Werkagenda opgave digitale transformatie

7 maart 2024

Werkagenda opgave digitale transformatie 2024

Waarom een werkagenda?

Binnen de opgave digitale transformatie werken we aan digitale thema's waarop we als organisatie willen versnellen. De werkagenda geeft richting aan de opgave en duidelijkheid aan de organisatie waarop we versnelling willen maken. Deze werkagenda beschrijft welke doelen we per thema nastreven en welke activiteiten daarbij horen. Omdat we agile werken bekijken we stap voor stap wat de juist interventies zijn per thema. We maken dus een inschatting van nuttige interventies, maar reflecteren continue op de effecten van eerdere interventies en bepalen volgens nieuwe stappen. Activiteiten en interventies moeten daarbij altijd terug te voeren zijn op de doelstellingen die we in deze werkagenda hebben opgesteld.

Deze werkagenda bouwt voort op afspraken en keuzes die in oktober 2022 zijn gemaakt bij aanvang van de opgave digitale transformatie en is geactualiseerd tijdens een werksessie met de wethouder digitalisering op 7 maart 2024. In de werkagenda blikken we terug en vooruit op eerder vastgestelde thema's en voegen we met 'algoritme en kunstmatige intelligentie' één nieuw thema toe aan de opgave digitale transformatie.

Uitgangspunten waar we naar handelen

- We werken agile zodat we beter in staat zijn in te spelen op veranderingen wanneer de omgeving (zowel intern als extern) deze van ons vraagt;
- We betrekken belanghebbenden in een zo vroeg mogelijk stadium bij (geplande) interventies zodat we daadwerkelijk toegevoegde waarde kunnen creëren;
- We werken volgens het principe 'leading by doing', waarbij we medewerkers meenemen in de nieuwe manier(en) van werken zodat medewerkers niet alleen het resultaat zien maar ook meemaken hoe we daartoe komen;
- We communiceren proactief over resultaten, voortgang en knelpunten zodat we transparant te werk gaan;
- We reflecteren continu op resultaten na interventies, zodat we ervan leren en indien nodig passende interventies kunnen doen;
- We voldoen waar dat mogelijk is altijd aan privacy-, archivering- en security-by-design en vragen om advies bij ethische kwesties (o.a. bij de adviescommissie digitale ethiek);
- We houden bij uitvoering van onze activiteiten altijd rekening met (aangekondigde) Europese en landelijke regel- en wetgeving;
- We volgen het informatiebeleid (DIB), de visie op dienstverlening en de visie op bedrijfsvoering.

Opbouw van de werkagenda

De werkagenda is opgebouwd vanuit een vaste structuur. De eerste pagina's van de werkagenda gaan over de missie van de opgave, wie waarvoor verantwoordelijk is en wanneer thema's in aanmerking komen als opgavethema. Vervolgens volgt een reflectie en vooruitblik op de opgavethema's van de opgave digitale transformatie.

Maatschappelijke opgave

Wat maakt dit voor een Nijmegenaar een belangrijk thema?

Doelen

Wat willen we binnen de opgave bereiken met dit thema?

Resultaten

Wat is er al bereikt in de opgave (of organisatie)?

Geplande activiteiten

Welke activiteiten of interventies zijn we van plan om uit te voeren?

Digitale transformatie

Missie: publieke waarden borgen in de gedigitaliseerde stad

1

Opgave
Juiste maatschappelijke randvoorwaarden voor digitale transformatie bereiken

Digitale samenleving

Geen digitale kansenongelijkheid
Privacy en autonomie geborgd
Digitaal veiligheid en gezondheid
Betrouwbare digitale infrastructuur
Bescherming menselijke waardigheid
Duurzaamheid in technologie

2

Opgave
Vertrouwen in moderne gemeente versterken en zelf digitaal transformeren

Digitale overheid

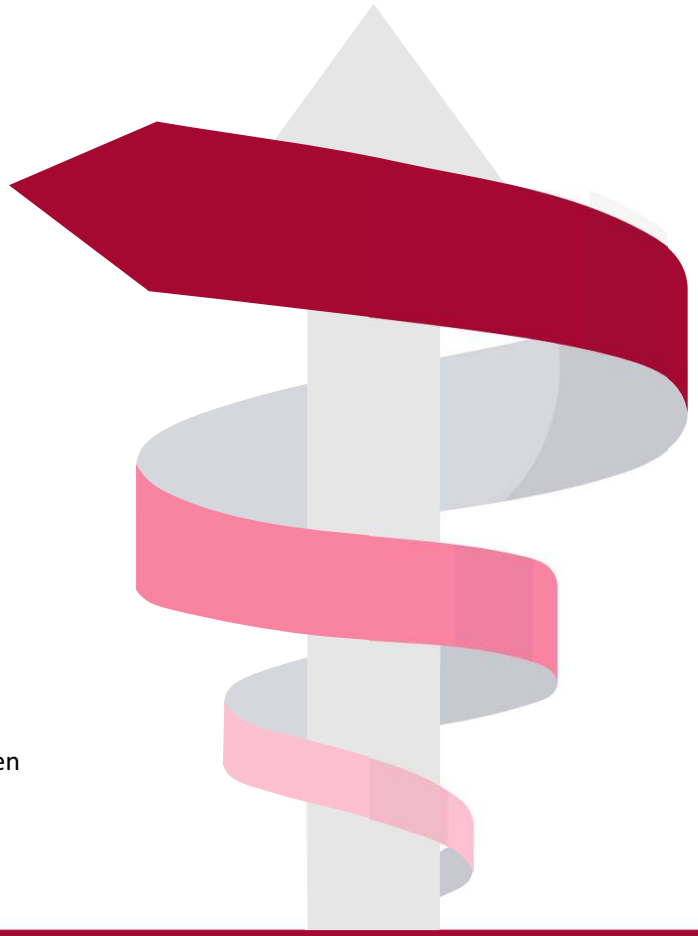
Verantwoorde en uitlegbare digitale processen
Inclusief en toegankelijk
Ruimte voor maatwerk
Als een platform opererend
Mens- en opgavegericht

3

Opgave
Juiste organisatorische randvoorwaarden voor digitale transformatie bereiken

Digitale bedrijfsvoering

Innovatief, digivaardig en datagestuurd
Integer en privacybeschermend
Continue afweging van publieke waarden
Inzet ICT onder regie en toezicht van mensen
Robuuste en veilige technologie



Opgave digitale transformatie

Versnelling en doorbraak

Bestuurlijk opdrachtgever (namens college)
Stelt vanuit bestuurlijk perspectief prioriteiten en maakt keuzes, zorgt voor samenhang met het coalitieakkoord en verdedigt keuzes en resultaten in politieke arena

Programma digitalisering

Going concern

Ambtelijk opdrachtgever
Creëert de randvoorwaarden en neemt belemmeringen weg voor het opgaveteam

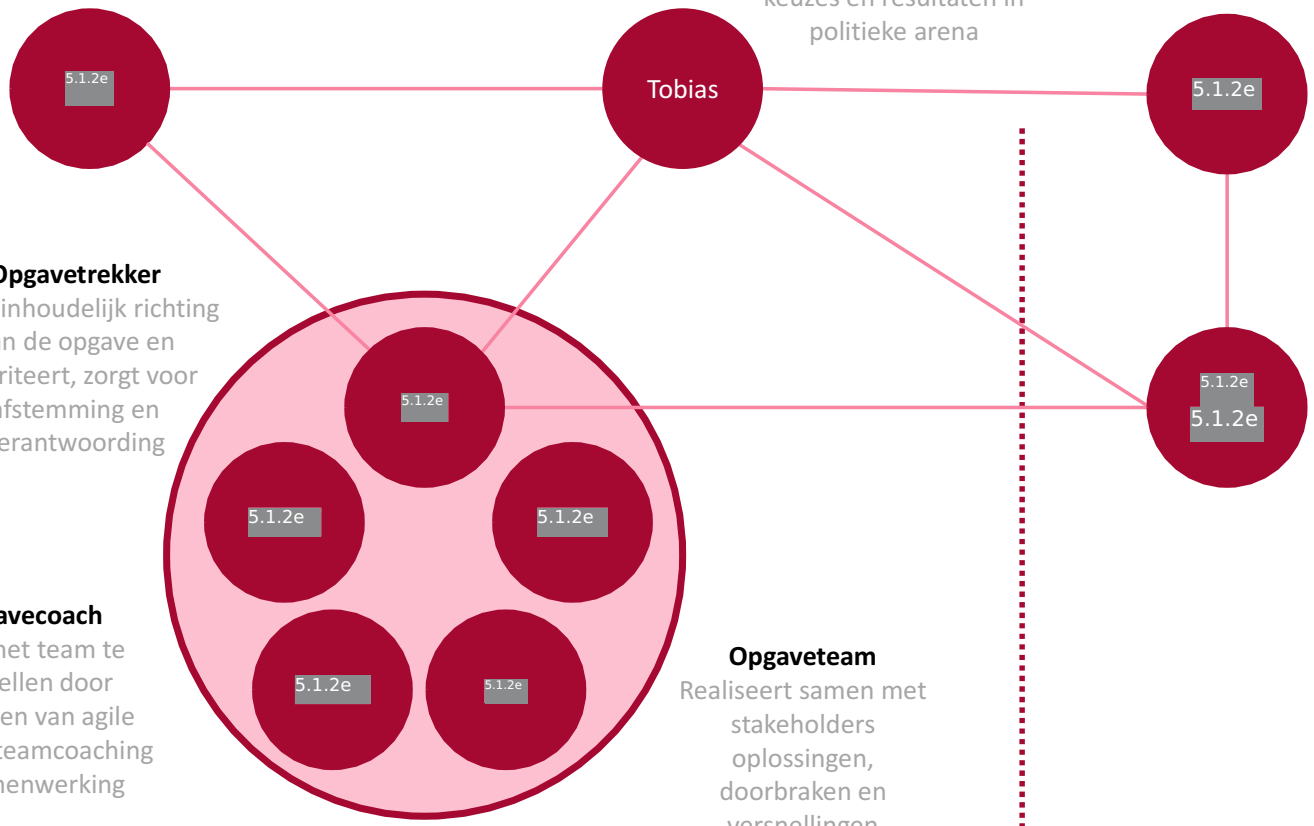
Concernmanager PIF
Creëert de randvoorwaarden en neemt belemmeringen weg voor het programma

Opgavetrekker
Geeft inhoudelijk richting aan de opgave en prioriteert, zorgt voor afstemming en verantwoording

CIO
Geeft inhoudelijk sturing aan de i-thema's die buiten de opgave vallen

Opgavecoach
Helpt het team te versnellen door faciliteren van agile werken, teamcoaching en samenwerking

Opgaveteam
Realiseert samen met stakeholders oplossingen, doorbraken en versnellingen



Afbakening: welke activiteiten doen we als opgave?

Initiëren wat we nog niet doen

Versnellen wat complex is

Wegnemen van obstakels

Rapporteren waar we staan

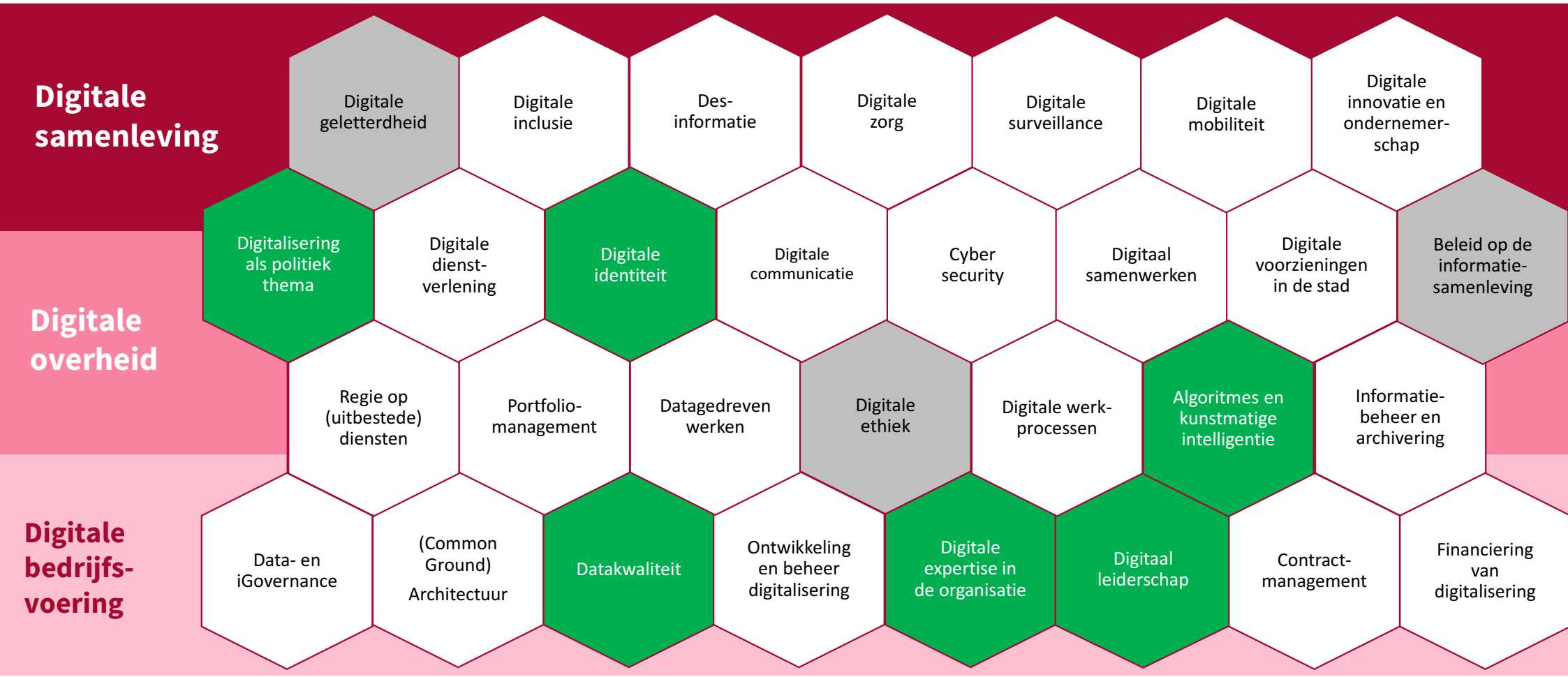
Vasthouden van aandacht

We doen nooit iets alleen in de opgave waar we zelf verantwoordelijk voor blijven

Opgavethema's

Opgave digitale transformatie

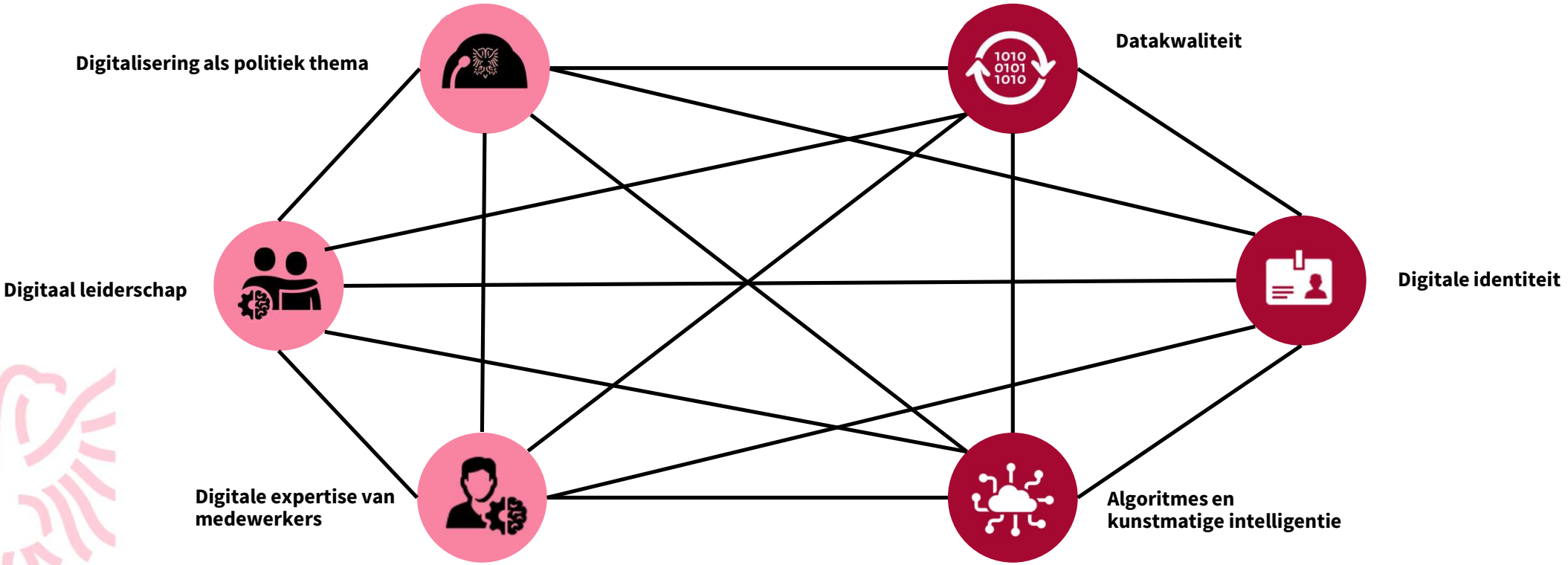
Scope opgave digitale transformatie



Huidige opgave digitale transformatie

Digitale verantwoordelijkheid en gedrag

Digitale voorzieningen en infrastructuur



5.1.2e 5.1.2e Product owner Digitalisering als politiek thema

Digitalisering als politiek thema

Maatschappelijke opgave

Bij veel onderwerpen waar gemeenteraadsleden om een oordeel wordt gevraagd, speelt digitale technologie een belangrijke rol. Of het nu gaat om de gemeentelijke dienstverlening, maatschappelijke ondersteuning, lokale economische ontwikkeling of het beheer en gebruik van openbare ruimte en infrastructuur. Steeds vaker wordt er gebruik gemaakt van digitale technologie. Digitale middelen zijn handig om de eigen dienstverlening te verbeteren of de openbare ruimte beter te benutten, maar is niet zonder risico's. Digitalisering beïnvloedt in positieve en negatieve zin de maatschappelijke verhoudingen, welzijn en welvaart in onze stad. En dat maakt digitalisering tot een politiek thema.

De gemeenteraad stuurt op hoofdlijnen en kan richting geven aan het college. Dit gebeurt meestal op maatschappelijke waarden, thema's en financiën. Hoewel de raad de afgelopen jaren steeds vaker over digitaliseringsthema's spreekt, zijn het beleid en de kaders voor de inzet en impact van digitale middelen de laatste jaren alleen door het College vastgesteld. Het is de opgave om van digitalisering een volwassen politiek thema te maken waarin raad en college sturen op publieke waarden in de digitale transformatie.

Doelen binnen dit opgavethema

1. We vergroten **de kennis, het bewustzijn en het urgentiegevoel bij de gemeenteraad en college**, zodat dilemma's bij digitalisering in de stad democratisch worden besproken en afgewogen.
2. We richten op basis van verwachtingen van de gemeenteraad en het college een **zorgvuldige werkwijze in voor het sturen op digitale thema's**, zodat het college kaders en richting heeft en de gemeenteraad hen daarop kan controleren en bijsturen.
3. We **implementeren de uitgewerkte sturingswijze in de P&C cyclus**, zodat de kaderstellende en controlerende rol structureel is ingericht.
4. We bieden voor de ambtelijke organisatie duidelijkheid **welke sturingswijze de gemeenteraad en het college hanteren** voor digitalisering zodat zij weten wat, wanneer en hoe daarover gerapporteerd moet worden.

Wat hebben we al bereikt?

- We organiseerden in maart 2023 een themamiddag 'Raad weten met digitalisering' voor de gemeenteraad waarin we een introductie gaven op de politieke aspecten van digitalisering en prioritaire thema's selecteerden in de digitale transformatie.
- We benutten één van de werkbezoeken van het college voor een inspiratiegesprek waarin het college in gesprek ging met experts uit verschillende werkvelden over de maatschappelijke impact van de digitale transformatie.
- We informeerden de gemeenteraad proactief over digitale ontwikkelingen en keuzes bij de inzet van de digitale identiteit Yivi
- Het college stelde een themagerichte aanpak vast voor de politieke sturing op digitalisering die is gedeeld met de raad, inclusief de vijf thema's waarover we hen actief informeren:
  - Privacy en informatieveiligheid
  - Digitale dienstverlening
  - Gegevensuitwisseling
  - Digitale geletterdheid en inclusie
  - Algoritmes en kunstmatige intelligentie
- In afstemming met de gemeenteraad zijn de kaders voor sturing op het thema privacy en informatiebeveiliging bepaald, inclusief indicatoren.

Geplande activiteiten 2024*

- We delen de eerste, jaarlijkse raadsinformatiebrief waarin we terug- en vooruitkijken op de vijf vastgestelde digitaliseringsthema's
- We delen een raadsinformatiebrief waarin aan de gemeenteraad wordt gerapporteerd over de indicatoren privacy en informatiebeveiliging
- De opgave Gemeentebrede Dienstverlening neemt het initiatief voor een themasessie met de gemeenteraad over (digitale) dienstverlening waarbij de opgave Digitale Transformatie ondersteunt
- We organiseren een themasessie met de gemeenteraad over gegevensuitwisseling.

* Onder voorbehoud, omdat activiteiten door voortschrijdend inzicht kunnen wijzigen

Vijf vastgestelde thema's voor politieke sturing op digitalisering

5.1.2e

5.1.2e

Product owner Digitaal leiderschap

Digitaal leiderschap

Maatschappelijke opgave

De wijze waarop Nijmegenaren onze producten en diensten aangeboden krijgen is afhankelijk van de keuzes die het management maakt of waar zij verantwoordelijkheid voor dragen. Het ontwikkelen en vergroten van het digitaal leiderschap van onze managers vergroot de kans dat publieke waarden en ethische kwesties bij innovatie en digitalisering zorgvuldig worden afgewogen. Denk bijvoorbeeld aan het:

- verbeteren van de dienstverlening aan inwoners en bedrijven door bijvoorbeeld het aanbieden van digitale diensten;
- verminderen van de administratieve last voor Nijmegenaren door het digitaliseren van formulieren en aanbieden van digitale selfservice mogelijkheden;
- verhogen van de participatie van inwoners en bedrijven in de besluitvorming door het gebruik van digitale platforms voor advies en inspraak;
- verhogen van de transparantie en toegankelijkheid van de gemeente door bijvoorbeeld het beschikbaar stellen van informatie via digitale kanalen.

Ook biedt aandacht voor digitaal leiderschap voordelen voor de bedrijfsvoering van gemeente Nijmegen. Zo kan verdere automatisering de efficiëntie van processen bevorderen. Maar ook bevorderen van digitale vaardigheden van medewerkers en sturing op benodigde digitale expertise bij het aantrekken van nieuwe medewerkers is onderdeel van digitaal leiderschap.

Doelen binnen dit opgavethema

1. We gebruiken een **eenduidig geformuleerde definitie van digitaal leiderschap**, zodat er meer duidelijkheid onder managers ontstaat over wat er van ze verwacht wordt
2. We **vergroten de kennis ("mindset") van managers** op het gebied van digitalisering en de impact op de benodigde sturing van gemeente Nijmegen, zodat er behoefte en urgentie ontstaat voor het verbeteren van hun eigen digitale leiderschap.
3. We **vergroten het vermogen ("skillset") van managers om randvoorwaarden te creëren** die nodig zijn om verantwoord met data en technologie om te gaan, zodat zij meer kunnen bijdragen aan de maatschappelijke opgaven en hun medewerkers beter kunnen faciliteren.
4. We maken het thema **digitaal leiderschap integraal onderdeel** van het **Management Development-programma**.

Wat hebben we al bereikt?

- Studenten van de Radboud Universiteit hielden interviews met managers en stelden een onderzoeksrapport op over digitaal leiderschap.
- Tijdens verschillende ambtelijke sessies is een richting bepaald voor de benodigde mindset en skillset van managers.
- In 2023 zijn twee workshops voor leidinggevenden georganiseerd:
  - Workshop ChatGPT. Doel van de workshop was om bewustzijn te creëren over de wijze waarop je ChatGPT kunt in kunt zetten, maar ook de risico's die er aan verbonden zijn.
  - Workshop Microsoft365. Doel van de workshop was om de leidinggevenden te informeren over de voortgang rondom de implementatie en de wijze waarop Microsoft365 kan helpen in de onderlinge samenwerking.
- Er is een werkprogramma voor 2024 opgesteld voor leidinggevenden met verschillende geplande activiteiten gericht op digitaal leiderschap.

Geplande activiteiten 2024*

- We organiseren een bewustwordingssessie met het GMT over het belang van digitaal leiderschap en managementverantwoordelijkheden bij digitalisering en brengen focus aan in de activiteiten voor 2024.
- We organiseren een workshop voor leidinggevenden over Microsoft365 en de wijze waarop leidinggevenden hun medewerkers kunnen ondersteunen bij deze nieuwe manier van digitaal samenwerken.
- We stellen een handleiding voor leidinggevenden op met adviezen voor gesprekken met medewerkers over digitale vaardigheden.
- We organiseren een workshop voor leidinggevenden over datagedreven werken.
- We brengen met een nieuwe promotiecampagne de trainingen over digitalisering/digitale vaardigheden op Studytube meer onder de aandacht bij leidinggevenden.
- We nemen digitaal leiderschap op in ROP's en vacatureteksten als onderdeel van de functie-eisen.
- We besteden in de week van de vitaliteit (oktober) ook aandacht aan digitale vitaliteit.
- We organiseren in de tweede helft van 2024 een inspiratiesessie over een actueel thema binnen de digitale transformatie (thema wordt nog bepaald).

* Onder voorbehoud, omdat activiteiten door voortschrijdend inzicht kunnen wijzigen

Digitale expertise van medewerkers

Vacant (zie geplande activiteiten 2024)
Product owner Digitale expertise van medewerkers

Maatschappelijke opgave

De manier waarop wij diensten aanbieden en communiceren met inwoners en bedrijven verloopt steeds meer digitaal. Nijmegenaren verwachten van ons als gemeente dat wij voor producten en diensten ook een digitale oplossingen bieden. Maar ook bij het aanbieden van een analoog alternatief gaat vaak intern een digitaal proces vooraf. Dit vraagt om medewerkers die weten hoe zij met deze digitale middelen moeten werken, welke kennis en gedrag daarbij gevraagd wordt en wat de mogelijke impact is van keuzes die ze maken en handelingen die ze uitvoeren.

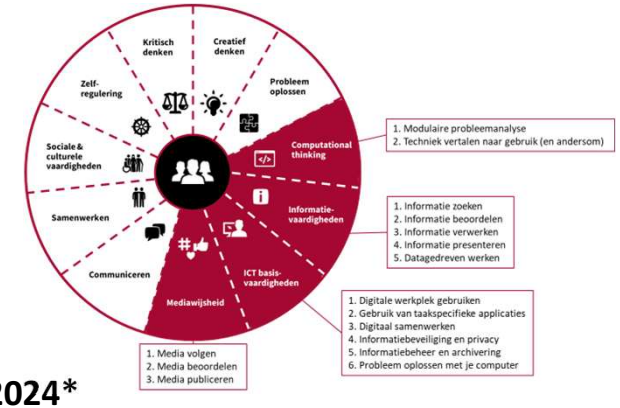
Betere digitale vaardigheden helpen om efficiënter te werken en beter in te kunnen spelen op de wensen en behoeften van Nijmegenaren. Het verkleint de risico's op datalekken, vergroot de kans op adoptie van innovatie, bevordert een goede afweging van publieke waarden en heeft niet in de laatste plaats ook een positieve invloed op het werkplezier van medewerkers. Steeds meer mensen verwachten dat ze op het werk kunnen werken met moderne technologie, maar ook met collega's die weten hoe ze daarmee om moeten gaan. Door de digitale expertise van onze eigen medewerkers te vergroten, worden we zo ook als werkgever aantrekkelijker voor nieuwe medewerkers.

Doelen binnen dit opgavethema

1. We **vergroten de kennis van medewerkers** op het gebied van de digitale transformatie en de impact voor gemeente Nijmegen, zodat er behoefte en urgentie ontstaat voor het verbeteren van hun eigen digitale expertise.
2. We **vergroten de vaardigheden van medewerkers** op het gebied van digitale tools en technologieën die relevant zijn voor hun werkzaamheden, zodat zij beter kunnen werken met digitale systemen, data, informatie en processen en zij nieuwsgierig, wendbaar en flexibel zijn bij het overstappen naar nieuwe digitale systemen of processen.
3. We **weten welke competenties er op hoofdlijnen voor medewerkers in onze organisatie nodig zijn**, zodat er gemeentebrede interventies gedaan kunnen worden om de digitale expertise van onze medewerkers kunnen vergroten
4. We hebben **een doelgroepgerichte aanpak** bij de inzet van interventies en communicatie voor het ontwikkelen van de digitale expertise van medewerkers**,** zodat deze interventies en communicatie aansluiten bij het werk en de belevingswereld van de medewerkers
5. We hebben **hulp aan medewerkers bij het gebruik van digitale tools georganiseerd**, zodat de vaardigheden van collega's en het verantwoord gebruik van digitale samenwerkingstools verbetert.

Wat hebben we al bereikt?

- We introduceerden vijf persona's in onze organisatie waarop we leeraanbod in digitale vaardigheden kunnen aanbieden
- We werkten de vier digitale vaardigheden van de 21e eeuwse vaardigheden concreter uit naar ontwikkelthema's waarop aanbod kan worden gecreëerd.
- Bijna 75% van de medewerkers van de gemeente Nijmegen volgden de leerlijn ransomware.
- We voerden een onderzoek uit onder medewerkers over hun leervoorkeuren en blik op digitale vaardigheden.
- We gingen met MT's in gesprek over de benodigde digitale vaardigheden voor de betreffende afdelingen.
- We hebben in onze organisatie een netwerk opgebouwd van +/- 100 digibuddies (verdeeld over alle afdelingen) die collega's gaan helpen bij het werken met MS365.
- We startten een projectgroep dat per doelgroep leerinterventies op de onderwerpen van de opgave Nijmegen van Nu bedenkt, prioriteert en coördineert (scrumteam Nijmegen van Nu). Het ontwikkelen van digitale vaardigheden is hier onderdeel van.



Geplande activiteiten 2024*

- We gaan vanaf juni 2024 werken met MS365 en gebruiken deze implementatie om medewerkers vaardiger te maken in het digitaal samenwerken.
- We bieden medewerkers en managers meerdere trainingen en workshops aan en nemen ze mee in de 'spelregels' bij gebruik van MS365.
- We breiden het aanbod van digitale vaardigheidstrainingen uit op NijmegenSchool
- We bieden een herhalingstraining informatiebewustzijn aan.
- We hebben extra aandacht voor phishingmails en het voorkomen van datalekken.
- We gaan een functie of rol creëren in de lijnorganisatie met specialisatie in (het aanleren van) archiveringsvaardigheden.
- We gaan een functie of rol creëren in de lijnorganisatie met specialisatie in (het aanleren van) digitale vaardigheden.
- We gaan met de iRvN in gesprek voor het geven van tooltrainingen aan medewerkers voor de tools waarover zij het functioneel beheer voeren.

* Onder voorbehoud, omdat activiteiten door voortschrijdend inzicht kunnen wijzigen

* Sommigen activiteiten overstijgen de verantwoordelijkheid van de opgave maar zijn voor de volledigheid wel opgenomen in de werkagenda

5.1.2e

5.1.2e

Product owner Datakwaliteit

Datakwaliteit

Maatschappelijke opgave

Vrijwel alle producten en diensten die we als gemeente Nijmegen aanbieden zijn gebaseerd op data. Om te weten of een riolering aan onderhoud toe is, of een Nijmegenaar in aanmerking komt voor een uitkering, of een parkeervergunning mag worden afgegeven. Het uitgangspunt hierbij is dat besluiten van de gemeente Nijmegen worden genomen op basis van kwalitatief goede data. Maar wanneer is die data nu goed? Of beter gezegd: goed genoeg? En als er onverhoopt iets misgaat, hoe merken we dat dan op en herstellen we dat? Wanneer besluiten worden genomen op basis van slechte data kunnen de gevolgen voor Nijmegenaren namelijk groot zijn, maar de impact verschilt nogal per product of dienst.

De gemeente Nijmegen moet borgen dat data onder alle omstandigheden beschikbaar is: tijdig, correct en volledig en alleen toegankelijk voor de juiste personen. Datagedreven werken helpt om de bedrijfsvoering efficiënter te maken en de kwaliteit van dienstverlening aan Nijmegenaren en bedrijven te verbeteren. De gemeente Nijmegen maakt zo nog meer impact bij de aanpak van maatschappelijke opgaven.

Doelen binnen dit opgavethema

1. We hanteren een **vastgestelde, gemeentebrede definitie van datakwaliteit**, zodat we transparant en eenduidig kunnen sturen
2. We geven i**nzicht in datasets en de kwaliteit** daarvan, zodat we kunnen prioriteren of en waar interventies gedaan moeten worden om de datakwaliteit te verbeteren
3. We richten per dataset een **totaal proces van inwinning tot gebruik inclusief terugmelding in**, zodat de datakwaliteit blijft voldoen aan de gestelde kwaliteitsregels
4. We zorgen ervoor dat we weten welke datakwaliteit per dataset nodig is, zodat medewerkers en Nijmegenaren kunnen **vertrouwen op de inhoud van het product of de dienst** die we als gemeente leveren.
5. We willen **voor iedere dataset van inwinning tot gebruik duidelijk en zichtbaar hebben hoe verantwoordelijkheden belegd zijn**, zodat we weten bij wie gerichte acties ter verbetering uitgezet kunnen worden

Wat hebben we al bereikt?

- We hebben het programma Datakwaliteit ontwikkeld dat per dataset bestaat uit:
  - een checklist voor data eigenaren om de benodigde rollen in te richten en vast te leggen;
  - het opstellen van kwaliteitsregels waaraan voldaan moet worden zodat deze ook gemonitord kunnen worden.
- We hebben in het GMT van augustus 2023 laten vaststellen dat we:
  - één gemeentebrede definitie hanteren voor datakwaliteit (zie grijs kader);
  - het programma Datakwaliteit in uitvoering brengen.
- We hebben een projectteam ingericht binnen het Datahuis met ondersteuning van het opgaveteam.
- We hebben een pilot doorlopen waarmee we een externe tool hebben getest op het meten van datakwaliteit. De pilot heeft ertoe geleid dat we besloten hebben zelf een tool te ontwikkelen door de data scientist van onze organisatie.
- Het projectteam heeft in de periode september 2023 tot februari 2024:
  - 16 gesprekken gevoerd met data-eigenaren waarmee het proces en inrichting van de benodigde rollen in beeld zijn gebracht. Aanvullend zijn er voor 15 processen oriënterende gesprekken gevoerd met data-eigenaren.
  - een tool ontwikkeld om per dataset tot kwaliteitsregels te komen en de kwaliteit van de gegevens in de dataset te meten. 4 datasets zijn inmiddels met de tool doorlopen. Voor twee datasets zijn de kwaliteitsregels vastgesteld, voor de andere twee zijn ze nog in bewerking.

Gemeentebrede definitie van datakwaliteit
Datakwaliteit is de mate waarin een dataverzameling de echte wereld representeert en bruikbaar is om publieke waarde te realiseren. De beoordeling van datakwaliteit bestaat uit een geborgd proces waarin alle benodigde rollen zijn ingevuld en monitoring van kwaliteitsregels die op drie niveaus wordt gedaan:
- technische kwaliteit: juiste indeling van de data (bijv. lengte van een telefoonnummer is correct)
- referentiële kwaliteit: juiste samenhang tussen verschillende data-entiteiten (bijv. naam hoort bij telefoonnummer)
- inhoudelijke kwaliteit: in juiste context met de 'echte' wereld (bijv. het telefoonnummer klopt ook echt)

Geplande activiteiten 2024*

- We leveren in afstemming met de data eigenaren in 2024 minimaal 10 verbeterplannen op waarin zowel proces als kwaliteit gegevens zijn opgenomen.
- We maken een dashboard in het eerste kwartaal waarmee we de voortgang visualiseren en waarmee we de gegevenskwaliteit per dataset in beeld brengen.
- We ontwikkelen een prioriteitenmatrix om keuzes te maken in de volgorde van de datasets.
- We gaan het programma datakwaliteit inpassen in de werkprocessen van de EI-teams.
- We gaan structurele capaciteit regelen voor het kunnen realiseren van het programma.

* Onder voorbehoud, omdat activiteiten door voortschrijdend inzicht kunnen wijzigen

5.1.2e 5.1.2e

Product owner Digitale identiteit

Digitale identiteit

Maatschappelijke opgave

Digitale zekerheid en zelfbeschikking zijn publieke waarden waar inwoners en bedrijven steeds meer om vragen. Fake news, catfishing en andere vormen van identiteitsfraude vragen om oplossingen die zekerheid bieden over authenticiteit. De overheid heeft zowel in de fysieke wereld als in de digitale wereld een grote rol bij het uitgeven van een betrouwbare digitale identiteiten, ook wel digitale bronidentiteit (DBI) genoemd. Ook is het wettelijk noodzakelijk dat de identiteit van een inwoner op een veilige en betrouwbare manier vastgesteld kan worden bij het aanvragen van publieksrechtelijke producten, diensten en uitwisselen van formele berichten.

Een digitale identiteit biedt Nijmegenaren en de gemeente zekerheid om op een vertrouwde manier digitaal zaken te regelen en helpt om vast te stellen of je met de juiste persoon te maken hebt. Een identiteit helpt om jezelf te identificeren, maar ook om grip te houden op welke eigenschappen (attributen) je voor welke dienst of welk product wil delen. Op Europees en landelijk niveau wordt er gewerkt aan digitale identiteiten op basis van attributen (zie uitleg Privacy by Design Foundation). Hiermee wordt veilig en privacyvriendelijk gebruik en uitgifte van identiteitsgegevens mogelijk. Een attribuut gebaseerde digitale identiteit bestaat naast een oplossing als DigiD. Het heeft een ander doel en is niet bedoeld als vervanging van DigiD. Een attribuut gebaseerde gegevensverwerking vraagt een andere werkwijze die ervoor zorgt dat we als gemeente minder gegevens gebruiken om een product of dienst te leveren (dataminimalisatie).

Doelen binnen dit opgavethema

1. We **stellen de attributen per taak, product of dienst vast inclusief de geldigheidsduur,** zodat het interne proces daarop (her)ingericht kan worden
2. We **publiceren een online attributenregister**, zodat Nijmegenaren kunnen zien welke attributen we voor welk proces verwerken.
3. We **helpen de Nijmegenaar bij het gebruik van Yivi en in het inladen van attributen in de wallet**, zodat ze op een juiste manier gebruik maken van Yivi
4. We **moedigen intern en extern het gebruik van Yivi aan**, zodat het gebruik van deze digitale identiteit wordt gestimuleerd
5. We **bieden Yivi als identificatiemiddel aan in onze online dienstverlening**, zodat Nijmegenaren alleen de gegevens kunnen delen die nodig zijn om een product of dienst te leveren
6. We **bereiden ons voor op landelijke en Europese wet- en regelgeving voor digitale identiteiten en wallets**, zodat we flexibel kunnen aansluiten op nieuwe ontwikkelingen.

Wat hebben we al bereikt?

- We geven Nijmegenaren de het mogelijk om op het Mijn Nijmegen portaal en enkele formulieren in te loggen met de digitale identiteit Yivi (als aanvulling op DigiD)
- We geven Nijmegenaren bij online aanvragen voortaan de mogelijkheid hun voorkeurskanaal aan te geven voor het communiceren met de gemeente.
- We gaven inhoudelijke afdelingen 15 adviezen over dataminimalisatie en Yivi voor online aan te vragen producten. Bij implementatie worden deze adviezen zoveel mogelijk doorgevoerd. Lukt dit niet door bijv. een benodigde technische aanpassing, een aanpassing in het proces of de verordening, dan wordt het op de roadmap gezet om later op te pakken.
- We geven procesverantwoordelijken en medewerkers van de afdeling uitleg over Yivi en moedigen het gebruik ervan aan.
- We hebben een start gemaakt met het attributenregister. Met belanghebbenden wordt deze verder verfijnd.
- We hebben periodiek contact met het ministerie van Binnenlandse Zaken over de ontwikkelingen van de NL referentiewallet en geven onze bevindingen en leerervaringen terug om het stelsel van wallets te verbeteren.
- We informeerden de gemeenteraad actief over de ontwikkelingen, kansen en beperkingen bij de implementatie van Yivi.

Geplande activiteiten 2024*

- We zorgen ervoor dat 80% van onze online dienstverlening is voorzien van de mogelijkheid om ook in te loggen met Yivi.
- We versimpelen processen voor de inwoner met gebruik van Yivi en passen waar mogelijk dataminimalisatie toe.
- We intensiveren de samenwerking met de Kamer van Koophandel om de dienstverlening voor bedrijven met Yivi te vereenvoudigen.
- We maken het mogelijk om met Yivi in te loggen op het belastingenportaal.
- We stellen het attributenregister online beschikbaar.
- We voeren gesprekken met de bibliotheek voor het bieden van hulp aan Nijmegenaren via de informatiepunten digitale overheid (IDO).
- We zorgen dat medewerkers bekend zijn met Yivi met een nog te bepalen activiteit of campagne.
- We blijven aan het ministerie van Binnenlandse Zaken onze bevindingen terugkoppelen om het stelsel van digitale wallets te verbeteren en blijven in gesprek om snel te kunnen anticiperen op landelijke ontwikkelingen van digitale wallets.
- We blijven de gemeenteraad actief informeren over bovengenoemde ontwikkelingen.

* Onder voorbehoud, omdat activiteiten door voortschrijdend inzicht kunnen wijzigen

Algoritmes en kunstmatige intelligentie

Maatschappelijke opgave

AI sinds de jaren ‘60 worden overheidstaken ondersteunt met digitale middelen. Automatisering is dan ook niet nieuw. Veel van de applicaties die we als gemeente gebruikten zijn al ingericht volgens algoritmische principes. De toegankelijkheid van deze techniek, de schaal waarop we als overheid onze taken automatiseren en aandacht voor de maatschappelijke implicaties ervan is de laatste jaren wel exponentieel gegroeid. ChatGPT heeft kunstmatige intelligentie (AI) - automatisering op basis van kansberekening - naar het grote publiek gebracht en heeft bovendien de schijnwerpers gezet op generatieve AI. Steeds meer leveranciers integreren nu ook (vormen van) kunstmatige intelligentie in hun applicaties. Dit alles levert nieuwe vraagstukken op:

- Waar automatisering eerst betekende ‘het technisch mogelijk maken van een vooraf gedefinieerd proces’ betekent het nu ook ‘het genereren van output op basis van kansberekening en waarschijnlijkheid.’ Dit betekent een fundamentele verandering van werk.
- De data die gebruikt worden om AI modellen te trainen zijn niet neutraal, beïnvloeden de output en dus de inhoud van processen.
- De inzet van algoritmes en AI bevordert de productiviteit van mensen en efficiency, maar niet altijd de kwaliteit van het werk.
- Het zorgt voor uitdagingen in vakmanschap en verhoudingen op afdelingen omdat er ook een groter verschil ontstaat in productiviteit tussen collega’s onderling.
- Automatisering heeft als bijeffect dat de uitvoering van processen minder zichtbaar wordt, maar we moeten kunnen blijven uitleggen hoe beslissingen tot stand zijn gekomen.

We willen voorkomen dat Nijmegenaren verstrikt raken in een systeemwerkelijkheid, maar willen ook de kansen van nieuwe technologie benutten om opgaven voor de stad te realiseren.

Doelen binnen dit opgavethema

1. We **bieden transparantie over de inzet van algoritmes en kunstmatige intelligentie**, zodat Nijmegenaren kunnen controleren waarvoor we deze technieken inzetten.
2. We laten **collega’s verantwoord experimenteren met (generatieve) AI**, zodat we werken aan hun ambtelijke vakmanschap.
3. We richten een **proces in voor de inzet van kunstmatige intelligentie**, zodat afwegingen en mogelijke bij-effecten zorgvuldig worden afgewogen.
4. We **bevorderen eenmalige registratie, meervoudig gebruik** bij het gebruik van registers, zodat we de administratielast verminderen en kwaliteit van de registraties bevorderen.
5. We **borgen de registratiewerkzaamheden in de lijnorganisatie**, zodat duidelijk is hoe en door wie de register worden bijgehouden.

Externe ontwikkelingen

- In maart 2022 is er een Tweede Kamer motie ingediend en aangenomen die het gebruik van het IAMA (op termijn) verplicht stelt.
- OpenAI lanceerde in november 2022 de eerste gratis versie van ChatGPT. Andere techbedrijven volgden snel met varianten.
- In december 2022 lanceerde de Rijksoverheid de eerste versie van het algoritmeregister. In januari 2024 werd ook de website gegevensbijbesluiten.overheid.nl geopend waarin je op kunt zoeken welke gegevens de overheid gebruikt bij het nemen van besluiten.
- In december 2023 heeft de EU een voorlopig akkoord bereikt over de AI Act waarmee de inzet van AI wordt gereguleerd.
- Het kabinet formuleerde in december 2023 voorlopig standpunt generatieve AI: “*Het gebruik van generatieve AI is toegestaan, als deze voldoet aan de geldende wet- en regelgeving. Om dit te controleren moet er per geval een risicoanalyse worden uitgevoerd.*”
- In januari 2024 presenteerde het kabinet hun visie op generatieve AI.
- De VNG werkt momenteel aan een handreiking verantwoord gebruik generatieve AI.

Wat hebben we al bereikt?

- We onderhouden en publiceren het verwerkingenregister waarmee we inzicht geven in het gebruik van persoonsgegevens.
- We voeren DPIA’s uit waarin we verantwoorden over de verwerking van persoonsgegevens.
- We stelden voor collega’s uitgangspunten op voor het gebruik van ChatGPT en andere vormen van generatieve AI.
- We zijn een pilot gestart waarin we de eerste algoritmes aan het landelijke algoritmeregister toevoegen.

Geplande activiteiten 2024*

- We bakenen de scope van het opgavethema algoritmes en kunstmatige intelligentie verder af
- We creëren leeraanbod voor het verantwoord gebruik van (generatieve) AI
- We starten een eigen pilot waarin we experimenteren met een eigen GPT tool als alternatief voor ChatGPT.
- We brengen de pilot voor het toevoegen van algoritmes aan het algoritmeregister onder bij de opgave digitale transformatie
- We onderzoeken harmonisatie en synchronisatie van de verschillende registers.
- We vertalen de Rijksvisie op generatieve AI, handreiking VNG (e.a. landelijke/Europese richtlijnen) naar beleid en uitgangspunten voor gemeente Nijmegen
- We organiseren de verantwoording en sturing op de inzet van algoritmes en kunstmatige intelligentie, waaronder IAMA’s (Impact Assesments Mensenrechten en Algoritmes)

* Onder voorbehoud, omdat activiteiten door voortschrijdend inzicht kunnen wijzigen. De doelen en activiteiten worden nog verder uitgewerkt met de te werven product owner.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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	4, 9, 10, 12, 13

0-pagina Collegevoorstel
Openbaar

Onderwerp
Vaststelling Verordening individuele inkomenstoeslag 2024

Opsteller	5.1.2e	**Behandeldatum**	16 april 2024
Programma	Werk en Inkomen	**Status**	Openbaar
Portefeuillehouder	J.A.R. Brom		

Advies

Aan de raad voor de stellen:

1. De Verordening individuele inkomenstoeslag 2017 in te trekken.
2. De Verordening individuele inkomenstoeslag 2024 vast te stellen, waarbij de belangrijkste wijziging is:
    a. Artikel 2: het mogelijk maken van ambtshalve toekenning voor inwoners die 36 maanden of langer een Participatiewetuitkering ontvangen en voldoen aan de vereisten. Zij krijgen de individuele inkomenstoeslag eenmaal per 12 maanden automatisch uitgekeerd. Het aanvraagformulier blijft bestaan voor overige rechthebbenden.

Opmerking

Tijdens de collegevergadering van 9 april 2024 wenste het college onderstaande punten uitgezocht te hebben voor een zorgvuldige afweging.

1. Een duidelijke definiëring wanneer er sprake is van geautomatiseerde besluitvorming door de lokale overheid.
Er is nog geen algemeen geaccepteerde definitie van een algoritme of een algoritmisch systeem. Wij als gemeente hanteren de volgende werkdefinitie van algoritme: “een set aan logische regels en instructies gericht op het oplossen van een probleem of bereiken van een doel, door interpretatie en vertaling van data.” Een algoritme is simpelweg een recept om ergens te komen, een "logisch model". Een strakke werkprocedure voor ambtenaren onder specifieke wetgeving en toezicht is daarmee ook een algoritme. Een algoritme is daarmee wel wat anders dan automatische besluitvorming. Van automatische besluitvorming is sprake indien een systeem zelfstandig aan de hand van een algoritme een besluit neemt op basis van data zonder menselijke tussenkomst of controle.

2. Welke documenten in het proces van de individuele inkomenstoeslag automatisch worden gegenereerd.
Op basis van een algoritme draaien we maandelijks een lijst uit met inwoners die recht hebben op ambtshalve toekenning. Hier staan zo’n 400 mensen per maand op. Deze lijst wordt gecontroleerd door een medewerker: klopt het aantal rechthebbenden op basis van wat je zou verwachten, staan er geen dubbelingen op, wat levert een steekproef van enkele rechthebbenden op? Vervolgens accordeert de medewerker de lijst. Na goedkeuring van de lijst worden de beschikkingen automatisch in bulk aangemaakt. Hierbij wordt gebruik gemaakt van dezelfde werkwijze als bij de energietoeslag.

3. Wat nodig is om te kunnen voldoen aan de wet (zoals de AVG).
De AVG staat aan het ambtshalve verstrekken niet in de weg. De doelgroep die we op het oog hebben voor de ambtshalve verstrekking is een groep waar we de gegevens al van verwerken in het kader van levensonderhoud/inkomensondersteuning. Deze ambtshalve verstrekking van de individuele inkomenstoeslag ligt in het verlengde van dat primaire doel. Daarmee is sprake van een zogeheten ‘verdere verwerking van persoonsgegevens die verenigbaar is met het oorspronkelijke doel’. De AVG staat een dergelijke verwerking toe. Wel vereist de AVG transparantie naar de betrokkene toe over hoe dit besluit tot stand is gekomen en op basis van welke gegevens dat besluit is genomen. Dit nemen we op in de beschikking. Het opnemen van algoritmes in het landelijk algoritmeregister is op dit moment nog niet verplicht, maar de verwachting is wel dat een dergelijke verplichting in de nabije toekomst er gaat komen.

Vervolgvel
1

---

4. De mogelijkheid om een bredere uitspraak te doen over geautomatiseerde besluitvorming.
Hier kunnen we geen sluitend antwoord op geven omdat dit per activiteit een eigen afweging vraagt. Bij beleidsvoorstellen waarbij automatisering als oplossing wordt voorgesteld wordt namelijk de beschrijving van de (geautomatiseerde) uitvoering van het werk maatschappelijk relevanter, omdat juist in de uitvoering waardenconflicten kunnen ontstaan. Dit vraagt in beleidsvoorstellen om een uitgebreidere beschrijving van de uitvoeringspraktijk. Om per geval de afweging te kunnen maken is beleid nodig onder welke voorwaarden (zowel organisatorisch, als juridisch als ethisch) wij automatisering aanvaardbaar vinden. Per geval zal aan de hand van deze voorwaarden een beoordeling nodig zijn of en hoe de voordelen opwegen tegen de potentiële negatieve bij-effecten. Aan beleid op algoritmes en kunstmatige intelligentie wordt momenteel weliswaar gewerkt, maar dat is er nog niet.

Aanpassing

- In het college- en raadsvoorstel is kanttekening 2.5 toegevoegd: ambtshalve toekennen is een vorm van geautomatiseerde besluitvorming.
- In het college- en raadsvoorstel is argument 2.3 aangevuld met een beschrijving van het uitvoeringsproces.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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

Nijmegen

Opdrachtbeschrijving sturing op algoritmes en AI

De wethouder digitalisering en directie zien beiden de noodzaak voor meer sturing op algoritmes en AI. Met deze opdrachtbeschrijving zetten we de verwachtingen op inhoud en proces neer voor deze beleidsopdracht.

Doel van de opdracht

Het doel is te komen tot:

- verantwoorde inzet van individuele beschikbare generatieve AI-tools door onze medewerkers;
- vastgestelde interne regels voor de inzet van algoritmes en AI;
- helderheid over bestuurlijke en ambtelijke verantwoordelijkheid op dit thema.

Dit voorstel sluit aan bij de volgende doelen van het programma ‘Bestuur en organisatie’:

- de belangrijkste risico's bij ons handelen zijn in beeld en worden beheerst;
- ons handelen is ethisch en in lijn met wet- en regelgeving;
- ons handelen is transparant en controleerbaar en er wordt verantwoording afgelegd;
- ons werk is slagvaardig en zorgvuldig uitgevoerd en volledig afgehandeld;
- ons werk is toekomstgericht en er wordt geleerd van het handelen om prestaties te verbeteren.

Definities van algoritmes en kunstmatige intelligentie

Er bestaan diverse beelden over wat te verstaan valt onder algoritmes en kunstmatige intelligentie. Binnen deze opdracht hanteren we de volgende definities:

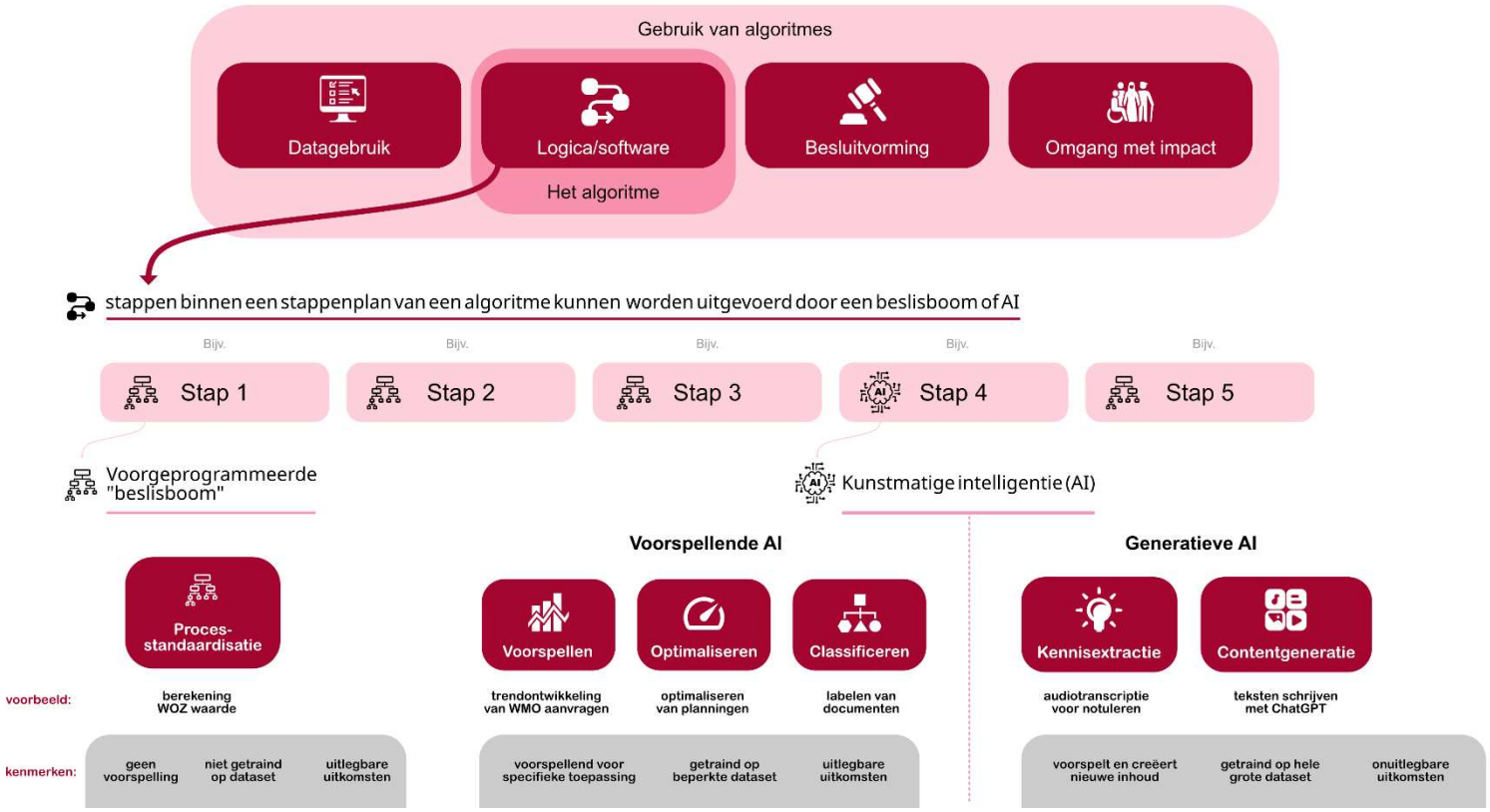
Algoritme

Er is nog geen algemeen geaccepteerde definitie van een algoritme, maar over het algemeen wordt gefocust op door computers uitgevoerde logica: een set aan logische regels en instructies gericht op het oplossen van een probleem of bereiken van een doel door interpretatie en vertaling van data. Een algoritme is kortgezegd een recept om ergens te komen.

Kunstmatige intelligentie

Ook voor kunstmatige intelligentie bestaat nog geen sluitende definitie. Binnen deze opdracht hanteren we de definitie zoals die ook in de Europese AI Act wordt gehanteerd: *“Een AI-systeem is een op een machine gebaseerd systeem dat is ontworpen om met verschillende niveaus van autonomie te werken en dat na het inzetten ervan aanpassingsvermogen kan vertonen, en dat, voor expliciete of impliciete doelstellingen, uit de ontvangen input afleidt hoe output te genereren zoals voorspellingen, inhoud, aanbevelingen of beslissingen die van invloed kunnen zijn op fysieke of virtuele omgevingen”* Een AI leert dus door statistiek toe te passen op data, genereert op basis daarvan output en kan daarmee een stap of stappen van een algoritme geautomatiseerd uitvoeren.

Binnen deze opdracht onderscheiden we in eerste instantie voorgeprogrammeerde algoritmes (beslisbomen) van kunstmatige intelligentie (AI). AI verdelen we vervolgens verder op in voorspellende en generatieve AI met ieder hun eigen toepassingen.



Scope

In de opdracht zullen we in ieder geval het geldende juridisch kader en aangekondigde wetgeving meenemen, zoals de Europese AI-verordening, Data Act, AVG en algemene beginselen van behoorlijk bestuur. We verwachten dat voor ‘eenvoudige’ algoritmes, voorspellende AI en generatieve AI verschillende risico’s en toepassingsmogelijkheden bestaan. De vorm te geven regels zullen met dit onderscheid rekening moeten houden. De focus van deze opdracht ligt op de omgang met AI-toepassingen, omdat we zien dat daar bestaande kaders te kort schieten. Wanneer de nieuwe kaders ook relevant zijn voor voorgeprogrammeerde algoritmes dan benoemen we dat.

Naast het soort algoritmes zien we kunstmatige intelligentie ook op verschillende manieren wortel schieten in onze organisatie. Binnen deze opdracht kijken we naar:

- het individueel gebruik van AI (zoals vrij toegankelijke generatieve AI en chatbots);
- leveranciers die (soms ongevraagd) AI-functionaliteit toevoegen aan applicaties;
- het inzetten van AI voor uitvoering van taken binnen werkprocessen;
- de ontwikkeling van eigen AI.

Zoals ook in de bepaling van de scope van dit opgavethema is afgesproken houden we de inzet van AI door Nijmegenaren of externe partijen waarmee wij geconfronteerd worden buiten scope. Ook de mogelijke impact van deze ontwikkeling op verhoudingen binnen

afdelingen (denk aan medewerkers die handig met AI zijn en hun collega's voorbijlopen) zullen we niet meenemen. Wel hebben we aandacht voor ethische aspecten, opleidingseisen en gevraagd digitaal leiderschap.

Bij de uitvoering van de opdracht volgen we de lijn van de (nog in ontwikkeling zijnde) landelijke beleidskaders en handreikingen, zoals:

- Principes voor de digitale samenleving (VNG, 2022)
- Overheidsbrede visie Generatieve AI (Rijksoverheid, 2024)
- Algoritmekader (Rijksoverheid, 2024)
- NDS: Nederlandse Digitaliseringsstrategie (Rijksoverheid, verwacht voorjaar 2025)

Ook het advies 'Kaders voor algoritmes' van de adviescommissie digitale ethiek dat momenteel in voorbereiding is input voor deze opdracht.

Opdrachtgeverschap en besluitvorming

Dit thema bevindt zich op het snijvlak van bestuurlijke en ambtelijke verantwoordelijkheid. Deze opdrachtbeschrijving gaat daarom uit van een gedeeld opdrachtgeverschap van de wethouder digitalisering en de directeur bedrijfsvoering. Onderdeel van dit beleidsproces is het verhelderen van bestuurlijke en ambtelijke aspecten bij de inzet van algoritmes en AI. Dit vraagt een open en onderzoekende houding van beide opdrachtgevers en afweging hoe zij respectievelijk het college en directie en/of GMT hierin mee willen nemen. Om die afweging te maken agenderen we gedurende het traject de deelonderwerpen in het PO digitalisering.

Resultaten en producten

We werken in deze opdracht toe naar een beleidsdocument dat gericht is op de interne organisatie waarin we de voorwaarden beschrijven voor de inzet van algoritmes en AI. Het stuk moet niet alleen uitgangspunten opleveren, maar ook doelstellingen die activerend werken. We volgen daarbij de richtlijnen van Frapper Toujours. De mate waarin college en raad betrokken zal worden zal ook het type document bepalen. De richtlijnen voor individueel gebruik van AI zijn het startpunt van dit traject wat we verder gaan uitbouwen. De directie is met deze richtlijnen al akkoord.

Uitvoerders en betrokken partijen

De opdracht zal worden uitgevoerd door het thema team 'Algoritmes en AI' binnen de opgave digitale transformatie met 5.1.2e als product owner en 5.1.2e als opgavetrekker. In dit multidisciplinaire team zit technische, juridische en inkoop expertise. Zij gaan intern in gesprek met inhoudelijke afdelingen waar op dit moment een AI-vraag speelt, maar ook met externe partijen (zoals de Radboud Universiteit) die over dezelfde vraagstukken nadenken. Andere betrokkenen als de CIO, CDO, CISO en functionaris gegevensbescherming zijn ook relevante interne stakeholders.

Benodigd budget en middelen

Los van de tijdsinvestering van betrokken partijen verwachten we geen aanvullend budget nodig te hebben voor de uitvoering van deze opdracht naast het al gevraagde werkbudget voor de opgave digitale transformatie.

Proces en tijdspad

We stellen voor het proces te volgen zoals eerder besproken met beide opdrachtgevers. Zie daarvoor bijlage “proces”. We verwachten een conceptversie in Q2 2025 te kunnen opleveren. Dit zal een tekst zijn waarmee we tussen opdrachtgevers een gesprek kunnen voeren over de verantwoordelijkheidsverdeling. Daarna volgen de stappen van bijschaven, afstemming en besluitvorming. Daar is de planning wat lastiger te bepalen vanwege de hoge afhankelijkheid van anderen. De ambitie is om in 2025 een vastgesteld beleid te hebben.

Bijlage 1. Proces uitvoering opdracht

Stap 1. Directie dezelfde informatiepositie over de opmars van AI

De opgave digitale transformatie geeft een presentatie aan de directie zodat zij dezelfde informatiepositie hebben als de wethouder. **(Afgerond)**

Stap 2. Gesprek wethouder en directie over opdrachtverstrekking

We organiseren een vervolggesprek waarin de wethouder in gesprek gaat met de directie en het opgaveteam over het verstrekken van een opdracht 'Sturing op algoritmes en AI'. **(Afgerond)**

Stap 3. Vaststelling en uitvoering opdracht

Wethouder digitalisering en directeur bedrijfsvoering geven akkoord op opdracht. Vervolgens gaat het opgaveteam aan de slag met de opdracht. Daarin nemen zij het advies mee van de adviescommissie Digitale Ethiek over kaders bij algoritmes. **(Huidige stap)**

Stap 4. Betrekken van het college, de gemeenteraad, directie en GMT

In het eerste kwartaal van 2025 informeren we over deze beleidsopdracht:

- het GMT en directie door de opdrachtbeschrijving ter informatie te delen;
- het college via een rondvraagmemo;
- de gemeenteraad via een raadsinformatiebrief.

Stap 5. Vaststelling door directie en college

Het document wordt via een directie- en collegevoorstel (incl. raadsbrief) ter besluitvorming voorgelegd aan het college en de directie.

Stap 6. Raadsbrief (informerend)

De vastgestelde raadsbrief wordt ter informatie met de gemeenteraad gedeeld.

Nijmegen

Bijlage 2. Richtlijnen gebruik AI

Inleiding

Met de lancering van ChatGPT raakte de ontwikkeling van AI in een stroomversnelling. We hebben daarna de eerste versie van onze principes voor het gebruik opgeschreven. Inmiddels zijn we ruim een jaar verder en is het tijd voor een update. We trekken de principes iets breder; we hebben het niet alleen over generatieve AI (zoals ChatGPT of afbeeldingsgeneratoren als Dall-E) maar ook over andere AI-toepassingen (zoals anonimiseringssoftware of kentekenscanners).

Als je AI-toepassingen wil gebruiken kan dat, als je je aan de volgende regels houdt. Op deze manier gebruiken we ze waar ze geschikt voor zijn. Heb je mooie voorbeelden uit je eigen praktijk? Ook dat horen we graag! Zo leren we samen beter werken met deze technologie.

Deze richtlijnen zijn gebaseerd op de kennis van nu (najaar 2024). Die kennis zal groeien. Daarom verversen we deze richtlijnen wanneer nodig.

1. Verdiep je in de mogelijkheden en beperkingen

AI is complex: het biedt veel kansen, maar er zitten ook haken en ogen aan. Zorg ervoor dat je daarvan op de hoogte bent en goed afgewogen de juiste tool kan gebruiken. Lees hier wat de beperkingen zijn.

2. Je bent zelf verantwoordelijk

Jij bent de expert en kent jouw vakgebied. Je bent verantwoordelijk voor je eigen werk. Als je een AI-hulpmiddel gebruikt blijft dat zo, net als wanneer je iets via Google opzoekt. Dat betekent ook dat je de resultaten uit de AI controleert vóór je ze gebruikt.

3. We delen geen gevoelige informatie

Vertrouwelijke informatie of persoonsgegevens delen we niet zomaar. Zeker niet met AI-chatbots of andere online hulpmiddelen. Alles wat je deelt wordt gebruikt door derden.

4. Zorg ervoor dat je de output kan beoordelen

Het kan dat een AI-tool foute resultaten genereert. Zorg ervoor dat je zelf kennis hebt over de inhoud, zodat je in staat bent de resultaten van de AI te herkennen en verbeteren.
Je kan een AI-tool dus niet vragen om een samenvatting van een tekst over een onderwerp waarvan je niet voldoende inhoudelijke kennis hebt. Je kunt namelijk niet beoordelen of er fouten in staan en/of de samenvatting goed is.

5. Gebruik AI niet meer dan nodig is

AI-toepassingen als ChatGPT en Copilot zijn gebaseerd op grote hoeveelheden informatie. Het verwerken daarvan vraagt veel rekenkracht en kost daardoor veel energie. Een vraag aan ChatGPT kost ongeveer 5 keer zo veel energie als eenzelfde vraag aan een zoekmachine als Google. Gebruik de juiste gereedschappen voor het werk. AI gebruik je als er geen beter gereedschap is.

Nijmegen

6. We doen een intake als we AI onderdeel willen maken van een werkproces

Wil je een AI-toepassing incidenteel gebruiken, bijvoorbeeld om je presentatie te verbeteren, of een alternatieve openingsparagraaf te krijgen voor je tekst? Volg dan bovenstaande regels. Wil je een toepassing structureel in een werkproces gaan gebruiken? Neem dan contact op met het opgaveteam Digitale Transformatie. We kijken dan met je mee. Zo zorgen we dat we verantwoord gebruik maken van de mogelijkheden van AI.

Het is nieuwe technologie, die snel verandert. Daarmee kunnen ook onze spelregels in de toekomst veranderen. Voor nu hanteren we deze spelregels.

Punten van aandacht bij bovenstaande regels:

- **Zorg voor context.** Een AI-model kent onze organisatie en jouw vraag niet. Beschrijf details over je probleem voor je je vraag stelt. Zo kan het gebruik maken van die informatie om een betere tekst te schrijven. Doe dit bij elke nieuwe 'chatsessie': Het model verandert tussendoor niet en gebruikt vaak niet de informatie die je in eerdere chatsessies hebt geschreven.
- Het is een techniek in opkomst, en daardoor **sterk veranderend**. Je kan er nog niet op vertrouwen dat het volgend jaar hetzelfde werkt, dus maak je werk niet afhankelijk van AI.
- De grote modellen achter de AI-tools worden maar af en toe bijgewerkt. Daardoor bevatten ze vaak niet de meest **actuele informatie**.
- Modellen worden getraind op veel openbaar beschikbare informatie, en bevatten dus ook **foute informatie**. Deze fouten liggen dus ook onder het antwoord wat jij krijgt.
- Elke AI heeft **vooroordelen** ingebakken, omdat de informatie waarmee deze getraind is dat ook heeft. Ben je hiervan bewust bij het stellen van vragen, en het gebruik van de antwoorden die je krijgt. Die kunnen diezelfde vooroordelen bevatten.
- Generatieve AI genereert antwoorden op basis van statistiek, niet op basis van kennis. Het kan dus **foute antwoorden** geven, wat ook wel 'hallucineren' wordt genoemd.
- De modellen zijn getraind op bestaande teksten en afbeeldingen. Delen van de uitvoer kunnen dus bestaan uit het werk van anderen, wat dus **plagiaat** is. Bovendien heb je niet zelf het auteursrecht op de teksten die voor je gegenereerd worden.
- AI is statistisch, dus bij dezelfde vraag is de kans groot dat je **wisselende antwoorden** krijgt. Daarmee werkt het fundamenteel anders dan de computersystemen die we tot nu toe gewend zijn.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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	3

Nijmegen

Onderwerp
Beleidsopdracht algoritmes en kunstmatige intelligentie

Opsteller	5.1.2e	**Behandeldatum**	N.t.b.
Programma	Bestuur en Organisatie	**Portefeuillehouder**	T.F.A. van Elferen

Kennisneming van
de beleidsopdracht algoritmes en kunstmatige intelligentie.

Inleiding
De opmars van kunstmatige intelligentie (hierna: AI) en algoritmes wordt steeds zichtbaarder in onze organisatie. Zo maken steeds meer collega's gebruik van vormen van generatieve AI (zoals ChatGPT), maar ook leveranciers voegen AI-toepassingen toe aan oplossingen die wij bij hen afnemen. Daarnaast wordt wet- en regelgeving steeds volwassener. Het is goed om daarbij te benadrukken dat niet iedere AI hetzelfde is. En Europese en landelijke wetgeving reguleert niet alles. Daarom werken we in opdracht van de wethouder digitalisering en directeur bedrijfsvoering aan beleidsregels voor de inzet van algoritmes en AI door gemeente Nijmegen.

Kernboodschap
We zien AI op verschillende manieren wortel schieten in onze organisatie. Binnen deze beleidsopdracht kijken we naar:

- het individueel gebruik van AI (zoals vrij toegankelijke generatieve AI en chatbots);
- leveranciers die (soms ongevraagd) AI-functionaliteit toevoegen aan applicaties;
- het inzetten van AI voor uitvoering van taken binnen werkprocessen;
- de eigen ontwikkeling van AI.

Deze beleidsopdracht is belegd bij de opgave digitale transformatie en bevindt zich op het snijvlak van bestuurlijke en ambtelijke verantwoordelijkheid. Onderdeel van dit beleidsproces is het verhelderen van deze verantwoordelijkheidsverdeling bij de inzet van algoritmes en AI. Daarom is gekozen voor een gedeeld opdrachtgeverschap van de wethouder digitalisering en directeur bedrijfsvoering.

We werken in deze beleidsopdracht toe naar voorwaarden voor de inzet van algoritmes en AI door de gemeente Nijmegen. Bij de uitvoering van deze opdracht sluiten we aan bij landelijke beleidskaders en handreikingen. Het doel is te komen tot:

- verantwoord, individueel gebruik van generatieve AI-tools door medewerkers;
- vastgestelde interne regels voor de inzet van algoritmes en AI in werkprocessen;
- helderheid over bestuurlijke en ambtelijke verantwoordelijkheid op dit thema.

De volledige reikwijdte van deze beleidsopdracht is uitgewerkt in de bijlage.

Vervolg
In het eerste kwartaal van 2025 wordt ook de gemeenteraad geïnformeerd over deze beleidsopdracht via een raadsinformatiebrief. De ambitie is om in het tweede kwartaal van 2025 een conceptversie van het beleid te bespreken met de opdrachtgevers en dat we voor het einde van het jaar dit beleid hebben vastgesteld.

Afdeling, naam, telefoonnummer
PI50, 5.1.2e, 5.1.2e

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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

GMT voorstel
Ter informatie

Onderwerp Opdracht algoritmes en kunstmatige intelligentie

Opsteller 5.1.2e & 5.1.2e
Programma Bestuur & Organisatie
Concernmanager 5.1.2e (als ambtelijk opdrachtgever opgave digitale transformatie)
Verantwoordelijk directeur 5.1.2e

Datum behandeling 29 januari 2025
Op iNsite: Ja

Kennisneming van
1. Kennis te nemen van de opdracht algoritmes en kunstmatige intelligentie

Inleiding
De opmars van kunstmatige intelligentie (hierna: AI) en algoritmes wordt steeds zichtbaarder in onze organisatie. Zo maken steeds meer collega's gebruik van vormen van generatieve AI (zoals ChatGPT), maar ook leveranciers voegen AI-toepassingen toe aan oplossingen die wij bij hen afnemen. Daarnaast wordt wet- en regelgeving steeds volwassener. Het is goed om daarbij te benadrukken dat niet iedere AI hetzelfde is. En Europese en landelijke wetgeving reguleert niet alles. Daarom werken we in opdracht van de wethouder digitalisering en directeur bedrijfsvoering aan beleidsregels voor de inzet van algoritmes en AI door gemeente Nijmegen.

Kernboodschap
We zien AI op verschillende manieren wortel schieten in onze organisatie. Binnen deze opdracht kijken we naar:

- het individueel gebruik van AI (zoals vrij toegankelijke generatieve AI en chatbots);
- leveranciers die (soms ongevraagd) AI-functionaliteit toevoegen aan applicaties;
- het inzetten van AI voor uitvoering van taken binnen werkprocessen;
- de eigen ontwikkeling van AI.

Deze opdracht is belegd bij de opgave digitale transformatie en bevindt zich op het snijvlak van bestuurlijke en ambtelijke verantwoordelijkheid. Onderdeel van dit beleidsproces is het verhelderen van deze verantwoordelijkheidsverdeling bij de inzet van algoritmes en AI. Daarom is gekozen voor een gedeeld opdrachtgeverschap van de wethouder digitalisering en directeur bedrijfsvoering.

We werken in deze opdracht toe naar voorwaarden voor de inzet van algoritmes en AI door de gemeente Nijmegen. Bij de uitvoering van deze opdracht sluiten we aan bij landelijke beleidskaders en handreikingen. Het doel is te komen tot:

- verantwoord, individueel gebruik van generatieve AI-tools door medewerkers;
- vastgestelde interne regels voor de inzet van algoritmes en AI in werkprocessen;
- helderheid over bestuurlijke en ambtelijke verantwoordelijkheid op dit thema.

De volledige reikwijdte van deze opdracht is uitgewerkt in de bijlage.

Communicatie
De komende weken wordt de organisatie actief geïnformeerd over de geactualiseerde spelregels bij het gebruik van AI. Deze zijn terug te vinden in de bijlage. Met de afdeling communicatie wordt nu gekeken welke strategie het beste is om zo veel mogelijk collega's te bereiken. Aan de concernmanagers wordt gevraagd of zij de bekendheid van deze geactualiseerde spelregels willen promoten. Daarnaast vindt er voor collega's op 27 februari een carrousel plaats die in het teken staat van kunstmatige intelligentie.

Vervolg
Tijdens de collegevergadering van 28 januari wordt het college geïnformeerd over deze opdracht via een rondvraagmemo. In het eerste kwartaal van 2025 wordt ook de gemeenteraad geïnformeerd via een raadsinformatiebrief. De ambitie is om in het tweede kwartaal van 2025 een conceptversie van het beleid te bespreken met de opdrachtgevers en dat we voor het einde van het jaar dit beleid hebben vastgesteld.

Bijlage(n)
1. 20240212 Opdrachtbeschrijving algoritmes en kunstmatige intelligentie

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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

Uitvoeringsagenda 2025

DIGITALE TRANSFORMATIE

27 februari 2025

Uitvoeringsagenda opgave digitale transformatie 2025

Waarom een uitvoeringsagenda?

Binnen de opgave digitale transformatie werken we aan digitale thema's waarop we als organisatie willen versnellen. De werkagenda geeft richting aan de opgave digitale transformatie en duidelijkheid aan de organisatie waarop we versnelling willen maken. Deze uitvoeringsagenda beschrijft welke doelen we per thema nastreven en welke activiteiten (interventies) we daarin voorzien. Omdat we agile werken bekijken we stap voor stap wat de juist interventies zijn per thema. We maken dus een inschatting van nuttige interventies, maar reflecteren continue op de effecten van eerdere interventies en bepalen volgens nieuwe stappen. Activiteiten en interventies moeten daarbij altijd terug te voeren zijn op de doelstellingen die we in deze uitvoeringsagenda hebben opgesteld.

Deze uitvoeringsagenda bouwt voort op afspraken en keuzes die in maart 2024 zijn gemaakt tijdens de jaarlijkse werksessie met de bestuurlijke en ambtelijke opdrachtgever over scope van de opgave digitale transformatie. Deze werkagenda blikt terug en vooruit op eerder vastgestelde thema's, presenteert nieuwe thema's die in aanmerking komen als nieuwe opgavethema's en adviseert over een vervolg.

Uitgangspunten waar we naar handelen

- We werken agile zodat we beter in staat zijn in te spelen op veranderingen wanneer de omgeving (zowel intern als extern) deze van ons vraagt;
- We betrekken belanghebbenden in een zo vroeg mogelijk stadium bij (geplande) interventies zodat we daadwerkelijk toegevoegde waarde kunnen creëren;
- We werken volgens het principe 'leading by doing', waarbij we medewerkers meenemen in de nieuwe manier(en) van werken zodat medewerkers niet alleen het resultaat zien maar ook meemaken hoe we daartoe komen;
- We communiceren proactief over resultaten, voortgang en knelpunten zodat we transparant te werk gaan;
- We reflecteren continu op resultaten na interventies, zodat we ervan leren en indien nodig passende interventies kunnen doen;
- We voldoen waar dat mogelijk is altijd aan privacy-, archivering- en security-by-design en vragen om advies bij ethische kwesties (o.a. bij de Adviescommissie Digitale Ethiek);
- We houden bij uitvoering van onze activiteiten altijd rekening met (aangekondigde) Europese en landelijke regel- en wetgeving;
- We volgen het informatiebeleid (DIB), de visie op dienstverlening en de visie op bedrijfsvoering.
- We stellen jaarlijks een uitvoeringsagenda op waarin we terug- en vooruitblikken op het verloop van de opgave digitale transformatie.

Opbouw van de werkagenda

De uitvoeringsagenda is opgebouwd vanuit een vaste structuur. De eerste pagina's van de agenda gaan over het hogere doel, wie waarvoor verantwoordelijk is en wanneer thema's in aanmerking komen als opgavethema. Vervolgens volgt een beschrijving van de inhoudelijke scope van de opgave met per thema een uitwerking van de maatschappelijke opgave, doelen, resultaten en geplande activiteiten.

Maatschappelijke opgave

Wat maakt dit voor een Nijmegenaar een belangrijk thema?

Doelen

Wat willen we binnen de opgave bereiken met dit thema?

Resultaten

Wat is er al bereikt in de opgave (of organisatie)?

Geplande activiteiten

Welke activiteiten of interventies zijn we van plan om uit te voeren?

Digitale transformatie

Missie: publieke waarden borgen in de gedigitaliseerde stad

1

Opgave
Juiste maatschappelijke randvoorwaarden voor digitale transformatie bereiken

Digitale samenleving

Geen digitale kansenongelijkheid
Privacy en autonomie geborgd
Digitaal veiligheid en gezondheid
Betrouwbare digitale infrastructuur
Bescherming menselijke waardigheid
Duurzaamheid in technologie

2

Opgave
Vertrouwen in moderne gemeente versterken en zelf digitaal transformeren

Digitale overheid

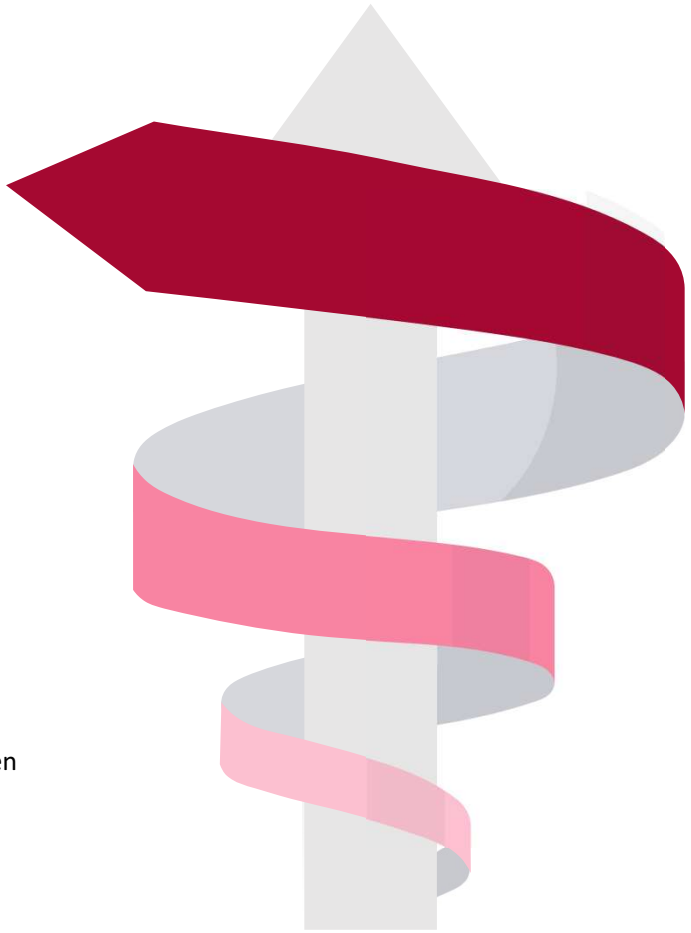
Verantwoorde en uitlegbare digitale processen
Inclusief en toegankelijk
Ruimte voor maatwerk
Als een platform opererend
Mens- en opgavegericht

3

Opgave
Juiste organisatorische randvoorwaarden voor digitale transformatie bereiken

Digitale bedrijfsvoering

Innovatief, digivaardig en datagestuurd
Integer en privacybeschermend
Continue afweging van publieke waarden
Inzet ICT onder regie en toezicht van mensen
Robuuste en veilige technologie



Opgave digitale transformatie

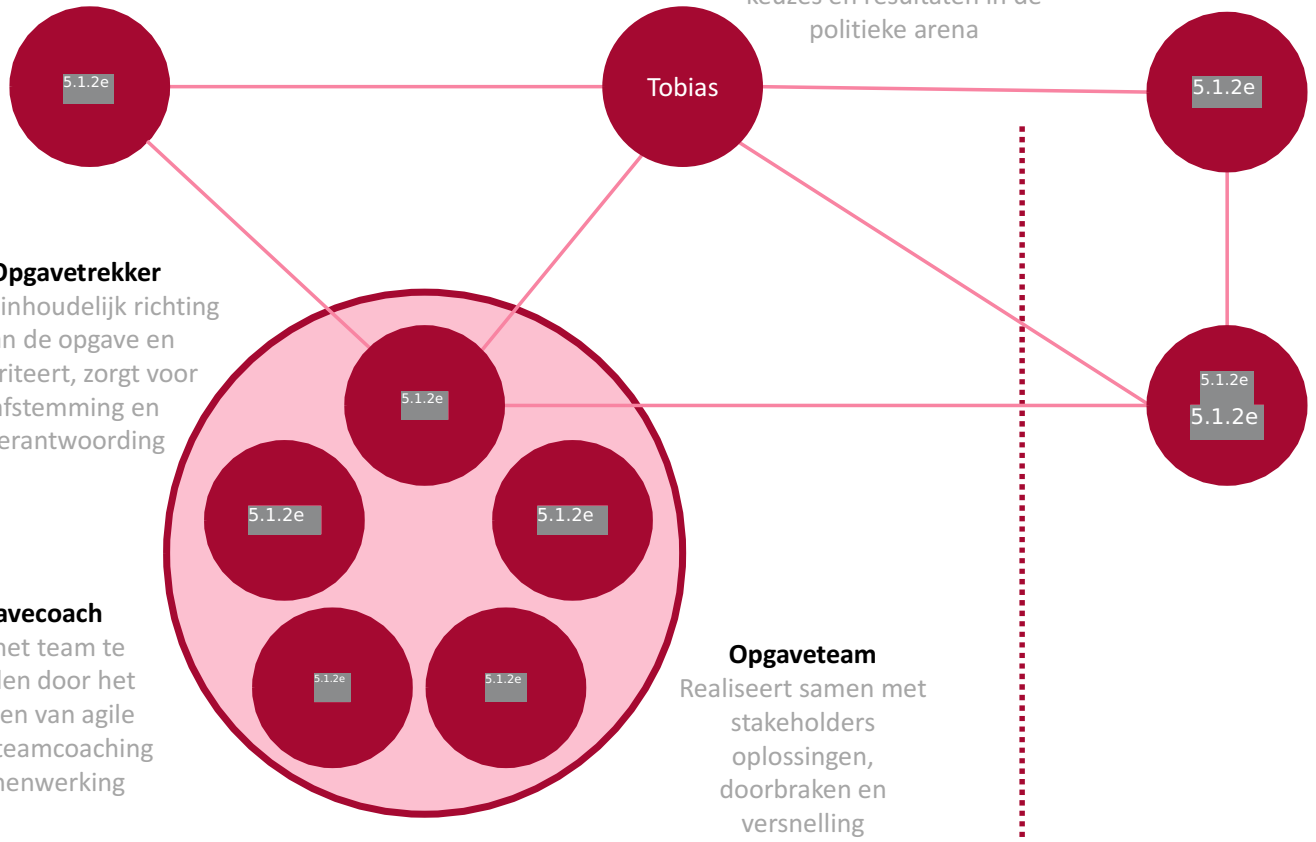
Versnelling en doorbraak

Bestuurlijk opdrachtgever (namens college)
Stelt vanuit bestuurlijk perspectief prioriteiten en maakt keuzes, zorgt voor samenhang met het coalitieakkoord en verdedigt keuzes en resultaten in de politieke arena

Programma digitalisering

Going concern

Ambtelijk opdrachtgever
Creëert de randvoorwaarden en neemt belemmeringen weg voor het opgaveteam



Concernmanager PIF
Creëert de randvoorwaarden en neemt belemmeringen weg voor het programma

Opgavetrekker
Geeft inhoudelijk richting aan de opgave en prioriteert, zorgt voor afstemming en verantwoording

CIO
Geeft inhoudelijk sturing aan de digitale thema's die buiten de opgave vallen

Opgavecoach
Helpt het team te versnellen door het faciliteren van agile werken, teamcoaching en samenwerking

Opgaveteam
Realiseert samen met stakeholders oplossingen, doorbraken en versnelling

Afbakening: welke activiteiten doen we als opgave?

Initiëren wat we nog niet doen

Versnellen wat complex is

Wegnemen van obstakels

Rapporteren waar we staan

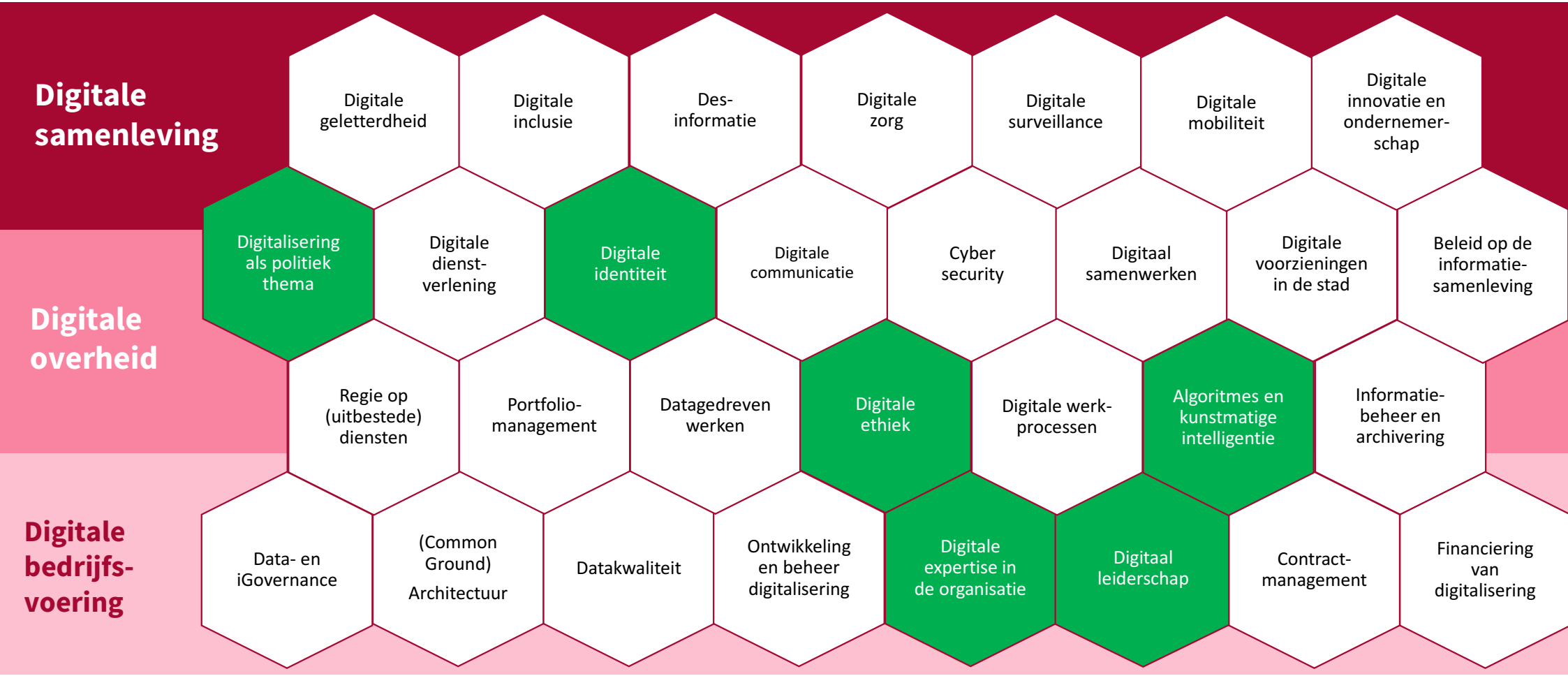
Vasthouden van aandacht

De opgave is een tijdelijk construct. Daarom moeten thema's en structurele activiteiten ook altijd door de lijnorganisatie geadopteerd kunnen worden.

Versnellingsthema's

Opgave digitale transformatie

Scope opgave digitale transformatie



Digitalisering als politiek thema

5.1.2e [redacted]
Product owner Digitalisering als politiek thema

Maatschappelijke opgave

Bij veel onderwerpen waar gemeenteraadsleden om een oordeel wordt gevraagd, speelt digitale technologie een belangrijke rol. Of het nu gaat om de gemeentelijke dienstverlening, maatschappelijke ondersteuning, lokale economische ontwikkeling of het beheer en gebruik van openbare ruimte en infrastructuur. Steeds vaker wordt er gebruik gemaakt van digitale technologie. Digitale middelen zijn handig om de eigen dienstverlening te verbeteren of de openbare ruimte beter te benutten, maar is niet zonder risico's. Digitalisering beïnvloedt in positieve en negatieve zin de maatschappelijke verhoudingen, welzijn en welvaart in onze stad. En dat maakt digitalisering tot een politiek thema.

De gemeenteraad stuurt op hoofdlijnen en kan richting geven aan het college. Dit gebeurt meestal op maatschappelijke waarden, thema's en financiën. Hoewel de raad de afgelopen jaren steeds vaker over digitaliseringsthema's spreekt, zijn het beleid en de kaders voor de inzet en impact van digitale middelen de laatste jaren alleen door het College vastgesteld. Het is de opgave om van digitalisering een volwassen politiek thema te maken waarin raad en college sturen op publieke waarden in de digitale transformatie.

Doelen binnen dit opgavethema

1. We vergroten **de kennis, het bewustzijn en het urgentiegevoel bij de gemeenteraad en college**, zodat dilemma's bij digitalisering in de stad democratisch worden besproken en afgewogen.
2. We richten op basis van verwachtingen van de gemeenteraad en het college een **zorgvuldige werkwijze in voor het sturen op digitale thema's**, zodat het college kaders en richting heeft en de gemeenteraad hen daarop kan controleren en bijsturen.
3. We **implementeren de uitgewerkte sturingswijze in de P&C cyclus**, zodat de kaderstellende en controlerende rol structureel is ingericht.
4. We bieden voor de ambtelijke organisatie duidelijkheid **welke sturingswijze de gemeenteraad en het college hanteren** voor digitalisering zodat zij weten wat, wanneer en hoe daarover gerapporteerd moet worden.

Vijf vastgestelde thema's voor politieke sturing op digitalisering

Wat hebben we al bereikt?

- We organiseerden in maart 2023 een themamiddag 'Raad weten met digitalisering' voor de gemeenteraad waarin we een introductie gaven op de politieke aspecten van digitalisering en prioritaire thema's selecteerden in de digitale transformatie.
- We benutten één van de werkbezoeken van het college voor een inspiratiegesprek waarin het college in gesprek ging met experts uit verschillende werkvelden over de maatschappelijke impact van de digitale transformatie.
- We informeerden de gemeenteraad proactief over digitale ontwikkelingen en keuzes bij de inzet van de digitale identiteit Yivi
- Het college stelde een themagerichte aanpak vast voor de politieke sturing op digitalisering die is gedeeld met de raad, inclusief de vijf thema's waarover we hen actief informeren:
    - Privacy en informatieveiligheid
    - Digitale dienstverlening
    - Gegevensuitwisseling
    - Digitale geletterdheid en inclusie
    - Algoritmes en kunstmatige intelligentie
- In afstemming met de gemeenteraad zijn de kaders voor sturing op het thema privacy en informatiebeveiliging bepaald, inclusief indicatoren.
- We informeerden de gemeenteraad actief over de ontwikkelingen, kansen en beperkingen bij de implementatie van de digitale identiteit Yivi.
- De opgave Gemeentebrede Dienstverlening organiseerde een themasessie met de gemeenteraad over (digitale) dienstverlening

Geplande activiteiten 2025 *

- We delen de opdracht algoritmes en AI met de gemeenteraad middels een raadinformatiebrief
- We delen een raadsinformatiebrief over gegevensuitwisseling en –gebruik met de gemeenteraad en organiseren een themasessie indien daar behoefte aan is.
- We delen onze voortgang en inzichten over digitale identiteit met de gemeenteraad in de vorm van een raadsinformatiebrief en organiseren een workshop over ID wallets indien daar behoefte aan is..
- We verkennen de mogelijkheid en toegevoegde waarde van een startnotitie digitale transformatie die we met de gemeenteraad kunnen delen.

** Onder voorbehoud, omdat activiteiten door voortschrijdend inzicht kunnen wijzigen*

Digitale expertise van medewerkers

Maatschappelijke opgave

De manier waarop wij diensten aanbieden en communiceren met inwoners en bedrijven verloopt steeds meer digitaal. Nijmegenaren verwachten van ons als gemeente dat wij voor producten en diensten ook digitale oplossingen bieden. Maar ook bij het aanbieden van een analoog alternatief gaat meestal intern een digitaal proces vooraf. Dit vraagt om medewerkers die weten hoe zij met deze digitale middelen moeten werken, welke kennis en gedrag daarbij gevraagd wordt en wat de mogelijke impact is van keuzes die ze maken en handelingen die ze uitvoeren.

Betere digitale vaardigheden helpen om efficiënter te werken en beter in te kunnen spelen op de wensen en behoeften van Nijmegenaren. Het verkleint de risico's op datalekken, vergroot de kans op adoptie van innovatie, bevordert een goede afweging van publieke waarden en heeft niet in de laatste plaats ook een positieve invloed op het werkplezier van medewerkers. Steeds meer mensen verwachten dat ze op het werk kunnen werken met moderne technologie, maar ook met collega's die weten hoe ze daarmee om moeten gaan. Door de digitale expertise van onze eigen medewerkers te vergroten, worden we zo ook als werkgever aantrekkelijker voor nieuwe mederkers

Doelen binnen dit opgavethema

1. We **vergroten de kennis van medewerkers** op het gebied van de digitale transformatie en de impact voor gemeente Nijmegen, zodat er behoefte en urgentie ontstaat voor het verbeteren van hun eigen digitale expertise.
2. We **vergroten de vaardigheden van medewerkers** op het gebied van digitale tools en technologieën die relevant zijn voor hun werkzaamheden, zodat zij beter kunnen werken met digitale systemen, data, informatie en processen en zij nieuwsgierig, wendbaar en flexibel zijn bij het overstappen naar nieuwe digitale systemen of processen.
3. We **weten welke competenties er op hoofdlijnen voor medewerkers in onze organisatie nodig zijn**, zodat er gemeentebrede interventies gedaan kunnen worden om de digitale expertise van onze medewerkers kunnen vergroten.
4. We hebben **een doelgroepgerichte aanpak** bij de inzet van interventies en communicatie voor het ontwikkelen van de digitale expertise van medewerkers**,** zodat deze interventies en communicatie aansluiten bij het werk en de belevingswereld van de medewerkers.
5. We hebben **hulp aan medewerkers bij het gebruik van digitale tools georganiseerd**, zodat de vaardigheden van collega's en het verantwoord gebruik van digitale samenwerkingstools verbetert.

5.1.2e

5.1.2e

Product owner Digitale expertise van medewerkers

Wat hebben we al bereikt?

- We hebben een adviseur leren en ontwikkelen geworven, die sinds januari 2025 tevens product owner is voor het ontwikkelen van de digitale expertise van medewerkers.
- Ruim 70% van de medewerkers van de gemeente Nijmegen volgden in 2024 de herhalingstraining Informatiebewustzijn.
- We initieerde het scrumteam Nijmegen van Nu waarin verschillende ontwikkeltrajecten van onze medewerkers (digitalisering, dienstverlening, participatie) geprioriteerd en gecoördineerd kunnen worden. Inmiddels functioneert dit team op eigen kracht en is het onder de naam 'Team Ambtelijk Vakmanschap' een pijler onder het programma Organisatieontwikkeling.
- We voerden een onderzoek uit onder medewerkers over hun leervoorkeuren en blik op digitale vaardigheden.
- We hebben in onze organisatie een netwerk opgebouwd van +/- 120 digibuddies (verdeeld over alle afdelingen) die collega's gaan helpen bij het werken met MS365.
- Digitale expertise van medewerkers is onderdeel van de vaardighedenmatrix voor Ambtelijk Vakmanschap (zie printscreen hiernaast) en daarmee een bouwsteen voor het programma Organisatieontwikkeling. In de vaardighedenmatrix zijn de verwachtingen op het gebied van digitale vaardigheden voor de komende tijd benoemd. Per onderwerp is beschreven waarom dit belangrijk is, wat een medewerker moet kennen/kunnen en waar meer informatie of training te vinden is. Daar waar nodig, is onderscheid gemaakt in persona's.
- We droegen bij aan de implementatie van Microsoft 365, o.a. door het organiseren van informatiesessies voor medewerkers, digibuddies en trainingen in de Nijmegenschool.
- We schreven een (ambtelijke) visie op digitale vaardigheden als bouwsteen voor het ambtelijk vakmanschap van onze medewerkers.

Digitale vaardigheden

	Op orde	Nog op ontwikkelen	Actie dit jaar
Gebruik digitale werkplek/ algemene kantoorapplicaties (o.a. Microsoft Word, Powerpoint, iNsite)	○	○	□
Digitaal samenwerken	○	○	□
Archiveren	○	○	□
Informatiebeveiliging/ -bewustzijn	○	○	□
Privacy (bijv. omgaan met persoonsgegevens en AVG)	○	○	□

	Op orde	Nog op ontwikkelen	Actie dit jaar
Gebruik afdelings-/taak-specifieke applicaties (zoals Suite, Coda)	○	○	□
Datagedreven werken (bijv. data begrijpen en gebruiken voor je werk)	○	○	□
Probleem oplossen op je computer	○	○	□
Zoekvaardigheden/ informatie zoeken	○	○	□

Geplande activiteiten 2025 *

- We starten begin 2025 met de testfase van de vaardighedenmatrix voor het ontwikkelen van ambtelijk vakmanschap van medewerkers. Digitale vaardigheden van medewerkers maakt hier onderdeel vanuit.
- Digitaal samenwerken is in 2025 een jaarthema vanuit ambtelijk vakmanschap. Dat betekent dat er gemeentebreed extra aandacht is voor dit onderwerp. Denk hierbij aan communicatie en training op het samenwerken en vergaderen met Microsoft Teams.
- We maken de kennisbank voor ambtelijk vakmanschap toegankelijk waarin ook de gevraagde digitale vaardigheden voor medewerkers zijn opgenomen. We beschrijven daarin per thema het **waarom, wat** en **hoe**.
- We verbeteren het aanbod aan digitale vaardigheidstrainingen voor medewerkers op StudyTube en de NijmegenSchool.
- We gaan een rol creëren in de lijnorganisatie met specialisatie in (het aanleren van) archiveringsvaardigheden.
- We gaan met de iRvN in gesprek voor het geven van gebruikerstrainingen aan medewerkers voor de tools waarover zij het functioneel beheer voeren.
- We bieden trainingen aan op het gebied van informatiebewustzijn, privacy en kunstmatige intelligentie.
- We zetten interne communicatiemiddelen in om de ontwikkeling in digitale vaardigheden te stimuleren.

** Onder voorbehoud, omdat activiteiten door voortschrijdend inzicht kunnen wijzigen. Sommigen activiteiten overstijgen de verantwoordelijkheid van de opgave omdat we intensief samenwerken met andere trajecten als Microsoft 365 en het programma Organisatieontwikkeling. Voor de volledigheid hebben we die activiteiten wel opgenomen in deze uitvoeringsagenda.*

Digitale verantwoordelijkheid en gedrag

Digitaal leiderschap

5.1.2e

5.1.2e

Product owner Digitaal leiderschap

Maatschappelijke opgave

De wijze waarop Nijmegenaren onze producten en diensten aangeboden krijgen is afhankelijk van de keuzes die het management maakt of waar zij verantwoordelijkheid voor dragen. Het ontwikkelen en vergroten van het digitaal leiderschap van onze managers vergroot de kans dat publieke waarden en ethische kwesties bij innovatie en digitalisering zorgvuldig worden afgewogen. Denk bijvoorbeeld aan het:

- verbeteren van de dienstverlening aan inwoners en bedrijven door bijvoorbeeld het aanbieden van digitale diensten;
- verminderen van de administratieve last voor Nijmegenaren door het digitaliseren van formulieren en aanbieden van digitale selfservice mogelijkheden;
- verhogen van de participatie van inwoners en bedrijven in de besluitvorming door het gebruik van digitale platforms voor advies en inspraak;
- verhogen van de transparantie en toegankelijkheid van de gemeente door bijvoorbeeld het beschikbaar stellen van informatie via digitale kanalen.

Ook biedt aandacht voor digitaal leiderschap voordelen voor de bedrijfsvoering van gemeente Nijmegen. Zo kan verdere automatisering de efficiëntie van processen bevorderen. Maar ook bevorderen van digitale vaardigheden van medewerkers en sturing op benodigde digitale expertise bij het aantrekken van nieuwe medewerkers is onderdeel van digitaal leiderschap.

Doelen binnen dit opgavethema

1. We gebruiken een **eenduidig geformuleerde definitie van digitaal leiderschap**, zodat er meer duidelijkheid onder managers ontstaat over wat er van ze verwacht wordt
2. We **vergroten de kennis ("mindset") van managers** op het gebied van digitalisering en de impact op de benodigde sturing van gemeente Nijmegen, zodat er behoefte en urgentie ontstaat voor het verbeteren van hun eigen digitale leiderschap.
3. We **vergroten het vermogen ("skillset") van managers om randvoorwaarden te creëren** die nodig zijn om verantwoord met data en technologie om te gaan, zodat zij meer kunnen bijdragen aan de maatschappelijke opgaven en hun medewerkers beter kunnen faciliteren.
4. We maken het thema **digitaal leiderschap integraal onderdeel** van het **Management Development-programma**.

Skillset Mindset

Wat hebben we al bereikt?

- Studenten van de Radboud Universiteit hielden interviews met managers en stelden een onderzoeksrapport op over digitaal leiderschap.
- Tijdens verschillende ambtelijke sessies is een richting bepaald voor de benodigde mindset en skillset van managers.
- Voor het GMT is een bewustwordingssessie georganiseerd over het belang van digitaal leiderschap en managementverantwoordelijkheden bij digitalisering.
- In 2023 en 2024 zijn workshops voor leidinggevenden georganiseerd:
    - Workshop ChatGPT over de mogelijkheden en de risico's die verbonden zijn aan het gebruik van ChatGPT.
    - Meerdere workshops over Microsoft365. Doel van de workshop was om de leidinggevenden te informeren over de implementatie en de wijze waarop Microsoft365 kan helpen in de onderlinge samenwerking.
- Er zijn twee online trainingen ontwikkeld, namelijk digitaal leiderschap en digitaal samenwerken voor leidinggevenden.
- Er is een koplopersgroep betere digitalisering gevormd, bestaande uit leidinggevenden die ervaringen en inspiratie uitwisselen op gebied van digitaal werken.

Geplande activiteiten 2025 *

- We organiseren een workshop voor leidinggevenden over Microsoft365 en de wijze waarop leidinggevenden hun medewerkers kunnen ondersteunen bij het digitaal samenwerken (meer focus op overzetten van documenten van de g-schijf naar Teams).
- We organiseren een workshop voor leidinggevenden over datagedreven werken.
- We organiseren een workshop voor leidinggevenden over een relevant en actueel digitaal thema voor de organisatie (bijvoorbeeld over algoritmes en kunstmatige intelligentie).
- We delen de ervaringen van de koplopersgroep digitale transformatie met een bredere groep leidinggevenden.
- We werken binnen het GMT aan de bewustwording van het ontwikkelen van hun eigen digitaal leiderschap (skillset en mindset).
- We adviseren en ondersteunen leidinggevenden bij het sturen op de ontwikkeling van digitale vaardigheden van medewerkers.
- We introduceren de leerlijn digitaal leiderschap. Deze zal toegevoegd worden aan de leerlijnen voor nieuwe leidinggevenden en wordt onder de aandacht gebracht van de zittende leidinggevenden.
- We voegen digitaal leiderschap toe aan de vaardighedenmatrix voor het ontwikkelen van ambtelijk vakmanschap.
- We maken digitaal leiderschap onderdeel van de nieuw te schrijven visie op leidinggeven (vanuit leidinggeven aan verandering).

** Onder voorbehoud, omdat activiteiten door voortschrijdend inzicht kunnen wijzigen. Sommigen activiteiten overstijgen de verantwoordelijkheid van de opgave omdat we intensief samenwerken met andere trajecten als Microsoft 365 en het programma Organisatieontwikkeling. Voor de volledigheid hebben we die activiteiten wel opgenomen in deze uitvoeringsagenda.*

5.1.2e

5.1.2e

Product owner Digitale identiteit

Digitale identiteit

Maatschappelijke opgave

Digitale zekerheid en zelfbeschikking zijn publieke waarden waar inwoners en bedrijven steeds meer om vragen. Fake news, catfishing en andere vormen van identiteitsfraude vragen om oplossingen die zekerheid bieden over authenticiteit. De overheid heeft zowel in de fysieke wereld als in de digitale wereld een grote rol bij het uitgeven van een betrouwbare digitale identiteiten, ook wel digitale bronidentiteit (DBI) genoemd. Ook is het wettelijk noodzakelijk dat de identiteit van een inwoner op een veilige en betrouwbare manier vastgesteld kan worden bij het aanvragen van publieksrechtelijke producten, diensten en uitwisselen van formele berichten.

Een digitale identiteit biedt Nijmegenaren en de gemeente zekerheid om op een vertrouwde manier digitaal zaken te regelen en helpt om vast te stellen of je met de juiste persoon te maken hebt. Een identiteit helpt om jezelf te identificeren, maar ook om grip te houden op welke eigenschappen (attributen) je voor welke dienst of welk product wil delen. Op Europees en landelijk niveau wordt er gewerkt aan digitale identiteiten op basis van attributen (zie uitleg Privacy by Design Foundation). Hiermee wordt veilig en privacyvriendelijk gebruik en uitgifte van identiteitsgegevens mogelijk. Een attribuut gebaseerde digitale identiteit bestaat naast een oplossing als DigiD. Het heeft een ander doel en is niet bedoeld als vervanging van DigiD. Een attribuut gebaseerde gegevensverwerking vraagt een andere werkwijze die ervoor zorgt dat we als gemeente minder gegevens gebruiken om een product of dienst te leveren (dataminimalisatie).

Doelen binnen dit opgavethema

1. We **stellen de attributen per taak, product of dienst vast inclusief de geldigheidsduur,** zodat het interne proces daarop (her)ingericht kan worden
2. We **helpen de Nijmegenaar bij het gebruik van Yivi en in het inladen van attributen in de wallet**, zodat ze op een juiste manier gebruik maken van Yivi
3. We **moedigen intern en extern het gebruik van Yivi aan**, zodat het gebruik van deze digitale identiteit wordt gestimuleerd
4. We **bieden Yivi als identificatiemiddel aan in onze online dienstverlening**, zodat Nijmegenaren alleen de gegevens kunnen delen die nodig zijn om een product of dienst te leveren
5. We **bereiden ons voor op landelijke en Europese wet- en regelgeving voor digitale identiteiten en wallets**, zodat we flexibel kunnen aansluiten op nieuwe ontwikkelingen.
6. We **verbeteren de dienstverlening voor de Nijmegenaar**, zodat het de Nijmegenaar minder moeite kost om producten en diensten online aan te vragen.
7. We zijn **transparant over de gegevens (attributen) die we per dienst of product** uitvragen, zodat vooraf bij Nijmegenaren bekend is welke gegevens nodig zijn om de aanvraag in behandeling te kunnen nemen.

Wat hebben we al bereikt?

- Nijmegenaren hebben de mogelijkheid om op het Mijn Nijmegen portaal en 80% van onze online aanvragen in te loggen met de digitale identiteit Yivi (als aanvulling op DigiD). We hebben hiervoor ook de benodigde attributen verder uitgewerkt.
- We gaven inhoudelijke afdelingen 90 adviezen over dataminimalisatie en Yivi voor online aan te vragen producten. Bij implementatie worden deze adviezen zoveel mogelijk doorgevoerd. Lukt dit niet door bijv. een benodigde technische aanpassing, een aanpassing in het proces of de verordening, dan wordt het op de roadmap gezet om later op te pakken.
- We verkennen met behulp van het innovatiebudget van het ministerie van Binnenlandse Zaken samen met andere overheden, leveranciers en onderzoeksbureaus hoe we de inzet van ID-wallets zoals Yivi kunnen verbeteren in het sociaal domein.
- We hebben feedback gegeven aan het ministerie van Binnenlandse Zaken (BZK) over de ontwikkelingen van de NL referentiewallet en organiseerden samen met hen beproevingsdagen van de NL-wallet.
- We geven procesverantwoordelijken en medewerkers uitleg over Yivi en moedigen het gebruik ervan aan.
- We hebben het bewustzijn van medewerkers vergroot door diverse acties.
- We hebben een juridische second opinion laten uitvoeren door het bureau ICTrecht op de rechtmatige inzet van Yivi.
- We informeerden de gemeenteraad actief over de ontwikkelingen, kansen en beperkingen bij de implementatie van Yivi.

Geplande activiteiten 2025 *

- We sluiten de laatste 20% van onze online dienstverlening aan op Yivi, voeren gesprekken met de afdelingen over dataminimalisatie en nemen de uitkomsten daarvan op in ons attributenregister.
- We maken het mogelijk om met Yivi in te loggen op het belastingenportaal, OpenStad en formulieren burgerzaken.
- We passen Yivi toe als alternatief voor eHerkenning.
- We intensiveren de samenwerking met de Kamer van Koophandel om de dienstverlening voor bedrijven met Yivi te vereenvoudigen.
- We voeren gesprekken met de bibliotheek voor het bieden van hulp aan Nijmegenaren via de informatiepunten digitale overheid (IDO).
- We zorgen dat medewerkers en Nijmegenaren bekend zijn met Yivi met een nog te bepalen activiteit of campagne.
- We blijven aan het ministerie van Binnenlandse Zaken onze bevindingen terugkoppelen om het stelsel van digitale wallets te verbeteren en blijven in gesprek om snel te kunnen anticiperen op landelijke ontwikkelingen van digitale wallets.
- We helpen ministerie van Binnenlandse Zaken bij de doorontwikkeling van de NL-wallet.
- We brengen de ethische aspecten van het gebruik van een ID-wallet in beeld.
- We leveren een toolkit voor andere gemeenten om ID-wallets te implementeren als één van de resultaten uit het innovatiebudget.
- We organiseren kennis- en testdagen voor het gebruik van ID-wallets (Yivi).
- We doen een aanvraag voor een nieuw innovatiebudget bij het ministerie van BZK voor verlenging van de ID-wallet pilot.
- We blijven de gemeenteraad actief informeren over bovengenoemde ontwikkelingen.
- We bereiden ons voor om digitale identiteit structureel te borgen in de staande organisatie zodat we het los kunnen laten als opgavethema.

** Onder voorbehoud, omdat activiteiten door voortschrijdend inzicht kunnen wijzigen*

Algoritmes en kunstmatige intelligentie

Maatschappelijke opgave

AI sinds de jaren ‘60 worden overheidstaken ondersteunt met digitale middelen. Automatisering is dan ook niet nieuw. Veel van de applicaties die we als gemeente gebruikten zijn al ingericht volgens algoritmische principes. De toegankelijkheid van deze techniek, de schaal waarop we als overheid onze taken automatiseren en aandacht voor de maatschappelijke implicaties ervan is de laatste jaren wel exponentieel gegroeid. ChatGPT heeft kunstmatige intelligentie (AI) - automatisering op basis van kansberekening - naar het grote publiek gebracht en heeft bovendien de schijnwerpers gezet op generatieve AI. Steeds meer leveranciers integreren nu ook (vormen van) kunstmatige intelligentie in hun applicaties. Dit alles levert nieuwe vraagstukken op:

- Waar automatisering eerst betekende ‘het technisch mogelijk maken van een vooraf gedefinieerd proces’ betekent het nu ook ‘het genereren van output op basis van kansberekening en waarschijnlijkheid.’ Dit betekent een fundamentele verandering van werk.
- De data die gebruikt worden om AI modellen te trainen zijn niet neutraal, beïnvloeden de output en dus de inhoud van processen.
- De inzet van algoritmes en AI bevordert de productiviteit van mensen en efficiency, maar niet altijd de kwaliteit van het werk.
- Het zorgt voor uitdagingen in vakmanschap en verhoudingen op afdelingen omdat er ook een groter verschil ontstaat in productiviteit tussen collega’s onderling.
- Automatisering heeft als bijeffect dat de uitvoering van processen minder zichtbaar wordt, maar we moeten kunnen blijven uitleggen hoe beslissingen tot stand zijn gekomen.

We willen voorkomen dat Nijmegenaren verstrikt raken in een systeemwerkelijkheid, maar willen ook de kansen van nieuwe technologie benutten om opgaven voor de stad te realiseren.

Doelen binnen dit opgavethema

1. We **stellen beleid vast voor algoritmes en AI** en **richten een proces in voor de inzet van kunstmatige intelligentie**, zodat we mogelijke juridische, technische, financiële en ethische bijeffecten zorgvuldig afwegen.
2. We laten **collega’s verantwoord experimenteren met (generatieve) AI**, zodat we werken aan hun ambtelijke vakmanschap.
3. We **bieden transparantie over de inzet van algoritmes en kunstmatige intelligentie**, zodat Nijmegenaren kunnen controleren waarvoor we deze technieken inzetten.
4. We zorgen dat onze **medewerkers over voldoende AI-geletterdheid beschikken** om verantwoord met AI om te gaan.

Wat hebben we al bereikt?

- Binnen het thema algoritmes en AI zijn vier sporen benoemd waarop we willen versnellen: keuzes & kaders, verantwoord experimenteren en leren, transparantie over algoritmegebruik en ontwikkeling van AI-geletterdheid.
- De hernieuwde spelregels voor de omgang met AI zijn vastgesteld door de directie en gedeeld met de organisatie.
- We zijn pilots met generatieve AI gestart voor:
    - het uitvoeren van audiotranscriptie en samenvatting van vergaderingen;
    - het vereenvoudigen van bewonersbrieven.
- We hebben bij drie afdelingen een algoritme beschreven voor opname in het algoritmeregister. Het gaat om anonimisering in het kader van de WOO, handhaving van adreskwaliteit bij verhuizingen en waardebepaling van woningen in het kader van de wet WOZ.
- We hebben een voorlopige selectie gemaakt voor het leeraanbod op AI in StudyTube.
- We zijn gestart met de opdracht voor beleid op algoritmes en AI waarbij we een gedeeld opdrachtgeverschap hanteren van de wethouder digitalisering en directeur bedrijfsvoering.
- We hebben naar aanleiding van de landelijke DPIA Microsoft 365 CoPilot besloten deze functionaliteit voorlopig niet aan te bieden aan onze organisatie.
- We hebben studenten van de honoursprogramma opdracht gegeven vopoor een onderzoek naar hoe wij AI-geletterdheid kunnen ontwikkelen in onze organisatie.
- We hebben als gevolg van bovenstaande activiteiten het afgelopen jaar veel expertise opgebouwd over de bruikbaarheid, regelgeving van en governance op AI.

Geplande activiteiten 2025 *

- We informeren de gemeenteraad over de opdracht algoritmes en AI via een raadsinformatiebrief.
- We ontwikkelen beleid op het gebied van algoritmes en AI.
- We organiseren de verantwoording en sturing op de inzet van algoritmes en kunstmatige intelligentie, waaronder IAMA’s (Impact Assesment Mensenrechten en Algoritmes) en maken dit onderdeel van het intakeproces voor i-activiteiten.
- We voeren een nieuwe pilot uit met open generatieve AI-modellen in eigen beheer.
- We leggen een backlog aan van potentiële use cases voor AI gebruik in en door de organisatie zodat we doelgerichter en praktijkgerichter kunnen experimenteren.
- We publiceren de 3 algoritmes in het landelijke algoritmeregister en beschrijven en publiceren ook de overige 2 algoritmes. Na de zomer evalueren we de pilot met de betrokken afdelingen, CIO, ambtelijk opdrachtgever en de wethouder digitalisering.
- We werken aan AI-geletterdheid, onder andere door inzet van een denktank van het honoursprogramma van de Radboud Universiteit.
- We bouwen het leeraanbod voor het verantwoord gebruik van (generatieve) AI uit op Studytube en de Nijmegenschool.
- We ontwikkelen een toolbox voor de omgang met generatieve AI door medewerkers binnen hun eigen vakgebied.

** Onder voorbehoud, omdat activiteiten door voortschrijdend inzicht kunnen wijzigen.*

Digitale ethiek in de ambtelijke organisatie

5.1.2e

5.1.2e

Product owner digitale ethiek

Maatschappelijke opgave

Digitalisering is nooit een doel op zich, maar een manier om te werken aan maatschappelijke opgaven. Als overheid proberen we onze taken goed en integer uit te voeren. Vrijwel alle deze taken worden ondersteund door digitale middelen. Digitalisering biedt veel kansen voor transparantie, toegankelijke dienstverlening en efficiency, maar verandert ook de verhouding tussen overheid en burger fundamenteel.
Deze transitie roept meerdere aandachtspunten op:

- Digitalisering voorziet in de behoefte om gemeentetaken effectiever uit te voeren en gewenst gedrag van burgers af te dwingen: automatisering van de deugd. Maar een effectievere taakuitvoering vergroot ook het risico op negatieve bij-effecten. (Maxim Februari, *Doe zelf normaal*)
- Ethiek is niet programmeerbaar en dus houdt een geautomatiseerde afweging geen rekening met ethiek. De individuele omstandigheden van een geval (context) worden dus niet automatisch meegenomen.
- Digitalisering biedt vaak een “quick fix”. De haast om crises en andere opgaven op te lossen maakt de inzet van technologie verleidelijk, maar ook vatbaar voor ongewenste bijeffecten.
- Beschikbaarheid van algoritmes en data vergroot het voorspellingsgeloof. Gedrag en ontwikkeling valt te voorspellen is de claim, maar het risico van een ‘self-fulfilling prophecy’ ligt ook op de loer.

Digitalisering biedt ons heel veel kansen om taken effectiever uit te voeren, maar technologie is nooit neutraal. De stad vraagt van ons dat we bij de inzet van digitale middelen een zorgvuldige belangenafweging van waarden maken en deze kunnen uitleggen. We moeten ethische kwesties dus vanuit verschillende perspectieven bekijken zodat we rechten en vrijheden van Nijmegenaren niet uit het oog verliezen. Met het inbedden van digitale ethiek in onze processen willen we expliciet maken welke ethische afwegingen gemaakt zijn bij onze digitaliseringsvraagstukken en opgaven.

Doelen binnen dit opgavethema

1. We **werken met een vastgestelde, gemeentebrede werkwijze voor digitale ethiek in de ambtelijke organisatie**, zodat een zorgvuldige ethische afweging van kansen en risico’s gemaakt wordt en indien nodig voorgelegd kan worden aan het bestuur.
2. We zetten de **organisatorische randvoorwaarden** neer voor de werkwijze, zodat deze ook kan worden uitgevoerd.
3. We hebben **afspraken gemaakt over de rolverdeling tussen de externe adviescommissie Digitale Ethiek en de ambtelijke werkwijze** voor het borgen van digitale ethiek.

Externe ontwikkelingen

- De parlementaire enquêtecommissie Fraudebeleid presenteerde op 26 februari 2024 het rapport ‘Blind voor mens en recht’ waarin o.a. wordt geconcludeerd: *“De informatisering en digitalisering heeft de overheid nieuwe mogelijkheden voor toezicht en fraudebestrijding geboden. (…) De overheid is blind geweest voor het feit dat achter elk (persoons)gegeven een mens schuilgaat en dat de waarborgen voor het uitwisselen, gebruiken en koppelen van gegevens daarmee ook waarborgen voor mensen zijn.”*
- Diverse gemeenten zijn gestart met een (externe) adviescommissie digitale ethiek. Soms bedoeld als adviesorgaan voor de gemeenteraad, soms voor het college. Ook zijn er gemeenten met een ambtelijke adviescommissie digitale ethiek. Bovendien zijn combinaties van deze varianten ook bekend.
- Gemeente Utrecht werkt al meerdere jaren met een eigen Utrechts ethische waardenmodel waar zij de inzet van digitale middelen aan toetsen: Uthiek.
- Gemeente Zwolle formuleerde vijf richtinggevenden principes rond digitalisering in de Zwolse samenleving ‘Waarde(n)volle Digitale Transitie’ dat als kompas dient bij het afwegen van kansen en risico’s van digitale technologieën in de samenleving.
- VNG heeft een uitvoeringsagenda Digitale Grondrechten en Ethiek 2023-2026 incl. handreiking digitale ethiek geformuleerd.
- In opdracht van het Ministerie van BZK stelde de Universiteit Utrecht in 2024 een rapport op voor de doorontwikkeling van Impact Assessments Mensenrechten en Algoritmes (IAMA): IAMA in Actie
- In november 2024 kwam de Interprovinciale Gids Digitale Ethiek uit

Wat hebben we al bereikt?

- We ondertekenden in 2018 samen met andere partijen in de stad het manifest Open en Weerbaar. Daarin is onder andere opgenomen: *“We laten nooit een zelflerend systeem een beslissing voor ons nemen.”*
- In januari 2023 is de externe adviescommissie Digitale Ethiek geïnstalleerd. Zij adviseren het college gevraagd en ongevraagd over digitaal ethische kwesties. De adviescommissie heeft inmiddels 3 adviezen afgegeven.
- In februari 2025 heeft de gemeenteraad kennisgemaakt met de adviescommissie Digitale Ethiek.
- In de ‘data protection impact assessments’ (DPIA’s) worden privacyrisico’s van een gegevensverwerking in kaart gebracht. Hierin is ook een ethische paragraaf opgenomen.
- We startten een pilot digitale ethiek waarin we een werkwijze verkennen waarmee we een ethische afweging structureel onderdeel kunnen maken van ons implementatietraject bij de inzet van technologie.

Geplande activiteiten 2025 *

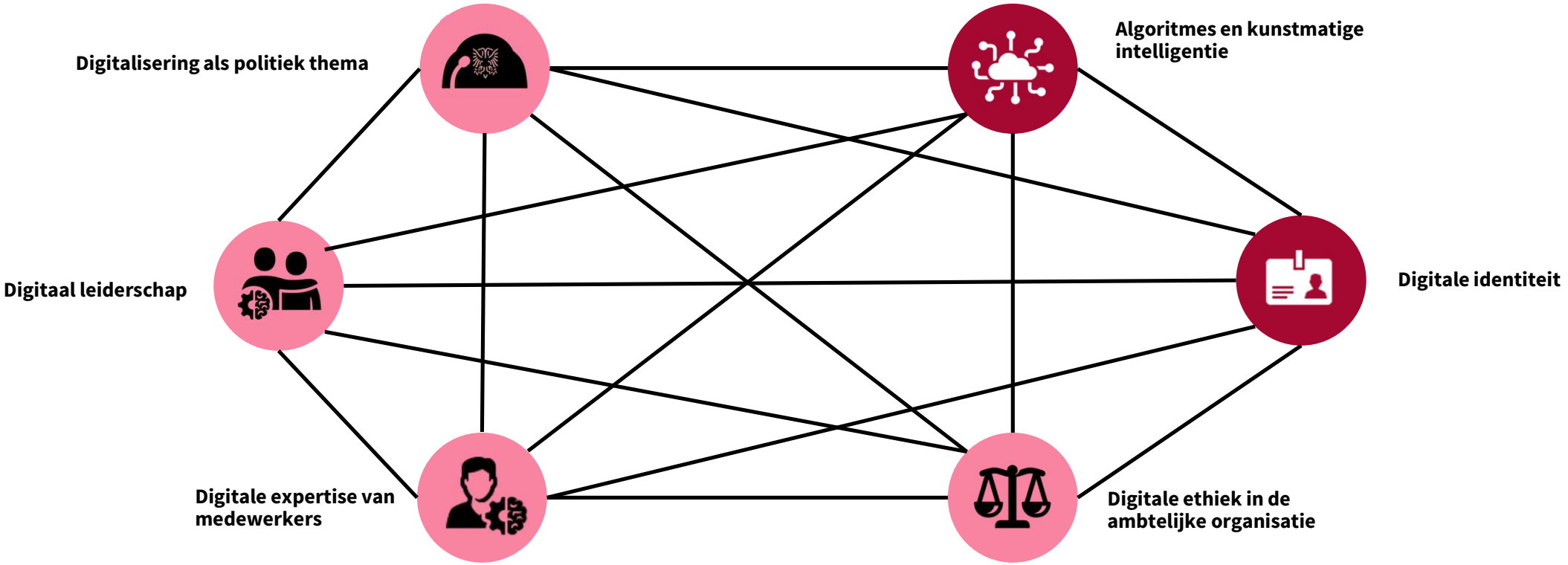
- We ronden de pilotfase af in het tweede kwartaal van 2025 met een voorstel aan de directie voor de wijze waarop we digitale ethiek in onze organisatie willen inbedden in bestaande processen, werkwijzen en structuren. Deze delen we ook met de wethouder digitalisering.
- We gaan in gesprek met de adviescommissie Digitale Ethiek over de rolverdeling tussen de commissie en de ambtelijke werkwijze.
- We organiseren een gesprek tussen de directie en de wethouder digitalisering over het voorstel om de verantwoordelijkheden goed af te bakenen. In gezamenlijkheid bepalen we aan wie en hoe het voorstel ter besluitvorming wordt voorgelegd.
- We bepalen na besluitvorming in overleg met de betrokkenen de vervolgstappen. Mogelijke vervolgacties zouden kunnen zijn:
    - We integreren de werkwijze in de intakeprocedure voor de inzet van nieuwe, digitale middelen.
    - We stellen een gemeentebreed waardenmodel vast voor vastlegging van een digitaal ethische afweging.

** Onder voorbehoud, omdat activiteiten door voortschrijdend inzicht kunnen wijzigen.*

Opgave digitale transformatie 2025

Digitale verantwoordelijkheid en gedrag

Digitale voorzieningen en infrastructuur



Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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	4, 8, 9, 10, 11, 13

Voorstel aan de directie
Wel op iNsite

Betreft

Onderwerp	Sturing op AI en algoritmes
Datum voorstel	28 oktober 2024
Steller	5.1.2e
Medeadvies	5.1.2e, 5.1.2e
Verantwoordelijke directeur	Gemeentesecretaris
Programma	Bestuur en organisatie
Doel van de behandeling	Ter besluitvorming
Samenvatting	De opmars van AI wordt steeds zichtbaarder in onze organisatie. We stellen daarom een actualisatie voor van de richtlijnen bij het gebruik van generatieve AI (o.a. ChatGPT). Aanvullend wil de wethouder digitalisering graag met de directie in gesprek over de bestuurlijke en ambtelijke verantwoordelijkheidsverdeling bij de sturing op de inzet van AI en algoritmes. Daarvoor doen we een procesvoorstel.
Besluit	Akkoord te gaan met de actualisatie van de richtlijnen voor het gebruik van (generatieve) AI Akkoord te gaan met het procesvoorstel om te komen tot beleidsregels voor algoritmes en AI

1. Probleemstelling

De opmars van AI en algoritmes wordt steeds zichtbaarder in onze organisatie. Ook wet- en regelgeving wordt volwassener. Europese en landelijke wetgeving reguleert echter niet alles. We hebben daarom ook beleidsregels op lokaal niveau op te stellen.

2. Doelstelling

Het doel is te komen tot:

- verantwoorde inzet van gratis beschikbare AI-tools door onze medewerkers;
- helderheid over bestuurlijke en ambtelijke verantwoordelijkheid op dit thema;
- vastgestelde beleidsregels voor de inzet van algoritmes en AI.

Dit voorstel sluit aan bij de volgende doelen van het programma ‘Bestuur en organisatie’:

- De belangrijkste risico's bij ons handelen zijn in beeld en worden beheerst;
- ons handelen is ethisch en in lijn met wet- en regelgeving;
- ons handelen is transparant en controleerbaar en er wordt verantwoording afgelegd;

Opgesteld door 5.1.2e, 5.1.2e, 5.1.2e **@nijmegen.nl**

- ons werk is slagvaardig en zorgvuldig uitgevoerd en volledig afgehandeld;
- ons werk is toekomstgericht en er wordt geleerd van het handelen om prestaties te verbeteren.

3. Argumenten

In juni 2023 zijn via iNsite de spelregels voor het gebruik van ChatGPT gedeeld. Daarbij was al aangekondigd dat we deze spelregels zouden actualiseren bij voortschrijdend inzicht.

Om een goed gesprek te kunnen voeren over de bestuurlijke en ambtelijke verantwoordelijkheidsverdeling stellen we voor om de directie kort mee te nemen in de verschillende vormen van AI en in hoeverre deze vormen onze organisatie op dit moment al raken. Op die manier heeft de directie dezelfde informatiepositie als de wethouder. Voor de overige argumentatie op het procesvoorstel voor de sturing op de inzet van AI en algoritmes verwijzen we naar de notitie '20241028 notitie beleidsregels inzet AI en algoritmes'.

4. Beleid en kaders

Op dit moment zijn al 'spelregels' voor het gebruik van ChatGPT van kracht en ook het digitaal informatiebeleid biedt uitgangspunten voor automatisering. Op juridisch vlak biedt de AVG ons kaders en vanaf februari 2025 worden de eerste bepalingen van de Europese AI Act ver kracht.

5. Kosten en baten

Omdat dit directievoorstel vooral voorstellen doet op richtlijnen en proces zijn er op dit moment nog geen kosten verbonden aan dit voorstel.

6. Inzet mensen en samenwerking

Algoritmes en AI is een thema dat onderdeel uitmaakt van de opgave Digitale Transformatie. Er is binnen de opgave al een multidisciplinaire werkgroep actief die zich met dit thema bezighoudt. Er wordt daarom geen aanvullende inzet gevraagd.

Bijlage(n):

- 20241028 Richtlijnen voor het gebruik van AI
- 20241028 Notitie beleidsregels inzet AI en algoritmes

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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

DATA PROTECTION IMPACT ASSESSMENT (DPIA)

Als gemeente zijn we verplicht een DPIA uit te voeren als er sprake is van een verhoogd risico op een inbreuk op de persoonlijke levenssfeer van onze inwoners. De DPIA vul je aan het begin van je project in. Hierdoor kunnen maatregelen voor het beschermen van data en het voorkomen van risico's vooraf meegenomen worden in de afweging om tot de verwerking over te gaan of waar mogelijk meegenomen worden in het ontwerp op programma van eisen van de aan te schaffen applicatie.

De DPIA vul je samen met je I-adviseur in. De DPIA is onderdeel van de intakeprocedure van het afstemmingsoverleg.

Project	: Transcribeersoftware
Afdeling	: Opgave Digitale Transformatie
Verantwoordelijk	: 5.1.2e
I-adviseur	: 5.1.2e
Datum	: 19 juni 2025

1. Inleiding op het project

1.1 Wat zijn de algemene achtergronden van het project?

Om het werk van de managementassistenten te verlichten en de wens om te starten met verantwoord gebruik van AI, heeft de gemeente Nijmegen een pilot uitgevoerd met transscriptiesoftware. Deze pilot is met positief resultaat afgerond. We hebben gekozen voor Microsoft Teams Premium. Hiermee voldoen we aan de vraag vanuit de werkvloer om een transcriptietool. De software zal zorgdragen voor het notuleren en samenvatten van vergaderingen.

Bij gebruik van de transcriptietool ziet het werkproces er als volgt uit:

- Aanvang: Notulist vraagt akkoord voor het opname van de vergadering voor het maken van een transcriptie.
- Bij akkoord: Opname en transcriptie wordt gestart.
- Bij geen akkoord: Er wordt handmatig genotuleerd.
- Opname wordt na het overleg (automatisch) opgeslagen in de OneDrive van de persoon die de transcriptie start. De opname is beschikbaar voor interne deelnemers aan het overleg, de transcriptie alleen voor deelnemers met een Teams Premium licentie.
- Na de vergadering: De software maakt een transcriptie en een samenvatting, deze is dus alleen voor de interne deelnemers met een Teams Premium licentie (de transcriptiesoftware) beschikbaar.
- De notulist controleert de transcriptie en samenvatting, voegt namen van de deelnemers toe als dit nodig is, past waar nodig de samenvatting aan en verwijdert gegevens die privacygevoelig of vertrouwelijk zijn. Na controle voegt de notulist het verslag toe aan de vergaderstukken voor het volgende overleg in Teams of iBabs. Op dat moment krijgen de andere deelnemers toegang. De deelnemers hebben de mogelijkheid om te reageren op de gemaakte notulen.
- Tijdens de volgende vergadering wordt het verslag besproken, worden wijzigingen doorgevoerd en wordt het verslag met inbegrip van wijzigingen vastgesteld. Daarna wordt de opname in Teams of op de iPhone verwijderd. Als het een eenmalige vergadering betreft, dan worden de notulen per mail vastgesteld, met een deadline voor de deelnemers om te reageren. Na de deadline wordt de opname verwijderd.
- Na de deadline wordt de opname verwijderd.

Het proces is afgerond op het moment dat de notulen door de deelnemende partijen aan de vergadering zijn vastgesteld, de aanpassingen door de notulist zijn verwerkt en de opname is verwijderd.

Deze DPIA zal gaan over het notuleerproces met gebruik van de transcribeertool bij werkoverleggen met enkel interne of een combinatie van interne en externe medewerkers. Verderop in de DPIA zal nader worden toegelicht bij welke soort vergaderingen deze transcriptietool kan worden toegepast.

1.2 Welk probleem lost deze gegevensverwerking op?

Het notuleren is tijdrovend en vereist veel concentratie tijdens het overleg, gericht op het maken van goede notities. Als mens zijn er beperkingen waardoor je niet alles wat gezegd wordt kan opvangen en onthouden. Vaak notuleren de managementassistenten en het kan voorkomen dat zij geen domeinexpertise hebben. Dit maakt handmatig notuleren foutgevoeliger.
Ook zorgt werkdruk ervoor dat de notulen soms pas een week later gemaakt worden, waardoor er informatie kan ontbreken. Met deze hulpmiddelen kan de notulist inhoudelijk(er) meeluisteren en heeft minder verwerkingstijd nodig per vergadering. Zo wordt er meer tijd vrijgemaakt voor overige werkzaamheden en verlaagt het de werkdruk bij medewerkers. Bevindingen uit de pilot bevestigen deze voordelen.

2. Doel en grondslag

2.1 Wat is het doel van de beoogde verwerking?

Waarom wil je gaan doen wat je bedacht hebt? Geef aan in welk kader deze verwerking plaatsvindt: bijvoorbeeld project of wetgeving.

De gemeente wil deze transcribeertool gaan gebruiken met het doel om sneller, efficiënter en kwalitatief betere notulen op te leveren.

2.2 Op welke grondslag is de verwerking gebaseerd?

De verwerking is in twee delen te onderscheiden: De verwerking van het stemgeluid (de opname en automatische transcriptie) en de inhoudelijk besproken informatie. Voor de verwerking van het stemgeluid geldt de grondslag toestemming. Deze toestemming zal aan de start van het overleg worden gevraagd en worden vastgelegd door de notulist. Als niet door alle deelnemers toestemming wordt gegeven wordt geen gebruik gemaakt van de transcriptietool. Als een deelnemer aan het overleg zijn toestemming later intrekt, wordt enkel de opname verwijderd, niet de transcriptie.

Het verwerken van de inhoudelijk besproken informatie in de transcriptie is gebaseerd op de grondslag *gerechtvaardigd belang*. Er is sprake van een gerechtvaardigd belang onder meer wanneer een verwerking aantoonbaar noodzakelijk is om bedrijfsactiviteiten te kunnen verrichten. Het houden van overleg en notuleren van de besproken onderwerpen is noodzakelijk om op een effectieve manier onze bedrijfsactiviteiten uit te voeren. De tool die we hierbij gebruiken draagt hieraan bij en valt daarom onder deze grondslag.

3. Achtergrond

3.1 Welke besluitvorming heeft plaatsgevonden op dit onderwerp?

Is er een ethische afweging gemaakt? Heeft er een oordeel van de ethische commissie plaatsgevonden? Beschrijf welke besluitvorming door het gemeentebestuur heeft plaatsgevonden over dit project of deze wetgeving. Ga ook in op eventuele maatschappelijke en bestuurlijke gevoeligheid of ethische dilemma's.

Met het bekender worden van verschillende AI-tools zijn er medewerkers die deze tools in hun dagelijks werk zijn gaan gebruiken. Als organisatie is nog geen keuze is gemaakt op welke manier we (veilig) willen omgaan met AI-tools. Er wordt wel gewerkt aan een beleid en onder andere het verantwoord testen is onderdeel van de Opgave die hiermee bezig is. Door eerst een pilot uit te voeren hebben we kunnen uitzoeken of we gebruik willen maken van dit soort tools en hoe dit dan op een veilige en verantwoorde manier kan. We hebben in de pilot gezien dat het van belang is:

- Gebruik de tool als aanvulling op een notulist, niet ter vervanging.
- Maak bij het controleren van de output gebruik van de transcriptie en de opname van de vergadering. Zo is goed terug te halen wat er daadwerkelijk gezegd is, en voorkom je onjuistheden.

3.2 Zijn er eerder DPIA's uitgevoerd op dit onderwerp?

Wat waren de gesignaleerde risico's en welke maatregelen zijn naar aanleiding daarvan genomen? Bij Ja, voeg deze toe als bijlage.

We maken gebruik van een nieuwe toepassing en het gaat om een nieuwe manier van werken dus er is geen gelijksoortige DPIA. Wel is de toepassing (Teams Premium) onderdeel van MS365. Er is een DPIA MS365.

3.3 Is er sprake van stelselmatige monitoring?

Dit is een verwerking die wordt gebruikt voor het structureel observeren, monitoren of controleren van betrokkenen.

Nee.

3.4 Is er sprake van matching of samenvoeging van datasets?

Wordt er een combinatie gemaakt van twee of meer verschillende bestanden van gegevens die voor verschillende doeleinden zijn verzameld?

Nee, elke vergadering is op zich staand en wordt opgenomen/getranscribeerd alleen voor de notulen die daarbij horen.

3.5 Is er sprake van innovatief gebruik van data?

Een nog niet (vaak) in de organisatie toegepaste nieuwe technologie of toepassing van technologie in pilotvorm, zoals het gebruik van Artificial Intelligence, machine learning of automatische besluitvorming.

Ja, er wordt gebruik gemaakt van AI-toepassingen, voor beide fases: Transcriptie m.b.v. een AI-model en verwerking tot een samenvatting/notulen door een taalmodel (LLM). We gaan in paragraaf 8 en de ethische bijlage in op de risico's hiervan.

4. Gegevens

4.1 Gaat het om een eenmalige uitwisseling van persoonsgegevens of structureel?

Heeft het een terugkerend karakter, noem dan de frequentie en als die er is ook de termijn.

Elke uitwisseling is incidenteel, maar vaak betreft het wel structurele overleggen met veelal dezelfde mensen.

4.2 Welke persoonsgegevens worden verwerkt?

Noem hier alle persoonsgegevens, dus de gegevens die herleidbaar zijn naar individuele inwoners.

Dit is sterk afhankelijk van de inhoud van de vergadering. In ieder geval zal worden verwerkt:

- Namen van betrokkenen
- Stemgeluid

We beperken de inzet tot vergaderingen die niet of beperkt de persoonlijke levenssfeer van de deelnemers of andere personen raken. In dit soort vergaderingen blijven de verwerkte gegevens ook beperkt tot de namen van de deelnemers, andere collega's die deel uitmaken van het team en de stemmen. We gebruiken de transcribeersoftware dus niet voor vergaderingen waar bijvoorbeeld dossiers van inwoners of medewerkers worden besproken.

Als er behoefte ontstaat om in andere situaties gebruik te maken van de transcribeertool, zal het gebruik van deze tool opnieuw beoordeeld worden in het licht van deze andere typen vergaderingen. Dit zal in een addendum bij deze DPIA worden gevoegd waarin die specifieke risico's en afwegingen worden behandeld én de persoonsgegevens die in dat geval zullen worden verwerkt.

4.3 Zijn dit bijzondere persoonsgegevens?

Geef aan of de te verwerken of verwerkte persoonsgegevens onder één of meerdere van de categorieën van bijzondere persoonsgegevens vallen:

Nee – er kan beargumenteerd worden dat de verwerking van stemgeluid een biometrisch gegeven omdat dit een fysiologisch kenmerk is van een persoon. Echter, voordat gesproken kan worden van een biometrisch persoonsgegeven moet er voldaan worden aan drie voorwaarden:

1. Aard van de gegevens: het moet gaan om fysieke -, fysiologische of gedragskenmerken die bij 1 persoon horen.
2. Middelen voor en wijze van verwerken: het gaat om persoonsgegevens die het resultaat zijn van een specifieke technische verwerking. Dit betekent dat gegevens met technische middelen worden geanalyseerd en vervolgens worden vergeleken met een bepaalde referentie.
3. Doel van de verwerking: verwerking maakt het mogelijk om iemands identiteit vast te stellen of bevestigen.

Of gegevens volgens de AVG biometrisch zijn, ligt dus aan de wijze waarop ze worden gebruikt. In dit geval worden de stemmen van de deelnemers opgenomen om de inhoud van het gesprek te kunnen vastleggen. Daarna wordt dit ook weer verwijderd. Het wordt niet gebruikt om iemand te identificeren of een referentiekader op te stellen. Daarom is hier geen sprake van een biometrisch gegeven én dus worden er in beginsel geen bijzondere persoonsgegevens verwerkt.

4.4 Is de beoogde verwerking proportioneel?

Geef aan wat het belang van inbreuk in privacy is in verhouding tot de inbreuk die gemaakt wordt door de voorgestelde wijze van gegevens verwerken. Hoe is deze inbreuk te verantwoorden?

De inbreuk houden we zo beperkt mogelijk tot enkel de naam en de opgenomen stem en die opname wordt ook direct na de verwerking weer verwijderd. Daarnaast is er de richtlijn dat andere gegevens ook niet verwerkt mogen worden, zoals gebeurt bij een bespreking van een persoonlijk dossier. De belangen die ermee worden gediend, namelijk nauwkeurigere verslaglegging, werklastvermindering en kortere doorlooptijden, wegen tegen de inbreuk op.

Subjectief bekeken, kan een medewerker wel ervaren dat het niet proportioneel is. Het is vooruitschrijdende, nieuwe technologie waarvan nog niet iedereen weet hoe het werkt. Hoewel er voordelen aan het gebruik van een AI-transcribeertool zitten, is het nog niet de norm in de maatschappij. Het kan worden ervaren als spannend en soms zijn mensen ronduit tegen het gebruik ervan. Hoewel de inbreuk beperkt is en opweegt tegen de voordelen, moet er rekening gehouden worden met het feit dat het minder proportioneel wordt ervaren. Daarom wordt vooraf ook gevraagd om toestemming van de deelnemers aan het overleg om te starten met een opname. Als iemand aangeeft bezwaren te hebben, dan wordt gewoon met de hand getranscribeerd. Verder is het niet bij iedere vergadering vanzelfsprekend om de transcribeertool te gebruiken.

4.5 Is de beoogde verwerking subsidiair?

Leg uit waarom de voorgestelde verwerking noodzakelijk is om het doel te bereiken. Leg ook uit dat het doel niet op een minder ingrijpende manier bereikt kan worden. Zijn er alternatieven onderzocht en waarom waren die niet geschikt?

Bij het gebruik van de transcribeertool is bewust gekozen voor een bepaald type vergadering waar in beginsel geen andere persoonlijke gegevens worden gedeeld naast de naam. De naam is nodig om in de uiteindelijke notulen terug te kunnen lezen wie wat heeft gezegd. Verder is het enkel middels het opnemen van de stem mogelijk om gebruik te maken van de tool.

Het alternatief is de huidige werkwijze met handmatige verwerking. Echter, deze technologie is in opkomst en op de werkvloer is er vraag naar het gebruik van deze tool. We passen het toe in een beheerste omgeving. De pilot heeft aangetoond dat deze methode winst in tijd en kwaliteit oplevert en dat verantwoord gebruik mogelijk is.

4.6 Worden de persoonsgegevens buiten de EER gebruikt?

Welk land/welke landen betreft het? Welke passende waarborgen zijn/worden in dat kader getroffen?

De opnames worden in de Teams-omgeving (tenant) van de gemeente Nijmegen verwerkt. De samenvatting die het programma met behulp van AI genereert wordt ook binnen de EU verwerkt.[1]

[1] https://learn.microsoft.com/en-gb/copilot/microsoft-365/microsoft-365-copilot-privacy?toc=%2Fcompliance%2Fassurance%2Ftoc.json&bc=%2Fcompliance%2Fassurance%2Fbreadcrumb%2Ftoc.json#microsoft-365-copilot-and-the-eu-data-boundary en https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-learn

5. Partijen

5.1 Welke partijen zijn bij de verwerking betrokken?

Tussen welke partijen worden de gegevens uitgewisseld? Van wie worden ze verkregen?

De gegevens worden uitgewisseld tussen deelnemers aan de vergaderingen. De deelnemers zijn collega's en externen (bijvoorbeeld aannemers). Voor de verwerking van de transcriptie en samenvatting wordt gebruik gemaakt van cloudopslag direct bij Microsoft (Teams Premium).

5.2 Wat zijn ieders rollen?

Verwerkingsverantwoordelijke, (sub)verwerker)?

Gemeente Nijmegen is verwerkingsverantwoordelijke. Microsoft is verwerker.

5.3 Welke overeenkomsten worden aangegaan als gevolg van die rollen?

Welke verwerkersovereenkomsten of overeenkomsten van medeverantwoordelijkheid worden opgesteld? Voeg deze als bijlage toe.

- Juridisch Framework van de VNG met Microsoft. Dit is een bijlage bij de DPIA MS365.

6. Zorgplicht

6.1 Op welke wijze is het project en haar analyses in begrijpelijke taal uit te leggen?

Geef een korte en heldere beschrijving die voldoet aan regels voor externe communicatie. Ook op het niveau van type gegevens, combinatie van datasets en doorslaggevende factoren voor de uitkomst.

We maken gebruik van software in de vorm van een transcribeertool om vergaderingen op te nemen en hier tekst van te maken. De software kan van deze tekst ook een verslag maken. Omdat we deze opnames maken worden de besproken onderwerpen tijdelijk opgeslagen als geluidsbestanden. We zorgen dat dit zo veilig mogelijk gebeurt:

- We maken geen opnames van gevoelige gesprekken.
- We verwijderen de bestanden meteen als het verslag af is.
- We maken alleen een opname als alle deelnemers het goed vinden.

6.2 Op welke wijze(n) worden betrokkenen geïnformeerd?

Hoe transparant bent u over uw project naar betrokkenen toe? Geef de communicatiewijze aan en welke middelen ingezet worden.

Iedereen die deelneemt wordt voorafgaand aan het overleg geïnformeerd. Organisatiebreed berichten we via het intranet dat je naam genoemd kan worden in overleggen waarin de transcribeertool gebruikt wordt.

6.3 Op welke manier zijn de rechten van betrokkenen geborgd in het proces?

Ga ook in op welk moment in het proces dit gebeurt.

We zorgen voor een zo beperkt mogelijke verwerking van persoonsgegevens. We gebruiken de oplossing niet voor gevoelige gesprekken en we verwijderen opnames zodra het verslag is vastgesteld. Verder kan iedereen ook gebruik maken van de reguliere rechten onder de AVG via het webformulier op de website van de gemeente.
Als er ongemak is over de transcribeertool kan dit ook altijd bij de leidinggevende worden aangekaart.

7. Informatiebeveiliging en vernietiging

7.1 Hoe lang worden de gegevens bewaard?

Noem ook de grondslag van de bewaartermijn.

We bewaren de opnames niet langer dan nodig voor het proces. Dit betekent dat de opname verwijderd wordt nadat het verslag is vastgesteld. Microsoft verwijdert de documenten volgens hun data-retentiebeleid.[2]

7.2 Wie is verantwoordelijk voor de vernietiging van de gegevens?

En wie ziet daarop toe? Noem voor beide aspecten organisaties of organisatie-onderdelen.

De afdeling waar de vergadering plaatsvindt is verantwoordelijk voor de vernietiging.

7.3 Is er een vastgesteld normenkader van toepassing op deze gegevensverwerking?

Het gaat hier om specifieke beveiligingsnormenkaders.

BIO.

7.4 Hoe worden de gegevens beveiligd? Hoe is het toezicht daarop georganiseerd?

Welke technische en organisatorische maatregelen zijn nu al genomen om de gegevens te beveiligen en risico's voor betrokkenen te voorkomen of te beperken? Denk hierbij aan autorisaties, validatie etc. Benoem ook of gegevens herleidbaar, gepseudonimiseerd of geanonimiseerd worden opgeslagen.

Teams Premium staat alleen toegang tot de opname toe aan deelnemers aan het overleg. De beveiligingsinstellingen komen overeen met de standaard MS Teams-instellingen.

8. Risico's

8.1 Benoem hieronder de risico's voor betrokkenen door de gegevensverwerking

Iedere verwerking kan, ondanks genomen maatregelen, risico's met zich meebrengen. Het is belangrijk dat we als organisatie deze risico's in beeld hebben, zodat we besluiten kunnen nemen met inachtneming van eventuele risico's. Het gaat hier zowel om beveiligingsrisico's als andere privacyrisico's. Risico is geformuleerd in termen van de waarschijnlijkheid dat zich het risico voordoet (kans) afgezet tegen de hoeveelheid schade of gevolgen die het risico kan hebben (de impact). Kortweg: risico = kans x impact.

- Datalekken van vertrouwelijke gegevens besproken in vergaderingen (bijv. over een aanbesteding). We kiezen voor goed beveiligde omgevingen, maar het zijn SAAS-oplossingen. Dat betekent dat data over de bespreking bij een derde partij beschikbaar komt. De kans op lekken is relatief klein.
- Gebruik bij vergaderingen waar het niet geschikt is, en te veel of gevoelige persoonsgegevens gedeeld worden.
- Gebruik zonder instemming van betrokken, zowel deelnemers aan de vergadering als derden die besproken worden in de vergadering. Dit betreft ook de deelnemers die mogelijk druk ervaren om akkoord te gaan met een opname.
- De kans dat onwaarheden in de notulen terechtkomen door gebruik van het AI-model, waar ten onrechte op vertrouwd wordt dat deze correct zijn (dit noemt men ook wel een confirmation bias).
- Niet tijdig verwijderen van de opname.

[2] https://learn.microsoft.com/en-gb/compliance/assurance/assurance-data-retention-deletion-and-destruction-overview#data-retention

- Ontwikkelingen Microsoft: De optie bestaat nu om een stemprofiel op te stellen.

8.2 Benoem de maatregelen die nog noodzakelijk zijn.

Het gaat hier om maatregelen om de gevolgen te voorkomen of de effecten van die risico's te mitigeren, die nog niet genomen zijn. Beschrijf ook de impact van deze maatregelen, op het doel van de gegevensverwerking en de kosten van deze maatregelen.

- Geen gebruik bij gevoelige vergaderingen – in de pilot was dit een gegeven. Bij autoriseren voor gebruik van Teams Premium wordt gevraagd voor welk type vergaderingen de gebruiker het gaat toepassen. Hierbij wordt alleen goedkeuring verleend voor vergaderingen zoals omschreven onder 4.2.
- Duidelijk bekend maken dat de opname verwijderd moet worden na vaststelling van de notulen, zowel bij de 'notulist' als bij de deelnemers van de vergadering. Zo zijn er meer controlepunten die zullen checken of een opname ook daadwerkelijk verwijderd wordt.
- Microsoft verwijdert opnames automatisch na 6 maanden, tenzij de bestandseigenaar expliciet aangeeft een opname langer te willen bewaren.
- Een maatregel die ook genomen zal worden is dat bij gemeentebrede uitrol er een werkinstructie gedeeld zal worden waar de tool niet alleen technisch wordt toegelicht maar ook de gebruiksregels zoals het verwijderen van de opname.
- We geven het advies geen stemprofiel te laten aanmaken door Microsoft Teams.

8.3 Wat is het restrisico dat overblijft?

Dit is het risico dat overblijft na uitvoering van de geadviseerde maatregel(en).

- Mensen kunnen eigenwijs zijn en toch een stemprofiel laten maken.
- Mensen met autorisatie die het toepassen bij 'gevoelige' vergaderingen.
- Over het hoofd zien dat er een stuk 'extra' of foutieve tekst door de tool in de notulen wordt gezet. Menselijk handelen is ook het over het hoofd zien van tekst. Dit risico wordt wel zo veel mogelijk voorkomen doordat er meerdere mensen naar het verslag kijken voordat het wordt vastgesteld.

Over het algemeen komt het restrisico neer op menselijk handelen.

Bijlage 1 Ethiek

1. Data-alertheid

1.1 Wat zijn de ethische effecten van dit project?

Op welke andere publieke waarden heeft deze gegevensverwerking ook effect? Het gaat hier om zowel mogelijk ongewenste of onbedoelde effecten.

Het is vooraf lastig in te schatten welke ethische effecten dit project zal hebben. Voor zover we een inschatting kunnen maken zal het naar de inwoner geen verschil uitmaken ten opzichte van de huidige werkwijze, zo lang we in ieder geval vasthouden aan de richtlijn dat we enkel de overleggen transcriberen die niet de persoonlijke levenssfeer raken.
Voor de medewerker kan het wel zorgen voor enige effecten. Ze worden op deze manier geconfronteerd met het gebruik van AI op de werkvloer. Net als bij iedere vorm van technologie zijn er voorstanders en tegenstanders, de mensen die zich snel aan kunnen passen en het eigen maken én de mensen die er meer moeite mee hebben. Vooral de mensen die tegen het gebruik zijn kunnen dit ervaren als onveilig, te ver vooruit willen lopen of dat ze wellicht vervangen worden.

Ook bestaat er een mogelijk spanningsveld op het gebied van inclusiviteit. Het zou kunnen zijn dat de transcribeertool niet goed werkt met alle stemmen. Denk aan man vs. vrouw of verschillende accenten. Hier kan nog geen oordeel over geveld worden omdat hier nog niet op getest is.

Een ander mogelijk effect kan zijn men zich anders gaat gedragen in vergaderingen omdat ze weten dat het gesprek wordt opgenomen. Vergaderen gaat niet alleen over informatie uitwisselen maar is ook een plek waar gebouwd wordt aan elkaars vertrouwen en relatie. Als mensen meer op hun hoede zijn over wat ze zeggen heeft dit invloed op de relatievorming.

Hoewel dit niet de intentie is, is dit mogelijk wel een onbedoeld effect. Een volledige toetsing van de ethische effecten en de vraag óf we dit willen zullen we nogmaals moeten verrichten wanneer de richtlijnen digitale ethiek tot stand zijn gekomen.

1.2 Welke inspanningen worden verricht om de mogelijk negatieve effecten van dit project te proberen voorkomen?

Beschrijf de maatregelen die genomen worden om deze negatieve ethische effecten te voorkomen of beperken.

De gemeente heeft binnen de opgave Digitale Transformatie een ‘Team AI en Algoritmes’ ingesteld – die toezicht heeft uitgeoefend op deze pilot. Binnen deze opgave houdt men zich ook bezig met de vraag hoe we verantwoord en veilig gebruik kunnen maken van deze technologie binnen de gemeente. Niet alleen door het opstellen van beleid, maar ook door te werken aan een wijze waarop de AI-geletterdheid binnen de gemeente verbeterd kan worden en hoe digitale ethiek geborgd kan worden. Het doel hiervan is dat iedereen mee kan gaan met de nieuwe ontwikkelingen.

1.3 In hoeverre is er sprake van (semi-)automatische besluitvorming?

Is er voorzien in menselijk contact met betrokkenen om een besluit uit te leggen en eventueel te heroverwegen?
Niet, deze tool neemt geen besluiten.

2. Vooringenomenheid (bias)

2.1 Zijn alle verschillende groepen betrokkenen vertegenwoordigd in de dataset(s)?

Wie missen er of zijn niet zichtbaar? Past dit bij het doel van de verwerking?

Niet van toepassing

2.2 Worden uitkomsten van de analyse weer gebruikt voor een vervolganalyse?

Op deze manier kan er een feedback loop ontstaan, waardoor vooringenomenheid van het model steeds versterkt wordt.

Niet van toepassing

2.3 Bestaat het gevaar dat bepaalde betrokkenen of groepen gediscrimineerd zouden kunnen worden door uw project?

Zijn er groepen betrokkenen die door de gegevensverwerking (verder) in een achterstandspositie terecht kunnen komen? Is er een risico dat de gegevensverwerking bestaande ongelijkheden versterkt?

Gezien het mogelijke effect op inclusiviteit, kunnen we hier uitsluitsel over geven. Omdat de notulen uiteindelijk door een mens worden herzien, kan dit wel hersteld worden.

3. Transparantie

3.1 Bestaat het risico op (publieke) verontwaardiging?

Hoe zal de gegevensverwerking politiek-maatschappelijk vallen? Als dit risico er is: welke maatregelen worden genomen om dit te beperken?

Omdat dit betrekking heeft op de bedrijfsvoering binnen de gemeente én er geen dossiers van inwoners besproken zullen worden bij gebruik van de transcribeertool, is het risico op (publieke) verontwaardiging laag. Het is een algemene trend, bij zowel overheidsinstellingen als bedrijven, om te kijken of er AI-toepassingen zijn die het werk efficiënter kunnen maken.
Door de werkwijze die we nu hanteren worden de risico's beperkt en worden er weinig persoonsgegevens verwerkt.

3.2 Kunnen betrokkenen bezwaar maken tegen uitkomsten van het project?

Is de formele bezwaarprocedure van toepassing? Zo nee, welke andere middelen hebben betrokkenen om bezwaar te maken?

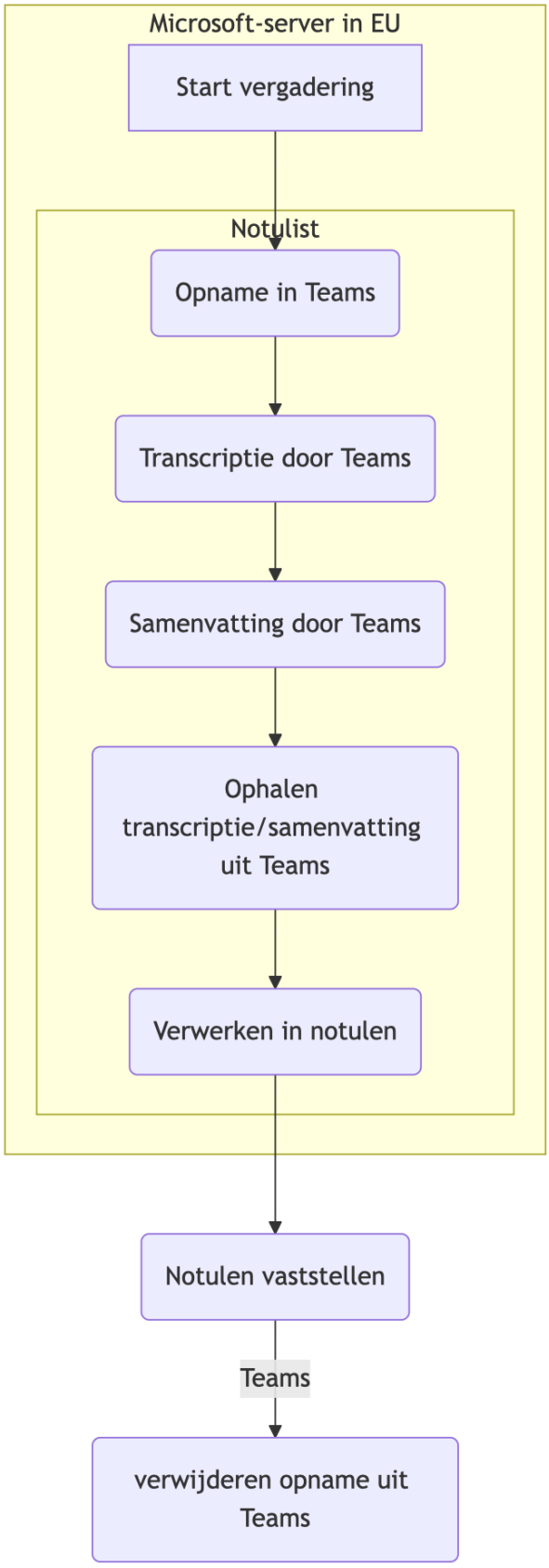
Omdat er geen sprake is van een besluitprocedure zal een betrokkene ook geen bezwaar kunnen maken tegen de uitkomst van het project. Wel is het natuurlijk mogelijk dat een medewerker bezwaren heeft tegen het gebruik van deze tool. Deze signalen hopen we van de werkvloer op te vangen. Dit wordt ook verwerkt in het vervolg van het project. Het uitgangspunt op het moment is dat als het niet verantwoord en veilig is dat we er niet mee doorgaan. Ook als het praktisch geen voordeel oplevert, dan zal er sneller voor gekozen worden om niet door te gaan met het gebruik van de transcribeertool. Dat volgt al snel als regelmatig de feedback wordt gegeven dat men bezwaren heeft tegen het opnemen.

3.3 Is een opt-out mogelijk voor betrokkene?

Kunnen betrokkenen weigeren hun gegevens te laten verwerken? Zo ja, op welk moment kunnen betrokkenen ervoor kiezen om deelname te beëindigen?

Dat is mogelijk. Aan het begin van een vergadering wordt altijd om toestemming gevraagd van de betrokkenen. Dit is het moment waarop ze kunnen aangeven dat ze dit niet willen. De transcribeertool zal dan niet worden gebruikt.

Bijlage 2 Processchema



Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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

Evaluatie AI-pilot transcriptiesoftware

Nut en noodzaak

Wat was het beoogde doel van de toepassing?

Tijdsbesparing. Doordat AI de notulist van een vergadering ondersteunt, heeft deze minder tijd nodig na de vergadering om de notulen en afspraken af te ronden.

Wordt dat doel bereikt met deze toepassing?

Ja. De tool geeft zowel de letterlijke transcripties als een samenvatting en actiepunten van de vergadering. Vooral die laatste twee zorgen ervoor dat de notulist veel minder tijd kwijt is om de vergadering samen te vatten. Alleen de output van de tool moet gecontroleerd worden.
Inzet van de tool kan daarmee personele inzet besparen.

Bijkomend voordeel is dat de notulisten aandachtiger kunnen deelnemen aan de vergadering. De transcriptie loopt mee, dus ze hoeven geen letterlijke aantekeningen meer te maken. Dat geeft hen de ruimte om meer op hoofdlijnen en actiepunten aantekeningen te maken, wat zorgt voor meer rust en overzicht en betere kwaliteit van de notulen.
De rol van de notulist/projectassistent bij een overleg kan veranderen, doordat er meer ruimte ontstaat om mee te denken en deel te nemen aan het gesprek. De pilotgroep geeft aan dat dit tot meer werkplezier leidt.

Welke tools zijn vergeleken? Welke heeft de voorkeur, en waarom?

Goodtape en Microsoft Premium zijn vergeleken.

Goodtape geeft goede transcripties. De werkwijze is dat er een opname wordt gemaakt van de vergadering, die later in Goodtape ingevoerd wordt. Goodtape zet dit dan om naar een transcriptie. Sinds kort heeft deze tool ook een samenvattingsmogelijkheid, maar deze geeft vaak foute samenvattingen.

Microsoft Teams Premium is een uitbreiding op onze Teams-licentie, en integreert ook met Teams. Bij een vergadering kan de transcriptie en samenvatting ‘aangezet’ worden door iemand met de juiste licentie. De vergadering wordt dan getranscribeerd en na afloop samengevat. Deze samenvattingen zijn zowel inhoudelijk als tekstueel verrassend goed. Ook maakt de tool een lijst met actiepunten. De notulist hoeft hier vaak maar weinig aan te passen.

Wat zijn de gevolgen bij het invoeren van deze toepassing?

Wat is de impact op het werkproces, wat voor beroep doet het op de digi-/AI-vaardigheid van collega’s?

De notulist moet er scherp op blijven de output van de tool altijd goed te controleren. De zogeheten *automation bias* ligt op de loer: het letterlijk overnemen van de suggesties van de tool. De output is vaak niet goed of volledig genoeg om dit te kunnen doen. Zeker bij gesprekken met juridische gevolgen zijn correcte samenvattingen belangrijk, en kunnen foute samenvattingen grote juridische of financiële gevolgen hebben.

De deelnemers aan de pilot waren zich goed bewust hiervan, maar dit is wel een punt van aandacht als de tool breder uitgerold wordt.

Wat zijn de beperkingen van de tool?

Met meerdere mensen in een vergadering kan het gebeuren dat mensen door elkaar heen praten. Transcriptiesoftware kan hier slecht mee omgaan, waardoor de output verslechtert. Het vraagt dus goede vergaderdiscipline om het beste resultaat uit de tool te krijgen. Ook los van transcriptiesoftware is dat een goede gewoonte.

De tools kunnen minder goed omgaan met hybride vergaderingen (vergaderingen waarbij er zowel mensen fysiek aanwezig zijn als online aansluiten). Het is dan voor de transcriptietool niet mogelijk om de verschillende 'live'-deelnemers uit elkaar te houden, waardoor de transcriptie niet de juiste uitspraken aan de juiste personen koppelt. Dit heeft voor de actiepunten en samenvatting echter geen grote gevolgen, omdat het relatief weinig werk is om deze fouten te corrigeren.

Techniek

Welk model wordt gebruikt?

Microsoft maakt gebruik van de 'Azure OpenAI service'. Dit maakt gebruik van modellen van OpenAI. Welke modellen exact worden gebruikt is niet bekend en Microsoft behoudt zich het recht voor dit te wijzigen.

Het precieze model dat GoodTape gebruikt is ook niet bekend gemaakt.

Waar draait het model, waar worden de data verwerkt?

Bij Microsoft Teams Premium: Het transcriptiemodel draait binnen onze Microsoft tenant, en wordt verwerkt door Microsoft. Dataverwerking valt onder de data-beschermingsafspraken zoals voor de gehele tenant gemaakt.[1]

GoodTape maakt gebruik van het Google Cloud Platform, en kan opschalen naar Azure. Ze verwerken alle data binnen de EU.

Op welke data is het model getraind? Zitten daar (ethische) bezwaren aan?

De modellen van OpenAI zijn niet open over de trainingsdata. De kans is aanwezig dat deze data ethisch bezwaarlijke bronnen bevat. OpenAI publiceert wel informatie over de maatregelen die worden genomen voor de preventie van schade door het model.[2]

Worden ingevoerde data gebruikt om het model verder te trainen?

Microsoft: Data wordt niet gebruikt om het model verder te trainen. Zie voetnoot 1.
GoodTape: Data wordt niet gebruikt om het model verder te trainen.[3]

Conclusie

De transcriptiesoftware heeft de meerwaarde bewezen. Het is geen vervanger van een notulist, maar maakt het werk daarvan efficiënter en eenvoudiger.
Het is lastig te kwantificeren hoeveel uur de tool aan personele besparing oplevert. Dat verschilt ook per type en inhoud van de vergadering. De tool levert tijdswinst op, maar afhankelijk van de vergadering en de vorm van de te leveren notulen is dit meer of minder.

---

[1] https://learn.microsoft.com/en-us/microsoftteams/privacy/intelligent-recap
[2] https://openai.com/index/gpt-4o-system-card/
[3] https://blog.goodtape.io/privacy/

Wel leidt het gebruik duidelijk tot verbeteringen in het werk: Het notuleren zelf wordt als minder stressvol ervaren. Daarnaast geven deelnemers duidelijk aan dat het hen in staat stelt de vergaderingen beter inhoudelijk te volgen, waardoor zij hun rol na afloop ook beter kunnen invullen.
Zowel GoodTape als Microsoft Teams premium geven goede resultaten. Vanwege de manier waarop genotuleerd wordt en het feit dat de samenvattingen van Microsoft Teams Premium veel bruikbaarder zijn, geven de deelnemers aan sterke voorkeur voor Teams Premium te hebben.

Aanbevelingen

We raden aan licenties Microsoft Teams Premium aan te bieden voor medewerkers in functies waar dit een duidelijke meerwaarde heeft:

- Een significant deel van de werkzaamheden moet bestaan uit het bijwonen en notuleren van vergaderingen
- Het zijn geen 'gevoelige' vergaderingen, waarin de tool gebruikt kan worden (zie ook de afspraken uit de DPIA)
- Het soort overleggen leent zich voor gebruik van de transcriptietool (vergaderdiscipline, mogelijkheid opnames met Teams te maken).

Voor het goed gebruik van de transcriptietool:

- Gebruik de tool als aanvulling op een notulist, niet ter vervanging.
- Maak bij het controleren van de output, gebruik van de transcriptie en de opname van de vergadering. Zo is goed terug te halen wat er daadwerkelijk gezegd is.
- Let op vergaderdiscipline; zorg dat er geen mensen tegelijk aan het woord zijn, benoem de structuur van de vergadering en vat actiepunten tijdens het overleg samen.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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

GMT voorstel
Ter informatie

Decharge stuurgroep AVG, vaststellen opdracht klankbordgroep AVG

Opsteller: 5.1.2e

Datum behandeling:
19 februari 2025
Op iNsite: Ja/nee

Programma: Bestuur en Organisatie
Concernmanager: 5.1.2e 5.1.2e, 5.1.2e, 5.1.2e
Verantwoordelijk directeur: 5.1.2e

Advies aan directie

- Decharge verlenen aan de stuurgroep AVG;
- De nieuwe opdracht aan de klankborgroep AVG vaststellen.

Decharge

Eind 2024 is het laatste afdelingsplan in het kader van het project 'Mijn afdeling AVG-proof' ingeleverd. Daarmee is dit project tot afronding gekomen. Dat betekent ook dat de opdracht waarvoor de stuurgroep destijds in het leven is geroepen, afgerond is. Daarom stellen we voor om de stuurgroep decharge te verlenen.

Probleemstelling

Met de afronding van Mijn afdeling AVG-proof, is het onderliggende doel – AVG-proof worden – nog niet bereikt. In principe liggen er slechts plannen om dit doel te bereiken. De plannen moeten nog wel uitgevoerd worden. Met de uitvoering van deze plannen werken wij toe naar het doel dat gesteld is in het privacybeleid, namelijk het bereiken van volwassenheidsniveau 3.
Vanuit die optiek is het onlogisch en onverstandig om de vinger aan de pols op concernniveau stop te zetten. Er is namelijk nog behoorlijk veel werk aan de winkel. Het is wel zo dat de bezetting vanuit het GMT verkleind kan worden en dat de frequentie van samenkomst verminderd kan worden.

Voorstel

Daarom doen we het voorstel voor een nieuwe opdracht, namelijk het monitoren van de voortgang van de door afdelingen ingediende plannen om AVG-proof te worden. Dit doen we in de vorm van de klankbordgroep AVG.
De klankbordgroep:

- Bestaat uit de voorzitter 5.1.2e), Stadscontroller, concernmanager PIF, Functionaris Gegevensbescherming en de Privacy Officer;
- Komt tweemaal per jaar samen, één keer rondom december en één keer rondom juni;
- Bespreekt in ieder geval de volgende thema's:
    - De jaarrapportage van de FG, waarin de stand van zaken betreffende de plannen van specifieke afdelingen onder andere in wordt meegenomen, en;
    - De raadsinformatiebrieven betreffende privacy en informatiebeveiliging, die twee keer per jaar verstuurd worden.

Vervolg

Halfjaarlijks komt de klankbordgroep AVG bij elkaar, om eerder genoemde thema's en mogelijk andere relevante zaken te bespreken.

Bijlage(n)

1. Memo voorzetting opdracht Stuurgroep AVG

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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

IT roadmap 2021-2026

1. Ambitiedocument & Adviesrapporten

Aanbevelingen
combineren

2021 Ambitie document

2022 Reken-kamer

2023 Cuccibu

2. Risico's & maatregelen

Aanbevelingen koppelen
aan **maatregelen**

2023

2024

3. Opvolging aanbevelingen

Verbeteracties
plannen

4. Kritische processen/ applicaties

Acties richten op
kritische applicaties

APP

2025

5. Prioritering & keuzes

Tijd, geld, keuzes

1
2
3

6. (Bij)sturen

Uitvoering, monitoring, communicatie

2026

⚠ 2. Risico's & maatregelen

Beleid/governance maatregelen

- Verdeling BIO2 maatregelen
- Informatiebeveiligings- & privacybeleid
- BIO2 hanteert een risicogebaseerde aanpak (2025)
- Bestuurlijke aandacht & bewustzijn
- Bestuur training cyberbeveiligingsrisico's
- Kritische prestatie-indicatoren
- Cyclus toetsen & rapporteren / verbeteren interne controle

Risico: Systemen niet beschikbaar (Cyber/DDos-aanvallen)

- Analyse
- Hackathon
- Medewerkers
- Voorkomen ongewenste toegang
- Certificering IRvN & afspraken met (cloud-) leveranciers
- Tenant scheiding
- ISMS
- Oefening crisisteam bedrijfscon-tinuïteit afd.
- Operationele Technologie (OT)

Risico: Vertrouwelijke gegevens op straat (datalek)

- Verwerkers) overeenkomsten privacy analyses
- Phishing
- Veilig mailen
- Mysteryy guest
- Lock screen
- Wachtwoord manager
- Inzicht in privacy by design projecten creëren
- Privacy ambassadeur

Risico: Medewerker

- Gebrekkige beveiliging applicaties aanpakken
- Periodiek (toegangs-) rechten beoordelen
- Gedeelde accounts minimaal
- Autorisatiematrix met functiescheiding
- RBAC / HelloID
- Verklaring omtrent gedrag
- Referenties
- Gedragsregels bedrijfsmiddelen

3. Opvolging aanbevelingen - verbeteracties per aanbeveling

= continu aandacht

Door:
- CISO
- SO
- CISO & SO
- Manager
- Raad
- Privacy officer en FG

Certificering IRvN & afspraken met (cloud-) leveranciers

2024: 95% 4 processen; start 1e deel TPM 15% 25%
2025: 75% 1e deel TPM gereed
2026: 2e deel TPM gereed?
2027: 100% jaarlijkse audit en BIO TPM; jaarlijkse audit en BIO TPM

Informatiebeveiligingsbeleid: verhelderen en actualiseren

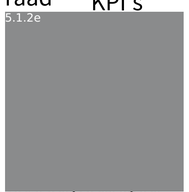
2024: 85% Actualiseren
2025: Huidig beleid 100%; BIO2 actualiseren 100%; Uitwerking IBB Vaststellen
2026: 100%

BIO2 hanteert een risicogebaseerde aanpak (2025)

2024: 50% Risico analyse elk 2 jr in GMT
2025: 50% Continuïteit dienstverlening in gemeentelijk Plan van Aanpak in college
2026: 95% Risico's beheerst elk 2 jr in GMT
2027: 95%

Kritische prestatie-indicatoren

2024: 50% Maart Bespreken KPI's met Raad; Maart Raadsbrief; halfjaarlijks vaststellen door college & raad; Juni Resultaten ENSIA
2025: 95% Okt. Raad bepaalt KPI's; Maart halfjaarlijks vaststellen door college & raad
2026: 95% Okt. Raad bepaalt KPI's; Maart halfjaarlijks vaststellen door college & raad
2027: 95% Okt. Raad bepaalt KPI's; Maart halfjaarlijks vaststellen door college & raad; Okt. Bespreken KPI's met Raad



Verwerkers overeenkomsten & privacy analyses uitwerken

2024: 95% Verwerkingsovereenkomsten uitwerken (proces)
2025: Privacy analyses uitwerken
2026: 100%
2027: Aangetoond? Bestaat het?

3. Opvolging aanbevelingen - verbeteracties per aanbeveling

= continu aandacht

PU 19-4 | VSA mrt | MO juni | FA sept | SR sept

Oefening bedrijfs-continuïteit afdelingen

50% → 2024 → Nieuwe crisisoefening 80% → 2025 → Nieuwe crisisoefening 80% → 2026 → Nieuwe crisisoefening 100% → 2027

Autorisatie matrix met functiescheiding opstellen

50% → 2024 → 50% → 2025 → 100% → 2026 → 2027

Role Based Access Control

Cyclus toetsen & rapporteren / verbeteren interne controle

50% → 2024 → 80% halfjaarlijkse review gebruikers rechten → 85% Verbeterde interne controle → 2025 → halfjaarlijkse review gebruikers rechten → 90% Verbeterde interne controle → 2026 → 100% hlfjrs review gebruikers rechten → 2027

Verhogen bewustzijn medewerkers

2024: 20% — Leerlijn herhaling iBewust; 18-3 tot 1-9-24; mystery guest werkplek; vergrendelen/clean desk; Hogeschool Saxion 0-meting; privacy ambassadeur; NymaCon Phishing compagne

2025: 66% — jaarlijkse leerlijn iBewust; privacy ambassadeur

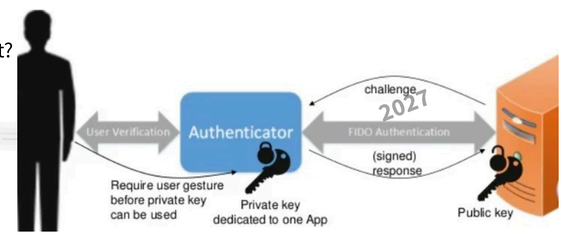
2026: 80% — jaarlijkse leerlijn iBewust; privacy ambassadeur

2027: jaarlijkse leerlijn iBewust

Phishing

2024 → 50% → 2025 → 2026

FIDO pilot?



Door:

Manager (RI)

CISO

Manager (RI)

CISO

Manager

CISO

Manager

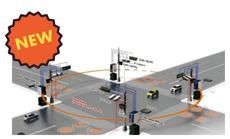
CISO

FG/Privacy officer en managers

NIEUW: Verbeteracties i.v.m. de NIS2/Cbw

= continu aandacht

Bestuur training cyberbeveiligingsrisico's



Operationele Technologie (OT)

analyse

ISMS

leveranciers overeenkomsten

2024 — 15% — 2025 — 50% — 2026 — 100% — 2027

2024 — 60% — 2025 — 80% — 2026 — 95% — 2027

2024 — 2025 — 100% — 2026 — 100% — 2027

2024 — 60% — 2025 — 95% — 2026 — 95% — 2027

2024 — 2025 — 2026 — Training cyberbeveiligingrisico's 100% — 2027

Door:

Groen = niet kritisch

Rood = kritisch

4. De kritische processen/applicaties

IBD risicoanalyse aanwezig

Kritische processen	Gevoelige applicatie(s)	Eigenaar
Verstrekken reisdocumenten	Reisdocumenten Aanvraag- en Archiefstation (RAAS).	**Publiekszaken**
Verstrekken rijbewijzen	Rijbewijs Backoffice Station.	
Verhuizingen		
Eerste inschrijving/hervestiging		
Spoedhuwelijken	Vrij BRP en BcGBA / GBA-V	
Burgerlijke stand - geboorte aangifte	Koppelmodule DIS; SIM	
Burgerlijke stand - overlijdens aangifte		
Klantenservice KCC	Typo3 CMS en Mitel CCM	
Vaststellen verkiezingsuitslag	OSV	
Innen leges	Key2betalen	
Financiën	ERPx (voorheen CODA) PowerToPay. ING electronic banking Gouw	**Financiën**
Verstrekken uitkeringen	Suites en Forus	**Inkomen, Zorg en Leerrecht**
Informatie cliënten uitkering	Suwinet	
Berichtenverkeer sociaal domein	Top corv	
Authenticeren en registreren	iPhone/iOS DigiD; Computerdevice	**PIF**
Uitbetalen salaris	Ge[redacted] en Beaufort	
Bewerken en opslag documenten	CorsaNext	
Toegangscontrole gebouwen	I-protect	

Kritische processen		Gevoelige applicatie(s)	Eigenaar
Verstrekken en beheren subsidies	✓		**MO**
Veiligheid	✓	BOPZ online,PGAx, VRGZ	**VJB**
Publiekscommunicatie	✓		
Informatievoorziening college tbv besluitvorming		iBabs, BBA	
Behandeling beroep en bezwaar	✓	JZ4ALL	
Beheer riool, verlichting en verkeer		Kikker	**Stadsbeheer**
Digitale handhaving en camerabewaking		CityPermit, VMC	
Automatisering	✓		**iRvN**
Toetsing lening& declaraties Toekomstbest. Wonen		DigiD, Corsa, Atlaz	**Stadsontwikkeling**
Toetsing Starterslening			
Vergunningverlening			**Stadsrealisatie**
Reserverings- en verhuurproces		Amis, Planon	**VSA**
Verkoop horeca en toegangsbewijzen		Kassa	
Gebouwenbeheersystemen			

5. Prioritering & keuzes

Impact/Inspanning matrix

Aanbevelingen 2025

- Informatie-beveiligings-beleid en uitwerking
- Certificering IRvN & afspraken met (cloud-) leveranciers
- BIO2 hanteert een risicogebaseerde aanpak (2025)
- Autorisatie matrix
- Cyclus toetsen & rapporteren / verbeteren interne controle
- NEW analyse
- NEW Operationele Technologie (OT)
- NEW ISMS

Aanbevelingen 2026

- NEW Bestuur training cyberbeveiligingsrisico's
- NEW THREAT

Continu aandacht, maar afgerond in: 2022 - 2025

- Personeel wijzigingsbeh…
- …ijzigings-beheer/ mutaties
- Bestuurlijke aandacht
- crisisteam Nijmegen
- Privacybeleid
- Bewustzijn
- KPI's
- wachtoord
- Afspraken met iRvN
- sys & system
- CISO FG Uitbreiding formatie
- Verwerkers overeenkomsten & privacy analyses

IMPACT

HIGH

- Bestuurlijke aandacht
- Autorisatie matrix
- NEW analyse
- Cyclus toetsen & rapporteren / verbeteren interne controle
- FIDO wachtwoord
- KPI's
- NEW Operationele Technologie (OT)

- BIO2 hanteert een risicogebaseerde aanpak (2025)
- Certificering IRvN & afspraken met (cloud-) leveranciers
- Informatie-beveiligings-beleid
- NEW ISMS

LOW

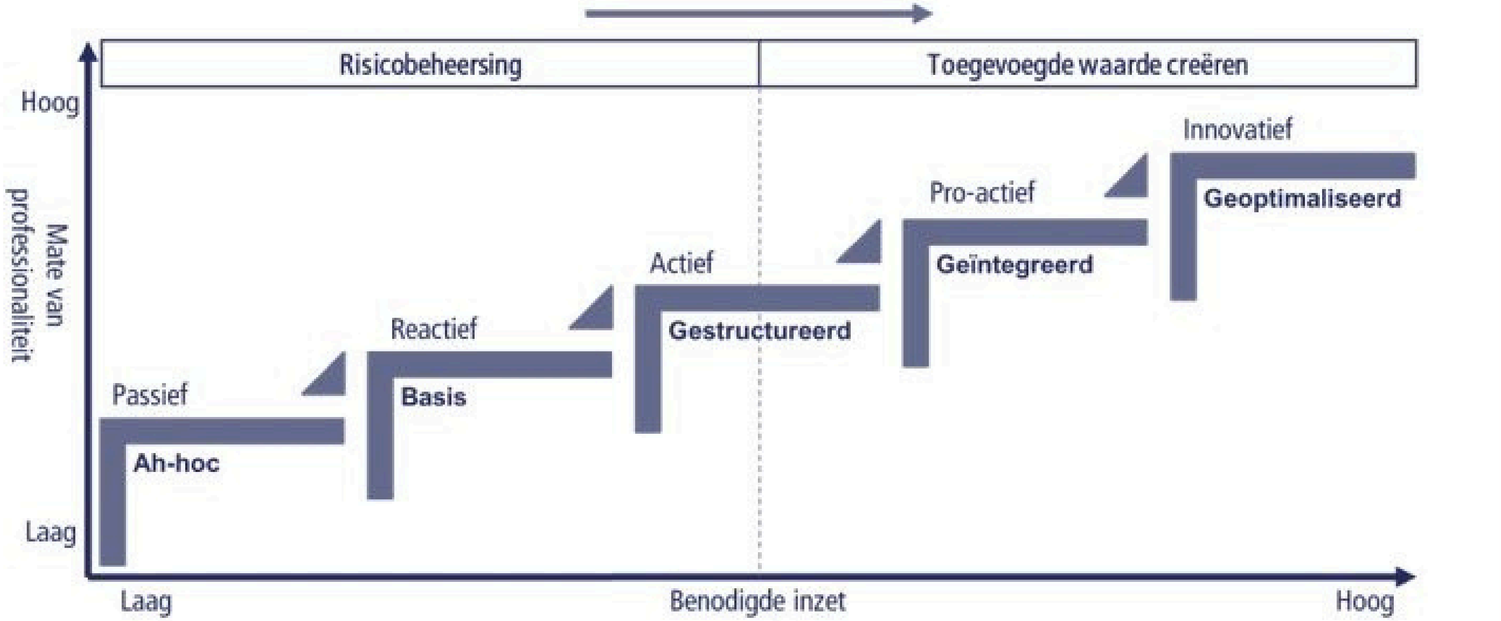
- BIO2 Afspraken met iRvN
- NEW Bestuur training cyberbeveiligingsrisico's
- Bewustzijn medew

- Verwerkers overeenkomsten & privacy analyses
- NEW THREAT

LOW HIGH

INSPANNING

Volwassenheidsniveau



- Niveau 1
- Niveau 2 ---> 2023/2024/2025
- Niveau 3 ---> 2026/2027
- Niveau 4
- Niveau 5

= continu aandacht

In 2025 bereikte verbeteracties

Verdeling BIO2 maatregelen

95% 2024 — 100% 2025 — 100% 2026 — 2027

Informatiebeveiligingsbeleid: verhelderen en actualiseren

25% 2024 — 75% 2025 — 100% 2026 — 2027

In 2024 bereikte verbeteracties

Verhogen bewustzijn medewerkers

20% 2024: Leerlijn herhaling iBewust; 18-3 tot 1-9-24; mystery guest werkplek; vergrendelen/clean desk; Hogeschool Saxion 0-meting; privacy ambassadeur; NymaCon Phishing compagne

66% 2025: jaarlijkse leerlijn iBewust; privacy ambassadeur

2026: jaarlijkse leerlijn iBewust; privacy ambassadeur

2027: jaarlijkse leerlijn iBewust

Tenant scheiding

50% 2024 — 100% 2025 — 2026 — 2027

BIO-verdeling met iRvN

95% 2024 — aanscherpen verdeling 100% — 100% 2025 — Mogelijke aanpassingen ivm de BIOS2 en NIS2 — 100% 2026 — CISO — 100% 2027

Door:

Raad — Privacy officer en FG

CISO — SO

Managers

CISO

CISO

= continu aandacht

In 2023 bereikte verbeteracties

sys & system

95% 2024 100% 2025 2026 2027

Wijzigings-beheer / mutaties

100% 2024 Controle 2025 Controle 2026 Controle 2027 Controle 100% Controle Controle Controle

Oefening crisisteam Nijmegen

25% 2023 100% Jaarlijkse crisisoefening 2024 100% Jaarlijkse crisisoefening 2025 100% Jaarlijkse crisisoefening 2026

Sterker wachtwoord

90% 2023 ww 8 tekens 2024 1 nov ww 15 tekens 95% 1 maart geïmplementeerd 2025 2026

Door:

= continu aandacht

In 2023 bereikte verbeteracties

Door:

Privacybeleid: verhelderen en actualiseren

Door: Privacy officer en FG

- 2023: 90% — Actualiseren
- 2024: 100% — Vastgesteld
- 2025
- 2026

Bestuurlijke aandacht & bewustzijn

Door: CISO, Privacy officer en FG

- 2023: 75% — tweemaal p/j terugkoppeling college aan raad (raadsbrieven en rapportages)
- 2024: ENSIA/BIO verantwoording & jaarrapport Privacy Raad gaat zelf KPI's bepalen — 95%
- 2025: tweemaal p/j terugkoppeling college aan raad (raadsbrieven en rapportages)
- 2026: ENSIA/BIO verantwoording & jaarrapport Privacy Raad gaat zelf KPI's bepalen — 95%

Uitbreiding formatie CISO & FG

Door: CISO, Privacy officer en FG

- 2023
- 2024: 100% — (formatie) budget toekennen
- 2025
- 2026

Verhogen bewustzijn medewerkers

Door: CISO, Privacy officer en FG

- 2023: 85% — e-learnings voltooid Privacy kits mystery guest en Ethisch hack; privacy ambassadeur; Veilig mailen; Escape room e-learning ransomware HackWijchen
- 2024: sterker ww & Bitwarden; privacy ambassadeur; e-learnings herhalen; Hackathon Nijmegen / NymaCon
- 2025: privacy ambassadeur; e-learnings herhalen; Hacknogintevullen
- 2026: 85%

Slotvragen

Vervolgafspraak prioritering/keuzes?

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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	2, 3, 6

10-09-25 Notulen klankbordgroep AVG

1. **Bespreking notulen vorige keer**
2. **Afscheid** 5.1.2e **welkom** 5.1.2e **(en** 5.1.2e **)**
3. **Jaarrapportage FG + Collegereactie**
4. **Must have DPIA's**
5. **Wvttk**

Notulen

Bespreking notulen vorige keer

- Geen opmerkingen

Afscheid 5.1.2e **welkom** 5.1.2e **(en** 5.1.2e **)**

- 5.1.2e zal vanaf 1 oktober optreden als nieuwe FG met als achtervang 5.1.2e.

Jaarrapportage FG

We moeten niet stilstaan na het AVG-proof plan. Het houdt namelijk niet op. Er komen nog meer spannende dingen aan. Er zijn bijvoorbeeld wel veel afgeronde DPIA's maar deze moeten we blijven controleren of bijwerken. Ook moet er meer focus naar de verwerkersovereenkomsten. Het sluiten van een verwerkersovereenkomst is stap 1, nu moeten we ook zorgen voor een goede uitvoering en naleving daarvan. We moeten als organisatie elkaar blijven steunen en controleren. Straks krijgen we meer ondersteuning door de claim.

5.1.2e stelt dat er nog werk aan de winkel is. We moeten bij volwassenheidsniveau 3 komen. 5.1.2e vraagt hoe het zit met het stijgen van de volwassenheidsniveaus. Komen daar grote verschillen in?

5.1.2e: de meetlat gaat tot en met 2027 niet meer veranderen, dit komt omdat er veel kritiek was op die continue veranderingen.

De FG rapportage is een meting van hoe je ervoor staat. Het is dus niet van belang hoe ver we zijn maar dat processen geregeld zijn en dat we verbeteringen zien. 5.1.2e kaart hierop aan dat het krijgen van meer steun door de claim die eraan komt, niet per definitie betekent dat alles gaat lukken binnen 2 jaar. We hebben een spannende belofte gedaan aan het bestuur. Het lijkt alsof het met extra ondersteuning moet gaan lukken, maar dit moeten we nog zien…

5.1.2e: Ten aanzien van het controlplan, zul je nooit helemaal bij zijn. Er komt altijd wel nieuwe wetgeving of DPIA's die vernieuwd moeten worden. Het gaat erom dat je niet achterloopt. We zijn nu een organisatie die de risico's in beeld heeft en je moet in staat zijn om hier op te acteren.

5.1.2e: Het is belang dat we deze gedachte ook goed uitleggen naar de raad toe.

Toelichting rapportage (5.1.2e)

- Meetlat verandert
- Verschuiving: meer focus op de verwerkersovereenkomsten dan de DPIA's
- Er zit groei in, we zijn langzaam steeds meer in control
- DPIA's moet ook vervangen worden constant.
- De producten zorgen niet voor 'in control zijn'… het gaat om je gedrag.
  5.1.2e: deze boodschap moeten we beter overbrengen → bewustzijn!

- IZL bijvoorbeeld → meer verwerkingen en DPIA's: meer intensiviteit van ons nodig.
  Het moeilijke is voor IZL dat ze nog heel veel moeten doen, terwijl zij eigenlijk al het meeste doen.
- Een andere afdeling heeft misschien minder te doen met privacy maar zij hebben hierdoor ook weinig bewustzijn, kennis en kunde.
- Omvang team Privacy is kwetsbaar → investeringen om groter team te maken.

5.1.2e: maatwerktrainingen kunnen veel bijdragen. We moeten naar een systeem om bewustzijn te creëren door middel van cursussen en trainingen. Omdat bewustzijn moeilijk meetbaar is en andere punten wel, is het soms lastig om te focussen op bewustzijn. Omdat je op de andere punten eerder wordt beoordeeld.

Reacties op jaarrapport

- We moeten aan de bak: bestuurlijk, communicatie (5.1.2e).
- Bewustwording is er bij PIF, ook al laten cijfers dit niet altijd zien. Hier zijn vaak ook weer goede redenen voor (5.1.2e).
- Het aantal inzageverzoeken BRP tellen niet meer mee als AVG-verzoeken.
- 4.4: de FG wil iets? → welk niveau wil je dit? (5.1.2e)
  Antwoord 5.1.2e: dit komt voort uit de wet (art. 35 AVG)
- Ook de FG constateert dat we meer man nodig hebben om het volwassenheidsniveau te kunnen bereiken.

Must have DPIA's

5.1.2e: een must-have lijst van DPIA's die we moeten hebben → overzicht. Deze DPIA's moeten het komende jaar geregeld zijn. Sommigen hebben we al, sommigen hebben bijwerking nodig en sommigen moeten er nog komen.

Afspraak: dit in het GMT brengen. Ook hiervoor moet bewustwording gecreëerd worden onder de managers. De managers moet een aanzet doen, dit zorgt voor aanscherping en opfrissing. We moeten bedenken hoe we dit in het GMT slim gaan agenderen in combinaties met de claim, de verwerkersovereenkomsten en de DPIA's (5.1.2e en 5.1.2e).

- 5.1.2e: een nuance → de must-have zijn niet de enige DPIA's die gedaan moeten worden!

Wvtkk

- 5.1.2e : ik heb jullie nodig om privacy te prioriteren in de stuurgroep organisatie ontwikkeling.
  Afspraak: 5.1.2e en 5.1.2e helpen 5.1.2e met de prioritering.
- 5.1.2e: MS365 DPIA → alles naar Teams of bedrijfsomgeving → 5.1.2e zegt dat Teams niet veel veiliger dan onze G-schijven. Nu nog geen oplossing.
- 5.1.2e : de afspraak is: geen bijzondere gegevens in Teams. Kijken naar waar de persoonsgegevens zitten. Waar moeten deze verwerkt worden? → als die er niet is, dan moet er een apart proces voor komen. Die is er nu nog niet, dus er wordt aan gewerkt (uitfaseren).

Rondvraag

- 5.1.2e: wat doen we met de volgende vergadering? → in januari inplannen.
  Er komen nog 2 raadsbrieven aan (in November). Elkaar meenemen via de mail om opmerkingen te geven.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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, 2

Notulen AVG stuurgroep 6-2-24

Notulen

Notulen vorige stuurgroep zijn verloren gegaan. We stellen vast dat de belangrijkste punten van vorige stuurgroep waren dat we het uitgebreid hebben gehad over mijn afdeling AVG proof. En dat we besloten hebben om de energiemeter zoals destijds voorgesteld vast te stellen.

IBD bijeenkomst

5.1.2e is bij IBD-bijeenkomst geweest voor een bijeenkomst over een nieuwe template voor een DPIA. Hieruit blijkt dat we qua DPIA op de goeie weg zijn. Het tweede punt was; waar sta je als gemeente. Daaruit blijkt dat we het niet zo gek doen. er zijn wel diverse gemeenten die voorlopen (Den Haag heeft. bv 300 DPIA's).
Enschede, Groningen zitten ongeveer op hetzelfde vlak. In Groningen en Enschede zit er wel meer tempo op de DPIA's. Groningen had er 100 per jaar, Enschede 60 voor een half jaar. Inhoudelijk zitten we op de goeie richting, qua niveau en insteek.
Vraag 5.1.2e: moeten wij dat template dan gaan gebruiken of is het meer ter toetsing?
Antwoord: nee, dit hoeven we niet exact te gebruiken. De invalshoeken die in het template staan moeten gebruikt worden, maar dat doen we momenteel al.

5.1.2e heeft wel gezien dat andere gemeenten het meer gestructureerd aanpakken. Zij zijn begonnen met het verwerkingsregister en hebben daar langs gelegd waarvoor DPIA's zijn en waarvoor niet.

5.1.2e brengt achtervang in. 5.1.2e: er is nog geen plaatsvervangend FG.
5.1.2e: hoe gaan we dat doen dan? Moeten we hiervoor een ROP maken of hoe willen we dat doen? de rol hoeft niet per se belegd te zijn Stadscontrol. De rol vereist wel bepaalde competenties en kennis.
Hoe groot is die rol? Moet dat uitgezet worden of kan iemand dat erbij doen?
Volgende keer als agendapunt terug laten komen: 'Wat doen we met de rol van plaatsvervangend FG?

Mijn afdeling AVG-proof

Kort memo maken met stand van zaken Mijn afdeling AVG Proof. Dit memo moet naar het GMT. In dit memo wordt aangegeven dat de afspraak was dat afronding Mijn afdeling AVG Proof eind 2023 plaats zou vinden, maar dat twee afdelingen daarin niet geslaagd zijn. Van deze afdelingen wordt verwacht dat zij uiterlijk 1 april de plannen om AVG-proof te worden inleveren. Er komt een check op het verwerkingsregister en daaruit volgt als het goed is een aantal DPIA's die nog gemaakt moeten worden. Dit wordt meegenomen in het memo.

5.1.2e en 5.1.2e maken zich zorgen over privacybewustzijn binnen MO. 5.1.2e gaat daarover in gesprek met 5.1.2e over de privacy binnen MO. We vermoeden dat de problemen een gevolg zijn van de 'eilandvorming' binnen MO, waarbij de meeste medewerkers zich bezig houden met hun eigen thema. Daardoor is het moeilijk om te sturen op zaken zoals privacy, want dan zijn er teveel aanspreekpunten. Er is overigens ook grote doorstroom, mogelijk is de inwerkprocedure niet compleet.
De uitkomsten van de Mijn afdeling AVG-proof plannen worden meegenomen in de prestatiedialoog. De voortgang van het uitvoeren van het plan wordt daarin ook meegenomen.

Lijst DPIA's

5.1.2e: hoe sturen we op DPIA's? wil een concernmanager daarop sturen? Weet een concernmanager welke DPIA's er allemaal zijn en lopen?
GMT gaat het erover hebben hoe ze willen sturen op dit soort dingen (DPIA's, maar ook archivering, e-learnings etc).

Controlplannen

De afspraak was om 15 januari alle stukken in te leveren. Twee afdelingen waren op tijd. De andere afdelingen waren een week later. Twee afdelingen hebben nog niet aangeleverd, dat zijn MO en IZL. MO is bewust van dat de aanlevering nog niet voldoende is.
Bij IZL is overleg geweest over de verlenging van de termijn. De naleving lijkt in orde, maar is veel werk. IZL heeft gevraagd om uitstel en levert op tijd aan om meegenomen te worden in het Controlplan 2023.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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

1802Notulen klankbordgroep AVG 16-1

Notulen

Akkoord met notulen.

5.1.2e gaat in op plv. FG. Zou Stadscontrol niet zelf een plv. FG in huis moeten hebben? 5.1.2e is net begonnen, zou dat een optie zijn? Nu is 5.1.2e plv. FG, is dat een wenselijke situatie? Afgelopen jaar heeft 5.1.2e 2 keer een casus meegelopen, dat is nog wel te doen. Maar in de toekomst als het nodig is, dan kan hij 5.1.2e niet volledig overnemen, mocht dat nodig zijn. We gaan toewerken naar een andere plv. FG dan 5.1.2e, in principe wordt dat 5.1.2e.
Afspraak: in Q2 (juni) komen we in dit gezelschap terug en bespreken we wie FG wordt en plv. FG. 5.1.2e is vanaf 1 oktober plv. FG, tot die tijd 5.1.2e. Zo valt het gelijktijdig met de vervanging van 5.1.2e als FG. In de tussentijd loopt 5.1.2e al mee binnen team privacy.

Opdracht klankbordgroep AVG

Opdracht stuurgroep was klaar; mijn afdeling AVG proof is afgerond. Nieuwe opdracht voor de klankbordgroep is monitoren van de grote doelstelling uit privacybeleid; het halen van volwassenheidsniveau 3.

Nog doen: memo vertalen naar GMT-voorstel, dat doet 5.1.2e in samenwerking met 5.1.2e. Dit voorstel is ter informatie, we stoppen de huidige opdracht en maken een nieuwe (decharge).

Controlplan

Morgen (17-1) deadline van aanleveren. SR, PU, SB, FA Hebben al aangeleverd. PIF, VJB, VSA nog geen informatie. Stadscontrol komt op tijd af. IZL krijgt DPIA's wel af, vwo's niet, MO komt woensdag, ST komt eind januari. Griffie en rekenkamer hebben rechtstreekse lijn met 5.1.2e.

Dit geldt ook voor de gemeentelijke ombudsman, die moet straks ook AVG proof zijn.

Directie hoeft eigenstandig niks aan te leveren.

5.1.2e wacht tot komende woensdag (22-1) voordat de herinnering stuurt.

Bij het nieuwe controlplan gaat 5.1.2e het stoplichtenschema updaten. Afdelingen krijgen dan dus nieuwe kleuren. Bij het GMT-voorstel moeten we duidelijk aangeven dat de kleuren van het huidige controlplan over 2023 gaan, dus niet over afgelopen jaar.

Mijn afdeling AVG proof

Alle plannen zijn binnen. IZL heeft laatste werkdag van 2024 het plan aangeleverd. Naar verwachting gaat MO dit jaar ook van rood af.

Raadsinformatiebrief

Is al een tijdje terug verstuurd. 5.1.2e vindt wel dat er nog een verbetering in zit in het vereenvoudigen van de brief. De brief kan slimmer. Tobias en 5.1.2e zijn daar niet op aangeslagen, maar alsnog goed om dat mee te nemen.

Met accountant is gesproken over IT-roadmap, ook daar moet eigenlijk een taalversimpeling plaatsvinden. Stappenplan in de roadmap wordt herijkt, met als doel dat het meer 'bekende' taal wordt.

Het lijkt erop dat de stap naar niveau 3 alleen maar groter wordt, oa gelet op aankomende wetgeving. De stap naar niveau 3 is niet hetzelfde als 2 jaar terug; het lijkt steeds moeilijker te worden om niveau 3 te bereiken. Er komen meer eisen bij, ook al is het doel niet veranderd. 5.1.2e: de doelpalen verschuiven.

De delta tussen 2 en 3 kunnen we heel reëel schetsen richting Tobias en bgm, en daarbij aangeven welke kosten, belemmering en administratieve last daarbij komen kijken.

5.1.2e: Elke stap vraagt meer van de organisatie; dat moet ook meegenomen worden. Je moet wel de afweging blijven maken tussen de druk die je legt op de organisatie, en wat het oplevert om AVG-proof te zijn. Het is wel zo dat we nu in een transitiefase zitten; als afdelingen elk jaar hetzelfde op moeten leveren, wordt het wel minder werk op den duur.

5.1.2e heeft wel het gevoel dat met de matrixen en persona's die we maken, dat we doelgerichter aan kunnen pakken. 5.1.2e heeft zorgen bij de discussie over de staf die gemeentebreed lopen. Het lijkt erop dat afdelingen met het aantrekken van een staf, soms interne bedrijfsvoeringsafdelingen overslaan. De staf is fijn als aanspreekpunt, maar de lijnorganisatie moet niet vergeten dat sommige punten onderdeel zijn van hun werk en dat soms andere afdelingen ook hulp kunnen bieden.

Het is een beleidsveld in ontwikkeling.

iBewustwording management

Er is een RASCI vastgesteld, daar zijn de verantwoordelijkheden van de collega's met een rol hierin vastgesteld. 5.1.2e gaf destijds aan; de managers hebben hier een belangrijke rol in. Het plan was om een casus te bespreken in het GMT. Dat is niet doorgegaan en zodoende bleef de vraag liggen wat we eraan gaan doen om het bewustzijn van managers op te krikken en goed te borgen.

Er ligt nu een plan, nu is de vraag hoe we dit gaan agenderen in het GMT. We willen in de MT's een casus op maat bespreken. We hoeven het GMT niet mee te nemen in de inhoud, een hamerstuk zou voldoende moeten zijn. 5.1.2e brengt het hamerstuk in binnen het GMT. Dan kunnen GMT-leden aangeven of ze er nog op willen verdiepen.

Als je dit apart agendeert bij MT's, voelt het als extra werk. Als je het onderdeel maakt van de termijnagenda, dan voelt het niet als extra werk. Je zou dan wel de casus binnen

45 moeten doen, anders blijft niks over van het MT. Je kan dit overwegen bij afdelingen waar het belang minder groot is. Je kan dan werken met een ‘light’ versie. Dat nog toevoegen aan het voorstel. Afdelingen daarbij inschatten op risico.

De halfjaarlijkse sessie voor nieuwe managers halen we er in principe uit, zodra die is opgenomen in het MD-programma voor nieuwe managers.

De belangen per thema verschillen per afdeling. Je zou tot de conclusie kunnen komen dat iBewustzijn voor sommige afdelingen essentieel is, maar voor andere minder.

To do voor voorstel hamerstuk: bespreekstuk aanpassen naar hamerstuk. RASCI meesturen als bijlage. We updaten de RASCI en doen die samen met het voortel voor iBewustzijn door het GMT als hamerstuk.

Eerste keer langskomen bij PIF.

WVTTK

Cyclus van klankbordgroep loopt niet lekker met de raadsinformatiebrief. Concept raadsinformatiebrief delen we via Teams met de leden van de klankbordgroep.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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, 2

DPIA Oordeel FG gemeente Nijmegen

DPIA: Doorontwikkeling Mijn Geldzaken (Innovadis)

Inleiding

Hierbij het oordeel van de FG Gemeente Nijmegen over de DPIA 'Doorontwikkeling Mijn Geldzaken (Innovadis)'. 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 oktober 2023 – februari 2024 hebben 5.1.2e , 5.1.2e en 5.1.2e 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 'Doorontwikkeling Mijn Geldzaken (Innovadis)' d.d. 06/02/2024. Deze versie vormt de onderlegger voor deze toetsing.

Bij deze DPIA horen de volgende bijlagen:
1. Getekende verwerkersovereenkomst Allegro
2. NL 920.1.1 - Innovadis B.V. - ISO 27001Oordeel matrix
3. 2023-2-3 IBD model VWO GN-Innovadis v1.0 -1x signed
4. Handleiding klantenportaal Den Bosch

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?	Neen.	Akkoord. Er dient wél z.s.m. (vóór 01/04/24) een DPIA aangaande de werking van het workflow systeem Allegro gemaakt te worden. Eventuele uitkomsten hiervan dienen in de naleving van déze DPIA meegenomen te worden.
2. Is het ethisch / politiek bestuurlijk verantwoord?	Ja. De GKB houdt zich bezig met sociale kredietverstrekking. De gemeente is vanuit de WGS verantwoordelijk voor de schuldhulpverlening. Het portaal Mijn Geldzaken heeft als doel om klanten beter te ondersteunen, zodat het proces klantvriendelijker wordt. Zij kunnen ieder moment hun gegevens inzien en de voortgang volgen. Aanvragen kunnen digitaal worden ingediend. Intermediairs krijgen met toestemming van de klant toegang.	Akkoord. De doorontwikkeling en uitbreiding van Mijn Geldzaken levert een verbetering van de dienstverlening op. De klanten kunnen in hun portaal de toestemming aan intermediairs ook weer intrekken. Klanten worden autonomer en zelfredzamer.
3. Juridische toets 3a. Doel / grondslag	3.a. Doel van deze gegevensverwerkingen: Algemeen belang (art. 6 lid 1 sub e). Schuldhulpverlening: De gemeente is volgens de Wet Gemeentelijke Schuldhulpverlening (WGS) artikel 3.1 lid a verantwoordelijk voor schuldhulpverlening. Budgetbeheer mogen we uitvoeren volgens de Wet op het financieel toezicht (Wft) artikel 3.5. Voor de GKB: De GKB houdt zich bezig met sociale kredietverstrekking. Dit is opgenomen in het Bankreglement 2017. De GKB moet zich houden aan de bepalingen in de Wet op het consumentenkrediet (Wck) en de Wet financiering decentrale overheden (Wet fido). Daarnaast is Het Besluit Gedragstoezicht financiële ondernemingen BGfo van toepassing.	3.a. Akkoord. Genoemde artikelen vormen het uitgangspunt van de uitvoering.
3.b. Proportionaliteit	3.b. 1. De GKB verstrekt sociale kredieten, omdat mensen hiervoor niet bij andere banken terecht kunnen. De gemeente heeft een wettelijke verplichting om inwoners met problematische schulden te helpen. 2. De gemeente heeft vanuit de WGS de verplichting om inwoners met problematische schulden te ondersteunen bij het vinden van een oplossing voor hun financiële situatie. De gemeente moet de schuldhulpverlening uitvoeren. Als we niet helpen komen inwoners nog verder in de problemen.	3.b. In de DPIA staat vermeld: 'We vragen niet alles op, alleen datgene wat nodig is'. Akkoord, met dien verstande dat per case moet worden gelogd wat de afwegingen zijn geweest om gegevens vast te leggen.

3.c. Subsidiariteit	3.c. De GKB houdt zich bezig met sociale kredietverstrekking voor inwoners die vallen onder het werkgebied. Door het digitaal maken van de aanvragen wordt tijd en moeite bespaard. We kunnen mensen beter helpen en er blijft meer tijd over om klanten te begeleiden. Door de uitbreiding van Mijn Geldzaken krijgt de klant meer zeggenschap over zijn eigen traject. Al dan niet met hulp van een intermediair. De klant wordt beter ondersteund, is autonomer en sneller zelfredzaam.	3.c. Akkoord.
3.d. Persoonsgegevens buiten EER gebruikt?	3.d. Neen	3.d. Akkoord.
3.e.Andere partijen betrokken?	3.e. Ja De regiogemeenten hebben de rol van verwerkingsverantwoordelijke voor zover de aanvrager van de desbetreffende lening woonachtig is in die gemeente. Kred'it en Innovadis hebben de rol van verwerker, met beiden hebben we een verwerkingsovereenkomst.	3.e. Akkoord. Kred'it is de softwareleverancier van Allegro. Hiervoor is met Kred'it B.V. op 21-12-2018 een verwerkersovereenkomst gesloten. Innovadis levert de diensten hosting, gebruik, onderhoud en beheer van Mijn Geldzaken. Hiervoor is op 09-02-2023 een verwerkersovereenkomst gesloten. Voor de regiogemeenten zijn nog geen overeenkomsten afgesloten.
3.f. Hoe lang worden gegevens bewaard en termijn en wijze van vernietiging?	3.f. Er is geen sprake van opslag van gegevens binnen Mijn Geldzaken. De gegevens worden in Allegro opgeslagen. Alle documenten worden in Corsa gezet. Daarvoor gelden de reguliere bewaartermijnen van Allegro en Corsa.	3.f. Akkoord, met dien verstande dat z.s.m. een DPIA voor Allegro moet worden opgesteld.
3.g. Hoe worden gegevens beveiligd?	3.g. Toegang tot Allegro gaat via persoonlijke autorisatie. Kred'it is NEN/ISO 27001 gecertificeerd. Periodieke externe controles in de vorm van audits worden uitgevoerd. Innovadis is ISO27001:2017 gecertificeerd door Brand Compliance B.V.	3.g. Akkoord. Hiervoor dient een autorisatiematrix aanwezig te zijn.
4. Risico's en voorgestelde maatregelen	Deze zijn afdoende beschreven.	Akkoord, voor zover de beschreven risico's. Restrisico zit in toekenning en intrekking van autorisaties.

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 zelf kent een "laag" risico.

NB.
Er dient z.s.m. een DPIA aangaande de werking van het workflow systeem 'Allegro' gemaakt te worden.

Daarnaast staan nog wat punten open die z.s.m. afgehandeld dienen te worden. In de DPIA worden deze genoemd:
'Maatregelen die nog noodzakelijk zijn:

- verwerkersovereenkomsten met de regiogemeenten
- Hoe check je of iemand een intermediair is? Kunnen zij inloggen via E-herkenning of machtiging DigiD?
- Opzet van controle logging, zodat duidelijk wordt of iemand met toestemming/autorisatie inlogt.'

Tevens dient het volgende opgepakt te worden:
In de DPIA staat vermeld: 'We vragen niet alles op, alleen datgene wat nodig is'.
Akkoord, met dien verstande dat per case moet worden gelogd wat de afwegingen zijn geweest om gegevens vast te leggen.

Eind 2024 zal deze DPIA op naleving getoetst worden.
Daar wordt gelet op de toekenning en intrekking van de autorisaties en op logging van uitvraag gegevens.

Ik adviseer hiermee positief en daarmee zijn de resterende risico's "aanvaardbaar".

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

PK/06/02/2024. DPIA 72.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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

DPIA Oordeel FG gemeente Nijmegen

DPIA: Individuele Inkomenstoeslag (ITT)

Inleiding

Hierbij het oordeel van de FG Gemeente Nijmegen over de DPIA 'Individuele Inkomenstoeslag (ITT)'. 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 januari – februari 2024 hebben 5.1.2e , 5.1.2e , 5.1.2e en 5.1.2e 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 'Individuele Inkomenstoeslag (ITT)' d.d. 30/01/2024.
Deze versie vormt de onderlegger voor deze toetsing.

Bij deze DPIA horen de volgende bijlagen:
1. Procestekening Individuele inkomens toeslag (is als bijlage aan de DPIA toegevoegd).

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?	Neen.	Akkoord. Er is wel een DPIA gemaakt betreft de Suite Sociaal Domein. Er is ook een DPIA gemaakt over uitwisseling van gegevens met het Inlichtingenbureau. Beide relevant omdat deze onderdeel zijn van het verwerkingsproces ITT.
2. Is het ethisch / politiek bestuurlijk verantwoord?	Ja. Hierdoor wordt het bereik van onze inkomensondersteunende regelingen (IIT) verbeterd en kunnen inwoners die het nodig hebben meer gebruik zullen maken van de regelingen.	Akkoord. Voor inwoners ontstaat er namelijk een eenduidige, laagdrempelige en gebruikersvriendelijke manier van aanvragen. Zowel voor een digitale aanvraag als een aanvraag op papier.
3. Juridische toets 3a. Doel / grondslag	3.a. Het doel: alle inwoners die daar recht op hebben maken gebruik van de inkomensregelingen. Een digitale toegangspoort waar alle inkomensregelingen op begrijpelijke wijze worden aangeboden en zo simpel mogelijk zijn aan te vragen maakt de drempel tot het doen van een aanvraag kleiner. Grondslag: De verwerking is een wettelijke verplichting op grond van artikel 36 Participatiewet. In artikel 8 lid 1 sub b Participatiewet wordt aangegeven dat de gemeente een verordening met regels moet opstellen voor de individuele inkomenstoeslag.	3.a. Akkoord. Zie de Verordening Individuele Inkomenstoeslag 2017 | Lokale wet- en regelgeving (overheid.nl). In de verordening zijn onder andere regels te vinden over het begrip "langdurig laag inkomen" en "zicht op inkomensverbetering".
3.b. Proportionaliteit	3.b. Het gaat om het uitvoeren van een wettelijke taak. De gegevens moeten verwerkt worden anders kan de aanvraag niet beoordeeld worden. Inwoners ontvangen in ruil voor deze gegevens (meerdere jaren) de individuele inkomenstoeslag.	3.b. In de DPIA staat vermeld: 'We vragen geen gegevens op die we niet nodig hebben'. Akkoord, met dien verstande dat per case moet worden gelogd wat de afwegingen zijn geweest om gegevens vast te leggen. Risico: te veel gegevens worden vastgelegd (middelhoog risico).
3.c. Subsidiariteit	3.c. Gegevens moeten verwerkt worden anders kan de aanvraag niet beoordeeld worden. Er wordt gewerkt binnen de kaders van kaders de Participatiewet, verordening en beleidsregel.	3.c. Akkoord. Een manier om minder gegevens op te vragen is door aanpassing van de verordening en beleidsregel van de gemeente Nijmegen. De gemeenteraad mag namelijk zelf bij verordening regels bepalen voor wat "een langdurig laag inkomen" en "zicht op inkomensverbetering" is.
3.d. Persoonsgegevens buiten EER gebruikt?	3.d. Neen	3.d. Akkoord.
3.e.Andere partijen betrokken?	3.e. Ja - Het Inlichtingenbureau. - Gegevens worden verwerkt in de Suite Sociaal Domein (Centric).	3.e. Akkoord. Zie DPIA Uitwisseling gegevens Inlichtingenbureau en DPIA Suite Sociaal Domein.

3.f. Hoe lang worden gegevens bewaard en termijn en wijze van vernietiging?	3.f. Eénmalige bijstandsuitkeringen dienen 10 jaar bewaard te worden. Het is dus niet nodig deze verstrekkingen te bewaren tot na het einde van de bijstandsuitkering.	3.f. Akkoord. Afdeling BDI zorgt voor vernietiging in samenspraak met de Regionale Archiefinspecteur.
3.g. Hoe worden gegevens beveiligd?	3.g. Gegevens worden bewaard in de Suite voor Sociaal Domein van Centric (data alleen toegankelijk voor IRVN en Nijmegen). De technische en organisatorische inrichtingsaspecten van de Suite zijn ook van toepassing op dit project.	3.g. Akkoord. Autorisatie, bewaartermijnen, logging zijn reeds geregeld in de Suite en voor documenten in Corsa. Hiervoor dient een autorisatiematrix aanwezig te zijn.
4. Risico's en voorgestelde maatregelen	Deze zijn afdoende beschreven.	Akkoord, voor zover de beschreven risico's. Restrisico zit in toekenning en intrekking van autorisaties en een goede logging van de afweging van uitvraag van benodigde gegevens per aanvraag.

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 zelf kent een "middel-hoog" risico.

Tevens dient het volgende opgepakt te worden:
In de DPIA staat vermeld: 'We vragen geen gegevens op die we niet nodig hebben'.
Akkoord, met dien verstande dat per case moet worden gelogd wat de afwegingen zijn geweest om gegevens vast te leggen.

Eind 2024 zal deze DPIA op naleving getoetst worden.
Daar wordt gelet op de toekenning en intrekking van de autorisaties en op logging van uitvraag gegevens.

Ik adviseer hiermee positief en daarmee zijn de resterende risico's "aanvaardbaar".

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

PK/13/02/2024. DPIA 73.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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

DPIA Oordeel FG gemeente Nijmegen

DPIA: Gebruik van inpandige foto's in WOZ-proces.

Inleiding

Hierbij het oordeel van de FG Gemeente Nijmegen over de DPIA 'Gebruik van inpandige foto's in WOZ-proces.'. 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 januari – februari 2024 hebben 5.1.2e ,5.1.2e en 5.1.2e 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 'Gebruik van inpandige foto's in WOZ-proces.' d.d. 22/02/2024. Deze versie vormt de onderlegger voor deze toetsing.

Bij deze DPIA horen de volgende bijlagen:

1. DPIA Gemeentebelastingen 29-11-2022 Definitief
2. Verwerkersovereenkomst applicatie gemeentelijke heffingen
3. Instructie-voor-gebruik-fotos-voor-WOZ-waardebepaling-2024
4. Uitvoeren bezwaar beroep

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.	Akkoord. Ja, voor Gemeentebelastingen is een DPIA opgesteld, deze DPIA over het gebruik van inpandige foto's in WOZ-proces sluit hier op aan.
2. Is het ethisch / politiek bestuurlijk verantwoord?	Ja. In eerste instantie wordt bij het ontvangen van inpandige foto's ingezet op het voorkomen van een verwerking van persoonsgegevens. De bewoner krijgt vooraf informatie om te voorkomen dat toch persoonsgegevens zichtbaar zijn op de inpandige foto's.	Akkoord. Is dat wel het geval, dan wordt de bewoner geïnformeerd over het feit dat er foto's zijn aangeleverd die persoonsgegevens bevatten, dat deze gegevens niet in het WOZ-waarderingsproces verwerkt mogen worden en daarom vernietigd zijn. Indien nodig wordt de bewoner verzocht nieuwe foto's aan te leveren.
3. Juridische toets 3a. Doel / grondslag	3.a. Doel: Indien belastingplichtige bezwaar heeft gemaakt tegen de vastgestelde waarde van een object tegen de objectkenmerken zijn onderbouwende gegevens noodzakelijk. Een waardebepaler kan op basis van de opgevraagde inpandige foto's of door belastingplichtige ingevuld formulier, beter beoordelen of het bezwaarschrift gegrond of ongegrond wordt verklaard. Grondslag: In het kader van artikel 20 Wet WOZ kunnen er regels worden gesteld voor de onderbouwing en de uitvoering van de waardebepaling. In artikel 3 van de Uitvoeringsregeling instructie waardebepaling Wet waardering onroerende zaken is opgenomen dat het College van Burgemeester en Wethouders voortdurend de waarde relevante objectgegevens verzamelt, analyseert en registreert.	3.a. Akkoord. Voor een nauwkeurige waardebepaling is informatie nodig over de objectkenmerken van een woning. Daarbij is een onderscheid tussen primaire objectkenmerken en secundaire objectkenmerken. Primaire objectkenmerken van een woning zijn bijvoorbeeld woonoppervlakte, perceel grootte en bouwjaar. De secundaire objectkenmerken van een woning zijn bijvoorbeeld de kwaliteit, de onderhoudstoestand of het voorzieningenniveau van een woning. Secundaire kenmerken zijn aan veranderingen onderhevig en hebben invloed op de waarde van de onroerende zaak. Secundaire objectkenmerken kunnen deels van buitenaf worden beoordeeld en gecontroleerd, maar vergen ook informatie over inpandige eigenschappen van de woning. Het inwinnen van deze informatie, na het indienen van een bezwaarschrift, gericht tegen de hoogte van de vastgestelde waarde, door belastingplichtige, kan op verschillende manieren plaatsvinden: 1. tijdens een inpandige opname; 2. met een (digitaal) inlichtingenformulier; of 3. via inpandige foto's.
3.b. Proportionaliteit	3.b. De betrokkene kan zelf de keuze maken om een inlichtingenformulier in te vullen of inpandige foto's in te zenden.	3.b. Keuze voor een van beide routes heeft geen effect op de beoordeling an sich. Het is wél zo dat foto's vaak een beter beeld geven dan schriftelijke informatie. Dit alles ter ondersteuning van het bezwaar dat een inwoner maakt.

3.c. Subsidiariteit	3.c. De bezwaarmaker heeft drie mogelijkheden om zijn bezwaar te ondersteunen: 1. tijdens een inpandige opname; 2. met een (digitaal) inlichtingenformulier; of 3. via inpandige foto's.	3.c. Akkoord. Het is aan de bezwaarmaker om een keuze te maken. Indien een keuze voor route 3 wordt gemaakt dient de beoordelaar conform deze DPIA te werk te gaan.
3.d. Persoonsgegevens buiten EER gebruikt?	3.d. Neen	3.d. Akkoord.
3.e.Andere partijen betrokken?	3.e. Ja - De belastingplichtige levert de foto's aan; - In de module binnen GouwBelastingen worden de foto's ingelezen en worden gekoppeld aan het betreffende object. - GouwIT is verwerker en de Gemeente Nijmegen is verwerkingsverantwoordelijke.	3.e. Akkoord. Zie bijlagen: 1. DPIA Gemeentebelastingen 29-11-2022 Definitief 2. Verwerkersovereenkomst applicatie gemeentelijke heffingen
3.f. Hoe lang worden gegevens bewaard en termijn en wijze van vernietiging?	3.f. - Belastinggegevens worden 7 jaar, conform de selectielijst bewaard, het jaar daarna worden de gegevens vernietigd. - Voor de overige foto's (die dus geen persoonsgegevens bevatten) geldt dat deze verwijderd worden op het moment dat ze niet meer noodzakelijk zijn voor het juist vaststellen of aantonen van de woningkenmerken in de WOZ-waarderingsprocedure.	3.f. Akkoord. Aangeleverde foto's die persoonsgegevens bevatten worden bij voorkeur helemaal niet opgeslagen (afhankelijk van wat de gebruikte (technische) middelen en methoden zijn die worden ingezet – niet in alle gevallen zal het mogelijk zijn om aangeleverde foto's niet (zeer kortstondig) op te slaan en na ontvangst en constatering direct vernietigd.
3.g. Hoe worden gegevens beveiligd?	3.g. De softwareleverancier GouwIT is in het bezit van een ISO 27001 en ISAE3402 type II certificeringen. De verwerkte gegevens worden gelogd bij de softwareleverancier die tevens voor een dagelijkse back-up zorgen	3.g. Akkoord. Jaarlijks worden de verslagen van de uitgevoerde audits opgevraagd bij de software leverancier.
4. Risico's en voorgestelde maatregelen	Deze zijn afdoende beschreven.	Akkoord. Restrisico: Het is altijd mogelijk dat er inpandige foto's worden toegezonden met persoonsgegevens erop, deze foto's worden per direct verwijderd en vernietigd.

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 zelf kent een "laag" risico.

Eind 2024 zal deze DPIA op naleving getoetst worden.
Daar wordt gelet op de toekenning en intrekking van de autorisaties en op logging.

Ik adviseer hiermee positief en daarmee zijn de resterende risico's "aanvaardbaar".

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

PK/26/02/2024. DPIA 74.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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

DPIA Oordeel FG gemeente Nijmegen

DPIA: Documentscanner, gezichtsscanner en biometrie

Inleiding

Hierbij het oordeel van de FG Gemeente Nijmegen over de DPIA 'Documentscanner, gezichtsscanner en biometrie'. 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 januari – februari 2024 hebben 5.1.2e , 5.1.2e en 5.1.2e 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 'Documentscanner, gezichtsscanner en biometrie' d.d. 22/02/2024.
Deze versie vormt de onderlegger voor deze toetsing.

Bij deze DPIA horen de volgende bijlagen:

1. Gegevensbeschermingseffectbeoordeling (PIA) Rijksdienst voor Identiteitsgegevens RNI
2. Implementatie-opzet gemeente ORIBI ID-Solutions

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?	Ten dele. A (Documentscanner): Nee B (Gezichtsscanner) :Ja, zie DPIA RNI en de landelijke DPIA RNI (bijlage) C (Biometrie): Nee	Akkoord. Zie ook bijlagen.
2. Is het ethisch / politiek bestuurlijk verantwoord?	Ja. Uit ervaring is gebleken dat de impact en gevolgen van fraude en ondermijning steeds meer toenemen. Daarom is het vaststellen van de identiteit van een persoon op basis van een geldig identiteitsdocument belangrijk. Naast het controleren van de echtheid van het document wordt ook beoordeeld of het document wel bij de eigenaar hoort. Daarvoor wordt de foto van het document met de aanwezige persoon vergeleken. Voor aanvraag en uitgifte van reisdocumenten is wettelijk de afname van de volgende biometrische gegevens vastgesteld.	Akkoord. Gezichtsvergelijking is moeilijk en de mens kan hierin fouten maken. Uit onderzoek blijkt dat de ondersteuning van geautomatiseerde gezichtsvergelijking tot betere resultaten leidt.
3. Juridische toets 3a. Doel / grondslag	3.a. *Doel*: A. Documentscanner Verwerking is noodzakelijk voor het deugdelijk vaststellen van de identiteit. B. Gezichtsscanner Verwerking is noodzakelijk voor het deugdelijk vaststellen van de identiteit. De automatische gezichtsvergelijking ondersteunt de medewerker aan de balie in de beoordeling of de persoon en het document daadwerkelijk bij elkaar horen en of daarmee de identiteit van de persoon vastgesteld kan worden. C. Biometrie Verwerking is noodzakelijk voor de uitvoering van een wettelijke taak waarbij het gaat om het aanvragen van een reisdocument. *Grondslag*: Verwerking is noodzakelijk voor de uitvoering van wettelijke taken	3.a. Akkoord. Betreft: - Paspoortwet. - Wet BRP. - Wet reglement rijbewijzen. - Wet AWB. (zie uitvoerig in de DPIA 2.2. Grondslagen).
3.b. Proportionaliteit	3.b. Document- en gezichtsherkenning: De inbreuk van de privacy wordt geminimaliseerd door het niet bewaren van persoonsgegevens (langer dan de afspraak), maar enkel de uitslag (enkel bij een negatieve uitslag). Biometrie: Voor het uitgeven van reisdocumenten zijn het verwerken van vingerafdrukken, pasfoto en een handtekening wettelijke voorgeschreven.	3.b. Akkoord.

3.c. Subsidiariteit	3.c. De instellingen van de apparatuur zijn hiervoor van belang. Het minst ingrijpende proces is het draaien op onze lokale server gebleken, waarbij geen dataverwerkers zijn betrokken. Daarnaast is het mogelijk om de instelling aan te zetten dat scans niet worden gedownload. Het bewaren van deze geminimaliseerde uitslag: een rapportage waarop enkel de uitslag te zien is in de vorm van een smiley, is noodzakelijk voor het kunnen hanteren van een vierogen principe bij uitvoering van het proces.	3.c. Akkoord. De gezichtsopname en de documentscan worden niet opgeslagen. Systeembeheerders hebben dus geen toegang daartoe. De live opname van de persoon wordt niet opgeslagen en is alleen gedurende het proces van identiteitsvaststelling in het systeem geregistreerd en voor de medewerker achter de balie zichtbaar. Het wordt dus tijdelijk gebruikt.
3.d. Persoonsgegevens buiten EER gebruikt?	3.d. Neen	3.d. Akkoord.
3.e.Andere partijen betrokken?	3.e. Ja *Burger*: Betrokkene, ondervindt de consequenties van de documentscan en gezichtsvergelijking, overhandigt zijn identiteitsdocumenten en werkt mee aan het maken van live document – en gezichtsopname. Dit geldt ook voor de vingerafdruk (biometrie). *Gemeente Nijmegen*: Verantwoordelijk voor het identificatieproces. Gemeente is verwerkingsverantwoordelijk. *Oribi en JCC* (geautomatiseerde vergelijkings-systemen): Beide staan lokaal of in de cloud.	3.e. Akkoord. De IRVN verwijdert in opdracht van de verantwoordelijke (gemeente Nijmegen) de gegevens, dit doen Oribi of JCC niet zelf. Zij zijn alleen verantwoordelijk voor het aanleveren van de apparatuur en de software.
3.f. Hoe lang worden gegevens bewaard en termijn en wijze van vernietiging?	3.f. A en B (Document – en gezichtsscanner): Voor het primaire doel, het deugdelijk vaststellen van de identiteit, zijn de gezichts- en documentscan niet langer nodig dan noodzakelijk voor de geautomatiseerde beoordeling (met andere woorden: de duur van het beoordelingsproces). De gegevens worden dan ook niet langer bewaard (mogelijkheid bestaat ook niet). C (Biometrie): De biometrische gegevens worden één dag bewaard om vervolgens te verwerken in het RAAS-systeem.	3.f. Akkoord. Mocht de uitslag van de gezichtsscan of de documentscan negatief zijn, dan wordt enkel de uitslag wel bewaard in Corsa. Hierin hanteren wij de bewaartermijnen die in Corsa zijn vastgesteld. In het RAAS-systeem worden de gegevens langer bewaard om bij bijvoorbeeld vermissing altijd te kunnen identificeren (dit met het oog op het voorkomen van identiteitsfraude). Het RAAS-systeem wordt beheerd door het ministerie (opdrachtgever reisdocumenten).
3.g. Hoe worden gegevens beveiligd?	3.g. A en B (Document – en gezichtsscanner): Alleen het resultaat van de gezichts- en de documentscan worden gelogd in de applicatie. Het betreft alleen een logregel zonder persoonsgegevens. C (Biometrie): De fysieke locatie waar de biometrische gegevens worden verwerkt is afgesloten en enkel toegankelijk voor geautoriseerde medewerkers.	3.g. Akkoord. Bij onregelmatigheden is dan ook altijd te achterhalen wie op welk moment toegang had tot de gegevens.
4. Risico's en voorgestelde maatregelen	Deze zijn afdoende beschreven.	Akkoord.

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 zelf kent een "laag" risico.

Eind 2024 zal deze DPIA op naleving getoetst worden.

Ik adviseer hiermee positief en daarmee zijn de resterende risico's "aanvaardbaar".

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

PK/11/03/2024. DPIA 75.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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

DPIA Oordeel FG gemeente Nijmegen

DPIA: Subsidies verstrekken

Inleiding

Hierbij het oordeel van de FG Gemeente Nijmegen over de DPIA ‘Subsidies verstrekken’. 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 januari – februari 2024 hebben 5.1.2e en 5.1.2e 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 ‘Subsidies verstrekken’ d.d. 14/02/2024.
Deze versie vormt de onderlegger voor deze toetsing.

Bij deze DPIA horen de volgende bijlagen:
- verwerkersovereenkomst met IRvN (getekend 2024)

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?	Nee	Akkoord.
2. Is het ethisch / politiek bestuurlijk verantwoord?	Ja. Gemiddeld worden er door instanties, verenigingen en burgers 1800 aanvragen voor een subsidie per jaar ingediend. Dit gebeurt nu door een simpel webformulier waarvan de gegevens handmatig worden overgenomen in het huidige systeem (Key2Subsidies van leverancier Centric). Gezien het contract met de huidige leverancier per 31-5-2025 afloopt geeft dat de kans om te zien wat er voor verbeteringen mogelijk zijn qua software en proces om de dienstverlening te optimaliseren. De bedoeling is om van een uitvoering- naar een uitvoering- en monitoringssysteem gaan. Streven: met de aanschaf van een nieuw systeem voldoen aan de archiefwet.	Akkoord. In de loop van het eerste kwartaal 2024 wordt een aanbesteding via de softwarebroker gestart. Planning per 1-1-2025 in productie. Deze DPIA wordt waar nodig verder aangevuld middels een addendum. .
3. Juridische toets 3a. Doel / grondslag	3.a. *Doel*: Op een betere manier invulling geven aan dienstverlening, wetgeving en sturing. *Grondslag*: Verwerking is noodzakelijk voor de uitvoering van een wettelijke taak zoals: - Artikel 213a Gemeentewet - Artikel 4.2 subsidierecht (AWB) - De Nijmeegse kaderverordening 2019	3.a. Akkoord. Uitgangspunt van de aanbesteding is te voldaan aan: - Archiefwet; - AVG; - De Nijmeegse kaderverordening subsidieverstrekking (2019); - uitvoeringsregelingen; - (financiële) rechtmatigheid m.b.t. accountantscontrole; - Informatievoorziening aan belanghebbenden (College, Raad, rekenkamer).
3.b. Proportionaliteit	3.b. Er wordt het minimum aan persoonsgegevens vastgelegd wat nodig is voor het verwerken van de aanvraag, het betalen van de subsidie aan de burger en het vaststellen van de rechtmatigheid.	3.b. Akkoord. Logging van handelingen is wel van belang.
3.c. Subsidiariteit	3.c. Er zijn geen alternatieven bekend. Zonder deze gegevens kan er geen subsidieverstrekking plaatsvinden.	3.c. Akkoord. Betreft optimalisering huidige werkwijze en toevoeging van functionaliteiten.
3.d. Persoonsgegevens buiten EER gebruikt?	3.d. Neen	3.d. Akkoord.
3.e.Andere partijen betrokken?	Gemeente Nijmegen, Centric en het IRVN. De nieuwe leverancier is nog onbekend.	3.e. Akkoord. Nijmegen verwerkingsverantwoordelijk en IRvN verwerker. Met de IRvN is een (nieuwe) verwerkersovereenkomst afgesloten. Actie: met nieuwe leverancier een verwerkersovereenkomst afsluiten.

3.f. Hoe lang worden gegevens bewaard en termijn en wijze van vernietiging?	3.f. Gegevens worden op basis van de archiefwet beheerd. Bewaartermijnen zijn daarop gebaseerd. Afhankelijk van de betreffende wetgeving is dit 7 tot 10 jaar(Art 4:69 AWB). De papieren dossiers worden door BDI beheerd en nadat de bewaartermijn verlopen is vernietigd.	3.f. Akkoord. De uitvoeringsorganisatie, de afdeling MO, is hiervoor verantwoordelijk.
3.g. Hoe worden gegevens beveiligd?	3.g. In de aanbesteding moet de leverancier voldoen aan onder andere de GIBIT, AVG en archiefwet. Dit wordt vastgelegd in het aanbestedingsdocument wat wordt opgesteld. GIBIT staat voor Gemeentelijke Inkoop bij IT Toolbox. Deze uniforme voorwaarden helpen gemeenten bij het professionaliseren van de inkoop van ICT-diensten.	3.g. Akkoord. In de GIBIT zijn ISO normeringen en dergelijke opgenomen.
4. Risico's en voorgestelde maatregelen	Deze zijn afdoende beschreven.	Akkoord. Bron voor de subsidieverlening is het subsidiesysteem. Autorisatie (met name intrekken ervan) is het belangrijkste risico.

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 zelf kent een "laag" risico.

In de loop van het eerste kwartaal 2024 wordt een aanbesteding via de softwarebroker gestart.
Planning per 1-1-2025 in productie.
Deze DPIA wordt waar nodig verder aangevuld middels een addendum.
Actie: met nieuwe leverancier een verwerkersovereenkomst afsluiten (indien van toepassing).

Eind 2024 zal deze DPIA op naleving getoetst worden.
Hierbij ligt de nadruk op het verstrekken en intrekken van autorisaties en logging van de handelingen.

Ik adviseer hiermee positief en daarmee zijn de resterende risico's "aanvaardbaar".

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

PK/18/03/2024. DPIA 76.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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

DPIA Oordeel FG gemeente Nijmegen

DPIA: Besluit bijstandverlening zelfstandigen BBZ

Inleiding

Hierbij het oordeel van de FG Gemeente Nijmegen over de DPIA 'Besluit bijstandverlening zelfstandigen BBZ'. 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 januari – maart 2024 hebben 5.1.2e , 5.1.2e , 5.1.2e , 5.1.2e en 5.1.2e 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 'Besluit bijstandverlening zelfstandigen BBZ' d.d. 06/03/2024.
Deze versie vormt de onderlegger voor deze toetsing.

Bij deze DPIA horen de volgende bijlagen:
- Decos: verwerkersovereenkomst

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?	Nee	Akkoord.
2. Is het ethisch / politiek bestuurlijk verantwoord?	Ja. Betreft verbetering van huidig proces.	Akkoord.
3. Juridische toets 3a. Doel / grondslag	3.a. *Doel*: Wanneer zelfstandigen onder de inkomensgrens zitten, komen zij in aanmerking voor een BBZ-uitkering. Zij dienen dan een aanvraag in die bij de gemeente in behandeling wordt genomen. Deze uitkering biedt zelfstandigen tijdelijke financiële ondersteuning wanneer er sprake is van een levensvatbaar bedrijf. Grondslag: Artikel 7 Participatiewet, en diverse losse artikelen in de BBZ (bv. Artikel 12).	3.a. Akkoord. Doel en grondslag veranderen niet door andere werkwijze.
3.b. Proportionaliteit	3.b. Wanneer de zelfstandige geen hulp zou krijgen wanneer deze onder de inkomensgrens leeft, kan dit leiden tot grotere en ernstige problematiek, denk aan schulden en dergelijke. Daarom is de mogelijkheid om een uitkering aan te vragen via de BBZ opgenomen.	3.b. Akkoord. Het verschilt per situatie welke gegevens er nodig zijn om tot een besluit te komen. Op basis van de antwoorden van de ondernemer op het aanvraagformulier worden bewijsstukken om tot een besluit te komen samengesteld. Logging van handelingen is wel van belang.
3.c. Subsidiariteit	3.c. De reden voor dit project, is dat er geen koppeling is met Corsa, wat betekent dat er geen digitale archivering plaatsvindt. Oftewel, alle relevante gegevens voor het dossier worden uitgeprint en gearchiveerd. In de nieuwe situatie wordt er na het indienen van de aanvraag automatisch een werkproces aangemaakt in de suite en een zaak binnen corsa. De aanvrager levert relevante gegevens via een uploadlink aan. Deze gegevens worden gearchiveerd in corsa.	3.c. Akkoord. Betreft optimalisering huidige werkwijze en toevoeging van functionaliteiten.
3.d. Persoonsgegevens buiten EER gebruikt?	3.d. Neen	3.d. Akkoord.
3.e.Andere partijen betrokken?	Gem Nijmegen is verwerkingsverantwoordelijke. Decos, Centric (middels IRvN) en Corsa (BCT) zijn verwerker.	3.e. Akkoord. Verwerkersovereenkomsten: zie bijlagen.
3.f. Hoe lang worden gegevens bewaard en termijn en wijze van vernietiging?	3.f. 10 jaar (zie selectielijst Archiefwet 2020)	3.f. Akkoord. BDI zorgt voor de vernietiging op het moment dat de bewaartermijn overschreden is. De verantwoordelijkheid daarvoor ligt bij de concernmanager van IZL.

3.g. Hoe worden gegevens beveiligd?	3.g. Er wordt momenteel onderzoek gedaan naar de privacyrisico's binnen de Suite. In de Suite is momenteel nog niet genoeg aandacht voor autorisaties, maar dat is één van de primaire aandachtspunten uit het onderzoek. Er wordt wel gelogd wie welke dossiers bekijkt. De autorisaties in Corsa zijn vanwege de AVG en de doelbinding die het vraagt gebaseerd op processen (zaaktypes) en functies (mandaat). Voor de zaaktypes van BBZ geldt de vertrouwelijkheidscode vSD04.	3.g. Akkoord. De functies die deze vertrouwelijkheid (vSD04) hebben, zijn: - Consulent BZ - Financieel Medewerker - Administratief medewerker
4. Risico's en voorgestelde maatregelen	Deze zijn afdoende beschreven.	Akkoord. Autorisatie (met name intrekken ervan) is het belangrijkste risico, evenals de controle op de logging.

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 zelf kent een "laag" risico.

Eind 2024 zal deze DPIA op naleving getoetst worden.
Hierbij ligt de nadruk op het verstrekken en intrekken van autorisaties en logging van de handelingen.

Ik adviseer hiermee positief en daarmee zijn de resterende risico's "aanvaardbaar".

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

PK/21/03/2024. DPIA 77.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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

DPIA Oordeel FG gemeente Nijmegen

DPIA: ETHOS Telonderzoek Gelderland Zuid

Inleiding

Hierbij het oordeel van de FG Gemeente Nijmegen over de DPIA 'ETHOS Telonderzoek Gelderland Zuid'.
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 januari – maart 2024 hebben 5.1.2e , 5.1.2e , 5.1.2e , 5.1.2e 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 'ETHOS Telonderzoek Gelderland Zuid' d.d. 04/04/2024.
Deze versie vormt de onderlegger voor deze toetsing.

Bij deze DPIA horen de volgende bijlagen:
- DPIA ETHOS telling Hogeschool Utrecht 040324
- Bijlage 1 DPIA ETHOS Telonderzoek bewaartermijn en encryptie
- Bijlage 2 ETHOS Telonderzoek werkwijze inwilliging recht op bezwaar en gegevenswisseling
- Bijlage 3 Gegevensuitwisselingsovereenkomst HU en telregio's ETHOS-telonderzoek_12-02-2024
- 240315_Advies ETHOS-telling Cuccibu
- Privacyverklaring ETHOS telonderzoek
- Vragenlijst ETHOS telling regio Gelderland-Zuid
- Samenwerkingsovereenkomst gem. Nijmegen – getekend
- Advies Ethische Commissie Hogeschool Utrecht - ETHOS Telonderzoek 2022

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. De Hogeschool Utrecht heeft een DPIA uitgevoerd op het verwerken van gegevens in het kader van het ETHOS-onderzoek.	Akkoord. Deze is opgenomen als bijlage bij deze DPIA. Daarnaast is op verzoek van diverse deelnemende gemeente (waaronder gemeente Nijmegen) een aanvullend onderzoek gedaan op de DPIA van de Hogeschool (zie rapportage Cuccibu). Dit heeft geleid tot een tweetal aanvullingen op deze DPIA van de HU (zie bijlagen 1. en 2.)
2. Is het ethisch / politiek bestuurlijk verantwoord?	Ja. Het college van burgemeester en wethouders heeft op 20 februari 2024 besloten om aan de telling deel te nemen. De Ethische Commissie Onderzoek Sociaal Domein van Hogeschool Utrecht heeft een positief oordeel gegeven	Akkoord. De onderzoeksopzet van de Hogeschool Utrecht heeft de toetsing van de ethische commissie van de betreffende instelling doorstaan (zie bijlage). Het oordeel van de ethische commissie is in de bijlage opgenomen.
3. Juridische toets 3a. Doel / grondslag	3.a. *Doel*: Het doel van de verwerking is het in kaart brengen van de groep (dreigend) dak- en thuislozen en hun kenmerken. Het doel van dit onderzoek is om deze groep beter in beeld te brengen, om zo beleid met betrekking tot deze doelgroep op te stellen en zo de doelstelling met betrekking tot dak- en thuisloosheid waar te kunnen maken. In het Nationaal Actieplan wordt daarbij aangestuurd op de inzet van de ETHOS-methode. *Grondslag:* De gemeente verwerkt persoonsgegevens van dak- en thuislozen ter vervulling van een taak van algemeen belang (art. 6 lid 1 onder e AVG). Het betreft dan de uitvoering van taken onder (o.a.) de Wet maatschappelijke ondersteuning (Wmo), de Wet op de gemeentelijke schuldhulpverlening (Wgs) en de Wet Basisregistratie Personen (Wet BRP). Hier betreft het een nieuwe verwerking van deze gegevens, namelijk de verstrekking van deze gegevens aan de Hogeschool Utrecht. Uit art. 5 lid 1 onder b AVG volgt dat een verdere verwerking van gegevens met het oog op wetenschappelijk onderzoek of statistische doeleinden verenigbaar mag worden geacht met het doel waarvoor de gegevens oorspronkelijk zijn verwerkt. De grondslag blijft de vervulling van een taak van algemeen belang (art. 6 lid 1 onder e AVG).	3.a. *Doel*: Onder de huidige monitoring (zoals die van het CBS) blijft een groot deel van de (dreigend) dak en thuislozen buiten beeld. Het onderzoek richt zich niet alleen op de vraag óf iemand ongewild dak- of thuisloos is, maar ook wat de aanleiding daarvoor is. Om dat onderzoek mogelijk te maken worden aan de HU (gepseudonimiseerd) gegevens verstrekt over de aanleiding en de bron van inkomen, maar bijvoorbeeld ook over de aanwezigheid van verslavingsproblematiek of een gezondheidsbeperking. *Grondslag:* De AVG biedt een grondslag voor deze verwerking. De gemeente verwerkt veel van deze gegevens al in het kader van bijzondere wetgeving. In deze bijzondere wetgeving worden nadere eisen gesteld aan de verstrekking van deze gegevens aan derden. Deze eisen gelden bovenop de eisen die de AVG en de UAVG stellen. Het betreft de volgende wetten: - *Wmo: art. 5.3.6* - *Jeugdwet: art. 7.3.12* Nadere eisen: Vragen van toestemming mag redelijkerwijs niet mogelijk zijn; Persoonlijke levenssfeer mag niet onevenredig worden geschaad; Betrokkene heeft geen uitdrukkelijk bezwaar gemaakt; Van de verstrekking wordt een aantekening in het dossier gemaakt.

	Art. 89 AVG; passende waarborgen; pseudonimisering Art. 89 AVG stelt wel nadere eisen aan de verwerking van persoonsgegevens in het kader van wetenschappelijk onderzoek/statistische doeleinden. De verwerking moet zijn onderworpen aan passende waarborgen voor de rechten en vrijheden van de betrokkene. Die maatregelen kunnen pseudonimisering bevatten. *Toestemming* Een van de vereisten die uit deze bijzondere bepalingen volgen is dat het vragen van toestemming redelijkerwijs niet mogelijk mag zijn. Los van de werklast is het bereiken van deze specifieke kwetsbare doelgroep een extra moeilijkheid. Contact leggen met deze mensen vraagt soms veel inzet en meerdere pogingen. Het vragen van toestemming blijkt een onevenredige inspanning te vergen. *Bezwaar* Indien een betrokkene niet meegeteld wenst te worden, kan hij bezwaar maken. Indien de betrokkene nog niet is meegeteld, wordt over hem geen vragenlijst ingevuld. Is over de betrokkene al wel een vragenlijst ingevuld, dan verwijdert De Hogeschool Utrecht de bijbehorende vragenlijst en zal de betrokkene niet worden meegenomen in het onderzoek.	*- Participatiewet: art. 65 lid 3* Nadere eisen: Persoonlijke levenssfeer van betrokkene mag niet onevenredig worden geschaad. *- Wet BRP: art. 3.13 (jo. Art. 44 Besluit BRP)* Nadere eisen: Verzoek afkomstig van instelling als bedoeld in art. 1.2 Wet op het hoger onderwijs en wetenschappelijk onderzoek; Waarborgen ter bescherming persoonlijke levenssfeer; De gegevens worden slechts in geanonimiseerde vorm beschikbaar gesteld; tenzij de ingeschrevene uitdrukkelijk met de verstrekking heeft ingestemd. *Toestemming en bezwaar:* Deze hele gang van zaken staat of valt met een goede communicatie. De gemeente zal de doelgroep zo goed mogelijk moeten informeren via zoveel mogelijk kanalen. Behalve flyers en posters en briefing via de bekende postadressen, betekent dit ook dat actief gecommuniceerd dient te worden (mondeling) op de bekende vindplaatsen van de doelgroep: de daklozenopvang (MFC), straatdoktor, de opvanglocaties van organisaties als Leger des Heils en Iris-zorg en andere bekende vindplaatsen. Daarnaast dient dit te geschieden in meerdere talen op zogenaamd B1 niveau. Ook dient het volgende te geschieden: De Wmo en de Jeugdwet eisen dat van de verwerking een aantekening wordt gemaakt in het dossier. De betrokken medewerkers zullen hierover geïnformeerd worden.
3.b. Persoonsgegevens (worden bijzondere persoonsgegevens verwerkt)?	3.b. Ja. De volgende bijzondere persoonsgegevens worden uitgevraagd: Nationaliteit; Geboorteland; Verblijfsstatus; Ziekte- of arbeidsongeschiktheidsuitkering; Verblijf in een instelling (algemeen ziekenhuis, GGZ-instelling, verslavingskliniek, P.I., forensisch psychiatrische kliniek, beschermd wonen, jeugdzorg, revalidatiecentrum, AZC); Huisuitzetting wet Damocles; De aanwezigheid van psychische problematiek/ verslaving; De aanwezigheid van lichamelijke problemen/fysieke beperking; (Vermoeden van) aanwezigheid verstandelijke beperking; Voormalig verblijf in instelling (gevangenis, jeugdzorg, psychiatrische voorziening);	3.b. De AVG en de UAVG kennen uitzonderingen op het verbod van het verwerken van bijzondere persoonsgegevens voor wetenschappelijk onderzoek/statistische doeleinden (art. 9 lid 2 onder j AVG; art. 24 UAVG). Criteria zie DPIA 4.3. Akkoord, mits de handelingen geschieden direct in de beveiligde omgeving onder een gepseudonimiseerde code. Er mogen geen aantekeningen van de invoer gemaakt worden.
3.c. Proportionaliteit	3.c. Door het invullen van de vragenlijsten wordt een inbreuk gemaakt op de privacy van betrokkenen. Deze is in de eerste plaats gelegen	3.c. Ook de gemeente Nijmegen heeft – gelet ook op het Nationale Actieplan – belang bij dit onderzoek. Het onderzoek bevat de

	in het feit dat over de betrokkenen een vragenlijst wordt ingevuld waarin een significante hoeveelheid (deels bijzondere) persoonsgegevens worden opgenomen. Ook zullen – door de gehanteerde definitie - personen onder het onderzoek zullen vallen die zichzelf mogelijk niet als dak- of thuisloos beschouwen. Dit zou voor hen ook als stigmatiserend ervaren kunnen worden. Er worden nodige maatregelen genomen om de inbreuk op de privacy van betrokkenen zoveel mogelijk te beperken, zoals pseudonimisering.	noodzakelijke stuurinformatie om als gemeente en als regio de ambitie om dakloosheid terug te dringen waar te maken. De gemeente moet – op geaggregeerd niveau – weten om welke groepen het gaat, waarom zij hun woning zijn verloren en wat zij nodig hebben om uit deze situatie te komen. Het college van burgemeester en wethouders heeft op 20 februari 2024 besloten om aan de telling deel te nemen.
3.d. Subsidiariteit	3.d. Een alternatieve onderzoek wijze zou zijn om het onderzoek te beperken tot een telling, en alle vragen naar profielkenmerken achterwege te laten. Daarmee zou echter de belangrijkste meerwaarde van dit onderzoek verloren gaan.	3.d. Akkoord. De gemeente is niet goed in staat om toegepast beleid te schrijven, indien er geen profielkenmerken van hen gevraagd worden Hiermee kunnen zij geen effectieve ondersteuning bieden en zal de ambitie van het Nationale Actieplan niet haalbaar zijn.
3.e. Persoonsgegevens buiten EER gebruikt?	3.e. Neen	3.e. Akkoord.
3.f. Andere partijen betrokken?	3.f. - De Hogeschool Utrecht bepaalt doel en middelen van de verwerking van de gegevens. De HU is verwerkingsverantwoordelijke. Crowdtech is verwerker voor de Hogeschool Utrecht. Zij hebben onderling een verwerkersovereenkomst afgesloten. - De gemeente Nijmegen verwerkt de betreffende gegevens reeds voor eigen doeleinden, zoals de uitvoering van taken onder de Wmo, de Wet BRP, etc. De gemeente Nijmegen is daarmee tevens verwerkingsverantwoordelijke.	3.f. Akkoord. Omdat doel en middelen van de verwerking van de gegevens door de Hogeschool Utrecht is vastgelegd (en de gemeente Nijmegen hier verder niet bij betrokken is), is geen sprake van een gezamenlijke verantwoordelijkheid. Beide partijen zijn zelfstandig verantwoordelijk voor hun verwerkingen. De Hogeschool Utrecht heeft zich op hetzelfde standpunt gesteld. Zie in de bijlagen de diverse afspraken hieromtrent.
3.g. Hoe lang worden gegevens bewaard en termijn en wijze van vernietiging?	3.g. De Hogeschool Utrecht bewaart de vragenlijsten 10 jaar. De pseudonimiseringscode en exacte leeftijd wordt ook 10 jaar bewaard in de digitale kluis.	3.g. Akkoord. Deze bewaartermijn volgt uit eisen van de Nederlandse Gedragscode Wetenschappelijke Integriteit.
3.h. Hoe worden gegevens beveiligd?	3.h. De vragenlijsten worden ingevoerd via een online omgeving van Crowdtech. Crowdtech voldoet aan de ISO 27001-norm voor informatiebeveiliging.	3.h. Akkoord. De Hogeschool Utrecht heeft een verwerkersovereenkomst met Crowdtech gesloten.
4. Risico's en voorgestelde maatregelen	Deze zijn afdoende beschreven.	Akkoord. Belangrijkste risico's zijn gelegen in: - Communicatie naar de doelgroep; - Proces en procedure bij in bezwaar gaan door betrokkene; - Moment van invoer van gegevens. Hierbij mogen geen gegevens of andere informatie omtrent de betrokkenen en doelgroep achterblijven.

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 zelf kent een "middelhoog" risico, mits….

Voorwaarden:
Dit niveau van 'middelhoog' wordt pas bereikt nadat de belangrijkste risico's worden verminderd middels uitvoering van de handelingen zoals in dit bovenstaand oordeel beschreven zijn.
Daarmee is uitvoering hiervan *voorwaardelijk* voor dit oordeel.

Hier volgt in het kort nog de belangrijke aanbevelingen:

- De gemeente zal de doelgroep zo goed mogelijk moeten informeren via zoveel mogelijk kanalen. Behalve flyers en posters en briefing via de bekende postadressen, betekent dit ook dat actief gecommuniceerd dient te worden (mondeling) op de bekende vindplaatsen van de doelgroep: de daklozen opvang (MFC), straatdoktor, de opvanglocaties van organisaties als Leger des Heils en Iris-zorg en andere bekende vindplaatsen;
- Daarnaast dient dit te geschieden in meerdere talen op zogenaamd B1 niveau;
- Er dient een goed proces en procedure ingericht te zijn bij 'in bezwaar gaan' door betrokkene;
- De Wmo en de Jeugdwet eisen dat van de verwerking een aantekening wordt gemaakt in het dossier. De betrokken medewerkers zullen hierover geïnformeerd worden;
- De invoerhandelingen geschieden direct in de beveiligde omgeving onder een gepseudonimiseerde code;
- Er mogen geen aantekeningen van de invoer gemaakt worden.

Direct nadat de gehele invoer van gegevens voor het onderzoek door de HU en (overige) handelingen vanuit de gemeente Nijmegen afgerond zijn, dient er een rapportage te worden gemaakt over bovenstaand proces met de nadruk op de onderdelen die hierboven genoemd zijn. Expliciet dient duidelijk gemaakt te worden, met een aantal voorbeelden uit de praktijk, op welke wijze met de doelgroep gecommuniceerd is. Ook moet duidelijk zijn hoeveel bezwaren (tegen deze verwerking) er zijn binnen gekomen.
Hiermee wordt een rapportage aangeleverd aan de FG die aangeeft op welke wijze de risico's tijdens het onderzoek tot een minimum beperkt zijn gebleven.
De concernmanager is verantwoordelijk voor het aanleveren van deze rapportage binnen de gestelde tijd (uiterlijk medio juni 2024).

Na voldaan van de voorwaarden adviseer ik hiermee positief en daarmee zijn de resterende risico's "aanvaardbaar".

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

PK/04/04/2024. DPIA 78.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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

DPIA Oordeel FG gemeente Nijmegen

DPIA: Suwinet

Inleiding

Hierbij het oordeel van de FG Gemeente Nijmegen over de DPIA 'Suwinet'.
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 januari – maart 2024 hebben 5.1.2e, 5.1.2e, 5.1.2e, 5.1.2e, 5.1.2e 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 'Suwinet' d.d. 28/03/2024.
Deze versie vormt de onderlegger voor deze toetsing.

Bij deze DPIA horen de volgende bijlagen:
- overeenkomst Bureau Keteninformatisering Werk en Inkomen (BKWI)
Deze is nog niet beschikbaar.

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?	Neen	Akkoord. Er is wel een vergelijkbare DPIA gemaakt betreffende de relatie met het Inlichtingenbureau met bureau Nieuwkomers.
2. Is het ethisch / politiek bestuurlijk verantwoord?	Ja. Op grond van art. 62, eerste lid, Wet Structuur uitvoeringsorganisatie werk en inkomen (Wet Suwi) dienen het UWV, de SVB en de colleges van B&W elkaar alle gegevens en inlichtingen te geven die noodzakelijk zijn voor de uitvoering van hun taken onder (o.a.) de Participatiewet en de Wet gemeentelijke schuldhulpverlening. Op grond van het tweede lid dienen zij daartoe gezamenlijk zorg te dragen voor de instandhouding van elektronische voorzieningen voor de verwerking van die gegevens. Deze uitwisseling vindt plaats via Suwinet.	Akkoord. De gemeente dient zich voor het gebruik van Suwinet te verantwoorden middels de jaarlijkse ENSIA-rapportage. Deze DPIA vormt mede de onderlegger voor deze verantwoording.
3. Juridische toets 3a. Doel / grondslag	3.a. *Doel*: Suwinet wordt gebruikt om de rechtmatigheid vast te stellen of inwoners recht hebben op de aanvragen die zij doen. Met name op het gebied van de participatiewet. Bovendien wordt Suwinet gebruikt in het kader van Schuldhulpverlening om een compleet te krijgen van de financiële situatie van de inwoner. *Grondslag:* De verwerking is noodzakelijk voor de uitvoering van een wettelijke taak (art. 6 lid 1 onder e AVG). Op grond van art. 53a Participatiewet (PW) dient het college onderzoek te verrichten. Daarbij dient het college gebruik te maken van (o.a.) de gegevens van het UWV en de gegevens uit de BRP, zo volgt uit de bepaling. Soortgelijke onderzoeksplichten zijn neergelegd in de Wet op de gemeentelijke schuldhulpverlening (art. 6 en 7 Wgs).	3.a. *Doel*: Het dient als middel om het recht op bijstand vast te kunnen stellen, dus zowel in geval van een aanvraag als bij een fraudeonderzoek. *Grondslag:* Op grond van de artikelen 63 en 64 PW dienen de daarin aangewezen personen en instanties (waaronder het UWV, de SVB en de Belastingdienst) de gevraagde inlichtingen aan het college te verstrekken. Voor schuldhulpverlening is dit vastgelegd in art. 8 lid 3 Wet gemeentelijke schuldhulpverlening (Wgs).
3.b. Persoonsgegevens Worden bijzondere persoonsgegevens verwerkt?	3.b. In beginsel niet, maar mogelijk bij uitkering is daar wel sprake van. Bijvoorbeeld als het gaat over Ziektewet of een Wajong uitkering.	3.b. Akkoord.
3.c. Proportionaliteit	3.c. Om het recht op bijstand vast te kunnen stellen, moet de gemeente bepaalde gegevens kunnen controleren. Het raadplegen van Suwinet geeft veel inzichten in de persoonsgegevens van de	3.c. De gemeente moet met grote zekerheid het recht op bijstand vaststellen. Als de gemeente dat niet kan, kan het in een later stadium

	aanvrager en leidt tot een relatief grote inbreuk op de privacy.	leiden tot terugbetalingen als een inwoner onterecht een uitkering heeft ontvangen.
3.d. Subsidiariteit	3.d. De gegevensuitvraag vindt allereerst bij de burger plaats door de vraagstelling in het aanvraagformulier. Daar moet de burger verklaringen afleggen omtrent woon- en leefsituatie, inkomen en vermogen. Het raadplegen van Suwinet dient ter controle.	3.d. Akkoord. De gegevens van het inlichtingenbureau zijn indicatief. Met name bij inkomstengegevens loopt het Inlichtingenbureau een paar weken achter. Een dienstverband kan in Suwinet nog als lopend staan, terwijl juist de beëindiging reden is voor de bijstandsaanvraag. Door de gegevens met elkaar te vergelijken en de klant op de afwijkingen te wijzen, wordt de rechtmatige verstrekking bevorderd.
3.e. Persoonsgegevens buiten EER gebruikt?	3.e. Neen	3.e. Akkoord.
3.f. Andere partijen betrokken?	3.f. Gegevens worden uitgewisseld tussen gemeente en Inlichtingenbureau. De gemeente is als raadpleger verwerkingsverantwoordelijke. Bureau Keteninformatisering Werk en Inkomen (BKWI), die Suwinet verzorgt, is verwerker.	3.f. Akkoord, mits: Actie: Met het BKWI moet een (verwerkers)overeenkomst worden vastgesteld.
3.g. Hoe lang worden gegevens bewaard en termijn en wijze van vernietiging?	3.g. Suwinet zelf bewaart geen gegevens. De bewaartermijnen van de gegevens in Suwinet zijn verbonden aan de bronsystemen waar de gegevens uitkomen.	3.g. Akkoord. NB. Wanneer het relevant is voor een aanvraag, kan er een printscreen gemaakt worden van de gegevens in Suwinet. Deze kunnen toegevoegd worden aan het dossier van een bepaalde klant. De bewaartermijn is vervolgens de reguliere bewaartermijn van de onderliggende voorziening (bij bijstand is dat 10 jaar).
3.h. Hoe worden gegevens beveiligd?	3.h. In Suwinet is er een autorisatiestructuur ingericht. Er is een autorisatiematrix. Ook wordt gelogd welke medewerkers welke dossiers bekijken.	3.h. Akkoord.
4. Risico's en voorgestelde maatregelen	Deze zijn afdoende beschreven.	Akkoord. Maatregelen die nog genomen moeten worden: Er moet een richtlijn worden vastgesteld voor wanneer gegevens uit Suwinet wel en niet opgenomen mogen worden in het dossier van een klant (dit moet nog gebeuren). Medewerkers moet een reden opgeven waarom bepaalde dossiers opgezocht worden, en daar voeren kwaliteitsmedewerkers steekproeven op uit.

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 zelf kent een "laag" risico.

Er dienen nog wel drie maatregelen op korte termijn genomen te worden.
Hier moet binnen drie maanden op gerapporteerd te worden door de concernmanager aan de FG.
Deze drie maatregelen zijn:

1. Met het BKWI moet een (verwerkers)overeenkomst worden vastgesteld.
2. Er moet een richtlijn worden vastgesteld voor wanneer gegevens uit Suwinet wel en niet opgenomen mogen worden in het dossier van een klant (dit moet nog gebeuren).
3. Medewerkers moet een reden opgeven waarom bepaalde dossiers opgezocht worden, en daar voeren kwaliteitsmedewerkers steekproeven op uit.

Eind 2024 zal deze DPIA op naleving getoetst worden.
Hierbij ligt de nadruk op het verstrekken en intrekken van autorisaties en logging van de handelingen.

Ik adviseer hiermee positief en daarmee zijn de resterende risico's "aanvaardbaar".

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

PK/09/04/2024. DPIA 79.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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

DPIA Oordeel FG gemeente Nijmegen

DPIA: Arbeidsovereenkomst / HRM Systemen

Inleiding

Hierbij het oordeel van de FG Gemeente Nijmegen over de DPIA 'Arbeidsovereenkomst / HRM Systemen'. 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 mei 2023 – maart 2024 hebben 5.1.2e, 5.1.2e, 5.1.2e en 5.1.2e 5.1.2e 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 'Arbeidsovereenkomst / HRM Systemen' dd 18/04/2024.
Deze versie vormt de onderlegger voor deze toetsing.

Bij deze DPIA horen de volgende bijlagen:
- Autorisaties Beaufort en Youforce
- Landscape Youforce
- HR Beaufort voor Payroll Gemal Direct
- Getekende overeenkomst Raet
- Raet verwerkersovereenkomst 20190121

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?	Neen	Akkoord. Er volgt nog een aparte DPIA betreffende ziekteverzuim.
2. Is het ethisch / politiek bestuurlijk verantwoord?	Ja. De gemeente Nijmegen is werkgever en heeft medewerkers in dienst. Deze werknemers voeren werkzaamheden voor en ten behoeve van de stad uit. Voor het uitvoeren van deze werkzaamheden ontvangen medewerkers een salaris. Er wordt een systeem met diverse modules gebruikt, die met elkaar gekoppeld zijn om zo te voldoen aan de basale taak van P&O: zorgen voor uitbetaling van de salarissen voor alle medewerkers die een arbeidsovereenkomst hebben met de gemeente Nijmegen en daarbij te voldoen aan alle wettelijke taken die voortvloeien uit deze arbeidsovereenkomst.	Akkoord. NB. Betreft ook: vergoeding voor werkzaamheden van wethouders en burgemeester, raadsleden fractie ondersteuning.
3. Juridische toets 3a. Doel / grondslag	3.a. *Doel*: Naleving van wet- en regelgeving als werkgever op het gebied van arbeidsrecht, belastingrecht, en andere relevante regelgeving wat betreft een arbeidsovereenkomst. *Grondslag:* De grondslag is gelegen in het uitvoering geven aan de arbeidsovereenkomst. De minimale vereisten hiervan zijn opgenomen in het Burgerlijk Wetboek. Het gebruik van deze systemen is ook noodzakelijk om te kunnen voldoen aan wettelijke verplichtingen op het gebied van belastingen en sociale zekerheid.	3.a. *Doel*: Betreft P&O systemen die ondersteunend zijn aan de relatie tussen management en personeel. Denk bijvoorbeeld aan recruitment, persoonlijke ontwikkeling, (bij)scholing, ziekteverzuim, functioneringsgesprekken en arbeidsvoorwaarden. *Grondslag:* Akkoord. NB. De medewerker heeft de gelegenheid toestemming te verlenen om deze gegevens te gebruiken voor doeleinden als: bloemetje / kaartje bij lief en leed, jubilea, of andere gebeurtenissen. Dit is dus facultatief.
3.b. Persoonsgegevens Worden bijzondere persoonsgegevens verwerkt?	3.b. Ja. Gegevens over gezondheid en welzijn: bijvoorbeeld informatie over ziekteverzuim frequentie etc. Gegevens over etnische afkomst: bijvoorbeeld informatie over ras of etnische achtergrond van een werknemer, dit gebeurt enkel op vrijwillige basis.	3.b. Akkoord. De registratie betreft etniciteit kwam voort uit de wet Samen die gold van 1-1-1998 en per 16-10-2003 is ingetrokken. (Stimulering arbeidsdeelname minderheden)
3.c. Proportionaliteit	3.c. Gegevens zijn nodig om de arbeidsovereenkomst vorm te geven. Een van de subdoelen betreft het uit betalen van de salarissen per maand aan de medewerkers.	3.c. De gemeente moet met grote zekerheid het salaris kunnen vaststellen. Als de gemeente dat niet goed doet, kan het leiden tot terugbetaling of nabetaling als een medewerker een onjuist bedrag heeft ontvangen.

3.d. Subsidiariteit	3.d. Door digitale verwerking van de gegevens en hieruit voortvloeiend de salarisbetaling is de kans op fouten afgenomen.	3.d. Akkoord. Incorrecte betaling leidt tot vervelende situaties voor de medewerkers en extra werk tot correctie.
3.e. Persoonsgegevens buiten EER gebruikt?	3.e. Neen	3.e. Akkoord.
3.f. Andere partijen betrokken?	3.f. Ja. De gemeente is verwerkingsverantwoordelijke. Visma Raet is verwerker. Andere betrokkenen zijn belastingdienst, ABP, UWV en ProAmbt. Zij verkrijgen onderdelen van de gegevensverwerking conform wettelijke kaders (belastingafdracht, pensioen, uitkering, WIA).	3.f. Akkoord, mits: Zie diverse bijlagen bij deze DPIA, waaronder de verwerkersovereenkomst met Visma Raet. .
3.g. Hoe lang worden gegevens bewaard en termijn en wijze van vernietiging?	3.g. De gegevens worden gedurende het dienstverband bewaard. Na einde van het dienstverband nog 5 jaar conform archiefwet. Belastingtechnische gegevens nog 7 jaar.	3.g. Akkoord. Er zijn nog papieren dossiers in omloop. Deze dienen zo mogelijk gedigitaliseerd cq vernietigd te worden conform termijnen. Vernietiging van gegevens vanuit Visma Raet / You Force dient ook te gebeuren. Actie: regelen dat dit alsnog geschiedt.
3.h. Hoe worden gegevens beveiligd?	3.h. Beveiliging vindt plaats door dagelijkse back-ups. Voor de software die binnen het gemeentenetwerk staat wordt dit verzorgd door het IRVN. Voor het Cloud gedeelte wordt dit gedaan door Visma RAET, de leverancier. Toegang tot de systemen is via autorisatierollen geregeld. Van wijzigingen vindt logging plaats	3.h. Akkoord.
4. Risico's en voorgestelde maatregelen	Deze zijn afdoende beschreven.	Akkoord. Maatregelen die nog genomen moeten worden: - Vernietiging van gegevens vanuit Visma Raet / You Force.

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 zelf kent een "middelhoog" risico.

Maatregelen die nog genomen moeten worden:
Vernietiging van gegevens vanuit Visma Raet / You Force.

Eind 2024 zal deze DPIA op naleving getoetst worden.
Hierbij ligt de nadruk op het verstrekken en intrekken van autorisaties en logging hiervan én vernietiging van gegevens (zowel papier als digitaal)

Ik adviseer hiermee positief en daarmee zijn de resterende risico's "aanvaardbaar".

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

PK/18/04/2024. DPIA 80.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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

DPIA Oordeel FG gemeente Nijmegen

DPIA: Proeftuin Samen Verder

Inleiding

Hierbij het oordeel van de FG Gemeente Nijmegen over de DPIA 'Proeftuin Samen Verder'. 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 mei 2023 – april 2024 hebben 5.1.2e , 5.1.2e , 5.1.2e , 5.1.2e , 5.1.2e , 5.1.2e 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 'Proeftuin Samen Verder - DPIA Proeftuin versie 4.0' d.d. 24/04/2023.
Deze versie vormt de onderlegger voor deze toetsing.

Bij deze DPIA horen de volgende bijlagen:
1. Privacy Protocol Proeftuin Samen Verder – Dukenburg
2. Samenwerkingsovereenkomst Proeftuin Samen Verder – Dukenburg

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?	Neen.	Akkoord.
2. Is het ethisch / politiek bestuurlijk verantwoord?	Ja. Het Toekomstscenario kind en gezinsbescherming is in 2021 door het ministerie van J&V, het ministerie van VWS en de Vereniging van Nederlandse Gemeenten bestuurlijk vastgesteld. Dit scenario schetst op hoofdlijnen hoe de kind- en gezinsbescherming er over 5 tot 10 jaar (2026-2031) uit zou kunnen zien. Dit betekent waarschijnlijk een verandering van het huidige stelsel en nieuwe vormen van samenwerking tussen de betrokken partners. In 2022 is Gelderland Zuid als officiële proeftuin gestart in Nijmegen-Dukenburg met de naam 'Samen Verder'. Professionals in de 'Proeftuin Samen Verder' gaan op een andere manier samenwerken met gezinnen en huishoudens (in de leeftijd van 0 tot 100), waarbij sprake is van meervoudige, complexe problematiek en waar onveiligheid speelt en/of ontwikkelingsbedreiging. De inwoners zijn bij de aanmelding bij de proeftuin woonachtig in het stadsdeel Dukenburg.	Akkoord. Het college heeft ingestemd met deze proeftuin: College van B&W: 20 december 2022, nr. E22.002471. Deze pilot duurt twee jaar. Bij vervolg krijgt de DPIA een update. Na deze looptijd geven de diverse proeftuinen in het land alle opgedane ervaringen en werkzame elementen terug aan het Ministerie van VWS, zodat zij dit kunnen meenemen in de stelselwijziging.
3. Juridische toets 3a. Doel / grondslag	3.a. *Doel* van deze gegevensverwerkingen: - Proeftuin Samen Verder is een samenwerkingsverband waarin zorg- en veiligheidspartners en gemeenten onder eenduidige regie werken aan complexe zorg- en veiligheidsproblemen. De doelstelling van de samenwerking is bijdragen aan de algemene veiligheid, het verbeteren van de persoonlijke situatie van gezinnen en huishoudens en deze op tijd en op de juiste manier helpen bij het herstellen én borgen van ieders veiligheid. Dit gebeurt door een combinatie van zorg, regie, begeleiding en drang en dwangkaders, hetgeen moet worden gezien als een zwaarwegend algemeen belang. *Grondslag* Artikel 6 (AVG) is de grondslag voor het verwerken en verstrekken van persoonsgegevens ten behoeve van het behandelen van een casus en de van toepassing zijnde taken van partijen.	3.a. Akkoord. Zie voor uitgebreider antwoord het Privacy Protocol. Specifiek voor de proeftuin geldt dat in deze samenwerking wordt verkend wat nodig is om effectieve kind- en gezinsbescherming te realiseren (in opdracht van het interbestuurlijk programma van min J&V en VWS i.s.m VNG). *Grondslag* In de DPIA zijn de subartikels (6.1. t/m 6.5.) verder uitgewerkt.

3.b. Persoonsgegevens Worden bijzondere persoonsgegevens verwerkt?	3.b. Ja. In het WIZPortaal worden bijzondere gegevens, met name gegevens over de gezondheid verwerkt. Grondslag hiervoor is terug te vinden in de Wmo en Jeugdwet, bv. Artikel 5.1.1 Wmo (voor gemeente, en 5.2 ev. Voor aanbieders en 7.4.0, 7.4.1, 7.4.3 Jw.	3.b. Akkoord.
3.c. Proportionaliteit	3.c. De noodzakelijk te verwerken gegevens verschillen per fase. Het werkproces voorziet er daarom in dat er per fase een afweging wordt gemaakt door de procesregisseur in samenspraak met de verstrekkende partij over de benodigde gegevens en te betrekken partijen. Daarbij zijn afspraken gemaakt over de wijze waarop gegevens slechts voor zover noodzakelijk en evenredig verwerkt worden. Op die manier is in het werkproces verankerd dat steeds opnieuw een noodzakelijkheidsafweging plaatsvindt omtrent de te verstrekken gegevens.	3.c. De afweging welke gegevens per keer vastgelegd worden, dient gelogd te worden. Hierdoor is het mogelijk de afweging te bezien en te beoordelen of deze proportioneel is. Dataminimalisatie is het uitgangspunt.
3.d. Subsidiariteit	3.d. Samenwerking tussen meerdere ketens is voor casuïstiek binnen Samen Verder nodig om tot een effectieve aanpak te komen. Het is in de reguliere samenwerking tussen partners binnen één keten niet mogelijk om deze problematiek effectief aan te pakken.	3.d. Akkoord. De werkwijze en de vastlegging van gegevens is mede onderdeel van de pilot. Evaluatie (na twee jaar) hiervan zal al dan niet leiden tot aanpassing van deze werkwijze.
3.e. Persoonsgegevens buiten EER gebruikt?	3.e. Neen	3.e. Neen
3.f. Andere partijen betrokken?	3.f. De partijen die onderdeel uit maken van de Proeftuin zijn de volgende: - Stichting OIDOS (Buurtteams Jeugd & Gezin) - Stichting Incluzio (Buurtteams Volwassenen) - Stichting Veilig Thuis - Gecertificeerde Instellingen - Stichting Moviera - Raad voor de Kinderbescherming - Reclassering (3RO) - Gemeente Nijmegen Stichting OIDOS beheert het registratiesysteem WIZ portaal en is dus verantwoordelijk voor het beheer van dit systeem. De Partijen binnen de Proeftuin zijn gezamenlijk verantwoordelijk voor de verwerking van persoonsgegevens die noodzakelijk zijn voor de uitvoer van de (jeugd)hulp in het kader van de Wmo en Jeugdwet; De gemeente Nijmegen is verantwoordelijk voor de verwerking van persoonsgegevens die noodzakelijk zijn voor de toeleiding naar voorzieningen of (jeugd)hulp.	3.f. Akkoord. Zie bijlagen: - Privacyprotocol - Samenwerkingsovereenkomst NB.: De professional van de Proeftuin heeft binnen de Proeftuin twee afzonderlijke rollen namelijk: - werkzaamheden met betrekking tot toeleiding naar voorzieningen en/of jeugdhulp. Deze toeleidingstaken voert de professional uit in het kader van de taken en bevoegdheden van het college van B&W. Hierop is het juridisch kader van de publiekrechtelijke taak van het college van B&W van toepassing; - werkzaamheden in het kader van zorg- of hulpverlening. Deze hulpverlening valt onder de Wmo en de Jeugdwet niet onder de publiekrechtelijke taak van het college van B&W. De professionals van de Proeftuin zijn gebonden aan beroepsgeheim.

3.g. Hoe lang worden gegevens bewaard en termijn en wijze van vernietiging?	3.g. *Bewaartermijn* De zelfde termijnen gelden zoals afgesproken met Stichting OIDOS voor de Buurtteams. Namelijk gedurende vijftien jaar dan wel twintig jaar nadat de aanvrager wiens dossier het betreft geen gebruik meer maakt van een voorziening zoals bedoeld in de Wmo dan wel Jeugdwet. *Vernietiging:* De cliëntgegevens zoals bedoeld in 4.2. lid 1is Stichting OIDOS verantwoordelijk om de gegevens te verwijderen. Zij beheren de gegevens in WIZ portaal en zijn verantwoordelijk voor vernietiging. Gemeente Nijmegen houdt een archief bij van de uitgegeven maatwerkvoorzieningen, bureau BDI ziet toe op vernietiging daarvan.	3.g. Akkoord. NB. Gemeente Nijmegen is verantwoordelijk voor de vernietiging van persoonsgegevens door de teamleider bij de eerste screening. Dit betreft bv e-mails. Advies: minimaal eens per maand actieve check op vernietiging van de gegevens die niet meer noodzakelijk zijn voor het proces.
3.h. Hoe worden gegevens beveiligd?	3.h. WIZ portaal is beveiligd met 2-factor authenticatie. Voor aanvullende informatie zie artikel 10 Samenwerkingsovereenkomst. Voor de gegevens bedoeld in 3.2. lid 2 geldt dat de documenten zijn opgeslagen binnen een beveiligde omgeving waar deelnemers middels uitnodiging van de accounthouder en door middel van een wachtwoord toegang hebben.	3.h. Akkoord. De toekenning en intrekking van de autorisaties zijn essentieel in dit proces. Advies: opstellen van een autorisatiematrix.
4. Risico's en voorgestelde maatregelen	Deze zijn afdoende beschreven.	Akkoord. Naleving van de afspraken gemaakt in het privacy protocol en de verwerkersovereenkomst zijn essentieel. Elk jaar dient rond de jaarwisseling een nalevingsrapportage te worden gemaakt (gedurende de pilot).

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 zelf kent een "middel hoog" risico.
Dit betreft een pilot voor de duur van 2 jaar. Bij verlenging dient een nieuwe DPIA (of update) gemaakt te worden.
De maatregelen die worden beschreven, zijn m.i. afdoende.

Er zijn wel een paar aandachtspunten voor het komende jaar:

- De afweging welke gegevens per keer vastgelegd worden, dient gelogd te worden.
  Hierdoor is het mogelijk de afweging te bezien en te beoordelen of deze proportioneel is.
  Dataminimalisatie is het uitgangspunt.
- Gemeente Nijmegen is verantwoordelijk voor de vernietiging van persoonsgegevens door de teamleider bij de eerste screening. Dit betreft bv e-mails.
  Advies: minimaal eens per maand actieve check op vernietiging van die gegevens die niet meer noodzakelijk zijn voor het proces.
- De toekenning en intrekking van de autorisaties zijn essentieel in dit proces.
  Advies: opstellen van een autorisatiematrix.
- Naleving van de afspraken gemaakt in het privacy protocol en de verwerkersovereenkomst zijn essentieel.
  Verplichting: Elk jaar dient rond de jaarwisseling een nalevingsrapportage te worden gemaakt (gedurende de pilot).

Eind 2024 zal deze DPIA op naleving getoetst worden.
Daar wordt gelet op bovenstaande aandachtspunten.

Ik adviseer hiermee positief en daarmee zijn de resterende risico's "aanvaardbaar".

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

PK/25/04/2024. DPIA 81.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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

DPIA Oordeel FG gemeente Nijmegen

DPIA: Verwerkingenlogging

Inleiding

Hierbij het oordeel van de FG Gemeente Nijmegen over de DPIA 'Verwerkingenlogging'. 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, tezamen een aanvaardbaar risico vormen bij het gebruik van privacygevoelige gegevens.

In de periode maart – april 2024 hebben 5.1.2e, 5.1.2e, 5.1.2e, 5.1.2e 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 'Verwerkingenlogging' d.d. 29/04/2023.
Deze versie vormt de onderlegger voor deze toetsing.

Bij deze DPIA horen de volgende bijlage:
1. AWS DATA PROCESSING ADDENDUM

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?	Neen.	Akkoord.
2. Is het ethisch / politiek bestuurlijk verantwoord?	Ja. De verwerkingenlogging betreft een opslag die de metadata van (persoons)gegevens vanuit verschillende applicaties registreert. De AVG vereist dat organisaties op aanvraag inzage geven in plaatsgevonden verwerkingen van (persoons)gegevens, dit is de transparantieplicht (artikel 5 AVG). Op dit moment is het niet mogelijk om aan deze eis te voldoen met als belangrijkste reden dat er geen goede vastlegging plaatsvindt van wanneer welke gegevensverwerking plaatsvindt. Door de VNG is een standaard ontwikkeld voor logging van verwerkingen Daarnaast is er de wens om de mate van transparantie te vergroten richting de Nijmegenaar.	Akkoord. Verwerkingenlogging draagt eraan bij om inzageverzoeken efficiënter en completer af te handelen. Het inzien van verwerkingen is momenteel een inefficiënt en on-transparant proces. Verwerkingenlogging stelt de inwoner in staat om direct inzage te krijgen in deze gegevens, via Mijn Nijmegen, zonder hiervoor eerst een (handmatig) inzageverzoek in te dienen bij de Gemeente Nijmegen.
3. Juridische toets 3a. Doel / grondslag	3.a. *Doel* van deze gegevensverwerkingen: - Het verbeteren van de administratie van verwerkingen. Door consistent en op een gestructureerde manier verwerkingen te loggen verbetert dit de administratie van de verwerkingen. Een gevolg hiervan en mede een (sub)doel van het project is het geautomatiseerd en daarmee sneller en vollediger inzicht in verwerkte (persoons)gegevens bieden aan burgers. *Grondslag* De AVG vereist dat organisaties op aanvraag inzage geven in plaatsgevonden verwerkingen van (persoons)gegevens, dit is de transparantieplicht (artikel 5 AVG). De grondslag van de verwerking van de (persoons)gegevens metadata is artikel 5 AVG.	3.a. Akkoord. *Doel:* Door verwerkingen digitaal te loggen en de mogelijkheid te bieden om deze verwerkingen digitaal weer op te halen geef je de burger een mogelijkheid om op eigen wijze (persoonlijke) verwerkte gegevens op te vragen. Dit vervult een deel van het recht op inzage. *Grondslag* Akkoord.
3.b. Persoonsgegevens Worden bijzondere persoonsgegevens verwerkt?	3.b. Ja. Er worden afgeleide bijzondere persoonsgegeven opgeslagen. Deze gegevens komen uit de metadata van de verwerking.	3.b. Akkoord. In de metadata van de verwerking staat wanneer de verwerking heeft plaatsgevonden (tijdstip) en wie deze aanvraag heeft gedaan (gebruikersnaam in combinatie met gepseudonimiseerd BSN).
3.c. Proportionaliteit	3.c. De inbreuk in privacy is niet groter dan de logging van verwerkingen die al heeft plaatsgevonden. De aangesloten applicaties loggen de verwerkingen en sturen deze enkel door naar de verwerkingenlogging.	3.c. Akkoord. De verwerkingenlogging gebruikt deze gelogde verwerkingen om meer transparantie te bieden richting de Nijmegenaar.

3.d. Subsidiariteit	3.d. Het verwerkte gegeven in de verwerkingenlogging (BSN) wordt enkel gebruikt om te kunnen achterhalen aan wie het logrecord toebehoort. Deze wijze van opslaan is noodzakelijk om verwerkingenlogging op een gestructureerde en efficiënte manier te realiseren.	3.d. Akkoord. De standaard maakt onderscheid tussen minimale logging en volledige logging. Applicaties die loggen zijn niet altijd in staat om een volledige log aan te bieden. In dat geval is het voor een applicatie mogelijk om een beperkte (minimale) log aan te leveren.
3.e. Persoonsgegevens buiten EER gebruikt?	3.e. Neen	3.e. Neen
3.f. Andere partijen betrokken?	3.f. - Gemeente Nijmegen is verwerking verantwoordelijke. - Amazon Web Services (AWS) biedt de infrastructuur voor het verwerken en opslaan van de verwerkinglogs en is dus een verwerker..	3.f. Akkoord. Zie bijlage overeenkomst met AWS.
3.g. Hoe lang worden gegevens bewaard en termijn en wijze van vernietiging?	3.g. *Bewaartermijn* Een verwerkinglog (logregel) heeft geen eigen bewaartermijn. Het onderliggende proces bepaalt de bewaartermijn. Het verwerkinglog maakt gebruik van de termijn van de oorspronkelijke verwerking. *Vernietiging:* Binnen de verwerkingenlogging is dit een geautomatiseerd proces.	3.g. Akkoord. NB. Een verwerkinglog wordt - op dit moment - enkel logisch verwijderd, een daadwerkelijke (fysieke) verwijdering van de verwerkinglog wordt niet uitgevoerd. De verwerkingenlogging standaard geeft namelijk aan dat een logrecord onomkeerbaar moet zijn. Als een gebruiker of applicatie deze specifieke verwerkinglog op een later moment probeert op te vragen of te wijzigen zal de verwerkingenlogging aangeven dat de verwerkinglog niet bestaat.
3.h. Hoe worden gegevens beveiligd?	3.h. Binnen de verwerkingenlogging is gekozen voor de bearer authenticatie methode. Een technische omschrijving van deze authenticatie methode is te vinden in bijlage 3 van de DPIA. De bijbehorende autorisatie scopes zijn terug te vinden in bijlage 2 van de DPIA.	3.h. Akkoord. Alle records worden versleuteld opgeslagen. Zodra een verwerkinglog record wordt ontvangen door de verwerkingenlogging vanuit een applicatie zal gevoelige informatie worden versleuteld. Additioneel worden gevoelige persoonsgegevens gepseudonimiseerd. Momenteel is dit alleen het BSN.
4. Risico's en voorgestelde maatregelen	Risico 3: Verwijderen De records niet alleen logisch verwijderen, maar daadwerkelijk verwijderen. Zodra de verwerkingenlogging de opdracht krijgt om een verwerkinglog record te verwijderen wordt de record ook daadwerkelijk verwijderd uit de opslaglocatie. Verder wordt bij een opdracht om een verwerkinglog record te updaten de gegevens van de record overschreven, in plaats van het aanmaken van een nieuwe record naast het al bestaande record. Risico 4: Bewaartermijn Een standaard bewaartermijn instellen.	Akkoord. Advies: uitvoeren van maatregelen benoemd onder restrisico's 3 en 4. Hiermee wordt voorkomen dat een logrecord nooit wordt verwijderd indien dit niet expliciet wordt aangegeven.

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 zelf kent een "laag" risico.

Nog op te pakken:
Advies: uitvoeren van maatregelen benoemd onder restrisico's 3 en 4 betreffende verwijderen en bewaren.
Actie: Hierover bij de toets op naleving (november 2024) terugkoppelen.

Eind 2024 zal deze DPIA op naleving getoetst worden.

Ik adviseer hiermee positief en daarmee zijn de resterende risico's "aanvaardbaar".

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

PK/29/04/2024. DPIA 82.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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

DPIA Oordeel FG gemeente Nijmegen

DPIA: Allegro

Inleiding

Hierbij het oordeel van de FG Gemeente Nijmegen over de DPIA 'Allegro'. 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, tezamen een aanvaardbaar risico vormen bij het gebruik van privacygevoelige gegevens.

In de periode september 2023 – april 2024 hebben 5.1.2e, 5.1.2e, 5.1.2e, 5.1.2e 5.1.2e, 5.1.2e 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 'Allegro' d.d. 29/04/2023.
Deze versie vormt de onderlegger voor deze toetsing.

Bij deze DPIA horen de volgende bijlagen:
1. Verwerkersovereenkomst. Kred'it B.V.Allegro
2. Bewaartermijnen Allegro

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?	Neen.	Akkoord.
2. Is het ethisch / politiek bestuurlijk verantwoord?	Ja. Betreftuitvoering van de Wet Gemeentelijke Schuldhulpverlening (WGS) voor de Gemeente Nijmegen. Onder schuldhulpverlening wordt verstaan: het helpen van inwoners bij het vinden van een geschikte oplossing voor hun problematische schulden. Ook de nazorg om terugval te voorkomen valt onder schuldhulpverlening.	Akkoord. Voor de uitvoering van deze wet wordt gebruik gemaakt van het programma Allegro van de leverancier Kredit. Allegro Basis ondersteunt alle primaire processen en heeft daarnaast een groot aantal aanvullende modules. Het pakket is modulair opgebouwd. Deze DPIA richt zich op Allegro in het algemeen en de modules die worden gebruikt binnen de verschillende fasen in de schuldhulpverlening.
3. Juridische toets 3a. Doel / grondslag	3.a. *Doel* van deze gegevensverwerkingen: Uitvoering geven aan de wettelijke taak (WGS) van de gemeente op het gebied van schuldhulpverlening. Voor verschillende fasen in de schuldhulpverlening zijn concrete doelen binnen de schuldhulpverlening geformuleerd: - Doel 1. Vroegsignalering; - Doel 2. Toegang tot schuldhulpverlening (en besluit daartoe); - Doel 3. Opstellen van het plan van aanpak (en besluit daartoe) *Grondslag* Wet Gemeentelijke Schuldhulpverlening: Artikel 6 Inlichtingenplicht Artikel 7 Medewerkingsplicht Artikel 8 Gegevensuitwisseling - 8.a Verwerken persoonsgegevens schuldhulpverlening - 8.b Verwerken persoonsgegevens wanneer college uit eigen beweging gesprek aanbiedt - 8.c Gebruik Burgerservicenummer - 8.d Gebruik gegevens sociaal domein.	3.a. Akkoord. *Doel:* Akkoord. NB. Na deze fasen volgt de daadwerkelijke uitvoering van de hulpverlening. *Grondslag* Akkoord. Een gedetailleerde uitwerking van de WGS en de daarbij noodzakelijke gegevensverwerking is terug te vinden in de handreiking (zie DPIA pagina 3.)
3.b. Persoonsgegevens Worden bijzondere persoonsgegevens verwerkt?	3.b. Neen.	3.b. Akkoord. Schuldhulpverlening heeft wél impact op het leven van betrokkenen.
3.c. Proportionaliteit	3.c. Er worden ook niet meer gegevens gebruikt dan de gegevens die zijn vermeld in de handleiding van de Autoriteit Persoonsgegevens. De gegevens van de inwoner moeten bekend zijn om te oordelen of schuldhulpverlening mogelijk is. Er moet gecontroleerd worden of de inwoner Nederlands ingezetene is en geen fraudehistorie	3.c. Akkoord. Digitale verwerking van de gegevens draagt bij aan een snelle en efficiënte en correcte schuldhulpverlening. Per proces zal de afweging moeten worden gemaakt wat proportioneel is per handeling.

	heeft. Er moet verder worden vastgelegd hoe de schuldhulpverlening moet worden ingezet (omvang, vorm en duur).	Advies is om deze afweging met logging zichtbaar te maken.
3.d. Subsidiariteit	3.d . Er worden niet meer gegevens gevraagd en vastgelegd dan noodzakelijk en toegestaan voor het doel. De modulaire opbouw maakt maatwerk mogelijk.	3.d. Akkoord. Allegro voldoet aan de eisen voor archivering en vernietiging.
3.e. Persoonsgegevens buiten EER gebruikt?	3.e. Neen	3.e. Neen
3.f. Andere partijen betrokken?	3.f. - Verwerkersverantwoordelijke : Gemeente Nijmegen - Verwerker : Kredit, leverancier van Allegro. - De inwoner verstrekt zijn/haar persoons- en financiële gegevens (inkomen, verplichtingen en schulden) aan de medewerker van bureau Financiële Ondersteuning. - Schuldeisers van de inwoner leveren met toestemming van de inwoner en op verzoek van de medewerker financiële gegevens aan t.b.v. een schuldregeling. -Crediteuren van de inwoner leveren met toestemming van de inwoner en op verzoek van de medewerker financiële gegevens aan t.b.v. een budgetbeheer.	3.f. Akkoord. Zie bijlage overeenkomst met Kredit.
3.g. Hoe lang worden gegevens bewaard en termijn en wijze van vernietiging?	3.g. *Bewaartermijn* Voor het overgrote deel is het uitgangspunt 60 maanden. Er zijn enkele uitzonderingen. Zo worden leningen, schuldregelingen, archief-items en agenda-items 120 maanden bewaard. BKR Toetsuitslagen worden 48 maanden bewaard. Klaarstaande brieven/rapporten, klaargezette documenten, nachtlogging, StUF berichten en Decos berichten worden 5 maanden bewaard. De KEP-GNP logging wordt 0 maanden bewaard. *Vernietiging:* De digitale vernietiging is geborgd in een jaarlijks proces	3.g. Akkoord. Zie bijlage 'Bewaartermijnen' voor de details. Allegro bevat een module die signaleert wanneer de bewaartermijn verstrijkt en de gegevens op de juiste manier kan verwijderen.
3.h. Hoe worden gegevens beveiligd?	3.h. - De informatiebeveiliging vindt plaats volgens algemeen erkende normen, namelijk: NEN/ISO 27001. Kredit is ISO 27001 gecertificeerd. - De toereikendheid blijkt uit periodieke externe controles te weten audits t.b.v. de 27001 certificering	3.h. Akkoord. Er is een jaarlijkse controle (en bijbehorende correctie) op de lijst van geautoriseerde collega's en er wordt per module geautoriseerd.
4. Risico's en voorgestelde maatregelen	Voldoende beschreven	Akkoord. Dit staat of valt met het toekennen en intrekken van autorisaties.

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 zelf kent een "middelhoog" risico.

Restrisico's betreffen toekennen en intrekken autorisaties.
Daarnaast attendeer ik op het volgende:
Per proces zal de afweging moeten worden gemaakt wat proportioneel is (wat betreft uitvraag en vastlegging persoonsgegevens) per handeling. Advies is om deze afweging met logging zichtbaar te maken.

Eind 2024 zal deze DPIA op naleving getoetst worden.

Ik adviseer hiermee positief en daarmee zijn de resterende risico's "aanvaardbaar".

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

PK/29/04/2024. DPIA 83.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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

DPIA Oordeel FG gemeente Nijmegen

DPIA: Koppeling Yivi - BRP

Inleiding

Hierbij het oordeel van de FG Gemeente Nijmegen over de DPIA 'Yivi - BRP'. 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, tezamen een aanvaardbaar risico vormen bij het gebruik van privacygevoelige gegevens.

In de periode mei 2023 – april 2024 hebben 5.1.2e , 5.1.2e , 5.1.2e , 5.1.2e 5.1.2e , 5.1.2e 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 'Koppeling Yivi - BRP' d.d. 30/04/2024. Deze versie vormt de onderlegger voor deze toetsing.

Bij deze DPIA horen de volgende bijlagen:
1. 190326 DPIA IRMA app Nijmegen Management Samenvatting (1.0)
2. 190326 DPIA Rapport IRMA app Nijmegen (1.0)
3. AWS_GDPR_DPA
4. Verwerkersovereenkomst IRVN.Nijmegen
5. Verwerkersovereenkomst Nijmegen_signed
6. T&T - Verwerkersovereenkomst (v18.03) Nijmegen
7. T&T ovk - 0268-18.01
8. 20190115_Juridische analyse IRMA def (v6.0)
9. Presentatie IRMA analyse

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. Op 26 maart 2019 is een DPIA van de originele koppeling opgeleverd (kenmerk BKBO/190124-1/DPIA). Dit rapport is als bijlage opgenomen.	Akkoord. Met de vernieuwing van de Yivi-BRP koppeling is rekening gehouden met de aanbevelingen uit deze DPIA.
2. Is het ethisch / politiek bestuurlijk verantwoord?	Ja. De Yivi applicatie maakt het mogelijk om op een privacy vriendelijke manier alleen die gegevens te delen met anderen die nodig zijn voor het leveren van een dienst. De gemeente Nijmegen gebruikt deze mogelijkheid in haar webformulieren en mijn.nijmegen.nl omgeving. De Gemeente Nijmegen maakt het mogelijk om - conform het collegeakkoord - gegevens te verstrekken voor de Yivi-app, maar ook om Yivi als privacy vriendelijk alternatief naast DigiD aan te bieden voor eigen dienstverlening.	Akkoord. Door deze verwerking verstrekt de gemeente, op expliciet verzoek van een inwoner, een aantal gegevens uit de BRP aan die inwoner. De inwoner moet beschikken over de Yivi applicatie, daarin worden de gevraagde gegevens opgeslagen.
3. Juridische toets 3a. Doel / grondslag	3.a. *Doel* van deze gegevensverwerkingen: De Yivi applicatie maakt het mogelijk om op een privacy vriendelijke manier alleen die gegevens te delen met anderen die nodig zijn voor het leveren van een dienst. De gemeente Nijmegen gebruikt deze mogelijkheid in haar webformulieren en mijn.nijmegen.nl omgeving. *Grondslag* - Het verstrekken van de gegevens middels de Yivi-BRP koppeling is gebaseerd op de verplichting om inzage in en een afschrift van de BRP-gegevens te verschaffen op grond van artikel 6, eerste lid, aanhef en onder c AVG jo. Artikel 2:55 Wet BRP jo. Artikel 15, eerste lid, AVG, i.c.m. p. 44 van de memorie van toelichting op de Wet BRP. - Artikel 89 AVG voor de verwerking gericht op statistiek.	3.a. *Doel:* Akkoord. Een inwoner kiest er zelf voor om deze gegevens in de Yivi app te laden, of om Yivi te gebruiken voor onthullen van gegevens. Als gemeente maken we geen exclusief gebruik van Yivi, een inwoner heeft altijd een andere keus, bijvoorbeeld DigiD gebruiken. *Grondslag* Akkoord. Volledigheidshalve, de grondslag voor de verwerking van de gegevens die de gemeente zelf ontvangt uit de Yivi app als iemand daarmee inlogt voor het aanvragen van een dienst, ligt in de grondslag van die specifieke dienst zelf.
3.b. Persoonsgegevens Worden bijzondere persoonsgegevens verwerkt?	3.b. Neen.	3.b. Akkoord.
3.c. Proportionaliteit	3.c. Het gebruik van een privacy-vriendelijk alternatief is hierdoor mogelijk gemaakt. Een gebruiker kiest er in alle vrijheid voor zijn eigen persoonsgegevens op te halen, de gemeente verstrekt de persoonsgegevens.	3.c. Akkoord. Proces is vergelijkbaar met DigiD proces, alleen met meer mogelijkheden tot dataminimalisatie vanuit het gezichtspunt van de gebruiker.
3.d. Subsidiariteit	3.d . Dit is een alternatieve gegevensverstrekking. Er zijn andere mogelijkheden waar een burger óók voor kan kiezen (inloggen via DigiD).	3.d. Akkoord. Keuze kan - door de burger - in vrijheid worden genomen. Gekozen route zal niet leiden tot een andere informatiepositie.

3.e. Persoonsgegevens buiten EER gebruikt?	3.e. Neen	3.e. Neen
3.f. Andere partijen betrokken?	3.f. • GBA-V, via leverancier T&T Vertrouwd Verbonden – Landelijke BRP voorziening. • IRvN – Koppeling tussen GBA-V en de Yivi-BRP koppeling. • Signicat – Identity broker verzorgt authenticatie met DigiD, verwerkt daarvoor de onthulde attributen (waaronder potentieel het BSN). • AWS – Public cloud provider waar de infrastructuur van de koppeling op draait. Gemeente Nijmegen is verantwoordelijk voor de verwerking. De andere partijen zijn verwerkers. • Stichting Privacy by Design.	3.f. Akkoord. Gemeente Nijmegen heeft met deze partijen verwerkingsovereenkomsten. Deze zijn als bijlagen opgenomen bij deze DPIA. NB. De Stichting Privacy By Design is de ontwikkelaar van de Yivi app. Dat is een zelfstandige verantwoordelijkheid. Een inwoner heeft een relatie met de stichting op het moment dat de app gebruikt wordt.
3.g. Hoe lang worden gegevens bewaard en termijn en wijze van vernietiging?	3.g. *Bewaartermijn* Voor de twee sets met persoons- en adresgegevens geld een verschillende geldigheid in de app (adres 1 jaar, persoonsgegevens 5 jaar), een gebruiker kan er altijd voor kiezen om de data eerder uit de Yivi-app te verwijderen. De statistieken die worden verzameld over het verstrekken worden 1.5 jaar bewaard, deze bevat geen persoonsgegevens. De applicatielogging wordt 1 maand bewaard, deze bevat geen persoonsgegevens. *Vernietiging:* Gegevens worden automatisch vernietigd volgens de geconfigureerde bewaartermijnen dit geldt voor de verzamelde statistieken en applicatielogging t.b.v. de koppeling.	3.g. Akkoord. NB. De gegevens in de Yivi-app zijn na het verlopen van de geldigheidstermijn niet meer bruikbaar maar nog wel zichtbaar in de applicatie voor de gebruiker. Het is niet meer mogelijk om deze gegevens te delen met een partij die erom vraagt. In de applicatie is zichtbaar dat de geldigheidsduur verstreken is. Een gebruiker kan er altijd voor kiezen zijn gegevens eerder uit de app te verwijderen. Hiervoor is de Gemeente Nijmegen niet verantwoordelijk.
3.h. Hoe worden gegevens beveiligd?	3.h. De gegevens worden in de Yivi applicatie versleuteld. De sleutel is beveiligd met de pincode die een inwoner zelf aan maakt . De gegevens zijn in de Yivi applicatie digitaal ondertekend door een sleutel die exclusief door gemeente Nijmegen beheerd wordt. De door Yivi gebruikte cryptografie hiervoor maakt het mogelijk voor een afnemer om te valideren dat de gegevens niet gewijzigd zijn sinds uitgifte. De applicatielogging is enkel toegankelijk voor het DevOps team.	3.h. Akkoord. Het is expliciet de verantwoordelijkheid van een afnemer om deze validatie uit te voeren. Hiervoor is het toekennen en intrekken van autorisaties van belang.
4. Risico's en voorgestelde maatregelen	Voldoende beschreven.	Akkoord. Dit staat of valt met het toekennen en intrekken van autorisaties.

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 zelf kent een "laag" risico.

Restrisico's betreffen toekennen en intrekken autorisaties van het DevOps team.

Eind 2024 zal deze DPIA op naleving getoetst worden.

Ik adviseer hiermee positief en daarmee zijn de resterende risico's "aanvaardbaar".

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

PK/30/04/2024. DPIA 84.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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

DPIA Oordeel FG gemeente Nijmegen

DPIA: E-depotvoorziening gemeente Nijmegen

Inleiding

Hierbij het oordeel van de FG Gemeente Nijmegen over de DPIA 'E-depotvoorziening gemeente Nijmegen. 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, tezamen een aanvaardbaar risico vormen bij het gebruik van privacygevoelige gegevens.

In de periode mei – juli 2024 hebben 5.1.2e , 5.1.2e , 5.1.2e 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 'E-depotvoorziening gemeente Nijmegen' d.d. 07/07/2024. Deze versie vormt de onderlegger voor deze toetsing.

Bij deze DPIA horen de volgende bijlagen:
1. Overdrachtseisen digitaal archief versie 1.2. 26-07-2021.
2. Beslisboom bepalen openbaarheidsbeperkingen en termijnen daarbij. September 2019.
3. Verwerkersovereenkomst Gemeente Nijmegen – DEVENTit Bv. Oktober 2021
4. Verwerkersovereenkomst gemeente Nijmegen – Picturae Bv. Oktober 2021.

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?	Neen	Akkoord. Deze Data Protection Impact Assesment (DPIA) richt zich alleen op de e-depotvoorziening. Er zal voor het collectiebeheersysteem een afzonderlijke DPIA worden opgesteld.
2. Is het ethisch / politiek bestuurlijk verantwoord?	Ja. De Archiefwet verplicht elke overheids-organisatie om haar informatie duurzaam toegankelijk te maken en te houden en te vernietigen wanneer de bewaartermijn is verlopen.	Akkoord.
3. Juridische toets 3a. Doel / grondslag	3.a. *Doel* van deze gegevensverwerkingen: Het doel is het in bewaring nemen, het preserveren (duurzaam toegankelijk houden), het beheren en het ontsluiten van digitale archieven (informatieobjecten en metadata). *Grondslag* De verwerking (archivering) vindt plaats op grond van een wettelijke taak. Namelijk binnen de kaders van de Archiefwet 1995 (AW), het Archiefbesluit (AB) en de Archiefregeling (AR).	3.a. *Doel:* Akkoord. *Grondslag* Akkoord.
3.b. Persoonsgegevens Worden bijzondere persoonsgegevens verwerkt?	3.b. Ja. - NAW-gegevens, Bankgegevens, e-mailadressen, Burgerservicenummers - Bijzondere persoonsgegevens zoals bedoeld in artikel 9 AVG (persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid). - Gegevens over de financiële of economische situatie van de betrokkene, zoals schulden, salaris – en betalingsgegevens. - (Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene, zoals gegevens over gokverslaving, prestaties op school of werk of relatieproblemen. - Gegevens die kunnen worden misbruikt voor (identiteits)fraude, zoals biometrische gegevens en kopieën van identiteitsbewijzen. - Gegevens over kwetsbare groepen zoals minderjarigen, mensen die te maken hebben met stalking of mensen die in een blijf-van-mijn-lijfhuis verblijven; - Gegevens van kinderen en mensen met een verstandelijke handicap.	3.b. Akkoord. Zowel digitale als analoge archieven die naar het RAN zijn overgebracht of door het RAN zijn verworven kunnen documenten bevatten waarin bijgaande gegevens zijn vastgelegd. Dit betekent niet dat in alle documenten alle hiernaast aangegeven gegevens zijn vastgelegd, het betekent dat documenten onderstaande gegevens *kunnen* bevatten. Daarnaast wordt binnen de e-depotvoorziening de volgende gegevens vastgelegd: - Gebruikersnamen - Wachtwoorden - E-mailadressen

3.c. Proportionaliteit	3.c. Het belang voor opname van dit archief is een algemeen cultuurhistorisch belang (op basis van de Archiefwet en aanverwante wet- en regelgeving). Wanneer documenten (bijzondere) persoonsgegevens bevatten wordt steeds afgewogen en bepaald of en zo ja, op welke wijze deze documenten al dan niet openbaar worden gemaakt.	3.c. Akkoord. Hierbij wordt gewerkt met beslisbomen voor het bepalen van openbaarheidsbeperkingen en de te hanteren termijnen alsook technische maatregelen die genomen kunnen worden m.b.t. beschikbaarstelling. Deze beslisbomen zijn opgenomen als bijlage van deze DPIA.
3.d. Subsidiariteit	3.d . Archief is volgend op bedrijfsvoering. Als er minder ingrijpende manieren zijn om het doel te bereiken heeft dat normaliter de voorkeur, bijvoorbeeld indien gepseudonimiseerde of geanonimiseerde gegevens voldoen.	3.d. Akkoord. Dit speelt bijvoorbeeld bij beleidsonderzoek. Daar gaat het immers niet om individuele casuïstiek, maar om een generiek beeld.
3.e. Persoonsgegevens buiten EER gebruikt?	3.e. Neen	3.e. Akkoord.
3.f. Andere partijen betrokken?	3.f. Tussen de volgende partijen worden gegevens uitgewisseld: • Vitec Memorix B.V. (voorheen Picturae ICT Bv) • DEVENTit B.V. De rol van de leveranciers – Vitec Memorix B.V. (voorheen Picturae ICT B.V.) en DEVENTit B.V. – is die van gegevensverwerker. De gemeente Nijmegen is de verwerkingsverantwoordelijke.	3.f. Akkoord. Gemeente Nijmegen heeft met deze partijen verwerkingsovereenkomsten. Deze zijn als bijlagen opgenomen bij deze DPIA.
3.g. Hoe lang worden gegevens bewaard en termijn en wijze van vernietiging?	3.g. *Bewaartermijn* Eeuwigdurende/permanente/blijvende bewaring. De grondslag van deze bewaartermijn ligt binnen de Archiefwet, het Archiefbesluit en de “Selectielijst gemeentelijke en intergemeentelijke organen”. Het belang van de informatie bepaalt hoe lang de informatie bewaard moet worden. De Archiefwet zelf bevat geen bewaartermijnen. Deze worden per organisatie vastgelegd in selectielijsten. *Vernietiging:* De meeste documenten komen uiteindelijk in aanmerking voor vernietiging. Een relatief klein deel van de documenten worden in de selectielijst aangemerkt als blijvend te bewaren. Deze documenten moeten (in principe binnen twintig jaar) worden overgebracht naar een archiefbewaarplaats.	3.g. Akkoord. De “Selectielijst gemeentelijke en intergemeentelijke organen” vormt de basis voor het bewaren en vernietigen van documenten bij gemeenten en intergemeentelijke organen. Deze selectielijst is opgesteld door de Vereniging Nederlandse Gemeenten (VNG). De meest recente selectielijst stamt uit 2020. NB. Er wordt niet vernietigd binnen de e-depotvoorziening. In de e-depotvoorziening wordt enkel blijvend te bewaren archief opgenomen. Vernietiging heeft vóór opname plaatsgevonden.
3.h. Hoe worden gegevens beveiligd?	3.h. Twee medewerkers van het RAN zijn geautoriseerd voor toegang tot de e-depotvoorziening en gekoppelde opslagsystemen. Autorisatie voor andere medewerkers kan alleen aangevraagd worden door de beheerder van de e-depotvoorziening	3.h. Akkoord.

	en alleen verleend worden door Vitec Memorix. De autorisaties worden jaarlijks gecontroleerd.	
4. Risico's en voorgestelde maatregelen	Voldoende beschreven.	Akkoord. Nog uit te voeren actie: 5.1.2h 5.1.2h 5.1.2h 5.1.2h 5.1.2h 5.1.2h 5.1.2h 5.1.2h 5.1.2h

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 zelf kent een "laag" risico.

Nog uit te voeren actie:

Eind 2024 zal deze DPIA op naleving getoetst worden.
Er zal dan duidelijkheid moeten komen over de invoering van de 2 Factor Authenticatie.

Ik adviseer hiermee positief en daarmee zijn de resterende risico's "aanvaardbaar".

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

PK/08/07/2024. DPIA 85.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenss feer	1
Wet open overheid	Art. 5.1 lid 2 sub h	De beveiliging van personen en bedrijven e n het voorkomen van sabotage	4, 5

DPIA Oordeel FG gemeente Nijmegen

DPIA: VTH Software voor BRIKS-taken

Inleiding

Hierbij het oordeel van de FG Gemeente Nijmegen over de DPIA 'VTH Software voor BRIKS-taken'. 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, tezamen een aanvaardbaar risico vormen bij het gebruik van privacygevoelige gegevens.

In de periode mei – juni 2024 hebben 5.1.2e, 5.1.2e, 5.1.2e, 5.1.2e 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 'VTH Software voor BRIKS-taken' d.d. 18/06/2024. Deze versie vormt de onderlegger voor deze toetsing.

Bij deze DPIA horen de volgende bijlagen:
-

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?	Neen	Akkoord.
2. Is het ethisch / politiek bestuurlijk verantwoord?	Ja. Nijmegen wil de BRIKS-taakuitvoering weer insourcen bij de eigen organisatie. Het gaat hierbij om alle VTH-taken (vergunningverlening, toezicht en handhaving) die samenhangen met de Omgevingswet-activiteiten die niet milieu gerelateerd zijn, te denken aan: bouwen, afwijken van het bestemmingsplan, brandveilig gebruiken, monumenten, slopen zonder asbest, uitwegen/ inritten, kappen, reclame, alsmede de taken die onder andere niet milieu gerelateerde regelgeving valt zoals de huisvestingswet en leegstandwet. Om de BRIKS-taken weer in Nijmegen uit te kunnen voeren, is voor de diverse VTH-processen een goede ICT-ondersteuning nodig: VTH-software.	Akkoord. Het doel van het project is dat er een VTH-systeem wordt aangeschaft, ingericht en uiterlijk op 1 januari 2025 in gebruik is genomen. Dit VTH-systeem wordt gebruikt om vergunningsprocedures te voeren, meldingen te ontvangen, toezicht te houden en zo nodig te handhaven bij overtredingen. In dit systeem worden persoonsgegevens gebruikt die voor dergelijke processen nodig zijn. Denk aan NAW-gegevens, KVK-gegevens, locatiegegevens, mailadressen, telefoonnummers en BSN/KVK-nummers. Deze DPIA wordt gebruikt bij de aanbesteding van de software (vorm van privacy by design).
3. Juridische toets 3a. Doel / grondslag	3.a. *Doel* van deze gegevensverwerkingen: Voldoen aan de wettelijke plicht om vergunningen, toezicht en handhaving van het omgevingsrecht te kunnen uitvoeren en daarbinnen samen te werken met andere bestuursorganen (zie hoofdstuk 2 Omgevingswet). *Grondslag* • Verwerking is noodzakelijk om te voldoen aan een wettelijke plicht (de verplichting om aanvragen en meldingen digitaal te kunnen ontvangen en aan te sluiten op het Digitale Stelsel Omgevingswet - artikel 14.1 Omgevingsbesluit). • Verwerking is noodzakelijk voor de uitvoering van een wettelijke taak (de toewijzing van de bevoegdheden uit de Omgevingswet aan de bestuursorganen van de gemeente - artikel 2.3 lid 1 Omgevingswet)	3.a. *Doel:* Akkoord. *Grondslag* Akkoord.
3.b. Persoonsgegevens Worden bijzondere persoonsgegevens verwerkt?	3.b. Neen: • NAW • Mailadres • Telefoonnummer • BSN of KVK-nummer	3.b. Akkoord. Dit zijn geen bijzondere persoonsgegevens.
3.c. Proportionaliteit	3.c. Alleen om de gegevens die nodig zijn voor het behandelen van een zaak en om correspondentie te kunnen voeren, worden opgevraagd.	3.c. Akkoord.

3.d. Subsidiariteit	3.d . Zonder de beoogde gegevens kan een individueel persoon of bedrijf niet geïdentificeerd en/of geadresseerd worden.	3.d. Akkoord.
3.e. Persoonsgegevens buiten EER gebruikt?	3.e. Neen	3.e. Akkoord.
3.f. Andere partijen betrokken?	3.f. Nog onbekend. Volgt ná de aanbesteding. Bij de verwerking van deze gegevens zijn gemeente Nijmegen en de leverancier van de VTH-software betrokken.	3.f. Akkoord. Een verwerkingsovereenkomst is onderdeel van de leveringsovereenkomst. Actie: na aanbesteding toevoegen aan dossier DPIA.
3.g. Hoe lang worden gegevens bewaard en termijn en wijze van vernietiging?	3.g. *Bewaartermijn* Afhankelijk van de landelijk afgesproken bewaartermijnen zoals vermeld in de Selectielijst Gemeenten. De persoonsgegevens worden niet langer bewaard dan noodzakelijk is voor de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt. De volgende termijnen worden in acht genomen: • De Persoonsgegevens worden op grond van de regelgeving voor fiscale gegevens en de Archiefwetgeving tot maximaal vijf jaar na sluiting van het dossier bewaard. • Voor zover dit voortvloeit uit de omschreven doelen of wanneer sprake is van bijzondere omstandigheden of incidenten kunnen de Persoonsgegevens langer dan de genoemde termijn worden bewaard. *Vernietiging:* Aan de hand van de selectielijst worden vernietigingslijsten samengesteld. Deze lijsten worden besproken in het overleg met Archief-inspectie, BDI en procesverantwoordelijke.	3.g. Akkoord. Voor de BRIKS taken komt het er in de praktijk op neer dat de meeste zaken permanent moeten worden bewaard. Daarom is het belangrijk om een koppeling te realiseren met het E-depot, zodat de overdracht van archieven soepel verloopt. De bewaring op grond van bijzondere omstandigheden of incidenten zal niet langer dan strikt noodzakelijk zijn. Indien archivering in Corsa plaatsvindt, is BDI verantwoordelijk voor het beheer
3.h. Hoe worden gegevens beveiligd?	3.h. Er zal alleen toegang tot de VTH-software zijn met licentie en autorisatie. Verschillende rollen hebben verschillende autorisaties.	3.h. Akkoord. In te regelen bij implementatie. Toevoegen aan dossier DPIA.
4. Risico's en voorgestelde maatregelen	Voldoende beschreven, voor zover dat in deze situatie mogelijk is. Er is een module Inzien in de applicatie, die de publicatie van stukken bij de publicatie van bekendmakingen mogelijk maakt. Deze stukken moeten dan eerst geanonimiseerd worden met de tool eAnonimiseren. Vanuit de zaak kunnen de betreffende documenten geopend worden, waarna automatisch de anonimiseringssoftware opent. Het is afhankelijk van de tool eAnonimiseren of dat anonimiseren (deels) geautomatiseerd kan worden.	Akkoord. Er zit een kwetsbaarheid in m.b.t. het (on)geautomatiseerd publiceren van niet geanonimiseerde bestanden zonder controlemechanisme. Dat betekent dat dit geregeld moet worden in de implementatie, hetzij door een geautomatiseerde koppeling met de tool eAnonimiseren, hetzij in een werkproces.

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 zelf kent een "laag" risico.

Nog uit te voeren acties na aanbesteding en implementatie:
- verwerkersovereenkomst met leverancier.
- autorisatiematrix
- het inregelen van eAnonimiseren, ten behoeve van het proces 'publicatie van stukken bij de publicatie van bekendmakingen'.

Eind 2024 zal deze DPIA op naleving getoetst worden.

Ik adviseer hiermee positief en daarmee zijn de resterende risico's "aanvaardbaar".

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

PK/18/07/2024. DPIA 86.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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

DPIA Oordeel FG gemeente Nijmegen

DPIA: Planon

Inleiding

Hierbij het oordeel van de FG Gemeente Nijmegen over de DPIA 'Planon'. 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, tezamen een aanvaardbaar risico vormen bij het gebruik van privacygevoelige gegevens.

In de periode dec 2023 – juli 2024 hebben 5.1.2e ,5.1.2e ,5.1.2e 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 'Planon' d.d. 16/07/2024. Deze versie vormt de onderlegger voor deze toetsing.

Bij deze DPIA horen de volgende bijlagen:
- Verwerkersovereenkomst IRvN – Gemeente Nijmegen 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?	Neen.	Akkoord.
2. Is het ethisch / politiek bestuurlijk verantwoord?	Ja. Voor facilitair management worden o.a. de klachten, wensen, informatie aanvragen, storingen (kortweg KWIS), cateringorders, inventaris/zaalreserveringen en zakelijke bezoekers geregistreerd. Omdat aan deze registratie 'vaak' een actie hangt, worden er persoonsgegevens geregistreerd. Bij het beheer van de gebouwen wordt voor onderhoud gewerkt met werkorders waarin contactgegevens van uitvoerders en aanspreekpunten worden verwerkt. Ook wordt de administratie van de huurcontracten bijgehouden binnen de applicatie. Ten behoeve van de contractadministratie worden NAW-gegevens, KVK-gegevens en contactgegevens van huurders bijgehouden.	Akkoord.
3. Juridische toets 3a. Doel / grondslag	3.a. *Doel* van deze gegevensverwerkingen: Deze verwerking is nodig om de facilitaire dienstverlening goed uit te kunnen voeren en optimaliseren en hierover te communiceren met bezoekers en medewerkers. De verwerkingen met betrekking tot het gebouwenbeheer zijn noodzakelijk om de financiële en contractuele afspraken met huurders te borgen. *Grondslag* Verwerking is noodzakelijk voor de behartiging van een gerechtvaardigd belang	3.a. *Doel:* Akkoord. *Grondslag* Akkoord.
3.b. Persoonsgegevens Worden bijzondere persoonsgegevens verwerkt?	3.b. Neen.	3.b. Akkoord. Zie DPIA ad 4.2. voor de lijst persoonsgegevens.
3.c. Proportionaliteit	3.c. De gegevens voor bezoekersregistratie zijn noodzakelijk om te kunnen verifiëren of toegangspassen aan de juiste persoon worden uitgereikt. De bezoekersregistratie dient daarmee de veiligheid in de gebouwen. Voor het gebouwenbeheer geldt dat de verwerking noodzakelijk is om de wederzijdse contractuele verplichtingen tussen huurder en eigenaar van de gebouwen goed na te kunnen komen.	3.c. Akkoord.
3.d. Subsidiariteit	3.d . De huidige administratie zoals die zich nu in Planon bevindt, is een doorontwikkeling van het ouderwetse kaartenbak-principe.	3.d. Akkoord.

3.e. Persoonsgegevens buiten EER gebruikt?	3.e. Nee, Planon draait on-premise in het datacenter van iRvN.	3.e. Akkoord.
3.f. Andere partijen betrokken?	3.f. De volgende partijen zijn betrokken: Nijmegen is verwerkingsverantwoordelijk. De verwerker is de IRvN.	3.f. Akkoord. De Verwerkersovereenkomst met de IRvN is bijgevoegd.
3.g. Hoe lang worden gegevens bewaard en termijn en wijze van vernietiging?	3.g. *Bewaartermijnen en Vernietiging:* De bezoekersgegevens worden maximaal 7 dagen bewaard. De gegevens ten behoeve van gebouwenbeheer en verhuur worden jaarlijks gecontroleerd waarbij de gegevens van huurders van wie de huurovereenkomst niet meer loopt worden opgeschoond voor zover andere wettelijke verplichtingen dit niet in de weg staan.	3.g. Akkoord. Verantwoordelijk voor vernietiging bezoekersgegevens: - manager Facilitair, afdeling PIF. Verantwoordelijk voor vernietiging van huurdersgegevens: - manager Vastgoed, afdeling VSA. De functioneel applicatiebeheerders van iRvN zien daarop toe.
3.h. Hoe worden gegevens beveiligd?	3.h. De applicatie zelf is enkel ontsloten via de beveiligde Citrix-omgeving en beveiligde verbindingen (https). Het netwerk is verder zodanig gesegmenteerd dat de front-end van de applicatie door middel van firewalls gescheiden is van de database en benodigde file-server. Gegevens worden beveiligd doormiddel van encryptie.	3.h. Akkoord. Twee maal per jaar vindt een gebruikersreview plaats waarin door zowel applicatiebeheerders van iRvN als betrokken afdelingen wordt gecontroleerd of de autorisaties nog conform deze doelstelling zijn of moeten worden aangepast.
4. Risico's en voorgestelde maatregelen	Het restrisico is altijd dat de gegevens uitgeprint worden, bijvoorbeeld op een werkorder, en vervolgens op een openbare plaats terecht komen. Na 7 dagen worden alle persoonsgegevens van de bezoeker geanonimiseerd.	Akkoord. Het doel is de applicatie als SaaS te gaan afnemen van de leverancier. Daarvoor dient t.z.t. een nieuwe DPIA gemaakt te worden, maar deze stap geeft de mogelijkheid om bijvoorbeeld werkorders volledig digitaal en via de applicatie met uitvoerders te delen.

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 zelf kent een 'laag' risico.

Eind 2024 zal deze DPIA op naleving getoetst worden.

Ik adviseer hiermee positief en daarmee zijn de resterende risico's "aanvaardbaar".

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

PK/18/07/2024. DPIA 87.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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

DPIA Oordeel FG gemeente Nijmegen

DPIA: Camera verkeerstellingen Heijendaal

Inleiding

Hierbij het oordeel van de FG Gemeente Nijmegen over de DPIA 'Camera verkeerstellingen Heijendaal'. 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, tezamen een aanvaardbaar risico vormen bij het gebruik van privacygevoelige gegevens.

In de periode mei – juni 2024 hebben 5.1.2e, 5.1.2e, 5.1.2e, 5.1.2e 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 'Camera verkeerstellingen Heijendaal' d.d. 18/07/2024. Deze versie vormt de onderlegger voor deze toetsing.

Bij deze DPIA horen de volgende bijlagen:
- Verwerkersovereenkomst uitvoering Verkeersonderzoek opheffen busbaan Heyendaalseweg.

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?	Neen	Akkoord.
2. Is het ethisch / politiek bestuurlijk verantwoord?	Ja. De infrastructuur op en rondom station Nijmegen Heyendaal wordt aangepast. Onduidelijk is wat de verkeerssamenstelling is, hoeveel verkeer er rijdt en wat de precieze terugslag is. Er ontstaat nu namelijk een terugslag (file) vanaf de rotonde Heyendaalseweg - Groenewoudseweg. Om de omvang van de terugslag in beeld te brengen wordt gebruik gemaakt van een verkeerstelling uitgevoerd door bureau Goudappel. Deze zal de telling uitvoeren door middel van camera's.	Akkoord. Op dit moment kan gemeten worden met tellussen (slangen over het wegdek die luchtsignalen naar een kastje sturen) of een wegkantradar. Deze kunnen slecht veel voertuigen tegelijkertijd tellen en daarmee zeggen ze weinig over hoeveel terugslag er is.
3. Juridische toets 3a. Doel / grondslag	3.a. *Doel* van deze gegevensverwerkingen: Het in kaart brengen van filevorming en de verkeerssamenstelling om deze gegevens te gebruiken voor het verbeteren van het verkeer. *Grondslag* • De grondslag is gelegen in artikel 44 van het Besluit administratieve bepalingen inzake het wegverkeer (BABW). Hierin wordt het bevoegd gezag (de gemeente) de bevoegdheid gegeven om een verkeersonderzoek in te zetten	3.a. *Doel:* Akkoord. *Grondslag* Akkoord.
3.b. Persoonsgegevens Worden bijzondere persoonsgegevens verwerkt?	3.b. Nee. Personen, voertuigen en kentekens zijn herkenbaar op de beelden, maar dit zijn geen bijzondere persoonsgegevens.	3.b. Akkoord.
3.c. Proportionaliteit	3.c. De verwerking geeft een behoorlijke privacy inbreuk op personen in het gebied. Personen kunnen namelijk herkenbaar op beeld komen. Op deze locatie wordt op vier dagen gemonitord. Betrokkenen kunnen een inzageverzoek, verzoek om correctie of gegevenswissing, of een bezwaar indienen via de reguliere weg (website).	3.c. Akkoord. Betrokkenen worden door middel van een poster geïnformeerd. Ze kunnen voor uitgebreide informatie een webpagina bereiken via een QR-code. De posters hangen rondom het gebied op de toeleidende wegen.
3.d. Subsidiariteit	3.d . Andere onderzoeksmethoden zoals telslangen, detectielussen en wegkantradars zijn minder betrouwbaar. Ze kunnen vaak niet goed onderscheid maken tussen verschillende voertuigen.	3.d. Akkoord. Telslangen en detectielussen zijn veel duurder dan een camera plaatsen en die laten uitlezen. De voertuigen met de hand tellen is ook geen realistisch alternatief.
3.e. Persoonsgegevens buiten EER gebruikt?	3.e. Neen	3.e. Akkoord.

3.f. Andere partijen betrokken?	3.f. De betrokken partijen zijn de gemeente Nijmegen, Goudappel en NDC Nederland. NDC Nederland plaatst de camera's en leest de beelden uit. Een medewerker van het bedrijf noteert geanonimiseerde gegevens over modaliteit, afstand en tijd. NDC stuurt die gegevens op aan onderzoeksbureau Goudappel. NDC verwijdert de camera's en verwijdert uiterlijk na één maand de beelden. Goudappel gebruikt de aangeleverde gegevens om een modelstudie uit te voeren en een advies uit te brengen aan Gemeente Nijmegen. Gemeente Nijmegen gebruikt dit advies in een ontwerp.	3.f. Akkoord. Goudappel is opdrachtnemer en verwerker. Hoewel Goudappel zelf geen persoonsgegevens verwerkt, worden er door de inzet van NDC Nederland wel persoonsgegevens verwerkt. NDC Nederland kan worden gezien als subverwerker. Met Goudappel is een verwerkersovereenkomst gesloten waarin NDC Nederland als subverwerker wordt vermeld. Deze overeenkomst is als bijlage bij deze DPIA gevoegd
3.g. Hoe lang worden gegevens bewaard en termijn en wijze van vernietiging?	3.g. *Bewaartermijn* Goudappel ontvangt alleen geaggregeerde en geanonimiseerde data (geen persoonsgegevens). NDC Nederland bewaart de oorspronkelijke data tot een maand na oplevering aan Goudappel. *Vernietiging:* Goudappel ziet toe op de vernietiging van de databestanden bij NDC Nederland.	3.g. Akkoord. ISO 27001 is van toepassing met verklaring van toepasselijkheid zoals bijgevoegd.
3.h. Hoe worden gegevens beveiligd?	3.h. • De camera maakt zogenaamde overzichtsbeelden (vanuit hoogte) waardoor individuele autobestuurders en andere weggebruikers (fietsers) zo min mogelijk herkenbaar in beeld komen. • Weggebruikers/voorbijgangers kunnen niet inloggen op de camera: Beelden worden alleen lokaal opgeslagen in een vandaalbestendige afgesloten kast (geen online toegang); • Beeldopnames worden alleen lokaal opgeslagen en geanalyseerd door daarvoor specifiek geautoriseerde medewerkers. De beelden worden niet op netwerkschijven gedeeld.	3.h. Akkoord. • Bij de beeldanalyse worden alleen mobiliteitsgegevens genoteerd: aantallen auto's (geen persoonsgegevens); • Na de beeldanalyse worden de beelden vernietigd (uiterlijk binnen één maand na oplevering van de resultaten).
4. Risico's en voorgestelde maatregelen	Voldoende beschreven.	Akkoord. Informeren van de voorbijgangers en weggebruikers is in deze cruciaal.

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 zelf kent een "middelhoog" risico.

Eind 2024 zal deze DPIA op naleving getoetst worden.
De wijze van communiceren naar betrokkenen en eventuele reacties op dit onderzoek zullen onderdeel moeten zijn van de rapportage.

Ik adviseer hiermee positief en daarmee zijn de resterende risico's "aanvaardbaar".

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

PK/18/07/2024. DPIA 88.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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

DPIA Oordeel FG gemeente Nijmegen

DPIA: Open Stad

Inleiding

Hierbij het oordeel van de FG Gemeente Nijmegen over de DPIA 'Open Stad'. 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, tezamen een aanvaardbaar risico vormen bij het gebruik van privacygevoelige gegevens.

In de periode mei – juli 2024 hebben 5.1.2e, 5.1.2e, 5.1.2e, 5.1.2e, 5.1.2e, 5.1.2e, 5.1.2e 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 'Open Stad' d.d. 23/07/2024. Deze versie vormt de onderlegger voor deze toetsing.

Bij deze DPIA horen de volgende bijlagen:
- Verwerkersovereenkomst Draad - Nijmegen

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?	Neen.	Akkoord.
2. Is het ethisch / politiek bestuurlijk verantwoord?	Ja. Het platform 'Open Stad' is een platform dat ingezet kan worden voor digitale participatie. De ontstaansgrond van de applicatie is in de Common Ground community. Er is een proef om het platform Open Stad in te zetten voor de mobiliteitstransitie Het huidige digitale participatie platform (Mijn Wijkplan) biedt onvoldoende mogelijkheden om goed samen te werken met de stad. Uiteindelijk moet het platform Open Stad breder in de organisatie ingezet kunnen worden om: • Inwoners te informeren over gemeentelijke en niet-gemeentelijke projecten en beleidsontwikkeling • Inwoners te betrekken bij gemeentelijke en niet-gemeentelijke projecten en beleidsontwikkeling • Inwonersinitiatieven op te halen in brede zin (inrichting openbare ruimte, maar optioneel ook sociale initiatieven) • Inwoners te betrekken bij inwonersinitiatieven.	Akkoord. Het is de bedoeling dat het platform voor meerdere processen ingezet gaat worden. Resultaten hiervan dienen gebruikt te worden bij de verdere implementatie van het platform Deze DPIA heeft als uitgangspunt de vervanging van het proces rondom Mijn Wijkplan bij de afdeling Stadsbeheer door het platform Open Stad. Indien meerdere en andere processen ook gebruik gaan maken van Open Stad zal dit kunnen leiden tot hetzij een nieuwe vergelijkbare DPIA gericht op een ander proces, hetzij tot een aanvulling / addendum op deze DPIA. Bij gebruik door meerdere afdelingen voor meerdere processen, kan het zijn dat de verantwoordelijkheid voor het gebruik van het platform niet meer bij de afdeling Stadsbeheer komt te liggen maar overgaat naar de concernafdeling VJB.
3. Juridische toets 3a. Doel / grondslag	3.a. *Doel* van deze gegevensverwerkingen: De Omgevingswet benadrukt op diverse plekken het belang van participatie. Met OpenStad wordt doorgegaan met het ophalen van inwonersinitiatieven voor de openbare ruimte. Het past binnen het participatie beleid voor het ruimtelijk domein. *Grondslag* - De grondslag betreft over het algemeen: toestemming van de betrokkene. Bij het aanmaken van een account - om een like, reactie of plan in te sturen - wordt *expliciet* toestemming gevraagd aan gebruikers om akkoord te gaan met de privacyverklaring door middel van een extra vinkje bij het aanmaken van een account. - Het kan voorkomen dat participatie in de Omgevingswet wordt voorgeschreven, zoals in artikel 16.55, lid 7 Omgevingswet. Dan is er sprake van uitvoering van een wettelijke taak.	3.a. *Doel:* Akkoord. *Grondslag* Akkoord. Bij de rapportage op naleving dient dit (uit vrije wil toestemminggeven) duidelijk zichtbaar gemaakt te worden.

3.b. Persoonsgegevens Worden bijzondere persoonsgegevens verwerkt?	3.b. Nee, in principe niet. Per project kan een privacyverklaring op maat worden gemaakt waarin mensen toestemming geven voor het verwerken van de benodigde persoonsgegevens. Zeer privacygevoelige gegevens zoals BSN, sekse, geloofsovertuiging etc. zullen nooit worden uitgevraagd.	3.b. Akkoord. Als er sprake is van een privacyverklaring op maat, dient dit vastgelegd en gelogd te worden.
3.c. Proportionaliteit	3.c. Inwoners kunnen zonder account de site gebruiken om voor hen relevante informatie op te zoeken. Om te reageren en dus te participeren, moet een account worden aangemaakt. De gegevens die hiervoor worden gebruikt zijn minimaal. De gebruikersnaam die wordt gekozen hoeft niet hetzelfde te zijn als de naam van de inwoner (een alias), waardoor de inwoner zelf kan kiezen voor een bepaald level van anonimiteit tegenover de andere gebruikers van de applicatie. Het e-mailadres is wel nog steeds zichtbaar voor de beheerder.	3.c. Akkoord. Zonder deze set aan gegevens komt de bruikbaarheid en het beheer van de site in gedrang. Bijvoorbeeld, als zomaar eenieder kan reageren op een initiatief voor een wijk waar ze niet in wonen
3.d. Subsidiariteit	3.d . De functionaliteiten in MijnWijkplan zijn niet meer toereikend voor het vormgeven van digitale participatie. De functionaliteiten van OpenStad zijn dat wel. Zo moet er ruimte komen op OpenStad om digitale participatie vorm te geven bij beleidsontwikkeling en projecten van zowel gemeente als externe initiatiefnemers. Zonder aanmaken van een account is het risico op misbruik (bijv. spamming door bots) groter.	3.d. Akkoord.
3.e. Persoonsgegevens buiten EER gebruikt?	3.e. Neen.	3.e. Akkoord.
3.f. Andere partijen betrokken?	3.f. De volgende partijen zijn betrokken: • Gemeente Nijmegen: verwerkingsverantwoordelijke • Draad: verwerker o Subverwerker: True BV o Subverwerker: Sendpro (vh Flowmailer BV)	3.f. Akkoord. Verwerkersovereenkomst met Draad is bijgevoegd.
3.g. Hoe lang worden gegevens bewaard en termijn en wijze van vernietiging?	3.g. *Bewaartermijnen en Vernietiging:* Als er een account aangemaakt is zullen de gegevens worden bewaard zolang dat account actief is. Het account wordt automatisch verwijderd na een jaar inactiviteit. Gebruikers worden hiervan op de hoogte gebracht. Eventueel uitgevraagde aanvullende gegevens worden verwijderd een half jaar na afloop van een project.	3.g. Akkoord. Er wordt een key-user aangewezen die verantwoordelijk is voor de naleving en controle van de vernietiging. In de rapportage over naleving dient aangegeven te worden welke functionaris dit is en welke werkwijze gehanteerd is. Een autorisatie matrix is gewenst.

3.h. Hoe worden gegevens beveiligd?	3.h. Inloggen op de backoffice-omgeving (de admin-inlog op de website) gebeurt met het nijmegen.nl e-mailadres en een zelfgekozen wachtwoord en MFA via SMS. Inloggen op de frontoffice (de gebruikersaccount op de publieke site) gebeurt door een zelfgekozen gebruikersnaam en wachtwoord. Onderzocht wordt nog of inloggen via Yivi mogelijk is.	3.h. Akkoord. Zie maatregelen bij risico's.
4. Risico's en voorgestelde maatregelen	Op dit moment wordt OpenStad gebruikt voor één project: de mobiliteitstransitie. Risico's moeten daaruit blijken. Voorbeelden zijn: • Medewerkers kunnen onterecht toegang hebben tot projectgegevens als de rechtenconfiguratie niet goed is (kan de beheerder een autorisatiematrix uitdraaien en kunnen we logging opvragen van wie wat gedaan heeft). Iemand die bijv. een site voor MO aanmaakt moet niet in een SB project terecht kunnen komen. • Medewerkers kunnen onterecht toegang hebben tot de applicatie als er geen deugdelijk gebruikersaccountbeheer is ingericht. • Inwoners die participeren kunnen mogelijk elkaars gegevens zien als deze niet goed afgeschermd worden. Het gaat hierbij enkel om naam en achternaam die getoond worden bij het reageren op de website, mits de betrokkene de volledige naam heeft ingevuld in zijn/haar/hun account i.p.v. een alias. E-mailadres is nooit aan de voorkant zichtbaar. Inwoners kunnen altijd zelf hun reacties nog verwijderen, of het laten verwijderen door de beheerder. Het is geen optie om te kiezen voor 'anoniem plaatsen'.	Akkoord. Mits mogelijke maatregelen worden uitgevoerd. Risico's moeten duidelijk worden in het project mobiliteitstransitie. Maatregelen moeten worden meegenomen bij bredere ingebruikname, waarbij ook de restrisico's duidelijk worden. Hierover dient in de rapportage over naleving van deze DPIA (najaar 2024) nader gerapporteerd te worden.

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 zelf kent een 'laag' (na uitvoering van alle genoemde maatregelen) tot 'middelhoog' (indien geen enkele maatregel uitgevoerd wordt) risico.

Maatregelen zijn benoemd bij:

2.
Implementeren van maatregelen gebaseerd op de resultaten afkomstig uit de proef bij de mobiliteitstransitie.

3.a.
Het expliciet vragen om toestemming aan de betrokkene.

3.b.
Als er sprake is van een privacyverklaring op maat, dient dit vastgelegd en gelogd te worden.

3.g.
Aanwijzen key functionaris en gebruikmaken van een autorisatiematrix.

4.
Beschrijven van maatregelen bij bredere ingebruikname, waarbij ook de restrisico's duidelijk worden.

Eind 2024 zal deze DPIA op naleving getoetst worden.

Ik adviseer hiermee positief en daarmee zijn de resterende risico's "aanvaardbaar".

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

PK/25/07/2024. DPIA 89.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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

DPIA Oordeel FG gemeente Nijmegen

DPIA: MS 365

Inleiding

Hierbij het oordeel van de FG Gemeente Nijmegen over de DPIA 'MS 365'. 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, tezamen een aanvaardbaar risico vormen bij het gebruik van privacygevoelige gegevens.

In de periode april – juli 2024 hebben 5.1.2e , 5.1.2e , 5.1.2e , 5.1.2e 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 'MS365' d.d. 29/07/2024. Deze versie vormt de onderlegger voor deze toetsing.

Bij deze DPIA horen de volgende bijlagen:
- Verwerkersovereenkomst IRvN – Gemeente Nijmegen getekend.
- VNG Framework Juridisch.
- Informatiebeheerplan MS 365.
- DPIA Exchange Online 13/10/20.
- Oordeel DPIA Exchange Online 16/10/20.
- Integriteits- en geheimhoudingsverklaring MS365

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, ten dele.	Ja. Akkoord. Er is een DPIA voor de overgang naar Exchange Online uitgevoerd. Naar aanleiding van deze DPIA zijn verschillende landelijk geadviseerde maatregelen genomen. Zie hiervoor de bijlagen (DPIA en Oordeel).
2. Is het ethisch / politiek bestuurlijk verantwoord?	Ja. De gemeente Nijmegen wil MS365 gaan gebruiken om de samenwerking binnen de organisatie te verbeteren, maar ook meteen zorgen voor informatiehuishouding die hierbij passend is, die veilig is en voldoet aan wet- en regelgeving.	Akkoord.
3. Juridische toets 3a. Doel / grondslag	3.a. *Doel* van deze gegevensverwerkingen: Het doel van MS365 is het bevorderen van samenwerken en niet zozeer het verwerken van persoonsgegevens. Het is echter niet uit te sluiten dat in sommige vormen van overleg persoonsgegevens worden vastgelegd. *Grondslag* • Het samenwerken binnen een digitale omgeving is gebaseerd op de grondslag gerechtvaardigd belang. • Wanneer een verwerking valt onder een specifieke gemeentelijke taak is er sprake van de grondslag algemeen belang, namelijk wanneer de verwerking noodzakelijk is om de publieke taak uit te voeren.	3.a. *Doel:* Akkoord. *Grondslag* Akkoord.
3.b. Persoonsgegevens Worden bijzondere persoonsgegevens verwerkt?	3.b. Nee. Het uitgangspunt is dat er geen bijzondere persoonsgegevens verwerkt zullen worden.	3.b. Akkoord.
3.c. Proportionaliteit	3.c. Hoewel verwerking van persoonsgegevens niet uit te sluiten is, zullen bij de gekozen doelen van samenwerking (beleid, projecten, overleg, kennisdeling) relatief weinig persoonsgegevens verwerkt worden. Een onvermijdelijke vorm van verwerking zijn de contactpersonen gegevens. Uitgangspunt 1 is dat de taken waarbij de meeste (bijzondere/gevoelige) persoonsgegevens worden verwerkt in een taak specifieke applicatie zullen worden verricht, niet in MS365. Uitgangspunt 2. Wanneer een Team(sites) persoonsgegevens bevatten, dient deze besloten gemaakt te worden en alleen medewerkers toegang te hebben die vanuit hun functie noodzakelijk bij deze gegevens moeten kunnen (volgt uit het informatiebeheerplan).	3.c. Akkoord. Er zullen verschillende vormen van vastlegging voor kunnen komen – denk hierbij aan e-mails, afspraken, acties, notities, documenten, videogesprekken, chats etc. Hierin kunnen in potentie verschillende vormen van persoonsgegevens worden vastgelegd. Belangrijk zijn beide genoemde inrichtingsprincipes (uitgangspunten). In de vraag naar naleving van deze DPIA zullen deze centraal staan: - lukt het de organisatie om waar sprake is van verwerking van (bijzondere) persoonsgegevens deze te doen plaats laten vinden in taak specifieke applicaties? - zijn teams waarin persoonsgegevens (anders dan de onvermijdelijke stamgegevens) worden verwerkt altijd 'besloten teams'.

3.d. Subsidiariteit	3.d . Zonder gebruik van MS365 is het gebruik van documentopslag op gemeenschappelijke netwerkschijven, met een zeer beperkte bescherming en geen mogelijkheid tot vernietiging. Met de invoering van MS365 en het invoeringstraject er omheen zal privacybescherming en archivering in ieder geval verbeterd worden.	3.d. Akkoord. Zonder gegevensverwerking in MS365 is de gegevensverwerking rond voorbereiden van beleid, projectuitvoering en overleg minder veilig en minder rechtmatig.
3.e. Persoonsgegevens buiten EER gebruikt?	3.e. In beperkte mate, met name om de performance van het MS365-platform te verbeteren.	3.e. Akkoord. Met Microsoft is de EU Boundary Act vastgesteld, die verwerking zoveel mogelijk binnen de grenzen van de EU laat plaatsvinden. Afspraken hierover zijn op Europees en rijksniveau gemaakt.
3.f. Andere partijen betrokken?	3.f. De volgende partijen zijn betrokken bij het functioneren van MS365: • ICT bedrijf Rijk van Nijmegen - verwerker • Microsoft - verwerker/verantwoordelijke • Microsoft is voor gemeente Nijmegen in principe verwerker. Zij verwerken echter ook diagnostische (persoons)gegevens om hun eigen dienstverlening te verbeteren. Voor dat deel zijn ze zelf verwerkingsverantwoordelijke. • Gemeente Nijmegen – verwerkingsverantwoordelijke • SplitVision – verwerker (archiveren)	3.f. Akkoord. De VNG heeft namens Nederlandse gemeente een Juridisch Framework met Microsoft afgesloten, dat dient als een verwerkersovereenkomst (zie bijlage). Verwerkersovereenkomst met de IRvN is bijgevoegd. Verwerkersovereenkomst met SplitVision moet nog bijgevoegd worden.
3.g. Hoe lang worden gegevens bewaard en termijn en wijze van vernietiging?	3.g. *Bewaartermijnen en Vernietiging:* Vernietiging van teams en sites verloopt volgens de in de DPIA onder 7.1. genoemde bewarings- en vernietigingstermijnen die per sitesjabloon zijn vastgelegd en daarmee per team of site (documentsets) worden uitgevoerd.	3.g. Akkoord. Zie ook bijgevoegd informatiebeheerplan voor MS365
3.h. Hoe worden gegevens beveiligd?	3.h. Toegankelijkheid en vertrouwelijkheid worden geregeld op het niveau van Team(sites), met name voor besloten Team(sites). Intern openbare Team(sites) bevatten intern openbare documenten en bestanden. Besloten Team(sites) bevatten (in principe) vertrouwelijke documenten en bestanden. Wanneer men een document vanuit een besloten Team(site) willen delen met iemand, dan dient deze lid gemaakt te worden van dit/deze Team(site). Een document of bestand in een intern openbaar Team(site) kan wel gedeeld worden buiten MS365 zonder dat deze persoon lid is van een Team(site).	3.h. Akkoord. De organisatie van beveiliging ligt voor het grootste (technische) deel bij het ICT-bedrijf Rijk van Nijmegen. Voor het organisatorische en technische deel ligt het toezicht bij de CISO en de security officers van Bureau Ontwikkeling I&A.
4. Risico's en voorgestelde maatregelen	Uitvoering van de maatregelen die zijn beschreven onder kop 8.2. van de DPIA	Akkoord. Mits mogelijke maatregelen worden uitgevoerd. Zie mn vragen bij proportionaliteit.

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 zelf kent een 'laag' (na uitvoering van alle genoemde maatregelen) tot 'middelhoog' (indien geen enkele maatregel uitgevoerd wordt) risico.

Hoewel verwerking van persoonsgegevens niet uit te sluiten is, zullen bij de gekozen doelen van samenwerking (beleid, projecten, overleg, kennisdeling) relatief weinig persoonsgegevens verwerkt worden.
Een onvermijdelijke vorm van verwerking zijn de contactpersonen gegevens.
Uitgangspunt 1 is dat de taken waarbij de meeste (bijzondere/gevoelige) persoonsgegevens worden verwerkt in een taak specifieke applicatie zullen worden verricht, niet in MS365.
Uitgangspunt 2. Wanneer een Team(sites) persoonsgegevens bevatten, dient deze besloten gemaakt te worden en alleen medewerkers toegang te hebben die vanuit hun functie noodzakelijk bij deze gegevens moeten kunnen (volgt uit het informatiebeheerplan).

De verwerkersovereenkomst met SplitVision moet nog bijgevoegd worden.

Eind 2024 zal deze DPIA op naleving getoetst worden.
Belangrijk hierbij is de uitvoering van beide genoemde inrichtingsprincipes (uitgangspunten).
In de vraag naar naleving van deze DPA zullen deze centraal staan:
- lukt het de organisatie om waar sprake is van verwerking van (bijzondere) persoonsgegevens deze te doen plaats laten vinden in taak specifieke applicaties?
- zijn teams waarin persoonsgegevens (anders dan de onvermijdelijke stamgegevens) worden verwerkt altijd 'besloten teams'.
Daarnaast wordt bekeken of alle maatregelen genomen zijn om de genoemde risico's te verkleinen. Hiervoor wordt de tabel 8.2. 'Benoem de maatregelen die nog noodzakelijk (en aanbevolen) zijn', als uitgangspunt gebruikt.
De nalevingsrapportage zal op bovenstaande invalshoeken gericht moeten zijn.

Ik adviseer hiermee positief en daarmee zijn de resterende risico's "aanvaardbaar".

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

PK/01/08/2024. DPIA 90.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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

DPIA Oordeel FG gemeente Nijmegen

DPIA: Cameratoezicht opvanglocatie Koudenhoek

Inleiding

Hierbij het oordeel van de FG Gemeente Nijmegen over de DPIA 'Cameratoezicht opvanglocatie Koudenhoek'. Gekozen is voor een systematische aanpak. Deze is terug te herleiden tot de oordeelsvorming van DPIA's in het algemeen. In deze wordt het 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, tezamen een aanvaardbaar risico vormen bij het gebruik van privacygevoelige gegevens.

In de periode juni – juli 2024 hebben 5.1.2e , 5.1.2e 5.1.2e en 5.1.2e 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 'Cameratoezicht opvanglocatie Koudenhoek' d.d. 29/07/2024. Deze versie vormt de onderlegger voor deze toetsing.

Bij deze DPIA horen de volgende bijlagen:

- Camera protocol gemeente Nijmegen TGO Koudenhoek
- Plattegrond camerabewaking TGO Koudenhoek v 1.17

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, voor de grotere, maar overigens vergelijkbare locatie 'Winkelsteeg' is eerder eenzelfde DPIA gemaakt voor het cameratoezicht.	Akkoord. Daarbij is een aantal aanbevelingen gegeven die voor de locatie Winkelsteeg zijn opgevolgd en die nu opgenomen zijn in deze nieuwe DPIA voor de locatie Koudenhoek.
2. Is het ethisch / politiek bestuurlijk verantwoord?	Ja. Voor de veiligheid van zowel medewerkers, vrijwilligers als bewoners op de opvanglocatie is 24-uurs cameratoezicht gewenst om zowel incidenten als ongewenst, agressief of strafbaar gedrag vroegtijdig te kunnen signaleren, en snel te kunnen acteren op incidenten, als achteraf het handelen van zowel medewerkers als bewoners te kunnen analyseren.	Akkoord. Daarnaast kunnen camerabeelden dienen als bewijslast mocht de politie na een incident over willen gaan op strafrechtelijk onderzoek.
3. Juridische toets 3.a. Doel / grondslag	3a. Doel en grondslag Het *doel* van de camera's is om veiligheid te garanderen voor medewerkers, vrijwilligers en bewoners. De camerabeelden dragen bij aan een veiligheidsgevoel voor de bewoners en helpen erbij om bij incidenten de juiste vervolgacties te kunnen nemen. De *grondslag* voor de verwerking zit hem in het gerechtvaardigd belang (artikel 6 lid 1 sub f AVG).	3a. Akkoord. Het college van burgemeester en wethouders van Nijmegen heeft op 16 april 2024 besloten om de TGO Koudenhoek in te zetten voor de crisisnoodopvang van 400 asielzoekers. Mocht er een incident zijn, dan dienen de camerabeelden als bewijs en is duidelijk wie bij het incident betrokken was. Bovendien bevorderen de camerabeelden het veiligheidsgevoel van de bewoners.
3.b. Persoonsgegevens Worden bijzondere persoonsgegevens verwerkt?	3.b. Ja, indirect. • Gegevens over levensbeschouwelijke overtuigingen: het komt voor dat mensen bidden in de algemene ruimte. Daar hangen camera's. Daaruit is een levensovertuiging af te leiden. • Mogelijk medische gegevens: er is een zorgplein. Via de camerabeelden kun je zien wie daar wacht voor een afspraak. Dat zijn beiden geen feitelijk gegevens, maar afgeleide gegevens op basis van interpretatie van beelden.	3.b. Akkoord. De beelden kunnen alleen (live) bekeken worden door de bewakers en de locatiebeheerder (via een VPN-verbinding op de telefoon). De beelden zijn verder voor niemand zichtbaar. Daarnaast kunnen de beelden achteraf uitgelezen worden in geval van incident. Zie ook Plattegrond Camerabewaking CNO Winkelsteeg.
3c. Proportionaliteit	3c. Er gebeuren regelmatig incidenten bij de opvang. De camera's helpen erbij om de veiligheid te garanderen. Ze hebben een preventieve werking; wanneer een ruzie dreigt te ontstaan kan er meteen ingegrepen worden en is duidelijk wie erbij betrokken zijn. De vluchtelingen in de opvang zijn zich er van bewust dat er camera's hangen, waardoor ze mogelijk minder snel escaleren.	3c. Akkoord. Deze beelden zijn terugkijkend te zien indien er een incident heeft plaatsgevonden en de beelden uitgezien worden door de locatiemanager en (mogelijk) door de politie.

3.d. Subsidiariteit	3.d. De camera's zijn alleen op het terrein gericht. Op de in- en uitgangen en niet daarbuiten. Daarnaast hangen er geen camera's in de sanitair- en slaapruimtes. Enkel in de algemene ruimtes, bij de in- en uitgang en buiten op het terrein.	3.d. Akkoord Live-opnames op monitors worden uitsluitend op een later tijdstip bekeken in een geval van een incident (beelden worden dan bewaard op een met wachtwoord beveiligde USB-stick).
3.e. Persoonsgegevens buiten EER gebruikt?	3.e. Neen.	3.e. Akkoord
3.f. Andere partijen betrokken?	3.f. Gemeente Nijmegen is verantwoordelijke. ISeeYou is geen verwerker, want de beelden draaien in de cameratorens zelf.	3.f. Akkoord. Kwetsbaar is het als de beelden over gezet zijn op de USB-stick. Deze dient versleuteld te zijn. Van belang is dat de gegevens op de USB-stick na gebruik weer vernietigd worden en deze niet gaat rondzwerven.
3.g. Hoe lang worden gegevens bewaard en wijze van vernietiging?	3.g. De beelden worden alleen lokaal offline bewaard en worden na 17 dagen automatisch overschreven. Deze beelden zijn dan definitief gewist. In geval van een incident worden de veiliggestelde beelden, indien opgevraagd of gevorderd, overgedragen aan de politie of hiertoe kortstondig bewaard, maximaal 14 dagen. Daartoe wordt gewerkt met een versleutelde USB-stick, die met een wachtwoord beveiligd is.	Akkoord. De beelden worden alleen gemaakt in het kader van veiligheid op de locatie. De beelden worden niet zomaar teruggekeken, ze kunnen alleen teruggekeken worden door de operationeel coördinator, de locatiemanager en het hoofd van de beveiliging. De beelden worden alleen lokaal offline bewaard en na maximaal 14 dagen overschreven.
3.h. Hoe worden gegevens beveiligd?	3.h. De opnames worden niet online bewaard maar analoog in de camera masten zelf. De beelden zijn alleen beschikbaar door deze door middel van een USB-stick over te zetten. De operationeel coördinator en locatiemanager zijn bevoegd om de beelden te bekijken. Er is altijd een operationeel coördinator op het terrein aanwezig. Dit geldt niet voor de locatiemanager. De locatiemanager kan de beelden enkel bekijken via een beveiligde VPN-verbinding via ISeeYou.	Akkoord. Er wordt gewerkt met een beveiligde USB-stick, die met een wachtwoord beveiligd is.
4. Risico's en voorgestelde maatregelen	Deze zijn afdoende beschreven.	Akkoord. Er is een cameraprotocol opgezet waarin staat hoe medewerkers om moeten gaan met de camerabeelden. Zie de bijlage.

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 zelf kent een "middelhoog" risico.

Kwetsbaar is het als de beelden over gezet zijn op de USB-stick. Van belang is dat de gegevens op de USB-stick na gebruik weer vernietigd worden en deze niet gaat rondzwerven. Dringend advies: zorg bij gebruik voor het vier ogen principe. Leg vast waarom, wanneer en door wie de beelden zijn bekeken (loggen van deze handelingen). Leg vast dat de beelden na gebruik worden vernietigd (4 ogen) en door wie. Gebruik alleen de versleutelde USB-stick. Daarmee wordt de toegang tot de USB-stick beveiligd.

De maatregelen die verder worden beschreven, zijn m.i. afdoende.

Eind 2024 zal deze DPIA op naleving getoetst worden.

- Daar wordt gelet op het omgaan met beelden op USB-sticks

Ik adviseer hiermee positief en daarmee zijn de resterende risico's "aanvaardbaar.

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

PK/05/08/2024. DPIA 91.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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

DPIA Oordeel FG gemeente Nijmegen

DPIA: Gebruik applicatie City Control Wpg werkzaamheden

Inleiding

Hierbij het oordeel van de FG Gemeente Nijmegen over de DPIA 'Applicatie City Control Wpg werkzaamheden'. Gekozen is voor een systematische aanpak. Deze is terug te herleiden tot de oordeelsvorming van DPIA's in het algemeen. In deze wordt het 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, tezamen een aanvaardbaar risico vormen bij het gebruik van privacygevoelige gegevens.

In de periode jan – sept 2024 hebben 5.1.2e , 5.1.2e en 5.1.2e 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 'Applicatie City Control Wpg werkzaamheden d.d. 05/09/2024. Deze versie vormt de onderlegger voor deze toetsing.

Bij deze DPIA hoort de volgende bijlage:

- Verwerkersovereenkomst Sigmax – Citycontrol Handhaving

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?	Neen. NB. Deze DPIA betreft de werkzaamheden van de boa's die vallen onder de Wpg. Aanvullend zal er nog een DPIA worden gemaakt voor de toezichthoudende taken, die vallen onder de AVG.	Akkoord. De aanvullende DPIA voor de toezichthoudende taken dient uiterlijk in Q4 2024 gemaakt te worden.
2. Is het ethisch / politiek bestuurlijk verantwoord?	Ja. Bij het handhaven in de Openbare Ruimte is het noodzakelijk om de persoonsgegevens gegevens te verwerken, om daadwerkelijk een bekeuring uit te kunnen schrijven. Bovendien is het nodig om deze gegevens vast te leggen, in dit geval in de applicatie 'City Control'.	Akkoord.
3. Juridische toets 3.a. Doel / grondslag	3a. Doel en grondslag Het *doel:* Met deze verwerking wordt bijgedragen aan het principe schoon, heel en veilig. Hierbij draagt de gemeente zorg om de veiligheid en leefbaarheid te waarborgen. De *grondslag* voor de verwerking: Op basis van artikel 142 lid 1 Wetboek van Strafrecht (hierna: Sr) zijn onze boa's belast met de opsporing van strafbare feiten. In artikel 142 lid 2 Sr staat aangeduid voor welke domeinen de boa's kunnen worden aangesteld. In dit geval werken alleen domein 1 aangewezen boa's en zijn deze voor een aantal strafbare feiten belast met de opsporing.	3a. Akkoord. Voor deze DPIA richten we ons specifiek op de werkzaamheden die worden uitgevoerd in de rol van boa. Deze taken worden uitgevoerd in de openbare ruimte. Denk aan het handhaven van de leefbaarheid en openbare orde. Specifiek zijn in de Regeling domeinenlijsten buitengewoon opsporingsambtenaar de strafbare feiten opgenomen waarop de domein 1 boa's kunnen handhaven en zo nodig een bekeuring kunnen uitschrijven. Om deze bekeuring administratief te kunnen verwerken wordt gebruik gemaakt van de applicatie City Control van de ontwikkelaar Sigmax.
3.b. Persoonsgegevens Worden bijzondere persoonsgegevens verwerkt?	3.b. Neen, in principe niet. De volgende gegevens worden vastgelegd: - Naam - Geboortedatum - Burgerservicenummer (BSN) - Adres - Kenteken van eventueel bij het strafbaar feit betrokken voertuig	3.b. Akkoord.
3c. Proportionaliteit	3c. De inbreuk is te verantwoorden, doordat de boa's een wettelijke taak hebben en belast zijn met de opsporing van strafbare feiten. Om de inbreuk te beperken worden alleen relevante Wpg-gegevens vastgelegd wanneer er een strafbaar feit wordt begaan, waarvoor de boa's bevoegd en aangewezen voor zijn.	3c. Akkoord.
3.d. Subsidiariteit	3.d. Op dit moment is City Control een van de meest gebruikte en betrouwbare applicaties, die door handhavingsteams gebruikt wordt. Andere manieren, zoals handmatige verwerkingen, zijn risicovoller.	3.d. Akkoord.

3.e. Persoonsgegevens buiten EER gebruikt?	3.e. Neen.	3.e. Akkoord
3.f. Andere partijen betrokken?	3.f. Verwerkingsverantwoordelijke: Gemeente Nijmegen • Subverwerkers: o Sigmax ICT Specialisten B.V., dit is een zusteronderneming van Verwerker. Van Sigmax ICT Specialisten wordt de hosting afgenomen. o Sigmax MobileSolutionsB.V., dit is een zusteronderneming van Verwerker. Van Sigmax Mobile SolutionsB.V. wordt de support afgenomen. Verwerker: Sigmax Law Enforcement B.V. is verantwoordelijk dat de applicatie voldoet aan geldende wet- en regelgeving en naar behoren werkt	3.f. Akkoord. De verwerkersovereenkomst met Sigmax is als bijlage bij deze DPIA toegevoegd.
3.g. Hoe lang worden gegevens bewaard en wijze van vernietiging?	3.g. Politiegegevens in City Control worden afhankelijk van de leeftijd van de bijbehorende registratie achter een bijbehorend schot geplaatst. De schotten zijn één, vijf en tien jaar. Na tien jaar wordt de registratie met politiegegevens automatisch geanonimiseerd / vernietigd (verwijderen is niet mogelijk). Wanneer een betrokkene zich succesvol beroept op recht van vergetelheid / vernietiging, kan de individuele registratie ad hoc geanonimiseerd worden. Dit is op basis van art. 14 Wpg.	Akkoord. De gegevens worden geautomatiseerd verwijderd. Periodiek (minimaal 1 keer per jaar) wordt door de beheerder (een boa die daartoe de rechten heeft in de applicatie), samen met een bevoegd persoon die geen taak heeft in het proces gecontroleerd of deze gegevens daadwerkelijk worden verwijderd.
3.h. Hoe worden gegevens beveiligd?	3.h. 1. De gegevens zijn onderhevig aan de bewaartermijn; 2. Minimaal 1 keer per jaar wordt een audit uitgevoerd op de logfiles en autorisatiematrix; 3. Jaarlijkse controle op de Compliancy van de leverancier; 4. Kennis en kunde wordt jaarlijks afgetoetst voor de Boa's;	Akkoord. Er is 1 beheerder (boa) die rechten heeft om zaken aan te passen.
4. Risico's en voorgestelde maatregelen	Deze zijn afdoende beschreven.	Akkoord.

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 zelf kent een 'laag' risico.

De maatregelen die verder worden beschreven, zijn m.i. afdoende.

De aanvullende DPIA voor de toezichthoudende taken dient uiterlijk in Q4 2024 gemaakt te worden.

Eind 2024 zal deze DPIA op naleving getoetst worden.
Daarbij wordt getoetst of de in de DPIA opgenomen maatregelen ook daadwerkelijk worden uitgevoerd.

Ik adviseer hiermee positief en daarmee zijn de resterende risico's "aanvaardbaar.

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

PK/19/09/2024. DPIA 92.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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

DPIA Oordeel FG gemeente Nijmegen

DPIA: Uitwisseling gegevens bedrijfsartsen

Inleiding

Hierbij het oordeel van de FG Gemeente Nijmegen over de DPIA 'Uitwisseling gegevens bedrijfsartsen'.
Gekozen is voor een systematische aanpak. Deze is terug te herleiden tot de oordeelsvorming van DPIA's in het algemeen. In deze wordt het 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 welke weergeeft of m.i. het gehele voorstel van maatregelen én te nemen maatregelen bij geconstateerde risico's, tezamen een aanvaardbaar risico vormen bij het gebruik van privacygevoelige gegevens.

In de periode jan – sept 2024 hebben 5.1.2e , 5.1.2e , 5.1.2e en 5.1.2e 5.1.2e 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 'Uitwisseling gegevens bedrijfsartsen' d.d. 24/09/2024.
Deze versie vormt de onderlegger voor deze toetsing.

Bij deze DPIA horen de volgende bijlagen:

- Raamovereenkomst Bedrijfsarts-arboarts Nijmegen LEV arbo
- Overeenkomst Gemeente Nijmegen – Lev Arbo B.V. inzake Verantwoordelijkheid onder de AVG

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?	Neen.	Akkoord. Er is wel een DPIA gemaakt over het proces van het verwerken van personeelsinformatie. In deze DPIA wordt verwezen naar dat proces en de bijbehorende systemen.
2. Is het ethisch / politiek bestuurlijk verantwoord?	Ja. De gemeente Nijmegen heeft als werkgever de wettelijke plicht haar medewerkers te ondersteunen bij re-integratie bij ziekte of preventief om uitval te voorkomen. Hiervoor kan het nodig zijn om een afspraak te maken met een bedrijfsarts.	Akkoord. Om afspraken te kunnen maken tussen bedrijfszorgverleners van arbodienst Lev Arbo en medewerkers moeten er gegevens worden uitgewisseld met Lev Arbo.
3. Juridische toets 3.a. Doel / grondslag	3a. Doel en grondslag Het *doel:* Doel is aanmelden van medewerkers zodat afspraak voor het spreekuur met de bedrijfsarts gemaakt kan worden. De *grondslag* voor de verwerking: De gemeente Nijmegen heeft als werkgever de wettelijke plicht haar medewerkers te ondersteunen bij re-integratie bij ziekte of preventief om uitval te voorkomen. Deze wettelijke plicht is neergelegd in de Arbeidsomstandighedenwet en de Wet verbetering Poortwachter. Op het verbod op het verwerken van bijzondere persoonsgegevens is in dit geval de uitzonderingsgrond van art. 9, tweede lid, onder b AVG van toepassing. Op grond van die bepaling mogen gegevens over gezondheid worden verwerkt voor zover noodzakelijk met het oog op de uitvoering van verplichtingen op het gebied van het arbeidsrecht, voor zover toegestaan bij nationaal recht.	3a. Akkoord. De nieuwe bedrijfsartsen werken met het verzuimsysteem planningsagenda.nl. Omdat een koppeling met Youforce technisch nog niet mogelijk is, vindt de gegevensuitwisseling op een andere manier plaats. Dit gebeurt door het invoeren van deze gegevens door de arbo consulent van de gemeente Nijmegen in planningsagenda.nl. Deze DPIA ziet op deze uitwisseling van gegevens. Art. 30, eerste lid, onder b, Uitvoeringswet AVG bepaalt vervolgens dat gegevens over gezondheid verwerkt mogen worden door (o.a.) werkgevers, voor zover noodzakelijk voor de re-integratie of begeleiding van werknemers in verband met ziekte of arbeidsongeschiktheid met Lev Arbo.
3.b. Persoonsgegevens Worden bijzondere persoonsgegevens verwerkt?	3.b. Neen, in principe niet. Het betreft de volgende persoonsgegevens: naam medewerker, geboortedatum, adres, mailadres (zakelijk & privé), functie, 1e ziektedag, contactpersoon (leidinggevende van medewerker, de casemanager voor het verzuim) en werkpatroon. In sommige situaties kunnen de volgende aanvullende gegevens worden verwerkt: verpleegadres, telefoonnummer (zakelijk & privé), omvang contract, in/uit dienst datum, afdeling, organisatie, bedrijfsonderdeel, verzuimmelding & datum & verwachte duur van verzuim, herstelmelding & datum, HR medewerker.	3.b. Akkoord. Aan de gegevens die worden verstrekt, en aan het feit dat deze gegevens worden verstrekt aan een bedrijfsarts, kan worden afgeleid dat een medewerker verzuimt, en dat er (mogelijk) iets aan de hand is met de gezondheid van de medewerker. In zoverre betreft het hier wel gegevens over gezondheid, en dus bijzondere persoonsgegevens.

3c. Proportionaliteit	3c. Om een medewerker die verzuimt wegens ziekte de juiste begeleiding en advisering van een bedrijfsarts te kunnen geven, is het belangrijk dat de gegevens zoals naam, functie en 1e ziektedag worden verstrekt voor het maken van een afspraak voor het spreekuur. Doel van de verwerking van de gegevens is het maken van een afspraak voor het spreekuur.	3c. Akkoord. Er worden geen gegevens over de toestand/gezondheid van de werknemer uitgewisseld.
3.d. Subsidiariteit	3.d. Omdat een koppeling met Youforce technisch nog niet mogelijk is, vindt de gegevensuitwisseling op een andere manier plaats.	3.d. Akkoord. Dit gebeurt door het invoeren van deze gegevens door de arbo consulent van de gemeente Nijmegen in planningsagenda.nl.
3.e. Persoonsgegevens buiten EER gebruikt?	3.e. Neen.	3.e. Akkoord
3.f. Andere partijen betrokken?	3.f. De gemeente Nijmegen is verwerkingsverantwoordelijke voor de verstrekking van de gegevens. Als werkgever moet de gemeente persoonsgegevens van haar werknemers bijhouden. De gemeente is verantwoordelijk voor de verwerking van deze gegevens. LEV Arbo is eveneens verwerkingsverantwoordelijke. Zij verwerkt de gegevens voor eigen doeleinden (het verlenen van bedrijfszorg) en bepaalt de middelen van de verwerking (planningsagenda.nl).	3.f. Akkoord. Er is dus sprake van een uitwisseling van persoonsgegevens tussen twee verwerkingsverantwoordelijken. Tussen de gemeente Nijmegen en LEV Arbo is een overeenkomst inzake verantwoordelijkheid onder de AVG getekend. Deze zit als bijlage bij deze DPIA. NB. Deze wordt na vaststelling van deze DPIA ondertekend en maakt integraal onderdeel uit van deze DPIA.
3.g. Hoe lang worden gegevens bewaard en wijze van vernietiging?	3.g. De bedrijfsarts heeft de wettelijke plicht om medische dossiers te bewaren, dit mag maximaal 15 jaar, tenzij er sprake is van een beroepsziekte, dan is de termijn langer. Ook als het verzuim beëindigd is, kan het nodig zijn dat de bedrijfsarts op basis van de NAW-gegevens de identiteit van de medewerker moet kunnen controleren. De bedrijfsarts is verantwoordelijk voor de vernietiging van de medische gegevens.	Akkoord. De NAW-gegevens zijn gekoppeld aan het medisch dossier en kunnen niet zonder meer verwijderd worden zodra het verzuim is beëindigd. Na de samenwerking tussen gemeente Nijmegen en LEV Arbo, worden alle medewerkers op inactief gezet door LEV arbo en zijn de gegevens niet meer toegankelijk voor LEV arbo.
3.h. Hoe worden gegevens beveiligd?	3.h. Planningsagenda is gecertificeerd conform ISO 27001 en NEN7510. Dit betekent inloggen met authenticatie, en autorisaties op basis van rollen. De arbo consulent is geautoriseerd om de persoonsgegevens in te voeren. Daarnaast heeft een collega dezelfde bevoegdheid in verband met vervanging van de werkzaamheden tijdens vakantie.	Akkoord. De toegang vindt plaats door middel van een wachtwoord en 2FA. Geadviseerd wordt eens per jaar de autorisatie van de arbo consulent en vervanger te checken op geldigheid in geval van wisseling van deze personele bezetting.
4. Risico's en voorgestelde maatregelen	Deze zijn afdoende beschreven.	Akkoord.

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 zelf kent een 'laag' risico.

De maatregelen die verder worden beschreven, zijn m.i. afdoende.

Tussen de gemeente Nijmegen en LEV Arbo is een overeenkomst inzake verantwoordelijkheid onder de AVG getekend. Deze zit als bijlage bij deze DPIA.
Actie: Deze wordt na vaststelling van deze DPIA ondertekend en maakt integraal onderdeel uit van deze DPIA.

Geadviseerd wordt eens per jaar de autorisatie van de arbo consulent en vervanger te checken op geldigheid in geval van wisseling van deze personele bezetting.

Eind 2024 zal deze DPIA op naleving getoetst worden.
Daarbij wordt getoetst of de in de DPIA opgenomen maatregelen ook daadwerkelijk worden uitgevoerd.

Ik adviseer hiermee positief en daarmee zijn de resterende risico's "aanvaardbaar.

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

PK/30/09/2024. DPIA 93.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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

DPIA Oordeel FG gemeente Nijmegen

DPIA: Workflowsysteem Vergunningen in Proces (VIP)

Inleiding

Hierbij het oordeel van de FG Gemeente Nijmegen over de DPIA 'Workflowsysteem Vergunningen in Proces (VIP)'. Gekozen is voor een systematische aanpak. Deze is terug te herleiden tot de oordeelsvorming van DPIA's in het algemeen. In deze wordt het 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 welke weergeeft of m.i. het gehele voorstel van maatregelen én te nemen maatregelen bij geconstateerde risico's, tezamen een aanvaardbaar risico vormen bij het gebruik van privacygevoelige gegevens.

In de periode jun – okt 2024 hebben 5.1.2e , 5.1.2e , 5.1.2e , 5.1.2e 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 'Workflowsysteem Vergunningen in Proces (VIP)' d.d. 02/10/2024.
Deze versie vormt de onderlegger voor deze toetsing.

Bij deze DPIA horen de volgende bijlagen:

- Verwerkersovereenkomst met Woweb is in ontwikkeling.

Het is zaak deze zo spoedig mogelijk vast te stellen (zie eindoordeel).

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?	Neen.	Akkoord.
2. Is het ethisch / politiek bestuurlijk verantwoord?	Ja. Vergunningverlening is een wettelijke taak van de gemeente. Het betreft het registreren van meldingen en beoordelen van vergunningsaanvragen. Het gaat dan onder meer om alcohol-, evenementen-, exploitatie-, marktplaats- en standplaatsvergunning.	Akkoord. Dit betreft activiteiten waarvoor bewoners en ondernemers toestemming nodig hebben van de gemeente, of die in ieder geval moeten worden gemeld. Toestemming wordt verleend middels een vergunning.
3. Juridische toets 3.a. Doel / grondslag	3a. Doel en grondslag Het *doel:* Het doel is een efficiënte en nauwkeurige beoordeling van een vergunningsaanvraag. De *grondslagen* vloeien voort uit diverse wettelijke taken, waaronder: • Algemene plaatselijke verordening gemeente Nijmegen • Alcoholwet • Verordening Winkeltijden Nijmegen 2016 (Rectificatie) • Marktverordening Nijmegen 2020 • Wet op de kansspelen • Besluit brandveilig gebruik en basishulpverlening overige plaatsen.	3a. Akkoord. Om het proces van een vergunningsaanvraag tot verlening (incl. eventuele handhaving op overtredingen) te borgen, gebruikgemaakt van het workflow systeem VIP. Deze DPIA is gericht op verwerking van persoonsgegevens in VIP (Vergunningen in Proces).
3.b. Persoonsgegevens Worden bijzondere persoonsgegevens verwerkt?	3.b. Nee, er worden geen bijzondere persoonsgegevens opgeslagen in VIP zelf. Binnen VIP worden de volgende persoonsgegevens verwerkt: • NAW-gegevens aanvrager • Burgerservicenummer (BSN) aanvrager • Naam en contactgegevens contactpersoon (adres, telefoonnummer en/of e-mailadres).	3.b. Akkoord. Daarnaast zijn er verschillende documenten die raadpleegbaar zijn via VIP die persoonsgegevens kunnen bevatten.
3c. Proportionaliteit	3c. Doordat de vergunningsaanvraag binnen VIP wordt doorlopen, wordt het werken in losse mappen, documenten en mailboxen tot een minimum beperkt. Er wordt doorlopend gekeken naar welke informatie benodigd is voor een vergunningsaanvraag (dataminimalisatie).	3c. Akkoord. Een vergunningsaanvraag kan door VIP efficiënter en nauwkeuriger worden beoordeeld, wat een voordeel oplevert voor aanvragers.
3.d. Subsidiariteit	3.d. Voor de ontwikkeling van VIP werd gewerkt in het systeem WRS. Daarnaast werd veel gewerkt in losse mappen, documenten en mailboxen. Omdat deze werkwijze op vele fronten kwetsbaar was, is ervoor gekozen om een nieuw workflow systeem te ontwikkelen.	3.d. Akkoord. Er worden enkel documenten en (persoons) gegevens bij aanvrager uitgevraagd die nodig zijn voor de behandeling van de desbetreffende vergunningsaanvraag. Hiervoor is een

	De werkprocessen zijn ingedeeld in een vaste structuur, waardoor er beter overzicht is en een makkelijke overdracht plaats kan vinden tussen collega's. Een vergunningsaanvraag kan hierdoor efficiënter en nauwkeuriger worden beoordeeld.	gestandaardiseerd en geautomatiseerd webformulier ontwikkeld per type vergunning. NB. Er is een koppeling met de BAG om adressen te valideren. Er is een koppeling met de BRP om BSN te valideren.
3.e. Persoonsgegevens buiten EER gebruikt?	3.e. Neen.	3.e. Akkoord
3.f. Andere partijen betrokken?	3.f. De gemeente Nijmegen is verwerkingsverantwoordelijke voor de verstrekking van de gegevens. Woweb is als leverancier van de applicatie verwerker.	3.f. Akkoord. NB. De verwerkersovereenkomst met Woweb moet nog afgesloten worden. Dat dient z.s.m. te geschieden. Deze maakt integraal onderdeel uit van deze DPIA.
3.g. Hoe lang worden gegevens bewaard en wijze van vernietiging?	3.g. Voor verleende/geweigerde vergunningen geldt doorgaans een bewaartermijn van 5 jaar, al kan dit verschillen per type vergunning. BDI is verantwoordelijk voor de vernietiging van gegevens in Corsa. De manager bureau Veilige & Weerbare stad is verantwoordelijk voor de vernietiging van gegevens in VIP.	Akkoord. Daarnaast worden enkele gegevens opgeslagen in Open Zaak (database van VIP). De bedoeling is om hiervoor op korte termijn een vernietigingsprotocol op te stellen, waarbij gegevens geautomatiseerd worden vernietigd conform de termijnen die het BDI aanhoudt.
3.h. Hoe worden gegevens beveiligd?	3.h. Het belangrijkste gegeven dat herleidbaar is, is het bsn. Deze wordt versleuteld opgeslagen in Open Zaak (database van VIP). Enkel de applicatie VIP heeft de "sleutel" om het bsn in te zien.	Akkoord. Er wordt in VIP gewerkt met verschillende autorisatieniveaus. Er zijn meerdere rollen binnen VIP: inzien, vergunningverlener, manager. Voor de module handhaving zijn er aparte autorisaties. Vergunningverleners kunnen enkel dát-informatie inzien. Halfjaarlijks wordt toezicht gehouden op de autorisaties. De functioneel beheer kent autorisaties toe met toestemming van de key-users.
4. Risico's en voorgestelde maatregelen	Deze zijn afdoende beschreven.	Akkoord. Er wordt binnen VIP gewerkt met autorisaties. Het autorisatieproces is (nog) niet geautomatiseerd.

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 zelf kent een 'laag' risico.

De maatregelen die verder worden beschreven, zijn m.i. afdoende.

Aanbevelingen:

- De verwerkersovereenkomst met Woweb is in ontwikkeling. Het is zaak deze zo spoedig mogelijk vast te stellen.
- Enkele gegevens worden opgeslagen in Open Zaak (database van VIP). De bedoeling is om hiervoor op korte termijn een vernietigingsprotocol op te stellen, waarbij gegevens geautomatiseerd worden vernietigd conform de termijnen die het BDI aanhoudt.
- Er wordt binnen VIP gewerkt met autorisaties. Het autorisatieproces is niet geautomatiseerd. Dit dient nog gerealiseerd te worden.

Eind 2025 zal deze DPIA op naleving getoetst worden.
Daarbij wordt getoetst of de in de DPIA opgenomen maatregelen ook daadwerkelijk worden uitgevoerd en de beide aanbevelingen uitgevoerd zijn.

Ik adviseer hiermee positief en daarmee zijn de resterende risico's "aanvaardbaar.

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

PK/31/10/2024. DPIA 94.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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

DPIA Oordeel FG gemeente Nijmegen

DPIA: Afhandelen bezwaar, beroep & klachten

Inleiding

Hierbij het oordeel van de FG Gemeente Nijmegen over de DPIA 'Afhandelen bezwaar, beroep & klachten'.
Gekozen is voor een systematische aanpak. Deze is terug te herleiden tot de oordeelsvorming van DPIA's in het algemeen. In deze wordt het 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 welke weergeeft of m.i. het gehele voorstel van maatregelen én te nemen maatregelen bij geconstateerde risico's, tezamen een aanvaardbaar risico vormen bij het gebruik van privacygevoelige gegevens.

In de periode jun tot nov 2024 hebben 5.1.2e, 5.1.2e, 5.1.2e, 5.1.2e, 5.1.2e, 5.1.2e 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 'Afhandelen bezwaar, beroep & klachten' d.d. 12/11/2024.
Deze versie vormt de onderlegger voor deze toetsing.

Bij deze DPIA hoort de volgende bijlage:

- Verwerkersovereenkomst met Woweb.

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?	Neen.	Akkoord.
2. Is het ethisch / politiek bestuurlijk verantwoord?	Ja. Het afhandelen van klachten, bezwaar en beroep is een wettelijke plicht voor de gemeente. Het betreft het recht van belanghebbende(n) op een volledige heroverweging in het streven naar rechtvaardige en proportionele besluitvorming en acceptatie van het genomen besluit. Hierdoor kunnen mogelijk fout genomen primaire besluiten hersteld worden. Wanneer er geen besluit genomen is, maar een inwoner zich wel oneerlijk behandeld voelt, dan kunnen zij via een klachtenprocedure hun onenigheid uiten.	Akkoord. NB: De scope van deze DPIA ziet op het proces vanaf de heroverweging van het primaire besluit, en dus niet op het primaire besluit zelf. Voor die processen dient, als het gaat om een hoog risicoverwerking, een zelfstandige DPIA afgesloten te worden. Dat betekent ook dat bijvoorbeeld de opslag in Corsa, voor zover het gaat om de stukken vanuit het primair besluit, niet binnen de scope van deze DPIA vallen. Ook de proportionaliteit en subsidiariteit van de primaire processen, valt hierbuiten.
3. Juridische toets 3.a. Doel / grondslag	3a. Doel en grondslag Het *doel:* Een volledige heroverweging van het primaire besluit, zodat de inwoner een zo rechtmatig mogelijk genomen besluit krijgt. De *grondslagen* Grondslag komt uit de Algemene wet bestuursrecht Awb. - Bij bezwaar: H6&7 - Bij beroep: H6&7 - Bij klachten: art. 9.1 Awb en verder	3a. Akkoord.
3.b. Persoonsgegevens Worden bijzondere persoonsgegevens verwerkt?	3.b. Nee, er worden (in principe) geen bijzondere persoonsgegevens verwerkt. Dit geldt voor klachten, bezwaar en beroep. In JZ4All: - voor- en achternamen, - bsn - telefoonnummer, - contactgegevens, - adresgegevens en - gegevens gemachtigde - afdeling primair besluit - onderwerp procedure - zaakhouder (medewerker JZ) De enige mogelijke bijzondere persoonsgegevens in JZ4All, vallen te halen uit het onderwerp van de procedure (bv. gehandicaptenparkeerkaart).	3.b. Akkoord. NB. In Corsa: de achterliggende stukken zelf, zoals: o primair besluit o onderbouwing bij primair besluit o het bezwaar/het beroep/de klacht of stukken die daarmee samenhangen, zoals bv. een uitnodiging voor een hoorzitting o de uitspraak Hier kán sprake zijn van bijzondere persoonsgegevens, die zijn dan ín het primaire proces verwerkt. Bovendien kunnen het ook méér stukken zijn dan bij de primaire aanvraag, als de jurist van mening is dat het besluit in primo nog onvoldoende gemotiveerd is.

3c. Proportionaliteit	3c. Om een klacht serieus te kunnen behandelen is het van belang op de hoogte te zijn van de context. Daarom moeten achterliggende stukken meegenomen worden in de beslissing op de klacht. In bezwaar is een volledige heroverweging vereist, dus alle gegevens die bij de primaire aanvraag worden verzameld, zijn daar ook nodig. De specifieke proportionaliteit en subsidiariteit is dus verbonden aan het primaire proces.	3c. Akkoord. Wanneer het gaat om bijzondere persoonsgegevens, komen deze vrijwel altijd voort uit stukken om bepaalde aanvragen te motiveren. Het kan wel voorkomen dat de jurist van mening is dat bij het primaire proces onvoldoende gemotiveerd is. Het kan daarom gebeuren dat er in bezwaar soms meer stukken verwerkt worden dan bij het primaire besluit.
3.d. Subsidiariteit	3.d. Noodzakelijk voor volledige heroverweging. Dus minder informatie is niet mogelijk. Dit is weer gelinkt aan het primaire proces; wat daar gevraagd wordt is nodig voor het bezwaar.	3.d. Akkoord.
3.e. Persoonsgegevens buiten EER gebruikt?	3.e. Neen.	3.e. Akkoord
3.f. Andere partijen betrokken?	3.f. De gemeente Nijmegen is verwerkingsverantwoordelijke voor de verstrekking van de gegevens. Woweb is leverancier van de applicatie JZ4ALL. (Zelfstandig) Verantwoordelijk: rechtbank	3.f. Akkoord. De verwerkersovereenkomst met Woweb is als bijlage toegevoegd.
3.g. Hoe lang worden gegevens bewaard en wijze van vernietiging?	3.g. De gegevens worden 7 jaar bewaard, tenzij er een uitspraak is die leidt tot een aanzienlijke beleidswijziging, dan moet het voor altijd bewaard worden. Voor de achterliggende stukken geldt de bewaartermijn van het primaire proces. Vernietiging: Gemeente Nijmegen, bureau BDI, concernmanager VJB: bij de bezwaren zelf.	Akkoord. NB. Primaire stukken: bij betreffende afdeling.
3.h. Hoe worden gegevens beveiligd?	3.h. Juristen en administratie hebben de rechten. Voor het benaderen van de databases is een extra 2 factor authenticatie stap vereist. De belangrijkste gegevens zijn de BSN nummers. Deze worden opgeslagen in Open Zaak en encrypted in JZ4ALL. Dit betekent dat het bsn niet zichtbaar, maar versleuteld staat opgeslagen in de database van JZ4ALL. Het bsn is dus alleen zichtbaar in de applicatie.	Akkoord. Aanbevolen wordt om met een autorisatiematrix te werken en deze eens per jaar op te schonen.
4. Risico's en voorgestelde maatregelen	Deze zijn afdoende beschreven.	Akkoord.

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 zelf kent een 'laag' risico.

De maatregelen die verder worden beschreven, zijn m.i. afdoende.

Aanbevolen wordt om met een autorisatiematrix te werken en deze eens per jaar op te schonen.

Eind 2025 zal deze DPIA op naleving getoetst worden.
Daarbij wordt getoetst of de in de DPIA opgenomen maatregelen ook daadwerkelijk worden uitgevoerd en de beide aanbevelingen uitgevoerd zijn. Nadrukkelijk wordt gekeken naar de werking van de autorisatiematrix.

Ik adviseer hiermee positief en daarmee zijn de resterende risico's 'aanvaardbaar'.

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

PK/12/11/2024. DPIA 95.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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

DPIA Oordeel FG gemeente Nijmegen

DPIA: Gebruik applicatie City Control AVG werkzaamheden

Inleiding

Hierbij het oordeel van de FG Gemeente Nijmegen over de DPIA 'Applicatie City Control AVG werkzaamheden'. Gekozen is voor een systematische aanpak. Deze is terug te herleiden tot de oordeelsvorming van DPIA's in het algemeen. In deze wordt het 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, tezamen een aanvaardbaar risico vormen bij het gebruik van privacygevoelige gegevens.

In de periode jan – nov 2024 hebben 5.1.2e , 5.1.2e en 5.1.2e 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 'Applicatie City Control AVG werkzaamheden' d.d. 04/11/2024. Deze versie vormt de onderlegger voor deze toetsing.

Bij deze DPIA hoort de volgende bijlage:

- Verwerkersovereenkomst Sigmax – Citycontrol Handhaving

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. NB. Deze DPIA betreft de werkzaamheden van de boa's die vallen onder de AVG.	Akkoord. De aanvullende DPIA voor de toezichthoudende taken WPG is reeds ingediend en beoordeeld (DPIA 92).
2. Is het ethisch / politiek bestuurlijk verantwoord?	Ja. De gegevens die worden verwerkt voor het uitschrijven van een bestuursrechtelijke overtreding vallen onder de Algemene verordening gegevensbescherming (hierna; AVG) De verwerking vindt plaats om de volgende redenen; 1. Om de geldigheid van het identiteitsbewijs te controleren en 2. om de last of boete naar het juiste adres te kunnen sturen van de overtreder.	Akkoord. Deze DPIA richt zich op de werkzaamheden die worden uitgevoerd in rol als toezichthouder en níet als boa.
3. Juridische toets 3.a. Doel / grondslag	3a. Doel en grondslag Het *doel:* Met deze verwerking wordt bijgedragen aan het principe schoon, heel en veilig. Hierbij draagt de gemeente zorg om de veiligheid en leefbaarheid te waarborgen. De *grondslag* voor de verwerking: De toezichthouders zijn belast met het uitvoeren van toezicht op de volgende wetten en verordeningen: Omgevingswet, Algemene Plaatselijke Verordening, Afvalstoffen-verordening 2022, BRP, Parkeerverordening 2007, Wegsleepverordening 2014, Verordening Winkeltijden, Haven- en kaderverordening 2016, De Wet milieubeheer, De Wet op de kansspelen, De Waterwet en Experiment gesloten coffeeshopketen gemeente Nijmegen.	3a. Akkoord. Voor deze DPIA richten zich specifiek op de werkzaamheden die worden uitgevoerd in rol als toezichthouder. Deze taken worden uitgevoerd in de openbare ruimte, denk aan het handhaven van de leefbaarheid en openbare orde.
3.b. Persoonsgegevens Worden bijzondere persoonsgegevens verwerkt?	3.b. Neen, in principe niet. De volgende gegevens worden vastgelegd: - Naam - Geboortedatum - Burgerservicenummer (BSN) - Adres - Kenteken van eventueel bij het bestuurlijk feit betrokken voertuig	3.b. Akkoord.
3c. Proportionaliteit	3c. De inbreuk is te verantwoorden, doordat de toezichthouders een wettelijke taak hebben en belast zijn met het toezichthouden op de verordeningen en wetten. Om de inbreuk te beperken worden alleen relevante persoonsgegevens vastgelegd wanneer er een overtreding wordt begaan of dient ter verzameling van informatie vanwege een overlast situatie.	3c. Akkoord.

3.d. Subsidiariteit	3.d. De impact voor de burger wordt zoveel mogelijk beperkt door alleen de gegevens te noteren die nodig zijn om 1. Iemands identiteit te kunnen verifiëren en te zorgen dat deze naar het juiste adres kan worden gestuurd 2. De boete uit te kunnen schrijven met eventueel het juiste kenteken.	3.d. Akkoord.
3.e. Persoonsgegevens buiten EER gebruikt?	3.e. Neen.	3.e. Akkoord
3.f. Andere partijen betrokken?	3.f. *Verwerkingsverantwoordelijke*: Gemeente Nijmegen. *Verwerker:* Sigmax Law Enforcement B.V. is verantwoordelijk dat de applicatie CityControl voldoet aan geldende wet- en regelgeving en naar behoren werkt. Subverwerkers: O Sigmax ICT Specialisten B.V., dit is een zusteronderneming van Verwerker (hosting). O Sigmax Mobile Solutions B.V., dit is een zusteronderneming van Verwerker (support).	3.f. Akkoord. De verwerkersovereenkomst met Sigmax is als bijlage bij deze DPIA toegevoegd.
3.g. Hoe lang worden gegevens bewaard en wijze van vernietiging?	3.g. De gegevens in CityControl worden afhankelijk van de leeftijd van de bijbehorende registratie achter een bijbehorend schot geplaatst. De schotten zijn één, vijf en tien jaar. Na tien jaar wordt de registratie automatisch geanonimiseerd/vernietigd (verwijderen is niet mogelijk). Wanneer een betrokkene zich succesvol beroept op recht van vergetelheid/vernietiging, kan de individuele registratie ad hoc geanonimiseerd worden wanneer de uitvoerende gebruiker hier het juiste recht toe heeft. Indien er een daadwerkelijke boete wordt opgelegd worden de gegevens in een andere applicatie (Corsa) 7 jaar na het opleggen van de boete bewaard. Dit volgt uit de selectielijst archiefwet 2020.	Akkoord. De gegevens worden geautomatiseerd verwijderd. Periodiek (minimaal 1 keer per jaar) wordt door de beheerder (een boa / toezichthouder die daartoe de rechten heeft in de applicatie), samen met een bevoegd persoon die geen taak heeft in het proces gecontroleerd of deze gegevens daadwerkelijk worden verwijderd.
3.h. Hoe worden gegevens beveiligd?	3.h. 1. Minimaal 1 keer per jaar wordt een audit uitgevoerd op de logfiles en autorisatiematrix; 2. Jaarlijkse controle op de Compliancy van de leverancier; 3. Kennis en kunde wordt jaarlijks afgetoetst voor de Boa's;	Akkoord. Er is 1 beheerder die rechten heeft om zaken aan te passen.
4. Risico's en voorgestelde maatregelen	Deze zijn afdoende beschreven.	Akkoord.

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 zelf kent een 'laag' risico.

De maatregelen die verder worden beschreven, zijn m.i. afdoende.

Eind 2025 zal deze DPIA op naleving getoetst worden.
Daarbij wordt getoetst of de in de DPIA opgenomen maatregelen ook daadwerkelijk worden uitgevoerd.

Ik adviseer hiermee positief en daarmee zijn de resterende risico's "aanvaardbaar.

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

PK/05/11/2024. DPIA 96.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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

DPIA Oordeel FG gemeente Nijmegen

DPIA Collectiebeheersysteem Regionaal Archief Nijmegen (Atlantis)

Inleiding

Hierbij het oordeel van de FG Gemeente Nijmegen over de DPIA 'Collectiebeheersysteem Regionaal Archief Nijmegen' (Atlantis).
Gekozen is voor een systematische aanpak. Deze is terug te herleiden tot de oordeelsvorming van DPIA's in het algemeen. In deze wordt het 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 welke weergeeft of m.i. het gehele voorstel van maatregelen én te nemen maatregelen bij geconstateerde risico's, tezamen een aanvaardbaar risico vormen bij het gebruik van privacygevoelige gegevens.

In de periode aug tot okt 2024 hebben 5.1.2e ,5.1.2e ,5.1.2e ,5.1.2e ,5.1.2e 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 Collectiebeheersysteem Regionaal Archief Nijmegen d.d. 11/11/2024.
Deze versie vormt de onderlegger voor deze toetsing.

Bij deze DPIA hoort de volgende bijlage:

- Verwerkersovereenkomst Gem. Picturae ICT Bv (tegenwoordig Vitec Memorix)
- Verwerkersovereenkomst Gem. Nijmegen – DEVENTit
- Overdrachtseisen Digitaal Archief RAN
- Huisregels RAN 2024 - Bijlage 12 Beslisbomen openbaarheid
- DPIA RAN E-depotvoorziening

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. Er is voor de e-depotvoorziening een afzonderlijke DPIA opgesteld.	Akkoord. Deze DPIA richt zich alleen op het collectiebeheersysteem.
2. Is het ethisch / politiek bestuurlijk verantwoord?	Ja. Ja. De Archiefwet verplicht elke overheids-organisatie om haar informatie duurzaam toegankelijk te maken en te houden en te vernietigen wanneer de bewaartermijn is verlopen.	Akkoord. Het RAN is verantwoordelijk voor het opnemen, opslaan, conserveren/preserveren, beschikbaar stellen en presenteren van blijvend te bewaren documenten/informatie van de in de DPIA genoemde overheden en samenwerkingsverbanden.
3. Juridische toets 3.a. Doel / grondslag	3a. *Doel* van deze gegevensverwerkingen: Het doel van de beoogde bewerking is het beheren, ontsluiten en beschikbaar stellen van analoge én digitale archieven. *Grondslag* De verwerking (archivering) vindt plaats op grond van een wettelijke taak. Namelijk binnen de kaders van de Archiefwet 1995 (AW), het Archiefbesluit (AB) en de Archiefregeling (AR).	3a. Akkoord. Het RAN heeft de (wettelijke) taak om overgebrachte (overheids)archieven duurzaam toegankelijk te maken, te beheren en beschikbaar te stellen. Het collectiebeheersysteem is noodzakelijk om deze taak uit te kunnen voeren: In het collectiebeheersysteem worden metadata en (multimedia)bestanden uit en over archieven en collecties (zowel analoog als digitaal) beheerd en beschikbaar gesteld en het collectiebeheersysteem voorziet ook in de toegang tot deze archieven en collecties.
3.b. Persoonsgegevens Worden bijzondere persoonsgegevens verwerkt?	3.b. Ja. De volgende persoonsgegevens worden verwerkt: - NAW-gegevens, Bankgegevens, e-mailadressen, Burgerservicenummers - Bijzondere persoonsgegevens zoals bedoeld in artikel 9 AVG (persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid). - Gegevens over de financiële of economische situatie van de betrokkene, zoals schulden, salaris – en betalingsgegevens. - (Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene, zoals gegevens over gokverslaving, prestaties op school of werk of relatieproblemen. - Gegevens die kunnen worden misbruikt voor (identiteits)fraude, zoals biometrische gegevens en kopieën van identiteitsbewijzen. - Gegevens over kwetsbare groepen zoals minderjarigen, mensen die te maken hebben	3.b. Akkoord. Het collectiebeheersysteem bevat voornamelijk gegevens óver de archieven en de collecties die het RAN beheert. In deze metadata zijn weinig persoonsgegevens te vinden, maar ze zijn er wel. Van steeds meer archiefstukken zijn er daarnaast steeds vaker scans beschikbaar die in veel gevallen op basis van OCR indirect doorzoekbaar zijn. Daarmee worden ook op grotere schaal persoonsgegevens opgenomen in het collectiebeheersysteem. Bezoekers van de digitale studiezaal – de publiekskant van het collectiebeheersysteem – kunnen openbare gegevens digitaal inzien. Sommige stukken met niet-openbare gegevens kunnen via de digitale studiezaal worden aangevraagd voor raadpleging op locatie. Daarnaast wordt binnen het collectiebeheersysteem de volgende gegevens vastgelegd: · Gebruikersnamen · Persoonsnamen · Wachtwoorden · E-mailadressen

	met stalking of mensen die in een blijf-van-mijn-lijfhuis verblijven; - Gegevens van kinderen en mensen met een verstandelijke handicap.	· Werkgever (herleidbaar uit gebruikersnaam en mailadres
3c. Proportionaliteit	3c. Wanneer documenten (bijzondere) persoonsgegevens bevatten wordt steeds afgewogen en bepaald of en zo ja, op welke wijze deze documenten al dan niet openbaar worden gemaakt. Daarbij wordt gewerkt met beslisbomen voor het bepalen van openbaarheidsbeperkingen en de te hanteren termijnen alsook technische maatregelen die genomen kunnen worden m.b.t. beschikbaarstelling. Persoonsgegevens die in het collectiebeheersysteem worden vastgelegd voor het kunnen uitvoeren van opdrachten worden na 12 maanden geautomatiseerd geanonimiseerd.	3c. Akkoord. Deze beslisbomen zijn opgenomen binnen de huisregels van het RAN. Deze zijn opgenomen als bijlage van deze DPIA. De functioneel beheerder ziet daarop toe.
3.d. Subsidiariteit	3.d. Archief is volgend op bedrijfsvoering. Als er minder ingrijpende manieren zijn om het doel te bereiken heeft dat normaliter de voorkeur, bijvoorbeeld indien gepseudonimiseerde of geanonimiseerde gegevens voldoen. Archieven die niet openbare persoonsgegevens bevatten worden niet gepubliceerd. De digitale studiezaal (de website van het RAN waarop informatie over en uit archieven wordt gepubliceerd) bevat zodoende alleen persoonsgegevens voor zover dat volgens wet- en regelgeving is toegestaan.	3.d. Akkoord. Dit speelt bijvoorbeeld bij beleidsonderzoek. Daar gaat het immers niet om individuele casuïstiek, maar om een generiek beeld.
3.e. Persoonsgegevens buiten EER gebruikt?	3.e. Neen.	3.e. Akkoord
3.f. Andere partijen betrokken?	3.f. Tussen de volgende partijen worden gegevens uitgewisseld: • Vitec Memorix B.V. (voorheen Picturae ICT) • DEVENTit B.V. De rol van de leveranciers – Vitec Memorix B.V. (voorheen Picturae ICT B.V.) en DEVENTit B.V. – is die van gegevensverwerker. De gemeente Nijmegen is de verwerkingsverantwoordelijke.	3.f. Akkoord. Gemeente Nijmegen heeft met deze partijen verwerkingsovereenkomsten. Deze zijn als bijlagen opgenomen bij deze DPIA.
3.g. Hoe lang worden gegevens bewaard en wijze van vernietiging?	3.g. *Bewaartermijn* Eeuwigdurende / permanente / blijvende bewaring. De grondslag van deze bewaartermijn ligt binnen de Archiefwet, het	Akkoord. De “Selectielijst gemeentelijke en intergemeentelijke organen” vormt de basis voor het bewaren en vernietigen van

	Archiefbesluit en de “Selectielijst gemeentelijke en intergemeentelijke organen”. Het belang van de informatie bepaalt hoe lang de informatie bewaard moet worden. De Archiefwet zelf bevat geen bewaartermijnen. Deze worden per organisatie vastgelegd in selectielijsten. *Vernietiging:* Archiefinformatie in het collectiebeheersysteem wordt in principe niet vernietigd. In sommige gevallen blijkt dat archiefinformatie ten onrechte als blijvend te bewaren is geregistreerd. In die gevallen wordt, aan de hand van eerdergenoemde selectielijsten, met terugwerkende kracht vernietigd. Dit wordt uitgevoerd door medewerkers inventarisatie, waarbij goedkeuring wordt verleend door de gemeentearchivaris.	documenten bij gemeenten en intergemeentelijke organen. Deze selectielijst is opgesteld door de Vereniging Nederlandse Gemeenten (VNG). De meest recente selectielijst stamt uit 2020. De meeste documenten komen uiteindelijk in aanmerking voor vernietiging. Een relatief klein deel van de documenten worden in de selectielijst aangemerkt als blijvend te bewaren. Deze documenten moeten (in principe na twintig jaar) worden overgebracht naar een archiefbewaarplaats. Persoonsgegevens die in het collectiebeheersysteem worden vastgelegd voor het kunnen uitvoeren van opdrachten worden na 12 maanden geautomatiseerd geanonimiseerd.
3.h. Hoe worden gegevens beveiligd?	3.h. Naast medewerkers van leverancier DEVENTit hebben zo’n 90 mensen toegang tot het collectiebeheersysteem. Het gaat om medewerkers en vrijwilligers van het RAN en medewerkers van regiogemeenten en gemeenschappelijke regelingen. Via een systeem van autorisaties wordt een gebruiker toegang verleend tot (een deel van) het systeem. Daarbij worden verschillende mutatieniveaus toegekend (van alleen raadplegen tot systeembeheer). Autorisaties worden toegekend op basis van noodzaak voor werkzaamheden	Akkoord. Gebruikers krijgen toegang tot het collectiebeheersysteem middels SSO. Hiervoor beheert de iRvN verschillende Cloud Security Groepen. De manager van het RAN moet toestemming verlenen om een nieuwe persoon aan een van de groepen te laten toevoegen. Medewerkers die de organisatie verlaten wordt dankzij het gebruik van SSO toegang tot het systeem ontzegd. Daarnaast worden inactieve gebruikers periodiek verwijderd.
4. Risico’s en voorgestelde maatregelen	Deze zijn afdoende beschreven.	Akkoord.

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 zelf kent een 'laag' risico.

De maatregelen die verder worden beschreven, zijn m.i. afdoende.

Eind 2025 zal deze DPIA op naleving getoetst worden.

Ik adviseer hiermee positief en daarmee zijn de resterende risico's 'aanvaardbaar'.

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

PK/14/11/2024. DPIA 97.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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

DPIA Oordeel FG gemeente Nijmegen

DPIA Registratie ontheemden opvanglocaties

Inleiding

Hierbij het oordeel van de FG Gemeente Nijmegen over de DPIA 'Registratie ontheemden opvanglocaties'. Gekozen is voor een systematische aanpak. Deze is terug te herleiden tot de oordeelsvorming van DPIA's in het algemeen. In deze wordt het 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 welke weergeeft of m.i. het gehele voorstel van maatregelen én te nemen maatregelen bij geconstateerde risico's, tezamen een aanvaardbaar risico vormen bij het gebruik van privacy gevoelige gegevens.

In de periode sept tot nov 2024 hebben 5.1.2e, 5.1.2e, 5.1.2e, 5.1.2e 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 'Registratie ontheemden opvanglocaties' d.d. 20/11/2024.
Deze versie vormt de onderlegger voor deze toetsing.

Bij deze DPIA hoort de volgende bijlage:

- Verwerkersovereenkomst met Kentrikos B.V. (deze moet nog ondertekend worden).

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?	Nee.	Akkoord.
2. Is het ethisch / politiek bestuurlijk verantwoord?	Ja. Gemeente Nijmegen heeft op 10 maart vanuit het college van B&W het besluit genomen 1000 Oekraïense ontheemden op te vangen binnen de gemeente. Dit heeft inmiddels geresulteerd dat op vijf gemeentelijke opvanglocaties (GO) een totaal van ongeveer 700 ontheemden worden opgevangen, 200 bewoners verblijven in zogeheten particuliere opvanglocaties (PO) (in huis bij bewoners uit de stad).	Akkoord. Gezien de gemeente hierin een hotelfunctie heeft is zij verplicht een registratie bij te houden wie er staat ingeschreven en overnacht op de locatie. Er wordt een bewonerspas aangemaakt. Deze dient ervoor om te monitoren of iemand daadwerkelijk uit of thuis is bij eventuele calamiteiten. Uiteindelijk wordt de bewoner bij burgerzaken ingeschreven en ontvangt daar een BSN-nummer.
3. Juridische toets 3.a. Doel / grondslag	3a. *Doel* van deze gegevensverwerkingen: Het doel van het project is een deugdelijke registratie van de ontheemden. *Grondslag* De wettelijke grondslag voor de uitvoering is te vinden in de Regeling Opvang Ontheemden Oekraïne (ROOO, artikel 2 en 3.)	3a. Akkoord.
3.b. Persoonsgegevens Worden bijzondere persoonsgegevens verwerkt?	3.b. Ja. De volgende persoonsgegevens worden verwerkt: - Voornaam, Patroniem en achternaam; - Foto van de locatiepas; - Burgerservicenummer; - Telefoonnummer; - E-mailadres; - Koppeling tussen ouder en kind; - Algemene opmerkingen; - Interne opmerkingen; - Alcoholgegevens; Bijzondere persoonsgegevens als: - Medische gegevens; - Ras en etnische afkomst;	3.b. Akkoord.
3c. Proportionaliteit	3c. De persoonsgegevens worden alleen verzameld, gebruikt en toegevoegd aan de registratie wanneer dit noodzakelijk is voor het contact in de betreffende zaak. Dit betekent dat alleen relevante en noodzakelijke gegevens worden verwerkt, wat helpt om de inbreuk op de privacy tot een minimum te beperken.	3c. Akkoord.
3.d. Subsidiariteit	3.d. In de huidige werkwijze zijn de gegevens verspreid over verschillende mailboxen, persoonlijke schijven en diverse lijstjes. Hierdoor ontbreekt het aan controle en	3.d. Akkoord. Deze DPIA is met name gericht op het invoeren van een geschikt registratiesysteem welke voldoet aan de eisen van de AVG.

	overzicht over deze gegevens. De implementatie van Nieuwkomersregistratie kan dit probleem aanpakken door de gegevens op een centrale en gestructureerde manier te beheren.	Daarmee worden een aantal huidige problemen van registratie, beheer en beveiliging opgelost.
3.e. Persoonsgegevens buiten EER gebruikt?	3.e. Neen.	3.e. Akkoord
3.f. Andere partijen betrokken?	3.f. Medewerkers gemeente Nijmegen: verwerkingsverantwoordelijke Kentrikos B.V. (leverancier van de applicatie): verwerker. Andere betrokkenen: Medewerkers gemeente Nijmegen (afdeling MO team Opvang): gebruiker van de applicatie (locatiemanagers hebben toegang tot alle gegevens en schrijven bewoners in- en uit van de locatie); Medewerkers van de zorginstanties (Sterker en Iriszorg): gebruiker van de applicatie (kunnen enkel gegevens inzien t.b.v. de zorg "medische opmerkingen en identificatie bij calamiteiten); Medewerkers van de beveiligingsdienst (ProToGa Beveiliging): gebruiker van de applicatie (kunnen enkel gegevens inzien t.b.v. de toegangscontrole en identificatie bij calamiteiten);	3.f. Akkoord. Nog uit te voeren actie: Met de firma Kentrikos dient nog een verwerkersovereenkomst afgesloten te worden.
3.g. Hoe lang worden gegevens bewaard en wijze van vernietiging?	3.g. *Bewaartermijn* De gegevens worden maximaal twee weken bewaard na uitschrijving. Dit kan met 28 dagen worden verlengd indien het onduidelijk is of de ontheemden enkel met vakantie is. *Vernietiging:* Binnen het systeem wordt ingericht dat de gegevens na uitschrijving automatisch worden verwijderd.	Akkoord. De opvanglocaties zijn hiervoor verantwoordelijk.
3.h. Hoe worden gegevens beveiligd?	3.h. Alle toegang tot gevoelige gegevens wordt gelogd en logs worden regelmatig beoordeeld om verdachte activiteiten te detecteren. Monitoringtools worden gebruikt om afwijkend gedrag te signaleren en alarmsystemen in werking te stellen bij verdachte activiteiten. Gevoelige persoonsgegevens worden versleuteld, zowel tijdens opslag (data-at-rest) als tijdens overdracht (data-in-transit). Er wordt gebruikgemaakt van sterke encryptie standaarden (AES-256 CBC) voor opslag en TLS (1.2 en 1.3) voor netwerk overdracht.	Akkoord. De leverancier heeft een beleid en werkwijze gegevensbescherming en informatiebeveiliging overhandigd in afwachting van een volledige ISO-270001-certificering. Deze wordt begin 2025 afgerond.

4. Risico's en voorgestelde maatregelen	Deze zijn afdoende beschreven. Er zijn drie verschillende soorten van autorisatie. Die zijn per functie verdeeld: • Beveiliging en BHV. Zij hebben toegang tot foto, kamernummer en voornaam en achternaam en telefoonnummer. • Zorgmedewerkers van Sterker hebben toegang tot voornaam, achternaam, BSN en medische opmerkingenveld. • Locatiemanagers hebben toegang tot foto, kamernummer, voornaam, achternaam, patroniem, geboortedatum, geboorteplaats, land van herkomst, telefoonnummer, email adres, algemene en medische opmerkingen en locatie.	Akkoord. Advies: Omdat er veel (externe) betrokkenen gebruik maken van het systeem dient er een goede autorisatiematrix opgesteld te worden. Deze dient regelmatig te worden gecontroleerd op validiteit.

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 zelf kent een 'middelhoog' risico.

De volgende maatregelen dienen bij de implementatie uitgevoerd te worden:

- Nog uit te voeren actie:
  Met de firma Kentrikos dient nog een verwerkersovereenkomst afgesloten te worden.
  Deze dient als bijlage toegevoegd te worden aan deze DPIA.
- Omdat er veel (externe) betrokkenen gebruik maken van het systeem dient er een goede autorisatiematrix opgesteld te worden.
  Deze dient regelmatig te worden gecontroleerd op validiteit.

De maatregelen die verder worden beschreven, zijn m.i. afdoende.

Eind 2025 zal deze DPIA op naleving getoetst worden.

Ik adviseer hiermee positief en daarmee zijn de resterende risico's 'aanvaardbaar'.

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

PK/02/05/2024. DPIA 98.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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

DPIA Oordeel FG gemeente Nijmegen

DPIA Ontheffingenloket Zero Emissiezones Stadslogistiek (ZES)

Inleiding

Hierbij het oordeel van de FG Gemeente Nijmegen over de DPIA 'Ontheffingenloket Zero Emissiezones Stadslogistiek (ZES)'.
Gekozen is voor een systematische aanpak. Deze is terug te herleiden tot de oordeelsvorming van DPIA's in het algemeen. In deze wordt het 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 welke weergeeft of m.i. het gehele voorstel van maatregelen én te nemen maatregelen bij geconstateerde risico's, tezamen een aanvaardbaar risico vormen bij het gebruik van privacy gevoelige gegevens.

In de periode sept tot nov 2024 hebben 5.1.2e , 5.1.2e , 5.1.2e 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 'Ontheffingenloket Zero Emissiezones Stadslogistiek (ZES)' d.d. 28/11/2024.
Deze versie vormt de onderlegger voor deze toetsing.

Bij deze DPIA horen de volgende bijlage:

- Beleidsregels ontheffingen nul-emissie-zone Nijmegen 2025
- Dienstverleningsovereenkomst Centraal Loket 1.0 Zero-Emissiezone
- DPIA Zero-emissieloket Amsterdam
- Mandaatbesluit ontheffingen Verkeersbesluit nul-emissiezone bedrijfs- en vrachtauto's
- Verkeersbesluit nul-emissiezone bedrijfs- en vrachtauto's binnenstad Nijmegen, Hof
- Verwerkersovereenkomst zero-emissieloketgemeenten dd 14-8-24 tussen gemeente Amsterdam en gemeente Nijmegen.

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?	Nee. Niet binnen de gemeente Nijmegen	Akkoord. NB de gemeente Amsterdam heeft een DPIA uitgevoerd. Deze is als bijlage toegevoegd.
2. Is het ethisch / politiek bestuurlijk verantwoord?	Ja. Het Klimaatakkoord zet in op een versnelling naar een volledig emissievrije stadslogistiek: de nul- of zero-emissie stadslogistiek (ZES). Dit gebeurt met het instellen van zero-emissiezones voor vracht- en bestelauto's in de dertig tot veertig grootste gemeenten vanaf 2025. Het doel in bredere zin is het verbeteren van leefbaarheid in gemeenten ten aanzien van de luchtkwaliteit. Er zijn twee soorten ontheffingen: landelijke en gemeente specifieke ontheffingen. Landelijke ontheffingen worden in het Centraal Ontheffingenloket 1.0 aangevraagd waarbij alle aangesloten gemeenten de gemeente Amsterdam gemandateerd hebben voor de beoordeling en beslissing ervan. De gemeentespecifieke ontheffingen (artikel 12 en 13) worden door de gemeente zelf beoordeeld, waarbij eveneens gebruik wordt gemaakt van de applicatie Centraal Ontheffingenloket 1.0.	Akkoord. Per 1 januari 2025 zijn op basis van gemeentelijk gepubliceerde verkeersbesluiten de zero-emissie (ZE) zones van kracht. Op basis van het in de betrokken gemeenten vastgestelde ontheffingenbeleid kunnen er ontheffingen aangevraagd worden. Deze DPIA ziet toe op de ontheffingsaanvragen die door gemeente Nijmegen worden beoordeeld. Het betreft dan aanvragen op grond van bedrijfseconomische belangen ofwel op grond van de hardheidsclausule c.q. afwijkingsbevoegdheid van de gemeente. De overige ontheffingsgronden worden onder mandaat door gemeente Amsterdam uitgevoerd voor alle gemeentes in Nederland. De verwerkingen die in dat kader plaatsvinden vallen – als gevolg van de mandatering – onder de verantwoordelijkheid van de gemeente Amsterdam. Deze verwerkingen vallen daarom niet onder de reikwijdte van deze DPIA.
3. Juridische toets 3.a. Doel / grondslag	3a. *Doel* van deze gegevensverwerkingen: Doel van de verwerking(en) is het beoordelen van en beslissen op ontheffingsaanvragen voor de Zero Emissiezones. *Grondslag* De verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang (art. 6, eerste lid, onder e AVG). Het betreft de uitvoering van de volgende wettelijke taken - Verkeersbesluit nul-emissiezone bedrijfs- en vrachtauto's centrum Nijmegen, Hof van Holland en Campus Heijendaal: Verkeersbesluit voor een nul-emissiezone voor bedrijfs- en vrachtauto's in de binnenstad van Nijmegen aan Hof van Holland en Campus Heijendaal te Nijmegen - Het verlenen van ontheffingen: Reglement verkeersregels en verkeerstekens 1990, artikel 87.	3a. Akkoord.
3.b. Persoonsgegevens Worden bijzondere persoonsgegevens verwerkt?	3.b. Neen. De volgende persoonsgegevens worden verwerkt:	3.b. Akkoord.

	- Kenteken; - Naam; - Bedrijfsnaam; - Telefoonnummer; - E-mailadres; - Adres aanvrager dan wel bedrijf (straatnaam, huisnummer, postcode, stad, land (alleen Europese landen)); - Financiële en bedrijfsgegevens: - Bewijs om de eigenaar van het voertuig vast te stellen; - Jaarrekeningen van de afgelopen drie jaar. - Btw-aangiften van het jaar van aanvraag; - Een overzicht van alle voertuigen van het bedrijf; - Contracten die laten zien dat aanvrager in de ZE-zone werkt; - Indien aanwezig, een standplaats- of marktvergunning; - Rittenstaten en facturen van vervoer naar de ZE-zone, met aanduiding van de omzet van die ritten, voor de ritten met het voertuig waarvoor ontheffing wordt aangevraagd; - Een eventueel aangevraagde offerte voor een voertuig dat wel de ZE-zone in mag of een offerte voor aanpassingen aan een bestaand voertuig; - Een plan van aanpak met de acties die aanvrager onderneemt om wel aan de toelatingseisen van de zero-emissiezone te voldoen.	Weliswaar wordt bij de ontheffingsgrond voor voertuigen die zijn aangepast vanwege een handicap, gevraagd naar een eventueel aanwezige gehandicaptenparkeerkaart, maar voor deze aanvragen is gemeente Amsterdam verwerkingsverantwoordelijke, waardoor deze gegevens geen onderdeel zijn van deze DPIA.
3c. Proportionaliteit	3c. De gegevens worden uitgevraagd om bij aanvraag het recht op een ontheffing te beoordelen en fraude hierin te voorkomen. Voor de werkwijze met een landelijk loket is landelijk gekozen.	3c. Akkoord. Er vindt alleen gegevensuitwisseling plaats als een ontheffing wordt aangevraagd op basis van de gemeentespecifieke gronden, die na screening door Amsterdam ontvankelijk blijkt. Alleen in deze gevallen wordt de aanvraag gedeeld met Nijmegen, ter beoordeling, aanvulling en besluit.
3.d. Subsidiariteit	3.d. Aanleveren van de bedrijfsgegevens is nodig om de aanvraag op deze grond te kunnen beoordelen. Een onafhankelijk adviesbureau beoordeelt of het bedrijf genoeg geld heeft om te kunnen investeren in een nieuw uitstootvrij voertuig of een gebruikt emissieklasse 6 voertuig.	3.d. Akkoord. De in paragraaf genoemde financiële en bedrijfsgegevens zijn volgens het adviesbureau allemaal nodig voor het beoordelen van de ontheffingsaanvraag.
3.e. Persoonsgegevens buiten EER gebruikt?	3.e. Neen.	3.e. Akkoord
3.f. Andere partijen betrokken?	3.f. Naam partij: RDW Open Data Rol: Verrijken kentekens met voertuiggegevens Overeenkomst /afspraken: RDW Open Data (er zit geen authenticatie op deze bron). Naam partij: RDW Gesloten Data	3.f. Akkoord, mits….. Bijgaand overzicht komt uit de DPIA gemaakt door Amsterdam. De mits…. Het is enigszins onduidelijk of de verwerkingen niet óók - ondanks genoemde mandatering –

	Rol: Verrijken kentekens met eigenaarsgegevens en postcode 6 Overeenkomst /afspraken: RDW Certificaat (username en wachtwoord) Naam partij: Rabobank Internet Kassa Rol: Betaalmogelijkheid leges (naam, email en telefoonnummer worden doorgegeven bij het starten van een betalingsverzoek.) Overeenkomst /afspraken: Overeenkomst via gemeente Amsterdam Naam partij: NPR Rol: Ontheffingen Informatie Systeem Overeenkomst /afspraken: RDW Certificaat en username (pin) Naam partij: G4 Rol: Initiator samenwerkwerkingsverband dat gemeente Amsterdam heeft gemandateerd voor als verwerkingsverantwoordelijke Overeenkomst /afspraken: Samenwerkingsovereenkomst Centraal Ontheffingenloket 1.0 Zero-Emissiezone Naam partij: Milieuzones.nl Rol: Te bevragen bron voor landelijke milieuzone ontheffingen Overeenkomst /afspraken: Ongeauthenticeerde bron Naam partij: Aangesloten gemeenten Rol: Hebben de gemeente Amsterdam gemandateerd voor de verwerking van gegevens van landelijke ontheffing. Zijn verwerkingsverantwoordelijke voor de gemeente specifieke ontheffingen (artikel 12 en 13) en hebben een overeenkomst dat gemeente Amsterdam de gegevens mag verwerken Overeenkomst /afspraken: Dienstverleningsovereenkomst Centraal Ontheffingenloket 1.0 Zero-Emissiezone. VWO als bijlage bij Dienstverleningsovereenkomst Centraal Ontheffingenloket 1.0 Zero-Emissiezone Naam partij: SHPV Rol: Verwerker van gemeenten voor beoordelen ontheffing art 12 Overeenkomst /afspraken: VWO Naam partij: Bureau voor Financieel adviseur Rol: Verwerker van SHPV voor financiële beoordeling ontheffing artikel 12,sub-verwerker van de gemeente Amsterdam	onder verwerkingsverantwoordelijkheid van de gemeente Nijmegen vallen. Hierover zal nader overleg plaatsvinden met gemeente Amsterdam. Indien nodig zal deze DPIA daarop worden aangepast/aangevuld. In dat geval zal ook een nieuwe verwerkersovereenkomst worden afgesloten. Het is zaak snel hierover duidelijkheid te verkrijgen (opstaande actie). Voor deze verwerkingen (gemeente specifieke ontheffingen art. 12 en art. 13) is Nijmegen verantwoordelijk en is de gemeente Amsterdam verwerker. (hierover is geen meningsverschil). Bijgevoegd zijn: - Dienstverleningsovereenkomst Centraal Ontheffingenloket 1.0 Zero-Emissiezone (bijlage) - Verwerkersovereenkomst zero-emissieloket gemeenten

	Overeenkomst /afspraken: VWO	
3.g. Hoe lang worden gegevens bewaard en wijze van vernietiging?	3.g. *Bewaartermijn* De bewaartermijn is de duur van de ontheffing plus 1 jaar. *Vernietiging:* Er draait binnen de applicatie een automatisch script dat ervoor zorgt dat bij het bereiken van het einde van de bewaartermijn de desbetreffende ontheffing en de gegevens worden verwijderd.	Akkoord. De applicatiebeheerder van de gemeente Amsterdam ziet erop toe dat dit daadwerkelijk gebeurt en doet hiervan jaarlijks verslag.
3.h. Hoe worden gegevens beveiligd?	3.h. Het BasisBeveiligingsNiveau (BBN) is: 2. Van toepassing zijnde maatregelen conform BBN2 zijn uitgevoerd. Er vindt continu vulnerability scanning, logging en monitoring plaats.	Akkoord.
4. Risico's en voorgestelde maatregelen	Deze zijn afdoende beschreven.	Akkoord. Van belang is dat het jaarverslag van de applicatiebeheerder - zijnde de gemeente Amsterdam - actief opgevraagd wordt en ook beoordeeld wordt. Hierover dient verslag te worden gedaan middels het jaarlijkse controlplan aan de FG van de gemeente Nijmegen.

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 zelf kent een 'laag' risico.

De volgende maatregelen dienen nog uitgevoerd te worden:
Uit de DPIA:
"Het is enigszins onduidelijk of de verwerkingen niet óók - ondanks genoemde mandatering – onder verwerkingsverantwoordelijkheid van de gemeente Nijmegen vallen. Hierover zal nader overleg plaatsvinden met gemeente Amsterdam. Indien nodig zal deze DPIA daarop worden aangepast/aangevuld. In dat geval zal ook een nieuwe verwerkersovereenkomst worden afgesloten."
Het is zaak snel hierover duidelijkheid te verkrijgen (opstaande actie). De maatregelen die verder worden beschreven, zijn m.i. afdoende.

Tevens:
Van belang is dat het jaarverslag van de applicatiebeheerder - zijnde de gemeente Amsterdam - actief opgevraagd wordt en ook beoordeeld wordt. Hierover dient verslag te worden gedaan middels het jaarlijkse controlplan aan de FG van de gemeente Nijmegen.

Eind 2025 zal deze DPIA op naleving getoetst worden.

Ik adviseer hiermee positief en daarmee zijn de resterende risico's 'aanvaardbaar'.

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

PK/02/12/2024. DPIA 99.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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

DPIA Oordeel FG gemeente Nijmegen

DPIA: Collectieve Aanvullende Zorgverzekering (CAZ)

Inleiding

Hierbij het oordeel van de FG Gemeente Nijmegen over de DPIA 'Collectieve Aanvullende Zorgverzekering'. Gekozen is voor een systematische aanpak. Deze is terug te herleiden tot de oordeelsvorming van DPIA's in het algemeen. In deze wordt het 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, tezamen een aanvaardbaar risico vormen bij het gebruik van privacygevoelige gegevens.

In de periode aug – nov 2024 hebben 5.1.2e , 5.1.2e en 5.1.2e 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 'Collectieve Aanvullende Zorgverzekering' d.d. 08/11/2024.
Deze versie vormt de onderlegger voor deze toetsing.

Bij deze DPIA hoort de volgende bijlage:

- Verwerkersovereenkomst BS&F
- DPIA van Gezond Verzekerd (BS&F)

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?	Neen	Akkoord. Als bijlage is wél de DPIA van Gezond Verzekerd (BS&F) toegevoegd.
2. Is het ethisch / politiek bestuurlijk verantwoord?	Ja. De Collectief Aanvullende Zorgverzekering (CAZ) is een onderdeel van de inkomensondersteunende maatregelen en ondersteunt inwoners met een laag inkomen bij het afsluiten van een aanvullende zorgverzekering	Akkoord. Naast een korting vanuit de verzekeraar geven gemeenten vaak een bijdrage in de premie van de aanvullende zorgverzekering binnen de Gemeentepolis. Deze bijdrage vormt categoriale bijzondere bijstand op grond van de Participatiewet (art. 35 lid 3).
3. Juridische toets 3.a. Doel / grondslag	3a. Doel en grondslag Het *doel:* Het doel van de verwerking is het verlenen van een collectieve aanvullende zorgverzekering op grond van de Participatiewet. De *grondslag* voor de verwerking: Uitvoering van een publiekrechtelijke taak op grond van artikel 35 lid 3 Participatiewet.	3a. Akkoord.
3.b. Persoonsgegevens Worden bijzondere persoonsgegevens verwerkt?	3.b. Neen, in principe niet. De volgende gegevens worden vastgelegd: Naam; adres; andere contactgegevens; geboortedatum; geslacht; nationaliteit; burgerlijke staat; samenstelling huishouden; vermogenspositie; loon, uitkeringen, inkomen; BSN.	3.b. Akkoord.
3c. Proportionaliteit	3c. Om in aanmerking te kunnen komen voor een CAZ moet de betreffende inwoner een aantal gegevens over diens vermogen en/of inkomen verstrekken. Deze verwerking brengt daarmee een behoorlijke inbreuk op de privacy van betrokkenen met zich mee. Daar staat tegenover dat het aanvragen van een CAZ vrijwillig is, en uiteindelijk ten goede komt aan de inkomenspositie van de betrokkene.	3c. Akkoord.
3.d. Subsidiariteit	3.d. De aanvraag wordt geregistreerd in de Suite Sociaal Domein van de gemeente Nijmegen. Dit gebeurt nu nog handmatig. De toetsing van de aanvragen vindt nu achteraf plaats. Dit proces wordt geautomatiseerd, waarbij aanvragen via Gezondverzekerd.nl rechtstreeks in de Suite van de gemeente Nijmegen worden ingevoerd. Door de koppeling kan informatie meteen in de Suite landen waardoor er minder controles achteraf nodig zijn. Dit werkt efficiënter en	3.d. Akkoord. Hoewel genoemde koppeling de aanleiding vormt voor het schrijven van deze DPIA, ziet de DPIA niet alleen op deze koppeling: de DPIA ziet toe op alle verwerkingen van persoonsgegevens in het kader van het verstrekken van een CAZ door de gemeente. Het gaat dan zowel om de verwerkingen die BS&F verricht als de verwerkingen die de gemeente Nijmegen verricht.

	minder foutgevoelig dan het huidige handmatige proces.	
3.e. Persoonsgegevens buiten EER gebruikt?	3.e. Neen.	3.e. Akkoord
3.f. Andere partijen betrokken?	3.f. *Verwerkingsverantwoordelijke*: Gemeente Nijmegen. *Verwerker:* BS&F BV. Zorgverzekeraars zijn ontvanger van de informatie.	3.f. Akkoord. De verwerkersovereenkomst met BS&F is als bijlage bij deze DPIA toegevoegd. De verwerkersovereenkomst met BS&F wordt vernieuwd en toegevoegd als bijlage na ondertekening.
3.g. Hoe lang worden gegevens bewaard en wijze van vernietiging?	3.g. Maximaal 10 jaar, conform de Archiefwet 1995 en de daarbij behorende Selectielijst gemeenten en intergemeentelijke organen 2020.	Akkoord. Binnen de gemeente heeft BDI een signalerende rol voor het bereiken van de bewaartermijnen. De afdeling is verantwoordelijk voor het opdracht geven tot vernietiging van de bepaalde informatie.
3.h. Hoe worden gegevens beveiligd?	3.h. Gegevens worden in de Suite en Corsa opgeslagen onder een werkproces Sociale Regelingen. Toegang tot de informatie in deze werkprocessen en documenten is geautoriseerd via rollen mandaten in de beide applicaties.	Akkoord. In de bijlage is de DPIA van Gezond Verzekerd (BS&F) toegevoegd, waarin zij beschrijven hoe zij de privacy van inwoners beschermen.
4. Risico's en voorgestelde maatregelen	Deze zijn afdoende beschreven.	Akkoord. Maatregelen die noodzakelijk zijn (par. 8.2. DPIA) dienen wel getoetst te worden op hun uitvoering. Eens per jaar een rapportage hierover (bij uitvraag van het controlplan) is hierin afdoende.

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 zelf kent een 'laag' risico.

De maatregelen die verder worden beschreven, zijn m.i. afdoende.

Nog uit te voeren actie:

- De verwerkersovereenkomst met BS&F wordt vernieuwd en toegevoegd als bijlage na ondertekening.

Eind 2025 zal deze DPIA op naleving getoetst worden.
Daarbij wordt getoetst of de in de DPIA opgenomen maatregelen ook daadwerkelijk worden uitgevoerd.
NB. Er zal hierin specifiek gekeken worden naar de 'Maatregelen die noodzakelijk zijn' (par. 8.2. DPIA).

Ik adviseer hiermee positief en daarmee zijn de resterende risico's "aanvaardbaar.

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

PK/02/12/2024. DPIA 100

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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

DPIA Oordeel FG gemeente Nijmegen

DPIA: Gelderse Monitor Jeugd

Inleiding

Hierbij het oordeel van de FG Gemeente Nijmegen over de DPIA 'Gelderse Monitor Jeugd.
Gekozen is voor een systematische aanpak. Deze is terug te herleiden tot de oordeelsvorming van DPIA's in het algemeen. In deze wordt het 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 welke weergeeft of m.i. het gehele voorstel van maatregelen én te nemen maatregelen bij geconstateerde risico's, tezamen een aanvaardbaar risico vormen bij het gebruik van privacygevoelige gegevens.

In de periode zomer 23 tot okt 2024 hebben 5.1.2e , 5.1.2e , 5.1.2e , 5.1.2e , 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 'Gelderse Monitor Jeugd' d.d. 25/10/2024.
Deze versie vormt de onderlegger voor deze toetsing.

Bij deze DPIA horen de volgende bijlage:

- DPIA tbv Gelderse Monitor 1.2
- GVJB Verbetermonitor Dataverwerking
- Governance Gelderse Monitor Jeugd
- DPIA v1.1 QA 01-08-2024 def
- Gemeente Nijmegen draagt Ketendata iJW over aan Initi8
- Identiteits- en toegangsbeheer (IAM) GMJ v1.0
- Verwerkersovereenkomst. stichting.inlichtingenbureau.gegevensknooppunt
- getekende 21131 verwerkersovereenkomst INITI8
- DPIA Initi8 2023
- DPIA Gegevensuitwisseling Ketenknooppunt
- PIA Monitor- en Stuurinformatie iJw v1.0
- PIA Ketendata iJw (Monitor- en Stuurinformatie iJw) v1.1

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. Een tweetal voorlopers, waarvan die van Initi8 grotendeels vervangen word door deze DPIA (aantal processen gaan anders verlopen); maar ook deels nog valide zijn, omdat alleen voor het aspect Jeugd een ander proces wordt ingericht, voor de andere componenten (zoals WMO) niet.	Akkoord. Het betreft de volgende DPIA's die hiermee gerelateerd zijn: DPIA 51 Initi8 2023. DPIA 52 Gegevensuitwisseling Ketenknooppunt Tevens zijn PIA's, opgesteld door het Inlichtingenbureau, van belang: PIA Voorziening iJw - Stuurinformatie iJw v1.0.: Deze beschrijft de data die het Inlichtingenbureau opslaat en verwerkt in het kader van monitor- en stuurinformatie. PIA Ketendata iJw (Monitor- en Stuurinformatie iJw) v1.1: het informatieproduct welke de gemeente kan gebruiken voor het zelf kunnen maken van monitor- en stuurinformatie.
2. Is het ethisch / politiek bestuurlijk verantwoord?	Ja. De Gelderse Verbeteragenda Jeugdbescherming (GVJB) is een samenwerking tussen 7 jeugdhulpregio's in Gelderland, 4 Gecertificeerde instellingen. Deze partijen hebben de gezamenlijke maatschappelijke opdracht om veiligheid in gezinnen te creëren door vroegtijdig te signaleren, snel bij te sturen en waar nodig effectief in te grijpen. Om inzicht te krijgen in de beoogde verbetering zijn vanuit de Gelderse Verbeteragenda door de werkgroep Monitoring 7 Kritische Prestatie Indicatoren (KPI's) geformuleerd. Om voortgang op de KPI's en daarmee samenhangend een aantal resultaatafspraken, te kunnen monitoren, is monitoring op Gelders niveau noodzakelijk. Hiervoor wordt een Gelderse Monitor Jeugd geïmplementeerd. Vanuit de GVJB is de vraag gesteld aan INITI8 om in deze monitor te voorzien.	Akkoord. Om inzicht te krijgen in de beoogde verbetering zijn 7 Kritische Prestatie Indicatoren (KPI's) geformuleerd. Deze KPI's geven inzage in de beoogde verbetering vanuit de Gelderse Verbeteragenda Jeugdbescherming en mogelijke trends en ontwikkelingen in het Gelderse zorglandschap. De informatie die daarmee gegenereerd wordt, wordt gebruikt voor regionale en lokale transformatieplannen om de jeugdhulp in Gelderland te verbeteren. Daarnaast geven de KPI's inzage in een aantal resultaatafspraken die als resultaatsverplichting zijn opgenomen in het uniforme contract tussen de 7 jeugdhulpregio's en de 4 Gecertificeerde instellingen. Voor de monitor wordt gebruik gemaakt van de gegevens uit het 'Berichtenverkeer Jeugdwet' (iJw Berichtenverkeer). Deze monitor wordt beschikbaar gesteld aan zowel regio's, gemeenten als Gecertificeerde instellingen.
3. Juridische toets 3.a. Doel / grondslag	3a. Doel en grondslag Het *doel:* De monitor levert strategische en tactische sturingsinformatie aan jeugdhulpregio's, gemeenten en gecertificeerde instellingen. De monitor geeft inzicht in de voortgang op de geformuleerde KPI's. Daarnaast geeft de monitor inzicht in de voortgang op de resultaatafspraken die gelden tussen jeugdhulpregio's, gecertificeerde instellingen en Jeugdhulpaanbieders.	3a. Akkoord. Door monitoring wordt het effect van de acties uit de Gelderse Verbeteragenda inzichtelijk. Hierdoor worden trends en ontwikkelingen in het Gelderse zorglandschap in beeld gebracht. Het gaat om informatie die nodig is voor de regionale transformatieplannen met als doel de jeugdbescherming en Jeugdhulp in Gelderland te verbeteren.

	De *grondslagen* De juridische grondslag is gelegen in de Jeugdwet (Art 6 lid 1 sub e AVG). • Het kunnen maken van resultaatafspraken, monitoren en het daarbij voeren van leveranciersmanagement-gesprekken in verband met de levering van voorzieningen, inclusief de aanbesteding hiervan • Het door de gemeenteraad op te stellen plan met betrekking tot het door het gemeentebestuur te voeren beleid • Het zorgdragen voor een kwalitatief en kwantitatief toereikend aanbod van gecertificeerde instellingen en juiste, passende en tijdige beschikbare jeugdhulp. • Het voldoen aan de door de minister van VWS in het belang van de beperking van uitvoeringslasten gestelde regels • De hun door de Jeugdwet opgedragen taakstelling • De samenwerking met andere colleges in verband met de doeltreffende en doelmatige uitvoering van de jeugdwet • De te treffen algemene maatregelen en bepaling van de aangewezen voorzieningen	(art. 2.11 Jeugdwet); (art 2.2 Jeugdwet); (art. 2.6 lid 1 sub a Jeugdwet) (art. 2.15 Jeugdwet). (art. 2.1 Jeugdwet); (art. 2.8 Jeugdwet); (art. 2.14 Jeugdwet);
3.b. Persoonsgegevens Worden bijzondere persoonsgegevens verwerkt?	3.b. De volgende persoonsgegevens worden verwerkt: - *BSN – Hash (gepseudonimiseerd)* De verzameling en verwerking van gepseudonimiseerde BSN gegevens is noodzakelijk om de jeugdhulpinzet en samenloop per jeugdige in kaart te brengen - *AGB code declarant/aanbieder* Gegevens over AGB code declarant/aanbieder is noodzakelijk om inzicht te krijgen in de KPI's. - *Gemeentecode* Gegevens over de gemeentecodes zijn noodzakelijk om inzicht te krijgen in de KPI's per gemeente en regio. - *Declaratiebedrag* Gegevens over declaratiebedragen zijn noodzakelijk om inzicht te krijgen in financiële waarde van ingezette jeugdhulp en de jeugdhulpkosten. - *Toegekend bedrag* Gegevens over toegekende bedragen zijn noodzakelijk om inzicht te krijgen in financiële waarde van ingezette jeugdhulp en de jeugdhulpkosten. - *Postcode* Gegevens over postcode zijn noodzakelijk om validatie van de monitor mogelijk te maken. Validatie vindt plaats voordat de gegevens beschikbaar worden gemaakt aan gebruikers.	3.b. Akkoord. NB. Het betreft bijzondere persoonsgegevens van een kwetsbare doelgroep. (KPI 4 & 5 GVJB). (KPI 1 t/m 7). AGB staat voor Algemeen Gegevensbeheer Zorgverleners. Zorgaanbieders hebben een unieke AGB-code. (KPI 1 t/m 7) (KPI 1) (KPI 1) Na validatie worden de gegevens gefilterd, daarmee komen ze niet beschikbaar voor gebruikers.

	- *Geslacht* Gegevens over geslacht zijn noodzakelijk om validatie van de monitor mogelijk te maken. Validatie vindt plaats voordat de gegevens beschikbaar worden gemaakt aan gebruikers. - - *Geboortedatum* Gegevens over leeftijd o.b.v. de geboortedatum zijn noodzakelijk om validatie van de monitor mogelijk te maken. Validatie vindt plaats voordat de gegevens beschikbaar worden gemaakt aan gebruikers. - *Productcodes van toegewezen jeugdhulp* Gegevens over productcodes zijn noodzakelijk om inzicht te krijgen in de ingezette jeugdhulpproducten. - *Toewijzingsnummer* Gegevens over toewijzingsnummers is noodzakelijk om inzicht te krijgen in de ingezette jeugdhulpproducten. - *Ingangsdatum toewijzing* Gegevens over de ingangsdatum van een toewijzing zijn noodzakelijk om inzicht te krijgen in de totaal ingezette jeugdhulpproducten, in vergelijking tot de toegewezen jeugdhulp - *Einddatum toewijzing* Gegevens over de einddatum van een toewijzing zijn noodzakelijk om inzicht te krijgen in de totaal ingezette jeugdhulpproducten, in vergelijking tot de toegewezen jeugdhulp - *Datum start zorg* Gegevens over de startdatum van de zorg zijn noodzakelijk om inzicht te krijgen in de totaal ingezette jeugdhulpproducten, de bijbehorende financiële waarde, eventuele samenloop, instroom, doorstroom en uitstroom. - *Datum stop zorg* Gegevens over de stopdatum van de zorg zijn noodzakelijk om inzicht te krijgen in de totaal ingezette jeugdhulpproducten, de bijbehorende financiële waarde, eventuele samenloop, instroom, doorstroom en uitstroom. - *Aantal eenheden* Gegevens over de eenheden van de zorg zijn noodzakelijk om inzicht te krijgen in de totaal ingezette jeugdhulp per product.	Na validatie worden de gegevens gefilterd, daarmee komen ze niet beschikbaar voor gebruikers. Na validatie worden de gegevens gefilterd, daarmee komen ze niet beschikbaar voor gebruikers. (KPI 1 t/m 7) (KPI 1 t/m 7) (KPI 6). (KPI 6) (KPI 1 t/m 7) (KPI 1 t/m 7) (KPI 1).
3c. Proportionaliteit	3c. De gegevensverwerking via het Inlichtingenbureau en INITI8 draagt in een belangrijke mate bij aan de monitoring van de Gelderse Verbeteragenda. En daarmee draagt het in een belangrijke mate bij aan een efficiënte, transparante en uniforme	3c. Akkoord. NB. De gegevens ‘Postcode’, ‘geslacht’ en ‘geboortedatum’ worden alleen gebruikt ter validatie en verder niet meer opgenomen in deze gegevensverwerking.

	uitvoering van de jeugdbescherming in Gelderland. De persoonsgegevens zijn noodzakelijk voor de berekening van de KPI's, wat betekent dat het zonder de verwerking van de genoemde persoonsgegevens het niet mogelijk is om de KPI's inzichtelijk te maken.	
3.d. Subsidiariteit	3.d. In de monitor wordt enkel gewerkt met pseudo-BSN-gegevens. Er is gekozen om te Pseudonimiseren in plaats van Anonimiseren. Pseudonimiseren wordt ingezet om 2 redenen: 1. Gegevens kunnen matchen uit andere datasets, dit gebeurt in het proces omdat er verschillende organisaties zijn die gegevens aanleveren. Door gegevens te pseudonimiseren blijven de versleutelde waarden hetzelfde in diverse datasets en zo kan bijvoorbeeld gecontroleerd worden of gegevens niet dubbel verwerkt worden. 2. Pseudonimiseren zorgt ervoor dat gegevens niet snel herleidbaar zijn naar een jeugdige, op basis van het BSN.	3.d. Akkoord. Er is hierdoor sprake van een zeer beperkte herleidbaarheid van de gegevens.
3.e. Persoonsgegevens buiten EER gebruikt?	3.e. Neen.	3.e. Akkoord. De gegevensverwerkingen vinden uitsluitend plaats in Nederland.
3.f. Andere partijen betrokken?	3.f. - *56 gemeenten (vertegenwoordigd in 7 Gelderse jeugdhulpregio's):* Elke individuele gemeente is verantwoordelijk voor haar wettelijke jeugdzorg taakstelling. Elke gemeente is eigenaar van de data in het iJw Berichtenverkeer binnen de gemeente. - *4 gecertificeerde instellingen:* Gecertificeerde instellingen zijn verantwoordelijk voor de uitvoer van de jeugdbescherming – en/of reclassering maatregelen. - *Jeugdhulpaanbieders:* De Jeugdhulpaanbieders zijn verantwoordelijk voor het organiseren van de essentiële functies in het kader de Jeugdhulp in de regio Gelderland. - *Het Inlichtingenbureau:* Het Inlichtingenbureau is beheerder van het Gemeentelijk Gegevensknooppunt. Als informatieknooppunt verzamelt het Inlichtingenbureau gegevens uit het iJw Berichtenverkeer in de Voorziening iJw en verwerkt deze gegevens in ketendatasets. Ten	3.f. Akkoord. Vanuit dit eigenaarschap is iedere gemeente verwerkingsverantwoordelijk voor de gegevensverwerking van data uit het iJw Berichtenverkeer ten behoeve van de monitor. Gemeenten zijn tevens gebruiker van de Gelderse Monitor Jeugd. In dat kader wisselen de instellingen iJw berichten uit met zorgaanbieders in het iJw Berichtenverkeer en zijn zij verstrekker van gegevens ten behoeve van de monitor. Gecertificeerde instellingen zijn tevens gebruikers van de Gelderse Monitor Jeugd. In dat kader wisselen de jeugdhulpaanbieders iJW berichten uit met gemeenten en zijn zij verstrekker van gegevens ten behoeve van de monitor. De Jeugdhulpaanbieders zijn tevens gebruikers van de Gelderse Monitor Jeugd. Alle individuele gemeenten hebben een verwerkersovereenkomst afgesloten met het Inlichtingenbureau om opdracht te geven voor de genoemde verwerkingen (zie bijlage).

	behoeve van de Gelderse Monitor Jeugd treedt het Inlichtingenbureau op als verwerker. - *INITI8:* Inti8 is ontvanger van de ketendatasets zoals beschikbaar gesteld door het Inlichtingenbureau. INITI8 treedt tevens op als verwerker van de ketendatasets. Na verwerking van deze gegevens in de Gelderse Monitor Jeugd zijn deze gegevens enkel beschikbaar voor regio's, gemeenten en gecertificeerde instellingen.	Alle individuele gemeenten sluiten een verwerkersovereenkomst af met INITI8 om opdracht te geven voor de genoemde verwerkingen (zie bijlage).
3.g. Hoe lang worden gegevens bewaard en wijze van vernietiging?	3.g. *Bewaartermijnen:* De gegevens in de monitor worden bewaard zolang er een geldige Raamovereenkomst bestaat voor de Gelderse Verbeteragenda voor de Jeugdbescherming. *Vernietiging:* INITI8 zal de data uiterlijk 6 maanden na verlopen van de raamovereenkomst verwijderen.	Akkoord.
3.h. Hoe worden gegevens beveiligd?	3.h. Toegang tot de monitor wordt geregeld in het proces voor identiteits- en toegangsbeheer. Dit proces beslaat het beheren van digitale identiteiten en het controleren van de toegang. Bij het verifiëren van de identiteit van de gebruiker, wordt door INITI8 gebruik gemaakt van Single Sign On (SSO) van Microsoft. Met SSO kunnen geautoriseerde personen met één set referenties via hun gebruikelijke/standaard computer login toegang krijgen tot de omgeving van de monitor. Zodra de identiteit van de gebruiker is geverifieerd, wordt toegang tot het dashboard verleend. Er zijn door INITI8 tevens een groot aantal technische voorzieningen getroffen ter beveiliging van de gevoelige data, zoals: - 24/7 Key camerabewaking en on site bewaakte Datacenters 5.1.2h 5.1.2h 5.1.2h 5.1.2h 5.1.2h - Encrypted laptops en harde schijven van medewerkers INITI8 - Centraal beheerd wachtwoord beleid (AD) voor medewerkers INITI8	Akkoord. Gebruikers krijgen alleen via hun eigen geregistreerde account bij de organisatie waar ze werkzaam voor zijn toegang tot de monitor. Gebruikersactiviteiten worden gemonitord en er worden rapporten over toegang en gebruik gegenereerd. NB: dit geheel dient regelmatig op 'naleving' gecontroleerd te worden.

	- Websites en portalen beveiligd met certificaten - HTTPS portal 5.1.2h 5.1.2h 5.1.2h - Gescheiden opslag, isolatie van identificerende en niet identificerende persoonsgegevens - Gescheiden gegevensdomeinen instellingen en netwerken.	
4. Risico's en voorgestelde maatregelen	Deze zijn afdoende beschreven. Het Governance proces beschrijft op welke wijze gemaakte afspraken gecontroleerd worden en door wie. Daarbij is het van belang de volledige benodigde keten voor het verwerken van privacygevoelige data te beschouwen. Elke deelnemende partij heeft zijn rol en verantwoordelijkheden. In het Governance proces wordt uitgegaan van een efficiënte en pragmatische aanpak.	Akkoord. NB. Dit geheel is een complexe organisatie waarin elke deelnemende partij de eigen verantwoordelijkheid moet nemen en regelmatig moet toetsen of iedere deelnemer zich houdt aan de overeengekomen afspraken.

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 zelf kent een 'middelhoog' risico:
- Het betreft bijzondere persoonsgegevens van een kwetsbare doelgroep.
- Dit geheel is een complexe organisatie waarin elke deelnemende partij de eigen verantwoordelijkheid moet nemen en regelmatig moet toetsen of iedere deelnemer zich houdt aan de overeengekomen afspraken.
- verantwoording zal dienen te geschieden aan de eigen FG. Daarnaast zullen de FG's van de deelnemende organisaties onderling ook hun verantwoording moeten delen. Mijn voorstel is dat dit in maart 2026 voor het eerst plaatsvindt. Initiatief om dit te organiseren, zal genomen moeten worden vanuit de projectorganisatie van de Gelderse Monitor.

Acties:
- Gebruikers krijgen alleen via hun eigen geregistreerde account bij de organisatie waar ze werkzaam voor zijn toegang tot de monitor.
- Gebruikersactiviteiten worden gemonitord en er worden rapporten over toegang en gebruik gegenereerd.
Dit geheel dient regelmatig op 'naleving' gecontroleerd te worden.

De maatregelen die verder worden beschreven, zijn m.i. afdoende.

Eind 2025 zal deze DPIA op naleving getoetst worden.
Daarbij wordt getoetst of de in de DPIA opgenomen maatregelen ook daadwerkelijk worden uitgevoerd en de beide aanbevelingen uitgevoerd zijn.

Ik adviseer hiermee positief en daarmee zijn de resterende risico's 'aanvaardbaar'.

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

PK/19/12/2024. DPIA 101

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenss feer	1
Wet open overheid	Art. 5.1 lid 2 sub h	De beveiliging van personen en bedrijven e n het voorkomen van sabotage	6, 7

DPIA Oordeel FG gemeente Nijmegen

DPIA Camerahandhaving geslotenverklaringen

Inleiding

Hierbij het oordeel van de FG Gemeente Nijmegen over de DPIA 'Camerahandhaving geslotenverklaringen'. Gekozen is voor een systematische aanpak. Deze is terug te herleiden tot de oordeelsvorming van DPIA's in het algemeen. In deze wordt het 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 welke weergeeft of m.i. het gehele voorstel van maatregelen én te nemen maatregelen bij geconstateerde risico's, tezamen een aanvaardbaar risico vormen bij het gebruik van privacy gevoelige gegevens.

In de periode sept tot dec 2024 hebben 5.1.2e , 5.1.2e , 5.1.2e , 5.1.2e 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 'Camerahandhaving geslotenverklaringen' d.d. 10/12/2024. Deze versie vormt de onderlegger voor deze toetsing.

Bij deze DPIA horen de volgende bijlage:

- Verwerkersovereenkomst Brickyard

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?	Nee.	Akkoord.
2. Is het ethisch / politiek bestuurlijk verantwoord?	Ja. Deze DPIA ziet op de inzet van cameratoezicht bij de handhaving op de verschillende geslotenverklaringen binnen de gemeente Nijmegen. Dit cameratoezicht vindt op een aantal locaties binnen de gemeente Nijmegen plaats. Het gaat om de Griftdijk, de Eerste Walstraat, de Tweede Walstraat, de Waalkade, de Molenstraat en de van Welderenstraat. Gemotoriseerde voertuigen mogen deze straten (vanaf een bepaald tijdstip) niet inrijden. Het doel van deze geslotenverklaringen is het verbeteren van de leefbaarheid in de betreffende straten.	Akkoord. Vanwege het grote verkeersaanbod is fysiek handhaven op geslotenverklaringen slecht uitvoerbaar. De fysieke inzet op deze plaatsen kan sterk worden beperkt door de inzet van cameratoezicht.
3. Juridische toets 3.a. Doel / grondslag	3a. *Doel* van deze gegevensverwerkingen: . Het doel van de inzet van cameratoezicht is om het handhaven op deze geslotenverklaringen mogelijk te maken. *Grondslag* Deze verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang (art. 6, eerste lid, onder e, AVG). Het betreft dan de uitvoering van enkele taken onder de Wet administratiefrechtelijke handhaving verkeersvoorschriften (Wahv). Art. 2, eerste lid, Wahv bepaalt dat ten aanzien van de in de bijlage van de wet opgenomen gedragingen die in strijd zijn met de van toepassing zijnde verkeersregelgeving, een administratieve sanctie kan worden opgelegd. Voor de geslotenverklaringen betreft het dan feitcodes R 550A, R 559, R 551B en R 554A.	3a. Akkoord. Art. 3, eerste lid, W.a.h.v. bepaalt vervolgens dat met het toezicht op de naleving van deze voorschriften zijn belast de bij AMvB aangewezen ambtenaren. In de regeling Domeinlijsten buitengewoon opsporingsambtenaar wordt de buitengewoon opsporingsambtenaar vervolgens aangewezen als bevoegd om te handhaven op C-borden in relatie tot de leefbaarheid.
3.b. Persoonsgegevens Worden bijzondere persoonsgegevens verwerkt?	3.b. Nee. Wel is er sprake van het verwerken van strafrechtelijke gegevens. Binnen Brickyard worden het kenteken en het fotografisch materiaal verwerkt. Personen en kentekens (behalve dat van de overtreder) worden in het fotografisch materiaal geautomatiseerd onherkenbaar gemaakt zodra een bekeuring of waarschuwing is uitgeschreven. Als een waarschuwingsbrief moet worden verstuurd, worden aan Cannock Chase het kenteken, datum & tijdstip van overtreding verstrekt.	3.b. Akkoord. De camera's monitoren structureel de inritten bij de geslotenverklaringen. Gemaakte opnames van overtredingen worden vervolgens dagelijks door een Boa van de gemeente Nijmegen bekeken en beoordeeld. Als deze controle is uitgevoerd wordt een export gemaakt naar het CJIB voor het innen van een opgelegde sanctie. Als er een waarschuwing moet worden uitgeschreven, wordt er geautomatiseerd een export gemaakt naar Cannock Chase voor het versturen van een waarschuwingsbrief. Hier is dus sprake van een structurele uitwisseling van gegevens.

	Als er een boete moet worden uitgeschreven, worden aan het CJIB het kenteken, datum & tijdstip van overtreding verstrekt.	
3c. Proportionaliteit	3c. De inzet van cameratoezicht kan een behoorlijke inbreuk op de privacy van betrokkenen met zich brengen. Er zijn echter maatregelen genomen om deze inbreuk tot een minimum te beperken. Zo zijn de camera's gericht op de achterkant van het voertuig, waarbij betrokkene zelf meestal niet zichtbaar in beeld komt. Alle beelden en gegevens van niet-betrokkenen worden geanonimiseerd. Daarnaast worden de kentekens van niet-geverbaliseerde voertuigen direct verwijderd.	3c. Akkoord. Mocht het uitkijken van de beelden om enige reden niet mogelijk zijn, worden vastgelegde kentekens en fotografische opnames na 48 uur automatisch verwijderd.
3.d. Subsidiariteit	3.d. Om te kunnen handhaven op de geslotenverklaringen moet te zien zijn dat iemand een geslotenverklaring passeert. Een beeldopname van de auto en het kenteken zijn de daarvoor minimaal benodigde gegevens. Door bovengenoemde maatregelen beperkt de verwerking van persoonsgegevens zich grotendeels tot deze gegevens. Het kan voorkomen dat personen herkenbaar in beeld komen, maar deze worden automatisch geanonimiseerd.	3.d. Akkoord. De camera's leggen, in die gevallen waarin de geslotenverklaring alleen geldt tussen bepaalde tijdstippen, alleen tussen die tijdstippen beeldmateriaal vast.
3.e. Persoonsgegevens buiten EER gebruikt?	3.e. Neen.	3.e. Akkoord
3.f. Andere partijen betrokken?	3.f. De gemeente Nijmegen is als opdrachtgever verwerkingsverantwoordelijke. Brickyard is verwerker voor de gemeente Nijmegen. Cannock Chase is verwerker van Brickyard en dus subverwerker van gemeente Nijmegen. Het CJIB is zelfstandig verwerkingsverantwoordelijk, nu het zijn eigen wettelijke taak heeft.	3.f. Akkoord Met Brickyard is een verwerkersovereenkomst afgesloten. Deze is als bijlage toegevoegd.
3.g. Hoe lang worden gegevens bewaard en wijze van vernietiging?	3.g. *Bewaartermijn* De bewaartermijnen uit de Wpg zijn hier van toepassing. Overtredingsgegevens worden 5 jaar bewaard. 1 Jaar direct zichtbaar en de resterende 4 jaar alleen op specifieke zoektermen. Na 5 jaar worden de persoonsgegevens uit de overtredingen geanonimiseerd. *Vernietiging:* Het vernietigen van de gegevens gebeurt binnen dit portaal geautomatiseerd middels ingestelde parameters. Dit wordt ieder	Akkoord. Mocht er geen overtreding zijn, worden de fotografische opnames direct verwijderd. Mocht de beelden niet kunnen worden uitgekeken dan worden fotografische opnames en kentekens na 48 uur geautomatiseerd verwijderd.

	kwartaal gecontroleerd volgens de WPG. Dit gebeurt door de coördinator Parkeren en een collega die buiten het systeem staat.	
3.h. Hoe worden gegevens beveiligd?	3.h. In de handhavingsapplicatie kan alleen worden ingelogd met een persoonlijke gebruikersnaam en wachtwoord. Gebruikersaccounts worden aangemaakt door een applicatiebeheerder.	Akkoord. Alle bewerkingen en inzagen worden per proces-verbaal gelogd. Op deze logging vindt minimaal 2 x per jaar een controle plaats.
4. Risico's en voorgestelde maatregelen	Het kan voorkomen dat een kenteken verkeerd wordt gelezen door de camera's. Hierdoor kan een persoon ten onrechte een waarschuwing of proces-verbaal ontvangen. Om bovengenoemd risico te beperken worden naast het kenteken ook kenmerken van het voertuig weergegeven in de applicatie. De verbalisant zal deze gegevens met elkaar vergelijken om op het juiste kenteken een proces-verbaal uit te schrijven. Door menselijke fouten is het desondanks mogelijk dat een verkeerde persoon een bekeuring krijgt. Dit risico zal in vrijwel alle gevallen worden ondervangen doordat de medewerker van Toezicht en Handhaving de boete zal laten intrekken, nadat uit een gemaakt bezwaar of verzoek om inzage blijkt dat de boete aan de verkeerde persoon is uitgeschreven.	Akkoord. Opgepast moet worden dat er teveel op de techniek vertrouwd wordt. Deze is maar een hulpmiddel. Voorkomen moet worden dat te makkelijk de camerabeelden leidend zijn bij eventuele bezwaren. Tussenkomst van een medewerker is altijd noodzakelijk. Dit om zogenaamde 'Amsterdamse' toestanden (bekeuringen bleven doorgaan terwijl ze -achteraf- aantoonbaar foutief waren) te voorkomen. Daarnaast is het van belang dat het geven en intrekken van autorisaties ook minimaal 2 keer per jaar gecontroleerd wordt.

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 zelf kent een 'middelhoog' risico.
Namelijk: opgepast moet worden dat er teveel op de techniek vertrouwd wordt. Deze is maar een hulpmiddel. Voorkomen moet worden dat te makkelijk de camerabeelden leidend zijn bij eventuele bezwaren. Tussenkomst van een medewerker is altijd noodzakelijk. Dit om zogenaamde 'Amsterdamse' toestanden (bekeuringen bleven doorgaan terwijl ze -achteraf- aantoonbaar foutief waren) te voorkomen.

Eind 2025 zal deze DPIA op naleving getoetst worden.
Speciale aandacht zal gegeven worden aan:

- Alle bewerkingen en inzagen worden per proces-verbaal gelogd. Op deze logging vindt minimaal 2 x per jaar een controle plaats.
- Van belang is dat het geven en intrekken van autorisaties ook minimaal 2 keer per jaar gecontroleerd wordt
- Check op (wijze van) afhandeling van bezwaren.

Ik adviseer hiermee positief en daarmee zijn de resterende risico's 'aanvaardbaar'.

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

PK/19/12/2024. DPIA 102

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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

DPIA Oordeel FG gemeente Nijmegen

DPIA Preventie met Gezag

Inleiding

Hierbij het oordeel van de FG Gemeente Nijmegen over de DPIA ‘Preventie met Gezag’.
Gekozen is voor een systematische aanpak. Deze is terug te herleiden tot de oordeelsvorming van DPIA’s in het algemeen. In deze wordt het 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 welke weergeeft of m.i. het gehele voorstel van maatregelen én te nemen maatregelen bij geconstateerde risico’s, tezamen een aanvaardbaar risico vormen bij het gebruik van privacygevoelige gegevens.

In de periode nov 2024 tot feb 2025 hebben 5.1.2e , 5.1.2e , 5.1.2e , 5.1.2e , 5.1.2e 5.1.2e 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 ‘Preventie met Gezag’ d.d. 13/02/2024.
Deze versie vormt de onderlegger voor deze toetsing.

Bij deze DPIA horen de volgende bijlage:

- Bijlage 1. Plan van Aanpak Nijmegen incl begroting
- Bijlage 2. DEF. Samen sterk voor jeugd en veiligheid
- Bijlage 3. DEF. Convenant groepsaanpak jeugd Nijmegen
- Bijlage 4. DEF. Convenant Lokale Persoons Gerichte Aanpak Jeugd Nijmegen
- Bijlage 5. Collegevoorstel Preventie met Gezag nov 2023
- Bijlage 6. Raadsbrief toekenning middelen nov 2023
- Bijlage 7. DEF. Intentieverklaring jeugd
- Bijlage 8. Verwerkersovereenkomst Straatcontact
- Bijlage 9. DPIA PlusMinMee tool

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, deels. Niet voor dit gehele programma, wel voor het onderdeel betreffende de taken van het Zorg en Veiligheidshuis (ZVH). Daarnaast is er een DPIA gemaakt voor de applicatie PlusMinMee.	Akkoord. Zie bijlage DPIA PlusMinMee tool van de organisatie Straatcontact.
2. Is het ethisch / politiek bestuurlijk verantwoord?	Ja. Om te voorkomen dat jongeren en jongvolwassenen tot en met 27 jaar de (georganiseerde en ondermijnende) criminaliteit ingaan of hierin verder afglijden, zet het ministerie van Justitie en Veiligheid sinds een aantal jaar extra in op preventie en repressie bij de aanpak van jeugdcriminaliteit. Gemeente Nijmegen is één van gemeenten die is uitgenodigd om deel te nemen aan het Rijksprogramma Preventie met Gezag, om zo de voedingsbodem voor georganiseerde en ondermijnende criminaliteit weg te nemen, ervoor te zorgen dat jongeren en jongvolwassenen niet in deze criminaliteit belanden of hierin verder afglijden, en om reeds bestaande criminele organisaties waarin jongeren en jongvolwassenen actief zijn te ontwrichten.	Akkoord. Sinds januari 2024 is gestart met de uitvoering van een programma/plan van aanpak rondom de aanpak van jeugdcriminaliteit. Dit heet 'Perspectief voor onze jeugd' (bijlage 1). In het document 'Samen sterk voor jeugd en veiligheid' (bijlage 2) is uitgebreid beschreven hoe deze samenwerking/gezamenlijke werkwijze eruitziet. Het gaat o.a. om de volgende partners: gemeenten (regisseurs veiligheid, procesregisseurs, handhaving, leerrecht jeugdcoaches), jongerenwerk, lokale teams, HALT, politie, OM, (jeugd)reclassering. De scope van de DPIA is de Groepsaanpak en de Lokale persoonsgerichte aanpak (LPGA). De PGA ZVH heeft een eigen convenant en DPIA. Binnen het wijkoverleg wordt geen persoonsinformatie gedeeld, dus dit valt buiten de DPIA.
3. Juridische toets 3.a. Doel / grondslag	3a. *Doel* van deze gegevensverwerkingen: Het inrichten van de groepsaanpak en de LPGA zorgt ervoor dat signalen rondom jeugd-groepen en (beginnende) jeugdcriminaliteit tijdig gesignaleerd kan worden en er passende interventies ingezet kunnen worden. Hiermee wordt gezorgd voor verminderen van overlast in Nijmeegse wijken, vermindering van verstoring van de openbare orde en het voorkomen dat jongeren doorgroeien binnen het criminele circuit (en daardoor in onveilige situaties verkeren). *Grondslag* a. De burgemeester voor de uitoefening van zijn wettelijke taken en bevoegdheden op het terrein van de handhaving van de openbare orde bij of krachtens hoofdstuk XI van titel III van de Gemeentewet, paragraaf 2.3 van de Politiewet 2012, artikel 13b van de Opiumwet of een gemeentelijke verordening en voor de uitoefening van zijn wettelijke taken en bevoegdheden bij of krachtens de Wet tijdelijk huisverbod en de artikelen 7:1, 7:2, 7:4 en 8:1 van de Wet verplichte geestelijke gezondheidszorg en de artikelen 29 tot en met 36 van de Wet zorg en dwang	3a. Akkoord. De groepsaanpak en Lokale Persoonsgerichte Aanpak Jeugd (LPGA) worden opgezet vanuit het programma 'Perspectief voor onze jeugd'/ Preventie met Gezag. Het programmaplan 'Perspectief voor onze Jeugd'/ Preventie met Gezag (bijlage 1) is vastgesteld door het college van B&W (zie bijlage 5 voor het collegevoorstel en bijlage 6 voor de raadsbrief). De gemeente Nijmegen ontvangt Rijksmiddelen ter uitvoering van dit plan. In de DPIA staan ook de wettelijke grondslagen voor de andere deelnemende partners opgenomen.

	psychogeriatrische en verstandelijk gehandicapte cliënten; b. Het college van burgemeester en wethouders voor de uitoefening van zijn wettelijke taken en bevoegdheden bij of krachtens de artikelen 2.1.1, eerste lid, 2.1.7, 2.3.1 tot en met 2.3.6, 2.3.9, 2.3.10 en 2.4.1 van de Wet maatschappelijke ondersteuning 2015, de artikelen 2.3 en 2.4 van de Jeugdwet, artikel 7 van de Participatiewet, artikel 3 van de Wet gemeentelijke schuldhulpverlening, artikel 16 van de Leerplichtwet 1969 en de wettelijke taken en bevoegdheden, bedoeld in de artikelen 5:1, 5:2, 5:3 en 5:16 van de Wet verplichte geestelijke gezondheidszorg, artikel 28c van de Wet zorg en dwang psychogeriatrische en verstandelijk gehandicapte cliënten en artikel 2:7 van het Besluit tenuitvoerlegging strafrechtelijke beslissingen.	
3.b. Persoonsgegevens Worden bijzondere persoonsgegevens verwerkt?	3.b. Ja, er worden bijzondere en/of strafrechtelijke persoonsgegevens van het casussubject (en personen uit diens huishouden) verwerkt. Partijen verwerken bijzondere persoonsgegevens enkel binnen de wettelijke kaders van de voor iedere partij toepasselijke wet- en regelgeving.	3.b. Akkoord. NB. Voor de Groepsaanpak (art. 10 convenant) en voor de LPGA (art. 7 convenant) zijn in de DPIA overzichten opgenomen van de diverse persoonsgegevens die verwerkt worden.
3c. Proportionaliteit	3c. De noodzakelijk te verwerken gegevens verschillen per fase. Het werkproces (zie bijlage 2) is er daarom in voorzien dat er per fase een afweging wordt gemaakt door de procesregisseur in samenspraak met de verstrekkende partij over de benodigde gegevens en te betrekken partijen. Daarbij zijn afspraken gemaakt over de wijze waarop gegevens slechts voor zover noodzakelijk en evenredig verwerkt worden. Op die manier is in het werkproces verankerd dat steeds opnieuw een noodzakelijkheidsafweging plaatsvindt omtrent de te verstrekken gegevens. Er wordt rekening gehouden met dataminimalisatie. Het uitgangspunt van de groepsaanpak en de LPGA is dat de aanmeldende partij met problemen wordt geconfronteerd die ertoe nopen de samenwerking te zoeken met deelnemers van de aanpakken. De noodzaak hiertoe kan per partij verschillen, en vergt een afweging van de aanmeldende partij voorafgaand aan de daadwerkelijke aanmelding. De procesregisseur velt hierover, o.b.v. de aangeleverde informatie, een oordeel en neemt een besluit of de casus wel of niet	3c. Akkoord, mits….. Hier moet opgemerkt worden dat de rol van procesregisseur een cruciale, maar óók een kwetsbare is. In de audit van het Veiligheidshuis is hierover geconcludeerd: “De rol van de procesregisseur in het casusoverleg is veelomvattend. Het leiden van de vergadering, sturen op afronding van casuïstiek én ondertussen zicht houden op (onnodige) verrijkingen van ketenpartners is veel. Geadviseerd wordt om te onderzoeken of het brede takenpakket van de procesregisseur in de praktijk leidt tot onrechtmatige informatiedeling tijdens het casusoverleg.” Citaat uit rapportage Audit ZVH sept 2022. Bezien moet worden of ook in dit kader naar het takenpakket van de procesregisseur gekeken moet worden. Voorkomen moet worden dat de intenties goed zijn, maar dat deze in de praktijk door de drukke werkzaamheden van de procesregisseur tot ongewenste effecten leiden (nl. ‘onrechtmatige informatiedeling tijdens het casusoverleg’).

	besproken gaat worden o.b.v. de problematiek.	
3.d. Subsidiariteit	3.d. Voor zowel de groepsaanpak als de LPGA geldt dat samenwerking tussen meerdere partijen noodzakelijk is om tot een effectieve aanpak te komen en daarmee de overlast en/of het probleemgedrag te doen verminderen. Het is in de reguliere samenwerking tussen partners, zonder uitwisseling van persoonsinformatie, niet mogelijk gebleken om deze problematiek effectief aan te pakken.	3.d. Akkoord. Binnen deze werkwijze is de procesregisseur is de bewaker van dataminimalisatie.
3.e. Persoonsgegevens buiten EER gebruikt?	3.e. Neen.	3.e. Akkoord
3.f. Andere partijen betrokken?	3.f. Groepsaanpak (zie art. 5 convenant): De gemeente Nijmegen (procesregisseurs) is verwerkingsverantwoordelijke in de zin van artikel 26 lid 1 AVG voor de verwerkingen in het registratiesysteem Pluminmee. LPGA (zie art. 4 convenant): De procesregisseurs verwerken persoonsgegevens in het kader van het convenant onder het gezag en de gezamenlijke verwerkingsverantwoordelijkheid van de partners.	3.f. Akkoord Met Straatcontact is een verwerkersovereenkomst afgesloten. Deze is als bijlage toegevoegd. Elke deelnemende partner is verantwoordelijk voor de gegevens die zij zelf verwerkt in het kader van deze werkwijze. Zie hiervoor is een overzicht gemaakt in paragraaf ‘5.2. Rollen van deelnemende partners’ van de DPIA.
3.g. Hoe lang worden gegevens bewaard en wijze van vernietiging?	3.g. *Bewaartermijn* Persoonsgegevens in het bestand worden niet langer bewaard dan noodzakelijk voor het doel of de doeleinden waarvoor ze worden verwerkt. *Vernietiging:* Persoonsgegevens in het bestand worden verwijderd zodra de verwerking daarvan niet langer nodig is voor het doel waarvoor zij zijn verwerkt, maar uiterlijk binnen 1 jaar na het vervallen van dat doel.	Akkoord. De manager van bureau Veilige en Zorgzame Stad is eindverantwoordelijk voor het bewaken van de vastgestelde termijnen en afspraken met betrekking tot gegevensvernietiging en – opslag. In de dagelijkse praktijk zijn de procesregisseurs verantwoordelijk voor de vernietiging van de gegevens. Tijdig verwijderen van gegevens: Elk halfjaar wordt hierop een check uitgevoerd door de procesregisseurs.
3.h. Hoe worden gegevens beveiligd?	3.h. Voor de groepsaanpak wordt gewerkt met applicaties PlusMinMee. Voor de LPGA gewerkt met de applicatie PgaX. Dit is een applicatie die momenteel ook al door de gemeente gebruikt wordt, onder andere bij het Zorg- en Veiligheidshuis.	Akkoord. Zie bijlage 9 voor de DPIA waarin staat beschreven hoe deze applicatie is beveiligd. Deze applicatie beschikt o.a. over een tweefactor-authenticatie. Deelnemers worden door de beheerder toegevoegd aan een casus.
4. Risico’s en voorgestelde maatregelen	Risico’s zijn beschreven in de DPIA: Er kan verschil van mening blijven bestaan tussen de jongeren binnen de groep en	Akkoord. Geadviseerd wordt na te gaan hoe vaak dit probleem zich voordoet en welke interventies

	partners over het wel of niet zijn van een overlastgevende / problematische jeugdgroep. Autorisaties zijn persoonsgebonden. Collega's kunnen dus niet zonder meer inloggen. Collega's worden door de procesregisseurs geautoriseerd (verstrekken autorisatie én intrekken autorisatie).	dan afdoende zijn om te voorkomen dat dit probleem blijft bestaan. Het aan- en afmelden van autorisaties van ketenpartners gebeurt handmatig door de procesregisseurs. Wanneer iemand wordt geautoriseerd voor PgaX en PlusMinMee wordt iemand geautoriseerd voor afzonderlijke casuïstiek en niet voor alle casuïstiek van een locatie.

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 een 'middelhoog' risico.
Dit betreft processen waarin veel (vaak bijzondere) persoonsgegevens verwerkt worden met meerdere partijen aan tafel ieder met een eigen verantwoordelijkheid.
Hier betreft het de verantwoordelijkheid van de gemeente Nijmegen om vanuit de rol van procesregisseur gegevens te verwerken binnen de applicaties PlusMinMee (voor de groepsaanpak) en PGAx (voor de Lokale Persoonsgerichte Aanpak Jeugd). En daarnaast, toe te zien op dataminimalisatie in de gehele procesaanpak.

Geadviseerd wordt om te onderzoeken of het brede takenpakket van de procesregisseur in de praktijk leidt tot onrechtmatige informatiedeling tijdens het casusoverleg (conform advies auditrapportage ZVH).

Geadviseerd wordt na te gaan hoe vaak het probleem zich voordoet dat er verschil van mening blijft bestaan tussen de jongeren binnen de groep en partners over het wel of niet zijn van een overlast gevende / problematische jeugdgroep.
En uit te zoeken welke interventies dan afdoende zijn om te voorkomen dat dit probleem blijft bestaan.

Eind 2025 zal deze DPIA op naleving getoetst worden.
Speciale aandacht zal gegeven worden aan:
De rol van de procesregisseur bij het verwerken van de gegevens in de beide applicaties en het toezien op dataminimalisatie binnen de gehele procesgang.

Ik adviseer hiermee positief en daarmee zijn de resterende risico's 'aanvaardbaar'.

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

PK/20/02/2025. DPIA 103

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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

DPIA Oordeel FG gemeente Nijmegen

DPIA Kandidaat Raadsleden

Inleiding

Hierbij het oordeel van de FG Gemeente Nijmegen over de DPIA 'Kandidaat Raadsleden'.
Gekozen is voor een systematische aanpak. Deze is terug te herleiden tot de oordeelsvorming van DPIA's in het algemeen. In deze wordt het 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 welke weergeeft of m.i. het gehele voorstel van maatregelen én te nemen maatregelen bij geconstateerde risico's, tezamen een aanvaardbaar risico vormen bij het gebruik van privacygevoelige gegevens.

In de periode sept 2024 tot feb 2025 hebben 5.1.2e , 5.1.2e , 5.1.2e 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 'Kandidaat Raadsleden' d.d. 03/02/2025.
Deze versie vormt de onderlegger voor deze toetsing.

Bij deze DPIA horen de volgende bijlage:

- Landscape You Force

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, ten dele	Akkoord. Er is DPIA Arbeidsovereenkomst HRM Systemen gemaakt en beoordeeld in 2024. Een deel van de uitvoering van het proces geschetst in deze DPIA volgt het geschetste proces van de arbeidsovereenkomst.
2. Is het ethisch / politiek bestuurlijk verantwoord?	Ja. Het kunnen laten starten van de uiteindelijk verkozen raadsleden met het raadswerk, voorzien van alle zaken die daarvoor nodig zijn.	Akkoord. Het betreft een eenvoudig proces die kandidaat raadsleden reeds registreert vóórdat zij wel of niet verkozen zijn.
3. Juridische toets 3.a. Doel / grondslag	3a. *Doel* van deze gegevensverwerkingen: Proces zorgt voor een snelle verwerking van de gegevens en daarmee verkrijgen van benodigde devices, voorafgaand aan installatie. *Grondslag* Deze verwerking is gebaseerd op toestemming van de betrokkene	3a. Akkoord. Hiermee kunnende nieuw verkozen raadsleden direct starten en hoeven zij niet een periode te wachten na verkozen te zijn, om hun raadswerk naar behoren te doen.
3.b. Persoonsgegevens Worden bijzondere persoonsgegevens verwerkt?	3.b. Nee. Betreft NAW-gegevens.	3.b. Akkoord.
3c. Proportionaliteit	3c. Minimale gegevensverwerking.	3c. Akkoord. Kandidaat raadsleden die níet verkozen zijn hebben wel toestemming gegeven voor verwerking van hun gegevens. Deze worden verwijderd indien niet verkozen.
3.d. Subsidiariteit	3.d. Reden is gelegen in snel verkrijgen van benodigd materiaal voor de raadsleden en Efficiencywinst in het ambtelijk voorbereidingsproces.	3.d. Akkoord.
3.e. Persoonsgegevens buiten EER gebruikt?	3.e. Neen.	3.e. Akkoord
3.f. Andere partijen betrokken?	3.f. De Gemeente Nijmegen is verantwoordelijk voor het verwerken van de persoonsgegevens. Youforce: verwerkt de gegevens. Kandidaatsraadslid: levert de persoonsgegevens aan.	3.f. Akkoord Zie DPIA Arbeidsovereenkomst / HRM Systemen. Er is een verwerkersovereenkomst met Youforce.
3.g. Hoe lang worden gegevens bewaard en wijze van vernietiging?	3.g. *Bewaartermijn* De gegevens worden gedurende het raadlidmaatschap bewaard. Na einde van het raadlidmaatschap nog 5 jaar conform archiefwet.	Akkoord. De medewerkers betrokken bij verwerking gegevens in Youforce dragen hier zorg voor.

	Belastingtechnische gegevens nog 7 jaar. *Vernietiging:* na beëindiging van de bewaartermijnen.	NB. Gegevens van niet gekozen raadsleden dienen meteen na de uitslag te worden verwijderd.
3.h. Hoe worden gegevens beveiligd?	3.h. Beveiliging vindt plaats door dagelijkse back-ups. Voor de software die binnen het gemeentenetwerk staat wordt dit verzorgd door het IRVN. Voor het Cloud gedeelte wordt dit gedaan door Visma RAET, de leverancier. Toegang tot de systemen is via autorisatierollen geregeld. Van wijzigingen vindt logging plaats	Akkoord. Toegang tot de systemen is via autorisatierollen geregeld. Van wijzigingen vindt logging plaats.
4. Risico's en voorgestelde maatregelen	Het risico tot verkeerd overnemen van de gegevens wordt op deze nieuwe wijze van werken al verkleind. Bij de huidige manier van werken (invoeren gegevens van de verkozen raadsleden) moet er zoveel werk worden verzet in zo weinig tijd dat het risico op het fout overnemen van gegevens veel groter is. Doordat dit werk nu voor een deel naar voren wordt gehaald, is er meer ruimte voor controle en wordt het risico dus al verkleind.	Akkoord.

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 zelf kent een 'laag' risico.
Ik adviseer hiermee positief en daarmee zijn de resterende risico's 'aanvaardbaar'.

Eind 2025 zal deze DPIA op naleving getoetst worden.
NB. Gegevens van niet gekozen raadsleden dienen meteen na de uitslag te worden verwijderd.

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

PK/10/03/2025. DPIA 104

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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

DPIA Oordeel FG gemeente Nijmegen

DPIA 105 Camerabewaking Zero Emissie Zones

Inleiding

Hierbij het oordeel van de FG Gemeente Nijmegen over de DPIA 'Camerabewaking Zero Emissie Zones'
Gekozen is voor een systematische aanpak. Deze is terug te herleiden tot de oordeelsvorming van DPIA's in het algemeen. In deze wordt het 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 welke weergeeft of m.i. het gehele voorstel van maatregelen én te nemen maatregelen bij geconstateerde risico's, tezamen een aanvaardbaar risico vormen bij het gebruik van privacygevoelige gegevens.

In de periode sept 2024 tot maart 2025 hebben 5.1.2e , 5.1.2e en 5.1.2e 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 'Camerabewaking Zero Emissie Zones' d.d. 20/03/2025.
Deze versie vormt de onderlegger voor deze toetsing.

Bij deze DPIA horen de volgende bijlage:

- Verwerkersovereenkomst Brickyard.

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, er is al een DPIA op de (reguliere) geslotenverklaringen.	Akkoord. Betreft DPIA 102 Camerahandhaving geslotenverklaringen dd 15-12-2024.
2. Is het ethisch / politiek bestuurlijk verantwoord?	Ja. Op 10 september 2024 is het Verkeersbesluit nul-emissiezone bedrijfs- en vrachtauto's binnenstad Nijmegen, Hof van Holland en Campus Heijendaal vastgesteld. In 3 zones in Nijmegen geldt een nul-emissie voor bedrijfsvoertuigen. Dit betekent dat vrachtauto's en bedrijfsbussen die een verbrandingsmotor hebben die zones niet in mogen rijden.	Akkoord. In de DPIA staat vermeld: "Voor de gemeente is het lastig om dit in persoon op alle locaties te handhaven. Daarom is ervoor gekozen om met camera's toezicht te houden op deze geslotenverklaringen. Als iemand de geslotenverklaring negeert, wordt er een foto van het voertuig gemaakt. Op basis van die foto wordt er een waarschuwing gegeven of een boete uitgeschreven."
3. Juridische toets 3.a. Doel / grondslag	3a. *Doel* van deze gegevensverwerkingen: Het doel van deze geslotenverklaringen is het verminderen van emissies door vrachtverkeer ter verbetering van de luchtkwaliteit en leefbaarheid. Het handhaven van de Zero Emissie (ZE)-zones is hier een onderdeel van. *Grondslag* Deze verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang (art. 6, eerste lid, onder e, Avg). Het betreft dan de uitvoering van enkele taken onder de Wet administratiefrechtelijke handhaving verkeersvoorschriften (Wahv). Art. 2, eerste lid. Voor de geslotenverklaringen vanwege een Milieuzone betreft het feitcodes R 571 g en R 571 h. art. 3, eerste lid, Wahv bepaalt vervolgens dat met het toezicht op de naleving van deze voorschriften zijn belast de bij amvb aangewezen ambtenaren	3a. Akkoord. Om de fysieke inzet te beperken is ervoor gekozen om dit middels camerahandhaving te doen In de regeling Domeinlijsten buitengewoon opsporingsambtenaar wordt de buitengewoon opsporingsambtenaar vervolgens aangewezen als bevoegd om te handhaven op C-borden in relatie tot de leefbaarheid.
3.b. Persoonsgegevens Worden bijzondere persoonsgegevens verwerkt?	3.b. Nee. Wel is er sprake van het verwerken van gegevens die onder de Wet Politiegegevens (Wpg) vallen.	3.b. Akkoord. Deze DPIA dient ook meegenomen te worden in de (jaarlijkse) Audit Wpg.
3c. Proportionaliteit	3c. De inzet van cameratoezicht kan een behoorlijke inbreuk op de privacy van betrokkenen met zich brengen. Er zijn echter maatregelen genomen om deze inbreuk tot een minimum te beperken. Zo zijn de camera's gericht op de achterkant van het voertuig, waarbij betrokkene zelf meestal niet zichtbaar in beeld komt. Verder worden alleen de kentekens en het beeldmateriaal van voertuigen waarvan middels de geautomatiseerde check is vastgesteld dat zij	3c. Akkoord. In de DPIA wordt onder de kop 'achtergronden" de procesgang beschreven in een vijftal controles. Hierin worden de voertuigen min of meer gescreend op de kenmerken die nodig zijn voor de uiteindelijke beoordeling: het identificeren van vrachtauto's en bedrijfsbussen die een verbrandingsmotor hebben en die dus niet deze zones mogen in rijden. Hier staat ook vermeld: "Alle overige ontvangen informatie van voertuigen die zijn gepasseerd

	binnen de verboden categorie vallen en niet over een ontheffing beschikken, uitgekeken door de BOA.	wordt binnen 24 uur weer verwijderd uit het systeem.”
3.d. Subsidiariteit	3.d. Voor handhaving moet te zien zijn dat iemand een geslotenverklaring passeert en moet die persoon te identificeren zijn. Een beeldopname van de auto en het kenteken zijn de daarvoor minimaal benodigde gegevens. Het kan voorkomen dat personen herkenbaar in beeld komen, maar deze worden automatisch geanonimiseerd.	3.d. Akkoord. Een alternatief zou zijn om fysiek te handhaven, maar het is niet haalbaar om 24/7 aanwezig zijn op alle plekken waar het gebied ingereden kan worden. NB: het gebied wordt omschreven in de DPIA onder paragraaf 1.
3.e. Persoonsgegevens buiten EER gebruikt?	3.e. Neen.	3.e. Akkoord
3.f. Andere partijen betrokken?	3.f. De gemeente Nijmegen is opdrachtgever. Brickyard levert het handhavingssysteem waarin de foto’s worden opgeslagen. Als er een waarschuwingsbrief moet worden verstuurd, worden de gegevens vanuit het handhavingssysteem gedeeld met Cannock Chase. Cannock Chase verstuurt vervolgens de waarschuwingsbrief. Indien er een bekeuring wordt opgelegd worden de gegevens van betrokkene gedeeld met het CJIB voor het innen van de boete.	3.f. Akkoord Er is een verwerkersovereenkomst met Brickyard, zie bijlage. Brickyard heeft voor de verwerkingen in het kader van het versturen van de waarschuwingsbrieven een verwerkersovereenkomst met Cannock Chase.
3.g. Hoe lang worden gegevens bewaard en wijze van vernietiging?	3.g. *Bewaartermijn* De bewaartermijnen uit de Wpg zijn hier van toepassing. Overtredingsgegevens worden 5 jaar bewaard. 1 Jaar direct zichtbaar en de resterende 4 jaar alleen op specifieke zoektermen. Na 5 jaar worden de persoonsgegevens uit de overtredingen geanonimiseerd. Belastingtechnische gegevens nog 7 jaar. *Vernietiging:* Mocht er geen overtreding zijn, worden de fotografische opnames direct verwijderd. Mocht de beelden niet kunnen worden uitgekeken dan worden fotografische opnames en kentekens na 48 uur geautomatiseerd verwijderd.	Akkoord. Het vernietigen van de gegevens gebeurt binnen de handhavingsapplicatie geautomatiseerd middels ingestelde parameters. Dit wordt ieder kwartaal gecontroleerd volgens de Wpg. Dit gebeurt door de coördinator Parkeren en een collega die buiten het systeem staat.
3.h. Hoe worden gegevens beveiligd?	3.h. Er kan alleen worden ingelogd met een persoonlijke gebruikersnaam en wachtwoord. Alle bewerkingen en inzagen worden per proces-verbaal gelogd. Op deze logging vindt minimaal 2 x per jaar een controle plaats. Toegang tot de systemen is via autorisatierollen geregeld. Van wijzigingen vindt logging plaats	Akkoord. Gebruikersaccounts worden aangemaakt door een applicatiebeheerder. Deze maakt alleen een account aan voor beëdigd boa’s. De administratief medewerkers bij Toezicht en Handhaving zijn geen Boa, maar zij hebben een “verklaring verwerking persoonsgegevens niet-Boa” ondertekend

4. Risico's en voorgestelde maatregelen	Het kan voorkomen dat een kenteken verkeerd wordt gelezen door de camera's. Hierdoor kan een persoon ten onrechte een waarschuwing of proces-verbaal ontvangen. Om dit risico te beperken worden naast het kenteken ook kenmerken van het voertuig weergegeven in de applicatie. De verbalisant zal deze gegevens met elkaar vergelijken om op het juiste kenteken een proces-verbaal uit te schrijven.	Akkoord. De medewerker van Toezicht en Handhaving zal de boete laten intrekken, als uit een gemaakt bezwaar of verzoek om inzage blijkt dat de boete aan de verkeerde persoon is uitgeschreven.

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 zelf kent een 'laag' risico.
Ik adviseer hiermee positief en daarmee zijn de resterende risico's 'aanvaardbaar'.

Eind 2025 zal deze DPIA op naleving getoetst worden.

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

PK/10/04/2025. DPIA 105.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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

DPIA Oordeel FG gemeente Nijmegen

DPIA Behandelen inzageverzoeken

Inleiding

Hierbij het oordeel van de FG Gemeente Nijmegen over de DPIA ‘Behandelen inzageverzoeken’.
Gekozen is voor een systematische aanpak. Deze is terug te herleiden tot de oordeelsvorming van DPIA’s in het algemeen. In deze wordt het 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 welke weergeeft of m.i. het gehele voorstel van maatregelen én te nemen maatregelen bij geconstateerde risico’s, tezamen een aanvaardbaar risico vormen bij het gebruik van privacygevoelige gegevens.

In de periode dec 2024 tot april 2025 hebben 5.1.2e , 5.1.2e , 5.1.2e 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 ‘Behandelen inzageverzoeken’ d.d. 08/04/2025.
Deze versie vormt de onderlegger voor deze toetsing.

Bij deze DPIA horen de volgende bijlage:

- Verwerkersovereenkomst IRvN

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?	Neen.	Akkoord.
2. Is het ethisch / politiek bestuurlijk verantwoord?	Ja. Gemeenten voeren een groot scala aan taken uit, waarbij zij in veel gevallen persoonsgegevens verwerken. Betrokkenen hebben op grond van art. 15 AVG recht op inzage in hun persoonsgegevens. Daartoe kunnen zij een verzoek bij de gemeente indienen. Om deze verzoeken af te kunnen handelen, is een intern werkproces opgezet om de betreffende persoonsgegevens te verzamelen. In dat proces worden – uiteraard – persoonsgegevens verwerkt.	Akkoord. Deze DPIA ziet op de verwerkingen van persoonsgegevens bij het afhandelen van inzageverzoeken. In hoofdzaak gaat het dan om drie verwerkingen: 1. Het vaststellen van de identiteit van verzoeker; 2. Het verzamelen van de persoonsgegevens; 3. Het verstrekken van de persoonsgegevens aan verzoeker. Het verwijderen van persoonsgegevens valt buiten de reikwijdte van deze DPIA.
3. Juridische toets 3.a. Doel / grondslag	3a. *Doel* van deze gegevensverwerkingen: Het doel van de verwerking is het verschaffen van inzage van zijn persoonsgegevens aan de betrokkene die daar om verzoekt.. *Grondslag* De grondslag is gelegen in een wettelijke verplichting onder art. 15 AVG om betrokkene inzage te verschaffen in zijn persoonsgegevens. De grondslag voor het verwerken van persoonsgegevens bij het vaststellen van de identiteit van betrokkene is gelegen in art. 12, zesde lid, AVG.	Akkoord.
3.b. Persoonsgegevens Worden bijzondere persoonsgegevens verwerkt?	3.b. Betrokkenen kunnen verzoeken om inzage in alle persoonsgegevens die de gemeente Nijmegen van hen verwerkt. In theorie kan dit dus elke categorie persoonsgegevens betreffen. Het kan dan o.a. gaan om: - NAW-gegevens; - Geboortedatum; - Geboorteplaats; - Burgerservicenummer (BSN); - Nationaliteit; - Gegevens over de gezondheid; - Financiële gegevens. - Contactgegevens.	Akkoord. NB.: Bij het behandelen van inzageverzoeken kunnen bijzondere persoonsgegevens worden verwerkt. Daarbij valt met name te denken aan gegevens over de gezondheid van betrokkenen, die bijvoorbeeld worden verwerkt in het kader van de Participatiewet of de Wet maatschappelijke ondersteuning (Wmo).
3c. Proportionaliteit	3c. Het doen van een inzageverzoek door betrokkene en de behandeling van dat verzoek door de medewerker brengen een inbreuk op de privacy van betrokkene met zich. In de eerste plaats zal betrokkene zich moeten identificeren.	Akkoord. In principe door middel van een digitaal identificatiemiddel, door toezending van een digitale kopie van het identiteitsbewijs of door het verschijnen in persoon.

	In de tweede plaats zal de behandelend medewerker alle persoonsgegevens van de betrokkene moeten verzamelen en beoordelen. Het doen van een inzageverzoek stelt de betrokkene in staat om te controleren of de gemeente op rechtmatige wijze persoonsgegevens van de betrokkene verwerkt. Dat belang weegt zwaar; het is één van de basisrechten van de betrokkene onder de AVG.	Hoewel de behandeling van een inzageverzoek dus een significante inbreuk op de privacy van betrokkene met zich brengt, weegt dat op tegen het belang (voor de aanvrager) dat daarmee is gemoeid.
3.d. Subsidiariteit	3.d. Om de betrokkene inzage in zijn persoonsgegevens te kunnen geven, zullen die gegevens door een medewerker verzameld moeten worden. Die verwerking gaat daarbij niet verder dan noodzakelijk, zolang slechts die gegevens worden verzameld waarvan betrokkene om inzage verzoekt. In dat verband zal bij een 'breed' inzageverzoek (waarbij betrokkene verzoekt om ál zijn persoonsgegevens) contact worden gezocht met de betrokkene om zijn verzoek zo goed mogelijk te specificeren. Het is immers denkbaar dat betrokkene lijkt te vragen om inzage in al zijn persoonsgegevens, maar eigenlijk alleen op zoek is naar (bijvoorbeeld) zijn bijstandsdossier.	Akkoord. Door contact te hebben met verzoeker over zijn verzoek kan worden voorkomen dat onnodig grote hoeveelheden persoonsgegevens worden verzameld.
3.e. Persoonsgegevens buiten EER gebruikt?	3.e. Neen.	Akkoord.
3.f. Andere partijen betrokken?	3.f. De gegevens worden verzameld, beoordeeld en verstrekt door (medewerkers van) de gemeente Nijmegen. Bij brede inzageverzoeken wordt zij daarbij ondersteund door de IRvN.	Akkoord. Tussen de gemeente Nijmegen en de IRvN is een verwerkersovereenkomst gesloten.
3.g. Hoe lang worden gegevens bewaard en wijze van vernietiging?	3.g. *Bewaartermijn* De gegevens waarvan om inzage wordt gevraagd worden bewaard tot het verstrijken van de bewaartermijn die voor de betreffende gegevens geldt. Dit is dus afhankelijk van de specifieke bewaartermijnen die op de betreffende gegevens van toepassing zijn. De documenten die voor het inzageverzoek verzameld worden, worden in het geval van een breed inzageverzoek tijdelijk opgeslagen op de g-schijf. *Vernietiging:* Het besluit en de documenten worden minimaal één jaar bewaard.	Akkoord. In de praktijk ligt de verantwoordelijkheid voor het vernietigen van de documenten (zowel in de Teams-map en op de g-schijf) bij team privacy.

3.h. Hoe worden gegevens beveiligd?	3.h. Zowel de map op Teams als op de g-schijf zijn besloten. Daarvoor zijn alleen de noodzakelijke medewerkers geautoriseerd. Er vindt geen logging plaats. Voor toegang tot de g-schijf moet wel ingelogd worden via Citrix, en dus vindt er een check plaats op het Active Directory (AD).	Akkoord. Advies: Eens per jaar actief de autorisaties opnieuw beoordelen.
4. Risico's en voorgestelde maatregelen	- (Onnodig) bewaren van kopieën van identiteitsbewijzen; - Onnodig verzamelen van persoonsgegevens; - Dubbele opslag van persoonsgegevens; - Verstrekking van de persoonsgegevens; - Onnodig bewaren van de mappen die aan betrokkenen zijn verstrekt; - Het risco dat documenten naar een verkeerd emailadres worden verstuurd.	Akkoord. Bij de rapportage over de naleving van deze DPIA dient actief gecommuniceerd te worden hoe vaak de genoemde risico's zich hebben voorgedaan in het afgelopen jaar.

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 zelf kent een 'laag' (bij een specifieke inzageverzoek) tot 'middelhoog' risico (bij een breed inzageverzoek.
Met name bij dit brede verzoek komen diverse (bijzondere) persoonsgegevens bij elkaar en heb je bijna een compleet beeld van een persoon. Met het genoemde risico van een verzending aan een verkeerd mailadres, acht ik het risico middelhoog.

Ik adviseer hiermee positief en daarmee zijn de resterende risico's 'aanvaardbaar'.

Eind 2025 zal deze DPIA op naleving getoetst worden.
Advies: Eens per jaar actief de autorisaties opnieuw beoordelen.
Bij de rapportage over de naleving van deze DPIA dient actief gecommuniceerd te worden hoe vaak de genoemde risico's zich hebben voorgedaan in het afgelopen jaar.

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

PK/17/04/2025. DPIA 106

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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

DPIA Oordeel FG gemeente Nijmegen

DPIA Corsa 2025

Inleiding

Hierbij het oordeel van de FG Gemeente Nijmegen over de DPIA 'Corsa 2025'.
Gekozen is voor een systematische aanpak. Deze is terug te herleiden tot de oordeelsvorming van DPIA's in het algemeen. In deze wordt het 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 welke weergeeft of m.i. het gehele voorstel van maatregelen én te nemen maatregelen bij geconstateerde risico's, tezamen een aanvaardbaar risico vormen bij het gebruik van privacygevoelige gegevens.

In de periode april 2024 tot april 2025 hebben 5.1.2e, 5.1.2e, 5.1.2e, 5.1.2e, 5.1.2e 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 'Corsa 2025' d.d. 11/04/2025.
Deze versie vormt de onderlegger voor deze toetsing.

Bij deze DPIA horen de volgende bijlage:

- Vertrouwelijkheidsgroepen Corsa overzicht
- Instructie toekennen autorisaties en vertrouwelijkheidsgroepen
- Afspraken toekennen autorisaties en vertrouwelijkheidsgroepen
- Werkwijze afsluiten en vernietigen digitale dossiers
- Procesbeschrijving vernietiging
- Overdracht aan BDI Corsa AVG
- Budgetverschuiving voor gemeentelijke voorziening DIVA
- GMT voorstel Corsa AVG proof 18 november 2020
- Quick PIA Corsa gemeente Nijmegen december 2018

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, er is in 2018 een Quick Pia gemaakt. Hierin zijn diverse tekortkomingen gesignaleerd waarvan geadviseerd werd, deze zo spoedig mogelijk aan te pakken. Dit proces ging te langzaam, waarop de FG heeft geïntervenieerd. De belangrijkste tekortkomingen: Veel persoonsgegevens in registraties en documenten zijn te zien door medewerkers die dit vanuit de AVG niet mogen zien, er wordt te veel persoonsgegevens vastgelegd en persoonsgegevens worden te lang bewaard.	Akkoord. Quick PIA (zie bijlage). In november 2020 is vanuit de rol FG een dringend advies gegeven om de problematiek rondom Corsa aan te pakken (zie bijlage GMT voorstel Corsa AVG proof 18 november 2020). Corsa was níet AVG-proof. Deze DPIA beschrijft de nieuwe werkwijze waarin 'voldoen aan de AVG' de norm is geworden.
2. Is het ethisch / politiek bestuurlijk verantwoord?	Ja. De verwerking van persoonsgegevens in het generieke RMA/DMS systeem Corsa is noodzakelijk voor de behandeling van aanvragen van ongeveer 400 processen. Corsa ondersteunt ofwel het hele proces van behandeling, ofwel alleen de opslag van documenten en bestanden in zaakdossiers, waarbij de rest van het proces ondersteund wordt door een specifieke procesapplicatie. Onderdeel van deze ondersteuning is de registratie van aanvragen en andere documenten die door inwoners of bedrijven opgestuurd worden, het doorzetten naar behandelaars, het vormen van dossiers, het bieden van zoekmogelijkheden en het op tijd vernietigen na afsluiting (of permanent bewaren).	Akkoord. Een generiek RMA/DMS systeem is nodig omdat niet voor ieder proces van de gemeente Nijmegen een eigen specifieke procesapplicatie beschikbaar is en als deze beschikbaar is, deze niet altijd aan de juiste eisen voldoet voor een duurzaam en veilig documentbeheer.
3. Juridische toets 3.a. Doel / grondslag	3a. *Doel* van deze gegevensverwerkingen: Het doel van het verwerken van persoonsgegevens is het zorgen voor behandeling van aanvragen, het binnen de juiste mandaten zorgen voor overzicht over verschillende (aan dezelfde inwoner gerelateerde) zaken en het kunnen sturen van brieven zoals ontvangstbevestigingen. *Grondslag* De verwerkingen in Corsa zijn noodzakelijk voor de vervulling van een taak van algemeen belang (art. 6, eerste lid, onder de AVG). Verder is verwerking noodzakelijk om te voldoen aan een wettelijke verplichting. Het betreft dan de verplichting onder art. 3 van de Archiefwet 1995.	Akkoord. Ook heeft de verwerking als doel om informatie op goede, geordende en beveiligde wijze te archiveren. Akkoord. De aanschaf en implementatie van een gemeente brede voorziening voor digitale documenten opslag en beheer (DOB) inclusief de (integrale) functionaliteit voor procesbeheersing, moet bijdragen aan makkelijk én verantwoord werken met digitale dossiers, in transparante, beheersbare en doelmatige processen. Zodat de papieren dossiers in die processen niet meer nodig zijn.
3.b. Persoonsgegevens Worden bijzondere persoonsgegevens verwerkt?	3.b. Gelet op de functie van Corsa als generiek DMS (Document Management System), is in	Akkoord.

	beginsel voor iedere categorie persoonsgegevens denkbaar dat deze in Corsa zijn opgenomen. Het gaat in ieder geval om naam, adres, woonplaats, geboortedatum, BSN, en contactgegevens. Ook financiële gegevens en gegevens over de gezondheid worden in Corsa verwerkt.	In Corsa worden gegevens over de gezondheid van personen verwerkt. Deze gegevens worden met name verwerkt in het kader van de uitvoering van taken binnen het sociaal domein.
3c. Proportionaliteit	3c. Binnen Corsa worden verschillende persoonsgegevens voor verschillende doeleinden verwerkt. Voor sommige gegevens dient Corsa voornamelijk als zaaksysteem, voor andere gegevens heeft Corsa met name een archieffunctie. Voor iedere verwerking van persoonsgegevens zal steeds afzonderlijk beoordeeld moeten worden of de verwerking proportioneel is. Voor zover de verwerking bestaat uit het archiveren van persoonsgegevens zullen daarbij steeds de bewaartermijnen uit de selectielijsten bij de Archiefwet worden gevolgd. Voor het toekennen van rechten en autorisaties voor inzage in dossiers hanteert BDI het handboek vertrouwelijkheidsgroepen Corsa overzicht. Per onderdeel is bepaald welke zaaktype/werkproces er wordt uitgevoerd, welk bureau hieraan gekoppeld is en welke functies de dossiers/documenten mogen inzien dan/wel wijzigen.	Akkoord. Belangrijkste verandering ten opzichte van de oude werkwijze is het instellen van autorisaties en vertrouwelijkheidsgroepen. Hiermee wordt in de praktijk van het gebruik van Corsa een relatie gelegd met de noodzakelijkheid van het inzien en verwerken van persoonsgegevens. Dat is nu slechts voorbehouden aan degene die dit ook nodig hebben voor hun werk. Van zogenaamd 'Nice to Know' naar 'Need to Know'. NB. De proportionaliteit hangt wel samen met de inrichting en kwaliteit van de vertrouwelijkheidsgroepen en de autorisaties. Als de groepen te groot worden gemaakt verliest het proces langzaam aan proportionele waarde. Te veel medewerkers kunnen dan gegevens inzien of bewerken terwijl dit niet primair voor hun werk noodzakelijk is. Het goed onderhouden van beiden is daarom doorslaggevend in deze procesgang (zie ook bijlagen: instructies en toekennen autorisaties en vertrouwelijkheidsgroepen).
3.d. Subsidiariteit	3.d. Een generiek RMA/DMS systeem is nodig omdat niet voor ieder proces van de gemeente Nijmegen een eigen specifieke procesapplicatie beschikbaar is en als deze beschikbaar is, deze niet altijd aan de juiste eisen voldoet voor een duurzaam en veilig documentbeheer.	Akkoord.
3.e. Persoonsgegevens buiten EER gebruikt?	3.e. Neen.	
3.f. Andere partijen betrokken?	3.f. BCT is de leverancier van Corsa. Alle gegevens worden echter lokaal opgeslagen. Er is dus geen sprake van een verwerkersrelatie.	Akkoord. Met BCT worden wél afspraken gemaakt over aanpassing en verbetering voor zover noodzakelijk.
3.g. Hoe lang worden gegevens bewaard en wijze van vernietiging?	3.g. *Bewaartermijn* Van toepassing is de Selectielijst gemeenten en intergemeentelijke organen 2020, vastgesteld door de VNG. In deze selectielijst is	Akkoord.

	vastgelegd welke informatie gedurende welke termijn bewaard moet worden. *Vernietiging:* BDI draagt een lijst voor waarvan de dossiers vernietigd mogen worden conform de selectielijst. De vernietigingslijst wordt samengesteld/vervaardigd vanuit Corsa. Op de lijst worden de volgende gegevens benoemd: 1. Welke dossiers het betreft. 2. Wat het resultaat is. Denk hierbij aan; vervallen, ingetrokken, niet doorgegaan etc. 3. Sluitingsdatum dossier. Normaliter wordt de datum van het laatste document tevens de sluitingsdatum. Wanneer bovenstaande metadata bekend zijn dan kan conform de selectielijst overgegaan worden tot een vernietigingsdatum.	
3.h. Hoe worden gegevens beveiligd?	3.h. Voor het toekennen van rechten en autorisaties voor inzage in dossiers hanteert BDI het handboek vertrouwelijkheidsgroepen Corsa overzicht. Het handboek is gebaseerd op zaaktypes vanuit de I-navigator gerelateerd aan het bureau waar het proces betrekking op heeft. En op grond van de functiebenaming en functiecode krijgen medewerkers van dat bureau toegang tot de dossiers. In Corsa worden mutaties en inzage van dossiers en documenten gelogd. De intentie is om periodiek de autorisaties per medewerker te controleren. Dat gebeurt nu nog niet omdat eerst de oude vertrouwelijkheden verwijderd moeten worden. Dit proces vindt thans geleidelijk plaats.	Akkoord. Zie bijlage: 'Vertrouwelijkheidsgroepen Corsa – overzicht' (D252046994).
4. Risico's en voorgestelde maatregelen	Het vernietigen van gegevens uit Corsa kan beter. Het vernietigen van dossiers en documenten is gebaseerd op de metadata die wij nodig hebben op grond waarvan wij een selectielijst kunnen maken. In 7.1 is een opsomming gemaakt van metadata die op dit moment in veel registraties in Corsa ontbreken. De volgende metadata ontbreken: • Resultaat (verleend, afgewezen, ingetrokken, etc.); • Sluitingsdatum; • Dossiersoort / zaaktype. De metadata zitten in Taak Specifieke Applicaties en niet in Corsa. T	Akkoord. NB. De organisatie is bezig om Corsa te verrijken met metadata. Om vernietiging grotendeels te automatiseren is de module Archief assistent van BCT aangeschaft. Het vernietigingsproces zal met een inhaalslag worden uitgevoerd. In de rapportage over naleving van deze DPIA zal op deze ontwikkeling nader gerapporteerd dienen te worden.

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 zelf kent een 'middelhoog' risico.
De proportionaliteit hangt samen met de inrichting en kwaliteit van de vertrouwelijkheidsgroepen en de autorisaties. Als de groepen te groot worden gemaakt verliest het proces langzaam aan proportionele waarde. Te veel medewerkers kunnen dan gegevens inzien of bewerken terwijl dit niet primair voor hun werk noodzakelijk is. Het goed onderhouden van beiden is daarom doorslaggevend in deze procesgang (zie ook bijlagen: instructies en toekennen autorisaties en vertrouwelijkheidsgroepen).

Ik adviseer hiermee positief en daarmee zijn de resterende risico's 'aanvaardbaar'.

Eind 2025 zal deze DPIA op naleving getoetst worden.
Naleving richt zich met name op het naleven van de afspraken rondom toekennen van autorisaties en inrichten van vertrouwelijkheidsgroepen. Het goed onderhouden van beiden is doorslaggevend in de procesgang. Dit betekent dat in een nalevingsrapportage hier specifiek aandacht aan besteed dient te worden.

Ten aanzien van de risico's:
De organisatie is bezig om Corsa te verrijken met metadata. Om vernietiging grotendeels te automatiseren is de module Archief assistent van BCT aangeschaft. Het vernietigingsproces zal met een inhaalslag worden uitgevoerd. In de rapportage over naleving van deze DPIA zal op deze ontwikkeling nader gerapporteerd dienen te worden.

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

PK/17/04/2025. DPIA 107

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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

DPIA Oordeel FG gemeente Nijmegen

DPIA Meld- en Herstel Omgevingen en app

Inleiding

Hierbij het oordeel van de FG Gemeente Nijmegen over de DPIA ‘Meld- en Herstel Omgevingen en app’.
Gekozen is voor een systematische aanpak. Deze is terug te herleiden tot de oordeelsvorming van DPIA’s in het algemeen. In deze wordt het 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 welke weergeeft of m.i. het gehele voorstel van maatregelen én te nemen maatregelen bij geconstateerde risico’s, tezamen een aanvaardbaar risico vormen bij het gebruik van privacygevoelige gegevens.

In de periode feb 2024 tot april 2025 hebben 5.1.2e , 5.1.2e , 5.1.2e , 5.1.2e 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 ‘Meld- en Herstel Omgevingen en app’ d.d. 29/04/2025. Deze versie vormt de onderlegger voor deze toetsing.

Bij deze DPIA horen de volgende bijlagen:

- Verwerkersovereenkomst met Woweb
- Verwerkersovereenkomst met Huis voor de Binnenstad
- Verwerkersovereenkomst met Huis voor de Vierdaagse feesten
- Verwerkersovereenkomst met Sight Landscaping

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?	Neen	Akkoord
2. Is het ethisch / politiek bestuurlijk verantwoord?	Meld & Herstel is een applicatie waarin inwoners van Nijmegen gebreken en overlast in de openbare ruimte kunnen melden. Inwoners hebben de mogelijkheid om anoniem te melden, maar kunnen er ook voor kiezen om hun naam en contactgegevens achter te laten zodat we hen een inhoudelijke terugkoppeling kunnen geven. De meldingen worden gecategoriseerd en binnen het systeem doorgezet naar de juiste behandelaar. Dit kunnen werknemers van de gemeenten zijn maar soms ook derden (zoals DAR of Spie).	Akkoord. Omdat meldingen ook aan derden doorgegeven worden zijn vele partijen betrokken. Zie vraag 'betrokkenen'.
3. Juridische toets 3.a. Doel / grondslag	3a. *Doel* van deze gegevensverwerkingen: De applicatie Meld & Herstel is een manier voor inwoners om de gemeente eenvoudig op de hoogte te stellen van gebreken die opgelost moeten worden en voor de organisatie een manier om de werkvoorraad te beheren. *Grondslag* Verwerking is noodzakelijk voor de uitvoering van een wettelijke taak: inwoners vragen om actie in hun belang of in het belang van een cliënt, m.b.t. openbare ruimte-gerelateerde kwesties m.b.t. bijv. overlast, veiligheid, bereikbaarheid en groenvoorziening. Voorbeelden van specifieke grondslagen: artikel 16 Wegenwet; artikel 172 Gemeentewet; artikel 2.1.5.1 APV Nijmegen; artikel 4.2.2.9 APV Nijmegen De verwerking van de contactgegevens ten behoeve van terugkoppeling van de voortgang van de melding, gebeurt op grond van toestemming.	3a. Akkoord. De persoonsgegevens die binnen dit proces worden verwerkt zijn enkel voor het geven van een terugkoppeling. Melders hebben de keuze om contactgegevens achter te laten, of anoniem te melden. Dit heeft geen effect op de afhandeling van de melding
3.b. Persoonsgegevens Worden bijzondere persoonsgegevens verwerkt?	3.b. Nee. Bewoners hebben altijd de mogelijkheid om een anonieme melding te doen. Dit kan ook zonder account aan te maken via de webapplicatie of telefonisch bij het KCC. Als men ervoor kiest om via de telefoonapp een melding te doen, dan moet er een account aangemaakt worden. Als ze kiezen voor een persoonlijke melding of account dan wordt het volgende verwerkt: voor- en achternaam; e-mailadres en/of telefoonnummer; locatie – dit kan mogelijk	3.b. Akkoord.

	resulteren in het verwerken van iemands woonadres.	
3c. Proportionaliteit	3c. Inwoners hebben de mogelijkheid om anoniem te melden als zij dat willen, maar dat betekent dat het niet mogelijk is om een terugkoppeling te geven. Wanneer inwoners hun e-mailadres achterlaten, wordt die terugkoppeling wel gegeven. Adresgegevens van de melder zijn niet nodig. Het gegeven dat gebruikt wordt is van de locatie waarover gemeld wordt. Niet iedere medewerker heeft dezelfde autorisatie, er wordt onderscheid gemaakt in rollen en rechten	3c. Akkoord. Het komt soms voor dat mensen per ongeluk hun eigen adres geven in plaats van de locatie waarover men meldt, maar dan worden deze gegevens niet als een woonadres, maar als locatie melding geregistreerd. Akkoord. Dit staat of valt wel met het onderhouden van de autorisaties.
3.d. Subsidiariteit	3.d. Het verwerken van de locatie is noodzakelijk omdat het duidelijk moet zijn wáár het onderwerp van de melding zich bevindt. De gegevens die landen in Meld & Herstel worden gebruikt om te bepalen waar de werkvoorraad ligt, want deze maken overzichtelijk waar in de openbare ruimte gebreken zijn die we moeten oplossen. Daarnaast worden de data gebruikt om te sturen (denk aan extra inzet van capaciteit op locaties met veel overlast).	3.d. Akkoord. Zonder deze locatie kan de melding niet opgepakt en opgelost worden. Verder is niet mogelijk om algemene problemen in de wijk in kaart te brengen. De locatie wordt niet geregistreerd als woonadres.
3.e. Persoonsgegevens buiten EER gebruikt?	3.e. Neen.	3.e. Akkoord
3.f. Andere partijen betrokken?	3.f. De Gemeente Nijmegen is verantwoordelijk voor het verwerken van de persoonsgegevens. Woweb is verantwoordelijk voor de applicatie en is verwerker. De volgende (andere) betrokken partijen zijn ook verwerkers: Huis voor de binnenstad; Acbn; Vierdaagsefeesten; Van Esch; Sight landscaping; Spie; Vitens; Keperinfra; Connexxion; ODRN; Felyx; Bolt; DAR	3.f. Akkoord De verwerkersovereenkomsten met genoemde partijen worden uiterlijk Q1 2025 door alle externe gebruikers ondertekend verzameld. Noodzakelijke actie voor 2025! Reeds in bezit zijn de overeenkomsten met Woweb, Huis voor de binnenstad, Vierdaagse feesten en Sight Landscapin (zie bijlagen). NB. Externe aanvragen komen binnen bij Key-Users van Meld&Herstel. Key-Users zorgen dat de gebruiker een verwerkersovereenkomst ontvangt. Overeenkomst wordt getekend door gebruiker en eindverantwoordelijke binnen de gemeente.
3.g. Hoe lang worden gegevens bewaard en wijze van vernietiging?	3.g. *Bewaartermijn* De gegevens worden 5 jaar bewaard. Meldergegevens worden na 365 dagen geanonimiseerd.	Akkoord.

	Vernietiging: Melderaccounts worden permanent verwijderd na 365 dagen inactiviteit.	
3.h. Hoe worden gegevens beveiligd?	3.h. Medewerkers loggen in met e-mailadres en wachtwoord. Niet iedereen heeft dezelfde autorisatie, er wordt onderscheid gemaakt in rollen en rechten (bijv. Voorraadbeheerders, behandelaars, key-users, inzage en admin). Externe behandelaren hebben ook een aparte rol, die mogen bijvoorbeeld alleen gegevens van de melder inzie als de melder daar nadrukkelijk toestemming voor heeft gegeven.	Akkoord.
4. Risico's en voorgestelde maatregelen	Risico's (bv verwerken adres melder) worden erkend en afgedekt (registreren als locatie).	Akkoord.

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 zelf kent een 'laag' risico.
Ik adviseer hiermee positief en daarmee zijn de resterende risico's 'aanvaardbaar'.

Uiterlijk 1 september 2025 dienen van de resterende verwerkers de verwerkersovereenkomsten ondertekend te zijn en naar ons toegezonden te worden.

Eind 2025 zal deze DPIA op naleving getoetst worden.
Hierbij zal nadrukkelijke gelet worden op het toekennen en intrekken van autorisaties.

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

PK/29/04/2025. DPIA 108

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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

DPIA Oordeel FG gemeente Nijmegen

DPIA Participatiewet en IOAW

Inleiding

Hierbij het oordeel van de FG Gemeente Nijmegen over de DPIA 'Participatiewet en IOAW'.
Gekozen is voor een systematische aanpak. Deze is terug te herleiden tot de oordeelsvorming van DPIA's in het algemeen. In deze wordt het 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 welke weergeeft of m.i. het gehele voorstel van maatregelen én te nemen maatregelen bij geconstateerde risico's, tezamen een aanvaardbaar risico vormen bij het gebruik van privacygevoelige gegevens.

In de periode dec 2024 tot april 2025 hebben 5.1.2e, 5.1.2e, 5.1.2e, 5.1.2e 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 'Participatiewet en IOAW' d.d. 14/04/2025.
Deze versie vormt de onderlegger voor deze toetsing.

Bij deze DPIA horen de volgende bijlage:

- Verwerkersovereenkomst IRvN

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. Voor deelprocessen zijn DPIA's opgesteld. - Sociale Recherche anonieme accounts (relevant voor aanvraag en beheer van Pw) - Gegevensuitwisseling Inlichtingenbureau en BNK (relevant voor alle onderdelen/fases van Pw en IOAW) - GWS/Suite Sociaal Domein (relevant voor alle onderdelen/fases van Pw en IOAW) - Besluit Bijzondere Bijstand Zelfstandigen (BBZ) (relevant voor alle onderdelen/fases van Pw en IOAW) - Suwinet (relevant voor alle onderdelen/fases van Pw en IOAW)	Akkoord. Betreft DPIA's: DPIA 32 Sociale Recherche Anonieme accounts; DPIA 35 Gegevensuitwisseling Inlichtingenbureau en BNK; DPIA 62 GWS/Suite Sociaal Domein; DPIA 77 Besluit Bijzondere Bijstand Zelfstandigen; DPIA 79 Suwinet.
2. Is het ethisch / politiek bestuurlijk verantwoord?	Ja. Iedereen die kan werken maar het op de arbeidsmarkt zonder ondersteuning niet redt, valt onder de Participatiewet (Pw). De Pw moet ervoor zorgen dat meer mensen werk vinden, ook mensen met een arbeidsbeperking. De Participatiewet is in 2015 ingevoerd en heeft als doel om zoveel mogelijk mensen met een arbeidsvermogen aan het werk te krijgen en ervoor te zorgen dat iedereen kan rekenen op een inkomen. Voor de IOAW-uitkering geldt dat men daarvoor in aanmerking kan komen als ze geboren zijn voor 1 januari 1965 en na hun 50ste werkloos zijn geworden maar nog niet de AOW-leeftijd hebben bereikt. Het is een aanvulling op het inkomen tot bijstandsniveau. Een verschil met de participatiewet is dat hier het vermogen niet meetelt. Het uitgangspunt van deze wetgeving is dat iedereen deelneemt aan de samenleving en, waar mogelijk, in eigen onderhoud voorziet.	Akkoord. Deze DPIA betreft de uitvoering van de hiernaast beschreven wetgeving, met uitzondering van het toezicht dat wordt gehouden door de sociale recherche. Dit wordt in een aparte DPIA beschreven. De Participatiewet kent in de organisatie de onderdelen: aanvraag, beheer, vorderingen en beëindiging. Per onderdeel (aanvraag, beheer, vorderingen en beëindiging) wordt in de DPIA toegelicht waarvoor de verwerking nodig is.
3. Juridische toets 3.a. Doel / grondslag	3a. *Doel* van deze gegevensverwerkingen: Uitvoering geven aan de wettelijke taak (Pw en IOAW) die de gemeente Nijmegen heeft. Door uitvoering te geven aan deze wetgeving zorgen de organisatie ervoor dat de inwoners die het nodig hebben mee kunnen draaien in de samenleving. *Grondslag* De verwerking gebeurt in het kader van een wettelijke verplichting in het kader van de Pw en IOAW, artikel 7 Pw en artikel 34 IAOW. Verder zijn in par. 6.6 Pw en 4.2 Pw artikelen opgenomen ten behoeve van gegevensuitwisseling (zoals met het UWV).	3a. Akkoord. NB. In Artikel 8. Verordeningen uitkeringen van de P-wet, heeft de raad via de verordening ruimte om lokale accenten aan te brengen, passend bij het Coalitieakkoord. Lokale invulling voor verplichtingen, maatregelen en tegenprestaties zijn vastgelegd in de beleidsregels en verordening, geldend voor zowel PW als IOAW.

3.b. Persoonsgegevens Worden bijzondere persoonsgegevens verwerkt?	3.b. In beginsel niet. Bij uitvraag naar 'arbeidsvermogen' kan sprake zijn van medische redenen / gegevens hieromtrent. Voor de Pw en IOAW worden de volgende gegevens opgevraagd: • Naam, adres, woonplaats, nationaliteit • Uitkeringen (bijv. WW, WIA, Wajong, Anw) • Arbeidsvermogen • Inkomsten • Studiefinanciering • Inschrijving Kamer van Koophandel • Kentekens op naam • Belastinggegevens • Woongegevens • Gegevens van partner, met betrekking tot inkomen, studie en bezit.	3.b. Akkoord. Het kan voorkomen dat er persoonsgegevens worden ontvangen die niet relevant zijn voor de aanvraag. In het geval van fysieke stukken worden deze gegevens teruggestuurd naar de afzender. In het geval van digitale stukken worden de gegevens verwijderd en wordt de inwoner hierover geïnformeerd. l NB. Kenteken op naam kan interessant zijn i.v.m. beoordelen vermogen.
3c. Proportionaliteit	3c. De verwerking van persoonsgegevens in het kader van de Pw en IOAW vraagt om een relatief grote inbreuk op de privacy van de inwoner. De organisatie vraagt een basis set aan info uit via een vragenformulier, met een vragenboom. Deze beweegt mee met de antwoorden van de klant. Hierdoor wordt zoveel mogelijk aan dataminimalisatie gedaan. De organisatie maakt de beweging van oudsher 'alles uitvragen wat mag', naar 'bewust uitvragen en afwegen wat we willen rapporteren'. In de voorbereidingen op de Participatiewet in Balans handelt de organisatie vanuit dit gedachtegoed. Vastlegging en logging: er wordt gewerkt met een vragenboom in het aanvraagformulier, hierdoor kan worden gevolgd waarom bepaalde gegevens zijn opgevraagd en vastgelegd. Middels interne controle- en verbetercyclus vindt steekproefsgewijs een controle plaats op proportionaliteit. De uitkomsten hiervan vormen de basis van de interne scholing. Tot slot wordt de wijze van (bij)scholing en kwaliteitstoetsing op de Participatiewet momenteel opnieuw/aangescherpt geformuleerd	3c. Akkoord. Advies: rapporteer in de naleving van deze DPIA wat de interne controle met betrekking tot opslag van gegevens en de noodzakelijkheid hiervan heeft opgeleverd (betreft met name proportionaliteit per aanvraag) en op welke wijze geleerd wordt van hetgeen aangetroffen is (terugkoppeling van mogelijke aanpassingen in de procesgang). NB. Op dit moment worden ook vragen gesteld op onderdelen waar uiteindelijk WerkBedrijf mee aan de slag gaat. Deze vragen zijn niet noodzakelijk voor het vaststellen van het recht op de uitkering. Wel zijn deze vragen noodzakelijk voor de uitvoering van de Participatiewet en als zodanig vastgelegd in een convenant met het WerkBedrijf. Een aandachtspunt hierbij is dat uiteindelijk niet alle klanten aangemeld worden bij WerkBedrijf. Dit betekent dat voor een bepaalde klantgroep meer informatie uitgevraagd wordt dan noodzakelijk is. Het aanvraagformulier Levensonderhoud wordt momenteel herzien en opnieuw opgesteld / ontwikkeld. Er is aandacht voor dit gegeven van de (te?) brede uitvraag aan de klant. Ook dit aspect dient gerapporteerd te worden in het nalevingsverslag 2025.
3.d. Subsidiariteit	3.d. De gegevens uitvraag vindt allereerst bij de burger plaats door de vraagstelling in het aanvraagformulier. Daar moet de aanvrager verklaringen afleggen omtrent woon- en	3.d. Akkoord. De procesgang is vastgelegd in werkinstructies voor uitvoerend medewerkers. Aandachtspunt

	leefsituatie, arbeidsgeschiktheid, inkomen en vermogen. Dit is noodzakelijk om het recht vast te stellen; deze gegevens zijn bepalend in het al dan niet toekennen van een uitkering, wijzigingen aanbrengen in de beheer fase en eventueel een beëindiging doorvoeren. Een burger kan bewust of onbewust gegevens achterhouden. Via de informatie-uitwisseling met instanties vindt verificatie plaats. Op deze wijze wordt voorkomen dat de klant achteraf geconfronteerd wordt met terugvorderingen als er toch geen recht blijkt te zijn. Deze gegevens zijn nodig om het recht vast te stellen en onnodige terugvordering te voorkomen. Dit betekent niet dat alle informatie vastgelegd hoeft te worden in het dossier, rapporteren dat bepaalde informatie is gezien/gecheckt, is voldoende. Denk hierbij aan het legitimatiebewijs wel/niet opslaan. In de gegevensuitwisseling per mail wordt gewerkt met Zivver (veilig mailen). In werkprocessen wordt niet gemaild.	hierbij is dat deze doorlopend worden bijgewerkt door team kwaliteit indien de procesgang wijzigingen kent. Dit vraagt en krijgt met name de aandacht in het voorbereidingstraject op de Participatiewet in Balans, waar de organisatie te maken heeft met proceswijzigingen. Via het inlichtingenbureau, Suwinet en de BRP vindt o.a. uitwisseling plaats.
3.e. Persoonsgegevens buiten EER gebruikt?	3.e. Neen.	3.e. Akkoord
3.f. Andere partijen betrokken?	3.f. De Gemeente Nijmegen is verantwoordelijk voor het verwerken van de persoonsgegevens. IRvN is de verwerker (Suite Sociaal Domein). Andere verwerkers: InlichtingenBureau (levert informatie via Suwi-Net), AWS & IRVN (Centric/Suite en ESB).	3.f. Akkoord Er is een verwerkersovereenkomst met de IRvN. Met AWS en Inlichtingenbureau zijn verwerkersovereenkomsten afgesloten. Deze zijn reeds bij de eerder genoemde DPIA's (ad. 1.) aangeleverd.
3.g. Hoe lang worden gegevens bewaard en wijze van vernietiging?	3.g. *Bewaartermijn* De bewaartermijn voor dossiers van bijstandsuitkeringen in het kader van de Participatiewet is 10 jaar. De bewaartermijn voor dossiers van zowel bijstandsuitkeringen als IOAW/Z-uitkeringen is 10 jaar (na laatste contact/bemoeienis) op grond van de Archiefwet 1995. *Vernietiging:* Na beëindiging van de bewaartermijnen. Vernietiging vindt plaats conform een door de gemeente vastgestelde procedure.	Akkoord.
3.h. Hoe worden gegevens beveiligd?	3.h. Autorisatie, bewaartermijnen, logging zijn reeds geregeld in de Suite en voor documenten in Corsa. Zie daarom ook DPIA Suite en DPIA Corsa.	Akkoord. Autorisaties toekennen en intrekken is essentieel in dit proces. Logging van handelingen (en keuzes over welke informatie wél en niet opgeslagen wordt en waarom) is essentieel voor bepaling van de proportionaliteit. Zoals eerder gesteld dient hierover in het nalevingsrapport opgenomen te worden wat de ervaringen en leereffecten zijn.

4. Risico's en voorgestelde maatregelen	Benoemde risico's zijn reëel.	Akkoord. Ervaringen hierover opnemen in de rapportage naleving 2025.

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 zelf kent een 'middelhoog' risico.
Het betreft een verwerking met veel (vaak gevoelige) gegevens van burgers.

De verwerking van persoonsgegevens in het kader van de Pw en IOAW vraagt om een relatief grote inbreuk op de privacy van de inwoner. De organisatie vraagt een basis set aan info uit via een vragenformulier, met een vragenboom. Deze beweegt mee met de antwoorden van de klant. Hierdoor wordt zoveel mogelijk aan dataminimalisatie gedaan.
De organisatie maakt de beweging van oudsher 'alles uitvragen wat mag', naar 'bewust uitvragen en afwegen wat we willen rapporteren'. In de voorbereidingen op de 'Participatiewet in Balans' handelt de organisatie vanuit dit gedachtegoed.
Vastlegging en logging: er wordt gewerkt met een vragenboom in het aanvraagformulier, hierdoor kan worden gevolgd waarom bepaalde gegevens zijn opgevraagd en vastgelegd. Middels interne controle- en verbetercyclus vindt steekproefsgewijs een controle plaats op proportionaliteit. De uitkomsten hiervan vormen de basis van de interne scholing.

Op de loer ligt dat te veel gegevens uitgevraagd worden. Dan is de werkwijze niet meer proportioneel.
Vandaar de volgende adviezen:
1. Rapporteer in de naleving van deze DPIA wat de interne controle met betrekking tot opslag van gegevens en de noodzakelijkheid hiervan, heeft opgeleverd en op welke wijze geleerd wordt van hetgeen aangetroffen is.
2. Autorisaties toekennen en intrekken is essentieel in dit proces.
Logging van handelingen (en keuzes over welke informatie wél en niet opgeslagen wordt en waarom) is essentieel voor bepaling van de proportionaliteit.
Hierover (logging en autorisaties) dient in het nalevingsrapport opgenomen te worden wat de ervaringen en leereffecten zijn.
3. Rapporteer over de procesgang met het Werkbedrijf.

Ik adviseer hiermee positief en daarmee zijn de resterende risico's 'aanvaardbaar'.

Eind 2025 zal deze DPIA op naleving getoetst worden met name gericht op bovenstaande adviezen.

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

PK/29/04/2025. DPIA 109

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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

DPIA Oordeel FG gemeente Nijmegen

Transcriptiesoftware

Inleiding

Hierbij het oordeel van de FG Gemeente Nijmegen over de DPIA ‘Transcribeersoftware’.
Gekozen is voor een systematische aanpak. Deze is terug te herleiden tot de oordeelsvorming van DPIA’s in het algemeen. In deze wordt het 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 welke weergeeft of m.i. het gehele voorstel van maatregelen én te nemen maatregelen bij geconstateerde risico’s, tezamen een aanvaardbaar risico vormen bij het gebruik van privacygevoelige gegevens.

In de periode september 2024 tot en met juni 2025 hebben 5.1.2e , 5.1.2e , 5.1.2e 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 ‘Transcriptiesoftware d.d. 19/06/2025. Deze versie vormt de onderlegger voor deze toetsing.

Bij deze DPIA horen de volgende bijlagen:

- DPIA MS365.

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?	De organisatie maakt gebruik van een nieuwe toepassing en een nieuwe manier van werken dus er is geen gelijksoortige DPIA. Wel is de toepassing (Teams Premium) onderdeel van MS365. Er is een DPIA MS365.	Akkoord DPIA MS365, nr. 90.
2. Is het ethisch / politiek bestuurlijk verantwoord?	Om het werk van de managementassistenten te verlichten en de wens om te starten met verantwoord gebruik van AI, heeft de gemeente Nijmegen een pilot uitgevoerd met transscriptiesoftware. Deze pilot is met positief resultaat afgerond en men wil hier nu verder mee. Er is gekozen voor Microsoft Teams Premium. De software zal zorgdragen voor het notuleren en samenvatten van vergaderingen. Een volledige toetsing van de ethische effecten en de vraag óf we dit willen zal de organisatie nogmaals moeten verrichten wanneer de richtlijnen digitale ethiek tot stand zijn gekomen.	Akkoord. Dit is de eerste verwerking van de organisatie waarbij AI wordt ingezet met een risico op confirmation bias (8.1). De FG beveelt nadrukkelijk aan om deze casus actief bij de ethische commissie onder de aandacht te brengen.
3. Juridische toets 3.a. Doel / grondslag	3a. *Doel* van deze gegevensverwerkingen: De organisatie wil deze transcribeertool gaan gebruiken met het doel om sneller, efficiënter en kwalitatief betere notulen op te leveren. *Grondslag* De verwerking is in twee delen te onderscheiden. De verwerking van het stemgeluid (de opname en automatische transcriptie) en de inhoudelijk besproken informatie: 1. Voor de verwerking van het stemgeluid: geldt de grondslag toestemming. Deze toestemming zal aan de start van het overleg worden gevraagd en worden vastgelegd door de notulist. Als niet door alle deelnemers toestemming wordt gegeven wordt geen gebruik gemaakt van de transcriptietool. Als een deelnemer aan het overleg zijn toestemming later intrekt, wordt enkel de opname verwijderd, niet de transcriptie. 2. Het verwerken van de inhoudelijk besproken informatie in de transcriptie is gebaseerd op de grondslag *gerechtvaardigd belang*. Er is sprake van een gerechtvaardigd belang onder meer wanneer een verwerking aantoonbaar noodzakelijk is om bedrijfsactiviteiten te kunnen verrichten. Het houden van overleg en notuleren van de besproken onderwerpen is noodzakelijk om op een effectieve manier onze bedrijfsactiviteiten uit te voeren. De tool die de	3a. Akkoord. Toestemming kan vrijelijk worden gegeven. Zonder toestemming zal met de hand worden genotuleerd, waardoor het overleg ook doorgang kan vinden. Hoewel het niet de bedoeling is om meer persoonsgegevens te delen dan de naam, zou dit wel het geval kunnen zijn. Bij autoriseren voor gebruik van Teams Premium wordt gevraagd voor welk type vergaderingen de gebruiker het gaat toepassen (8.2). Wij adviseren om binnen een maand een werkinstructie te maken voor het geval dit toch gebeurt.

	organisatie hierbij gebruikt draagt hieraan bij en valt daarom onder deze grondslag.	
3.b. Persoonsgegevens Worden bijzondere persoonsgegevens verwerkt?	3.b. Nee. Welke gegevens worden verwerkt is afhankelijk van de inhoud van de vergadering. In ieder geval zal worden verwerkt: - Namen van betrokkenen - Stemgeluid De inzet van de transcribeersoftware zal worden beperkt tot vergaderingen die niet of beperkt de persoonlijke levenssfeer van de deelnemers of andere personen raken. In dit soort vergaderingen blijven de verwerkte gegevens ook beperkt tot de namen van de deelnemers, andere collega's die deel uitmaken van het team en de stemmen. De software wordt dus niet gebruikt voor vergaderingen waar bijvoorbeeld dossiers van inwoners of medewerkers worden besproken. Verwerking van stemgeluid kan een biometrisch gegeven (valt onder bijzondere persoonsgegevens) zijn.	3.b. Akkoord. Omdat in dit geval stemmen van de deelnemers niet worden gebruikt om iemand te identificeren of een referentiekader op te stellen, is geen sprake van een biometrisch gegeven en vindt er geen verwerking van bijzondere persoonsgegevens plaats.
3c. Proportionaliteit	3c. De inbreuk wordt door de organisatie zo beperkt mogelijk gehouden tot enkel de naam en de opgenomen stem en die opname wordt ook direct na de verwerking weer verwijderd. Daarnaast is er de richtlijn dat andere gegevens ook niet verwerkt mogen worden, zoals gebeurt bij een bespreking van een persoonlijk dossier. Medewerkers wordt om toestemming gevraagd om de softwaretool in te kunnen zetten. Als iemand aangeeft bezwaren te hebben, dan wordt gewoon met de hand genotuleerd.	3c. Akkoord.
3.d. Subsidiariteit	3.d. Bij het gebruik van de transcribeertool is bewust gekozen voor een bepaald type vergadering waar in beginsel geen andere persoonlijke gegevens worden gedeeld naast de naam. De naam is nodig om in de uiteindelijke notulen terug te kunnen lezen wie wat heeft gezegd. Verder is het enkel middels het opnemen van de stem mogelijk om gebruik te maken van de tool.	3.d. Akkoord. Onder 8.1 en 8.2 staat het risico beschreven dat de software toch wordt gebruikt bij gevoelige persoonsgegevens. Bij autoriseren voor gebruik wordt gevraagd voor welk type vergaderingen de gebruiker de software gaat toepassen. De organisatie moet alert blijven op de juiste toepassing van de tool door de medewerkers. Dit zal terugkomen in de naleving 2025.

	Het alternatief is de huidige werkwijze met handmatige verwerking. De pilot heeft aangetoond dat deze transcribeersoftware winst in tijd en kwaliteit oplevert en dat verantwoord gebruik mogelijk is. Daarnaast wordt de tool toegepast in een beheerste omgeving.	
3.e. Persoonsgegevens buiten EER gebruikt?	3.e. Neen.	3.e. Akkoord
3.f. Andere partijen betrokken?	3.f. De gegevens worden uitgewisseld tussen deelnemers aan de vergaderingen. De deelnemers zijn collega's en externen (bijvoorbeeld aannemers). Voor de verwerking van de transcriptie en samenvatting wordt gebruik gemaakt van cloudopslag direct bij Microsoft (Teams Premium). Gemeente Nijmegen is verwerkingsverantwoordelijke. Microsoft is verwerker.	3.f. Akkoord Microsoft is gebonden aan het Juridisch Framework van de VNG met Microsoft. Dit is een bijlage bij de DPIA MS365.
3.g. Hoe lang worden gegevens bewaard en wijze van vernietiging?	3.g. *Bewaartermijn* De organisatie bewaart de opnames niet langer dan nodig voor het proces. Dit betekent dat de opname verwijderd wordt nadat het verslag is vastgesteld. *Vernietiging:* De afdeling waar de vergadering plaatsvindt is verantwoordelijk voor de vernietiging. Microsoft verwijdert opnames automatisch na 6 maanden, tenzij de bestandseigenaar expliciet aangeeft een opname langer te willen bewaren.	Akkoord. Dit zal terugkomen in de naleving 2025.
3.h. Hoe worden gegevens beveiligd?	3.h. Teams Premium staat alleen toegang tot de opname toe aan deelnemers aan het overleg. De beveiligingsinstellingen komen overeen met de standaard MS Teams-instellingen. BIO.	Akkoord.
4. Risico's en voorgestelde maatregelen	Bij gemeentebrede uitrol zal er een werkinstructie opgesteld worden waar de tool niet alleen technisch wordt toegelicht maar ook de gebruiksregels zoals het verwijderen van de opname.	Akkoord. Binnen een maand dient er een werkinstructie opgesteld te zijn en deze maakt integraal onderdeel uit van deze DPIA.

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 zelf kent een 'laag' risico.
Ik adviseer hiermee positief en daarmee zijn de resterende risico's 'aanvaardbaar'.

Dit is de eerste verwerking van de organisatie waarbij AI wordt ingezet met een risico op confirmation bias. De FG beveelt nadrukkelijk aan om deze casus actief bij de ethische commissie onder de aandacht te brengen.

Hoewel het niet de bedoeling is om meer persoonsgegevens te delen dan de naam, zou dit wel het geval kunnen zijn. Wij adviseren om binnen een maand een werkinstructie te maken voor het geval dit toch gebeurt. In deze werkinstructie wordt de tool niet alleen technisch toegelicht maar worden ook de gebruiksregels zoals het verwijderen van de opname beschreven. De instructie maakt integraal onderdeel uit van deze DPIA.

Eind 2025 zal deze DPIA op naleving getoetst worden.
Hierbij zal nadrukkelijk worden gelet op het verwijderen van opnames en toekennen en intrekken van autorisaties.

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

KR/PK/10/07/2025. DPIA 110.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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

DPIA Oordeel FG gemeente Nijmegen

Verkoop entreetickets VSA-speeltuinen en Triavium

Inleiding

Hierbij het oordeel van de FG Gemeente Nijmegen over de DPIA 'Verkoop entreetickets VSA-speeltuinen en Triavium'.
Gekozen is voor een systematische aanpak. Deze is terug te herleiden tot de oordeelsvorming van DPIA's in het algemeen. In deze wordt het 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 welke weergeeft of m.i. het gehele voorstel van maatregelen én te nemen maatregelen bij geconstateerde risico's, tezamen een aanvaardbaar risico vormen bij het gebruik van privacygevoelige gegevens.

In de periode november 2024 tot en met juli 2025 hebben 5.1.2e, 5.1.2e, 5.1.2e, 5.1.2e 5.1.2e 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 'Verkoop entreetickets VSA-speeltuinen en Triavium. dd. 02/07/2025. Deze versie vormt de onderlegger voor deze toetsing.

Bij deze DPIA horen de volgende bijlagen:

- Verwerkersovereenkomst De Haan Kassasystemen

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?	Neen, er is wel een DPIA van het verhuursysteem Amis (verhuur sport en welzijnslocaties)	Akkoord DPIA nr. 42.
2. Is het ethisch / politiek bestuurlijk verantwoord?	Om te kunnen controleren of iemand die toegang wil tot een van de genoemde locaties ook de abonnementhouder is, is het nodig de identiteit en geldigheid van het abonnement te kunnen controleren. Gezien de doelgroep mede bestaat uit een leeftijdsgroep die nog geen identiteitsbewijs op zak heeft om zich te legitimeren is gekozen voor een gepersonaliseerde toegangspas.	Akkoord. Omdat sprake is van diversificatie van tarieven op basis van leeftijd is het ook nodig de geboortedatum te verwerken.
3. Juridische toets 3.a. Doel / grondslag	3a. *Doel* van deze gegevensverwerkingen: Controleren van het persoonsgebonden gebruik van de pas (voorkomen van misbruik). Het terugvinden van een klantenkaart in het kassasysteem (voorkomt het aanmaken van een extra klantenrecord bij verlies van pas). Het verkopen van een abonnement tegen het juiste tarief. *Grondslag* Deze verwerking geschiedt op basis van een gerechtvaardigd belang zoals bedoeld in artikel 6 lid 1 sub f AVG.	3a. Akkoord. Een bezoeker kan, tijdens de aanschaf van een abonnement, te allen tijde aangeven dat hij of zij (een deel van) de gegevens niet wil aanleveren. Het gevolg hiervan is dat er geen abonnement kan worden aangeschaft. Op dat moment kan de bezoeker een anoniem toegangsticket kopen, waarmee de betreffende locatie alsnog bezocht kan worden. Als exploitatieverantwoordelijke van de locaties speeltuin de Leemkuil, speeltuin Brakkefort en ijsbaan Triavium is de gemeente Nijmegen verantwoordelijk voor het verschaffen van toegang tot de betreffende locaties.
3.b. Persoonsgegevens Worden bijzondere persoonsgegevens verwerkt?	3.b. Niet per se. De pasfoto kan een bijzonder persoonsgegeven zijn wanneer daaruit ras/etniciteit of religie is af te leiden. De volgende gegevens worden verwerkt: De voor- en achternaam van de persoon, de pasfoto en de geboortedatum.	3.b. Akkoord. Het doel van de verwerking is niet gericht op het maken van onderscheid op grond van de bijzondere persoonsgegevens die mogelijk uit de foto af te leiden zijn.
3c. Proportionaliteit	3c. De verwerkte set gegevens is de minimale set die nodig is om een pas voor abonnement-houders te maken om te controleren of de persoon die het abonnement gebruikt ook de eigenaar er van is.	3c. Akkoord.
3.d. Subsidiariteit	3.d. Het alternatief (verificatie op basis van het identiteitsbewijs) is gezien doelgroep (veelal kinderen) niet realistisch en brengt meer privacy-risico's met zich mee.	3.d. Akkoord.
3.e. Persoonsgegevens buiten EER gebruikt?	3.e. Neen.	3.e. Akkoord

3.f. Andere partijen betrokken?	3.f. Kassaleverancier de Haan en haar onderaannemer HD Services (hosting server), de gebruikers van het kassasysteem (VSA). Leverancier De Haan is verwerker t.b.v. het leveren van het kassa- en toegangssysteem. HD services is subverwerker en onderaannemer van De Haan t.b.v. de hosting van de applicatie. Medewerkers van de genoemde speeltuinen en de schaatsbaan zijn gebruiker van het systeem.	3.f. Akkoord
3.g. Hoe lang worden gegevens bewaard en wijze van vernietiging?	3.g. *Bewaartermijn* Anderhalf seizoen. Om te voorkomen dat er dubbele klantenrecords in de database worden aangemaakt, krijgt de bezoeker die vorig seizoen een abonnement heeft gebruikt, tot halverwege het daaropvolgende seizoen de kans om een nieuw abonnement aan te schaffen. Daarna worden de gegevens geanonimiseerd. Dit is geen geautomatiseerd proces.. *Vernietiging:* In de backoffice kan een datum worden opgegeven en vervolgens een opdracht tot anonimiseren. Alle klantenrecords voor de opgegeven datum worden vervolgens versleuteld en zijn – zelfs niet voor de Haan – niet meer te ontsleutelen.	Akkoord. De gemeente kan de Haan een opdracht geven tot daadwerkelijk verwijderen. Zij moeten dan handmatig een query schrijven waarmee het gewenste deel van de database wordt verwijderd. Uitgezocht moet worden welke kosten hiermee gemoeid zijn en of dat nog proportioneel is. De voorkeur van de FG gaat uit naar verwijdering.
3.h. Hoe worden gegevens beveiligd?	3.h. De toegang tot het kassasysteem is beveiligd met een twee-factor authenticatie. Daarnaast is op account niveau in te stellen welke rechten het betreffende account heeft binnen het kassasysteem.	Akkoord.
4. Risico's en voorgestelde maatregelen	De kassabediende kan geen gegevens exporteren naar andere systemen.	Akkoord.

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 zelf kent een 'laag' risico.
Ik adviseer hiermee positief en daarmee zijn de resterende risico's 'aanvaardbaar'.

Er is één uitzoekpunt.
Op dit moment worden de gegevens na gebruik geanonimiseerd. Deze zijn hierdoor zowel voor de gebruikers als de leverancier onleesbaar. Op zich volstaat dat.
Krachtiger is als deze daadwerkelijk vernietigd worden. Uitgezocht moet worden welke kosten hiermee gemoeid zijn. De FG heeft een voorkeur voor daadwerkelijke vernietiging.

Eind 2025 zal deze DPIA op naleving getoetst worden. Dan moet ook het kostenplaatje van vernietiging in beeld zijn.

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

PK/05/08/2025. DPIA 111.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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

DPIA Oordeel FG gemeente Nijmegen

Verkeersmanagement met behulp van overzichtscamera's

Inleiding

Hierbij het oordeel van de FG Gemeente Nijmegen over de DPIA 'Verkeersmanagement met behulp van overzichtscamera's'.
Gekozen is voor een systematische aanpak. Deze is terug te herleiden tot de oordeelsvorming van DPIA's in het algemeen. In deze wordt het 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 welke weergeeft of m.i. het gehele voorstel van maatregelen én te nemen maatregelen bij geconstateerde risico's, tezamen een aanvaardbaar risico vormen bij het gebruik van privacygevoelige gegevens.

In de periode januari tot en met augustus 2025 hebben 5.1.2e, 5.1.2e, 5.1.2e, 5.1.2e 5.1.2e, 5.1.2e, 5.1.2e 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 'Verkeersmanagement met behulp van overzichtscamera's dd. 08/08/2025. Deze versie vormt de onderlegger voor deze toetsing.

Bij deze DPIA horen de volgende bijlagen:

- geen

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?	Neen.	Akkoord
2. Is het ethisch / politiek bestuurlijk verantwoord?	Verkeersmanagement beoogt een optimale doorstroming van verkeer binnen de gemeente, en draagt bij aan de veiligheid en bereikbaarheid van het centrumgebied. De inzet van cameratoezicht is gericht op het goed functioneren van de verkeersstromen in het stedelijk gebied en sluit aan bij de bredere beleidsdoelstellingen zoals verwoord in de Uitvoeringsagenda Verkeersmanagement Nijmegen.	Akkoord. Vanuit de Verkeersmanagement Centrale (VMC) centrale kunnen verkeersregelaars direct inspelen op onvoorziene situaties, zoals ongevallen of foutief gebruik van rijrichtingen, en waar nodig passende maatregelen treffen. De exacte locaties van de geplaatste overzichtscamera's zijn opgenomen in bijlage 2 van deze DPIA.
3. Juridische toets 3.a. Doel / grondslag	3a. *Doel* van deze gegevensverwerkingen: a. het verzekeren van de veiligheid op de weg; b. het beschermen van weggebruikers en passagiers; c. het in stand houden van de weg en het waarborgen van de bruikbaarheid daarvan; d. het zoveel mogelijk waarborgen van de vrijheid van het verkeer. *Grondslag* De verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang die aan de verwerkingsverantwoordelijke is opgedragen. Deze taak blijkt uit de Wegenverkeerswet 1994, Artikel 2, lid 1, onder a t/m d.	3a. Akkoord. Het doel van de verwerking wordt bepaald in de Wegenverkeerswet 1994, Artikel 2, lid 1. Regels rondom de inzet van technieken zoals observatiecamera's, VRI's, DRIP en PRIS worden, zoals bepaald in de Wegenverkeerswet, Artikel 14, lid 1 bij algemene maatregel van bestuur vastgesteld.
3.b. Persoonsgegevens Worden bijzondere persoonsgegevens verwerkt?	3.b. Neen. Er worden beelden verwerkt van verkeersdeelnemers, waarbij deelnemers herkenbaar in beeld kunnen komen. Daarnaast kunnen kentekens zichtbaar in beeld komen.	3.b. Akkoord. Het doeleinde van de verwerking is niet gericht op het verwerken van bijzondere persoonsgegevens dan wel op het onderscheid maken op grond van een bijzonder persoonsgegeven.
3c. Proportionaliteit	3c. De camera's zijn uitsluitend gericht op verkeerssituaties, niet op het gericht volgen van personen. Persoonsgegevens worden dus slechts in beperkte mate verwerkt, als gevolg van verkeersdeelname. De camerabeelden worden niet langer bewaard dan strikt noodzakelijk. Ook is het aantal camera's beperkt tot strategische punten die verkeerskundig relevant zijn.	3c. Akkoord. Op basis van camerabeelden kan de verkeersmanagement centrale actuele verkeersdrukte beoordelen, verkeersregelinstallaties aansturen, hulpdiensten informeren en samenwerking zoeken met andere partijen zoals politie en handhaving (zie ook advies m.b.t. afgiftebeleid)
3.d. Subsidiariteit	3.d. Alternatieven zoals handmatige monitoring of periodieke metingen bieden hiervoor onvoldoende actuele informatie en missen de mogelijkheid tot directe interventie.	3.d. Akkoord. Voor het uitvoeren van verkeersmanagement bij reguliere verkeerssituaties, bij ongevallen, evenementen of andere afwijkingen, is het noodzakelijk dat de operators direct zicht hebben op de verkeerssituatie ter plaatse.

3.e. Persoonsgegevens buiten EER gebruikt?	3.e. Neen.	3.e. Akkoord
3.f. Andere partijen betrokken?	3.f. De gemeente Nijmegen is verwerkingsverantwoordelijke voor de observatiecamera's die worden ingezet vanuit de Verkeersmanagementcentrale (VMC). Er vindt geen uitwisseling van persoonsgegevens plaats met andere partijen. Alle verwerking gebeurt intern. Het eerste- en tweedelijns onderhoud aan de camera's wordt uitgevoerd door Artec Parkeer & Elektra Installateurs te Nijmegen. Artec heeft geen toegang tot persoonsgegevens. De leverancier van het Video Management Systeem (Genetec) heeft in incidentele gevallen toegang tot persoonsgegevens, maar uitsluitend tijdens gepland onderhoud aan de server(s). Deze toegang vindt plaats onder strikte voorwaarden en onder verantwoordelijkheid van de gemeente.	3.f. Akkoord NB. Er zijn geen structurele verwerkers: Bij de verwerking van camerabeelden is geen sprake van structurele inzet van verwerkers in de zin van artikel 4 lid 8 AVG. De observatiecamera's en het bijbehorende VMS worden beheerd vanuit de gemeentelijke VMC. Genetec wordt niet als verwerker aangemerkt, omdat er geen sprake is van zelfstandige verwerking. Toegang tot persoonsgegevens is beperkt tot incidenteel onderhoud, onder toezicht van de gemeente, en op basis van vooraf afgestemde procedures. Aangezien er geen structurele verwerkers zijn aangemerkt, is geen verwerkersovereenkomst opgesteld.
3.g. Hoe lang worden gegevens bewaard en wijze van vernietiging?	3.g. *Bewaartermijn* Beelden van de observatiecamera's worden 7 dagen bewaard. Deze termijn is noodzakelijk voor de afhandeling van incidenten en schadegevallen. *Vernietiging:* De data worden automatisch overschreven. De operationeel verantwoordelijke beheerder is hiervoor verantwoordelijk.	Akkoord.
3.h. Hoe worden gegevens beveiligd?	3.h. Het gehele netwerk van camera's, randapparatuur, firewall en Genetec server is geplaatst binnen een LAN-omgeving binnen het eigen glasvezelnetwerk van de gemeente Nijmegen. 5.1.2h 5.1.2h. Vanaf de camera tot aan de server wordt gebruik gemaakt van Radius Authenticatie waardoor het voor onbevoegden onmogelijk is de server te benaderen. 5.1.2h 5.1.2h 5.1.2h. De Genetec server maakt gelaagde autorisatie mogelijk waardoor per functie kan worden ingesteld wie live mag meekijken en wie beelden mag terugkijken en/of veiligstellen. 5.1.2h 5.1.2h 5.1.2h. Beeldmateriaal wordt alleen afgegeven na een vordering door de politie.	Akkoord. Beeldmateriaal kan niet worden gemanipuleerd doordat deze voorzien is van een watermerk. Verder is beeldmateriaal encrypted zodra deze wordt veiliggesteld. De toegang tot de VMC is middels een toegangscontrolesysteem beveiligd. Niet geautoriseerden komen er niet onbegeleid binnen. 5.1.2h 5.1.2h 5.1.2h 5.1.2h 5.1.2h 5.1.2h 5.1.2h. Het operationele toezicht op de gegevensbeveiliging wordt verzorgd door de operationeel verantwoordelijke beheerder.

4. Risico's en voorgestelde maatregelen	In de risico paragraaf staan diverse aanbevelingen opgenomen. Risico 1. Afgifte beeldmateriaal aan de verkeerde persoon. Risico: medium Advies: stel een afgifte protocol op met daarin duidelijk aan wie beelden mogen worden afgegeven en wat de procedure is. Denk daarbij ook aan: - Legitimatieplicht; - Wijze van afgifte en het gebruik van cybersecurity veilige methoden; - Instellen watermerk in Genetec Risico 2. Oneigenlijk gebruik beeldmateriaal. Risico: medium Advies: cameraprotocol opstellen voor operators met instructies omtrent doelen en de handelwijze bij live meekijken. Draag zorg voor een privacymask van de omgeving of draag zorg voor het blurren van de gezichten van personen en kentekens uit de omgeving van de gefilmde weg. Risico 3. Beelden worden te vroeg verwijderd en kunnen niet meer dienen als bewijsmateriaal. Risico Laag. Advies: protocol vaststellen dat bij ieder incident de gegevens direct worden veiliggesteld. Risico 4. Slechte informatievoorziening aan betrokkenen. Beelden worden verwijderd voordat een betrokkenen gebruik heeft kunnen maken van het recht op inzage. Risico Hoog/Midden. Advies: zorg ervoor dat betrokkenen adequaat geïnformeerd worden over hun rechten. Dit kan door de privacyverklaring op de website te zetten van de gemeente. In verband met de diverse soorten van cameragebruik is het wellicht verstandig om 1 Privacyverklaring cameragebruik op te nemen. Hierbij kunnen alle onderdelen van het camera gebruik worden benoemd inclusief de specifieke doelen en opslagtermijnen. Plaats borden ruim voor het bereik van de 1e camera (wellicht bij ingang Nijmegen) waarbij verwezen wordt naar het feit dat er sprake is van camerabewaking. Voorzie dat bord van een URL die direct verwijst naar de privacy verklaring. Neem in het op te stellen protocol voor centralisten de procedure op voor het melden van datalekken.	Akkoord. Binnen zes maanden dient aangegeven te worden op welke wijze de aanbevelingen opgevolgd zijn.

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 zelf kent een 'middelhoog' risico. Deze wordt verlaagd nadat de voorgestelde maatregelen ingevoerd zijn. Hierover dient binnen zes maanden gerapporteerd te worden.
De genoemde maatregelen (in adviesvorm geformuleerd) zijn:

Risico 1. Afgifte beeldmateriaal aan de verkeerde persoon. Risico: medium
Advies: stel een afgifte protocol op met daarin duidelijk aan wie beelden mogen worden afgegeven en wat de procedure is.
Denk daarbij ook aan:
- Legitimatieplicht;
- Wijze van afgifte en het gebruik van cybersecurity veilige methoden;
- Instellen watermerk in Genetec

Risico 2. Oneigenlijk gebruik beeldmateriaal. Risico: medium
Advies: cameraprotocol opstellen voor operators met instructies omtrent doelen en de handelwijze bij live meekijken.
Draag zorg voor een privacymask van de omgeving of draag zorg voor het blurren van de gezichten van personen en kentekens uit de omgeving van de gefilmde weg.

Risico 3. Beelden worden te vroeg verwijderd en kunnen niet meer dienen als bewijsmateriaal. Risico Laag.
Advies: protocol vaststellen dat bij ieder incident de gegevens direct worden veiliggesteld.

Risico 4. Slechte informatievoorziening aan betrokkenen. Beelden worden verwijderd voordat een betrokkenen gebruik heeft kunnen maken van het recht op inzage. Risico Hoog/Midden.
Advies: zorg ervoor dat betrokkenen adequaat geïnformeerd worden over hun rechten. Dit kan door de privacyverklaring op de website te zetten van de gemeente. In verband met de diverse soorten van cameragebruik is het wellicht verstandig om 1 Privacyverklaring cameragebruik op te nemen. Hierbij kunnen alle onderdelen van het camera gebruik worden benoemd inclusief de specifieke doelen en opslagtermijnen.
Plaats borden ruim voor het bereik van de 1e camera (wellicht bij ingang Nijmegen) waarbij verwezen wordt naar het feit dat er sprake is van camerabewaking. Voorzie dat bord van een URL die direct verwijst naar de privacy verklaring. Neem in het op te stellen protocol voor centralisten de procedure op voor het melden van datalekken.

Ik adviseer hiermee positief (na uitvoering van de genoemde maatregelen) en daarmee zijn de resterende risico's 'aanvaardbaar'.

Eind 2025 zal deze DPIA op naleving getoetst worden.

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

PK/25/08/2025. DPIA 112.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenss feer	1
Wet open overheid	Art. 5.1 lid 2 sub h	De beveiliging van personen en bedrijven e n het voorkomen van sabotage	3

DPIA Oordeel FG gemeente Nijmegen

Cameratoezicht Selectief Toegang Systeem

Inleiding

Hierbij het oordeel van de FG Gemeente Nijmegen over de DPIA 'Cameratoezicht Selectief Toegang Systeem'. Gekozen is voor een systematische aanpak. Deze is terug te herleiden tot de oordeelsvorming van DPIA's in het algemeen. In deze wordt het 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 welke weergeeft of m.i. het gehele voorstel van maatregelen én te nemen maatregelen bij geconstateerde risico's, tezamen een aanvaardbaar risico vormen bij het gebruik van privacygevoelige gegevens.

In de periode januari tot en met augustus 2025 hebben 5.1.2e , 5.1.2e , 5.1.2e , 5.1.2e 5.1.2e , 5.1.2e , 5.1.2e 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 'Cameratoezicht Selectief Toegang Systeem dd. 12/08/2025. Deze versie vormt de onderlegger voor deze toetsing.

Bij deze DPIA horen de volgende bijlagen:

- geen

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?	Neen.	Akkoord
2. Is het ethisch / politiek bestuurlijk verantwoord?	In het stadscentrum worden veel functies gecombineerd. Dit gebied is in transitie van een plek om te kopen naar een plek om te ontmoeten. Verblijven, beleven en recreëren worden steeds belangrijker. De nadruk ligt hier op de voetganger en op verblijven. De binnenstad is daarom uitsluitend voor motorvoertuigen toegankelijk op genoemde venstertijden.	Akkoord. Venstertijden zijn: ma-di-wo-vr-za: 6-12 uur en 18-23 uur do 6-12 uur zo 6-13 uur.
3. Juridische toets 3.a. Doel / grondslag	3a. *Doel* van deze gegevensverwerkingen: Het doel van de verwerking is het op een gecontroleerde en handhaafbare manier beperken van gemotoriseerd verkeer in het voetgangersgebied van de binnenstad van Nijmegen. *Grondslag* De verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang die aan de gemeente is opgedragen (artikel 6, lid 1 onder e van de AVG). Deze taak vloeit voort uit artikel 2 van de Wegenverkeerswet 1994.	3a. Akkoord. Door middel van kentekenherkenning en automatische toegangscontrole wordt ongeautoriseerd verkeer geweerd, conform het gemeentelijk verkeers- en ontheffingenbeleid. In aanvulling hierop zijn de Beleidsregels ontheffingen artikel 87 RVV 1990 van toepassing, zoals vastgesteld in het Gemeenteblad Nr. 308733 van 13 juli 2023. Deze beleidsregels vormen het kader voor het verlenen en controleren van toegang tot het afgesloten voetgangersgebied.
3.b. Persoonsgegevens Worden bijzondere persoonsgegevens verwerkt?	3.b. Neen. Persoonsgegevens die verwerkt worden zijn: 1. Camerabeelden van voertuigen en personen 2. Camerabeelden van kentekens	3.b. Akkoord. Het doeleinde van de verwerking is niet gericht op het verwerken van bijzondere persoonsgegevens dan wel op het onderscheid maken op grond van een bijzonder persoonsgegeven.
3c. Proportionaliteit	3c. De inbreuk op de persoonlijke levenssfeer is beperkt: alleen voertuigen die het gebied binnenrijden worden vastgelegd via kentekencamera's. Er is geen sprake van continue observatie of monitoring van gedrag binnen het gebied. Camerabeelden worden bewaard binnen een beperkt tijdsbestek en uitsluitend gebruikt voor toegangscontrole en incidentafhandeling.	3c. Akkoord. De gemeente streeft ernaar om de binnenstad autoluw te houden, waarbij het voetgangersgebied alleen toegankelijk is voor voertuigen met een geldige ontheffing.
3.d. Subsidiariteit	3.d. Voor de toegangscontrole tot het voetgangersgebied van de binnenstad is een kentekenherkenningssysteem, een efficiënte, betrouwbare en gebruiksvriendelijke methode is om voertuigen met een geldige ontheffing automatisch te herkennen en toegang te verlenen.	3.d. Akkoord. Gelet op de operationele context van het systeem – waarbij ook tijdelijke, incidentele en telefonisch afgegeven ontheffingen verwerkt moeten kunnen worden – geldt kentekenherkenning als het minst ingrijpende en tegelijk doelmatige middel.

3.e. Persoonsgegevens buiten EER gebruikt?	3.e. Neen.	3.e. Akkoord
3.f. Andere partijen betrokken?	3.f. De gemeente Nijmegen is verwerkingsverantwoordelijke. Er heeft met betrekking tot de overzichtscamera's geen uitwisseling van gegevens plaats. De data van de kentekencamera's worden verwerkt door software van IP-Parking op een lokale server. Het onderhoud van de camera's heeft plaats door Artec Parkeer & Elektra Installateurs te Nijmegen. Dit betreft 1e lijn onderhoud aan de camera's. Artec heeft geen toegang tot de persoonsgegevens. De leverancier van het Genetec Video Management Systeem heeft toegang tot de persoonsgegevens tijdens onderhoud aan de server.	3.f. Akkoord NB. Er zijn geen structurele verwerkers: Bij de verwerking van camerabeelden is geen sprake van structurele inzet van verwerkers in de zin van artikel 4 lid 8 AVG. De observatiecamera's en het bijbehorende VMS worden beheerd vanuit de gemeentelijke VMC. Genetec wordt niet als verwerker aangemerkt, omdat er geen sprake is van zelfstandige verwerking. Toegang tot persoonsgegevens is beperkt tot incidenteel onderhoud, onder toezicht van de gemeente, en op basis van vooraf afgestemde procedures. Aangezien er geen structurele verwerkers zijn aangemerkt, is geen verwerkersovereenkomst opgesteld.
3.g. Hoe lang worden gegevens bewaard en wijze van vernietiging?	3.g. *Bewaartermijn* De gegevens worden 21 dagen bewaard. Deze termijn is noodzakelijk voor de afhandeling van incidenten en schadegevallen. *Vernietiging:* De data worden na 21 dagen automatisch overschreven.	Akkoord. De operationeel verantwoordelijke beheerder is hiervoor verantwoordelijk.
3.h. Hoe worden gegevens beveiligd?	3.h. Het gehele netwerk van camera's, randapparatuur, firewall en Genetec server is geplaatst binnen een LAN-omgeving binnen het eigen glasvezelnetwerk van de gemeente Nijmegen. 5.1.2h 5.1.2h . Vanaf de camera tot aan de server wordt gebruik gemaakt van Radius Authenticatie waardoor het voor onbevoegden onmogelijk is de server te benaderen. 5.1.2h 5.1.2h 5.1.2h . De Genetec server maakt gelaagde autorisatie mogelijk waardoor per functie kan worden ingesteld wie live mag meekijken en wie beelden mag terugkijken en/of veiligstellen. 5.1.2h 5.1.2h 5.1.2h . Beeldmateriaal wordt alleen afgegeven na een vordering door de politie.	Akkoord. Beeldmateriaal kan niet worden gemanipuleerd doordat deze voorzien is van een watermerk. Verder is beeldmateriaal encrypted zodra deze wordt veiliggesteld. De toegang tot de VMC is middels een toegangscontrolesysteem beveiligd. Niet geautoriseerden komen er niet onbegeleid binnen. 5.1.2h 5.1.2h 5.1.2h 5.1.2h 5.1.2h 5.1.2h 5.1.2h . Het operationele toezicht op de gegevensbeveiliging wordt verzorgd door de operationeel verantwoordelijke beheerder.
4. Risico's en voorgestelde maatregelen	In de risico paragraaf staan diverse aanbevelingen opgenomen. Risico 1. Afgifte beeldmateriaal aan de verkeerde persoon. Risico: medium.	Akkoord.

	Advies: stel een afgifte protocol op met daarin duidelijk aan wie beelden mogen worden afgegeven en wat de procedure is. Denk daarbij ook aan: - Legitimatieplicht; - Wijze van afgifte en het gebruik van cybersecurity veilige methoden; - Instellen watermerk in Genetec Risico 2. Oneigenlijk gebruik beeldmateriaal. Risico: medium Advies: cameraprotocol opstellen voor operators met instructies omtrent doelen en de handelwijze bij live meekijken. Duidelijk omschrijven wat er wel en niet mag, welke doelen er zijn maar ook de afspraken vastleggen omtrent het veiligstellen van beelden en het gebruik van smart device waarmee illegaal beeldmateriaal kan worden vastgelegd. Draag zorg voor een privacymask van de verdere omgeving of draag zorg voor het blurren van de gezichten van passanten die de STS niet gebruiken. Risico 3. Beelden worden te vroeg verwijderd en kunnen niet meer dienen als bewijsmateriaal. Risico Laag. Advies: protocol vaststellen dat bij ieder incident de gegevens direct worden veiliggesteld en wat hiervan de maximale bewaartermijn is. Risico 4. Slechte informatievoorziening aan betrokkenen. Beelden worden verwijderd voordat een betrokkenen gebruik heeft kunnen maken van het recht op inzage. Risico Hoog/Midden. Advies: zorg ervoor dat betrokkenen adequaat geïnformeerd worden over hun rechten. Dit kan door de privacyverklaring op de website te zetten van de gemeente. In verband met de diverse soorten van cameragebruik is het wellicht verstandig om 1 Privacyverklaring cameragebruik op te nemen. Hierbij kunnen alle onderdelen van het camera gebruik worden benoemd inclusief de specifieke doelen en opslagtermijnen. Plaats borden ruim voor het bereik van de 1e camera (wellicht bij ingang Nijmegen) waarbij verwezen wordt naar het feit dat er sprake is van camerabewaking. Voorzie dat bord van een URL die direct verwijst naar de privacy verklaring. Neem in het op te stellen protocol voor centralisten de procedure op voor het melden van datalekken.	Binnen zes maanden dient aangegeven te worden op welke wijze de aanbevelingen opgevolgd zijn.

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 zelf kent een 'middelhoog' risico. Deze wordt verlaagd nadat de voorgestelde maatregelen ingevoerd zijn. Hierover dient binnen zes maanden gerapporteerd te worden.
De genoemde maatregelen (in adviesvorm geformuleerd) zijn:

Risico 1. Afgifte beeldmateriaal aan de verkeerde persoon. Risico: medium.
Advies: stel een afgifte protocol op met daarin duidelijk aan wie beelden mogen worden afgegeven en wat de procedure is.
Denk daarbij ook aan:
- Legitimatieplicht;
- Wijze van afgifte en het gebruik van cybersecurity veilige methoden;
- Instellen watermerk in Genetec

Risico 2. Oneigenlijk gebruik beeldmateriaal. Risico: medium
Advies: cameraprotocol opstellen voor operators met instructies omtrent doelen en de handelwijze bij live meekijken.
Duidelijk omschrijven wat er wel en niet mag, welke doelen er zijn maar ook de afspraken vastleggen omtrent het veiligstellen van beelden en het gebruik van smart device waarmee illegaal beeldmateriaal kan worden vastgelegd. Draag zorg voor een privacymask van de verdere omgeving of draag zorg voor het blurren van de gezichten van passanten die de STS niet gebruiken.

Risico 3. Beelden worden te vroeg verwijderd en kunnen niet meer dienen als bewijsmateriaal. Risico Laag.
Advies: protocol vaststellen dat bij ieder incident de gegevens direct worden veiliggesteld en wat hiervan de maximale bewaartermijn is.

Risico 4. Slechte informatievoorziening aan betrokkenen. Beelden worden verwijderd voordat een betrokkenen gebruik heeft kunnen maken van het recht op inzage.
Risico Hoog/Midden.
Advies: zorg ervoor dat betrokkenen adequaat geïnformeerd worden over hun rechten. Dit kan door de privacyverklaring op de website te zetten van de gemeente. In verband met de diverse soorten van cameragebruik is het wellicht verstandig om 1 Privacyverklaring cameragebruik op te nemen. Hierbij kunnen alle onderdelen van het camera gebruik worden benoemd inclusief de specifieke doelen en opslagtermijnen. Plaats borden ruim voor het bereik van de 1e camera (wellicht bij ingang Nijmegen) waarbij verwezen wordt naar het feit dat er sprake is van camerabewaking. Voorzie dat bord van een URL die direct verwijst naar de privacy verklaring. Neem in het op te stellen protocol voor centralisten de procedure op voor het melden van datalekken.

Ik adviseer hiermee positief (na uitvoering van de genoemde maatregelen) en daarmee zijn de resterende risico's 'aanvaardbaar'.

Eind 2025 zal deze DPIA op naleving getoetst worden.

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

PK/25/08/2025. DPIA 113.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenss feer	1
Wet open overheid	Art. 5.1 lid 2 sub h	De beveiliging van personen en bedrijven e n het voorkomen van sabotage	3

DPIA Oordeel FG gemeente Nijmegen

Cameratoezicht Parkeergarages

Inleiding

Hierbij het oordeel van de FG Gemeente Nijmegen over de DPIA ‘Parkeergarages’.
Gekozen is voor een systematische aanpak. Deze is terug te herleiden tot de oordeelsvorming van DPIA’s in het algemeen. In deze wordt het 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 welke weergeeft of m.i. het gehele voorstel van maatregelen én te nemen maatregelen bij geconstateerde risico’s, tezamen een aanvaardbaar risico vormen bij het gebruik van privacygevoelige gegevens.

In de periode januari tot en met augustus 2025 hebben 5.1.2e , 5.1.2e , 5.1.2e , 5.1.2e 5.1.2e , 5.1.2e , 5.1.2e 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 ‘Cameratoezicht Parkeergarages dd. 07/08/2025. Deze versie vormt de onderlegger voor deze toetsing.

Bij deze DPIA horen de volgende bijlagen:

- Verwerkersovereenkomst met IP Parking B.V.

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?	Neen.	Akkoord
2. Is het ethisch / politiek bestuurlijk verantwoord?	Gemeente Nijmegen beheert een aantal gemeentelijke parkeervoorzieningen, waaronder zes openbare parkeergarages en twee parkeerterreinen. Deze parkeerlocaties zijn uitgerust met: • Kentekencamera's bij de in- en uitritten, die onderdeel zijn van het Parkeer Management Systeem (PMS). • Overzichtscamera's, gericht op de verkeersdoorstroming en veiligheid op het terrein zelf. Deze camerabeelden worden live bekeken en opgeslagen binnen de gemeentelijke infrastructuur en maken het mogelijk om toezicht te houden, incidenten af te handelen en de parkeersystemen op afstand aan te sturen.	Akkoord. Het gaat om de volgende locaties: • Parkeergarages: Keizer Karelgarage, Eiermarktgarage, Kelfkensbosgarage, Mariënburggarage, Parkeergarage Centraal Station en Van Schaeck Mathonsingel; • Parkeerterreinen: Plein 1944 en P+R Nijmegen-Noord.
3. Juridische toets 3.a. Doel / grondslag	3a. *Doel* van deze gegevensverwerkingen: De verwerking van camerabeelden in gemeentelijke parkeervoorzieningen dient het doel om het dagelijks beheer van deze parkeergarages en parkeerterreinen effectief, veilig en doelmatig uit te voeren. Dit houdt in dat de gemeente toezicht kan houden op verkeersstromen, storingen kan signaleren en direct kan ingrijpen bij incidenten die de veiligheid, toegankelijkheid of doorstroming belemmeren. *Grondslag* De verwerking is gebaseerd op artikel 6, lid 1 onder e van de Algemene Verordening Gegevensbescherming (AVG): de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang die aan de gemeente is opgedragen. Deze taak is vastgelegd in de Wegenverkeerswet 1994, artikel 2, lid 1. Gemeenten zijn daarin als wegbeheerder verantwoordelijk voor het waarborgen van de verkeersveiligheid, het beschermen van weggebruikers, het bruikbaar houden van de infrastructuur en het bevorderen van de doorstroming.	3a. Akkoord. Op basis van vaste jurisprudentie worden gemeentelijke parkeergarages en parkeerterreinen aangemerkt als onderdeel van de openbare weg. Daarmee valt de inzet van cameratoezicht binnen de uitvoering van een publiekrechtelijke beheertaak.
3.b. Persoonsgegevens Worden bijzondere persoonsgegevens verwerkt?	3.b. Neen. Er worden beelden verwerkt van voertuigen waarbij kentekens zichtbaar in beeld komen en beelden van de bestuurders van de voertuigen en eventuele passagiers, met name wanneer zij zich als voetganger door de parkeergarage of over het parkeerterrein bewegen.	3.b. Akkoord. Het doeleinde van de verwerking is niet gericht op het verwerken van bijzondere persoonsgegevens dan wel op het onderscheid maken op grond van een bijzonder persoonsgegeven.

3c. Proportionaliteit	3c. De persoonsgegevens die verwerkt worden zijn beperkt tot wat noodzakelijk is voor het bereiken van de gestelde doelen. De beelden worden ook niet langer bewaard dan noodzakelijk en toegang tot de beelden is beperkt tot werknemers voor wie het noodzakelijk is om de beelden te bekijken. In de praktijk worden er door klanten claims ingediend met betrekking tot schade door bijvoorbeeld de slagboom. Gemiddeld is dat binnen de periode van 21 dagen.	3c. Akkoord. Kentekenherkenning voor het Parkeer Management Systeem is nodig, omdat het kenteken uitsluitend gebruikt wordt voor het aansturen van de slagbomen en na 21 dagen worden gewist.
3.d. Subsidiariteit	3.d. Parkeermanagement op basis van kentekenherkenning is niet op een minder ingrijpende manier mogelijk die net zo goed werkt. Alle minder ingrijpende mogelijkheden (gebruik van een ticket, QR-code of app) vereisen een handmatige handeling waardoor het doel “vergemakkelijken uitrijden en bevorderen doorstroming” niet kan worden bereikt. Verhalen van schade op de veroorzaker is ook niet op een minder ingrijpende manier te bereiken.	3.d. Akkoord.
3.e. Persoonsgegevens buiten EER gebruikt?	3.e. Neen.	3.e. Akkoord
3.f. Andere partijen betrokken?	3.f. De gemeente Nijmegen is verwerkingsverantwoordelijke. Er vindt met betrekking tot de overzichtscamera’s geen uitwisseling van gegevens plaats. De data van de kentekencamera’s worden verwerkt door IP-Parking . Het onderhoud van de camera’s vindt plaats door Artec Parkeer & Elektra Installateurs te Nijmegen. Dit betreft 1e lijn onderhoud aan de camera’s. Artec heeft geen toegang tot de persoonsgegevens. De leverancier van het Genetec Video Management Systeem heeft toegang tot de persoonsgegevens tijdens onderhoud aan de server.	3.f. Akkoord Met IP Parking B.V. is inmiddels een verwerkersovereenkomst afgesloten
3.g. Hoe lang worden gegevens bewaard en wijze van vernietiging?	3.g. *Bewaartermijn* De beelden van de overzichtscamera’s worden 21 dagen bewaard, tenzij beelden langer moeten worden bewaard voor het afhandelen van schadegevallen. De betreffende beelden worden dan veiliggesteld en bewaard tot na de afhandeling. *Vernietiging:* De data worden na 21 dagen automatisch overschreven.	Akkoord. De operationeel verantwoordelijke beheerder is hiervoor verantwoordelijk.

3.h. Hoe worden gegevens beveiligd?	3.h. Het gehele netwerk van camera's, randapparatuur, firewall en Genetec server is geplaatst binnen een LAN-omgeving binnen het eigen glasvezelnetwerk van de gemeente Nijmegen. 5.1.2h 5.1.2h Vanaf de camera tot aan de server wordt gebruik gemaakt van Radius Authenticatie waardoor het voor onbevoegden onmogelijk is de server te benaderen. 5.1.2h 5.1.2h 5.1.2h. De Genetec server maakt gelaagde autorisatie mogelijk waardoor per functie kan worden ingesteld wie live mag meekijken en wie beelden mag terugkijken en/of veiligstellen. 5.1.2h 5.1.2h 5.1.2h. Beeldmateriaal wordt alleen afgegeven na een vordering door de politie.	Akkoord. Beeldmateriaal kan niet worden gemanipuleerd doordat deze voorzien is van een watermerk. Verder is beeldmateriaal encrypted zodra deze wordt veiliggesteld. De toegang tot de VMC is middels een toegangscontrolesysteem beveiligd. Niet geautoriseerden komen er niet onbegeleid binnen. 5.1.2h 5.1.2h 5.1.2h 5.1.2h 5.1.2h 5.1.2h 5.1.2h. Het operationele toezicht op de gegevensbeveiliging wordt verzorgd door de operationeel verantwoordelijke beheerder.
4. Risico's en voorgestelde maatregelen	In de risico paragraaf staan diverse aanbevelingen opgenomen. Risico 1. Afgifte beeldmateriaal aan de verkeerde persoon. Risico: medium. Advies: stel een afgifte protocol op met daarin duidelijk aan wie beelden mogen worden afgegeven en wat de procedure is. Denk daarbij ook aan: - Legitimatieplicht; - Wijze van afgifte en het gebruik van cybersecurity veilige methoden; - Instellen watermerk in Genetec Risico 2. Oneigenlijk gebruik beeldmateriaal. Risico: medium Advies: cameraprotocol opstellen voor operators met instructies omtrent doelen en de handelwijze bij live meekijken. Duidelijk omschrijven wat er wel en niet mag, welke doelen er zijn maar ook de afspraken vastleggen omtrent het veiligstellen van beelden en het gebruik van smart device waarmee illegaal beeldmateriaal kan worden vastgelegd. Risico 3. Beelden worden te vroeg verwijderd en kunnen niet meer dienen als bewijsmateriaal. Risico Laag. Advies: protocol vaststellen dat bij ieder incident de gegevens direct worden veiliggesteld. Zorg dat betrokkenen adequaat geïnformeerd worden over hun rechten.	Akkoord. Binnen zes maanden dient aangegeven te worden op welke wijze de aanbevelingen opgevolgd zijn.

	Risico 4. Slechte informatievoorziening aan betrokkenen. Beelden worden verwijderd voordat een betrokkenen gebruik heeft kunnen maken van het recht op inzage. Risico Hoog/Midden. Advies: plaats een privacyverklaring “cameratoezicht gemeente Nijmegen” als eerste tegel op de hoofdpagina van het parkeerdeel van de website. Plaats een bord ruim voor het bereik van de 1e camera bij de parkeergarage waarbij verwezen wordt naar het feit dat er sprake is van camerabewaking. Voorzie dat bord van een URL die direct verwijst naar de privacy verklaring. Neem in het op te stellen protocol voor centralisten de procedure op voor het melden van datalekken.	

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 zelf kent een 'middelhoog' risico. Deze wordt verlaagd nadat de voorgestelde maatregelen ingevoerd zijn. Hierover dient binnen zes maanden gerapporteerd te worden.
De genoemde maatregelen (in adviesvorm geformuleerd) zijn:

In de risico paragraaf staan diverse aanbevelingen opgenomen.

Risico 1. Afgifte beeldmateriaal aan de verkeerde persoon. Risico: medium.
Advies: stel een afgifte protocol op met daarin duidelijk aan wie beelden mogen worden afgegeven en wat de procedure is.
Denk daarbij ook aan:
- Legitimatieplicht;
- Wijze van afgifte en het gebruik van cybersecurity veilige methoden;
- Instellen watermerk in Genetec

Risico 2. Oneigenlijk gebruik beeldmateriaal. Risico: medium
Advies: cameraprotocol opstellen voor operators met instructies omtrent doelen en de handelwijze bij live meekijken.
Duidelijk omschrijven wat er wel en niet mag, welke doelen er zijn maar ook de afspraken vastleggen omtrent het veiligstellen van beelden en het gebruik van smart device waarmee illegaal beeldmateriaal kan worden vastgelegd.

Risico 3. Beelden worden te vroeg verwijderd en kunnen niet meer dienen als bewijsmateriaal. Risico Laag.
Advies: protocol vaststellen dat bij ieder incident de gegevens direct worden veiliggesteld.
Zorg dat betrokkenen adequaat geïnformeerd worden over hun rechten.

Risico 4. Slechte informatievoorziening aan betrokkenen. Beelden worden verwijderd voordat een betrokkenen gebruik heeft kunnen maken van het recht op inzage. Risico Hoog/Midden.
Advies: plaats een privacyverklaring "cameratoezicht gemeente Nijmegen" als eerste tegel op de hoofdpagina van het parkeerdeel van de website. TPlaats een bord ruim voor het bereik van de 1e camera bij de parkeergarage waarbij verwezen wordt naar het feit dat er sprake is van camerabewaking. Voorzie dat bord van een URL die direct verwijst naar de privacy verklaring.
Neem in het op te stellen protocol voor centralisten de procedure op voor het melden van datalekken.

Ik adviseer hiermee positief (na uitvoering van de genoemde maatregelen) en daarmee zijn de resterende risico's 'aanvaardbaar'.

Eind 2025 zal deze DPIA op naleving getoetst worden.

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

PK/26/08/2025. DPIA 114.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenss feer	1
Wet open overheid	Art. 5.1 lid 2 sub h	De beveiliging van personen en bedrijven e n het voorkomen van sabotage	4

DPIA Oordeel FG gemeente Nijmegen

DPIA Cameratoezicht Scanauto Parkeren
Inleiding

Hierbij het oordeel van de FG Gemeente Nijmegen over de DPIA 'Cameratoezicht Scanauto Parkeren'.
Gekozen is voor een systematische aanpak. Deze is terug te herleiden tot de oordeelsvorming van DPIA's in het algemeen. In deze wordt het 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 welke weergeeft of m.i. het gehele voorstel van maatregelen én te nemen maatregelen bij geconstateerde risico's, tezamen een aanvaardbaar risico vormen bij het gebruik van privacygevoelige gegevens.

In de periode januari tot en met augustus 2025 hebben 5.1.2e , 5.1.2e , 5.1.2e , 5.1.2e 5.1.2e , 5.1.2e , 5.1.2e en 5.1.2e gewerkt aan de voorbereiding van deze DPIA. Dit heeft geleid tot een aantal op- en aanmerkingen die meegenomen zijn in de definitieve versie DPIA 'Cameratoezicht Scanauto Parkeren' dd. 05/08/2025. Deze versie vormt de onderlegger voor deze toetsing.

Bij deze DPIA horen de volgende bijlagen:

- Verwerkersovereenkomst Sigmax Law Enforcement B.V. en haar zusteronderneming Sigmax ICT Specialisten B.V..

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?	Nee.	Akkoord. Er zijn wel DPIA's gemaakt over het gebruik van de applicatie City Control AVG (DPIA 96) en Wpg (DPIA 92). Deze wordt in deze DPIA ook genoemd bij gebruik van de opslag van gegevens.
2. Is het ethisch / politiek bestuurlijk verantwoord?	Gemeente Nijmegen heeft een integraal parkeerbeleid, waaronder parkeerregulering. Dit parkeerbeleid is omgezet in concrete maatregelen. Een van de concrete maatregelen is het controleren op en sanctioneren van verkeersovertredingen (zoals bv verkeerd parkeren) of het opleggen van een naheffingsaanslag parkeerheffing (zoals bv onbetaald parkeren op een betaalde parkeerplaats). Vanwege het grote gebied dat moet worden gecontroleerd, wordt een scanauto ingezet die met kentekencamera's en daarbij behorende software de kentekens van de geparkeerde auto's vastlegt. Met de gegevensverwerking worden de maatregelen uit het integrale parkeerbeleid uitgevoerd en/of bewaakt.	Akkoord. Met dien verstande dat geadviseerd wordt aan de afdeling Stadsbeheer om dit project aan te melden bij de interne digitale ethische commissie en hen advies te vragen over de ethische aspecten van deze wijze van uitvoering. Vanuit de FG-rol zal de ethische commissie worden gevraagd over deze uitvoeringswijze een advies uit te brengen.
3. Juridische toets 3.a. Doel / grondslag	3a. *Doel* van deze gegevensverwerkingen: De beoogde gegevensverwerking met behulp van de camera's en het City Control-platform dient de volgende doelen: 1. Het registreren van kentekens, voertuigen, locaties en tijdstippen van geparkeerde voertuigen door middel van ANPR-camera's in de scanauto. 2. Het vergelijken van de geregistreerde gegevens met het parkeerrechtenregister in City Control om vermoedelijke parkeerrecht-overtredingen te signaleren. 3. Het doorsturen van vermoedelijke parkeerrecht-overtredingen met bijbehorende gegevens naar een toezichthouder, zodat deze de situatie ter plaatse kan beoordelen en zo nodig een naheffing of bekeuring kan. opleggen. *Grondslag* 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, artikel 6.1 lid e van de AVG; Artikel 225, van de Gemeentewet stelt vast, dat het heffen van belasting door de	3a. Akkoord. NB Bij het uitvoeren van deze DPIA is niet gebleken dat er een algemene maatregel van bestuur is vastgesteld voor de inzet van een scanauto voorzien van camera's met kentekenherkenning.

	gemeente op parkeren van een voertuig, of vanwege een verleende vergunning voor het parkeren van een voertuig, mogelijk is in het kader van parkeerregulering. Artikel 234 en 235 van de gemeentewet beschrijven vervolgens de mogelijkheden tot naheffingsaanslag en belastingverordening. De heffing van parkeerbelasting is vastgesteld in de "Verordening op de heffing en de invordering van parkeerbelastingen gemeente Nijmegen 2025". Waar dit van toepassing is en voor wie dit geldt is vastgesteld in het "Besluit tot aanwijzing en uitwerking betaald parkeren 2025".	
3.b. Persoonsgegevens Worden bijzondere persoonsgegevens verwerkt?	3.b. Nee, in principe niet. Zeer incidenteel kunnen bijzondere categorieën van persoonsgegevens worden afgeleid uit de camerabeelden. Het zou dan moeten gaan om personen verder weg in het beeld. Die worden namelijk niet geblurd omdat ze niet herkend worden als persoon. Deze verwerking wordt in de AVG genuanceerd in overweging 51: "The processing of photographs will not systematically be a sensitive processing (…)".	3.b. Akkoord. Het doeleinde van de verwerking is niet gericht op het verwerken van bijzondere persoonsgegevens dan wel op het onderscheid maken op grond van een bijzonder persoonsgegeven.
3c. Proportionaliteit	3c. De beelden worden in de scanauto niet bewaard/opgeslagen. Toegang tot de beelden via de app van City Control is beperkt tot ambtenaren die geautoriseerd zijn om de beelden te bekijken. Deze ambtenaren zijn of beëdigd of hebben een NDA (geheimhoudingsverklaring) getekend.	3c. Akkoord.
3.d. Subsidiariteit	3.d. Parkeerbeheer door middel van een scanauto met kentekencamera's is niet op een minder ingrijpende manier mogelijk die net zo goed werkt. Alle minder ingrijpende mogelijkheden vereisen een handmatige handeling die de inzet van vele opsporingsambtenaren zou vergen.	3.d. Akkoord. Met name rondom subsidiariteit (uitvoering middels een scan auto) wordt aangeraden om hierbij de interne ethische commissie te betrekken.
3.e. Persoonsgegevens buiten EER gebruikt?	3.e. Neen.	3.e. Akkoord
3.f. Andere partijen betrokken?	3.f. De scanauto en de kentekencamera's zijn eigendom van de gemeente Nijmegen. De bestuurders zijn in dienst van de gemeente Nijmegen. De kentekens worden autonoom verkregen door het maken van opnames. De gefilmde kentekens, voertuig, omgeving en locatie coördinaat worden direct verzonden naar de server van City Control waarvoor reeds een DPIA is geschreven.	3.f. Akkoord Zie DPIA 92 en DPIA 96 Gebruik applicatie City Control AVG (92) en Wpg (96) werkzaamheden.

	Verwerkingsverantwoordelijke: het college van Burgemeesters en Wethouders van de gemeente Nijmegen Verwerker: Sigmax Law Enforcement B.V. en haar zusteronderneming Sigmax ICT Specialisten B.V..	Er is een verwerkersovereenkomst met Sigmax afgesloten. Deze is als bijlage toegevoegd.
3.g. Hoe lang worden gegevens bewaard en wijze van vernietiging?	3.g. *Bewaartermijn* De beelden van de overzichtscamera's worden niet bewaard in de scanauto. Er is slechts sprake van het maken van foto's welke direct worden doorgestuurd naar de City Control server. De gegevens in CityControl worden afhankelijk van de leeftijd van de bijbehorende registratie achter een bijbehorend schot geplaatst. De schotten zijn één, vijf en tien jaar. Na tien jaar wordt de registratie automatisch geanonimiseerd/vernietigd (verwijderen is niet mogelijk). *Vernietiging:* Er is voor deze DPIA alleen sprake van het doorsturen van gegevens en niet van het vernietigen van gegevens. De scanauto heeft geen harde schijf. Dit is daarom niet van toepassing.	Akkoord. Hier wordt het proces doorlopen zoals beschreven in DPIA's 92 en 96.
3.h. Hoe worden gegevens beveiligd?	3.h. Met betrekking tot de technische maatregelen geldt dat de persoonsgegevens vanuit de scanauto versleuteld worden verzonden middels SSL. Deze gegevens worden verzonden naar het Centraal Beheerplatform. De toegang tot de City Control server is beveiligd 5.1.2h waarbij elke cliënt, scanwagen of gebruiker, een unieke sleutel nodig heeft om verbinding te verkrijgen met het Beheerplatform. Zonder deze sleutel is het niet mogelijk om in te loggen op het Centraal Beheerplatform. Alle toegang tot de City Control Server wordt apart gelogd en is inzichtelijk voor de daartoe bevoegde gebruikers.	Akkoord. Er is geen sprake van opslag in de scanauto. Zodra de chauffeur plaats neemt in de scanauto logt deze in op het platform met deze unieke code en start met de werkzaamheden. Zie DPIA 92 en DPIA 96.
4. Risico's en voorgestelde maatregelen	In de risico paragraaf staan drie aanbevelingen opgenomen. 1. Diefstal Scanauto. Het risico hierop is midden. Advies: Maak een cameraprotocol waarin alle ge- en verboden worden opgenomen alsmede de werkwijze met de scanauto. Neem hierin op dat de chauffeur als deze uitstapt de motor	Akkoord. Binnen zes maanden dient aangegeven te worden op welke wijze de aanbevelingen zijn opgevolgd. Diefstal van een scanauto die in bedrijf is kan leiden tot opnames van kentekens in maar ook buiten Nijmegen.

	van het voertuig uit doet en de sleutel bij zich houdt. Onderzoek tevens of er op afstand door de chauffeur kan worden uitgelogd. 2. Onvoldoende transparantie richting betrokkenen Advies: Zorg voor een zichtbare privacyverklaring over cameratoezicht (incl. scanauto) op de parkeersectie van de website, vul de algemene privacyverklaring aan met cameratoezicht, beschrijf de rechten van betrokkenen en een contactadres, geef op de boetepagina uitleg over de scanauto en verwerk in het protocol een procedure voor het melden van datalekken. 3. Datalek door chauffeur Scanauto: Advies: Technisch gezien is het mogelijk om een foto te maken per telefoon van het scherm in de auto. Met een protocol leg je vast wat er wel of niet gedaan mag worden en kan het risico verlaagd worden.	

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 zelf kent een 'middelhoog' risico. Deze wordt verlaagd nadat de voorgestelde maatregelen ingevoerd zijn. Hierover dient binnen zes maanden gerapporteerd te worden.
De genoemde maatregelen (in adviesvorm geformuleerd) zijn:

In de risico paragraaf staan drie aanbevelingen opgenomen.

1. Diefstal Scanauto.

Het risico hierop is midden.

Advies: Maak een cameraprotocol waarin alle ge- en verboden worden opgenomen alsmede de werkwijze met de scanauto. Neem hierin op dat de chauffeur als deze uitstapt de motor van het voertuig uit doet en de sleutel bij zich houdt. Onderzoek tevens of er op afstand door de chauffeur kan worden uitgelogd.

2. Onvoldoende transparantie richting betrokkenen

Advies: Zorg voor een zichtbare privacyverklaring over cameratoezicht (incl. scanauto) op de parkeersectie van de website, vul de algemene privacyverklaring aan met cameratoezicht, beschrijf de rechten van betrokkenen en een contactadres, geef op de boetepagina uitleg over de scanauto en verwerk in het protocol een procedure voor het melden van datalekken.

3. Datalek door chauffeur Scanauto:

Advies: Technisch gezien is het mogelijk om een foto te maken per telefoon van het scherm in de auto.

Met een protocol leg je vast wat er wel of niet gedaan mag worden en kan het risico verlaagd worden.

NB.
Geadviseerd wordt aan de afdeling Stadsbeheer om dit project aan te melden bij de interne digitale ethische commissie en hen advies te vragen over de ethische aspecten van deze wijze van uitvoering.
(Ook) Vanuit de FG-rol zal de ethische commissie worden gevraagd over deze uitvoeringswijze een advies uit te brengen.

Ik adviseer hiermee positief (na uitvoering van de genoemde maatregelen) en daarmee zijn de resterende risico's 'aanvaardbaar'.

Eind 2026 zal deze DPIA op naleving (mede van de uitvoering van de adviezen) getoetst worden.

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

KR/18/09/2025. DPIA 115.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenss feer	1
Wet open overheid	Art. 5.1 lid 2 sub h	De beveiliging van personen en bedrijven e n het voorkomen van sabotage	4

DPIA Oordeel FG gemeente Nijmegen

DPIA Lokale aanpak isolatie

Inleiding

Hierbij het oordeel van de FG Gemeente Nijmegen over de DPIA 'Lokale aanpak isolatie'. Gekozen is voor een systematische aanpak. Deze is terug te herleiden tot de oordeelsvorming van DPIA's in het algemeen. In deze wordt het 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 welke weergeeft of m.i. het gehele voorstel van maatregelen én te nemen maatregelen bij geconstateerde risico's, tezamen een aanvaardbaar risico vormen bij het gebruik van privacygevoelige gegevens.

In de periode februari 2024 tot september 2025 hebben 5.1.2e, 5.1.2e, 5.1.2e, 5.1.2e, 5.1.2e, 5.1.2e, 5.1.2e 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 'Lokale aanpak isolatie' d.d. 30 september 2025.
Deze versie vormt de onderlegger voor deze toetsing.

Bij deze DPIA horen de volgende bijlage:

- Bijlage 1: Doelbinding
- Bijlage 2: Gegevensuitwisselingsovereenkomst
- Bijlage 3: Monitoringsbestanden ter SiSa verantwoording
- Bijlage 4: Schematisch overzicht proces en gegevens

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?	Nee.	Akkoord.
2. Is het ethisch / politiek bestuurlijk verantwoord?	Ja. Het project geeft uitvoering aan het collegeakkoord, het Programma Energie Besparen Woningen, het Uitvoeringsplan Isoleren Woningen, het Nationaal Isolatieprogramma (NIP), de Specifieke Rijksuitkering Lokale Aanpak Isolatie (Spuk LAI), de Specifieke Rijksuitkering Energiearmoede en de Gebiedsgerichte Aanpak Isolatie voortkomend uit het programma Energie besparen woningen en de Spuk LAI. In het collegeakkoord 'Ons Nijmegen, Stad van Iedereen' staat dat het gemeentebestuur extra wil inzetten op het isoleren van woningen. Om deze ambitie rond de opgave voor energie besparen concreet te maken heeft de gemeenteraad 28 februari 2023 het Programma Energie Besparen Woningen 2023- 2030 (PEBW) vastgesteld. Dit programma is onderverdeeld in vier actielijnen te weten: 1) gebiedsgerichte aanpak slecht geïsoleerde koopwoningen met een lage WOZ (met speciale aandacht voor huishoudens met het risico op energiearmoede); 2) grootschalige aanpak huurwoningen vastgelegd in de prestatieafspraken; 3) aanpak koopwoningen op eigen regie eigenaren en; 4) besparingen op de energierekening met eenvoudige maatregelen. Met deze gegevensverwerking wordt het mogelijk een specifieke doelgroep in Nijmegen gericht te benaderen om daarmee een adequate besteding van de Spuk LAI en de Spuk energiearmoede middelen te bewerkstelligen.	Akkoord Met dien verstande dat geadviseerd wordt om dit project aan te melden bij de interne digitale ethische commissie en hen advies te vragen over de ethische aspecten van deze wijze van uitvoering. Vanuit de FG-rol zal de ethische commissie worden gevraagd over deze uitvoeringswijze een advies uit te brengen.
3. Juridische toets 3.a. Doel / grondslag	3a. *Doel* van deze gegevensverwerkingen: De verwerking is noodzakelijk om de juiste doelgroep te bereiken. Juist de inwoners die nog niet bezig zijn met verduurzaming, wilt de gemeente activeren en begeleiden naar een isolatiemaatregel. Dit vraagt een proactieve benadering. Gebleken is dat een huis aan huis aanpak hier het beste werkt.	3a. Akkoord.

	Grondslag De verwerking van persoonsgegevens in het kader van het project *Lokale Aanpak Isolatie* vindt plaats op basis van artikel 6, eerste lid, onder e van de Algemene Verordening Gegevensbescherming (AVG): *"de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen."* De gemeente voert met dit project een taak van algemeen belang uit die bestaat uit het bevorderen van energiebesparing, het bestrijden van energiearmoede en het verbeteren van de kwaliteit en duurzaamheid van de woningvoorraad. Deze taak is geworteld in diverse wettelijke en beleidsmatige kaders, waaronder: • De Klimaatwet (artikel 2); • Onder de Omgevingswet (artikel 1.3, artikelen 2.1 en 2.2) • De Wet Milieubeheer (artikel 5.1 en 5.4); • Het Nationaal Isolatieprogramma (NIP) en de Regeling Reductie Energiegebruik Woningen (RREW); • De Gemeentewet (artikel 108 en 149 en 160); • De Wet publieke gezondheid; • Lokale beleidsnota's en duurzaamheidsprogramma's, waarin de gemeentelijke ambitie tot het versterken van sociale, economische en ecologische leefomstandigheden is verankerd. Daarnaast zijn er nog een aantal specifieke wetsartikelen die het verwerken van de persoonsgegevens afkomstig uit bepaalde bronnen toestaan: • Specifiek voor de verwerking van WOZ-gegevens: Staatsblad 2025, nr. 103; • Artikel 47 Kadasterwet. De gegevensverwerking is noodzakelijk om huishoudens gericht te kunnen benaderen, maatwerkondersteuning te bieden, en de effectiviteit en doelmatigheid van het beleid te waarborgen. Ter onderbouwing van het gebruik van brongegevens zijn in bijlage 1 van deze DPIA doelbindingstoetsen uitgevoerd.	De gemeente heeft doelbindingstoetsen uitgevoerd. Door de doelbindingstoetsen uit te voeren motiveert de gemeente dat de verwerkingen in lijn liggen met de doeleinden waarvoor de gegevens mogen worden gebruikt. Het gaat niet om verdergaande verwerking, profilering of commercieel gebruik, maar om toepassing binnen hetzelfde juridische en beleidsdomein.

3.b. Persoonsgegevens Worden bijzondere persoonsgegevens verwerkt?	3.b. Er worden geen bijzondere persoonsgegevens verwerkt. De volgende persoonsgegevens worden verwerkt: Eigenaar-bewoners van woningen en appartementen die binnen de LAI-doelgroep vallen, worden aangeschreven door de gemeente. Voor de selectie van bewoners (LAI-doelgroep) die worden aangeschreven worden uit de databases de volgende persoonsgegevens verwerkt: • WOZ-waarde; • Wel of geen eigenaar-bewoner (eigendomsgegevens en bewonersgegevens); • Adres; • Soort woning; • Wel of niet onderdeel van een VVE; • Bouwjaar; • Vastgesteld energielabel; • BAG ID.	3.b. Akkoord. Deze DPIA kent een lange aanloop. Er is eerder een DPIA opgesteld specifiek betreffende de vraag of, binnen deze aanpak, het lijstwerk energietoeslag gekoppeld mag worden aan andere data om op deze manier in contact te kunnen komen met de doelgroep huiseigenaren met energiearmoede. Uitkomst van dat onderzoek was dat, op grond van de geheimhoudingsplicht binnen de Participatiewet, koppeling van deze data niet mogelijk bleek. Dit werd bevestigd door het advies van advocatenkantoor Hekkelman. Om deze reden is het lijstwerk energietoeslag geen onderdeel van voorliggende DPIA.

3c. Proportionaliteit	3c. Er worden uitsluitend gegevens verwerkt die noodzakelijk zijn voor het realiseren van het doel, namelijk het bereiken van bewoners met een relevante isolatiebehoefte. Hieronder wordt per gegevenscategorie toegelicht waarom verwerking noodzakelijk is: • Adresgegevens (straatnaam, huisnummer, postcode en woonplaats) zijn essentieel om woningen te kunnen selecteren en te benaderen. Zonder deze gegevens is het onmogelijk om de doelgroep te definiëren of hen op woningniveau te bereiken. • Eigenaarschap (of een woning bewoond wordt door de eigenaar) of VvE is noodzakelijk, omdat de LAI zich richt op eigenaar-bewoners. Huurders vallen buiten de reikwijdte van het programma. • De WOZ-waarde van een woning biedt een indicatie van de woningwaarde. Enkel woningen onder een bepaalde WOZ-waarde vallen binnen de doelgroep. • Het energielabel, evenals woningkenmerken zoals type woning, bouwjaar en constructieve eigenschappen, zijn nodig om de isolatiegeschiktheid van woningen vast te stellen. • Het BAG-ID (Basisregistratie Adressen en Gebouwen) is een technisch hulpmiddel voor het koppelen en verifiëren van adresgegevens uit verschillende bronnen. Het BAG-ID wordt alleen intern gebruikt binnen datakoppelingen en heeft geen communicatiefunctie.	3c. Akkoord Er vindt geen verwerking van bijzondere of gevoelige persoonsgegevens (zoals gezondheid of inkomen) plaats. Daarnaast zijn de gekozen criteria (bouwjaar, energielabel, eigendom, WOZ-waarde) rechtstreeks gekoppeld aan de beleidsdoelstelling (energiearmoede en isolatiebehoefte). Ook de combinatie van bronnen is onderbouwd in de DPIA. In het proces wordt op de volgende wijze rekening gehouden met dataminimalisatie: • Burgers die niet willen deelnemen aan de aanpak en dit naar aanleiding van de brief aangeven, worden door de Gemeente verwijderd uit de bestanden. Tevens wordt met de externe adviespartij afgesproken dat zij in dat geval ook de persoonsgegevens van die burger verwijderen. Deze afspraak is neergelegd in de gegevensuitwisselingsovereenkomst. • Burgers die niet willen deelnemen aan de aanpak en dit naar aanleiding van het contact met de externe adviespartij aangeven, worden verwijderd uit de bestanden van de adviespartij alsook de Gemeente. Deze afspraak is neergelegd in de gegevensuitwisselingsovereenkomst. • De externe adviespartij ontvangt enkel de gegevens noodzakelijk voor het contact opnemen, zie stroomschema dataminimalisatie. • De gemeente zorgt er expliciet voor dat kopieën worden verwijderd, zie stroomschema dataminimalisatie. • De gemeente verwerkt gegevens op adresniveau, het is de keuze van de bewoner-eigenaar/VvE om contactgegevens te verstrekken aan de externe adviespartij.
3.d. Subsidiariteit	3.d. Om de doelgroep te bepalen, een brief te kunnen versturen naar de woning in de doelgroep en advies door te externe derde partij mogelijk te maken, moeten er bepaalde (persoons)gegevens worden verwerkt. In de praktijk zijn er geen werkbare alternatieven voorhanden die hetzelfde doel kunnen bereiken. Om woningen met een laag energielabel, onder een bepaalde WOZ-waarde	3.d. Akkoord Met name rondom subsidiariteit wordt aangeraden om hierbij de interne ethische commissie te betrekken.

	te identificeren, zijn specifieke gegevens zoals bouwjaar, woningtype, energielabel, WOZ-waarde en eigenaarsstatus onmisbaar. Het gebruik van geaggregeerde of statistische gegevens op wijk- of buurtniveau is hiervoor ontoereikend, omdat het geen directe toewijzing van maatregelen aan individuele woningen mogelijk maakt. Evenmin is het realistisch om het programma volledig te baseren op vrijwillige aanmeldingen. De doelgroep bestaat grotendeels uit huishoudens die isolatiemaatregelen niet spontaan aanvragen vanwege beperkte informatie, middelen of vertrouwen. Een uitsluitend passieve benadering zou resulteren in significant onderbereik en zou leiden tot een ongelijk effect van het beleid. Juist een actieve, op gegevens gebaseerde benadering is noodzakelijk om deze inwoners wél te bereiken. Deze verwerking vormt de minst ingrijpende optie die nog effectief is. Er bestaat op dit moment geen redelijk alternatief dat hetzelfde resultaat kan bereiken met minder impact op de persoonlijke levenssfeer.	
3.e. Persoonsgegevens buiten EER gebruikt?	3.e. Neen.	3.e. Akkoord
3.f. Andere partijen betrokken?	3.f. - De gemeente is verwerkingsverantwoordelijke. - De externe adviespartij is zelfstandig verwerkingsverantwoordelijke. Met deze externe adviespartij wordt een gegevensuitwisselingsovereenkomst afgesloten.	3.f. Akkoord, mits de gegevensuitwisselingsovereenkomst voorafgaand aan de verstrekking van gegevens met de externe adviespartij wordt afgesloten. In deze overeenkomst dient expliciet opgenomen te worden dat de gegevens die de adviespartij ontvangt van de gemeente Nijmegen niet voor andere doeleinden mogen worden gebruikt dan voor de opdracht die expliciet vanuit de gemeente Nijmegen aan hen is gegeven.
3.g. Hoe lang worden gegevens bewaard en wijze van vernietiging?	3.g. *Bewaartermijn en vernietiging:* Teams Persoonsgegevens van betrokkene die deelnemen, worden maximaal 24 maanden na het succesvol afronden van de verantwoording aan het Rijk bewaard in verband met transparantie, verantwoordingsplicht en herleidbaarheid. Daarna worden deze gegevens vernietigd. Persoonsgegevens van bewoners die reeds zijn benaderd en hebben aangegeven niet te willen deelnemen aan het isolatieprogramma, worden uit bestanden verwijderd (ook zo afgesproken met de externe adviespartij).	Akkoord. In de gegevensuitwisselingsovereenkomst dient expliciet opgenomen te worden binnen welke termijn de adviespartij de gegevens dient te vernietigen.

	Emails E-mails die in Outlook blijven staan worden op een meer simpele wijze bewaard of vernietigd: • Alle medewerkers mogen onbelangrijke en persoonlijke e-mails nog steeds zelf vernietigen, als ze uit dienst of met pensioen gaan en ook tussentijds. • Alle overgebleven e-mails worden na 7 jaar vernietigd, ook als medewerkers vertrokken zijn bij de gemeente Nijmegen, of met pensioen gegaan zijn. Het beheer van deze "wees"-mailboxen van vertrokken medewerkers (voor bijv. toegang bij informatie in het kader van informatieverzoeken) dient bij hiertoe gemachtigde secretariaten en BDI te komen liggen. De afdeling is zelf verantwoordelijk voor opschoon acties.	
3.h. Hoe worden gegevens beveiligd?	3.h. • Beveiligde teams omgeving met enkel toegang voor geautoriseerde medewerkers; • Data uitwisseling via Zivver; • Verwerkersovereenkomst en gegevensuitwisselingsovereenkomsten met betrokken derde partijen; • Logging in de systemen; • Er worden beveiligingseisen gesteld aan de externe adviespartij in overleg met de security officer.	Akkoord.
4. Risico's en voorgestelde maatregelen	De risico's en adviezen zijn beschreven in de DPIA (zie paragraaf 9.1).	Akkoord. Benoemde risico's zijn reëel en de voorgestelde mitigerende maatregelen zijn afdoende. De FG onderstreept daarbij nadrukkelijk het belang om betrokkenen geruime tijd voor het verstrekken van gegevens aan derden zo volledig mogelijk te informeren (over het hoe en waarom, welke gegevens uit welke bronnen worden samengevoegd en rechten die betrokkenen o.g.v. de AVG kunnen uitoefenen). Dit, zodat de betrokkenen ervoor kunnen kiezen om niet mee te doen en hun gegevens verwijderd kunnen worden. Idealiter zou zijn dat de gegevens dus in dergelijke gevallen helemaal niet hoeven te worden doorgegeven aan de externe adviespartij.

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 een 'middelhoog' risico.
Dit vanwege de samenvoeging van meerdere bronnen met uiteenlopende oorspronkelijke doelen. Door deze bronnen te combineren ontstaat een omvangrijk en herleidbaar beeld van individuele huishoudens waarin eigendom, bewoning, woningkenmerken en energieprestatie worden samengebracht. Hoewel elk van de afzonderlijke verwerkingen op zichzelf verenigbaar is met de oorspronkelijke doelstelling van de bronregistratie, maakt de samenvoeging dat extra zorgvuldig moet worden gekeken naar doelbinding, proportionaliteit, subsidiariteit en beveiliging van gegevens.
Daarnaast brengt de huis-aan-huisaanpak, door haar proactieve karakter, een verhoogd risico met zich mee omdat betrokkenen onverwachts kunnen worden benaderd. Hierdoor bestaat het risico dat zij onvoldoende geïnformeerd zijn over de verwerking van hun gegevens of geen reële mogelijkheid hebben om hun rechten uit te oefenen. Dit vraagt om extra aandacht voor transparantie en beperking van de gegevensverwerking tot wat strikt noodzakelijk is (dataminimalisatie).
Het voorgaande maakt dat geadviseerd wordt om dit project aan te melden bij de interne digitale ethische commissie en hen advies te vragen over de ethische aspecten van deze wijze van uitvoering. Vanuit de FG-rol zal de ethische commissie worden gevraagd over deze uitvoeringswijze een advies uit te brengen.

Grootste risico's zijn dat de gegevens voor andere doeleinden worden gebruikt en betrokkenen onvoldoende worden geïnformeerd en daarmee niet in staat worden gesteld om hun rechten op grond van de AVG uit te oefenen. De mitigerende maatregelen die worden beschreven in de DPIA verlagen deze risico's.
Aanvullend hierop beveelt de FG aan om in de gegevensuitwisselingsovereenkomst expliciet op te nemen dat de gegevens die de adviespartij ontvangt van de gemeente Nijmegen niet voor andere doeleinden mogen worden gebruikt dan voor de opdracht die expliciet vanuit de gemeente Nijmegen aan hen is gegeven. De FG onderstreept daarbij nadrukkelijk het belang om betrokkenen geruime tijd voor het verstrekken van gegevens aan derden zo volledig mogelijk te informeren (over het hoe en waarom, welke gegevens uit welke bronnen worden samengevoegd en rechten die betrokkenen o.g.v. de AVG kunnen uitoefenen).

Eind 2026 zal deze DPIA op naleving getoetst worden.
Speciale aandacht zal gegeven worden aan:
Dataminimalisatie in het proces en opvolging geven aan ingekomen verzoeken van betrokkenen.

Ik adviseer hiermee positief en daarmee zijn de resterende risico's 'aanvaardbaar'.

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

KR/24/10/2025. DPIA 116

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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

DPIA Oordeel FG gemeente Nijmegen

DPIA Meldpunt Wet goed verhuurderschap

Inleiding

Hierbij het oordeel van de FG Gemeente Nijmegen over de DPIA 'Meldpunt Wet goed verhuurderschap' (in het vervolg: het meldpunt). Gekozen is voor een systematische aanpak. Deze is terug te herleiden tot de oordeelsvorming van DPIA's in het algemeen. In deze wordt het 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 welke weergeeft of m.i. het gehele voorstel van maatregelen én te nemen maatregelen bij geconstateerde risico's, tezamen een aanvaardbaar risico vormen bij het gebruik van privacygevoelige gegevens.

In de periode december 2023 tot september 2025 hebben 5.1.2e, 5.1.2e, 5.1.2e, 5.1.2e 5.1.2e 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 'Meldpunt wet goed verhuurderschap' d.d. 5 september 2025.
Deze versie vormt de onderlegger voor deze toetsing.

Bij deze DPIA horen de volgende bijlage:

- Bijlage 2: Verwerkersovereenkomst Stichting Huurteams/Meldpunt;
- Bijlage 3: Verwerkersovereenkomst Roxit (Rx.Mission);
- Bijlage 4: Dienstverleningsovereenkomst meldpunt (Stichting Huurteams Nijmegen);
- Bijlage 5: Archiveringsafspraken.

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?	Nee.	Akkoord.
2. Is het ethisch / politiek bestuurlijk verantwoord?	Ja. De Wet goed verhuurderschap (WGV) verplicht gemeenten om een meldpunt in te richten waar meldingen over ongewenst verhuurgedrag van particulieren verhuurders en verhuurbemiddelaars kunnen worden gedaan en om toezicht te houden op en handhaving toe te passen bij overtredingen van de wet. De gemeente heeft het meldpunt belegd bij de Stichting Huurteams Nijmegen (SHN).	Akkoord.
3. Juridische toets 3.a. Doel / grondslag	3a. *Doel* van deze gegevensverwerkingen: Het primaire doel is bescherming van huurders tegen slecht verhuurderschap en het bevorderen van een eerlijke en veilige woonomgeving. Door meldingen te ontvangen en te verwerken krijgt de gemeente inzicht in potentiële overtredingen van de wet en kan zij gerichte maatregelen nemen om misstanden te herstellen of te voorkomen. Voor een effectieve handhaving is het noodzakelijk dat ook gegevens van verhuurders worden verwerkt. *Grondslag* Om te voldoen aan de wettelijke verplichting om een meldpunt in te richten op grond van de Wet goed verhuurderschap, is het noodzakelijk om persoonsgegevens te verwerken. Omdat de wet niet expliciet voorschrijft welke gegevens verwerkt moeten worden, is de verwerking gebaseerd op de grondslag taak van algemeen belang (artikel 6, lid 1, sub e AVG en artikel 6 lid 3 AVG). In dit geval komt de wettelijke plicht voort uit de Wet goed verhuurderschap.	3a. Akkoord. Omdat de wet geen uitputtende opsomming geeft van de persoonsgegevens die verwerkt moeten worden, is het logisch om te spreken van een noodzakelijke verwerking voor het uitvoeren van de taak van algemeen belang. Het gaat hier om de bescherming van huurders en het voorkomen en aanpakken van malafide verhuurpraktijken.
3.b. Persoonsgegevens	3.b. In de DPIA staat beschreven welke categorieën persoonsgegevens worden verwerkt van de melder en verhuurder. Het meldpunt is primair gericht op het ontvangen en behandelen van meldingen van de doelgroep (voormalig) huurders. Andere	3.b. Akkoord. Melders kunnen ervoor kiezen om anoniem te melden. Dit houdt in dat zij geen naam, e-mailadres of telefoonnummer achterlaten. Bij

Worden bijzondere persoonsgegevens verwerkt?	melders wordt medegedeeld dat hun melding niet onder de WGV valt en eventueel geadviseerd een ander 'loket' te zoeken. Persoonsgegevens van derden worden alleen verwerkt voor zover dit noodzakelijk is voor de beoordeling of onderbouwing van de melding, maar ook voor eventuele vervolgacties zoals handhaving of signalering. Het is mogelijk dat er sprake is van bijzondere persoonsgegevens in de context van meldingen bij het externe meldpunt, afhankelijk van de aard van de melding. Deze gegevens vereisen extra bescherming vanuit de AVG omdat ze gevoeliger van aard zijn. Bijvoorbeeld: Als de melder meldt dat hij/zij gediscrimineerd wordt op basis van ras of etnische achtergrond.	anonieme meldingen wordt geen contact opgenomen met de melder, tenzij deze alsnog op eigen initiatief contact opneemt. Anonieme meldingen worden in beginsel wel beoordeeld en geregistreerd, maar de mogelijkheden tot dossieropbouw of handhaving zijn vaak beperkter. Niet-relevante persoonsgegevens worden niet opgenomen in het dossier en zo mogelijk verwijderd of geanonimiseerd. Gegevens worden in ieder geval nooit gedeeld met externe partijen of er moet nadrukkelijk toestemming zijn verleend. Deze gegevens worden enkel bewaard indien ze relevant zijn voor de melding.
3c. Proportionaliteit	3.c. De gegevens worden uitsluitend verwerkt om de melding te kunnen beoordelen en te bepalen of sprake is van een overtreding van de Wet goed verhuurderschap. De inbreuk op de privacy van de verhuurder is beperkt en proportioneel, omdat de gegevens uitsluitend worden gebruikt voor het specifieke doel van behandeling melding en handhaving. De gegevens worden zorgvuldig beschermd en zijn alleen toegankelijk voor degenen die direct betrokken zijn bij de afhandeling van de melding. Gezien het belang van effectieve afhandeling van de melding en de bescherming van de melder, is de beperkte inbreuk op de privacy gerechtvaardigd.	3c. Akkoord. Daarbij geldt dat niet méér gegevens worden vastgelegd dan strikt noodzakelijk is. Informatie die niet relevant blijkt, wordt niet bewaard of verwijderd zodra dit duidelijk is. Zodra de gegevens niet langer nodig zijn, worden deze verwijderd.
3.d. Subsidiariteit	3.d. Alternatief zou zijn om minder gegevens te vragen of meldingen enkel anoniem te laten doen. Anonieme meldingen kunnen huurders de kans geven misstanden te rapporteren zonder angst voor repercussies. Echter, er zijn belangrijke beperkingen. Anonieme meldingen bieden vaak niet genoeg details om effectief onderzoek te doen, zoals data, namen of locaties. Dit bemoeilijkt verificatie en gericht handelen. Bovendien is	3.d. Akkoord.

	terugkoppeling naar de melder niet mogelijk, waardoor aanvullende informatie niet kan worden verkregen. Voor effectieve handhaving is een compleet dossier nodig, wat moeilijk te realiseren is bij anonieme meldingen. Desondanks blijft het belangrijk en wettelijk noodzakelijk om de mogelijkheid voor anonieme meldingen te bieden. Meldingen die niet onder de wet vallen worden verwijderd.	
3.e. Persoonsgegevens buiten EER gebruikt?	3.e. Neen.	3.e. Akkoord
3.f. Andere partijen betrokken?	3.f. De gegevens worden uitgewisseld tussen het meldpunt (Stichting Huurteams Nijmegen), de Gemeente en het systeem Rx.Mission. De gemeente is verwerkingsverantwoordelijke. Stichting Huurteams Nijmegen en Rx.Mission zijn verwerkers.	3.f. Akkoord Er is met het meldpunt een dienstverleningsovereenkomst incl. archiveringsafspraken en een verwerkingsovereenkomst afgesloten. Met Roxit (Rx.Mission) is vanuit de BRIKS afdeling een verwerkersovereenkomst afgesloten. Beide overeenkomsten maken onderdeel uit van deze DPIA.
3.g. Hoe lang worden gegevens bewaard en wijze van vernietiging?	3.g. *Bewaartermijn* De termijnen die zijn vastgesteld in het Besluit Goed Verhuurderschap worden gehanteerd. De gegevens worden verwijderd: a. Op het moment dat is vastgesteld dat de melding ongegrond/onjuist is. b. Direct nadat melder is doorverwezen naar een andere instantie, tenzij gegevens bewaard moeten blijven t.b.v. dossieropbouw. c. Op het moment dat besloten wordt niet over te gaan tot bestuurlijke handhaving, tenzij gegevens bewaard moeten blijven t.b.v. dossieropbouw. d. Op het moment dat besluit tot handhaving als gevolg van de melding onherroepelijk is. *Vernietiging:* Vernietiging vindt plaats als aan de volgende voorwaarden is voldaan: - Wettelijke bewaartermijn is verstreken. - Gegevens zijn niet langer noodzakelijk voor het doel waarvoor ze oorspronkelijk zijn verwerkt. Nijmegen is als bevoegd gezag (taak wettelijk opgedragen aan de gemeente)	Akkoord. Bewaartermijn in het kader van dossieropbouw: vier jaar na het tijdstip waarop de melding is gedaan worden de gegevens verwijderd. Uitzondering hierop zijn juridische vervolgprocedures die kunnen maken dat gegevens langer kunnen worden bewaard (5 – 10 jaar). Zodra de juridische of administratieve noodzaak vervalt, worden de gegevens verwijderd of geanonimiseerd.

	verantwoordelijk voor deze taak en voor de informatie die daaruit voortkomt. Dus ook vernietiging. Het Meldpunt archiveert en vernietigt gegevens zelfstandig in hun eigen systemen. Dit wordt geborgd in de samenwerkingsovereenkomst met bijlage over archiveringsaspecten. Binnen Nijmegen: • **Corsa**: De archivering en vernietiging in Corsa wordt beheerd door BDI. Zij stellen de vernietigingslijsten op en coördineren de uitvoering, met instemming van de proceseigenaar. • **Rx.Mission**: In RX.Mission ligt de verantwoordelijkheid voor beheer en vernietiging bij de proceseigenaar. BDI monitort periodiek de kwaliteit van de dossierregistratie en archiefprocessen, inclusief vernietiging.	In de loop van 2025 maakt het meldpunt, in samenwerking met de gemeente, gebruik van Rx.Mission voor het beheer en de vernietiging van gegevens. Dit systeem wordt ingericht volgens de principes van privacy by design en archiving by design, wat betekent dat de bescherming van persoonsgegevens en de tijdige vernietiging al in de ontwerpfase van het systeem zijn geïntegreerd. De procesverantwoordelijke speelt een centrale rol bij de inrichting en het beheer van archiverings- en vernietigingsprocessen binnen Rx.Mission, met advies van BDI.
3.h. Hoe worden gegevens beveiligd?	3.h. Momenteel verstrekt het Meldpunt de gegevens alleen aan het contact binnen de Gemeente Nijmegen, via SharePoint. Dit platform is alleen toegankelijk voor de personen die daarvoor zijn aangemeld, zodat de gegevens goed beveiligd blijven. Daarnaast maakt het meldpunt gebruik van hun eigen systeem, Vesta, dat ISO gecertificeerd is. In 2025 is het plan om over te stappen naar het systeem RX.Mission. Dit systeem biedt een verhoogde beveiliging en is ontworpen om beter te voldoen aan de privacywetgeving, met extra waarborgen voor de gegevensbeveiliging en -privacy en (automatische) verwijdering van gegevens. Het gebruik van RX.Mission zorgt ervoor dat de gegevens van melders op een veilige, transparante en verantwoorde manier worden verwerkt en opgeslagen.	Akkoord. Het toezicht op de beveiliging van de gegevens is georganiseerd door zowel het Meldpunt Huurders Nijmegen als de Gemeente Nijmegen. Beiden zorgen ervoor dat er regelmatige controles en audits plaatsvinden om de beveiliging te waarborgen. Medewerkers krijgen toegang op basis van hun rol en de noodzaak voor gegevensverwerking. Toegang tot Rx.Mission is strikt beperkt tot geautoriseerde medewerkers van de gemeente Nijmegen en, indien noodzakelijk, medewerkers van Stichting Huurteams Nijmegen (meldpunt).
4. Risico’s en voorgestelde maatregelen	Risico’s zijn beschreven in de DPIA. Huidige handmatige verwerking brengt de volgende risico's met zich mee: - Onbevoegde toegang. - Onnodig bewaren van (bijzondere) persoonsgegevens. - Onvolledige of onjuiste registratie.	Akkoord. Om deze risico's te mitigerende wordt in de loop van 2025 een overgegaan op het geautomatiseerde systeem Rx.Mission.

	- Gebrek aan traceerbaarheid: moeilijk te achterhalen wie welke gegevens heeft ingevoerd of gewijzigd. - Overtreding van bewaartermijnen. - Verlies van gegevens: door technische problemen of menselijke fouten. Risico's aan Rx.Mission: - Datalekken ondanks geavanceerde beveiligingsmaatregelen. - Onvolledige configuratie: bij de inrichting van het systeem kunnen fouten optreden, bijv. niet correct instellen toegangsrechten. - Misbruik van toegang. Voordelen van Rx.Mission: - Toegangscontrole: waardoor risico op onbevoegde toegang geminimaliseerd wordt. - Audit-trails: Rx.Mission houdt bij wie, wanneer en welke wijzigingen worden aangebracht. - Bewaartermijnen worden toegekend bij inrichting. - Vermindering van menselijke fouten door geautomatiseerde workflows. Restrisico is menselijk handelen.	Door een combinatie van de voordelen van het nieuwe systeem en aanvullende maatregelen, zoals regelmatige controles, training van medewerkers, en continu toezicht op beveiligingsinstellingen, kan het meldpunt een balans vinden tussen het benutten van de technologie en het minimaliseren van risico's voor betrokkenen.

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 een 'middelhoog' risico.
Dit volgt uit het feit dat naast reguliere persoonsgegevens ook bijzondere persoonsgegevens verwerkt kunnen worden en dat melders zich vaak in een kwetsbare positie bevinden. Tegelijkertijd is de inrichting van het meldpunt expliciet in de wet vastgelegd en is de verwerking beperkt tot noodzakelijke gegevens. Daarnaast is de verwerking ook omgeven door passende waarborgen zoals beveiliging, doelbinding, beperkte toegang en mogelijkheid tot anoniem melden. Om de risico's van de handmatige verwerking van persoonsgegevens te mitigeren, wordt in de loop van 2025 overgegaan op Rx.Mission. Daarmee is de inbreuk op de privacy proportioneel en voldoende beheersbaar.

Eind 2026 zal deze DPIA op naleving getoetst worden.
Speciale aandacht zal gegeven worden aan:
De overgang naar Rx.Mission, logging en toekennen en intrekken van autorisaties.

Ik adviseer hiermee positief en daarmee zijn de resterende risico's 'aanvaardbaar'.

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

KR/09/10/2025. DPIA 117

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief 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

Richtlijnen gebruik AI

Inleiding

Met de lancering van ChatGPT raakte de ontwikkeling van AI in een stroomversnelling. We hebben daarna de eerste versie van onze principes voor het gebruik opgeschreven. Inmiddels zijn we ruim een jaar verder en is het tijd voor een update. We trekken de principes iets breder; we hebben het niet alleen over generatieve AI (zoals ChatGPT of afbeeldingsgeneratoren als Dall-E) maar ook over andere AI-toepassingen (zoals anonimiseringssoftware of kentekenscanners).

Als je AI-toepassingen wil gebruiken kan dat, als je je aan de volgende regels houdt. Op deze manier gebruiken we ze waar ze geschikt voor zijn. Heb je mooie voorbeelden uit je eigen praktijk? Ook dat horen we graag! Zo leren we samen beter werken met deze technologie.

Deze richtlijnen zijn gebaseerd op de kennis van nu (september 2024). Die kennis zal groeien. Daarom verversen we deze richtlijnen wanneer nodig.

1. Verdiep je in de mogelijkheden en beperkingen

AI is complex: het biedt veel kansen, maar er zitten ook haken en ogen aan. Zorg ervoor dat je daarvan op de hoogte bent en goed afgewogen de juiste tool kan gebruiken. Lees hier wat de beperkingen zijn.

2. Je bent zelf verantwoordelijk

Jij bent de expert en kent jouw vakgebied. Je bent verantwoordelijk voor je eigen werk. Als je een AI-hulpmiddel gebruikt blijft dat zo, net als wanneer je iets via Google opzoekt. Dat betekent ook dat je de resultaten uit de AI controleert vóór je ze gebruikt.

3. We delen geen gevoelige informatie

Vertrouwelijke informatie of persoonsgegevens delen we niet zomaar. Zeker niet met AI-chatbots of andere online hulpmiddelen. Alles wat je deelt wordt gebruikt door derden.

4. Zorg ervoor dat je de output kan beoordelen

Het kan dat een AI-tool foute resultaten genereert. Zorg ervoor dat je zelf kennis hebt over de inhoud, zodat je in staat bent de resultaten van de AI te herkennen en verbeteren.
Je kan een AI-tool dus niet vragen om een samenvatting van een tekst over een onderwerp waarvan je niet voldoende inhoudelijke kennis hebt. Je kunt namelijk niet beoordelen of er fouten in staan en/of de samenvatting goed is.

5. Gebruik AI niet meer dan nodig is

AI-toepassingen als ChatGPT en Copilot zijn gebaseerd op grote hoeveelheden informatie. Het verwerken daarvan vraagt veel rekenkracht en kost daardoor veel energie. Een vraag aan ChatGPT kost ongeveer 5 keer zo veel energie als eenzelfde vraag aan een zoekmachine als Google. Gebruik de juiste gereedschappen voor het werk. AI gebruik je als er geen beter gereedschap is.

6. We doen een intake als we AI onderdeel willen maken van een werkproces

Wil je een AI-toepassing incidenteel gebruiken, bijvoorbeeld om je presentatie te verbeteren, of een alternatieve openingsparagraaf te krijgen voor je tekst? Volg dan bovenstaande regels. Wil je een toepassing structureel in een werkproces gaan gebruiken? Neem dan contact op met het opgaveteam Digitale Transformatie. We kijken dan met je mee. Zo zorgen we dat we verantwoord gebruik maken van de mogelijkheden van AI.

Het is nieuwe technologie, die snel verandert. Daarmee kunnen ook onze spelregels in de toekomst veranderen. Voor nu hanteren we deze spelregels.

Punten van aandacht:

- **Zorg voor context.** Een AI-model kent onze organisatie en jouw vraag niet. Beschrijf details over je probleem voor je je vraag stelt. Zo kan het gebruik maken van die informatie om een betere tekst te schrijven. Doe dit bij elke nieuwe ‘chatsessie’: Het model verandert tussendoor niet en gebruikt vaak niet de informatie die je in eerdere chatsessies hebt geschreven.
- Het is een techniek in opkomst, en daardoor **sterk veranderend**. Je kan er nog niet op vertrouwen dat het volgend jaar hetzelfde werkt, dus maak je werk niet afhankelijk van AI.
- De grote modellen achter de AI-tools worden maar af en toe bijgewerkt. Daardoor bevatten ze vaak niet de meest **actuele informatie**.
- Modellen worden getraind op veel openbaar beschikbare informatie, en bevatten dus ook **foute informatie**. Deze fouten liggen dus ook onder het antwoord wat jij krijgt.
- Elke AI heeft **vooroordelen** ingebakken, omdat de informatie waarmee deze getraind is dat ook heeft. Ben je hiervan bewust bij het stellen van vragen, en het gebruik van de antwoorden die je krijgt. Die kunnen diezelfde vooroordelen bevatten.
- Generatieve AI genereert antwoorden op basis van statistiek, niet op basis van kennis. Het kan dus **foute antwoorden** geven, wat ook wel ‘hallucineren’ wordt genoemd.
- De modellen zijn getraind op bestaande teksten en afbeeldingen. Delen van de uitvoer kunnen dus bestaan uit het werk van anderen, wat dus **plagiaat** is. Bovendien heb je niet zelf het auteursrecht op de teksten die voor je gegenereerd worden.
- AI is statistisch, dus bij dezelfde vraag is de kans groot dat je **wisselende antwoorden** krijgt. Daarmee werkt het fundamenteel anders dan de computersystemen die we tot nu toe gewend zijn.

Weren risicovolle applicaties update 0825

Inleiding
In januari 2025 is er een lijst van risicovolle applicaties gepubliceerd met de instructie aan medewerkers om deze niet te installeren of geïnstalleerd te hebben op hun werk devices.

Ontwikkeling
In navolging van het advies gegeven in januari heeft de CISO een uitvraag gedaan om de populariteit van Chinese, Russische en Iraanse apps in de Apple appstore te controleren.

Applicaties
In het resultaat van de uitvraag valt de Chinese app **rednote** op. Deze lijkt populairder te worden in Amerika al blijft de populariteit wat achter in Europa.
Bij het bekijken van de huidige lijst kan de vraag op komen welke applicaties feitelijk beschikbaar zijn in Europa en gebruikt zouden worden door onze medewerkers. Tegen deze achtergrond zouden een aantal applicaties van de lijst afgevoerd kunnen worden. Niet omdat ze veilig zouden zijn voor ons maar omdat ze op dit moment niet aangeboden worden in de Apple appstore.

Kanttekeningen
Zoals bij alle informatiebeveiligingsmaatregelen is het nodig een beoordeling te maken van het risico dat wij lopen. Het aanpassen van de lijst vestigt de aandacht op het probleem en is goed voor bewustwording. Tegelijkertijd zou het verwijderen van applicaties van de lijst de indruk kunnen wekken dat deze nu veilig zijn. Bovendien is mijn inschatting op dit moment dat het risico niet wezenlijk veranderd is gezien de bekendheid van rednote, iets dat we wel zouden moeten monitoren.

Advies
Op basis van bovenstaande wordt geadviseerd
- om de lijst van te weren applicaties niet aan te passen op dit moment.
- de uitvraag aan het eind van 2025 te herhalen.

Bijlage 1: Te weren applicaties

Land	Applicatie	Functie
China	TikTok	Bewerken en delen video
	WeChat	Berichten delen
	UC Browser	Web browser
	Shein	Shopping
	Pinduoduo	Shopping
	Temu	Shopping
	AliExpress	Shopping
	CapCut	Video editing

	Lemon8	Life style
	CamScanner	Document scanner
	TurboVPN	VPN applicatie
	SHAREit	Delen bestanden
	QQ Messenger/International	Berichten delen
Rusland	Telegram	Berichten delen
	FaceApp	Foto`s editen
	Yandex apps	Zoekmachine, virtueel toetsenbord
Iran	Mobogram	Berichten delen
	iGap	Berichten delen

Bijlage 2: Bronnen

https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2023Z04749&did=2023D11252

https://vng.nl/sites/default/files/2023-05/advies-over-het-gebruik-van-apps-uit-landen-met-een-offensief-cyberprogramma.pdf

https://www.ncsc.nl/wat-kun-je-zelf-doen/weerbaarheid/beschermen/apps-uit-landen-met-een-offensief-cyberprogramma-tegen-nederlandse-belangen

https://www.ncsc.nl/actueel/nieuws/2024/septe/18/nederlandse-apparaten-onderdeel-van-chinees-botnet

https://ecer.minbuza.nl/-/europese-commissie-leidt-dsa-procedure-tegen-temu-in-en-spreekt-met-consumentenautoriteiten-temu-aan-op-schending-consumentenrecht

Bijlage_2_-_Overzicht_te_weren_applicaties_door_gemeente_Amsterdam_d_d__25_april_2024

ChatGPT prompt: create a table of apps with privacy or data breach concerns by country of origin (en variaties hier op)