet. Ook is in deze overeenkomsten niet voor elk specifiek gegeven aangegeven of dit een (bijzonder) persoonsgegeven betreft. Het ontbreken van deze informatie belemmert de externe controleerbaarheid, en is daarmee een obstakel voor de verantwoording van het (juist) gebruik van gegevens in het datawarehouse.

Integriteit: De Adviescommissie constateert dat de in de DPIA's geadviseerde strengere screening van de systeembeheerders niet is gerealiseerd. Ook is de geadviseerde *logging* van activiteiten in het datawarehouse niet geïmplementeerd, waardoor achteraf niet kan worden gecontroleerd wie wat met de gegevens in het datawarehouse heeft gedaan. Dit beperkt de mogelijkheid tot toezicht voor zowel de Functionaris Gegevensbescherming als de Chief Data Officer. Het gebrek aan rollen- en rechtenbeheer – alle personen met toegang tot load 1 van het datawarehouse hebben volledige beheer van alle gegevens en alle functies, ondanks dat dit niet nodig is voor de werkzaamheden van individuele personen – levert bovendien onnodig grote integriteitsrisico's op. Daarbij moet ook aandacht worden besteed aan scenario's waarbij derden via de systeembeheerders onrechtmatig toegang krijgen tot het datawarehouse, bijvoorbeeld als gevolg van ondermijnende activiteiten of identiteitsfraude.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	1