DPIA Oordeel FG gemeente Nijmegen
DPIA: Opslag van analysedata in een datawarehouse

Inleiding

Hierbij het oordeel van de FG Gemeente Nijmegen over de DPIA 'Opslag van analysedata in een datawarehouse'. Gekozen is voor een systematische aanpak. Deze is terug te herleiden tot de oordeelsvorming van DPIA's in het algemeen. In deze wordt oordeel en het daarmee gepaard gaande advies van de opgestelde DPIA weer aan een (meta) oordeel onderworpen. Dat betekent dat niet de diepte ingegaan wordt over de te nemen maatregelen, maar wél of er maatregelen genomen worden, op welk oordeel deze gebaseerd zijn én of oordeelsvorming en genomen maatregelen voorzien zijn van deugdelijke argumentatie.
Uiteindelijk uit zich dit in een eindoordeel die weergeeft of m.i. het gehele voorstel van maatregelen én te nemen maatregelen bij geconstateerde risico's, te samen een aanvaardbaar risico vormen bij het gebruik van privacygevoelige gegevens.

In de periode jan tot okt 2022 hebben Arjen Verhulst, Agethe Derks, Paul Geurts, Niels de Jager, Stijn Verhagen en ondergetekende gewerkt aan de voorbereiding van deze DPIA. Dit heeft geleid tot een aantal op- en aanmerkingen die meegenomen zijn in de definitieve versie DPIA 'Opslag van analysedata in een datawarehouse' dd 03/10/22. Deze versie vormt de onderlegger voor deze toetsing.

Bij deze DPIA horen de volgende bijlagen:

- Opzet GLO / Voorbeeld GLO.
- Privacy Impact Assessment Data Warehouse 10 nov 2017.
- Concept Collegevoorstel 'Gebruik datawarehouse Gemeente Nijmegen en beleggen restrisico'.
- Verwerkersovereenkomst IRvN (getekend).

Oordeel matrix

De oordeelmatrix is opgebouwd uit een viertal invalshoeken.
De hieronder gehanteerde invalshoeken zijn

- Zijn er reeds DPIA's op dit onderwerp uitgevoerd. En wat zijn daarvan de conclusies?
- Ethisch / politiek bestuurlijke vraag
- Juridische scan (dit betreft meerdere vragen)
- De geconstateerde risico's en voorgestelde maatregelen

Vraag	Argumentatie	Oordeel
1. Zijn er reeds DPIA's op dit onderwerp uitgevoerd?	Ja, in november 2017 is er een DPIA uitgevoerd door BKBO, het Bureau voor Kwaliteitsborging bij de Overheid.	In de nieuwe DPIA (versie 2022) staat aangegeven op welke wijze met de 25 adviezen uit de DPIA 2017 is omgegaan. Op één aanbeveling na (beveiligde werkplekken) worden alle aanbevelingen en adviezen opgevolgd.
2. Is het ethisch / politiek bestuurlijk verantwoord?	Het is aan het College om hier een antwoord op te geven. In een bijlage over de ethische kant van dit datawarehouse wordt hier dieper op ingegaan.	Advies is om dit voorstel ook aan te beiden aan de nieuw opgerichte 'Adviescommissie Digitale Ethiek' en haar te vragen haar zienswijze hierop te geven.
3. Juridische toets a. Doel / grondslag	a. Het doel is duidelijk omschreven. De grondslag is voor de onderdelen in Load 2 duidelijk: deze volgt de grondslag van de onderliggende gegevensverzameling. Voor Load 1 is deze problematischer. Het DWH heeft geen eenduidige en duidelijke grondslag. Er zijn echter wel aanknopingspunten bij de grondslag van "algemeen belang". (zie DPIA DWH). Deze werkwijze is van tijdelijke aard. Samen met VNG -als onderdeel van het traject Common Ground- wordt gezocht naar directe ontsluiting van de bronnen (load2) en daarmee aansluiting bij de grondslag van de gegevensverwerking per dataset en doel. Daarmee zou de huidige load 1 (en de problematische grondslag hiervan) komen te vervallen.	a. In 2017 is er een DPIA gemaakt over de privacy aspecten van het Datawarehouse. In deze DPIA stonden 25 verbeterpunten aangegeven. Deze zijn in de afgelopen 5 jaar opgepakt en vrijwel allemaal uitgevoerd. Dat is een positief gegeven. Maar het probleem van de grondslag is hiermee niet opgelost. Ondanks 'aanknopingspunten', die genoemd zijn in deze DPIA blijft deze problematisch. Vandaar dat het College een uitspraak zal moeten doen over het aanvaarden van de verantwoordelijkheid over het restrisico: het ontbreken van een eenduidige grondslag. Een nieuwe werkwijze (samen te ontwikkelen in VNG verband) moet ervoor zorgen dat dit probleem in de toekomst wordt opgelost.
b. Proportionaliteit	b. Deze wordt met name vormgegeven via de lijn Load 1 naar Load 2. In deze stap worden gegevens geanonimiseerd en soms geaggregeerd. De stap vanuit de oorspronkelijke gegevensverzamelingen naar Load 1 vindt alleen plaats als er vraag is tot het verzamelen van gegevens. Dit dient in de GLO aangegeven te worden. Andere gegevens worden niet opgenomen. De verwerking stelt de gemeente in staat haar processen beter, sneller en actueler te evalueren en aan te passen.	b. Proportionaliteit wordt door diverse acties vormgegeven. Toch blijft de gegevensverzameling van Load 1 kwetsbaar voor privacy risico's. De GLO's dienen dit grotendeels af te vangen. Van belang is deze up to date te houden en bij wijzigingen direct de gegevensverzameling in Load 1 aan te passen.
c. Subsidiariteit	c. Subsidiariteit: - met een andere werkwijze wordt de kwaliteit van het datawarehouse aangetast en daarmee het doel geschaad.	c. Sinds de introductie van het Datawarehouse in 2017 (en het oordeel en de 25 adviezen die hierin genoemd staan) is er gezocht naar een werkwijze die minder privacy risico's met zich mee brengt. Het opvolgen van 24 van

	- De introductie van GLO's is een duidelijke verbetering ten opzichte van de privacyrisico's die benoemd zijn in het oordeel over het Datawarehouse 2017.	de 25 adviezen is een forse stap voorwaarts. Het werken met GLO's geeft meer zekerheid omtrent het zorgvuldig omgaan met privacy. Restrisico's blijven óók in deze nieuwe werkwijze bestaan, al zijn ze duidelijk minder dan in de vorige versie. Over de resterende restrisico's moet het College een oordeel geven.
d. Persoonsgegevens buiten de EER gebruikt?	d. Neen.	d. Akkoord.
e. Andere partijen betrokken? (verwerkers / subverwerkers)?	e. Ja, De IRvN. Zij zijn verwerker van de gegevens. Met de IRvN is een verwerkersovereenkomst opgesteld.	e. Akkoord. Verwerkersovereenkomst (getekend) met de IRvN is als bijlage toegevoegd.
f. Hoe lang worden gegevens bewaard en termijn en wijze van vernietiging?	f. De bewaartermijnen volgen de bewaartermijnen van de oorspronkelijke gegevensverzamelingen. Vernietiging in het oorspronkelijke bestand betekent dus ook vernietiging in Load 1 én Load 2. Belanghebbenden kunnen hun rechten uitspreken conform het privacy-beleid. Dit betekent recht op verwijdering of vergetelheid. Mutaties vinden plaats in de oorspronkelijke bestanden en dit werkt door in het Datwarehouse.	f. Akkoord. Hier dient wel (minimaal) ieder jaar (evidence based) een check op te worden gedaan.
g. Hoe worden gegevens beveiligd?	g. Beveiliging vindt plaats via autorisatie en 2 Factor Authenticatie. Autorisaties voor Load 1 en Load 2 zijn gescheiden.	g. Autorisatie voor Load 1 vindt plaats bij de IRvN. Logging is nu nog niet mogelijk. Dit wordt in 2023 geregeld.
4. Risico's en voorgestelde maatregelen	Deze zijn duidelijk beschreven in de DPIA. Een datawarehouse van deze omvang en deze doelstelling vormt een privacy risico voor belanghebbenden. Belanghebbenden moeten hun recht kunnen uitvoeren. Hiervoor is communicatie over het datawarehouse van belang. Ondanks de vernieuwende vorm en werkwijze (en daarmee enorme verbetering) ten opzichte van de oorspronkelijke opzet van het datawarehouse blijft er een restrisico over. Hierover dient het College een uitspraak te doen.	Getracht is via een andere werkwijze de privacy risico's zo veel mogelijk te verminderen (mitigeren). Dit is gedaan door 24 van de 25 maatregelen uit het eerste advies over te nemen en uit te voeren. Het probleem blijft zitten in de grondslag. Deze is weliswaar omschreven maar de onderbouwing is 'dun'. Een duidelijke grondslag ontbreekt. Voor Load 2 geldt dat de grondslag hiervoor de grondslag van de oorspronkelijke gegevensverzameling volgt. Wijzigingen hierin worden direct verwerkt in Load 1 en Load 2. Het College dient een uitspraak te doen over de aanvaardbaarheid van de restrisico's. Tenslotte: Naleving van de afspraken is essentieel voor het beheersen van de genoemde restrisico's. Dat betekent dat na aanvaarding door het College de organisatie een nalevingsstrategie moet vaststellen gebaseerd op deze DPIA en haar oordeel en dat élk jaar verantwoording

		(evidence based) dient afgelegd te worden aan de FG over de uitvoering van deze naleving.

Eindoordeel

In dit onderdeel geef ik aan welke maatregelen genomen moeten worden. Welke attentiepunten er zijn bij de uitvoering van dit project. De mate waarin risico's onderkend zijn, afgedekt worden door maatregelen en welk oordeel ik daarover heb. Dat oordeel betreft de risico's die overblijven na handeling: zijn deze te kwalificeren als "hoog", "middel" of "laag" met als eindoordeel is dit m.i. "aanvaardbaar" of "niet-aanvaardbaar".

Deze gegevensverwerking kent – na uitvoering van genoemde adviezen en het afdekken van het restrisico door het College - een "middelhoog" risico.

Onderbouwing
Het Datawarehouse (DWH) heeft *geen eenduidige en duidelijke grondslag*, want:
• de gemeente heeft geen toestemming van de betrokkenen gevraagd.
• er is geen overeenkomst naar privaatrecht met betrokkenen.
• een vitaal belang voor alle individuele inwoners is niet aanwezig.
• er is geen duidelijke wettelijke basis.

Er zijn in de DPIA wel aanknopingspunten genoemd bij de grondslag van "algemeen belang".
- Artikel 213a Gemeentewet
  Het college verricht periodiek onderzoek naar de doelmatigheid en de doeltreffendheid van het door hem gevoerde bestuur.

- Artikel 6, lid 4 van de AVG, Jo artikel 23 van de AVG, mits het primaire wettelijke kader geen verbod heeft tot verdere verwerking:
Wanneer de verwerking voor een ander doel dan dat waarvoor de persoonsgegevens zijn verzameld niet berust op toestemming van de betrokkene of op een Unierechtelijke bepaling of een lidstaatrechtelijke bepaling die in een democratische samenleving een noodzakelijke en evenredige maatregel vormt ter waarborging van de in artikel 23, lid 1, bedoelde doelstellingen houdt de verwerkingsverantwoordelijke bij de beoordeling van de vraag of de verwerking voor een ander doel verenigbaar is met het doel waarvoor de persoonsgegevens aanvankelijk zijn verzameld onder meer rekening met:
ieder verband tussen de doeleinden waarvoor de persoonsgegevens zijn verzameld, en de doeleinden van de voorgenomen verdere verwerking;
b) het kader waarin de persoonsgegevens zijn verzameld, met name wat de verhouding tussen de betrokkenen en de verwerkingsverantwoordelijke betreft;
c) de aard van de persoonsgegevens, met name of bijzondere categorieën van persoonsgegevens worden verwerkt, overeenkomstig artikel 9, en of persoonsgegevens over strafrechtelijke veroordelingen en strafbare feiten worden verwerkt, overeenkomstig artikel 10;
d) de mogelijke gevolgen van de voorgenomen verdere verwerking voor de betrokkenen;
e) het bestaan van passende waarborgen, waaronder eventueel versleuteling of pseudonimisering.

- Artikel 89 van de AVG
  Waarborgen en afwijkingen in verband met verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden.
  Gegevens in het datawarehouse worden verwerkt voor *statistische* doeleinden; het doen van onderzoek. Dat maakt het mogelijk wel op grote schaal persoonsgegevens te verwerken, mits de beveiliging en doelbinding van die gegevens goed op orde is.

Het is aan het College een uitspraak te doen of zij de restrisico's die gepaard gaan met deze werkwijze willen aanvaarden en hiervoor de verantwoordelijkheid willen nemen. Dit besluit is noodzakelijk om deze werkwijze tijdelijk door te laten gaan.

Streven naar tijdelijkheid
In de DPIA staat verwoord dat de Gemeente Nijmegen wil aansluiten bij het landelijke Common Ground gedachtegoed, een set aan informatiearchitectuurprincipes. Een van deze principes is dat data zoveel mogelijk wordt opgehaald bij de bron, via services. Daarmee zou de huidige Load1 komen te vervallen. En daarmee zou het probleem van de grondslag komen te vervallen.

Veel applicaties en services zijn er (technisch) nog niet op ingericht om grote hoeveelheden data ook zo te kunnen ontsluiten. Dit principe is dus nog niet toepasbaar op het uitvoeren van analyses waarmee het inzetten van een datawarehouse een noodzakelijke, tijdelijke tussenstap is. In de toekomst zullen meer applicaties en processen hun data wel rechtstreeks kunnen ontsluiten, dat ze ook bruikbaar zijn voor analyses. Daar zullen we dan ook op overstappen.
Vanuit de FG-rol wil ik periodiek (minstens één keer per jaar) op de hoogte gehouden worden van de vorderingen op dit vlak. Uiteindelijk is het doel van dit traject om deze tijdelijke situatie op te heffen.

Collegebesluit
De restrisico's voor deze huidige werkwijze dienen afgedekt te worden door een uitspraak van het College.
Indien het College akkoord gaat met de restrisico's, kan wat mij betreft een positief advies gegeven worden op de onderliggende DPIA. De hierin genoemde restrisico's zijn immers voor het College "aanvaardbaar".

Het College wordt gevraagd om deze DPIA en haar oordeel aan te bieden aan de Adviescommissie Digitale Ethiek met het verzoek hierover een zienswijze te geven.

Naleving
In het najaar van 2022 zal een nalevingsstrategie opgesteld dienen te worden op basis van deze DPIA en het gegeven oordeel. Deze dient aangeboden te worden aan de FG-er van de gemeente Nijmegen.

In het najaar 2023 zal vanuit de functionaris voor de gegevensbescherming actief getoetst worden of de maatregelen uit deze DPIA en de naleving hiervan daadwerkelijk opgevolgd worden. Daartoe dient de betreffende afdeling zélf evidenced based (op bewijs gebaseerd) de onderleggers hiervoor aan te leveren.

Tot slot:
Op basis van deze DPIA zie ik – vooralsnog - geen reden om een voorafgaande raadpleging te hebben met de Autoriteit Persoonsgegevens.

Ik wacht de zienswijze van de Adviescommissie Digitale Ethiek met belangstelling af (mits het College deze voor te stellen stap overneemt).

PK/27/10/2022