From: "5.1.2e " <5.1.2e @helmond.nl>
Sent: 2/10/2025 3:41:13 PM
To: "5.1.2e " <5.1.2e 5.1.2e @helmond.nl>
Cc:
Subject: RE: Zaaknummer: 52373526,

Dag 5.1.2e

Bedankt voor de informatie. Goed dat het wordt opgepakt. Graag ontvang ik het besluit van de stuurgroep.
Verder heb ik een aantal vragen met betrekking tot de vraag of mijn adviezen zijn opgevolgd.

1. Betekent dit dat de directeur Sociaal Domein en Veiligheid en Naleving heeft besloten om mijn adviezen om past te starten met
- de signaaloverleggen **nadat,** het proces (de processen) en de informatiestromen goed in beeld zijn gebracht. Er daarnaast een risico-analyse (waaronder een DPIA)[1] is uitgevoerd, alle privacy en informatiebeveiligingsrisico's zijn herkend en erkend en er passende maatregelen zijn getroffen.
- het delen van informatie met de andere deelnemers als zij kunnen aantonen dat ook zij passende maatregelen hebben getroffen. Vraag als bewijs het FG advies van de partners op de door hen uitgevoerde DPIA.

Niet over te nemen?

2. Ik heb geadviseerd om in dat geval:
   - (expliciet) een besluit te nemen en de afwijking te onderbouwen, mij hierover te informeren en het besluit vast te leggen in het zaaksysteem. Graag ontvang ik deze onderbouwing, zodat ik het kan vastleggen in het zaaksysteem. Of is er mss besloten om dit advies niet op te volgen? In dat geval hoor ik graag waarom dit advies niet is overgenomen.
   - In ieder geval een besluit te nemen over het (z.s.m.) alsnog uitvoeren van een Risico-analyse (RA). In het besluit concreet vast te leggen wanneer de risico analsye zal zijn uitgevoerd en hier daadwerkelijk op te sturen. Zorg ook dat er voldoende capaciteit beschikbaar is voor het uitvoeren van deze RA. Dit kan betekenen dat er moet worden geprioriteerd. Graag ontvang ik dit besluit. Of is er mss besloten om dit advies niet op te volgen? In dat geval hoor ik graag waarom dit advies niet is overgenomen.
   - Met de partners af te spreken wanneer zij (uiterlijk) een FG advies overleggen en stuur hier op. Leg deze afspraak schriftelijk vast en informeer de FG. Graag ontvang ik het besluit. Of is er mss besloten om dit advies niet op te volgen? In dat geval hoor ik graag waarom dit advies niet is overgenomen.
3. Verder heb ik in het advies aangegeven dat men zich de volgende zaken dient te realiseren:
   - dat betrokkenen grote privacyrisico's lopen en dat zij hierdoor nadelige gevolgen kunnen ondervinden die haaks staan op de doelen die met dit project worden beoogd
   - dat er niet kan worden aangetoond dat er een goede afweging is gemaakt tussen de privacyrechten van betrokkenen en andere belangen.
   - dat er wordt gehandeld in strijd met de Algemene verordening gegevensbescherming en mogelijk ook de Wet politiegegevens. Hiervoor kan de Autoriteit Persoonsgegevens een boete opleggen. Is dit meegewogen in de besluitvorming?

Is dit meegewogen in de besluitvorming? Graag ontvang ik hierover informatie met bij voorkeur een bewijs.

4. Tot slot heb ik geadviseerd om mijn advies te delen met de stuurgroep.
   Is dit advies overgenomen, heeft de stuurgroep mijn advies ontvangen? Zo nee, dan hoor ik graag waarom dit advies niet is overgenomen.

Jouw reactie (of de reactie van 5.1.2e) bewaar ik bij de zaak.

Aanvullend advies:
- Zorg dat de driehoek mijn advies ontvangt en de besluiten over het al dan niet opvolgen van de adviezen met onderbouwing ontvangt.

Een FG advies is namelijk zwaarwegend wat betekent dat hier alleen gemotiveerd van afgeweken kan worden. Burgemeester en wethouders zijn verantwoordelijk en zijn degene die een afweging moeten maken. Dat betekent dat zij ook moeten weten dat er wordt afgeweken van het FG advies en waarom dit is gebeurd. Het is bovendien

belangrijk dat een onderbouwing wordt afgelegd, zodat verantwoording kan worden afgelegd aan betrokkenen en eventueel aan de toezichthouder (de Autoriteit Persoonsgegevens).

Groeten 5.1.2e

Met vriendelijke groet,

Gemeente Helmond

5.1.2e
Functionaris voor de gegevensbescherming

Afdeling Concern control
Postbus 950, 5700 AZ, Helmond
Telefoonnummer 5.1.2e

Kom bij ons werken! Kijk eens op www.helmond.nl/werkenbij.

Van: 5.1.2e <5.1.2e 5.1.2e@helmond.nl>
Verzonden: maandag 10 februari 2025 15:09
Aan: 5.1.2e <5.1.2e@helmond.nl>
Onderwerp: Re: Zaaknummer: 52373526

Dag 5.1.2e,

De stuurgroep heeft vorige week ingestemd met het voorstel dat ik had gedaan.
Privacy/informatieveiligheid is expliciet als aandachtspunt besproken en we hebben afgesproken daarvan werk te maken. Zoals jou bekend heb ik hierover contact met de informatieadviseurs en strategisch privacy adviseurs, en bespreken 5.1.2e en ik dit in de eerstvolgende besturingsdriehoek zorg & veiligheid met burgemeester en wethouder.
Dit als update, ter informatie.

Groet,
5.1.2e

Van: 5.1.2e <5.1.2e@helmond.nl>
Verzonden: dinsdag 4 februari 2025 09:42
Aan: 5.1.2e <5.1.2e 5.1.2e@helmond.nl>
CC: 5.1.2e <5.1.2e 5.1.2e@helmond.nl>
Onderwerp: RE: Zaaknummer: 52373526

Hoi 5.1.2e,

Bij deze alsnog het advies.
Ik heb een controlevraag: ik had zelf ook al gezien dat ik het advies was vergeten en het 5 minuten later alsnog verstuurd. Heb je dat niet gehad? Als je dat niet hebt gehad, moet ik even op onderzoek uit wat er mis is gegaan.

Groeten 5.1.2e

Met vriendelijke groet,

Gemeente Helmond

5.1.2e
Functionaris voor de gegevensbescherming

Afdeling Concern control
Postbus 950, 5700 AZ, Helmond
Telefoonnummer 5.1.2e

#Makers van de toekomst

Kom bij ons werken! Kijk eens op www.helmond.nl/werkenbij.

Van: 5.1.2e <5.1.2e 5.1.2e @helmond.nl>
Verzonden: maandag 3 februari 2025 19:34
Aan: 5.1.2e <5.1.2e @helmond.nl>
CC: 5.1.2e <5.1.2e 5.1.2e @helmond.nl>
Onderwerp: FW: Zaaknummer: 52373526

Dag 5.1.2e, fijn dat je betrokken bent bij dit project. Ik zie alleen in de bijlage je advies niet. Wil je dat alsnog even mailen?

Ik heb het inderdaad besproken met 5.1.2e. Het is een dilemma dat begrijp ik maar al te goed. We gaan het nu eerst in de stuurgroep bespreken waarna het onderwerp ook terugkomt op de bestuurlijke tafel in de besturingsdriehoek met wethouder Tuerlings en de burgemeester. Ook bestuurlijke is het belang om de risico's waar jij op duidt in beeld te hebben.

We houden je op de hoogte.

Gr. 5.1.2e

Van: Postbus KlantenInfo <gemeente@helmond.nl>
Verzonden: woensdag 29 januari 2025 13:04
Aan: 5.1.2e <5.1.2e 5.1.2e @helmond.nl>; 5.1.2e <5.1.2e 5.1.2e @helmond.nl>
Onderwerp: Zaaknummer: 52373526

Dag 5.1.2e

Op 4 februari staat voor de stuurgroep preventie met gezag een voorstel geagendeerd. Als ik het goed begrijp is het besluit nodig om te kunnen starten. Ik heb van 5.1.2e het concept voorstel ontvangen. Mijn advies is echter om eerst een risico analyse uit te voeren, de nodige maatregelen te treffen en daarna pas te starten. Ik besprak met 5.1.2e de wens om toch alvast te starten, ik heb aangegeven dat er minimaal een concreet plan moet liggen om alsnog een risico analyse uit te voeren (goede bedoelingen zijn er nl al een jaar) en dat er een specifiek besluit nodig is over het al dan niet starten, waarbij op de risico's wordt gewezen. 5.1.2e heeft aangegeven dat hij het voorstel nog zal aanpassen en ik heb afgesproken dat ik een advies zou opstellen. Dit advies vind je in de bijlage. Het advies is aan

jou gericht omdat ik de andere deelnemers niet kan adviseren. Dat moeten hun eigen FG's doen. Graag ontvang ik jouw besluit en tzt ook het besluit van de stuurgroep. Met vriendelijke groet 5.1.2e

---

[1] *De termen Risico analyse en DPIA worden door elkaar gebruikt. Een DPIA is in deze casus, gelet op de hoge risico's, verplicht op grond van de AVG. Met een DPIA worden de privacyrisico's voor betrokkenen in beeld gebracht. De term Risico analyse is breder, er wordt niet alleen een DPIA uitgevoerd maar ook worden de risico's voor de organisatie in beeld gebracht. De gemeente Helmond heeft als afspraak dat er bij het uitvoeren van een DPIA altijd de brede Risico analyse wordt uitgevoerd.*

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	1, 2, 3, 4

Scenario’s bezoekerspassen

Advies van de FG en de Ciso




Gemeente Helmond

Advies: Geen afwijking.

Advies:

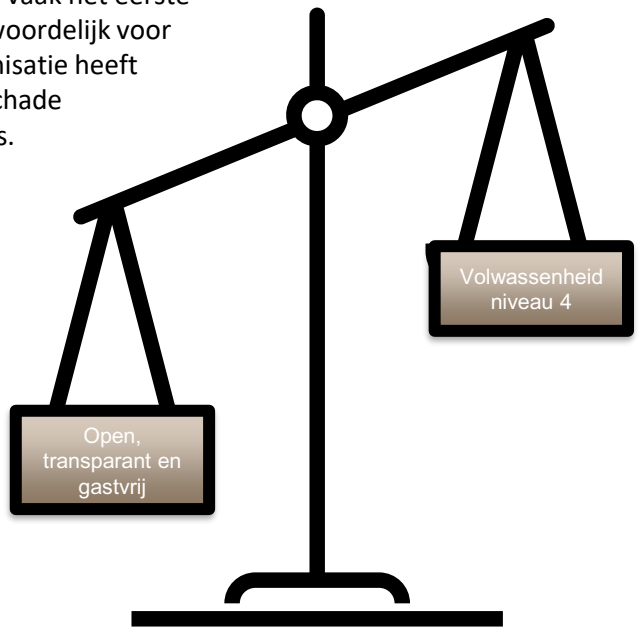
- Wijk niet af van het vastgestelde beleid

Indien de stuurgroep toch wil afwijken van het beleid:

- Leg de afwijking voor aan het college. Zodat zij de afweging kunnen maken of; de wens om open, transparant en gastvrij te zijn, zwaarder moet wegen dan de ambities op het gebied van informatieveiligheid en privacy.

Risico's

In de gemeente zijn zeer veel (persoons)gegevens aanwezig, zowel op fysieke media als digitaal. Voor zowel criminelen als burgers/organisaties zijn deze gegevens veel waard. Daarnaast heeft de gemeente processen die voor zeer veel inwoners relevant zijn en daardoor is de continuïteit belangrijk. De gemeente is vanuit de overheid vaak het eerste aanspreekpunt voor burgers. De gemeente neemt besluiten of is verantwoordelijk voor de uitvoering van besluiten die impact hebben op deze burgers. De organisatie heeft hierdoor een **hoog risicoprofiel**. Een actor kan potentieel grote fysieke schade aanbrengen ten aanzien van het gebouw en de medewerkers / bezoekers. Daarnaast kan informatie van inwoners, organisaties en de gemeente ingezien worden of schade ondervinden.



Maatregelen

Het ontwerp van het Huis voor de Stad zorgt ervoor dat de kans op onbevoegde toegang groot is. De toe te passen beveiligingsmaatregelen moeten de risico's terugbrengen tot een acceptabel niveau. Het is aan het management om te bepalen wat acceptabel is. Wat zij acceptabel vinden is vastgelegd in het "Beleid fysieke beveiliging Huis voor de stad". Dit beleid is een consensusdocument tussen de visie: "open, transparant en gastvrij" en de ambities op het gebied van informatiebeveiliging en privacy (volwassenheidsniveau 4).

Wijk niet af van het beleid.

Afwijking van het beleid betekent niet alleen dat **de risico's** op onbevoegde toegang **onaanvaardbaar groot** worden. Het betekent ook dat de ambitie om op het gebied van informatiebeveiliging en privacy te groeien in volwassenheid vertraging oploopt. Het op 8 maart 2019 door het college vastgestelde **ambitie van volwassenheidsniveau van 4 wordt onhaalbaar**.

(zie zaak 5000037).

Gemeente Helmond

Beleidsuitgangspunten

Advies:

- Werk scenario 1b, 1c, 2b, 4 en 5 niet verder uit. Zij voldoen niet aan het beleid.

In de tabel wordt aangegeven op welke punten de scenario's in ieder geval niet kunnen voldoen aan het vastgestelde beleid.

Doelstelling behorend bij volwassenheidsniveau 4:
Toegang tot gebouwen, gebouwen en gebieden moet worden gerechtvaardigd, geautoriseerd, geregistreerd en gecontroleerd. Dit geldt voor alle personen die het pand betreden, inclusief personeel, tijdelijk personeel, klanten, verkopers, bezoekers of enige andere derde partij. (NOREA, zie ook document beveiligingsniveau fysieke beveiliging 2021 CISO)

De vertaling hiervan in het "Beleid fysieke beveiliging Huis voor de stad":
Zonering:

- De publieke zone (zone 1) wordt afgeschermd van de overige zones door middel van speedgates voorzien van paslezers.
- In zone 2 bevinden zich de raadzaal en de commissie- en fractiekamers. Dit is een semi-publieke zone. Tijdens de publieke openstelling, gelden hier dezelfde maatregelen als in zone 3 en buiten deze uren is er sprake van een publieke zone. Zone 3 is de medewerkerszone. Tot slot bevat zone 4 beveiligde ruimtes.
- Het vergadercentrum bevindt zich in zone 2. Ook in zone 3 bevinden zich vergaderruimtes.

Maatregel uit het beleid / Punten waarop scenario's niet voldoen	1c	1b	2b	4	5
Onbevoegden kunnen worden herkend omdat medewerkers en bezoekers hun toegangspas zichtbaar dragen.				x	x
Bezoekers dragen een toegangspas en worden begeleid door een medewerker óf zij dragen een herkenbare toegangspas die is te onderscheiden van medewerkerspassen en andere toegangspassen.		x		x	x
Bezoekers worden geregistreerd en geïdentificeerd.	x			x	x
Toegangsrechten worden automatisch ingetrokken. (na 24 uur bij een dagpas en na verstrijken van de afgesproken termijn bij een tijdelijke pas).				x	x
Onbegeleide bezoekers en medewerkers die geen medewerkerspas of bezoekerspas dragen worden aangesproken.		x	x	x	x
Er is een proces van uitgifte en beheer. (registratie, intrekken, afhandeling van vermiste toegangspassen).	x			x	x

Gemeente Helmond

Mogelijke oplossingen

Advies:

- Kies voor scenario 1a. Zorg dat bij de uitwerking wordt voldaan aan het beleid.

Bij keuze voor uitwerking van scenario 2a:

- Breng in beeld of software en proces zodanig zijn in te richten dat wordt voldaan aan het beleid. Onderzoek welke risico's dit scenario met zich meebrengt.

Bij keuze voor scenario 3:

- Tref maatregelen om te voorkomen dat medewerkers het proces onjuist uitvoeren.

Scenario 1a

Met dit scenario kan worden voldaan aan het beleid. **Dit scenario heeft de voorkeur.**
Een aantal van de geformuleerde consequenties was (in principe) voorzien, want ze volgen uit het beleid. Zoals de **consequentie** dat:

1. Capaciteit nodig is van hospitallity medewerkers.
2. Er meerdere medewerkers geautoriseerd moeten worden voor de bezoekersregistratie
3. Bezoekers geïdentificeerd moeten worden.
4. Dit niet kan worden toegepast buiten dienstverleningstijden.

Consequentie	Corresponderende maatregel in het "Beleid fysieke beveiliging Huis voor de Stad".
1 en 2	Aan medewerkers van het interne servicepunt en hospitallity medewerkers zijn de volgende taken gemandateerd: • Het beheren, uitgeven en intrekken van (bezoekers)toegangspassen. • De afhandeling van 'vermiste' toegangspassen.
3	Bezoekers worden geregistreerd en geïdentificeerd.
4	Tijdens de publieke openstelling gelden hier dezelfde maatregelen als in zone 3 en buiten deze uren is er sprake van een publieke zone.

Scenario 2a

Deze functionaliteit is nu niet in huis. Het is afhankelijk van de aangeschafte software en de inrichting van het proces of aan alle maatregelen kan worden voldaan. **Dit scenario heeft daarom niet de voorkeur**.

Scenario 3.

Met dit scenario is het mogelijk om te voldoen aan alle in het beleid opgenomen maatregelen. Dit scenario heeft niet de voorkeur, omdat het proces complexer is, waardoor het risico bestaat op frustratie en verzet bij medewerkers en het onjuist uitvoeren van het proces (het werkproces omzeilen)**. Dit scenario heeft daarom niet de voorkeur**.

Afdeling: Veiligheid en Naleving
Onderwerp: Convenant ‘Aanpak drugslocaties Oost-Brabant 2025-2030’.
Djuma: 52428624

Situatie

Binnenkort zal het Drugsconvenant Oost-Brabant 2025-2030 in het burgemeester overleg en in het college worden behandeld. Dit convenant vervangt per 1 april as. het huidige Hennepconvenant en regelt onder andere de verstrekking van persoonsgegevens door de Politie en het Openbaar Ministerie aan de burgemeester in het kader van bestuurlijke opvolging.

In de bijlage bij het convenant wordt ook gesproken over een operationeel overleg, waarin persoonsgegevens gedeeld gaan worden met deelnemende partijen. Uit navraag is gebleken dat er binnen Helmond al enkele jaren in het kader van het Hennepconvenant geen operationeel overleg plaatsvindt en ook niet meer bestaat. Ook is dit proces eerder niet beschreven. Momenteel wordt onderzocht of dit in andere gemeenten wel gebeurt en of daar werkprocessen voor zijn vastgesteld. Het voornemen is om deze processen over te nemen of, indien nodig, een werkproces op te stellen en in te richten voor Helmond of de Peelgemeenten. Daarnaast is het voornemen om een risico analyse uit te voeren.

Het Proces

Het collegevoorstel moet voorzien zijn van een privacy-advies. Indien het college wordt geïnformeerd conform onderstaand advies (én het advies inhoudelijk wordt overgenomen) dan kan in het voorstel worden verwezen naar dit advies. (zorg dat het is toegevoegd aan de stukken).
Mochten de adviezen niet worden overgenomen dan dient de FG in de gelegenheid gesteld te worden om te adviseren over het collegevoorstel, alvorens het wordt aangeboden aan het college.

Advies

<u>Als ik het goed begrijp:</u>

1. Is het voorstel: ondertekenen van het convenant
2. Worden er (nog) geen gegevens gedeeld met andere partijen (in het operationeel overleg).
3. Ontvangen we gegevens van politie en OM op grond van dit convenant. We ontvangen die gegevens in het kader van bestuurlijke opvolging.

Ad 2 het operationeel overleg.
Goed dat eerst de processen die voortkomen uit het operationeel overleg worden beschreven en dat er vervolgens risico analyse op wordt uitgevoerd. Ik lees hier in dat dit alles zal plaatsvinden voordat er daadwerkelijk wordt gestart met een operationeel overleg.

Ik adviseer om in het collegevoorstel ook op te nemen

- dat het operationeel overleg nog niet plaatsvindt en
- dat hier pas mee zal worden gestart zodra de processen zijn beschreven, risico’s bekend zijn en voldoende mitigerende maatregelen zijn getroffen.

Ad 3. Bestuurlijke opvolging
Het feit dat we gegevens ontvangen in het kader van bestuurlijke opvolging, betekent ook dat we persoonsgegevens verwerken op grond van het convenant. Ook bv het ontvangen, raadplegen en opslaan van dergelijke gegevens zijn namelijk verwerkingen. Kennelijk zijn deze gegevens nodig voor de processen die we uitvoeren in het kader van bestuurlijke opvolging. Het convenant is een

maatregel om de risico's die optreden binnen deze processen te verkleinen. In het convenant maak je namelijk afspraken over de wijze waarop je dit doet. Dit roept bij mij 2 vragen op:

a. Zijn alle risico's van deze processen (die worden uitgevoerd in het kader van bestuurlijke opvolging) in beeld, worden ze alle risico's weggenomen met dit convenant of zijn er nog aanvullende maatregelen nodig?
b. Zijn we in staat om ons te houden aan het convenant en kunnen we dat aantonen? Het convenant bevat ongetwijfeld bepalingen die lijken op: "we houden ons aan de privacywetgeving en we beveiligen de informatie". Om aan te kunnen tonen dat we ons aan de privacywetgeving houden, moeten we de risico's kennen en kunnen laten zien dat we voldoende maatregelen hebben getroffen (wat ons weer bij vraag a brengt).

Ik verwacht dat het hierbij gaat om bestaande processen (in het kader van bestuurlijke opvolging), maar dat op deze processen nog niet eerder risico analyse is uitgevoerd. Behalve het tekenen van dit convenant is het dus ook belangrijk dat de onderliggende processen worden aangepakt. Daarmee bedoel ik dat processen worden beschreven, informatiestromen in beeld gebracht, risico's benoemd en maatregelen getroffen. Dit is nodig om aan te kunnen tonen dat er wordt voldaan aan de privacywetgeving. Door bovendien verantwoording af te leggen over de naleving van de BIO kan er ook worden aangetoond dat de gegevens veilig zijn.

Ik adviseer

- Om in het collegevoorstel deze vervolgstap te beschrijven met een (eventueel meerjarige) aanpak.
- de afdelingsmanager om deze aanpak ook op te nemen in de jaarplannen van de afdeling.

Overigens

Dit advies is uitgebracht door de FG, de onafhankelijk toezichthouder op de naleving van de AVG. Onder de AVG is een FG advies geen dwingend advies, maar een zwaarwegend advies. Dat houdt in dat afgeweken kan worden van het advies, mits dit beargumenteerd wordt vastgelegd.

Collegevoorstel besluitvormend

Portefeuillehouder	A. Bonte	**Besluitdatum:**	26 november 2024
Opdrachtgever	5.1.2e	**Commissie:**	n.v.t.
Opsteller	5.1.2e		
Datum	20-11-2024	**Raad:**	n.v.t.
Concernplanning-nummer	10.318		
Zaaknummer	52222030		
Documentnummer	52264121		

Onderwerp
Verkeersbesluit geslotenverklaring Broekstraat

Voorstel
1. Een wegafsluiting voor gemotoriseerd verkeer te realiseren op de Broekstraat in Helmond, door het plaatsen van verkeersborden model C01 met onderbord “uitgezonderd (brom)fietsen”.

Inleiding (inclusief voorgeschiedenis besluitvorming)
De wegenstructuur van Brandevoort is geënt op het gebruik van De Voort, de Brandevoortsedreef en de Neervoortsedreef voor gemotoriseerd doorgaand verkeer. Om sluipverkeer tussen Brandevoort en Mierlo te voorkomen is in het Masterplan Brandevoort vastgesteld dat de kleine verbindingen tussen deze twee kernen worden afgesloten. Dit is voor alle tussenliggende wegen gedaan, behalve voor de Broekstraat.

De gemeente Geldrop-Mierlo heeft ten tijde dat het bestemmingsplan Brandevoort II ter inzage lag bezwaar gemaakt tegen de afsluiting van de Broekstraat omdat zij zich zorgen maakte over de bereikbaarheid van bewoners in het gebied ’t Broek (het gebied boven het Eindhovens kanaal). In 2017 zijn hierover nadere bestuurlijke afspraken gemaakt, waarna het bezwaar door de gemeente Geldrop-Mierlo is ingetrokken. De bestuurlijke afspraak is dat, in het geval van een afsluiting, de verbinding 't Broek – Brandevoort (die loopt via de Broekstraat) toegankelijk blijft voor de bewoners van gebied 't Broek. Deze toegankelijkheid kan op meerdere manieren worden ingericht. In dit geval is de keuze gevallen op een afsluiting met kentekenherkenning waarbij ontheffing kan worden verleend aan een specifieke groep. Camerahandhaving maakt geen onderdeel uit van dit verkeersbesluit (die wordt uitsluitend genomen om de juiste bebording te kunnen plaatsen), maar is wel noodzakelijk om de afsluiting goed te kunnen laten functioneren.

Tevens is het in het bestuurlijke overleg afgesproken dat een afsluiting pas wordt gerealiseerd bij de vervolmaking van Liverdonk, óf bij klachten van bewoners. Inmiddels ontvangt de gemeente Helmond steeds meer meldingen over sluipverkeer en daarmee samenhangende problemen. Ook is de vervolmaking van Liverdonk vanaf voorjaar 2025 een feit, waardoor het nu noodzakelijk is de geslotenverklaring in te stellen.

Impact op stad en inwoners
Door het sluipverkeer te voorkomen en dit verkeer te geleiden naar de hoofdwegenstructuur wordt de leefbaarheid in de directe omgeving verbeterd (verkeersveiliger en minder verkeersoverlast).

Argumenten
1.1 Maatregel sluit aan op ambitieakkoord 2022-2026 en Mobiliteitsvisie Helmond 2040
Met het ambitieakkoord 2022-2026 streeft het college naar een inclusieve, leefbare en gezonde stad en ook in de Mobiliteitsvisie Helmond 2040 plaatst de gemeente Helmond de leefkwaliteit in de stad centraal. In het verkeersnetwerk geven we hier onder meer vorm aan door het verkeer zo snel mogelijk via de hoofdstructuur af te wikkelen en zo min mogelijk (doorgaand) verkeer in de wijken. Met het afsluiten van de Broekstraat wordt bijgedragen aan deze beleidsuitgangspunten.

1.2 De wijk is in aanbouw en het aantal meldingen van verkeersoverlast in de wijk neemt toe
De wijk is deels gereed. Er zijn nog een drietal woningen in aanbouw welke nog een uiterlijk bouwtermijn hebben tot voorjaar 2025. Daarnaast neemt het aantal meldingen over verkeersoverlast in de wijk steeds meer toe. De afsluiting is in lijn met de afspraken gemaakt ten tijde van het bestemmingsplan (bij toenemende overlast en vervolmaking van

Liverdonk afsluiten).

1.3 Draagvlak Geldrop-Mierlo
Met de gemeente Geldrop-Mierlo heeft bestuurlijke afstemming plaatsgevonden. Geldrop-Mierlo heeft nogmaals aangegeven dat kan worden ingestemd met de maatregel, mits er voor de bewoners van 't Broek doorgang wordt gegarandeerd. In deze selectieve doorgang kan worden voorzien door middel van een ondersteunende maatregel in de vorm van een ontheffingenbeleid.

1.4 Gezien de gevoeligheid wordt dit besluit voorgelegd aan het college
Het nemen van verkeersbesluiten is gemandateerd aan de teammanager van team Mobiliteit & Milieu. Alleen bij 'politiekgevoelige verkeersbesluiten' wordt het besluit voorgelegd aan het college. Gezien de aandacht die dit onderwerp heeft bij omwonenden en gebruikers van de route en ook de noodzakelijke afstemming met buurgemeente Geldrop Mierlo leggen we dit verkeersbesluit aan het college voor.

Kanttekeningen en risico's
1.1 Extra omrijdtijden kan tot onvrede leiden bij huidige gebruikers van deze route
Met de maatregel wordt de leefbaarheid in de straat en de aangrenzende woonwijk verbeterd. Consequentie is ook dat het doorgaande verkeer dat momenteel gebruik maakt van deze route beperkt moet omrijden en dat zij de maatregel dan mogelijk ook niet steunen. Dit kan voor deze groep een reden zijn om bezwaar in te dienen. De gemeente Helmond is van mening dat het nadeel van extra rijtijden niet opweegt tegen het voordeel van de verbeterde leefkwaliteit in de wijk Liverdonk.

1.2 Camerabewaking is noodzakelijk om maatregelen te kunnen handhaven en vraagt om een vervolgproces
Hoewel formeel de afsluiting kan worden aangeduid met bebording worden aanvullende maatregelen noodzakelijk geacht om de afsluiting op een juiste wijze te kunnen laten functioneren. Dit vraagt om een vervolgproces (o.a. afstemming met CVOM, politie en college) dat kan worden opgestart na vaststelling van dit verkeersbesluit.

In het proces is de afweging gemaakt om de afsluiting te handhaven middels een cameraregistratiesysteem gelijk als in centrum Helmond en centrum Brandevoort. Vanwege de bestuurlijke afspraak om een specifieke groep inwoners van 't Broek doorgang te verlenen zijn er drie opties mogelijk.

1. Een afsluiting zonder aanvullende maatregelen.
   Het nadeel hiervan is dat handhaving moeilijk waar te maken is verband met de inzet van Boa's met als gevolg dat er onrechtmatig gebruik wordt gemaakt van deze verkeersroute.
2. Een andere optie is het plaatsen van een fysieke afsluiting, bijv. een pollerpaal of slagboom.
   Nadeel hiervan is dat deze onderhoudsgevoelig zijn, duur zijn in de aanschaf en dat hulpdiensten hinder kunnen ondervinden van een fysieke afsluiting (bijv. door een vergeten pas, niet geregistreerd kenteken, defect of vandalisme) en daardoor niet tijdig kunnen reageren bij een calamiteit.
3. Handhaving middels kentekenherkenning
   Hierbij wordt middels een ANPR camera gecontroleerd of een voertuig toegangsrechten heeft. Er is geen fysieke afsluiting. Er is hiermee en 24 uurs controle waarbij handhaving alleen plaatsvindt in geval van een overtreding.

1.3 Kentekentoegang kent een lagere privacy impact
Voor de effectiviteit van de verkeersmaatregel is het van belang dat er maatregelen worden getroffen om inrijden tegen te gaan. Dit kan door middel van fysieke afsluiting dan wel door handhaving. Afsluiten met kentekentoegang is een vorm van handhaving.

Zowel het fysiek afsluiten, als het afsluiten met Kentekentoegang kent gevolgen voor de privacy. In beide gevallen moet een bepaalde doelgroep (de ontheffinghouders, o.a. bepaalde bewoners, bedrijven, hulpdiensten) gebruik kunnen blijven maken van deze doorgang. Hiervoor moeten de kentekens van deze voertuigen worden vastgelegd en gecontroleerd bij de afsluiting middels een kentekencamera (of een pas bij voertuigen zonder kenteken).

Hierbij heeft een fysieke afsluiting een hogere impact op de privacy. De reden hiervoor is dat, naast de kentekencamera, er in dit geval een overzichtscamera moet worden geplaatst die continu beelden maakt. Dit is nodig voor de veiligheid, om het op afstand, handmatig bedienen van de fysieke afsluiting mogelijk te maken. Ook worden de overzichtscamera's gebruikt bij het achterhalen van veroorzakers van schade.

Bij handhaving met een kentekencamera wordt elke keer dat iemand de Broekstraat inrijdt een foto gemaakt en gegevens opgeslagen. De gegevens worden na 72 uur vernietigd indien degene die inrijdt hiervoor een vergunning heeft. Ze worden bewaard wanneer er sprake is van een overtreding.

Deze inbreuk op de privacy bij handhaving met een kentekencamera achten we proportioneel omdat effectiviteit van de verkeersmaatregel zwaarder weegt dan de inbreuk op de privacy van betrokkenen.
In beide gevallen dienen wel de regels uit de AVG te worden nageleefd (o.a. tijdig vernietigen van beelden en ze mogen alleen door een bevoegde ambtenaar worden uitgekeken).

Juridische context en impact privacy
Conform de wegenverkeerswetgeving vraagt het instellen van een geslotenverklaring om een verkeersbesluit.

Voor het vervolgproces (uitkijken foto's, versturen waarschuwingen, opleggen boetes) kan worden aangesloten op het bestaande proces hiervoor voor de voetgangersgebieden in het centrum en Brandevoort.

De FG deelt de conclusie dat de verwerking van persoonsgegevens bij handhaving met een kentekencamera proportioneel is mits de adviezen die FG en CISO op 15 september 2024 hebben gegeven bij het bestaande proces worden opgevolgd. Dit betekent onder ander dat de beelden van degene die de Broekstraat onmiddellijk worden verwijderd nadat is vastgesteld dat er geen sprake is van een overtreding. Door het FG en CISO-advies op te volgen wordt er voor de informatieverwerking bij een cameraregistratiesysteem voldaan aan de uitgangspunten van de AVG waardoor privacy is gewaarborgd (zie ook kanttekening 3).

Financiën en prioritering
Er zijn kosten gemoeid met de bebording. Deze kosten worden gedekt uit de post verkeerstechnische voorzieningen (5.1.2i)

Communicatie
Het verkeersbesluit wordt op de gebruikelijke wijze gepubliceerd in het wijkblad en in de Staatscourant en ligt ter inzage in het Huis van de Stad.

Participatie
Bij het opstellen van bestemmingsplan Brandevoort II heeft er in het verleden participatie en besluitvorming plaatsgevonden. Omdat deze maatregel pas veel later wordt uitgevoerd zijn er recentelijk twee inloopbijeenkomsten geweest voor de omwonenden waar de plannen zijn toegelicht. Ook heeft recent bestuurlijke afstemming plaatsgevonden met de gemeente Geldrop-Mierlo.

Uitvoering, evaluatie en vervolg
1) Doorlopen bezwarentermijn verkeersbesluit (zes weken)
2) Uitvoering maatregelen op straat

Bijlagen
- VKB 24023 Geslotenverklaring Broekstraat DEF.pdf

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	1
Wet open overheid	Art. 5.1 lid 2 sub i	Het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen	3

From: "5.1.2e " <5.1.2e @helmond.nl>
Sent: 4/2/2025 8:44:15 AM
To: "5.1.2e " <5.1.2e @helmond.nl>
Cc: 5.1.2e @helmond.nl>
Subject: FW: Adviesverzoek bestuurlijk behandelvoorstel

Hoi 5.1.2e

Goed dat je aan privacy en informatiebeveiliging denkt.
5.1.2e en ik hebben een advies opgesteld, (zie bijlage) ik wil je vragen om dit document toe te voegen aan de zaak. Verder wil ik je vragen om de onderstaande tekst toe te voegen aan het voorstel.

Juridische context en impact privacy
De ontwerpbegroting wordt, gelet op artikel 35 lid 1 van de Wgr, twaalf weken voordat de begroting ter vaststelling aan het algemeen bestuur van de ODZOB wordt aangeboden, toegezonden aan de raden en staten voor een zienswijze. De raden en staten kunnen tot uiterlijk 8 juni 2025 een zienswijze indienen bij het dagelijks bestuur van de ODZOB. Privacy- en informatiebeveiligingsrisico's zijn meegenomen in de gekwantificeerde risico's. Bovendien zijn met de ODZOB afspraken gemaakt over de veilige omgang van de informatie over onze inwoners en de ODZOB legt hier verantwoording over af.

Wanneer je de het advies en de rode tekst toevoegd zijn privacy en informatiebeveiliging voldoende opgenomen in het collegevoorstel

Groeten 5.1.2e
Met vriendelijke groet,

Gemeente Helmond

5.1.2e
Functionaris voor de gegevensbescherming

Afdeling Concern control
Postbus 950, 5700 AZ, Helmond
Telefoonnummer 5.1.2e

#Makers van de toekomst

Kom bij ons werken! Kijk eens op www.helmond.nl/werkenbij.

Van: 5.1.2e <5.1.2e @helmond.nl>
Verzonden: dinsdag 1 april 2025 15:31
Aan: Postbus Juridisch Team Gemeente Helmond <JT@helmond.nl>; 5.1.2i @helmond.nl>
Onderwerp: Adviesverzoek bestuurlijk behandelvoorstel

Hallo collega's,

Onlangs hebben we de ontwerpbegroting 2026 en meerjarenraming 2027-2029 van de ODZOB (en MRE, GGD, VRBZO) ontvangen met de mogelijkheid om daar vanuit Helmond een zienswijze op in te dienen. Voor de behandeling in het college en de gemeenteraad heb ik bijgevoegde conceptvoorstellen gemaakt. Alle documenten, waaronder de ontwerpbegroting, memo verkenning besparingen ODZOB, conceptadviezen, etc. zijn te raadplegen via Djuma (nr. 52451198) door op de volgende link te klikken: Zaaksysteem. Financieel adviseur 5.1.2e heb ik specifiek gevraagd om te adviseren over de geel gearceerde passage indexeringen in de concept zienswijzebrief.

Graag ontvang ik vóór woensdag 9 april a.s. jullie advies.

P.S. De ontwerpbegrotingen 2026 van ODZOB, GGD, MRE en VRBZO worden tegelijk behandeld in het college, commissie en raad volgens onderstaande planning. Er kan niet worden geschoven met de data!

- College – 15 april
- Adviescommissie – 15 mei 2025
- Raadsvergadering – 20 mei 2025

Bij voorbaat dank.

Groet,

5.1.2e

Afdeling Stedelijk Beleid, Team Mobiliteit & Milieu

Afdeling/Programma:	Stedelijk beleid
Onderwerp:	Ontwerpbegroting ODZOB
Zaak:	52451198
Datum:	2 april 2025

Aanleiding

Aan college en gemeenteraad wordt de ontwerpbegroting van de ODZOB voorgelegd. Het advies heeft betrekking op het collegevoorstel.

Advies

1. Voor dit collegevoorstel:
    a. Zorg dat informatiebeveiliging en privacyrisico's zijn meegenomen in de gekwantificeerde risico's.

2. Met betrekking tot dienstverlening door ODZOB:
    a. Laat de ODZOB ook jaarlijks verantwoording afleggen over informatiebeveiliging en privacy.

Toelichting

Als gemeente zijn we wettelijk verplicht om de basistaken door de ODZOB uit te laten voeren. Deze verplichting is geregeld in het Omgevingsbesluit. Naast de basistaken heeft Helmond ook de niet-verplichte verzoektaken aan de ODZOB overgedragen.

De verantwoordelijkheid die de ODZOB heeft om (persoons- en politie-) gegevens veilig te verwerken neemt niet weg dat de gemeente ook verantwoordelijkheid blijft dragen voor de data van de inwoners, die met de ODZOB worden uitgewisseld en door hen worden verwerkt. Het buiten de eigen deur plaatsen van taken ontslaat je niet van deze verantwoordelijkheid.

Het is daarom van belang dat afspraken worden gemaakt over het veilig verwerken van data en dat periodiek wordt gecontroleerd of deze afspraken ook worden nagekomen. Dit is meegenomen in de dienstverleningsovereenkomst die onlangs is vastgesteld. Laat bovendien de ODZOB niet alleen verantwoording afleggen over de doelen en de middelen, maar ook over informatiebeveiliging en privacy.

Het niet op orde hebben van informatiebeveiliging en privacy brengt bovendien financiële risico's met zich mee. Hier dient rekening mee gehouden te zijn bij de gekwantificeerde risico's.

2 april 2025

5.1.2e (Chief information security officer)

5.1.2e (Functionaris voor de gegevensbescherming)

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	1, 2, 3
Wet open overheid	Art. 5.1 lid 2 sub i	Het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen	1

Programma: Altijd Verbonden
Onderwerp: Veilig mailen, inzet AI-systeem
Djuma: 51953884

Inhoud

1. Inleiding. 1
2. Risico analyse AI systeem. 1
2.1 Transparantie. 2
2.2 Rolverdeling. 2
2. Advies. 3

1. Inleiding.

De gemeente Helmond heeft een functionaliteit voor veilig mailen en het delen van grote bestanden aangekocht bij Zivver. Medewerkers kunnen Veilig mailen inzetten wanneer zij gevoelige informatie moeten versturen. De gemeente heeft nog geen (gemeente)breed beleid, waarin is vastgelegd in welke situaties beveiligd dient te worden gemaild.

Gebruikers worden ondersteund bij het gebruik van Zivver. Zivver geeft namelijk een melding, waarbij de gebruiker de suggestie krijgt om veilig mailen te gebruiken. Zivver heeft de functionaliteit om hierbij kunstmatige intelligentie in te zetten. Daarbij wordt op basis van machine learning modellen bepaald of de inhoud van een bericht gevoelig is. Het model werkt door te leren van eerder verzonden berichten en te herkennen wanneer een concept vergelijkbaar is met berichten die in het verleden veilig zijn verzonden. Deze techniek verbetert de meldingen, waardoor het aantal valse meldingen afneemt (het AI-systeem). De AI-techniek is niet exclusief. Dat wil zeggen dat het model leert van alle berichten van alle klanten. Oftewel de gegevens uit de mails van de gemeente Helmond worden ook gebruikt voor de verbetering van het product voor andere klanten.

2. Risicoanalyse AI-systeem.

De gemeente Helmond heeft geen risicoanalyse uitgevoerd op het AI-systeem. Zivver heeft wel een DPIA uitgevoerd op de techniek. De gemeente Helmond heeft deze DPIA[1] (onder geheimhouding) ontvangen.

Naar aanleiding van de DPIA hebben FG en CISO nog aanvullende vragen gesteld aan/opmerkingen gemaakt richting Zivver. Op 11 december 2023 hebben we antwoorden ontvangen[2].
We hebben vervolgens een suggestie gedaan rondom de transparantie van de gegevensverwerking en nog een discussie gevoerd over de rolverdeling.

[1] Bijlage: DPIA - Machine learning-enhanced business rules (doc. nummer 51953887).
[2] Bijlage: Antwoord op vragen d.d. 11 dec 23 (doc. nummer 51953900).

2.1 Transparantie.

De Ciso heeft de suggestie gedaan om in de White paper informatie op te nemen over de inzet van machine learning/AI. Hierop heeft Zivver laten weten[3] dat zij de White paper geen geschikte locatie vonden. Ze deden de suggestie om daarover in de verwerkersovereenkomst meer informatie op te nemen dan wel in hun documentatieportaal.

Conclusie:

Het is gepast dat Zivver op de (in de mail van 12 januari 2024) aangegeven plek in hun documentatieportaal nadere informatie opneemt over de inzet van machine learning/AI. Verduidelijking in de verwerkersovereenkomst is niet nodig. We hebben dit op 24 maart 2024 per mail bevestigd[4]

2.2 Rolverdeling.

Bij de inzet van machine learning (binnen het AI-systeem) wordt data gebruikt, de vraag is wie verwerkersverantwoordelijk is voor de persoonsgegevens die daarbij worden verwerkt.
Zivver is van mening dat de gemeente verwerkersverantwoordelijke is. De FG van Helmond is het hiermee niet eens, zij meent dat Zivver verwerkingsverantwoordelijke is.

Standpunt van Zivver:

De gemeente is verwerkingsverantwoordelijk, omdat de data die wordt verwerkt onderdeel is van het aangekochte product. Bovendien is in de verwerkersovereenkomst opgenomen dat deze verwerkingen namens de klanten plaatsvinden.

Standpunt van FG van Helmond

De vraag wie verwerkingsverantwoordelijk moet worden beantwoord aan de hand van de vraag wie er feitelijk invloed heeft. De gemeente Helmond heeft deze invloed niet. Zij hebben namelijk geen invloed op het doel waarmee de data wordt verwerkt en de wijze waarop het model wordt getraind. De beslissingen daarover worden genomen door Zivver. Gemeente Helmond neemt weliswaar een product af wat continu wordt verbeterd, maar ze kan geen feitelijke invloed uitoefenen op de wijze waarop dit gebeurt. Dat verandert niet door hierover afspraken te maken in de verwerkersovereenkomst.

De FG van Helmond heeft hierover op 27 december 2023 per mail contact gehad[5]. Daarnaast heeft zij op 15 januari 2024 telefonisch contact gehad met de FG van Zivver (5.1.2e).

De FG van Zivver gaf tijdens dit gesprek aan dat hij regelmatig een gesprek heeft met Zivver over de rollen en informatiedeling. Bij de eerdere gesprekken zijn beide standpunten (over de rolverdeling) besproken. Zivver heeft vervolgens de genoemde keuze gemaakt, hij vindt de gegeven uitleg verdedigbaar. De FG van Helmond heeft vervolgens aangegeven dat zij de gegeven uitleg niet begrijpt en ze heeft onderbouwd waarom. De FG van Zivver vindt ook deze uitleg verdedigbaar. Hij bedankt voor de gegeven feedback. De feedback is voor hem reden om opnieuw het gesprek (over de rolverdeling) aan te gaan met Zivver.

Op 24 maart 2024 heeft de FG per mail[4] navraag gedaan naar het huidige standpunt van Zivver. Hier is op 27 maart 2024 nog geen reactie op ontvangen.

Conclusie:

[3] Bijlage: Reactie op vraag transparantie 12 januari 2024 (doc. nummer 51953889).
[4] Bijlage: Mail met vraag over standpunt rolverdeling d.d. 24 maart 24 (doc. nummer 51953896).
[5] Bijlage Vragen FG over rolverdeling 27 dec 23 (doc. nummer 51953888).

Er is (in ieder geval op dit moment) geen overeenstemming over de rolverdeling.
Zivver gaat er van uit dat de gemeente Helmond verwerkersverantwoordelijk is voor de verwerkingen die worden uitgevoerd om te kunnen leren van eerder verzonden berichten.

Dit betekent dat er twee opties zijn:

1. De gemeente Helmond gebruikt de functionaliteit (het AI-systeem) en accepteert het standpunt van de leverancier.
2. De gemeente Helmond volgt het standpunt van de FG. Dat betekent dat de functionaliteit niet kan worden gebruikt.

Het is aan de proceseigenaar om de risico's af te wegen en een keuze te maken.

De keuze voor optie 1 betekent dat de gemeente Helmond ook verantwoordelijk wordt gehouden voor een rechtmatige en eerlijke verwerking van persoonsgegevens tijdens het machine learning proces (binnen het AI-systeem). Aangezien de data niet exclusief wordt ingezet voor Helmond, betekent dit dat de gemeente Helmond ook verantwoordelijk is voor de rechtmatige en eerlijke verwerking van persoonsgegevens ten behoeve van andere klanten van Zivver. Dit terwijl zij hierop geen enkele invloed kan uitoefenen en een grondslag voor het gebruik van persoonsgegevens ten behoeve van andere klanten ontbreekt.

Ook in het kader van de op 9 december 2023 aangenomen maar nog niet van toepassing zijnde AI-act is het van belang om de onderlinge verantwoordelijkheden op een juiste manier vast te stellen. De AI-act stelt namelijk eisen aan de inzet van AI. Daarmee kan een onjuiste rolverdeling ook tot gevolg hebben dat de gemeente een grotere verantwoordelijkheid krijgt ten aanzien van de kwaliteit van het AI-systeem en de naleving van de AI act.

Omdat de gemeente de door Zivver uitgevoerde DPIA heeft ontvangen heeft zij wel inzicht gekregen in de wijze waarop Zivver op dit moment machine learning inzet. Geconcludeerd kan worden dat dit op **dit moment** voldoende veilig gebeurt. De privacy risico's voor betrokkenen (de afzenders en geadresseerden van de mails) zijn hierdoor klein.

2. Advies.

- Maak geen gebruik van het AI-systeem, omdat er geen overeenstemming is over de rolverdeling.
- Als de proceseigenaar na afweging van alle risico's toch kiest voor het gebruik van het AI-systeem:
  - Blijf met Zivver in gesprek over de rolverdeling.
  - Sluit een verwerkersovereenkomst.
  - Neem het AI-systeem op in het register van verwerkingen.
  - Vermeld in het register van verwerkingen uitdrukkelijk dat er gebruik wordt gemaakt van een algoritme, zodat deze verwerking in de toekomst eenvoudig kan worden opgenomen in het nog te ontwikkelen algoritme register.
- De FG en de Ciso te informeren over het besluit. (wordt er wel of niet gekozen voor gebruik van het AI-systeem).
- Als er wordt gekozen voor het gebruik van het AI-systeem: De FG en de Ciso te informeren over de wijze waarop gevolg wordt gegeven aan de geadviseerde maatregelen.
- Dit advies, het besluit en de gegeven terugkoppeling vast te leggen in de projectadministratie.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens geanonimiseerd op grond van:

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

Afdeling/Programma: S&B

Onderwerp: Bezwaarschrift in verband met audio-opnamen

Djuma: 51896054

Aanleiding

Het Juridisch Team van de afdeling Strategie & Bestuur wil graag audio-opnames gaan maken van de hoorzittingen van de bezwaarschriftencommissies met als doel om de werkdruk te verminderen voor de medewerkers. De Verordening bezwaar Helmond 2023 is hiervoor aangepast[1]. De afdeling heeft het plan om deze opnames te maken door middel van een smartphone waarna deze worden opgeslagen in Djuma.

Conclusie

Op grond van de uitgevoerde risico analyse kan **niet** worden vastgesteld dat er passende technische en organisatorische maatregelen zijn getroffen, die de persoonsgegevens beschermen tegen onrechtmatige verwerking en inbreuken op de beschikbaarheid, integriteit en vertrouwelijkheid.

Advies

1. Voer een nieuwe risico analyse uit.
2. Onderzoek, aan de hand van een programma van eisen, welke audio apparatuur het meest geschikt is.
3. Start pas met audioverslagen als er adequate apparatuur is aangeschaft. Op voorhand kan er niet van uitgegaan worden dat opnames via de Smartphone adequaat zijn.

Toelichting

Wanneer inwoners en andere betrokkenen het niet eens zijn met een besluit van de gemeente kunnen zij bezwaar maken. De algemene wet bestuursrecht bevat bepalingen over de wijze waarop een bezwaarschrift moet worden behandeld. Daarbij is ook vastgelegd[2] dat er van een hoorzitting een verslag moet worden gemaakt. Er is niet vastgelegd op welke wijze dit dient te gebeuren. Het is toegestaan om uit de beslissing op bezwaar blijkt van hetgeen er tijdens de hoorzitting is verhandeld.

De gemeenteraad van Helmond heeft ervoor gekozen om een audioverslag te maken van de hoorzitting. Dit betekent dat zij er voor hebben gekozen om een woordelijk verslag vast te leggen. Dit grijpt ernstiger in, in de persoonlijke levenssfeer van betrokkenen dan een verslag op hoofdlijnen.

Bezwaarschriften kunnen betrekking hebben op situaties die ernstig ingrijpen in de persoonlijke levenssfeer van mensen. Ter zitting kunnen zeer gevoelige en bijzondere persoonsgegevens worden uitgewisseld. Inbreuk op de beveiliging kan dan ook ernstige gevolgen hebben voor betrokkenen.

[1] Verordening behandeling bezwaarschriften Helmond 2023 (officiele-overheidspublicaties.nl)
[2] Artikel 7:7 Algemene wet bestuursrecht

De persoonsgegevens dienen dan ook goed te zijn beveiligd. Door technische maatregelen te treffen en deugdelijke opname apparatuur te gebruiken. Daarnaast dienen er passende organisatorische maatregelen (zoals werkinstructies) te worden getroffen.

Scope

In scope van deze DPIA zijn:

- Het proces 'bezwaarschrift' (zaaktypenummer B0756), het onderdeel verslaglegging van de hoorzitting;

Out-of-scope van deze DPIA zijn:

- De overige processtappen uit het proces bezwaarschrift.
- De ondersteunende applicatie Octopus is niet meegenomen in deze risicoanalyse, aangezien deze applicatie op korte termijn wordt uitgefaseerd ten behoeve van Djuma.
-

Gebruikte stukken

De FG en de CISO hebben het advies gebaseerd op de volgende documenten welke zijn bijgesloten in het dossier:

- Procesplaat Bezwaarschrift;
- Pre-DPIA rapport;
- DPIA Bezwaarschrift in verband met audio-opnamen;
- Quickscan RA bezwaarschrift in verband met audio-opnamen;
- Risicoanalyse Bezwaarschrift in verband met audio-opnamen;
- GAP-P Bezwaarschrift in verband met audio-opnamen;
- Verordening behandeling bezwaarschriften Helmond 2023.

Bijlage

1 Toets van de risicoanalyse

Een risicoanalyse heeft betrekking op informatieveiligheid en privacy. Voor privacy geldt dat de AVG een aantal vereisten stelt aan de uit te voeren risicoanalyse. Dit zijn de volgende vereisten:

1. Een systematische beschrijving van de beoogde verwerking en de doeleinden;
2. Een beoordeling van de noodzaak en de evenredigheid;
3. Een beoordeling van de risico's voor de rechten en vrijheden van betrokkenen;
4. Een overzicht van beoogde maatregelen om deze risico's aan te pakken.

Ad 1 een systematische beschrijving

Omschrijving	Toelichting
De risicoanalyse vermeldt: de persoonsgegevens die worden verwerkt	Zie pagina 9 van het DPIA rapport. Welke persoonsgegevens worden verwerkt? * Beeldmateriaal (videomateriaal, audiomateriaal) * Contactgegevens (e-mailadres, telefoonnummer, adres)

	* Identiteitsgegevens (identificatienr, paspoortnummer, BTW-nummer ZZP'er) * Locatiegegevens (lengtegraad, breedtegraad) * Persoonlijke gegevens (naam, geboortedatum, geboorteplaats, geslacht, gezinssamenstelling) Welke bijzondere persoonsgegevens worden verwerkt? * Biometrische gegevens * BSN * Financiële persoonsgegevens * Gezondheidsgegevens * Ras of etnische afkomst * Religieuze of levensbeschouwelijke overtuigingen * Seksueel gedrag of seksuele gerichtheid
De risicoanalyse vermeldt: de ontvangers van deze persoonsgegevens	Pag. 7 van de DPIA vermeldt de volgende partijen: Ontvangers van (van wie ontvangen): Bezwaarmaker(s) en belanghebbenden, Ontvangers (aan wie verstrekt): de audio-opnames worden niet verstrekt. De interne schriftelijke verslagen zijn bedoeld voor procespartijen, gerechten, ander interne teams en bestuurders. Daarnaast worden er gegevens ontvangen van commissieleden en ambtenaren die aanwezig zijn tijdens de hoorzitting. De audioverslagen worden niet verstrekt. Niet is uitgewerkt op welke wijze de audioverslagen worden omgezet in schriftelijke verslagen. De verordening spreekt over **ook** een schriftelijk verslag (artikel 14 lid 3). Dit betekent dat er in bepaalde situaties sprake is van twee verslagen. Het audioverslag én een schriftelijk verslag.
De risicoanalyse vermeldt: de periode gedurende welke de persoonsgegevens worden bewaard	De risico analyse bevat de officiële bewaartermijnen (blz 12), die zijn gekoppeld aan het dossier in het zaaksysteem Dit zijn de volgende bewaartermijnen. Informeel afgehandeld: vernietigen 5 jaar na afhandeling Informeel afgehandeld met financiële consequenties: vernietigen 7 jaar na afhandeling Gegrond met financiële consequenties: vernietigen 7 jaar na afhandeling Ongegrond met financiële consequenties: vernietigen 7 jaar na afhandeling Gegrond: 5 jaar na afhandeling Gegrond met invloed op een te bewaren zaak: bewaren Afgebroken: vernietigen 1 jaar na afhandeling Ongegrond: vernietigen 5 jaar na afhandeling Niet ontvankelijk verklaard: vernietiging 1 jaar na afhandeling Ingetrokken: vernietigen 1 jaar na afhandeling De risico analyse gaat niet in op de wijze waarop de audio-opnamen worden opgeslagen in het zaaksysteem. Bovendien ontbreekt informatie over de wijze hoe de informatie wordt vernietigd op de opname apparatuur. Het risico bestaat dat de opnames meervoudig worden opgeslagen.
De risicoanalyse bevat een functionele beschrijving van de verwerking	Op pagina 9 en 10 van het DPIA rapport wordt de levensscyclus van de bezwaarprocedure beschreven:

	1. Bezwaarschrift ontvangen via Djuma (eventueel via postkamer) plus aanmaken zaak; 2. Beoordelen ontvankelijkheid; 3. (eventueel hersteltermijn bij niet-ontvankelijkheid); 4. Ontvangstbevestiging naar bezwaarmaker; 5. Informeren vakafdeling met de vraag om contact op te nemen met de bezwaarmaker om te onderzoeken of de zaak informeel kan worden afgedaan. Zo niet, dan wordt er een hoorzitting ingepland; 6. Aanleveren verweerschrift inclusief inhoudelijk dossier vanuit de vakafdeling aan de secretaris van de bezwaarschriftencommissie; 7. Secretaris verspreid de stukken aan de bezwaarmaker (en eventuele belanghebbenden) en de leden van de bezwaarschriftencommissie per post; 8. Hoorzitting (waarin de audio-opnames worden gemaakt); 9. Uitwerking advies bezwaarschriftencommissie door secretaris; 10. Advies ter toetsing voorleggen aan leden bezwaarschriftencommissie; 11. Afstemmen met de vakafdeling of het advies al dan niet wordt gevolgd; 12. Beslissing op bezwaarschrift; 13. Afronden zaak in Djuma. Stap 8 is onvoldoende uitgewerkt. De levenscyclus die samenhangt met de audio opnamen ontbreekt dan ook. Hierdoor bestaat er geen inzicht in de risico's die samenhangen met de audio opnamen.
De risicoanalyse bevat de activa waarop persoonsgegevens steunen (hardware, software, netwerken, mensen, papier of papiertransmissiekanalen)	Pagina 10 DPIA beschrijft het MAPOOD-principe van de bezwaarschriftenprocedure en de voorgestelde middelen. Opmerkelijk is de keuze voor de smartphone en dat er geen alternatieven zijn onderzocht. **Mens: Welke mensen gebruiken het systeem?** Leden bezwaarschriftencommissies (alleen papieren dossiers) Bezwaarmakers (alleen papieren dossiers) Derde belanghebbenden (alleen papieren dossiers) Secretaris en ondersteuners bezwaarschriftencommissie (behandelaar) Teamleider S&B.JT (ambtelijk opdrachtgever) Afdelingshoofd: S&B (ambtelijk opdrachtgever) Medewerkers vakafdeling (adviseurs) **Apparatuur: Welke apparatuur kent het systeem?** Smartphone Laptops (er wordt geen gebruikgemaakt van de audiovisuele ondersteuning van de commissiekamers) Servers Visma Circle **Programmatuur: Welke programmatuur kent het systeem?** Dictafoon-app (Apple) Djuma Word **Organisatie: Welke organisatieonderdelen hebben met het systeem te maken?** Het systeem zal vooral gebruikt worden in het Huis voor de Stad. **Omgeving: Welke fysieke omgevingen zijn er voor het systeem?** Afdeling Strategie & Bestuur, Juridisch Team Desbetreffende vakafdeling **Diensten: Welke diensten horen bij het systeem?** Behandelen bezwaarschriften Ook dit onderdeel gaat voornamelijk in op de bezwaarprocedure, inzicht in de verwerkingen rondom de audio opnamen is onvoldoende. Het is niet duidelijk waar opslag (= verwerking)allemaal plaatsvindt; in ieder geval op iPhone en in Djuma, maar wellicht ook nog (tijdens overzetten) op de laptop?

Ad 2 De noodzaak en de evenredigheid wordt beoordeeld

Omschrijving	Toelichting
De risicoanalyse vermeldt de grondslag en de doeleinden van de verwerking.	Pag 11 van de DPIA bevat de grondslag: Artikel 14 lid 1 Verordening behandeling bezwaarschriften Helmond 2023 (art. 6 lid 1 sub e AVG, Publieke taak). Het doel staat op pagina 7 van de DPIA, namelijk: 1. Het behandelen van een bezwaar(schrift); 2. Verminderen administratieve lasten S&B.JT.
De risicoanalyse vermeldt welke gegevens en verwerkingen proportioneel is voor het bereiken van dit doel	De risico analyse gaat op pagina 11 weliswaar in op de noodzaak en proporitonaliteit van de verwerking van persoonsgegevens ten behoeve van de bezwaarprocedure. Er wordt echter niet ingegaan op de noodzaak en de proportionaliteit van de verslag legging door middel van audio apparatuur. Audio opnames van de hoorzitting, leggen vast wat er letterlijk is gezegd tijdens de hoorzitting. Dat is een ernstigere ingreep in de persoonlijke levenssfeer dan schriftelijke verslaglegging op hoofdlijnen. De gemeenteraad heeft voor deze ingrijpendere verwerking gekozen. De gemaakte afweging ontbreekt echter in de stukken. Ook is niet afgewogen waarom het noodzakelijk is om, indien van toepassing, naast een schriftelijk verslag ook het audio verslag te bewaren. Dit betekent namelijk dat er in dat geval twee verslagen aanwezig zijn.
De risicoanalyse vermeldt of er een minder ingrijpende gegevensverwerking mogelijk is	Er is een minder ingrijpende verwerking mogelijk (namelijk schriftelijke verslaglegging). De DPIA vermeldt niet de gemaakte afweging. Daarnaast blijkt uit de DPIA niet dat er (mogelijk) minder ingrijpende alternatieven van audioverslaglegging zijn onderzocht.
De risicoanalyse bevat een omschrijving van de maatregelen die worden getroffen om de verwerking te beperken tot de ter zake dienende noodzakelijke gegevens	Deze ontbreken. Er wordt immers niet ingegaan op het proces rondom het opnemen, overdragen naar djuma, opslaan, bewaren en vernietigen van gegevens. Het risico bestaat dat het audio verslag te lang of dubbel wordt bewaard bijvoorbeeld omdat het audioverslag zowel op de opname apparatuur als in Djuma is opgeslagen. Indien in de voorgeschreven gevallen wordt verzocht om een schriftelijk verslag, is er sprake van een dubbele opslag.
De risicoanalyse bevat een omschrijving van de maatregelen die worden getroffen om te zorgen dat geen function creep[3] optreedt.	Dit ontbreekt.
De risicoanalyse bevat een omschrijving van de maatregelen die worden getroffen om ervoor te zorgen dat gegevens niet langer dan noodzakelijk worden opgeslagen in een vorm die het mogelijk maakt om betrokkene te identificeren.	In de pre-DPIA (pag 5) is aangegeven dat de handhaving van de bewaartermijnen automatisch is ingericht. Op die manier worden persoonsgegevens in het zaaksysteem niet langer bewaard dan noodzakelijk voor het doel. Inzicht en daarmee maatregelen die er voor moeten zorgen dat het audio verslag niet langer dan noodzakelijk wordt bewaard op de gebruikte opname apparatuur en (eventuele) laptop ontbreekt.
De risicoanalyse bevat een omschrijving van de wijze waarop betrokkene	De betrokkenen worden onvoldoende geïnformeerd over hun rechten, en er is geen verwijzing naar de algemene privacyverklaring van de

[3] function creep is wat er gebeurt als we technologie en systemen gebruiken op een andere manier dan in de eerste instantie eigenlijk bedoeld is, met name wanneer het nieuwe doel resulteert in een inbreuk op de privacy.

(toereikend) wordt geïnformeerd.	gemeente Helmond. Daarnaar moet worden verwezen, of er moet een aparte privacyverklaring worden opgesteld. (pagina 12 DPIA)
De risicoanalyse bevat een omschrijving van hoe betrokkenen hun rechten uit kunnen oefenen: a. rechten van inzage b. recht op rectificatie en verwijdering c. recht op bezwaar d. recht op beperking van de verwerking	Op pagina 12 DPIA wordt verwezen naar het feit dat via het webportaal een verzoek m.b.t. de rechten van de betrokkene kan worden ingediend. Echter, op de webpagina van de gemeente Helmond met informatie over de bezwaarschriftprocedure, kan de verwijzing daar naartoe duidelijker worden weergegeven door een knop te maken naar het webportaal. Dit kan worden verbeterd door: • Op de webpagina van 'bezwaar' duidelijk naar te verwijzen naar de privacyverklaring van de gemeente Helmond. • Op de webpagina van 'bezwaar' duidelijk te verwijzen naar het webportaal via welke (potentiële) bezwaarmakers gebruik kunnen maken van de volgende rechten: recht op toegang, recht op inzage, recht op rectificatie, recht op gegevenswissing/vergetelheid, recht op beperking van de verwerking en recht op bezwaar tegen de verwerking.
De risicoanalyse beschrijft de relatie met verwerkers	Visma Circle is (als leverancier van het zaaksysteem) een verwerker van de gemeente Helmond. Zie pagina 7 DPIA. In de voorgestelde werkwijze worden opnames gemaakt met de Smartphone er wordt daarbij gebruik gemaakt van de dictafoon App. Daarnaast wordt er mogelijk ook informatie opgeslagen op de laptop. De relatie met deze leveranciers (Apple, Microsoft) ontbreekt in de DPIA.
De risicoanalyse beschrijft de waarborgen omtrent internationale doorgifte	De DPIA vermeldt ten onrechte dat alle data blijft binnen de Europese Economische Ruimte blijft. Bij gebruik van de Smartphone, worden er gegevens verwerkt door Apple dit is een Amerikaans bereikt. Niet is onderzocht of Apple afdoende maatregelen heeft getroffen om te voldoen aan Europese regelgeving.
De risicoanalyse vermeldt of voorafgaande raadpleging nodig is.	N.v.t. er is geen hoog risico dat niet kan worden gemitigeerd.

Ad 3 de risico's voor de rechten en vrijheden van betrokkenen

Omschrijving	Toelichting
De risicoanalyse brengt de risico's voldoende in beeld.	Aangezien onvoldoende zicht is op de processen rondom de de audio opnames, zijn de risico's ook niet voldoende in beeld.
De bedreigingen die kunnen leiden tot onrechtmatige toegang zijn benoemd. De mogelijke gevolgen voor de rechten en vrijheden van betrokkenen zijn geïdentificeerd. Ze zijn benoemd vanuit het perspectief van betrokkenen en er is daarbij ook gedacht aan de gevolgen die dit heeft op het recht op: • zelfstandigheid (bijvoorbeeld de mogelijkheid om bepaalde handelingen uit te voeren);	Er is geen zicht op de bedreigingen die kunnen leiden tot onrechtmatige toegang op de audioverslagen op de iphone. Ook de bedreigingen die kunnen leiden tot onrechtmatige toegang tot de gegevens op het moment dat zij worden overgezet van iphone naar het zaaksysteem ontbreken. Verslaglegging van alle hoorzittingen vinden plaats door middel van een audioverslag. Dat geldt ook voor de hoorzitting van kamer 2. In deze kamer worden gevoelige onderwerpen behandeld. De zitting vindt daarom ook plaats achter gesloten deuren. Een audioverslag bevat de letterlijke weergave van wat er tijdens een hoorzitting is gezegd. Bij schriftelijke verslaglegging bevat slechts een weergave van wat er is gezegd. Dit betekent ook dat er veel meer informatie van betrokkenen wordt vastgelegd en dat daarmee de risico's op nadelige gevolgen voor betrokkenen veel groter zijn in het geval dat er sprake is van onrechtmatige toegang.

• vrij blijven van stigmatisering (bijvoorbeeld niet op een bepaalde wijze behandeld worden op basis van bepaalde kenmerken); • gelijkheid (bijvoorbeeld het op dezelfde wijze benaderd worden als andere betrokkenen); • vrij blijven van manipulatie (bijvoorbeeld niet beïnvloed worden op gedrag op basis van een (afwijkend) levenspatroon); • integriteit (verlies van eigenheid, waardigheid en ongeschondenheid, niet jezelf kunnen zijn, je moeten aanpassen aan wat anderen vinden hoe je moet zijn); • ongestoord leven (waarbij het bijvoorbeeld kan gaan om identiteitsfraude of (onaangenaam) afbreken van rust en stilte). • eigenwaarde (bijvoorbeeld geen afbreuk aan persoonlijkheid). • autonomie (bijvoorbeeld geen beperking van de vrijheid om eigen regels te volgen) Vooral van zaken als stigmatisering, ongelijkheid, manipulatie en niet ongestoord kunnen leven kunnen betrokkenen last hebben. • Daarnaast zijn de risico's voor de organisatie benoemd.	Denk bv aan een uitgebreide beschrijving van de gezondheid, terwijl in een schriftelijk volstaan kan worden met de beperkingen die worden ervaren.
De waarschijnlijkheid en ernst zijn ingeschat.	De waarschijnlijkheid tot onrechtmatige toegang is groter als gegevens vaker en op meerdere plekken worden opgeslagen. (bv op de iphone én in het zaaksysteem". De gevolgen voor betrokkenen zijn ernstiger bij ongewenste toegang tot een audioverslag dan bij ongewenste toegang tot een schriftelijk verslag op hoofdlijnen.
De bedreigingen die kunnen leiden tot ongewenste wijziging zijn benoemd. (inbreuk op de integriteit van de gegevens)	Zie opmerkingen bij ongewenste toegang. Aanvullend kan worden opgemerkt. Dat het relevant is dat de opname kwaliteit zodanig is dat er geen misverstand kan ontstaan over wat er is gezegd. Dat betekent dat de opname kwaliteit goed dient te zijn. Slechte kwaliteit van de opname, is een inbreuk op de integriteit van de gegevens.

De mogelijke gevolgen voor de rechten en vrijheden van betrokkenen zijn geïdentificeerd. Ze zijn benoemd vanuit het perspectief van betrokkenen en er is daarbij ook gedacht aan de bij het vorige punt genoemde gevolgen. Daarnaast zijn de risico's voor de organisatie benoemd	Het maken van een hoorverslag is voorgeschreven ten behoeve van een beslissing. Daarnaast is het voorgeschreven met het oog op oordeelsvorming door de rechter in het geval er beroep wordt ingesteld. Het audioverslag wordt niet verstrekt, dat betekent dat er in het geval er beroep wordt ingesteld alsnog een schriftelijk verslag op hoofdlijnen dient te worden opgesteld. Onjuiste of onduidelijke verslaglegging kan invloed hebben op het schriftelijke verslag en daarmee op het oordeel van de rechtbank.
De waarschijnlijkheid en ernst zijn ingeschat.	Het valt te verwachten dat dit een goede kwaliteit van de opname in een grote ruimte niet mogelijk is met behulp van een iphone. De waarschijnijkheid is daarom groot. De gevolgen voor betrokkenen kunnen groot zijn, omdat het verslag bijdraagt aan de oordeelsvorming. De beslissing op een bezwaar of een beroepszaak heeft gevolgen voor betrokkenen. Hoe ernstig dit is, is mede afhankelijk van de aard van het bezwaarschrift.
De bedreigingen die kunnen leiden tot het niet beschikbaar zijn van gegevens zijn benoemd. De mogelijke gevolgen voor de rechten en vrijheden van betrokkenen zijn geïdentificeerd. Ze zijn benoemd vanuit het perspectief van betrokkenen en er is daarbij ook gedacht aan de bij het vorige punt genoemde gevolgen. Daarnaast zijn de risico's voor de organisatie benoemd	Zie de twee vorige punten.
De waarschijnlijkheid en ernst zijn ingeschat.	Zie eerdere punten

Ad 4 de maatregelen worden benoemd

Omschrijving	Toelichting
De beoogde maatregelen om de risico's aan te pakken worden bepaald en zijn voldoende.	Die zijn onvoldoende in beeld.

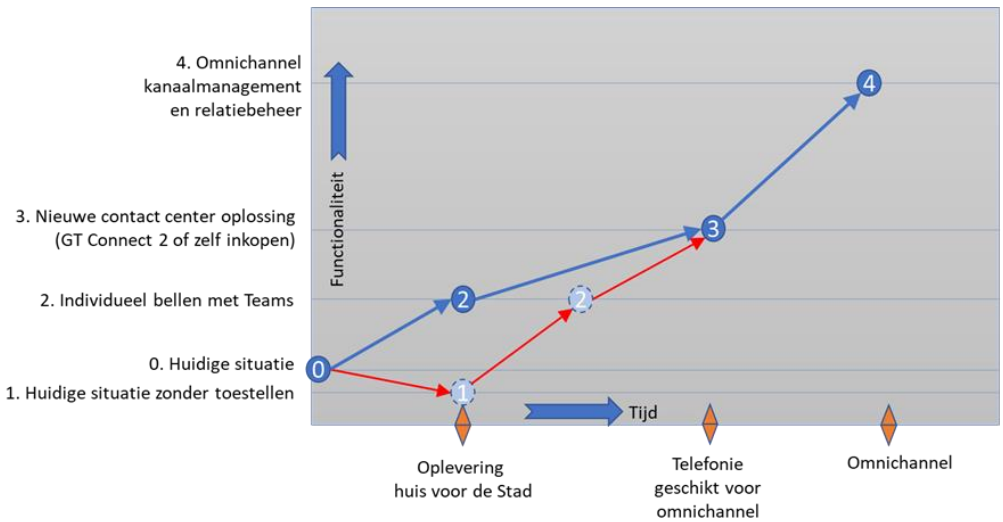
Afdeling/Programma: Altijd Verbonden

Onderwerp: Bellen via MS Teams

Aanleiding

Achtergrond
In 2024 wordt het nieuwe Huis voor de Stad geopend met allerlei nieuwe voorzieningen voor hybride werken. In het kader van het programma Altijd Verbonden kunnen medewerkers op locatie in het Huis voor de Stad werken of juist op een externe locatie thuis of bij een relatie. Om dit mogelijk te maken zijn verschillende veranderingen doorgevoerd zoals de nieuwe werkplek voor plaats onafhankelijk werken en vergadervoorzieningen voor hybride vergaderingen.
In het nieuwe Huis voor de Stad zijn geen voorzieningen opgenomen voor het gebruik van vaste telefoontoestellen, zodat iedereen moet werken met de laptop of smartphone via draadloos internet of een 3G/4G/5G-verbinding om te kunnen bellen.
De Coronapandemie heeft geleerd dat vaste telefoons nog nauwelijks worden gebruikt; het meeste individuele telefoonverkeer wordt via smartphones gevoerd. De contactcentra van TD en Sociaal Domein werken momenteel nog wel via vaste toestellen en de telefooncentrale. In het Huis voor de Stad zal echter ook dit telefoonverkeer via een softwareoplossing (moeten) gaan lopen.

Doel
Het project, dat deel uitmaakt van de omnichannel dienstverlening, heeft tot doel alle telefoonverkeer via vaste toestellen te migreren naar laptops en smartphones, zodat iedereen vanaf de oplevering van het Huis voor de Stad plaats onafhankelijk en zonder (vast) telefoontoestel kan bellen.



Afbeelding: groeipad omnichannel telefonie.

Om dit mogelijk te maken zijn de volgende oplossingen nodig:

- Voor het individuele telefoonverkeer met vaste toestellen wordt gemigreerd naar bellen via MS Teams, zodat medewerkers kunnen bellen vanaf hun laptop met headset of met de Teams-app op de smartphone.

- Voor contactcentra blijft het telefoonverkeer via de Mitel centrale lopen. Om zonder toestel te kunnen bellen wordt een applicatie van Mitel beschikbaar gesteld op de laptop.

Voor medewerkers betekent dit dat alle individuele communicatiekanalen samen komen in Teams op de standaard werkplek en op de smartphone. Daardoor wordt het telefoonverkeer plaats-onafhankelijk. Naast het plaats onafhankelijk kunnen werken is deze verandering ook een belangrijke stap naar omnichannel dienstverlening. Alle gesprekken via Teams kunnen in principe in de nabije toekomst eenvoudig worden vastgelegd in de contacthistorie van de klant, wanneer blijkt dat klantgericht werken en privacywetgeving dit toelaten.

De groei naar omnichannel dienstverlening wordt ook aangegrepen om de telefonische bereikbaarheid te verbeteren. Naast de invoering van de nieuwe technologie worden ook nieuwe afspraken gemaakt over de telefonische bereikbaarheid zodat het doorschakelen van gesprekken van contactcenter naar afdeling of medewerker verbetert.

Samenvatting
Kernachtig weergegeven heeft dit project tot doel te gaan (spraak/audio) bellen via MS Teams. Niet meer en niet minder. Het is de bedoeling dat alleen 1 op 1 gesprekken gaan plaatsvinden. Dus géén groepsgesprekken en géén video bellen. Deze mogelijkheden zitten dan ook niet in scope van dit project.

Medewerkers gaan, in plaats van met vaste telefoons en/of de belapplicatie van de smartphone, bellen via de MS Teams applicatie op laptop of smartphone. Dit houdt in, dat een medewerker bereikbaar blijft op zijn directe vaste 0492-telefoonnummer en wanneer de medewerker op dat vaste nummer wordt gebeld wordt dit automatisch doorgeschakeld naar de MS Teams app en 'rinkelt' Teams en kun je het gesprek aannemen in de MS Teams app.

Uitgaande gesprekken, zowel intern als extern, kunnen ook via de MS Teams app worden opgezet. Dit alles gaat via het Public Switched Telephone Network (PSTN); en dan alleen bellen met spraak/audio. Hiervoor zijn alleen naam en telefoonnummer noodzakelijk. *Beeldbellen met klanten is op dit moment niet voorzien en valt daarmee buiten scoop van dit project.*

Gebruikte stukken

De FG en de CISO hebben het advies gebaseerd op de volgende documenten:
- DPIA;
- Startnotitie project vervanging vaste telefonie;
- PQR-adviesrapport security M365 *);
- Project start architectuur vervanging vaste telefonie;
- Door Privacy Company (5.1.2e) uitgevoerde DPIA's, DTIA's en DRia's op de diverse MS365 tools, waaronder MS Teams.

*): In het adviesrapport van PQR, over de security van het M365-platform, wordt gesteld dat 'external access', het communiceren met particulieren en burgers, zou moeten worden geblokkeerd, omdat dit gegevensverlies-, phishing- en social engineering-risico's met zich mee zou kunnen brengen. Deze stelling en het bijbehorende advies heeft vooral betrekking op beeldbellen en is voor het via spraak/audio bellen via MS Teams niet van toepassing en valt daarmee buiten scope van dit project.

Nadere toelichting: het is niet mogelijk om over te gaan naar beeldbellen (wat op dit moment ook niet is voorzien in het project) als er met een telefoonnummer wordt gebeld.

Wordt er met een e-mailadres met een particulier/burger voor een Teams-meeting gebeld dan is dit wél aan de orde. Met deze toelichting en wetende, dat beeldbellen geen onderdeel uitmaakt van dit project -en in de nabije toekomst ook niet is voorzien- kan dit risico buiten beschouwing worden gelaten. Het valt niet binnen de scope van het project bellen via MS Teams.

Conclusie

Met het (spraak/audio) bellen via MS Teams zullen contact- en persoonsgegevens worden verwerkt van medewerkers van de gemeente Helmond en hun externe relaties, leveranciers en ketenpartners. Daarnaast wordt (evenals bij bellen via n vaste verbinding) persoonsgegevens verwerkt in het gevoerde gesprek zelf.

In algemene zin geldt dat er passende technische en organisatorische maatregelen moeten worden getroffen, om de persoonsgegevens te beschermen tegen onrechtmatige verwerking en inbreuken op de beschikbaarheid, integriteit en vertrouwelijkheid. De uitgevoerde risicoanalyse geeft inzicht in de geconstateerde risico's en de te nemen maatregelen om deze risico's te mitigeren.

Door middel van de baseline toets is bepaald dat het gewenste/vereiste beschermingsniveau gemiddeld BNN2 is. De risico's t.a.v. beschikbaarheid en vertrouwelijkheid scoort ***'midden'***, het risico t.a.v. integriteit scoort ***'laag'***.

De uitgevoerde risicoanalyse voldoet aan de daaraan door wet- en regelgeving gestelde eisen. De te treffen maatregelen mitigeren in voldoende mate de risico's.

De conclusie uit de DPIA is dat de verwerking een 'aanvaardbaar' privacy risico vormt, voor de betrokkenen, medewerkers en relaties van de gemeente Helmond. Het privacy risico is aanvaardbaar mits voor de start van het project bellen via MS Teams de onderstaande maatregelen te implementeren.

Het niet opvolgen van dit advies en het niet implementeren van de (aanvullende) maatregelen betekent dat de privacy risico's voor betrokkenen blijven bestaan. Zowel de proceseigenaar als de gemeente Helmond blijven daarmee risico lopen. Het niet opvolgen van dit advies betekent dat de proceseigenaar de geconstateerde rest-risico's accepteert. Hij zal daarbij beargumenteerd moeten vastleggen waarom dit rest-risico acceptabel wordt geacht.

Advies

De FG en CISO adviseren om:

- Alle volgende maatregelen op te nemen in een *plan van aanpak*.
    - Richt een relatiebeheersysteem in.
    - Tref tot de inrichting van het relatiebeheersysteem maatregelen om te borgen
        - dat gegevens inderdaad niet (in- en/of extern) worden gedeeld tenzij betrokkene hier uitdrukkelijk toestemming voor heeft gegeven.
        - medewerkers zich houden aan de organisatieafspraken, rondom het bewaren en delen van contactgegevens.
    - Beschrijf (ook voor de huidige situatie) wanneer er niet langer sprake is van een actieve relatie.
    - geef duidelijk aan wat de gevolgen van het bestuderen van de gebruiksvoorwaarden/privacybeleid van MS Teams op de bewaartermijn zijn.
    - Leg de verwerking van contactgegevens vast in het register van verwerkingen.
    - Leg bij elke verwerking vast dat (telefoon)gesprekken plaatsvinden via Teams

- Maak geen gebruik van de mogelijkheid om gesprekken op te nemen binnen teams.
- Neem maatregelen om te borgen dat gesprekken niet worden opgenomen denk daarbij aan:
  - Bewustwording
  - Technische maatregelen die het opnemen onmogelijk maken
- Mocht er toch behoefte bestaan aan het maken van opnames: voer eerst een risico analyse uit om vast te stellen wat de mogelijkheden en risico's zijn. Er moet bv voorkomen worden dat opgenomen gesprekken onbeheerd worden opgeslagen.
- Maak geen gebruik van de mogelijkheid om gesprekken te loggen.
- Neem technische maatregelen die logging onmogelijk maken.
- Mocht er toch behoefte bestaan aan het loggen van gesprekken, onderbouw dan de noodzaak en voer een risico analyse uit om vast te stellen wat de mogelijkheden en risico's zijn.
- Maak beeldbellen met inwoners/particulieren onmogelijk door:
  - In de communicatie, te wijzen op de organisatieafspraak dat er met inwoners/particulieren niet via beeldbellen wordt gecommuniceerd.
  - Technische maatregelen te treffen die beeldbellen onmogelijk maken.
  - Op te halen of en zo ja waar er wel behoefte bestaat aan beeldbellen en een planning te maken voor (eventuele) invoering van beeldbellen
- Tref maatregelen om functioncreep te voorkomen. Tref in ieder geval de volgende maatregelen:
  - Voer een risico analyse uit voordat gestart wordt met het opbouwen van een klantbeeld
  - Creëren bewustwording en stel richtlijnen en procedures op ter voorkoming van function creep.
- Stem, om de vertrouwelijkheid en de integriteit van de gespreksgegevens te borgen, de maatregelen die volgen uit de risicoanalyse van het telefonieproject af op de activiteiten voor de beveiliging van MS365.
- Standaardiseer naar smartphones van een gemeente, voor iedereen die zonder laptop bereikbaar moet zijn.
- Neem in de communicatie rondom de invoeren van telefonie via teams ook mee dat vertrouwelijke gesprekken worden gevoerd op een plek waar niet kan worden meegeluisterd. (ook niet door collega's met een andere taak).
- Maak afspraken over de telefonische bereikbaarheid met medewerkers
- Instrueer medewerkers van contactcenters over het doorschakelen van gesprekken
- Instrueer de servicedesk over hoe calls over telefonie afgehandeld moeten worden.

- Voeg dit plan van aanpak toe aan de projectadministratie, bewaak de voortgang en stuur op de implementatie van de aanvullende maatregelen. Rapporteer over de voortgang van het plan van aanpak.
- De rapportages op te slaan in Djuma en niet op een lokale schijf/teams/SharePoint, in verband met de handhaving van bewaartermijnen;
- In geval aanvullende vragen, functionaliteiten, dienstverlening worden toegevoegd aan het project een aanvullende risicoanalyse uit te voeren en waar nodig aanvullende maatregelen te treffen;
- De risicoanalyse over drie jaar, bij wijzigingen van het proces of de gebruikte systemen te herhalen.

Voor een uitgebreidere toelichting op bovenstaande adviezen wordt kortheidshalve verwezen naar bijlage 1.

Reactie FG en CISO

Bovenstaand advies van de SPO is gezien op 23 augustus 2023 gezien en aangepast door de FG en wordt gedragen door FG en CISO. Het kan dan ook worden gezien als een advies van FG en CISO.

Bijlage 1 Toets van de risicoanalyse

Een risicoanalyse heeft betrekking op informatieveiligheid en privacy. Voor privacy geldt dat de AVG een aantal vereisten stelt aan de uit te voeren risicoanalyse: Dit zijn de volgende vereisten:

1. Een systematische beschrijving van de beoogde verwerking en de doeleinden;
2. Een beoordeling van de noodzaak en de evenredigheid;
3. Een beoordeling van de risico's voor de rechten en vrijheden van betrokkenen:
4. Een overzicht van beoogde maatregelen om deze risico's aan te pakken.

Ad 1 een systematische beschrijving

Omschrijving	Toelichting
De risicoanalyse vermeldt: de persoonsgegevens die worden verwerkt	Aangegeven wordt dat contact- en persoonlijke gegevens (naam en telefoonnummer) worden verwerkt. Niet rechtstreeks in MS Teams, maar in daaraan gekoppelde MS applicaties. In dit geval MS Outlook. Daarnaast (en niet in de stukken vermeld), worden er tijdens de gevoerde gesprekken gegevens verwerkt.
De risicoanalyse vermeldt: de ontvangers van deze persoonsgegevens	De verwerkte persoonsgegevens worden (volgens opgave) niet met derden gedeeld. De gegevens worden alleen gebruikt om telefonisch (via geluid en spraak) contact op te kunnen nemen met derden. Er is nu nog geen relatiebeheersysteem van de gemeente. Hierdoor is er geen centraal beheer ook niet op het (in- en/of extern) delen van (contact)gegevens. Eventuele ontvangers van persoonsgegevens die tijdens het gesprek zijn gedeeld, zijn onderdeel van het proces waarover het gesprek wordt gevoerd en komen hier niet terug. *Advies:* - *Richt een relatiebeheersysteem in.* - *Tref tot die tijd maatregelen om te borgen dat gegevens inderdaad niet (in- en/of extern) worden gedeeld tenzij betrokkene hier uitdrukkelijk toestemming voor heeft gegeven.* - *Neem dit op in het op te stellen plan van aanpak aanvullende maatregelen voor implementatie*.
De risicoanalyse vermeldt: de periode gedurende welke de persoonsgegevens worden bewaard	In de DPIA, hoofdstuk 3, fundamentele principes, wordt dat aangegeven: niet langer bewaard dan nodig is; gegevens worden bewaard zolang er sprake is van een actieve relatie. Zodra deze is beëindigd worden de gegevens verwijderd. Handhaving van de bewaartermijn wordt geautomatiseerd afgedwongen. Opgemerkt wordt, dat het kan zijn dat MS Teams zelf voorwaarden stelt aan de bewaartermijn. Daarom worden in een latere fase de gebruiksvoorwaarden en het privacybeleid van MS Teams geraadpleegd en bestudeert. Er is nu nog geen relatiebeheersysteem van de gemeente. Hierdoor is er geen centraal beheer ook niet op het bewaren van (contact)gegevens van onze relaties.

	Het eventueel bewaren van persoonsgegevens die tijdens het gesprek zijn gedeeld, is onderdeel van het proces waarover het gesprek wordt gevoerd en komt terug bij het proces zelf en niet in deze analyse. *Advies:* *- Richt een relatiebeheersysteem in;* *- Beschrijf (ook voor de huidige situatie) wanneer er niet langer sprake is van een actieve relatie.* *-Tref (tot de inrichting van het relatiebehersysteem maatregelen om te borgen medewerkers zich houden aan de organisatieafspraken.* *- geef duidelijk aan wat de gevolgen van het bestuderen van de gebruiksvoorwaarden/privacybeleid van MS Teams op de bewaartermijn zijn.* *Neem dit op in het op te stellen plan van aanpak aanvullende maatregelen voor implementatie*.
De risico analyse bevat een functionele beschrijving van de verwerking	Zie hiervoor de project start architectuur (PSA). *Advies:* *-Leg de verwerking van contactgegevens vast in het register van verwerkingen.* *-Leg bij elke verwerking vast dat (telefoon)gesprekken plaatsvinden via Teams* *Neem dit op in het op te stellen plan van aanpak aanvullende maatregelen voor implementatie*.
De risicoanalyse bevat de activa waarop persoonsgegevens steunen (hardware, software, netwerken, mensen, papier of papiertransmissiekanalen)	Zie ook de Project Start Architectuur. Mens: medewerkers van de gemeente Helmond en haar externe relaties. Apparatuur: computers en servers die zich in Nederland bevinden. Programmatuur: het MS365 platform, meer specifiek MS Teams (PSTN-functionaliteit). *Specifiek t.b.v. het KCC is dit het Mitel Contact Center, welke voor deze risicoanalyse buiten scope valt.* Organisatie: Microsoft en gemeente Helmond.

Ad 2 De noodzaak en de evenredigheid wordt beoordeeld

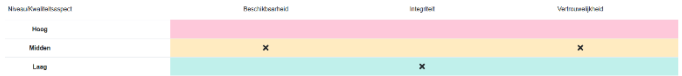
Omschrijving	Toelichting
De risicoanalyse vermeldt de grondslag en de doeleinden van de verwerking	Om haar taken als gemeente, zijnde het vervullen van een taak van algemeen belang en/of het vervullen van een taak in het kader van de uitoefening van het openbaar gezag, moet de gemeente voor haar relaties en ketenpartners ook telefonisch goed bereikbaar zijn en moet de gemeente haar medewerkers in staat stellen te kunnen bellen met relaties, burgers en ketenpartners. De gemeente heeft een *gerechtvaardigd belang* om dit in relatie tot haar taak te realiseren. Het doel van de verwerking is het uitvoeren van telefonie via MS Teams. Hiervoor zullen vooral namen en telefoonnummers worden verwerkt, welke in de contactgegevens in MS Outlook worden bewaard/opgeslagen. De grondslag voor het verwerken van persoonsgegevens binnen de gevoerde gesprekken volgt uit de gemeentelijke taak die op dat moment wordt uitgevoerd.
De risicoanalyse vermeldt welke gegevens en verwerkingen er noodzakelijk zijn voor het bereiken van dit doel	Behalve contactgegevens, worden er ook gegevens verwerkt tijdens het telefoongesprek zelf. Teams kent de mogelijkheid om gesprekken op te nemen. Daarnaast kent de telefonieoplossing van Teams de mogelijkheid om gesprekken loggen, zoals ook in de Mitelomgeving. Het gaat hierbij om metadata over het contact met bv het telefoonnummer, het tijdstip en de duur van het gesprek. Er is niet beschreven of van de mogelijkheid om gesprekken op te nemen en/of te loggen gebruik wordt gemaakt. En, indien dit het geval is, of dit noodzakelijk is voor het te bereiken doel (dan wel een minder ingrijpende oplossing mogelijk is). Of het delen van persoonsgegevens via een gesprek noodzakelijk is, is onderdeel van het proces ten behoeve waarvan het gesprek wordt gevoerd. De beoordeling vindt niet in deze analyse plaats. *Advies:* - *Maak geen gebruik van de mogelijkheid om gesprekken op te nemen binnen teams* - *Neem maatregelen om te borgen dat gesprekken niet worden opgenomen denk daarbij aan:* ▪ *Bewustwording* ▪ *Technische maatregelen die het opnemen onmogelijk maken* - *Mocht er toch behoefte bestaan aan het maken van opnames: voer eerst een risico analyse uit om vast te stellen wat de mogelijkheden en risico's zijn. Er moet bv voorkomen worden dat opgenomen gesprekken onbeheerd worden opgeslagen.* - *Maak geen gebruik van de mogelijkheid om gesprekken te loggen.* - *Neem technische maatregelen die logging onmogelijk maken.* - *Mocht er toch behoefte bestaan aan het loggen van gesprekken, onderbouw dan de noodzaak en voer een risico analyse uit om vast te stellen wat de mogelijkheden en risico's zijn.* *<u>Neem dit op in het op te stellen plan van aanpak aanvullende maatregelen voor implementatie</u>*.
De risicoanalyse vermeldt of er een minder ingrijpende gegevensverwerking mogelijk is	Zie vorig punt. De analyse heeft betrekking op telefonie (audio/spraak). Via teams is het ook mogelijk om beeld te bellen (via e-mail). Beeldbellen is ingrijpender dan (spraak/audio)bellen. Beeldbellen valt buiten scope van dit project. Beeldbellen is echter wel mogelijk, maar op basis van organisatieafspraken (nog) niet toegestaan. Dit project is hét moment om (aanvullende) maatregelen te treffen om nakoming van deze afspraak te borgen.

	Advies: *Maak beeldbellen met inwoners/particulieren onmogelijk door:* - *In de communicatie, te wijzen op de organisatieafspraak dat er met inwoners/particulieren niet via beeldbellen wordt gecommuniceerd.* - *Technische maatregelen te treffen die beeldbellen onmogelijk maken.* - *Op te halen of en zo ja waar er wel behoefte bestaat aan beeldbellen en een planning te maken voor (eventuele) invoering van beeldbellen* *Neem dit op in het op te stellen plan van aanpak aanvullende maatregelen voor implementatie*.
De risicoanalyse bevat een omschrijving van de maatregelen die worden getroffen om de verwerking te beperken tot de ter zake dienende noodzakelijke gegevens	*Zie de adviezen hierboven bij de beoordeling van de noodzakelijkheid en de vraag of er een minder ingrijpende manier mogelijk is.*
De risicoanalyse bevat een omschrijving van de maatregelen die worden getroffen om te zorgen dat geen function creep[1] optreedt.	Op het eerste oog vormt function creep een gering risico. Het verwerken van contactgegevens heeft als doel contact op te kunnen nemen met betrokkenen. Wel bestaat het risico dat een contactgegeven is doorgegeven aan de gemeente voor een specifieke taak en dat het gegeven (intern) wordt uitgewisseld en wordt gebruikt voor een andere taak. Al zal betrokkene hier in het algemeen geen problemen mee hebben, er mag toch niet voetstoots van uit worden gegaan. Alleen met toestemming kunnen de contactgegevens (intern) worden gedeeld. *Advies:* *zie het advies bij onderdeel 1: de ontvangers van de persoonsgegevens.* Individueel bellen wordt gezien als een essentiële stap in het verbeteren van de klantgerichtheid. Men wil contacten met klanten en relaties registreren, zodat een klantbeeld wordt opgebouwd zodat bij gesprekken kan worden teruggegrepen op contacten die al zijn geweest. Het opbouwen van een klantbeeld is een nieuwe verwerking, met een nieuw doel die mogelijk een inbreuk vormt op de privacy. Zonder risico analyse de contactgegevens gebruiken voor dit doel is function creep. *Advies:* *Tref maatregelen om functioncreep te voorkomen. Tref in ieder geval de volgende maatregelen:* - *Zie hiervoor de hierboven al genoemde adviezen bv bij het onderdeel 1 de ontvangers van de persoonsgegevens.* - *Voer een risico analyse uit voordat gestart wordt met het opbouwen van een klantbeeld* - *Creëren bewustwording en stel richtlijnen en procedures op ter voorkoming van function creep*. *Neem dit op in het op te stellen plan van aanpak aanvullende maatregelen voor implementatie*.
De risicoanalyse bevat een omschrijving van de maatregelen die worden getroffen om ervoor te zorgen dat gegevens niet	Zie adviezen bij onderdeel 1: het bewaren van persoonsgegevens.

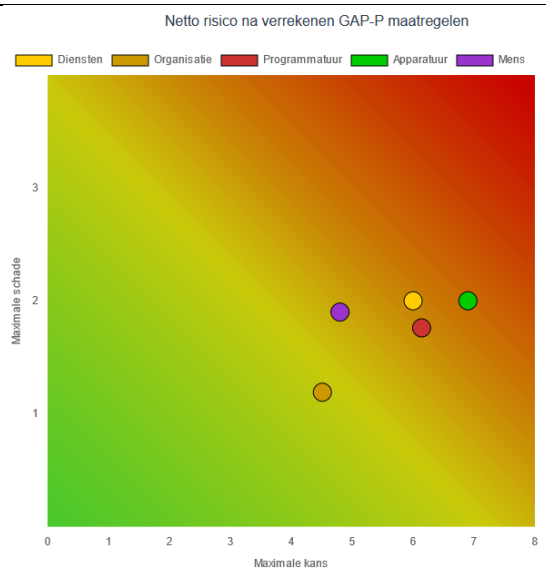
[1] function creep is wat er gebeurt als we technologie en systemen gebruiken op een andere manier dan in de eerste instantie eigenlijk bedoeld is, met name wanneer het nieuwe doel resulteert in een inbreuk op de privacy.

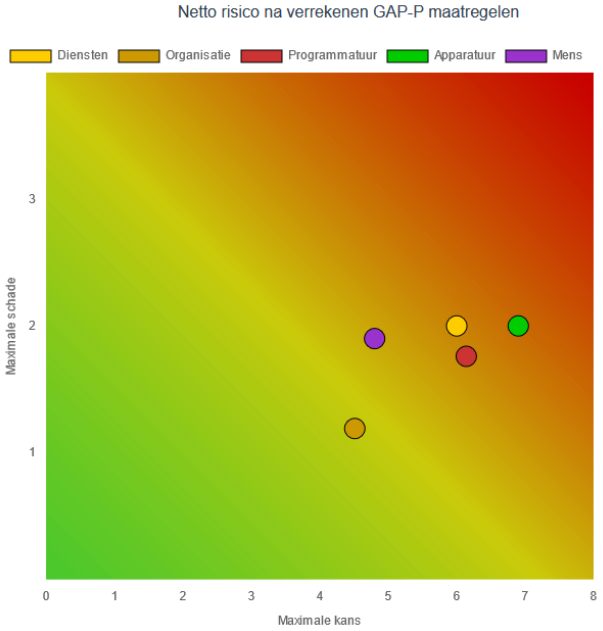
langer dan noodzakelijk worden opgeslagen in een vorm die het mogelijk maakt om betrokkene te identificeren.	
De risicoanalyse bevat een omschrijving van de wijze waarop betrokkene (toereikend) wordt geïnformeerd.	Er wordt open en transparant gecommuniceerd. In de privacyverklaring op de website van de gemeente Helmond is hier voor iedereen nadere informatie over te vinden.
de risicoanalyse bevat een omschrijving van hoe betrokkenen hun rechten uit kunnen oefenen: a. rechten van inzage b. recht op rectificatie en verwijdering c. recht op overdraagbaarheid van gegevens d. recht op bezwaar e. recht op beperking van de verwerking	In de risicoanalyse wordt verwezen naar de standaard procedure voor rechten van betrokkenen van de gemeente. Er wordt helder en duidelijk aangegeven tot wie men zich moet wenden in voorkomend geval. Dit is ook nog eens opgenomen in de privacyverklaring op de website.
de risicoanalyse beschrijft de relatie met verwerkers	Microsoft is de verwerker. De verplichtingen zijn vastgelegd in een overeenkomst en verwerkersovereenkomst.
De risicoanalyse beschrijft de waarborgen omtrent internationale doorgifte	Doorgifte van informatie buiten de EER is niet van toepassing. Gegevensverwerking (hosting) vindt plaats binnen de Europese Unie. Microsoft heeft als land van herkomst de Verenigde Staten, volgens de technische documentatie zijn er voldoende maatregelen getroffen om te voorkomen dat er gegevens worden verstrekt aan de VS. E.e.a. is beschreven in de door Privacy Company (in de persoon van 5.1.2e) uitgevoerde DPIA's/DTIA's. Microsoft heeft op basis hiervan aanvullende maatregelen getroffen en garanties geboden.
de risicoanalyse vermeldt of voorafgaande raadpleging nodig is	Is niet van toepassing. Er is geen sprake van de noodzakelijkheid tot voorafgaande raadpleging bij de AP.

Ad 3 de risico's voor de rechten en vrijheden van betrokkenen

Omschrijving	Toelichting
de risicoanalyse brengt de risico's voldoende in beeld.	De grootste (classificatie "midden") risico's beschikbaarheid en vertrouwelijkheid van gegevens.  In de gesprekken kan (zeer) persoonlijke of gevoelige informatie worden gedeeld. Het is daarom van belang dat de gesprekken zijn beveiligd tegen onbevoegde toegang. Om de gewenste situatie te bereiken moet een session border controller (SBC) ingericht worden. Alle andere componenten zijn beschikbaar als onderdeel van Mitel of als onderdeel van Microsoft365 E5. Deze componenten worden door dit project (her-)ingericht en moeten voldoende zijn beveiligd zodat de gesprekken, beschikbaar zijn, niet worden gecorrumpeerd (integriteit) en vertrouwelijk blijven.
De bedreigingen die kunnen leiden tot onrechtmatige toegang zijn benoemd.	Parallel aan dit project wordt de beveiliging van MS365 in de volle breedte aangepakt waarbij eerst alle mogelijkheden binnen de E3 licentie worden benut en in een later fase alle mogelijkheden van de E5 licentie.

De mogelijke gevolgen voor de rechten en vrijheden van betrokkenen zijn geïdentificeerd. Ze zijn benoemd vanuit het perspectief van betrokkenen en er is daarbij ook gedacht aan de gevolgen die dit heeft op het recht op : • zelfstandigheid (bijvoorbeeld de mogelijkheid om bepaalde handelingen uit te voeren); • vrij blijven van stigmatisering (bijvoorbeeld niet op een bepaalde wijze behandeld worden op basis van bepaalde kenmerken); • gelijkheid (bijvoorbeeld het op de zelfde wijze benaderd worden als andere betrokkenen); • vrij blijven van manipulatie (bijvoorbeeld niet beïnvloed worden op gedrag op basis van een (afwijkend) levenspatroon); • integriteit (verlies van eigenheid, waardigheid en ongeschondenheid, niet jezelf kunnen zijn , je moeten aanpassen aan wat anderen vinden hoe je moet zijn); • ongestoord leven (waarbij het bijvoorbeeld kan gaan om identiteitsfraude of (onaangenaam) afbreken van rust en stilte). • eigenwaarde (bijvoorbeeld geen afbreuk aan persoonlijkheid). • autonomie (bijvoorbeeld geen beperking van de vrijheid om eigen regels te volgen) Vooral van zaken als stigmatisering, ongelijkheid, manipulatie en niet ongestoord kunnen leven kunnen betrokkenen last hebben. • Daarnaast zijn de risico's voor de organisatie benoemd.	Het project vervangt alle telefoontoestellen voor softwarematige oplossingen die beschikbaar komen op laptops, tablets en smartphones het beheer van mobiele devices is daarom van invloed op de beveiliging van de via teams gevoerde gesprekken. Het hybride en plaatsonafhankelijk werken, valt buiten scope van dit project maar brengt wel risico's met zich mee met betrekking tot een inbreuk op de vertrouwelijkheid van de gevoerde gesprekken. Men dient zich bewust te zijn van de mogelijkheid tot meeluisteren. Wanneer een collega met een ander taak meeluistert is er ook sprake van onbevoegde toegang. (denk aan medewerker vergunningen die hoort wat een collega van het sociaal domein bespreekt met een inwoner). *Advies:* - *Om de vertrouwelijkheid en de integriteit van de gespreksgegevens te borgen dient de invoering van maatregelen die volgen uit de risicoanalyse van het telefonieproject moet afgestemd worden op de activiteiten voor de beveiliging van MS365.* - *Standaardiseer naar smartphones van een gemeente, voor iedereen die zonder laptop bereikbaar moet zijn.* - *Neem in de communicatie rondom de invoeren van telefonie via teams ook mee dat vertrouwelijke gesprekken worden gevoerd op een plek waar niet kan worden meegeluisterd. (ook niet door collega's met een andere taak).* *<u>Neem dit op in het op te stellen plan van aanpak aanvullende maatregelen voor implementatie</u>*

De waarschijnlijkheid en ernst zijn ingeschat.	
De bedreigingen die kunnen leiden tot ongewenste wijziging zijn benoemd. De mogelijke gevolgen voor de rechten en vrijheden van betrokkenen zijn geïdentificeerd. Ze zijn benoemd vanuit het perspectief van betrokkenen en er is daarbij ook gedacht aan de bij het vorige punt genoemde gevolgen. Daarnaast zijn de risico's voor de organisatie benoemd	Telefoonnummer kunnen onjuist worden genoteerd/opgeslagen. Zie eerdere opmerkingen en adviezen mbt een relatiebeheersysteem. Daarnaast kan een onvoldoende beveiligd netwerk niet alleen leiden tot een inbreuk in de vertrouwelijkheid maar ook van invloed zijn op de kwaliteit van de gesprekken. Zie het advies bij bedreigingen die kunnen leiden tot onrechtmatige toegang.
De waarschijnlijkheid en ernst zijn ingeschat.	Dit is niet van toepassing.
De bedreigingen die kunnen leiden tot het niet beschikbaar zijn van gegevens zijn benoemd. De mogelijke gevolgen voor de rechten en vrijheden van betrokkenen zijn geïdentificeerd. Ze zijn benoemd vanuit het perspectief van betrokkenen en er is daarbij ook gedacht aan de bij het vorige punt genoemde gevolgen. Daarnaast zijn de risico's voor de organisatie benoemd	In de huidige situatie zijn er veel verschillende manieren van werken met vaste en mobiele telefoons waardoor er minder grip is op de telefonische bereikbaarheid van medewerkers. Door de verandering is er een kans om weer meer uniformiteit te krijgen in het telefonisch verkeer gericht op het verbeteren van de bereikbaarheid en ter voorbereiding op omnichannel dienstverlening. Het project heeft impact vanwege het anders inrichten en beheren van de huidige telefonieoplossing in Mitel zodat deze geschikt is om gesprekken door te schakelen naar Teams. Een deel van de inrichting in Mitel zal verplaatsen naar Microsoft Phonesystem dat in combinatie met Teams het individuele telefoonverkeer zal regelen. Dit is een uitbreiding voor het beheer van MS 365 en specifiek de applicaties MS Phone system en Teams. De servicedesk moet geïnstrueerd worden hoe calls over telefonie afgehandeld moeten worden. *Advies* - *Maak afspraken over de telefonische bereikbaarheid met medewerkers* - *Instrueer medewerkers van contactcenters over het doorschakelen van gesprekken*

	- *Instrueer de servicedesk over hoe calls over telefonie afgehandeld moeten worden.* *<u>Neem dit op in het op te stellen plan van aanpak aanvullende maatregelen voor implementatie</u>*
De waarschijnlijkheid en ernst zijn ingeschat.	Ja, deze zijn ingeschat. 

Ad 4 de maatregelen worden benoemd

Voldoet	Omschrijving	Toelichting
Geheel	de beoogde maatregelen om de risico's aan te pakken worden bepaald en zijn voldoende.	Zie de geadviseerde maatregelen en De met het projectteam besproken en in hoofdstuk 8 van de DPIA vermeldde maatregelen.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	2, 9

From: "5.1.2e " <5.1.2e @helmond.nl>
Sent: 10/27/2024 1:05:23 PM
To: "5.1.2e " <5.1.2e 5.1.2e @helmond.nl>, "5.1.2e " <5.1.2e @helmond.nl>
Cc:
Subject: Nieuwe versie brief RHCe beperken openbaarheid

Hallo 5.1.2e,

Het al dan niet ondertekenen van de door een aantal andere gemeenten opgestelde brief, is niet de kern van de zaak en van het door mij gegeven advies. De kern is de te volgen werkwijze.
Om misverstanden te voorkomen hierbij mijn advies met betrekking tot de werkwijze rondom openbaarheid.

Mijn advies
Mijn advies is:
Volg de door de RHCE beschreven werkwijze, (in ieder geval totdat er een gezamenlijke vastgestelde andere aanpak is).

Voor zover dit advies niet wordt opgevolgd:
Volg de door de RHCE beschreven werkwijze, totdat de gemeente Helmond

- een aangepaste (eigen)werkwijze heeft beschreven en
- op deze werkwijze een risico analyse is uitgevoerd en
- voldoende maatregelen zijn getroffen om de risico's voor betrokkenen te mitigeren tot een acceptabel niveau. Betrek daarbij ook het risico dat er (vanwege het ontbreken van een eenduidig standpunt) misverstanden kunnen ontstaan tussen RHCE en de gemeente over de werkwijze,

Voor het niet opvolgen van dit advies is minimaal vereist dat gemotiveerd wordt vastgelegd waarom dit advies niet wordt opgevolgd én dat is aangegeven op welke termijn wel een risico analyse wordt uitgevoerd.

Overigens adviseer ik om sowieso een risico analyse in te plannen voor het overdragen van archiefstukken.

Toelichting

1. In de brief van RHCE wordt een werkwijze beschreven.
2. De brief die is opgesteld is door een aantal deelnemende gemeenten geeft aan dat zij de door de RHCE beschreven werkwijze niet zullen volgen.

Mijn advies:
Op verzoek van 5.1.2e heb ik beide brieven beoordeeld.

1. Naar mijn oordeel borgt de door het RHCE (1) beschreven werkwijze een goede bescherming van de persoonsgegevens bij openbaarmaking van het archief. Daarmee geef ik geen oordeel over de vraag of dit (archieftechnisch) een juiste en ook een werkbare werkwijze is.
2. Naar mijn oordeel brengt het niet volgen van de door het RHCE beschreven werkwijze risico's met zich mee voor de bescherming van de persoonsgegevens van onze inwoners. De reden hiervoor is dat ik het niet hebben van eenduidige, afspraken en het volgen van een eigen werkwijze een risico vindt voor de bescherming van de persoonsgegevens in de archiefstukken. Het risico dat er onrechtmatig persoonsgegevens worden verwerkt is te groot.

Ik heb daarom geadviseerd om de door het RHCE beschreven werkwijze op te volgen of opnieuw in gesprek te gaan om te komen tot een werkwijze waar overeenstemming over is.

Groeten 5.1.2e

Zie ook DJuma zaak 52251175
Ik heb de concept brief van de collega gemeenten nog niet toegevoegd aan deze zaak (vanwege de vertrouwelijkheid). Aan jullie het vriendelijke verzoek om dit alsnog te doen zodra die is verstuurd.

Met vriendelijke groet,

Gemeente Helmond

5.1.2e
Functionaris voor de gegevensbescherming

Afdeling Concern control
Postbus 950, 5700 AZ, Helmond
Telefoonnummer 5.1.2e

#Makers van de toekomst

Kom bij ons werken! Kijk eens op www.helmond.nl/werkenbij.

Van: 5.1.2e <5.1.2e 5.1.2e @helmond.nl>
Verzonden: dinsdag 15 oktober 2024 11:25
Aan: 5.1.2e <5.1.2e @helmond.nl>; 5.1.2e <5.1.2e @helmond.nl>
Onderwerp: RE: Nieuwe versie brief RHCe beperken openbaarheid

5.1.2e, 5.1.2e,

Wat betreft de BBO sluit ik me aan bij de andere gemeenten. Vandaar dat ik het verzoek heb gedaan onze naam eronder te zetten.
Voor wat betreft ‘goede voet staan met RHCE’; daar maak ik me totaal niet druk om. Ik heb regelmatig contact met de inspecteurs van het RHCE, en dat contact is altijd goed, gemoedelijk en daarnaast inhoudelijk ook nuttig en kundig.

Als er dossiers worden overgedragen naar het RHCE houden wij vingers aan de pols wat betreft persoonsgegevens. Dan lijkt dit me voor nu voldoende

Gemeente Helmond

5.1.2e

Senior adviseur informatievoorziening
Afd. IVA / Team Informatiediensten

M: 5.1.2e

😉

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens geanonimiseerd op grond van:

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

Afdeling/Programma: Huis voor de Stad

Onderwerp: Cameraplan.

Datum: 31 januari 2024

Aanleiding

De gemeente wil videocameratoezicht (VCT) inzetten om haar bedrijfsmiddelen te beschermen. Daarnaast moet VCT de veiligheid van bezoekers en personeel vergroten. Tot slot wil de gemeente met de inzet van VCT criminaliteit voorkomen of de impact van strafbare feiten beperken.

Tegelijkertijd is de inzet van VCT een grote inbreuk op de privacy van bezoekers en werknemers. Om deze inbreuk te beperken heeft de de directie van de gemeente Helmond het “Camerabeleid gemeentelijke panden” (verder: camerabeleid) vastgesteld. De FG heeft op 2 mei 2022 geadviseerd over dit camerabeleid. Zij heeft geconcludeerd dat het camerabeleid een goed kader bevat voor de invoering van VCT in de gemeentelijke panden. Zij heeft daarnaast adviezen gedaan voor een verdere (concrete) inrichting van het VCT.

Voor het gemeentelijk pand “Huis voor de Stad”, heeft de gemeente het gebruik van VCT nader geconcretiseerd. In het document “Overzicht camera’s gemeente Helmond (Huis voor de stad)” (verder: overzicht) wordt per camera een nadere onderbouwing gegeven. Daarnaast heeft ze een implementatiehandreiking opgesteld met een overzicht van de beveiligingsmaatregelen. Beide documenten zijn een bijlage van het camerabeleid. Ze zijn ter advisering voorgelegd aan FG en CISO.

De FG en CISO hebben beoordeeld of beide documenten voldoen aan het (nog niet officieel vastgestelde) gemeentelijke camerabeleid. Daarnaast hebben zij beoordeeld of de gegeven adviezen zijn opgevolgd.

Conclusie

Zowel het overzicht als de implementatiehandreiking voldoen aan het gemeentelijke beleid en de gegeven adviezen zijn opgevolgd.

Het overzicht

De gemaakte keuzes rondom het open karakter en de dienstverleningsvisie maken de gemeente kwetsbaarder voor incidenten. Dit heeft ook tot gevolg dat er een meer ingrijpend VCT nodig is om de bedrijfsmiddelen te beschermen. Binnen de gemaakte keuzes is de wijze waarop VCT is ingericht, binnen het Huis voor de stad, rechtmatig en voldoet het aan het gemeentelijke camerabeleid. Bij de toelichting leest u waarom we tot deze conclusie komen.

Dat neemt niet weg dat de gemeente haar bedrijfsmiddelen ook op andere manieren adequaat had kunnen beschermen. Men had kunnen kiezen voor middelen die minder ingrijpen in de persoonlijke levenssfeer van inwoners en medewerkers. De gemeente heeft echter het open karakter van het Huis voor de Stad zwaarder laten wegen dan de privacy van inwoners en medewerkers.

De beheersmaatregelen

De gemeente treft, conform beleid en advies, beheersmaatregelen om de impact van het VCT te verminderen. De implementatiehandreiking geeft aan op welke wijze deze beheersmaatregelen worden geïmplementeerd. Niet alle in de implementatiehandreiking genoemde documenten zijn al opgesteld en beoordeeld. Zij worden te zijner tijd ter beoordeling voorgelegd aan FG en CISO.

Advies

- Stel het camerabeleid vast
- Implementeer de beheersmaatregelen conform de implementatiehandreiking
- Leg de in de implementatiehandreiking opgenomen, nog op te stellen documenten ter advisering voor aan FG en CISO.

Toelichting

Videocamera toezicht kan helpen om eigendommen, bezoekers en personeel te beschermen. Maar de inbreuk op de privacy van bezoekers en werknemers is groot. De beelden leggen immers ook de aanwezigheid en het gedrag van de personen in betrokken ruimten vast.

Daarom moet aan de volgende voorwaarden worden voldaan:

1. Er moet sprake zijn van een gerechtvaardigd belang.
2. Het gebruik van videocamera's moet noodzakelijk zijn en een onderdeel van een breder pakket van maatregelen.
3. Er moet een privacytoets worden uitgevoerd, oftewel de belangen van degene die worden gefilmd moet worden afgewogen tegen het belang van de gemeente.

Omdat deze voorwaarden gelden voor elke camera afzonderlijk heeft de gemeente in het overzicht, per camera geconcretiseerd of er wordt voldaan aan de voorwaarden.

1. Gerechtvaardigd belang

Er is sprake van een gerechtvaardigd belang. In het overzicht worden per camera het belang en de verwerkingsdoeleinden beschreven. Dat er sprake is van een reëel gerechtvaardigd belang is in het camerabeleid onderbouwd.
In de implementatiehandreiking is opgenomen dat een incidentenregistratie wordt bijgehouden. Bovendien is opgenomen dat het reële gerechtvaardigde belang elk half jaar wordt geëvalueerd. Met behulp van een incidentenregistratie kan namelijk het reële risico per camera (of een set van camera's) worden vastgesteld. Daarmee kan het reële gerechtvaardigde belang verder worden onderbouwd. Overigens kan uit de incidentenregistratie ook blijken dat er geen sprake meer is van een reëel gerechtvaardigd belang, omdat er geen of slechts weinig incidenten hebben plaatsgevonden.

2. De Noodzaak van de camera's.

In het beleid is vastgelegd dat VCT enkel wordt ingezet als onderdeel van een pakket maatregelen en indien vastgesteld is dat overige maatregelen het gerechtvaardigd belang onvoldoende behartigen.

De aanvullende maatregelen zijn beschreven in het overzicht. Hiermee is onderbouwd dat VCT inderdaad een onderdeel is van een pakket maatregelen. Het gerechtvaardigde belang had echter ook voldoende behartigd kunnen worden op een manier die minder ingrijpt in de persoonlijke levenssfeer van bezoekers en medewerkers, als de organisatie andere keuzes had gemaakt. Hieronder wordt beschreven waarom de FG dit vindt.

2.1. Algemene beoordeling van de noodzaak.

De gemeente Helmond heeft namelijk gekozen voor een open inrichting van het Huis voor de Stad. Het, conform advies van de CISO in 2020, plaatsen van middelen die de toegang beperken (zoals een stackdoor, hoge toegangspoorten of afgesloten deuren) passen hier, naar mening van de organisatie, niet bij. Daarnaast is er gekozen om de traditionele wijze van dienstverlening achter een (af te schermen) balie plaats te laten maken voor een dynamischer concept met een persoonlijke benadering. Deze wijze van benadering is gebaseerd op de dienstverleningsvisie.

Dit alles moet er toe bijdragen dat bezoekers zich welkom moeten voelen. Deze keuzes betekenen echter ook dat de organisatie kwetsbaarder is voor agressie en ook voor beschadiging en diefstal van bedrijfsmiddelen. De kans op een incident is door de gemaakte keuzes groter, waardoor de behoefte bestaat om het pand te beveiligen met 5.1.2h De organisatie kiest er daarmee voor om[1]:

- De focus niet te leggen op voorkomen van incidenten, maar op repressie en controle. Met camerabeelden kan namelijk achteraf worden vastgesteld wat er is gebeurd, zodat er opgetreden kan worden. Dit terwijl uit onderzoek blijkt dat de preventieve werking van camera's gering is[2].
- Minder belang toe te kennen aan de inbreuk op de persoonlijke levenssfeer van bezoekers en medewerkers, dan aan het gewenste open karakter.

2.2. Beoordeling van de noodzaak per categorie camera.

Hierna volgt een beoordeling per groep camera's. Deze groepen zijn gebaseerd op de in paragraaf 2 van het beleid genoemde categorieën.

5.1.2h

2.1.1. Camera's gevestigd aan de buitenzijde van het gebouw.

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
5.1.2h
5.1.2h
5.1.2h
5.1.2h
5.1.2h

[2] Citaat van hoogleraar Digitale surveillance Marc Schuilenburg, Het Erasmusmagazine d.d. 25 mei 2023 Rotterdamse aanslagen: Waarom nóg meer camera's ondermijnend werken - Erasmus Magazine. Zie ook: Professor Criminologie Jelle Janssens (UGent): "de effectiviteit van camerabewaking is nog niet eenduidig aangetoond in wetenschappelijk onderzoek". In Smart citiy en camerabeleid in de stad Genk: naar een doordachte en gedragen visie

5.1.2h

2.2.2. **Camera’s gevestigd in de publieke hal**

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

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

5.1.2h

5.1.2h

5.1.2h

5.1.2h

5.1.2h

5.1.2h

5.1.2h

5.1.2h

2.2.3. **Camera's gevestigd in de publieke zone gericht op zone-overgangen**

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

5.1.2h

5.1.2h

5.1.2h

5.1.2h

5.1.2h

5.1.2h

3. De Privacy toets

In het overzicht heeft de gemeente Helmond per camera de belangen van degenen die (kunnen) worden gefilmd afgewogen tegen de belangen van de gemeente. Daarbij heeft de gemeente aangegeven op welke wijze de impact voor betrokkenen wordt beperkt. Daarnaast wordt in de implementatiehandreiking, in algemene zin aangegeven op welke wijze uitvoering wordt gegeven aan deze maatregelen. Daarbij is ook het gegeven advies opgevolgd.

Om opzet en bestaan te borgen, is het noodzakelijk dat het cameratoezicht wordt geïmplementeerd conform de implementatiehandreiking. De implementatiehandreiking bevat nog een aantal uit te werken stukken. Daarover is afgesproken dat ze worden voorgelegd aan CISO en FG.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub h	De beveiliging van personen en bedrijven en het voorkomen van sabotage	3, 4, 5, 6

Afdeling/Programma:	Stedelijk beleid
Onderwerp:	Samenwerkovereenkomst tbv Stichting Land van Peel
Zaak:	52473921
Datum:	7 april 2025

Aanleiding

Aan college het college wordt gevraagd om in te stemmen met de samenwerkingsovereenkomst gemeenten Peelregio ten behoeve van de ondersteuning “Stichting Land van de Peel”. Het advies heeft betrekking op dit collegevoorstel.

Conclusie

Privacy en informatiebeveiliging spelen niet bij dit collegevoorstel.

Bij het kopje privacy kan de volgende tekst worden opgenomen:

De afspraken hebben geen betrekking op het delen van (bedrijfs)informatie noch persoonsgegevens met de Stichting. Het is ook niet de bedoeling om deze gegevens te delen met de stichting. Privacy en informatiebeveiliging spelen daarom niet. Zie voor het volledige advies document….

Toelichting

De gemeenten Asten, Deurne, Gemert-Bakel, Helmond, Laarbeek en Someren (hierna: Peelgemeenten) zijn in januari 2021 gestart met een gezamenlijke marketing onder de naam ‘Land van de Peel’. Berenschot heeft, desgevraagd, geadviseerd om hiervoor een zelfstandige stichting op te richten. De stichting is afhankelijk van publieke financiering. Ten behoeve van deze financiële ondersteuning wordt een samenwerkingsovereenkomst afgesloten. De samenwerkingsovereenkomst heeft geen betrekking op het delen van bedrijfsinformatie of persoonsgegevens (van de gemeente Helmond) met de Stichting.

De Stichting is daarnaast zelf verantwoordelijk voor een beveiliging van haar informatie en het naleven van de privacyregels. Het collegevoorstel heeft daarom geen impact op de beveiliging van onze informatie of de privacy van onze inwoners en medewerkers. Voor zover er wel behoefte ontstaat om bedrijfsinformatie of persoonsgegevens te delen dan is eerst een gedegen onderzoek nodig naar:

- Doel
- Grondslag
- Subsidiariteit en proportionaliteit
- Informatiebeveiligings- en privacyisco’s
- Mitigerende maatregelen.

7 april 2025

5.1.2e (Chief information security officer)
5.1.2e (Functionaris voor de gegevensbescherming)

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens geanonimiseerd op grond van:

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

Advies van de FG

Van: 5.1.2e
Verzonden: woensdag 3 januari 2024 09:49
Aan: 5.1.2e <5.1.2e @helmond.nl>; 5.1.2e <5.1.2e @helmond.nl>
CC: 5.1.2e <5.1.2e @helmond.nl>
Onderwerp: RE: Zorg- en Veiligheidshuis BZO

Dag 5.1.2e,

Samengevat:
Het is belangrijk dat andere afdelingen worden betrokken en dat er een risico analyse wordt uitgevoerd.
Dit is nodig ongeacht of er wordt meegewerkt aan de detacheringsovereenkomst of niet.

Toelichting
Gelet op de mail stel je me eigenlijk de *volgende vraag:*
Klopt het dat we in de regio blijven voldoen aan de wettelijke vereisten als we meewerken aan een detacheringsovereenkomst? Blijft de uitwisseling van gegevens daardoor mogelijk.
Hier kan ik geen bevestigend antwoord op geven.

Ik begrijp het volgende uit de mail:

Er werken nu medewerkers van de gemeente Helmond bij het Zorg en Veiligheidshuis. Het is de bedoeling dat zij in dienst komen bij het Zorg en Veiligheidshuis (ZVHBZO). Met de detacheringsovereenkomst is een juridische constructie bedacht. Deze constructie moet ervoor zorgen dat deze medewerkers weliswaar in dienst zijn van het ZVH BZO maar dat zij toch namens de gemeente Helmond werken. Daarmee zou er niets veranderen aan de verantwoordelijkheid die de gemeente Helmond heeft met betrekking tot de gegevens die worden verwerkt binnen het ZVHBZO.

Of dit juridisch klopt kan ik niet beoordelen.

Juridische constructies (alleen) zijn echter *nooit een oplossing* van een probleem. Er ontstaan door dergelijke oplossingen nieuwe problemen en/of oude problemen blijven voortbestaan.

Welke problemen dat zijn zal een risico analyse (DPIA) duidelijk maken. De afdeling(en) waar de desbetreffende medewerkers nu werken zijn verantwoordelijk voor het uitvoeren van een dergelijke risico analyse.

Het is dus in ieder geval nodig om een risico analyse uit te voeren op de onder onze verantwoordelijkheid (of zij nu bij ons in dienst zijn of bij ons gedetacheerd zijn).

Pas als alle risico's in beeld zijn en passende maatregelen zijn getroffen kan ik vaststellen dat er wordt voldaan aan de wettelijke vereisten en dat uitwisseling van gegevens rechtmatig is. Het ZVH BZO kan dat aantonen met een PDCA cyclus.

Achtergrond en geschiedenis:

Eind 2022 is een DPIA uitgevoerd op de verwerking van gegevens in het ZVBHZO

Daarin lees ik:
Het zorg en Veiligheidshuis heeft zelf geen grondslag om gegevens te verwerken. De deelnemende partners zijn gezamenlijk verantwoordelijk die zij verwerken op locatie of in de systemen van het ZVHBZO.
Juridisch gezien worden er binnen de omgeving van ZVHBZO geen gegevens verwerkt, dit geschiedt direct tussen betrokkenen in een specifieke casus.

De gezamenlijke FG's hebben in hun advies van begin 2023 al hun zorgen geuit over deze constructie.
In ons advies lees ik onder andere:

- De invulling van de gezamenlijke verwerkingsverantwoordelijkheid in relatie tot de individuele verwerkingsverantwoordelijkheden heeft als risico dat partijen naar elkaar verwijzen voor de invulling van de verwerkingsverantwoordelijkheden, met als risico dat de rechten en vrijheden van betrokkenen tussen wal en schip terecht komen. We adviseren daarom:
  - om gegevensdeling, het verwerken van persoonsgegevens en de gemaakte afspraken ook periodiek onder de aandacht brengen van de partners;
  - om de partner te ondersteunen bij het voorkomen van onrechtmatige gegevensdeling door de procesregisseur specifiek te laten vragen naar de rechtsgrond en partners aan te spreken op hergebruik van de verkregen informatie (function creep);
  - om de afweging om betrokkenen niet te informeren niet bij de partner te laten, maar altijd onderdeel te laten zijn van de casusbespreking.
- Daarnaast adviseren wij elke afzonderlijke partner, om een DPIA uit te voeren op de onder hun verantwoordelijkheid verwerkte persoonsgegevens in ZVH BZO.
- In je mail van 17 mei 2022 geef je aan dat er continue gewerkt wordt aan het verantwoord omgaan met persoonsgegevens. Advies daarbij is dit vast te leggen in een Plan, Do, Check en Act (PDCA-cyclus), zodat dit ook aangetoond kan worden. Wellicht ten overvloede: een DPIA moet actueel gehouden worden. Dat wil zeggen dat een DPIA minimaal eens per drie jaar zou moeten worden herhaald. Indien de verwerking tussentijds wijzigt, kan dit aanleiding zijn om de DPIA eerder te herhalen.

Met vriendelijke groet,

Gemeente Helmond

5.1.2e
Functionaris voor de gegevensbescherming

Afdeling IVA
Postbus 950, 5700 AZ, Helmond
Telefoonnummer 5.1.2e

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens geanonimiseerd op grond van:

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

Afdeling/Programma: Altijd Verbonden

Onderwerp: Digitaal ondertekenen

Datum: 19 juli 2024

Aanleiding

Achtergrond
Binnen de gemeente Helmond zijn we voortdurend bezig met het digitaliseren van onze werkprocessen. De communicatie met en richting de inwoners en organisaties gaat steeds vaker digitaal. Nu de Wet modernisering elektronisch bestuurlijk verkeer (Wmebv) in werking is getreden krijgt de burger het recht op digitaal zakendoen met de overheid. Hier draagt het elektronisch ondertekenen van documenten aan bij.

Daarnaast vormt de Europese eIDAS-verordening ook een reden om over te gaan naar de digitale ondertekening. De eIDAS-verordening staat voor 'Electronic Identities And Trust Services'. Met deze verordening hebben de Europese lidstaten afspraken gemaakt om dezelfde begrippen, betrouwbaarheidsniveaus en onderlinge digitale infrastructuur te gebruiken. Een elektronische ondertekening die voldoet aan de eIDAS-standaarden, volgt bepaalde technische- en veiligheidsmaatregelen.

Voor verreweg de meeste documentsoorten binnen de gemeente is er geen wettelijke verplichting voor ondertekening. Het ondertekenen van documenten is vaak een gewoonte. Het is ook een vorm van risicomanagement: een ondertekening heeft een juridische waarde en is als het goed is te herleiden naar de persoon die beslissingsbevoegd is om een besluit te nemen. De beslissingsbevoegdheid is geregeld in de Mandaatregeling van de gemeente Helmond.

Doel
De gemeente Helmond wil daar waar mogelijke de 'natte handtekening' vervangen door een elektronische handtekening en daarvoor een applicatie inzetten die dat eenvoudig ondersteunt. Naast de al ingezette digitalisering van de communicatie (post) wordt met het elektronisch ondertekenen een volgende stap gezet in de verdergaande digitalisering.

Resultaat
Met elektronisch ondertekenen worden doorlooptijden aanzienlijk korter. Het zorgt voor een verhoging van de efficiëntie en een verbetering van de bedrijfsvoering. Printen en scannen behoren tot het verleden, waardoor enorme hoeveelheden papier worden bespaard. De klant of leverancier hoeft niet meer te wachten op een postbode. Ook de interne ondertekening van stukken verloopt sneller. Dit is belangrijk, omdat de gemeente veel werkprocessen heeft die, vanwege een wettelijke grondslag, een beperkte afhandelingstermijn hebben. Tot slot draagt het sneller ontvangen van te ondertekenen stukken bij aan een goede samenwerking.

De verwerving, de implementatie, het eigenaarschap en het beheer en onderhoud van een organisatiebreed in te zetten elektronische handtekeningtool vormen de afgeleide doelstelling voor dit project.

In scope
In scope van deze risicoanalyse zijn:

- De gemeentelijke processen die een wettelijk verplicht ondertekenmoment bevatten, waarbij de 'natte handtekening' vervangen wordt (daar waar mogelijk) door de digitale handtekening.
- De processtap van ondertekenen middels de daarvoor aanbestede applicatie van ValidSign.
- De gemeentelijke processen die geen wettelijk verplicht ondertekenmoment bevatten maar waarbij ondertekening wél gewenst is en de 'natte handtekening' vervangen wordt (daar waar mogelijk) door de digitale handtekening.
- De opgestelde richtlijn 'elektronisch ondertekenen gemeente Helmond'.
- Het proces dat door ValidSign wordt verricht naar aanleiding van het aanbieden en ondertekenen van documenten via ValidSign.

Betrokken partijen
Verwerkingsverantwoordelijke: het College van B&W van de gemeente Helmond
Verwerker: ValidSign
Ontvangers: medewerkers van de gemeente Helmond en externen (inwoners, leveranciers, etc.)

Gebruikte stukken
De FG en de CISO hebben het advies gebaseerd op de volgende documenten uit zaaknummer 52064492:

- 52119642 → Procesbeschrijving ValidSign Procesbeschrijving ValidSign.docx
- 52119612 → Advies van FG en CISO e-mail beleid d.d. 13 februari 2024 Advies van FG en CISO email beleid .pdf
- 52113735 → Reactie ValidSign op uitvraag documentatie m.b.t. informatiebeveiliging en privacy ValidSign - Gemeente Helmond.pdf
- 52113705 → Voorbeeld – via ValidSign ondertekend document (PV Kempengemeenten) Documents for inschrijfformulier PV Kempengemeenten.zip
- 52113689 → Voorbeeld – Bewijsdocument na ondertekening via ValidSign Bewijsdocument.pdf
- 52113638 → Bevestiging ValidSign dataverwerking enkel binnen de EER Verwerking data ValidSign.pdf
- 52113606 → Reactie ValidSign m.b.t. vraag over persoonsgegevens van betrokkenen Re Vraag m.b.t. ValidSign.pdf
- 52064758 → Richtlijn 'elektronisch ondertekenen gemeente Helmond' Richtlijn elektronisch ondertekenen Helmond.docx
- 52064756 → ISO 9001 certificaat ValidSign B.V. DigiTrust Certificaat ISO 9001 ValidSign B.V.pdf
- 52064755 → NEN 7510 certificaat ValidSign B.V. DigiTrust Certificaat NEN 7510 ValidSign B.V.pdf
- 52064754 → ISO 27001 certificaat ValidSign B.V. DigiTrust UK Certificate ISO 27001 ValidSign B.V.pdf
- 52064753 → Verklaring van Toepasselijkheid ValidSign ISO 27001 V1.5 28-2-2022 Verklaring van Toepasselijkheid ValidSign ISO 27001 V1.5 28-2-2022.pdf
- 52064745 → Projectplan Digitaal Ondertekenen Projectplan Digitaal Ondertekenen.docx
- 52064751 → Programma van Eisen_elektronisch ondertekenen concept
- 52133136 → RE_Casuïstiek ValidSign; Mailwisseling van 6 juni tot 13 juni 2024 betreffende inhoudelijke en technische vragen over de werking van ValidSign

Conclusie

Het risico voor de schending van de privacy van betrokkenen is gering. Met de oplossing van ValidSign worden persoonsgegevens verwerkt:

1. De voor- en achternaam, het e-mailadres, het mobiele telefoonnummer (indien gebruikt) en het IP-adres van de ondertekenaar (zie 'Reactie ValidSign m.b.t. vraag over persoonsgegevens van betrokkenen). Deze informatie wordt opgeslagen in een audit-trail/bewijsdocument en in een certificaat dat onderdeel uitmaakt van de ondertekende brief.
2. Een kopie van de brief die digitaal ondertekend moet worden, met alle in deze brief aanwezige persoonsgegevens. Deze brief wordt encrypted opgeslagen en is niet toegankelijk voor medewerkers van ValidSign.
3. Een kopie van de ondertekende brief. Deze brief wordt encrypted opgeslagen en is niet toegankelijk voor medewerkers van ValidSign.

Op basis van de hiervoor genoemde documenten 52064751, 52133136, 52064754, 52064753, 52113735 en 52119642 zijn er toereikende technische en organisatorische maatregelen getroffen om de persoonsgegevens te beschermen tegen onrechtmatige verwerking en inbreuken op de beschikbaarheid, integriteit en vertrouwelijkheid. Zo zal voor de toegang van het systeem voor medewerkers van gemeente Helmond gebruik gemaakt gaan worden van Single Sign On (SSO) en voor externe ondertekenaars van 2 factor authenticatie. Zowel tijdens transport als opslag worden gegevens versleuteld.

Naast de daadwerkelijke digitale ondertekening met certificaat stuurt ValidSign een audit-trail/ bewijsdocument mee zodra een document ondertekend wordt via de software (zie 'Voorbeeld – Bewijsdocument na ondertekening via ValidSign). Hiermee kan worden aangetoond dat het document ondertekend is door de juiste persoon. Welke medewerkers van de gemeente Helmond bevoegd zijn om te ondertekenen is vastgelegd in het mandaatregister.

Advies

Onderstaande geadviseerde maatregelen zijn op basis van de uitgevoerde risicoanalyse en de toets daarvan (zie bijlage 1) overgenomen en daar waar nodig aangevuld door FG en CISO:

1. Werk de processtappen betreffende het digitaal aanbieden en ondertekenen van documenten waarbij de applicatie van ValidSign wordt ingezet uit (in Bizagi) en publiceer deze op de Helmondse Processenpagina.
2. Voeg ValidSign als het gebruikte systeem toe aan alle verwerkingen in het register van verwerkingen waarbij digitaal ondertekend wordt.
3. Stel een instructie op voor het gebruik van de applicatie van ValidSign bij het digitaal aanbieden en ondertekenen van documenten.
4. Neem in deze instructie ook op:
    a. Hoe er wordt omgegaan met de audit-trail/het bewijsdocument;
    b. Hoe er uitvoering kan worden gegeven aan het handmatig verwijderen van documenten in de ValidSign omgeving;
    c. Op welke wijze er wordt geborgd dat documenten te lang de status "in Progress" behouden.
5. Stel een algemeen beleid op voor (veilige) e-mail (zie eerder gegeven advies door FG & CISO n.a.v. het project 'Veilig Mailen' d.d. 13 februari 2024) waarin vermeld wordt hoe de gemeente Helmond omgaat met formele besluiten per e-mail (zie risicoanalyse 'Projectplan Digitaal Ondertekenen').
6. Communiceer:

   a. De richtlijn ‘elektronisch ondertekenen gemeente Helmond’ binnen de organisatie bij de implementatie en uitrol van de applicatie van ValidSign;
   b. Alle opgestelde instructies.
7. Verifieer de ondertekenbevoegdheden vanuit de mandaatregeling n.a.v. de nieuwe organisatie-indeling die sinds 1-7-2024 inwerking is getreden.
8. Informeer de organisatie goed en breed over mandaten en ondertekenbevoegdheden met extra aandacht voor de nieuwe organisatie-indeling die sinds 1-7-2024 inwerking is getreden (zie risicoanalyse ‘Projectplan Digitaal Ondertekenen’).
9. Geef uitleg (d.m.v. training) op verschillende niveaus in de organisatie over het gebruik van de applicatie van ValidSign én aangesloten systemen (Djuma, RIS/BIS) bij de implementatie en uitrol van de applicatie van ValidSign, zodat geborgd kan worden dat de juiste stukken, door bevoegde personen op de gewenste en afgesproken manier digitaal worden ondertekend en verspreid naar de beoogd ontvangers (zie risicoanalyse ‘Projectplan Digitaal Ondertekenen’).
10. Sluit een verwerkersovereenkomst af met ValidSign. Gebruik hiervoor de standaardovereenkomst van de IBD.

De FG en CISO adviseren daarbij nog om:

- Alle nog te implementeren maatregelen die in bovenstaande adviezen worden genoemd over te nemen in een plan van aanpak, dit plan van aanpak toe te voegen aan de projectadministratie en implementatie hiervan te bewaken
- De risicoanalyse te herhalen over drie jaar, of bij wijziging van het proces of de gebruikte systemen.

Bijlagen

1 Toets van de risico analyse

Een risico analyse heeft betrekking op informatieveiligheid en privacy. Voor privacy geldt dat de AVG een aantal vereisten stelt aan de uit te voeren risico analyse: Dit zijn de volgende vereisten:

1. Een systematische beschrijving van de beoogde verwerking en de doeleinden;
2. Een beoordeling van de noodzaak en de evenredigheid;
3. Een beoordeling van de risico's voor de rechten en vrijheden van betrokkenen:
4. Een overzicht van beoogde maatregelen om deze risico's aan te pakken.

Ad 1 een systematische beschrijving

Voldoet	Omschrijving	Toelichting
Voldoet	De risico analyse vermeldt: de persoonsgegevens die worden verwerkt	Ja, het gaat hierbij om de volgende gegevens: - Voor- en achternaam - E-mailadres - Mobiele telefoonnummer (indien gebruikt) - IP-adres Zie: Reactie ValidSign m.b.t. vraag over persoonsgegevens van betrokkenen Re Vraag m.b.t. ValidSign.pdf en zaaknummer 52113606. Daarnaast worden te ondertekenen brieven in de omgeving van ValidSign opgeslagen. Dit betekent dat ook alle in deze brieven vermelde persoonsgegevens worden verwerkt. Behalve de adressering bevatten brieven (soms) ook inhoudelijke informatie over betrokkenen. Dit kunnen ook bijzondere of gevoelige persoonsgegevens zijn. Als maatregel hiervoor wordt versleuteling toegepast waardoor medewerkers van ValidSign geen inzage hebben in de documenten.
Voldoet	De risico analyse vermeldt: de ontvangers van deze persoonsgegevens	Ja, dat zijn de volgende partijen: - Medewerkers van de gemeente Helmond - Externe (inwoners, leveranciers, etc.) Zie: Projectplan Digitaal Ondertekenen Projectplan Digitaal Ondertekenen.docx en zaaknummer 52064745.
Voldoet	De risico analyse vermeldt: de periode gedurende welke de persoonsgegevens worden bewaard	Ja, voor de transactie en alle verwante gegevens geldt binnen de ValidSign omgeving een bewaartermijn van 90 dagen. Dat geldt dus voor zowel het getekende document het ongetekende document als de audit trail/het bewijsdocument. Voor een 'in progress' zijnde transactie geldt een bewaartermijn van één jaar. Zodra het document alsnog getekend is, gaat de bewaartermijn van 90 dagen in. Daarnaast heeft de initiatiefnemer de mogelijkheid om documenten handmatig eerder te verwijderen binnen de ValidSign-omgeving. We adviseren om gebruik te maken van deze mogelijkheid en dit op te nemen in een instructie. Zie: Procesbeschrijving ValidSign Procesbeschrijving ValidSign.docx en zaaknummer 52119642.
Voldoet	De risico analyse bevat een functionele beschrijving van de verwerking	Ja, de levenscyclus van de verwerking wordt beschreven in de procesbeschrijving van ValidSign.

		Zie: Procesbeschrijving ValidSign Procesbeschrijving ValidSign.docx en zaaknummer 52119642.
Voldoet	De risico analyse bevat de activa waarop persoonsgegevens steunen (hardware, software, netwerken, mensen, papier of papiertransmissiekanalen)	Ja, dit is beschreven in de procesbeschrijving van ValidSign en wordt daarnaast toegelicht per mail door ValidSign. Het betreft een SAAS-applicatie die gehost wordt door KPN. Naast de hosting voert KPN ook managed services uit op de OS- en middleware laag van de ValidSign applicatie. Zie: Procesbeschrijving ValidSign Procesbeschrijving ValidSign.docx en zaaknummer 52119642. Zie: Reactie ValidSign op uitvraag documentatie m.b.t. informatiebeveiliging en privacy ValidSign - Gemeente Helmond.pdf en zaaknummer 52113735.

Ad 2 De noodzaak en de evenredigheid wordt beoordeeld

Voldoet	Omschrijving	Toelichting
Voldoet	De risico analyse vermeldt de grondslag en de doeleinden van de verwerking	De grondslag voor deze verwerking is Art. 6 lid 1 sub e AVG (taak van algemeen belang), Gemeentewet. Het doel van de verwerking: de mogelijkheid van digitaal ondertekenen van documentendoor gemeente Helmond ondersteunt het recht van de burger op digitaal zakendoen met de overheid. Daarnaast zegt de wet dat een digitale handtekening dezelfde rechtsgeldigheid heeft als een handgeschreven handtekening, indien de methode voor authenticatie die daarbij is gebruikt, voldoende betrouwbaar is. Hierover zijn ook in Europa afspraken gemaakt. Deze zijn vastgelegd in de eIDAS, zie: (https://www.rijksoverheid.nl/onderwerpen/inloggen-europese-economische-ruimte/alles-wat-u-moet-weten-over-eidas)
Voldoet	De risico analyse vermeldt welke gegevens en verwerkingen er noodzakelijk zijn voor het bereiken van dit doel	Ja, zie de eerdergenoemde Procesbeschrijving ValidSign Procesbeschrijving ValidSign.docx en zaaknummer 52119642. Daarnaast geeft ValidSign aan dat zij via de “backoffice” de logging van de transactie kunnen monitoren. De gelogde gegevens heeft ValidSign nodig om op een juiste wijze support te kunnen bieden en medewerkers van de gemeente Helmond optimaal te ondersteunen. ValidSign heeft verder géén inzage in de inhoud van digitaal aangeboden documenten ter ondertekening. Zie: Reactie ValidSign m.b.t. vraag over persoonsgegevens van betrokkenen Re Vraag m.b.t. ValidSign.pdf en zaaknummer 52113606.
Voldoet	De risico analyse vermeldt of er een minder ingrijpende gegevensverwerking mogelijk is	Ten aanzien van de gekozen oplossing voor digitaal ondertekenen is geen minder ingrijpende gegevensverwerking mogelijk die het voor ValidSign mogelijk maakt om op een juiste wijze support te kunnen bieden en medewerkers van de gemeente Helmond optimaal te ondersteunen.
	De risico analyse bevat een omschrijving van de	Ja, ValidSign heeft bevestigd dat zij enkel en alleen inzage hebben in gelogde gegevens die noodzakelijk zijn om op een juiste wijze support

Voldoet	maatregelen die worden getroffen om de verwerking te beperken tot de ter zake dienende noodzakelijke gegevens	te kunnen bieden en medewerkers van de gemeente Helmond optimaal te ondersteunen. Zie: Reactie ValidSign m.b.t. vraag over persoonsgegevens van betrokkenen Re Vraag m.b.t. ValidSign.pdf en zaaknummer 52113606.
Voldoet	De risico analyse bevat een omschrijving van de maatregelen die worden getroffen om te zorgen dat er geen function creep[1] optreedt.	Ja, ValidSign heeft bevestigd dat zij enkel en alleen inzage hebben in de gegevens die noodzakelijk zijn voor hen om op een juiste wijze support te kunnen bieden en medewerkers van de gemeente Helmond optimaal te ondersteunen, enkel ten behoeve van het doel van digitaal ondertekenen. Zie: Reactie ValidSign m.b.t. vraag over persoonsgegevens van betrokkenen Re Vraag m.b.t. ValidSign.pdf en zaaknummer 52113606.
Voldoet	De risico analyse bevat een omschrijving van de maatregelen die worden getroffen om ervoor te zorgen dat gegevens niet langer dan noodzakelijk worden opgeslagen in een vorm die het mogelijk maakt om betrokkene te identificeren.	Ja, in de procesbeschrijving van ValidSign staat beschreven dat de data na 90 dagen automatisch wordt verwijderd door ValidSign. Daarnaast heeft de initiatiefnemer de mogelijkheid om een document handmatig eerder te verwijderen binnen de ValidSign-omgeving. Zie: Procesbeschrijving ValidSign Procesbeschrijving ValidSign.docx en zaaknummer 52119642.
Voldoet	De risico analyse bevat een omschrijving van de wijze waarop betrokkene (toereikend) wordt geïnformeerd.	Ja, dit staat vermeld in de privacyverklaring op de website van ValidSign. Zie: https://www.validsign.eu/nl/privacy/
Voldoet	De risico analyse bevat een omschrijving van hoe betrokkenen hun rechten uit kunnen oefenen: a. rechten van inzage b. recht op rectificatie en verwijdering c. recht op overdraagbaarheid van gegevens d. recht op bezwaar e. recht op beperking van de verwerking	Ja, dit staat vermeld in de privacyverklaring op de website van ValidSign. Zie: https://www.validsign.eu/nl/privacy/
Voldoet	De risico analyse beschrijft de relatie met verwerkers	Ja, ValidSign is in dit geval de verwerker van de gemeente Helmond. Hiervoor wordt nog een verwerkersovereenkomst opgesteld met ValidSign.
Voldoet	De risico analyse beschrijft de waarborgen omtrent internationale doorgifte	Ja, want ValidSign heeft bevestigd dat de data enkel en alleen wordt verwerkt binnen de EER. Zie: Bevestiging ValidSign dataverwerking enkel binnen de EER Verwerking data ValidSign.pdf en zaaknummer 52113638.

[1] function creep is wat er gebeurt als we technologie en systemen gebruiken op een andere manier dan in de eerste instantie eigenlijk bedoeld is, met name wanneer het nieuwe doel resulteert in een inbreuk op de privacy.

Voldoet	De risico analyse vermeldt of voorafgaande raadpleging nodig is	N.v.t. er is geen hoog risico dat niet kan worden gemitigeerd.

Ad 3 de risico's voor de rechten en vrijheden van betrokkenen

Voldoet	Omschrijving	Toelichting
Voldoet	De risico analyse brengt de risico's voldoende in beeld.	Ja, de risico's staan beschreven in het projectplan en dit advies. Zie: Projectplan Digitaal Ondertekenen Projectplan Digitaal Ondertekenen.docx en zaaknummer 52064745.
Voldoet	De bedreigingen die kunnen leiden tot onrechtmatige toegang zijn benoemd. De mogelijke gevolgen voor de rechten en vrijheden van betrokkenen zijn geïdentificeerd. Ze zijn benoemd vanuit het perspectief van betrokkenen en er is daarbij ook gedacht aan de gevolgen die dit heeft op het recht op : • zelfstandigheid (bijvoorbeeld de mogelijkheid om bepaalde handelingen uit te voeren); • vrij blijven van stigmatisering (bijvoorbeeld niet op een bepaalde wijze behandeld worden op basis van bepaalde kenmerken); • gelijkheid (bijvoorbeeld het op de zelfde wijze benaderd worden als andere betrokkenen); • vrij blijven van manipulatie (bijvoorbeeld niet beïnvloed worden op gedrag op basis van een (afwijkend) levenspatroon); • integriteit (verlies van eigenheid, waardigheid en ongeschondenheid, niet jezelf kunnen zijn , je moeten aanpassen aan wat anderen vinden hoe je moet zijn); • ongestoord leven (waarbij het bijvoorbeeld kan gaan om identiteitsfraude of (onaangenaam) afbreken van rust en stilte). • eigenwaarde (bijvoorbeeld geen afbreuk aan persoonlijkheid).	De belangrijkste risico's zijn benoemd in het projectplan en dit advies. Voor deze risico's staan in dit advies maatregelen beschreven die de risico's moeten mitigeren. Zie: Projectplan Digitaal Ondertekenen Projectplan Digitaal Ondertekenen.docx en zaaknummer 52064745.

	• autonomie (bijvoorbeeld geen beperking van de vrijheid om eigen regels te volgen) Vooral van zaken als stigmatisering, ongelijkheid, manipulatie en niet ongestoord kunnen leven kunnen betrokkenen last hebben. • Daarnaast zijn de risico's voor de organisatie benoemd.	
Gedeeltelijk	De waarschijnlijkheid en ernst zijn ingeschat.	Dit staat gedeeltelijk beschreven in het projectplan. Zie: Projectplan Digitaal Ondertekenen Projectplan Digitaal Ondertekenen.docx en zaaknummer 52064745.
Voldoet	De bedreigingen die kunnen leiden tot ongewenste wijziging zijn benoemd. De mogelijke gevolgen voor de rechten en vrijheden van betrokkenen zijn geïdentificeerd. Ze zijn benoemd vanuit het perspectief van betrokkenen en er is daarbij ook gedacht aan de bij het vorige punt genoemde gevolgen. Daarnaast zijn de risico's voor de organisatie benoemd.	De belangrijkste risico's zijn benoemd in het projectplan en dit advies. Voor deze risico's staan in dit advies maatregelen beschreven die de risico's moeten mitigeren. Zie: Projectplan Digitaal Ondertekenen Projectplan Digitaal Ondertekenen.docx en zaaknummer 52064745.
Gedeeltelijk	De waarschijnlijkheid en ernst zijn ingeschat.	Dit staat gedeeltelijk beschreven in het projectplan. Zie: Projectplan Digitaal Ondertekenen Projectplan Digitaal Ondertekenen.docx en zaaknummer 52064745.
Voldoet	De bedreigingen die kunnen leiden tot het niet beschikbaar zijn van gegevens zijn benoemd. De mogelijke gevolgen voor de rechten en vrijheden van betrokkenen zijn geïdentificeerd. Ze zijn benoemd vanuit het perspectief van betrokkenen en er is daarbij ook gedacht aan de bij het vorige punt genoemde gevolgen. Daarnaast zijn de risico's voor de organisatie benoemd.	De belangrijkste risico's zijn benoemd in het projectplan en dit advies. Voor deze risico's staan in dit advies maatregelen beschreven die de risico's moeten mitigeren. Zie: Projectplan Digitaal Ondertekenen Projectplan Digitaal Ondertekenen.docx en zaaknummer 52064745.

Gedeeltelijk	De waarschijnlijkheid en ernst zijn ingeschat.	Dit staat gedeeltelijk beschreven in het projectplan. Zie: Projectplan Digitaal Ondertekenen Projectplan Digitaal Ondertekenen.docx en zaaknummer 52064745.

Ad 4 de maatregelen worden benoemd

Voldoet	Omschrijving	Toelichting
Voldoet	De beoogde maatregelen om de risico's aan te pakken worden bepaald en zijn voldoende.	Ja, deze maatregelen zijn in dit document opgenomen onder het kopje ‘Advies’.

Afdeling: Transactionele Dienstverlening/ Ambtenaar van de burgerlijke stand.

Onderwerp: Digitalisering akten van de burgerlijke stand

Datum: 15-2-2023, HM/AL

Aanleiding

Het Huis voor de Stad (HvdS) biedt onvoldoende ruimte om de tientallen jaargangen akten burgerlijke stand op te slaan. Opslag buiten het HvdS brengt echter veel inefficiënties met zich mee: akten worden immers veelvuldig (ca. 3000x per jaar) door de collega's van Transactionele Dienstverlening (TD) en door onze klanten opgevraagd. Het wordt derhalve wenselijk geacht om de akten van de burgerlijke stand te digitaliseren, zodat ze snel en gemakkelijk zijn te benaderen.

De afdeling is daarom een project gestart om de (bestaande) akten van de burgerlijke stand te digitaliseren. Voor het digitaliseren van deze akten wil de afdeling een externe partij inschakelen. Nadat de akten zijn gedigitaliseerd worden ze ingelezen in de iBrondocumenten. iBrondocumenten is een bedoelde module bij het bij gemeente Helmond in gebruik zijnde systeem iBurgerzaken.

Er is een risico analyse uitgevoerd op het project om bestaande akten van de burgerlijke stand te digitaliseren en men vraagt advies van de FG en CISO.

Het besluit om bestaande akten te digitaliseren, bevat echter ook het impliciete besluit om te gaan werken met digitale akten en om iBrondocumenten te gaan gebruiken[1]. Over het besluit om te gaan werken met digitale akten en iBrondocumenten is geen advies gevraagd. Procesbeschrijvingen die betrekking hebben op het digitaliseren van nieuwe akten van de Burgerlijke Stand en het verwerken van latere vermeldingen zijn (nog) niet beschikbaar, omdat het buiten scope van het project valt[2].

De FG en de CISO hebben het advies gebaseerd op de volgende documenten:

- Startnotitie d.d. 20 september 2022
- Proces Digitaliseren akten BS
- Concept Programma van Eisen
- Sessie 1 verkenning proces
- Sessie 2 oriëntatie privacy
- Sessie 3 oriëntatie dreigingen en risicobronnen

Conclusie

De privacy risico's voor betrokkenen zijn groot.

Er kan niet worden vastgesteld of het digitaliseren van de bestaande akten van de burgerlijke stand gerechtvaardigd is. Dit is een gevolg van het feit dat (nog) niet inzichtelijk is gemaakt of het verwerken van een extra (blijvende) digitale versie van de akten van de burgerlijke stand in iBurgerzaken gerechtvaardigd is en alle met deze extra verwerking samenhangende privacyrisico's voor betrokkenen zijn teruggebracht tot een voor betrokkene aanvaardbaar niveau.

[1] Zie mail van de FG naar aanleiding van startnotitie d.d. 12 september 2022
[2] Zie mail 5.1.2e d.d. 25 januari 2023

Het toch al starten met het digitaliseren van de bestaande akten van de burgerlijke stand heeft als risico dat:
- achteraf moet worden vastgesteld, dat de digitalisering niet gerechtvaardigd is;
- de gedigitaliseerde documenten niet aansluiten op de vereiste maatregelen;
- er te lang extra exemplaren van de digitale akten beschikbaar moeten blijven omdat nog niet kan worden overgegaan tot importeren/converteren van de akten in iBrondocumenten.

De keuze voor het beschreven (gewenste) proces wordt niet onderbouwd. Dit proces bevat een groot aantal extra verwerkingen en overdracht, transport, digitalisering en opslag van originele akten vormen een groot risico. Het is niet duidelijk of er niet een minder ingrijpende oplossing mogelijk is, waarbij ook minder verwerkingen plaatsvinden. De noodzaak van de verwerkingen staat daarmee niet vast.

Er zijn aanvullende passende maatregelen nodig om de persoonsgegevens te beschermen tegen onrechtmatige verwerking en inbreuken op de beschikbaarheid, integriteit en vertrouwelijkheid. Wanneer deze maatregelen niet worden uitgevoerd zijn de restrisico's voor betrokkenen onaanvaardbaar hoog.

Gezien de impact die de nog aanwezige risico's kunnen hebben op onze inwoners en onze dienstverlening, adviseren de FG en de CISO daarom om vóór de start van het digitaliseren van de bestaande akten de onderstaande maatregelen te implementeren. Het niet opvolgen van dit advies en het inrichten van deze maatregelen betekent dat de privacy risico's voor betrokkenen onacceptabel hoog zijn en dat de ambtenaar van de burgerlijke stand en daarmee de gemeente tot het moment van implementatie een risico loopt.

Advies aan de ambtenaar van de burgerlijke stand.

De FG en CISO adviseren om:
1. Een risico afweging te maken over de implementatie van iBrondocumenten en de risico's bij het gebruik van de (extra) digitale akte van de burgerlijke stand en iBrondocumenten in beeld te brengen. De noodzakelijke maatregelen te benoemen en te treffen en aan de hand daarvan vast te stellen of deze werkwijze gerechtvaardigd is.
2. Pas als is vastgesteld dat gebruik van de (extra) digitale akte van de burgerlijke stand in iBrondocumenten gerechtvaardigd is over te gaan tot digitalisering van alle bestaande akten van de burgerlijke stand.
3. Te onderzoeken of er een andere minder ingrijpende en met minder verwerkingen gepaard gaande digitalisering mogelijk is (zie bijlage onderdeel 2b, 2c, 2d en 2f). Denk bijvoorbeeld aan het door gemeente Helmond zelf scannen van de bestaande akten, het scannen op locatie bij de gemeente Helmond in plaats van op locatie van de leverancier, of door de gedigitaliseerde akten niet aan te leveren op een usb stick maar beschikbaar te stellen via een toereikend beveiligde cloud oplossing.
4. Wanneer er na onderzoek, of omdat het advies van de FG en de CISO niet wordt overgenomen, toch wordt gekozen voor de gewenste/voorgestelde werkwijze: te onderbouwen waarom een andere minder ingrijpende werkwijze niet mogelijk is en deze onderbouwing schriftelijk vast te leggen.
5. Wanneer het advies van de FG en de CISO niet wordt overgenomen en er toch al wordt gestart met het digitaliseren van de bestaande akten conform de voorgestelde/gewenste werkwijze adviseren de FG en CISO om:
    a. Te kiezen voor een leverancier die ISO 27001 gecertificeerd is.

b. Het certificaat en de daarbij behorende verklaring van toepasselijkheid vooraf bij de leverancier op te vragen en te controleren.
c. Het proces tussen en scannen en de opslag op de USB stick bij de leverancier in beeld te brengen (zie bijlage onderdeel 1e).
d. Betrokkenen te informeren, over de digitalisering van de akten van de burgerlijke stand, bijvoorbeeld door middel van een privacyverklaring op de gemeentelijke website (zie bijlage onderdeel 2g).
e. De algemene inkoopvoorwaarden van de gemeente Helmond van toepassing te verklaren.
f. te zorgen dat gegevens niet langer worden bewaard dan noodzakelijk (zie bijlage onderdeel 1c en 2f):
    i. Te kiezen voor een leverancier die de opdracht binnen de kortst mogelijke tijd kan opleveren (van ontvangst van de originele akten tot terugsturen van de originele akten).
    ii. Het aantal originele akten dat een batch mag bevatten, zodanig te beperken dat de periode waarin een leverancier de originele akten bezit zo kort mogelijk is en het aantal akten waar meerdere versies van bestaan zo klein mogelijk blijft.
    iii. De digitale opslag bij de leverancier vier weken na oplevering van de digitale akte te vernietigen.
    iv. De USB stick binnen vier weken na ontvangst te vernietigen.
    v. De werkprocessen zodanig in te richten dat de originele akten binnen de periode van vier weken zijn gecontroleerd (op afwijkingen en fouten) en ingelezen.
g. De volgende afspraken vast te leggen met de leverancier die de akten digitaliseert:
    i. De termijn waarbinnen de opdracht moet zijn afgerond en er daarbij voor te zorgen dat de termijn dat de leverancier toegang heeft tot de akten van de burgerlijke stand zo kort mogelijk is.
    ii. Vernietiging van de digitale opslag bij de leverancier vier weken na oplevering.
    iii. Bewijs te overleggen van de vernietiging van de digitale opslag middels logging, rapportages en screenshots van de situatie voorafgaand en ná de vernietiging
    iv. Welke beheersmaatregelen de leverancier heeft ingericht voor het transport van de fysieke akten. Wij adviseren hierbij minimaal vergelijkbare maatregelen te hanteren als door de gemeente worden gehanteerd bij het transport van de dubbelen van de akten naar de centrale bewaarplaats, zoals deugdelijke verpakking, aangetekende verzending, track en trace en bevestiging van verzending en van ontvangst
    v. Welke beheersmaatregelen de leverancier heeft ingericht voor transport, gebruik en wissen van de op een usb stick opgeslagen informatie, conform onderdeel A.8.3 uit bijlage A bij ISO27001:2017 c.q. paragraaf 8.3 van de BIO. De informatie dient in ieder geval encrypt (bij voorkeur op basis van bitlocker) op de usb stick te worden opgeslagen en de sleutel dient op een toereikend beveiligde manier, bijvoorbeeld via SMS, te worden gedeeld
    vi. De originele akten dienen te worden bewaard in een ruimte die voldoet aan de wettelijke eisen voor opslag van akten van de burgerlijke stand.
    vii. Toegang tot de akten tijdens het uitvoeren van de opdracht.

viii. Afspraken over beschikbaarheid van de originele akten op het moment dat een burger verzoekt om een afschrift of een uittreksel.
ix. De eisen die worden gesteld aan de digitale scans van de leverancier. Zorg dat de digitale scans voldoen aan de wettelijke eisen, goed leesbaar zijn en niet te wijzigen zijn.
x. Metadatering zodanig dat geborgd is dat de akten terugvindbaar zijn, in het bijzonder ter borging dat zowel het importeren in iBrondocumenten als het opzoeken/terugvinden met de functionaliteit van iBrondocumenten/iBurgerzaken correct werkt.
xi. De wijze waarop de ontvangst en het versturen van de zending wordt vastgelegd, gecontroleerd en gemeld.

h. De volgende afspraken vast te leggen met Pink Roccade:
   i. over de beschikbaarheid van iBurgerzaken tijdens de conversie/overzetting van de digitale akten.
   ii. Wat te doen bij (onherstelbare) afwijkingen/verstoringen/fouten? Wie is waarvoor verantwoordelijk? Wie lost de afwijking/verstoring/fout op? Binnen welke termijn moet een afwijking/verstoring/fout opgelost worden?
   iii. Testen van de conversie/overzetting.

i. Stel een plan van aanpak op, met instructies voor de medewerkers rondom
   i. Het klaarmaken van de batch.
   ii. Het aantal originele akten dat een batch mag bevatten.
   iii. Wie de batch mag klaarmaken.
   iv. De vastlegging van de verzending van de batch.
      - Aantal documenten
      - Datum verzending
   v. Op welke wijze inzicht wordt verkregen in de verstuurde akten, zodanig dat bij verlies of onbevoegde toegang bekend is welke documenten er geraakt zijn.
   vi. Het in ontvangst nemen van de originele documenten en de USB stick. Leg daarbij vast:
      - Met hoeveel personen de zending in ontvangst wordt genomen
      - Wat hun functie is
      - Op welke wijze de ontvangst wordt gecontroleerd op volledigheid. Er kan daarbij worden gekozen voor een globale telling, mits er een met aan zekerheid grenzende waarschijnlijkheid kan worden vastgesteld dat de telling klopt.
      - Op welke wijze de ontvangst wordt vastgelegd.
      - Aan wie de zending wordt overgedragen.
      - Waar de zending wordt opgeslagen na ontvangst.
   vii. De controle van de kwaliteit van de digitalisering op volledigheid en juistheid van de akten in iBrondocumenten.
   viii. De technische controle op het foutloos converteren en importeren van de digitale bestanden.
   ix. Werkwijze in het geval het aantal retour ontvangen documenten niet overeenstemt met het aantal verzonden documenten.
   x. Werkwijze/procedure in geval van interne verstoringen

xi. Werkwijze in geval van fouten met betrekking tot de beeldkwaliteit. Leg daarbij vast:
- De verantwoordelijkheden.
- De termijn waarbinnen de fout moet worden opgelost.
- Op welke locatie de originele akte wordt gescand.

xii. Toegang tot documenten en de usb stick.

j. Zorg dat deze werkwijze/procedure toegankelijk is voor medewerkers en informeer ze er over.

k. Bewaar de originele akten en de digitale versies in een ruimte die voldoet aan de wettelijke eisen voor opslag van akten van de Burgerlijke stand. Stel deze eisen aan:
   i. De plek waar de batch met een x aantal originele akten van de burgerlijke stand worden bewaard tot aan transport
   ii. Het middel waarmee de akten en de USB stick worden getransporteerd
   iii. De plek waar de leverancier de originele akten bewaart
   iv. De USB stick
   v. De opslag van de originele akten na digitalisering.

6. Het gebruik van digitale akten van de burgerlijke stand toe te voegen aan het register van verwerkingen.
7. Alle nog te implementeren maatregelen over te nemen in een plan van aanpak, voeg dit plan van aanpak toe aan de projectadministratie en bewaak de implementatie hiervan.

Toelichting

De ambtenaar van de burgerlijke stand is (zelf) verantwoordelijk voor de naleving van de AVG bij de uitvoering van zijn taken.

De wet[3] draagt de ambtenaar van de burgerlijke stand een aantal taken op, zoals het samenvoegen van de (losbladige) akten van de burgerlijke stand tot registers, het toevoegen van latere vermeldingen en alles wat nodig is om deze registers in stand te houden[4].

Aangezien de wet deze taak opdraagt aan de ambtenaar van de burgerlijke stand, is hij bij de uitvoering van deze taken zelfstandig en staat hij niet in een hiërarchische verhouding noch tot collega's noch tot het gemeentebestuur.

Voor de akten van de burgerlijke stand mag uitsluitend wit normaal schrijfpapier worden gebruikt[5]. De beschreven losse bladen moeten worden samengevoegd tot een register en door de ambtenaar van de burgerlijke stand zorgvuldig in een afgesloten, tegen brand beschermde ruimte worden bewaard. Ze mogen alleen uit deze ruimte worden verwijderd als dit noodzakelijk is voor de uitoefening van de dienst[6]. Daarnaast dient de ambtenaar van de burgerlijke stand dubbelen van de akten over te brengen naar de centrale bewaarplaats: de Justitiële Informatiedienst. Dubbelen kunnen in digitale vorm worden aangeboden.

[3] Burgerlijk Wetboek, boek 1.
[4] Artikel 16a
[5] Artikel 1 en 2 Regeling papier, andere gegevensdragers en middelen voor de opmaak van de akten van de burgerlijke stand.
[6] Besluit burgerlijke stand 1994, tweede afdeling

De wet verplicht dus tot twee exemplaren van de akten van de Burgerlijke stand. Daarnaast wil de gemeente een derde (blijvende) digitale versie, opslaan in iBrondocumenten. Dit is een extra akte, wat in strijd is met het principe van dataminimalisatie. Er "ontstaat" immers een extra (digitale) versie van de akten van de burgerlijke stand, en dat is meer dan op grond van de wet noodzakelijk wordt geacht. De extra (blijvende digitale) versie vergroot het risico op onbevoegde toegang en op fouten.

Het valt echter niet te ontkennen dat de wet niet aansluit bij het huidige digitale tijdperk. De behoefte aan een digitale versie van de akte van de burgerlijke stand is daarom te begrijpen en kan worden gezien als noodzakelijk voor een goede uitvoering van deze aan de ambtenaar van de burgerlijke stand opgedragen taak. Mits de met deze extra verwerking samenhangende grotere risico's voor betrokkenen zijn teruggebracht tot een voor betrokkene aanvaardbaar niveau.

Het is de CISO en de FG echter niet gebleken dat de keuze om gebruik te gaan maken van een digitale akte is gebaseerd op een risico afweging, waarbij voldoende maatregelen zijn getroffen om de privacy risico's voor betrokkenen terug te brengen naar een aanvaardbaar niveau.

Nu het niet vaststaat dat het gebruik van (een extra, blijvende) digitale versie van de akten van de burgerlijke stand gerechtvaardigd is, valt ook niet vast te stellen of het digitaliseren van de bestaande akten gerechtvaardigd is. Een uitzondering hier op is de circa 3% van de bestaande akten (9.100 van de 270.000 akten[7]), die zijn aangetast door inktvraat. Het doel van digitalisering van deze akten is het tegengaan van inktvraat.

Door al te starten met het digitaliseren van de bestaande akten bestaat het risico dat achteraf blijkt dat de wijze waarop de akten zijn gedigitaliseerd niet aansluit bij de maatregelen die nodig zijn om op een veilige en verantwoorde wijze gebruik te kunnen maken van digitale akten.

Bijlage 1 bevat de volledige beoordeling van de risico analyse

Toelichting risicomanagement

Risicomanagement is het proces dat organisaties uitvoeren waarbij risico's worden geïdentificeerd en gekwantificeerd gevolgd door vaststelling en uitvoering van beheersmaatregelen. Met beheersmaatregelen worden activiteiten bedoeld waarmee de kans van optreden of de gevolgen van risico's positief worden beïnvloed. Tot slot wordt dit gehele proces continu gemonitord en wordt over het risicomanagement verantwoording afgelegd aan belanghebbenden.

In de kern is een risico analyse een document, waarin de ambtenaar van de burgerlijke stand de risico's van de gegevensverwerking inventariseert. Met deze inventarisatie is het mogelijk om een op een risicoafweging gebaseerde keuze te maken niet alleen vanuit het perspectief van de organisatie maar ook vanuit het perspectief van de mensen van wie de persoonsgegevens worden verwerkt (de "betrokkenen").

Doel van de uitgevoerde risico analyse is om een verantwoorde oplossing te vinden voor een gesignaleerd probleem. In de praktijk, en ook in deze situatie, zien we dat een risicoanalyse wordt uitgevoerd op een al gekozen oplossing. Dat is een gemiste kans, en het schept het (onterechte) beeld dat het uitvoeren van een risico analyse de voortgang van een project belemmerd.

[7] Bron Concept Programma van Eisen.

Door vroeg te beginnen is het gemakkelijker om aan de wettelijke vereiste principes van privacy by design en privacy by default te voldoen en wordt voorkomen dat achteraf (dure of vertragende) maatregelen moeten worden getroffen.

Het doel is om een oplossing tegenover de risico's maatregelen te zetten. Het is daarnaast een belangrijk proces om te beoordelen of de verwerking van persoonsgegevens rechtmatig en behoorlijk is. Het is óók een document waarmee de ambtenaar van de burgerlijke stand intern én extern verantwoording aflegt over de gemaakte keuzes bij de gegevensverwerking.

De AVG schrijft voor dat bij iedere uitgevoerde risico analyse een advies wordt gevraagd aan de Functionaris Gegevensbescherming (FG), de onafhankelijk toezichthouder op de naleving van de AVG. Onder de AVG is een FG advies geen dwingend advies, maar een zwaarwegend advies. Dat houdt in dat de ambtenaar van de burgerlijke stand kan afwijken van het advies, mits dit beargumenteerd wordt vastgelegd.

Bijlage

1 Toets van de risico analyse digitaliseren bestaande akten burgerlijke stand.

Een risico analyse heeft betrekking op informatieveiligheid en privacy. Voor privacy geldt dat de AVG een aantal vereisten stelt aan de uit te voeren risico analyse: Dit zijn de volgende vereisten:

1. Een systematische beschrijving van de beoogde verwerking en de doeleinden;
2. Een beoordeling van de noodzaak en de evenredigheid;
3. Een beoordeling van de risico's voor de rechten en vrijheden van betrokkenen:
4. Een overzicht van beoogde maatregelen om deze risico's aan te pakken.

Ad 1 een systematische beschrijving

	Omschrijving	Toelichting
a.	De risico analyse vermeldt: de persoonsgegevens die worden verwerkt	Ja zie blz 4 van "Sessie 2 oriëntatie privacy". De akten van de burgerlijke stand bevatten de levensloop van inwoners. (geboorte, huwelijk, kinderen, overlijden). Daarnaast wordt er bij het digitaliseren van de akten metadata verwerkt, zie blz 13 van "Sessie 2 oriëntatie privacy".
b.	De risico analyse vermeldt: de ontvangers van deze persoonsgegevens	Ja zie blz 5 van "Sessie 2 oriëntatie privacy". Behalve de leverancier die de bestaande akten zal scannen, ontvangt mogelijk ook een koerier en/of een clouddienst de gegevens.
c.	De risico analyse vermeldt: de periode gedurende welke de persoonsgegevens worden bewaard	Nee, de bewaartermijn is nog niet ingericht, zie blz 5 van "Sessie 2 oriëntatie privacy". Het digitaliseren van de bestaande akten van de burgerlijke stand brengt (in de gekozen werkwijze) extra verwerkingen met zich mee: 1. Een digitale versie van de bestaande akten op USB. 2. Een tijdelijke digitale versie bij de leverancier. Er zijn geen afspraken gemaakt over de termijnen van bewaren en de wijze van vernietiging van deze extra verwerkingen.
d.	De risico analyse bevat een functionele beschrijving van de verwerking	Ja zie blz 9 van "Sessie 2 oriëntatie privacy".
e.	De risico analyse bevat de activa waarop persoonsgegevens steunen (hardware, software, netwerken, mensen, papier of papiertransmissiekanalen)	Deels. Zie blz 8, 9 en 10 van "Sessie 2 oriëntatie privacy". Niet in beeld zijn de activa rondom het scannen van de bestaande akten. Het gaat daarbij om het proces tussen en scannen en de opslag op de USB stick.

Ad 2 De noodzaak en de evenredigheid wordt beoordeeld

Voldoet	Omschrijving	Toelichting
a.	De risico analyse vermeldt de grondslag en de doeleinden van de verwerking	Ja, zie blz 3 van "Sessie 2 oriëntatie privacy". De ambtenaar van de burgerlijke stand is verantwoordelijk voor de instandhouding van de registers van akten van de burgerlijke stand. Het terugdringen van inktvraat is een gerechtvaardigd doel voor 3% van de aangeboden akten (9.100 van de 270.000 akten[8]). De Grondslag voor deze verwerking is: artikel 6 lid 1 sub e van de AVG.

[8] Bron Concept Programma van Eisen.

		Voor de overige 97% geldt dat het doel van de verwerking bestaat uit een efficiënte bedrijfsvoering en dienstverlening is. Er kan niet worden vastgesteld of er sprake is van een gerechtvaardigd doel (zie toelichting).
b.	De risico analyse vermeldt welke gegevens en verwerkingen er noodzakelijk zijn voor het bereiken van dit doel	Er wordt beschreven op welke wijze de bestaande akten worden gedigitaliseerd, zie blz 8 en 9 van de “Sessie 2 oriëntatie privacy”. Daarmee ontstaan naast de 2 wettelijke verplichte verwerkingen en de blijvende digitale versie in IBrondocumenten nog diverse extra verwerkingen zoals: 1. Het klaarmaken en bewaren van een batch (met x aantal originele akten) 2. Het vervoer van (de batch) met originele akten van de gemeente naar de leverancier. 3. De opslag van de originele akten bij de leverancier. 4. Het scannen van de originele akte door de leverancier. 5. Het aanmaken van de metadata door de leverancier. 6. De opslag van een tijdelijke digitale versie bij de leverancier. 7. Een opslag van een tijdelijke digitale versie op USB. 8. Het vervoer van de originele akten en de USB van de leverancier naar de gemeente. 9. Het importeren van de gedigitaliseerde akten in iBurgerzaken. 10. De opslag van metadata. De risico analyse onderbouwt niet waarom deze werkwijze en daarmee deze extra verwerkingen noodzakelijk zijn.
c.	De risico analyse vermeldt of er een minder ingrijpende gegevensverwerking mogelijk is	Een minder ingrijpende verwerking is het zelf scannen van de bestaande akten van de burgerlijke stand. Zie blz 12 “Sessie 2 oriëntatie privacy”. Ook is het minder ingrijpend wanneer er wordt gekozen voor een proces waarbij minder extra verwerkingen (zie vorig punt) noodzakelijk zijn. Alternatieven worden niet benoemd in de risico analyse. De risico analyse onderbouwt niet waarom er niet is gekozen voor een minder ingrijpende verwerking.
d.	De risico analyse bevat een omschrijving van de maatregelen die worden getroffen om de verwerking te beperken tot de ter zake dienende noodzakelijke gegevens	Omdat de noodzaak van de gekozen werkwijze niet is onderbouwd en alternatieven met een afweging over de gemaakte keuze ontbreken kan niet worden vastgesteld dat er maatregelen zijn getroffen om de verwerking te beperken tot de terzake dienende noodzakelijke gegevens.
e.	De risico analyse bevat een omschrijving van de maatregelen die worden getroffen om te zorgen dat geen function creep[9] optreedt.	Niet van toepassing voor het digitaliseren van de bestaande akten. Dit is wel een aandachtspunt voor het gebruik van iBrondocumenten.
f.	De risico analyse bevat een omschrijving van de maatregelen	Er is niet vastgesteld dat de extra opslag van de akten (de fysieke akten bij de leverancier, de digitale akte op de USB-Stick en de

[9] function creep is wat er gebeurt als we technologie en systemen gebruiken op een andere manier dan in de eerste instantie eigenlijk bedoeld is, met name wanneer het nieuwe doel resulteert in een inbreuk op de privacy.

	die worden getroffen om ervoor te zorgen dat gegevens niet langer dan noodzakelijk worden opgeslagen in een vorm die het mogelijk maakt om betrokkene te identificeren.	tijdelijke digitale opslag bij de leverancier) noodzakelijk is. Bovendien zijn er nog geen afspraken gemaakt over het bewaren en vernietigen van deze tijdelijke gegevens.
g.	De risico analyse bevat een omschrijving van de wijze waarop betrokkene (toereikend) wordt geïnformeerd.	Betrokkenen worden niet geïnformeerd over het digitaliseren Zie blz 15 van “Sessie 2 oriëntatie privacy”.
h.	de risico analyse bevat een omschrijving van hoe betrokkenen hun rechten uit kunnen oefenen: a. rechten van inzage b. recht op rectificatie en verwijdering c. recht op overdraagbaarheid van gegevens d. recht op bezwaar e. recht op beperking van de verwerking	De risico analyse bevat een beschrijving van de wijze waarop betrokkenen hun rechten kunnen uitoefenen met betrekking tot de akten van de burgerlijke stand, zie blz 14 “Sessie 2 oriëntatie privacy”.
i.	de risico analyse beschrijft de relatie met verwerkers	Ja zie blz 13 van “Sessie 2 oriëntatie privacy”.
j.	De risico analyse beschrijft de waarborgen omtrent internationale doorgifte	Nee, De algemene inkoopvoorwaarden van de gemeente Helmond verbieden internationale doorgifte naar landen met een niet passende bescherming.
k.	de risico analyse vermeldt of voorafgaande raadpleging nodig is	Nvt

Ad 3 de risico’s voor de rechten en vrijheden van betrokkenen

Voldoet	Omschrijving	Toelichting
a.	de risico analyse brengt de risico’s voldoende in beeld. De risico bronnen zijn benoemd. De mogelijke gevolgen voor de rechten en vrijheden van betrokkenen zijn geïdentificeerd en benoemd vanuit het perspectief van betrokkenen.	Zie blz 14 en 15 van “Sessie 2 oriëntatie privacy”. Zie voor de risico bronnen: “Sessie 3 Oriëntatie dreigingen en risico bronnen”. In het document “Sessie 1 Verkenning proces” zijn een aantal risico’s benoemd. **Risico’s voor de organisatie**: Een inbreuk op beschikbaarheid, integriteit of vertrouwelijkheid van de akten van de burgerlijke stand kan leiden tot de verstoring van de dienstverlening, imagoverlies en financiële schade.
b.	De bedreigingen die kunnen leiden tot onrechtmatige toegang zijn benoemd.	**Conclusie FG en CISO:** De voorgestelde werkwijze brengt een extra verwerkingen met zich mee en daarmee extra risico op onrechtmatige toegang. Onrechtmatige toegang kan plaatsvinden doordat: - de batch met een originele akten niet op een veilige wijze wordt bewaard totdat ze worden verstuurd naar de leverancier;

		- er bij de leverancier te veel medewerkers toegang hebben tot de te digitaliseren akten; - er bij de leveranciers te veel medewerkers toegang hebben tot de tijdelijke digitale opslag bij de leverancier; - er iets mis gaat bij het transport van de originele akten; - er iets mis gaat bij het transport van de usb-stick;
c.	De waarschijnlijkheid en ernst zijn ingeschat.	**Conclusie FG en CISO:** Vanwege de aard van de gegevens leidt onrechtmatige toegang tot de akten tot ernstige gevolgen voor betrokkenen. De vele transport momenten, het gebruik van de USB stick en het groot aantal akten maakt de kans dat de gevolgen optreden groot. Hoe groter het aantal originele akten dat gelijktijdig wordt aangeboden en digitale bestanden dat een USB-stick bevat hoe groter de impact als er daadwerkelijk iets mis gaat. Aanvullende maatregelen zijn noodzakelijk om de restrisico's terug te brengen naar een acceptabel niveau.
d.	De bedreigingen die kunnen leiden tot ongewenste wijziging zijn benoemd.	**Conclusie FG en CISO:** De voorgestelde werkwijze brengt extra verwerkingen met zich mee en daarmee extra risico dat er een verschil ontstaat tussen de diverse versies. Dit kan ontstaan doordat: - bij het scannen fouten optreden; - er fouten ontstaan bij het metadateren en het (gescheiden) opslaan van de scan (image) en de metadata; - er fouten ontstaan bij het overzetten van de data op een usb-stick; - er fouten ontstaan bij het importeren (converteren) van de bestanden op de usb-stick in iBrondocumenten; - onbevoegden toegang krijgen tot de gegevens en wijzigingen aanbrengt in de data. -
e.	De waarschijnlijkheid en ernst zijn ingeschat.	**Conclusie FG en CISO:** Vanwege het feit dat een akte van de burgerlijke stand een brondocument is leiden onjuiste gegevens tot zeer ernstige gevolgen voor betrokkenen. De vele transport momenten, het gebruik van de USB stick en het groot aantal akten maakt de kans dat de gevolgen optreden groot. Hoe groter het aantal originele akten dat gelijktijdig wordt aangeboden en digitale bestanden dat een USB-stick bevat hoe groter de impact als er daadwerkelijk iets mis gaat. Daarnaast is er weinig ervaring met het extern (vanuit een usb-stick) converteren/importeren van digitale akten in iBrondocumenten. Er is nog geen plan van aanpak voor deze conversie. Zolang hierover geen duidelijkheid bestaat moet de kans dat er iets mis gaat bij de conversie als zeer groot worden ingeschat. Aanvullende maatregelen zijn noodzakelijk om de restrisico's terug te brengen naar een acceptabel niveau.
f.	De bedreigingen die kunnen leiden tot het niet beschikbaar zijn van gegevens zijn benoemd.	**Conclusie FG en CISO:** De voorgestelde werkwijze brengt extra verwerkingen met zich mee en daarmee zijn er extra risico's op tijdelijk verlies van gegevens. Dit kan ontstaan doordat: - er iets mis gaat in het proces waardoor originele akten kwijt raken of verloren gaan; - er iets mis gaat in het proces waardoor een usb-stick kwijt raakt of verloren gaat;

		- de originele akte voor het scannen bij de leverancier ligt terwijl de akte voor de dienstverlening nodig is. - Tijdens het importeren/converteren van de digitale akten, er iets mis gaat en iBurgerzaken niet beschikbaar is.
g.	De waarschijnlijkheid en ernst zijn ingeschat.	**Conclusie FG en CISO:** Vanwege het feit dat een akte van de burgerlijke stand een brondocument is, is (definitief) verlies van de originele akte zeer ernstig. De kans dat dit optreedt is minimaal aangezien er dubbelingen van de akten centraal worden bewaard. Verlies van de USB stick heeft geen ernstige gevolgen voor de beschikbaarheid omdat het origineel nog beschikbaar is. Voor de beschikbaarheid van de originele akten en de beschikbaarheid van iBurgerzaken dienen aanvullende maatregelen te worden getroffen.

Ad 4 de maatregelen worden benoemd

Voldoet	omschrijving	Toelichting
a.	de beoogde maatregelen om de risico's aan te pakken worden bepaald en zijn voldoende.	De noodzakelijke maatregelen zijn terug te vinden in het advies van de FG en de CISO.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens geanonimiseerd op grond van:

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

Advies SPO team + FG en CISO

Afdeling/Programma: Digitale Stad – Digital Twin

Onderwerp: Applicatie DIGITWIN Argaleo

11 juli 2023, FvH

Aanleiding

Achtergrond

Het programma Digitale Stad Helmond heeft als één van haar doelstellingen om een Open Urban Platform i.c.m. Digital Twinning te ontwikkelen. Het Open Urban Platform en de Digital Twinning applicaties moet het datagedreven werken gaan ondersteunen. Op basis van data (informatie) verzameld uit de openbare ruimte wordt de gemeente Helmond in staat gesteld om meer dan nu besluiten nemen op basis van feiten (data). *Bron: PSA*

We karakteriseren een Digital Twin als een virtuele omgeving met een actueel overzicht van de toestand van (een deel van) de stad (op basis van verschillende statische en dynamische databronnen). Digital Twins stellen ons tevens in staat om (op termijn) beleidsmaatregelen en andere geplande ingrepen te simuleren en testen. De Digital Twin kent verschillende toepassingen: dashboarding, monitoring, scenario's doorrekenen, voorspellen en uiteindelijk zelfs (automatisch) interveniëren, maar het blijft vooral een hulpmiddel om vanuit een gedeeld, eenduidig inzicht en uitzicht met elkaar het goede gesprek te voeren. Als professionals onder elkaar, met externe partners, met bestuur en politiek en met onze inwoners en bedrijven. *Bron: PSN.*

Binnen de pilot wordt gestart met (enkel) data die wordt verkregen van Resono.

Doel

Kort gezegd heeft dit project de volgende twee doelstellingen:

1. Het doel is om te beoordelen in welke mate en hoe digital twinning kan bijdragen aan een datagedreven organisatie;
2. Met name om het monitoren van bezoekersstromen en vastgoedontwikkeling (bijvoorbeeld inzicht soorten winkels en spreiding ervan).

Scope

In scope van deze DPIA zijn:

- De persoonsgegevens die middels de Digital Twin worden gebruikt.
- Andere data (buiten persoonsgegevens) dia middels de Digital Twin worden gebruikt.
- Informatiebeveiligingsmaatregelen die door Argaleo zijn genomen.

Out-of-scope van deze DPIA zijn:

- De processen binnen de gemeente Helmond waarvoor Digital Twin wordt ingezet.
- Het toevoegen van extra of nieuwe databronnen.

Commented [ ]: Feedback voor (voor een volgende keer): citeer niet uit bronnen maar analyseer deze bronnen en neem in het advies jouw analyse/samenvatting weer. Dit geldt voor het volledige advies.

Betrokken partijen

Verwerkingsverantwoordelijk: gemeente Helmond
Is zelfstandig verwerkingsverantwoordelijk en sluit een licentieovereenkomst af met Argaleo met het doel om gebruik te kunnen maken van Digital Twin.

Zelfstandig verwerkingsverantwoordelijke: Argaleo
Argaleo is de leverancier van de applicatie Digital Twin, welke de gemeente Helmond van plan is om in te zetten ter verwezenlijking van de hiervoor genoemde doelstellingen. DIGITWIN maakt standaard gebruik van de datadienst Omgevingsserver, ook wel data-as-a-service. Dit is altijd actueel digitaal dataloket. Het digitale dataloket wordt (in deze pilot) doorlopend verrijkt met data die wordt verkregen van Resono. Digitwin biedt de mogelijkheid om te koppelen met eigen statistische en live databronnen. Hier wordt (vooralsnog) geen gebruik van gemaakt. De gemeente Helmond kan Digitwin met nieuwe gegevens verrijken. Die gegevens maken we 'hapklaar' door alle data te combineren en te visualiseren. Digitwin brengt de data in beeld, het biedt inzicht en overzicht met visualisaties Om gebruik te ku.nnen maken van de diensten van Argaleo is een account nodig, hierbij worden persoonsgegevens verwerkt. Argaleo is zelfstandig verwerkingsverantwoordelijke voor de verwerking van deze persoonsgegevens. Zij bepaalt immers welke persoonsgegevens hiervoor noodzakelijk zijn.

Commented [redacted]: Wie is hier wij? Argaleo vermoed ik? Zie tekstvoorstel. Deze tekst verwijderen.

Verstrekker Resono
Resono levert aan Argaleo geaggregeerde data zonder gepseudonimiseerde ID's . De data die wordt verstrekt is zodanig bewerkt dat deze niet is terug te leiden naar individuen. Daardoor ontvangt Argaleo **geen** persoonsgegevens van Resono. (zie DPIA Digitwin voor uitleg van de wijze van anonimiseren)

Doel en middelen voor het verzamelen van de data wordt bepaald door Resono, zij zijn zelfstandig verwerkingsverantwoordelijk voor de persoonsgegevens die zij verwerken om te komen tot de te verstrekken data(sets). .

Verwerker van Argaleo: BIT
Verzorgt de 'hosting' voor de systemen van Argaleo. Uit het privacybeleid kan worden opgemaakt dat zij slechts data verwerken binnen de Europese Economische Ruimte (namelijk in Nederland), waardoor op alle accountgegevens van de medewerkers van de gemeente Helmond geen extra maatregelen genomen hoeven te worden om een eventuele transfer van persoonsgegevens buiten de Europese Economische Ruimte mogelijk te maken. Verder is deze partij gecertificeerd voor ISO27001 (informatiebeveiliging).

Verwerker van Argaleo: STRATO
Verzorgt de 'hosting' voor de systemen van Argaleo. Uit het privacybeleid kan worden opgemaakt dat zij data verwerken in Duitsland, waardoor op alle accountgegevens van de medewerkers van de gemeente Helmond geen extra maatregelen genomen hoeven te worden om een eventuele transfer van persoonsgegevens buiten de Europese Economische Ruimte mogelijk te maken. Verder is deze partij gecertificeerd voor ISO27001 (informatiebeveiliging).

Gebruikte stukken

De FG en de CISO hebben het advies gebaseerd op de volgende documenten welke zijn bijgesloten in het dossier:

- Projectstartnotitie Digital Twin
- Projectstartarchitectuur Digital Twin
- Quickscan informatiebeveiliging en Privacy Digital Twin
- RA Digital Twin
- Argaleo – bijgewerkte Privacy en Security Statement
- Resono Hyperfence classification and modeling white paper
- Resono representativiteit white paper
- Resono security en privacybeleid

Conclusie

1. Digitwin wordt gevuld met anonieme data. Buurtniveau is het laagste detailniveau waarop data wordt gepresenteerd in Digital Twin, waardoor het niet mogelijk is om individuele personen te onderscheiden zonder gebruik te maken van (andere) externe bronnen. Hierdoor is de AVG (nu) niet van toepassing op de gebruikte data in Digital Twin, maar wél voor de gebruikersaccounts van de Helmondse medewerkers. Dit kan veranderen als er extra databronnen worden toegevoegd aan Digital Twin.
2. Er is geen duidelijke proceseigenaar die verantwoordelijk is voor deze applicatie, aangezien het Helmondse Strategisch Informatiebeveiligingsbeleid niet de mogelijkheid biedt om (tijdelijke) programmamanagers aan te stellen tot proceseigenaars, maar alleen afdelingsmanagers.
3. Zelfs wanneer een programmamanager zich gedraagt als ‘proceseigenaar’ is het nog steeds niet helder aan wie het programma ‘Digitale Stad’ wordt overgedragen wanneer dit wordt afgerond. Het risico bestaat dat niemand zich verantwoordelijk zal voelen voor het beheer van de Digital Twin wanneer dit vanuit het programma wordt overgedragen naar een van de afdelingen.
4. Het is onduidelijk of het mogelijk is om de Digital Twin te koppelen aan de Helmondse Azure Active Directory.
5. Digital Twin ondersteund twee-factor-authenticatie, Fedrated Login en/of SAML. Let op: hoewel een SAML-koppeling mogelijk is, zit daarin een kwetsbaarheid verscholen.
6. Digital Twin is nog niet opgenomen in de Helmondse autorisatiematrixen.
7. Argaleo gebruikt momenteel TLS 1.2 terwijl bij TLS 1.3 een aantal onveilige algoritmes uit versie 1.2 komen te vervallen.

Advies

1. Voor een nieuwe risico analyse uit, voordat extra databronnen worden toegevoegd aan Digital Twin.
2. Stel een afdelingsmanager aan als proceseigenaar aan die tijdens en na het project de verantwoordelijkheid op zich neemt voor het beheer van Digital Twin. Het is zeer sterk aan te raden dat dit de afdelingsmanager is van de afdeling die het meest gebruik zal gaan maken van de Digital Twin.
3. (zie vorige advies)
4. Vraag bij de leverancier na of het mogelijk is om Digital Twin te koppelen aan de Helmondse Azure Active Directory omgeving, en realiseer deze koppeling. Wanneer dat niet mogelijk blijkt te zijn, dient twee-factor-authenticatie te worden ingesteld in combinatie met Federated Login. Het is af te raden om gebruik te maken van SAML. Bij Fedrated Login wordt de autorisatie namelijk doorgegeven waarbij het wachtwoord en de gebruikersnaam wordt beschermd, terwijl dat bij SAML niet het geval is.
5. (zie vorig advies)

Commented [redacted]: Ik begrijp deze zin niet goed. [redacted] heb je een aanvulling?

6. Neem Digital Twin op in de autorisatiematrixen op rollenniveau, wijs hiervoor een functioneel beheerder aan die deze applicatie zal gaan beheren.
7. Vraag aan de leverancier of er actuele plannen zijn om over te stappen op TLS 1.3, en verzoek om dat zo snel mogelijk te doen wanneer hiertoe nog geen plannen zijn.

Reactie FG en CISO

Bovenstaand advies van de SPO is gezien en wordt gedragen door FG en CISO. Het kan dan ook worden gezien als een advies van FG en CISO.

21/6/2023 HM/AL

Toelichting risicomanagement

Risicomanagement is het proces dat organisaties uitvoeren waarbij risico's worden geïdentificeerd en gekwantificeerd gevolgd door vaststelling en uitvoering van beheersmaatregelen. Met beheersmaatregelen worden activiteiten bedoeld waarmee de kans van optreden of de gevolgen van risico's positief worden beïnvloed. Tot slot wordt dit gehele proces continu gemonitord en wordt over het risicomanagement verantwoording afgelegd aan belanghebbenden.

In de kern is een risicoanalyse een document, waarin de gemeente de risico's van de gegevensverwerking inventariseert, vanuit het perspectief van de mensen van wie de persoonsgegevens worden verwerkt (de "betrokkenen") en vanuit het perspectief van de organisatie.

Doel van de uitgevoerde risicoanalyse is om tegenover de risico's maatregelen te zetten. Het is daarnaast een belangrijk proces om te beoordelen of de verwerking van persoonsgegevens rechtmatig en behoorlijk is. Het is óók een document waarmee het college intern én extern verantwoording aflegt over de gemaakte keuzes bij de gegevensverwerking.

Onder de AVG is een FG-advies geen dwingend advies, maar een zwaarwegend advies. Dat houdt in dat afgeweken kan worden van het advies, mits dit beargumenteerd wordt vastgelegd.

Bijlage

1 Toets van de risicoanalyse

Een risicoanalyse heeft betrekking op informatieveiligheid en privacy. Voor privacy geldt dat de AVG een aantal vereisten stelt aan de uit te voeren risicoanalyse. Dit zijn de volgende vereisten:

1. Een systematische beschrijving van de beoogde verwerking en de doeleinden;
2. Een beoordeling van de noodzaak en de evenredigheid;
3. Een beoordeling van de risico's voor de rechten en vrijheden van betrokkenen;
4. Een overzicht van beoogde maatregelen om deze risico's aan te pakken.

Ad 1 een systematische beschrijving

	Omschrijving	Toelichting
Voldoet	De risicoanalyse vermeldt: de persoonsgegevens die worden verwerkt	Ja, dat is vermeld op pagina 8 van het DPIA rapport. Het gaat daarbij om de volgende gegevens: -e-mailadres; -wachtwoord; -voornaam;

		-achternaam. Deze gegevens worden geregistreerd in een Identity Access Management systeem van Argaleo. (pagina 8 DPIA)
Voldoet	De risicoanalyse vermeldt: de ontvangers van deze persoonsgegevens	Ja, dat zijn de volgende partijen: Zelfstandige verwerkingsverantwoordelijke: Argaleo Verwerker van Argaleo: BIT en STRATO AG (voor hosting). (pagina 9 DPIA)
Voldoet	De risicoanalyse vermeldt: de periode gedurende welke de persoonsgegevens worden bewaard	Ja, er is vermeld dat de gegevens worden opgeslagen gedurende de tijd dat het account voor Digital Twin actief is. Daarna worden de gegevens verwijderd. (pagina 8 en 20 DPIA)
Voldoet	De risicoanalyse bevat een functionele beschrijving van de verwerking	Ja, want op pagina 9 t/m 11 van de DPIA is vermeld welke persoonsgegevens worden verwerkt en dat dit geschiedt voor identificering/authentisering. Verder wordt de levenscyclus beschreven van de persoonsgegevens.
Voldoet	De risicoanalyse bevat de activa waarop persoonsgegevens steunen (hardware, software, netwerken, mensen, papier of papiertransmissiekanalen)	Ja, want dit is beschreven op pagina 11 DPIA aan de hand van het MAPOOD-principe. Het betreft hier een SAAS-applicatie waarbij het merendeel van de hardware en software wordt beheerd door de leverancier (Argaleo).

Ad 2 De noodzaak en de evenredigheid wordt beoordeeld

Voldoet	Omschrijving	Toelichting
Voldoet	De risicoanalyse vermeldt de grondslag en de doeleinden van de verwerking.	Ja, want op pagina 12 DPIA staat dat de gegevensverwerking voor de volgende 2 doelen geschiedt: Deze gegevensverwerking heeft 2 doelen: 1. Het doel is om te beoordelen in welke mate en hoe digital twinning kan bijdragen aan een datagedreven organisatie; 2. Met name om het monitoren van bezoekersstromen en vastgoedontwikkeling (bijvoorbeeld inzicht soorten winkels en spreiding ervan). De grondslag voor het verwerken van de accountgegevens is de licentieovereenkomst, welke grondslag in art. 6 lid 1 sub b AVG.
Voldoet	De risicoanalyse vermeldt welke gegevens en verwerkingen proportioneel is voor het bereiken van dit doel	Ja, want de proportionaliteits- en subsidiariteitstoets zijn gedaan op pagina 15 DPIA. Daarin is aangegeven dat de genoemde gegevens nodig zijn om de gebruikers van de accounts te kunnen authentiseren.
Voldoet	De risicoanalyse vermeldt of er een minder ingrijpende gegevensverwerking mogelijk is	Ja, want de proportionaliteits- en subsidiariteitstoets zijn gedaan op pagina 15 DPIA. Daarin is aangegeven dat de genoemde gegevens nodig zijn om de gebruikers van de accounts te kunnen authentiseren.
Voldoet	De risicoanalyse bevat een omschrijving van de maatregelen die worden getroffen om de verwerking te beperken tot de ter zake dienende noodzakelijke gegevens	N.v.t. want hierin is de gemeente Helmond afhankelijk van de leverancier Argaleo. De verwerking voldoet aan de vereisten van gegevensminimalisatie (art. 5 lid 1 sub c AVG). (pagina 6 DPIA).

Voldoet	De risicoanalyse bevat een omschrijving van de maatregelen die worden getroffen om te zorgen dat geen function creep[1] optreedt.	N.v.t. want dit systeem verwerkt in zijn primaire functies, namelijk het bieden van een kijkdoos van de stad, geen persoonsgegevens waardoor op de privacy van de inwoners van de gemeente Helmond geen inbreuk wordt gemaakt. (pagina 13 DPIA).
Voldoet	De risicoanalyse bevat een omschrijving van de maatregelen die worden getroffen om ervoor te zorgen dat gegevens niet langer dan noodzakelijk worden opgeslagen in een vorm die het mogelijk maakt om betrokkene te identificeren.	N.v.t. want de verwerking van de persoonsgegevens zit aan de kant van Argaleo, welke partij zelfstandig verwerkingsverantwoordelijk is voor het beheer van de accountgegevens. (pagina 8 DPIA)
Voldoet	De risicoanalyse bevat een omschrijving van de wijze waarop betrokkene (toereikend) wordt geïnformeerd.	N.v.t. want de gemeente Helmond verwerkt in deze applicatie geen persoonsgegevens waarvoor zij verantwoordelijk is. Argaleo is namelijk zelfstandig verwerkingsverantwoordelijk.
Voldoet	De risicoanalyse bevat een omschrijving van hoe betrokkenen hun rechten uit kunnen oefenen: a. rechten van inzage b. recht op rectificatie en verwijdering c. recht op overdraagbaarheid van gegevens ~~d. recht op bezwaar~~ e. recht op beperking van de verwerking	Ja, want dit is beschreven op pagina 21 van de DPIA. Daarin is vermeld dat de betrokkenen hun rechten kunnen uitoefenen door zich met het verzoek te wenden tot info@argaleo.com. Om er zeker van te zijn dat het verzoek door de juiste persoon is gedaan, kan Argaleo vragen om een kopie van het ID-bewijs mee te sturen. Daarbij dient een kopie van de pasfoto te worden gemaakt waarbij de MRZ, het paspoortnummer en het BSN zwart moeten worden gemaakt ter bescherming van de privacy. Argaleo reageert binnen 4 weken op het verzoek. Het recht op bezwaar is hier niet van toepassing aangezien de grondslag hier een licentieovereenkomst betreft (art. 21 lid 1 AVG).
Voldoet	De risicoanalyse beschrijft de relatie met verwerkers	N.v.t. aangezien er ten aanzien van de gemeente Helmond geen verwerkers zijn, omdat Argaleo zelfstandig verwerkingsverantwoordelijk is. Er is wel wat beschreven over de verwerkers van Argaleo als onderdeel van de risicoanalyse op pagina 8, 9, 11 en 22 van de DPIA.
Voldoet	De risicoanalyse beschrijft de waarborgen omtrent internationale doorgifte	N.v.t. alle data blijft binnen de Europese Economische Ruimte.
Voldoet	De risicoanalyse vermeldt of voorafgaande raadpleging nodig is.	N.v.t. er is geen hoog risico dat niet kan worden gemitigeerd.

Ad 3 de risico's voor de rechten en vrijheden van betrokkenen

Voldoet	Omschrijving	Toelichting
Voldoet	De risicoanalyse brengt de risico's voldoende in beeld.	Ja, want de informatiebeveilingsrisico's zijn benoemd op pagina 13 en 14 van de DPIA. Zo is er een risico benoemd m.b.t. het feit dat Digi Twin gebruikmaakt van TLS 1.2. in plaats van TLS 1.3., maar ook het feit dat SAML niet moet worden gebruikt als Single Sign On-mechanisme, maar Federated Login of twee-factor-authenticatie.

[1] function creep is wat er gebeurt als we technologie en systemen gebruiken op een andere manier dan in de eerste instantie eigenlijk bedoeld is, met name wanneer het nieuwe doel resulteert in een inbreuk op de privacy.

Voldoet	De bedreigingen die kunnen leiden tot onrechtmatige toegang zijn benoemd. De mogelijke gevolgen voor de rechten en vrijheden van betrokkenen zijn geïdentificeerd. Ze zijn benoemd vanuit het perspectief van betrokkenen en er is daarbij ook gedacht aan de gevolgen die dit heeft op het recht op: • zelfstandigheid (bijvoorbeeld de mogelijkheid om bepaalde handelingen uit te voeren); • vrij blijven van stigmatisering (bijvoorbeeld niet op een bepaalde wijze behandeld worden op basis van bepaalde kenmerken); • gelijkheid (bijvoorbeeld het op dezelfde wijze benaderd worden als andere betrokkenen); • vrij blijven van manipulatie (bijvoorbeeld niet beïnvloed worden op gedrag op basis van een (afwijkend) levenspatroon); • integriteit (verlies van eigenheid, waardigheid en ongeschondenheid, niet jezelf kunnen zijn, je moeten aanpassen aan wat anderen vinden hoe je moet zijn); • ongestoord leven (waarbij het bijvoorbeeld kan gaan om identiteitsfraude of (onaangenaam) afbreken van rust en stilte). • eigenwaarde (bijvoorbeeld geen afbreuk aan persoonlijkheid). • autonomie (bijvoorbeeld geen beperking van de vrijheid om eigen regels te volgen) Vooral van zaken als stigmatisering, ongelijkheid, manipulatie en niet ongestoord kunnen leven kunnen betrokkenen last hebben.	De mogelijke gevolgen voor de rechten van de betrokkenen zijn hier heel laag, aangezien er geen persoonsgegevens worden verwerkt in de primaire functie van Digital Twin. Het gaat hier slechts om inloggegevens waarbij een eventueel hack slechts vervelend is voor de accounthouders, maar er is verder geen groot risico voor de betrokkenen, temeer wanneer Digital Twin kan worden aangesloten op de Helmondse Azure Active Directory. De verdere risico's zijn weergegeven in de quickscan.

	• Daarnaast zijn de risico's voor de organisatie benoemd.	
Voldoet	De waarschijnlijkheid en ernst zijn ingeschat.	Ja, deze zijn gekwantificeerd op pagina 29 t/m 31 van de DPIA, en in de quickscan.
Voldoet	De bedreigingen die kunnen leiden tot ongewenste wijziging zijn benoemd. De mogelijke gevolgen voor de rechten en vrijheden van betrokkenen zijn geïdentificeerd. Ze zijn benoemd vanuit het perspectief van betrokkenen en er is daarbij ook gedacht aan de bij het vorige punt genoemde gevolgen. Daarnaast zijn de risico's voor de organisatie benoemd	Ja, deze zijn gekwantificeerd op pagina 29 t/m 31 van de DPIA en in de quickscan.
Voldoet	De waarschijnlijkheid en ernst zijn ingeschat.	Ja, deze zijn gekwantificeerd op pagina 29 t/m 31 van de DPIA en in de quickscan.
Voldoet	De bedreigingen die kunnen leiden tot het niet beschikbaar zijn van gegevens zijn benoemd. De mogelijke gevolgen voor de rechten en vrijheden van betrokkenen zijn geïdentificeerd. Ze zijn benoemd vanuit het perspectief van betrokkenen en er is daarbij ook gedacht aan de bij het vorige punt genoemde gevolgen. Daarnaast zijn de risico's voor de organisatie benoemd	Ja, deze zijn gekwantificeerd op pagina 29 t/m 31 van de DPIA en in de quickscan.
Voldoet	De waarschijnlijkheid en ernst zijn ingeschat.	Ja, deze zijn gekwantificeerd op pagina 29 t/m 31 van de DPIA en in de quickscan.

Ad 4 de maatregelen worden benoemd

Voldoet	Omschrijving	Toelichting
Voldoet	De beoogde maatregelen om de risico's aan te pakken worden bepaald en zijn voldoende.	Ja, deze maatregelen zijn in dit document opgenomen als 'oplegnotitie'.

Ad 5 terugkoppeling proceseigenaar

Onder deze kop heeft de proceseigenaar de gelegenheid om aan de FG/CISO terugkoppeling te verschaffen over de implementatie van het advies. Dit verloopt volgens het pas toe of leg uit principe

(ptolu) waarbij de proceseigenaar de mogelijkheid heeft om het advies over te nemen, of nader te onderbouwen waarom het advies niet wordt overgenomen.

Reactietermijn proceseigenaar: 11 augustus 2023
2. Stel een afdelingsmanager aan als proceseigenaar aan die tijdens en na het project de verantwoordelijkheid op zich neemt voor het beheer van Digital Twin. Het is zeer sterk aan te raden dat dit de afdelingsmanager is van de afdeling die het meest gebruik zal gaan maken van de Digital Twin.
Reactie proceseigenaar:
4. Vraag bij de leverancier na of het mogelijk is om Digital Twin te koppelen aan de Helmondse Azure Active Directory omgeving. Wanneer dat niet mogelijk blijkt te zijn, dient twee-factor-authenticatie te worden ingesteld in combinatie met Federated Login. Het is af te raden om gebruik te maken van SAML. Op die manier wordt de autorisatie doorgegeven waarbij het wachtwoord en de gebruikersnaam beschermd, terwijl dat bij SAML niet het geval is.
Reactie proceseigenaar:
6. Neem Digital Twin op in de autorisatiematrixen op rollenniveau, wijs hiervoor een functioneel beheerder aan die deze applicatie zal gaan beheren.
Reactie proceseigenaar:
7. Vraag aan de leverancier of er actuele plannen zijn om over te stappen op TLS 1.3, en verzoek om dat zo snel mogelijk te doen wanneer hiertoe nog geen plannen zijn.
Reactie proceseigenaar:

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	1, 2, 3

Afdeling/Programma:	Altijd Verbonden
Onderwerp:	Veilig e-mailen
Datum:	13 februari 2024

Aanleiding

De gemeente Helmond heeft veilig e-mailen ingericht. Ze heeft daarnaast een specifiek e-mailbeleid (E-mailbeleid – uitwisseling persoonlijke gezondheidsinformatie) opgesteld. Dit beleid moet zorgen voor een zo veilig en betrouwbaar mogelijke uitwisseling van persoonlijke gezondheidsinformatie (artikel 3.29 van NTA 7516:2019).

Conclusie

Het beleid bevat goede uitgangspunten om veilige en betrouwbare uitwisseling van persoonlijke gezondheidsinformatie via e-mail te waarborgen. Dit beleid voorziet niet in:

- Een werkwijze rondom veilig e-mailen in het algemeen
- Een werkwijze rondom veilig chatgebruik
- Duidelijke instructies voor medewerkers.

Advies aan directie

- Stel het beleid vast.
- Geef de afdelingsmanager Sociaal Domein de opdracht om:
    - Werkinstructies op te stellen voor medewerkers
    - Te monitoren op naleving van het beleid en hierover verantwoording af te leggen
- Geef de afdelingsmanager IVA opdracht om:
    - Een algemeen beleid voor veiig e-mail en chatgebruik op te stellen.

5.1.2e, FG
5.1.2e, CISO

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens geanonimiseerd op grond van:

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

Afdeling Sociaal Domein
Onderwerp: Review JIKP
Datum: 6 maart 2024
Djuma: 51892136

Aanleiding

In 2019 heeft de gemeente Helmond de DPIA opgesteld ten behoeve van het JIKP. ((jongeren in een kwetsbare positie). De gemeente Deurne heeft (als samenwerkende partner), deze DPIA[1] ontvangen. Zij hebben nu gevraagd of de gemeente Helmond deze DPIA wil reviewen en zij het vernieuwde exemplaar kunnen ontvangen.

De DSPO heeft de uitgevoerde DPIA voorzien van opmerkingen (documentnummer 51892211) en addendum opgesteld 51892208).

Conclusie

De review is geen inhoudelijke beoordeling van de uitgevoerde DPIA.
De uitgevoerde DPIA voldoet niet aan eerdere adviezen van de FG van de gemeente Helmond.
Er kan niet worden vastgesteld dat voldoende maatregelen zijn getroffen om de risico's voor betrokkenen terug te brengen tot een acceptabel niveau.

Toelichting

In 2019 heeft een advies uitgebracht over het JIKP (zie bijlage 1)[2]. De gemeente Helmond heeft vervolgens een DPIA uitgevoerd. Deze DPIA[1] heeft de FG ontvangen, zij heeft indertijd met de uitvoerders van de DPIA afgesproken dat zij nog geen advies zou uitbrengen. De reden hiervoor was dat de RMC taak is gedelegeerd aan de GGD en de gemeente Helmond deze taak in mandaat uitvoert. De ondersteunende applicatie bevindt zich in Eindhoven. Met andere woorden de onderlinge verhoudingen en verantwoordelijkheden zijn niet duidelijk en dat brengt (grote) risico's met zich mee. Er is afgesproken dat een uitwerking van de verantwoordelijkheden zou worden opgepakt en dat de DPIA vervolgens ter advisering zou worden voorgelegd (zie bijlage 2).
Dit is niet meer gebeurd. De FG heeft wel in een mail aangegeven wat er ontbrak in de voorgelegde DPIA[1.] . Dit is dus hetzelfde document als waar nu een review op heeft plaatsgevonden.
(en waar nu een review op heeft plaatsgevonden).

6 maart 2024
5.1.2e
Functionaris voor de gegevensbescherming

[1] DPIA, v1.2 november 2019
[2] Zie ook Verseon: 34104197

Bijlage 1

Advies: FG aan de proceseigenaar Leerplicht
Inzake: uitvoeren DPIA aanschaf monitor JIKP

Advies

- Om de benodigde kennis op gebied van DPIA uit te breiden adviseer ik de DPIA niet extern uit te laten voeren.
- Omdat in de gemeente Eindhoven exact hetzelfde vraagstuk heeft gespeeld adviseer ik de DPIA van de gemeente Eindhoven als basis te gebruiken en aan te passen aan de Helmondse situatie.
- De FG van Eindhoven heeft over de DPIA in Eindhoven geadviseerd en een aantal aanbevelingen gedaan, ik adviseer deze aanbevelingen mee te nemen in de in Helmond uit te voeren DPIA. Voor wat betreft de verder uit te werken beveiliging van de informatie adviseer ik gebruik de maken van de risico inventarisatietool van de gemeente Helmond.
- Ik adviseer daarnaast in de DPIA aandacht te besteden aan het vraagstuk wie verantwoordelijk is voor de verwerking van de persoonsgegevens (GGD of gemeente) en de daarmee samenhangende risico's en maatregelen om deze risico's weg te nemen.
- Ik adviseer in de DPIA aandacht te besteden aan het risico dat er onjuiste gegevens worden verwerkt en de maatregelen die worden getroffen om de datakwaliteit te garanderen.
- Tot slot adviseer ik de DPIA uit te voeren voordat wordt gestart met de aanbesteding en om in ieder geval de service manager te betrekken bij de aanbesteding.

Aanleiding

Met ingang van 1 januari 2019 is de Wet educatie en beroepsonderwijs, en andere onderwijswetgeving, aangepast. Als gevolg van deze wetswijziging is de RMC taak van de gemeente uitgebreid[3]. Jongeren in kwetsbare posities moeten optimaal worden ondersteund bij het vinden van een passende plek, dankzij een sluitend regionaal vangnet van partijen uit onderwijs, gemeenten, zorg en arbeid.
Ter ondersteuning van een sluitende gezamenlijke aanpak wil men een applicatie aanschaffen waar zowel ambtenaren als generalisten, functionarissen van werkbedrijven en onderwijsprofessionals toegang toe hebben.
Aangezien het hier gaat om een nieuwe verwerking met hoge privacy risico's is het uitvoeren van een DPIA noodzakelijk. Aan de FG is advies gevraagd over de wijze waarop de DPIA moet worden uitgevoerd.

Toelichting

In de gemeente Eindhoven speelt hetzelfde, zij hebben reeds een applicatie aangeschaft en een DPIA uitgevoerd. De FG van Eindhoven heeft over deze DPIA geadviseerd (zie bijlagen). Aangezien de risico's die betrokkenen lopen overeenkomen kan de in Eindhoven uitgevoerde DPIA met de aanbevelingen van de FG in Eindhoven worden overgenomen en aangepast aan de Helmondse situatie.

Ik heb de in Eindhoven uitgevoerde DPIA beoordeeld en ik mis maatregelen om de datakwaliteit te waarborgen. Verschillende partners hebben toegang tot de informatie, voegen informatie toe en gebruiken deze informatie. Het risico dat er onjuiste gegevens worden verwerkt neemt daardoor toe.

[3] nieuwe volzin in artikel 8.3.2, eerste lid, Wet educatie en beroepsonderwijs, 162b, eerste lid, Wet op de expertisecentra en 118h eerste lid, Wet op het voortgezet onderwijs

Daarnaast heeft het college heeft in 2017 besloten de RMC taken te delegeren aan de GGD[4]. Daarmee hebben zij de verantwoordelijkheid voor het goed uit voeren van deze taken overgedragen aan de GGD. Dit roept de vraag op of deze nieuwe RMC taak ook is gedelegeerd aan de GGD en daarmee over de vraag wie verwerkingsverantwoordelijke is (De GGD of de gemeente) De DPIA hoort hier uitsluitsel over te geven en de hiermee samenhangende risico's in beeld te brengen. Zie mijn eerdere advies over de delegatie van de RMC taken aan de GGD[5] en de analyse gemaakt naar aanleiding van de aanschaf van de leerlingenregistratie (CLR)[6].

Doel van de DPIA is de risico's van een verwerking van persoonsgegevens in beeld te brengen, voordat die verwerking plaatsvindt. Het gaat daarbij om risico's op gebied van privacy en informatieveiligheid van de verwerking voor betrokkenen (degenen wiens persoonsgegevens worden verwerkt). Door de DPIA in een zo vroeg mogelijk stadium uit te voeren kan direct rekening gehouden worden met de uitkomsten. Wanneer de risico's op inbreuk op de privacy pas in een later stadium worden onderkend, is de kans groot dat noodzakelijke aanpassingen veel tijd en geld kosten. Dit is ook de reden dat ik adviseer de DPIA uit te voeren voordat de aanbesteding wordt gestart. In de wensen en eisen kan dan rekening worden gehouden met de uitkomsten van de DPIA. Op zijn minst dient de servicemanager betrokken te worden bij het inkooptraject zodat wordt geborgd dat in de aanbesteding privacy en informatiebeveiligingseisen voldoende gewicht krijgen.

Analyse bevoegdheid

Uit de gemeenschappelijke regeling blijkt dat alle RMC taken bij de GGD neer te leggen. Deze RMC taken zijn vastgelegd in een aantal artikelen [5]. De nieuwe RMC taak is met deze wetswijziging niet vastgelegd in een nieuw artikel, de bestaande artikelen zijn gewijzigd. Dit betekent dat de wetswijziging onder het bestaande delegatiebesluit valt, oftewel dat de GGD ook de verwerkingsverantwoordelijke is van deze nieuwe taak.

In de DPIA van Eindhoven is men er van uitgegaan dat de verantwoordelijkheid van de verwerking bij de gemeente Eindhoven zou liggen, op grond van bestuurlijke besluitvorming[7]. Ik heb hiervan geen bewijzen gezien en in ieder geval zou deze besluitvorming dan moeten worden geformaliseerd en leiden tot een aanpassing van de gemeenteschappelijke regeling. De bepalingen van de gemeenschappelijke regeling lijken mij leidend.

De gemeente heeft de GGD RMC taken gedelegeerd en de GGD heeft de uitvoering van deze taken vervolgens gemandateerd aan de leerplichtambtenaren van de gemeente. Daarnaast heeft zij de uitvoering van de rechten van betrokkene[8] gemandateerd aan de gemeente. Dit verandert niets aan het feit dat de GGD verwerkingsverantwoordelijke is en dat de gemeente en de GGD aanvullende afspraken moeten maken over de wijze waarop de gemeente namens de GGD gegevens verwerkt.

11 juli 2019
IVA HM

[4] https://zoek.officielebekendmakingen.nl/stcrt-2017-70565.html en Verseon documentnummer 34105278
[5] Verseon zaaknummer 33927569, document 34021070
[6] Verseon document 33927602 5 artikel 118h van de Wet op het voortgezet onderwijs, artikel 8.3.2 van de Wet educatie en beroepsonderwijs en artikel 162b van de Wet
op de expertisecentra
[7] Informatie van de FG van Eindhoven d.d. 1 juli 2019
[8] Artikel 12 tot en met 21 en 77 van de AVG

Bijlage 2

ddd **o:** 5.1.2e [5.1.2e @helmond.nl]; 5.1.2e [5.1.2e @helmond.nl]; 5.1.2e [5.1.2e @helmond.nl]; 5.1.2e [5.1.2e @helmond.nl]

From: 5.1.2e

Sent: Mon 23-12-2019 10:26:02

Importance: Normal

Subject: DPIA rapportage monitor jikp

Received: Mon 23-12-2019 10:26:00

Dag 5.1.2e ,

Van 5.1.2e kreeg ik de DPIA, omdat de uitwerking van het feit dat de taak is gedelegeerd aan de GGD nog ontbreekt (wordt uitgewerkt in het eerste kwartaal van 2020) sprak ik af dat ik nog geen advies uitbreng. Na uitwerking door de werkgroep wordt de DPIA opnieuw aan mij voorgelegd.

Inmiddels heb ik de DPIA die ik van 5.1.2e kreeg wel globaal bekeken.

Ik zie dat het dezelfde DPIA is als die van Eindhoven, met dien verstande dat het is aangepast aan het Helmondse proces. Er zijn verder de volgende inhoudelijke aanpassingen gedaan:

1. de toevoeging van de rol van de GGD en dat in het eerste kwartaal van 2020 nadere afspraken worden gemaakt.
2. een uitbreiding van de grondslagen
3. een uitwerking van de grondslag toestemming
4. de uitwerking van werkafspraken in het eerste kwartaal van 2020
5. een uitwerking van het proces datalek.

6. een nadere uitleg over de bewaartermijn Wmo en Jeugdwet

Het is belangrijk om te beseffen dat mijn advies nog niet (volledig) is opgevolgd (ook voor wat betreft andere punten het GGD punt. Dat geef ik je alvast mee zodat hier ook rekening mee gehouden kan worden voordat de DPIA ter advisering aan me wordt voorgelegd.

Het advies is niet opgevolgd voor wat betreft de volgende punten:

1. neem de aanbevelingen van de FG van Eindhoven over
   - I gezamenlijke verantwoordelijkheid en het convenant
     - a borging dat wordt voldaan aan de informatieverplichting (door school blz 14 en 17)
     - b rechten van betrokkenen inclusief recht op bezwaar
     - c het aanstellen van een ketenregisseur
   - II toestemming en hoe te handelen bij ontbreken toestemming en informeren partners hiervan
   - III bewaartermijn hoe wordt geborgd dat gegevens worden gewist
   - V gebruik de risico inventarisatietool (advies van mij) om inzichtelijk te maken hoe invulling wordt gegeven aan het gemeentelijke informatiebeveiligingsbeleid (advies fg Eindhoven)
   - VI Werkinstructies doen recht aan gezamenlijke verantwoordelijkheid en geef kaders en richtlijnen aan verwerkers
2. de verdeling van de verantwoordelijkheden tussen gemeente en GGD
3. aandacht voor het risico dat onjuiste gegevens worden verwerkt

1. <u>Het overnemen van de aanbevelingen van de FG van Eindhoven</u>

Ad I het convenant

sub a, Dit zie ik in het geheel niet terug

sub b, In het convenant is hierover in zeer algemene zin iets opgenomen. De onderliggende afspraken zijn relevant voor het borgen dat betrokkenen ook daadwerkelijk zijn rechten kan uitoefenen.
sub c Dit zie ik in het geheel niet terug

Ad II Toestemming
De FG van Eindhoven adviseert om de grondslag toestemming niet te gebruiken. In de DPIA van Helmond wordt ingegaan op waarom deze grondslag wel wordt gebruikt en onder welke voorwaarden. (zie blz 14). DE FG adviseert ook om vast te leggen hoe er wordt omgegaan met de situatie waarin geen toestemming wordt verleend. Dit zie ik niet terug komen.

Ad III Wissen van gegevens
Dit zie ik niet terug komen

Ad V inzichtelijk maken hoe wordt voldaan aan het gemeentelijke informatiebeveiligingsbeleid.
Dit is niet inzichtelijk gemaakt. de risicoinvenatarisatietool is niet ingevuld

Ad VI het opstellen van Werkinstructies
Aangegeven wordt dat in het eerste kwartaal van 2020 wordt uitgewerkt.

Het convenant bindt partijen en maakt algemene afspraken. Elke partij belooft om op een bepaalde manier te handelen. Het is van belang om te weten (en vast te leggen) welke maatregelen elke convenantpartner en de convenantpartners gezamenlijk hebben getroffen om te borgen dat de afspraken ook worden nagekomen. Het is dus van belang om goede werkinstructies en processen vast te stellen

Ad 2 de verdeling van de verantwoordelijkheden tussen de gemeente en de GGD.

hierover mailde ik al (zie hieronder), deze uitwerking is relevant. Ook voor bijvoorbeeld de bepaling wie de verwerkersovereenkomst moet tekenen.

Ad 3 het verwerken van onjuiste gegevens

Hierover zie ik niets terug komen.

Zie ook Verseon zaak 34104197 voor alle stukken. de mailwisseling met 5.1.2e en deze mail zijn daar ook opgeslagen

Met vriendelijke groet,

5.1.2e
Functionaris voor de gegevensbescherming

IVA/CO
Postbus 950, 5700 AZ, Helmond
Weg op den Heuvel 35, 5701 NV Helmond
Tel. 5.1.2e

https://www.helmond.nl/werkenbij

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	1, 4, 5

Afdeling/Programma: A&E

Onderwerp: Kentekenherkenning voetgangerzones

15 september 2024

Inhoud

Inhoud 1
Aanleiding 2
Conclusie 2
Advies 2
AVG en Wpg 2
AVG (het verlenen van toegang) 2
Wpg (digitale handhaving) 3
Scope: 3
Toelichting 4
1. Doel van de verwerking van persoons- en politiegegevens 4
2. Zowel de AVG als Wpg zijn van toepassing bij kentekenherkenning. 4
2.1 Kentekenherkenning bestaat uit 2 onderdelen: 4
2.2 De levenscyclus en het relevante kader 4
3. De verwerking van persoonsgegevens voor het verlenen van toegang. 5
3.1 Het doel kan op een minder ingrijpende wijze worden bereikt. 5
3.2 De extra gegevensverwerking is proportioneel mits zij beperkt blijft tot de noodzakelijke persoonsgegevens. 6
3.3 Het is niet noodzakelijk om na stap 3 nog persoonsgegevens te verwerken. 6
4 De verwerking van politiegegevens voor het uitvoeren van digitale handhaving. 6
Bijlage 8
1. Toets van de risicoanalyse 8
Bijlage 15
2. Terugkoppeling proceseigenaar 15

Aanleiding

De gemeente heeft in het centrum en in Brandevoort (De Plaetse) gebieden aangewezen als voetgangerszone. Alleen toegelaten voertuigen mogen deze zone inrijden, zodat deze gebieden autoluw blijven. Om uitvoering te geven aan dit beleid, kan de gemeente verkeerskundige maatregelen treffen:

1. *Toegangscontrole vooraf*. Binnenrijden wordt voorkomen met een fysieke barrière (bijvoorbeeld Pollerpalen).
2. *Vaststelling achteraf*. Binnenrijden wordt beïnvloedt door een virtuele barrière. Daarbij wordt achteraf met behulp van een camera op basis van het kenteken (kentekenherkenning) vastgesteld of men inrijdrechten heeft en het dus was toegestaan om binnen te rijden.

Op 22 februari 2022 heeft het college besloten[1] om het gebruik van Pollerpalen (1) te vervangen door kentekenherkenning. Inmiddels is het systeem geïmplementeerd en is op advies van de CISO en FG een risicoanalyse uitgevoerd.

Conclusie

Het besluit van het college om over te gaan tot kentekenherkenning heeft tot gevolg dat er meer persoonsgegevens worden verwerkt. Dit betekent dat het besluit een grotere impact heeft op de privacy van betrokkenen. Alhoewel het college bij haar besluit niet expliciet deze gevolgen heeft meegewogen, kan worden geconcludeerd dat het college deze toename van verwerking van persoonsgegevens proportioneel vindt. Deze conclusie wordt gedeeld door FG en CISO, mits de verwerking van persoonsgegevens beperkt blijft tot het noodzakelijke. Hiervoor zijn aanvullende maatregelen nodig.

Om kentekenherkenning mogelijk te maken is bij Brickyard de applicatie ‘Bluebrick’ afgenomen. Dit betreft een SAAS oplossing. De FG en CISO stellen vast dat Brickyard voldoende toereikende beveiligingsmaatregelen heeft getroffen. Dit stellen zij vast aan de hand van de volgende documenten:

- K1-rapport Brickyard implementatie, Document: 51841917;
- SLA Definitief 26-06-2023, Document: 51841803;
- Brickyard ISAE 3402 - Report (2021), Document: 51841905;
- ISOIEC-27001 Certificaat, Document: 51841906;
- Waysis verklaring Bink Advies ISO 27001 audit, Document: 51841920;
- Verklaring van Toepasselijkheid ISO 27001 Waysi, Document: 51841919;

Advies

AVG en Wpg

1. Breng het register van verwerkingen in overeenstemming met de aangepaste manier van werken. Doe dit zowel voor wat betreft de Avg als de Wpg.
2. Neem op de informatiepagina een verwijzing op naar de privacyverklaring van de gemeente Helmond.

AVG (het verlenen van toegang)

1. Bewaar de persoonsgegevens zo kort mogelijk door ze
    a. onmiddellijk te verwijderen na vaststelling dat er geen sprake is van een overtreding.

[1] Zie zaak 50466429

   b. onmiddellijk over te dragen en te behandelen als politiegegevens na vaststelling dat er sprake is van een overtreding.
2. Pas daarom de bewaartermijn van “niet-overtreders” aan van 72 uur naar 0 uur na vaststelling dat men terecht toegang heeft verkregen tot de autoluwe zone.
3. Richt autorisaties zodanig in, dat niemand toegang heeft tot de persoonsgegevens in de periode van vastleggen van de toegang tot de autoluwe zone, tot vernietiging of overdragen van deze gegevens.

Wpg (digitale handhaving)

1. Werk conform het beoordelingskader parket[2]
2. Beschrijf de digitale handhavingsprocessen en leg ze vast in een procesplaat in Bizagi en publiceer deze op de Helmondse Processenpagina.
3. Beschrijf rollen, procedures en/of werkinstructies, om te borgen dat:
   a. Er gewerkt wordt conform het beoordelingskader parket[2]
   b. Er alleen politiegegevens worden verwerkt om digitaal te kunnen handhaven.
   c. Er geen bovenmatige politiegegevens worden verwerkt.
   d. Er geen vermenging ontstaat tussen persoonsgegevens en politiegegevens.
4. Voer periodiek controle’s uit op doelbinding en noodzakelijkheid van de gegevensverwerking en rapporteer hierover.
5. Stel een autorisatiematrix op (voor zover nog niet aanwezig) en werk conform deze autorisatiematrix.
6. Voer periodiek controle’s uit op accounts, rollen en rechten.
7. Besteedt aandacht aan bewustwording en de geheimhoudingsplicht met betrekking tot de verwerking van politiegegevens.
8. Mocht de dienstverlener PCH in de toekomst worden ingeschakeld om boa’s te leveren, breng dan opnieuw de risico’s en de noodzakelijke maatregelen in beeld en sluit een verwerkersovereenkomst af.

Scope:

In scope van deze DPIA zijn:

- De persoonsgegevens die middels het camerasysteem worden verwerkt, inclusief de bijbehorende applicaties.
- De politiegegevens die door de Buitengewone opsporingsambtenaren (BOA’s) worden verwerkt.
- Informatiebeveiligingsmaatregelen die door Brickyard zijn genomen.

Out-of-scope van deze DPIA zijn:

- De persoonsgegevens die worden verwerkt ten behoeve van de registratie van ontheffinghouders.
- De processen die door CJIB en Cannock Chase worden verricht naar aanleiding van de genomen foto’s van potentiële overtreders.

[2] Beoordelingskader Parket CVOM voor digitale handhaving bij geslotenverklaringen en voetgangersgebieden d.d. 18 april 2023, document: 51874664.

Toelichting

1. Doel van de verwerking van persoons- en politiegegevens

Het doel van de verwerking is:

- Een autoluw centrumgebied borgen;
- Het gedrag van de bestuurders beïnvloeden.

2. Zowel de AVG als Wpg zijn van toepassing bij kentekenherkenning.

2.1 Kentekenherkenning bestaat uit 2 onderdelen:

1. *Verlening van toegang, door vaststelling achteraf.*

Er is sprake van een virtuele barrière omdat men weet dat men gecontroleerd wordt. De praktijk[3] leert dat een virtuele barrière werkt, mits de verkeersmaatregel logisch is en duidelijk staat aangegeven. Dit betekent dat er daadwerkelijk weinig bestuurders zonder inrijdrechten het autoluwe gebied binnenrijden. De enkeling die dat wel doet begaat een overtreding.

2. *Digitale handhaving.*

Voor de effectiviteit van de verkeersmaatregel is het van belang dat er daadwerkelijk wordt opgetreden bij een overtreding. De keuze voor vaststelling achteraf impliceert daarom ook een keuze voor digitale handhaving door Buitengewone opsporingsambtenaren van de gemeente.

2.2 De levenscyclus en het relevante kader

Per onderdeel is een ander kader van toepassing[4]:

Verlening van toegang	Kader
1. De camera fotografeert de kentekens van alle voertuigen die het autoluw gebied inrijden. 2. De foto's worden opgeslagen in een database in Bluebrick, ze worden (minimaal) 72 uur bewaard 3. Deze database vergelijkt deze kentekens, door middel van een koppeling, met de kentekens met inrijdrechten die zijn geregistreerd in BLOXX.	• Er is sprake van persoonsgegevens. • Algemene verordening gegevensbescherming (AVG). • Artikel 149 en 150 van de Wegenverkeerswet 1994. • Artikel 87 Reglement verkeersregels en verkeerstekens 1990 (RVV 1990). • Beleidsregels ontheffingen geslotenverklaring en voetgangszones Helmond 2024. • Verkeersbesluit 2104 (document 50898178 en 50898179).
Digitale handhaving	Kader
4. Zodra een voertuig zonder inrijdrechten wordt geregistreerd (overtreder), slaat het systeem het kenteken (versleuteld) op. 5. De buitengewoon opsporingsambtenaar (BOA) van de gemeente controleert de foto's van overtreders. 6. De BOA blurt de foto, zodat enkel de relevante politiegegevens zichtbaar zijn en er wordt voldaan aan de vereisten van een digitale overtredingsopname[5].	• Er is sprake van politiegegevens. • Wet politiegegevens. • Artikel 10 RVV 1990. • Artikel 62 RVV 1990 juncto Bijlage 1 hoofdstuk C (geslotenverklaring) • Artikel 6.2 van de Beleidsregels Buitengewoon Opsporingsambtenaar. • Onderdeel 10 van de bijlage bij de Regeling domeinlijsten Buitengewoon opsporingsambtenaar.

[3] Afweging en advies stadsafsluiting Helmond. Documentnummer 50898175
[4] zie ook document 51841337 Setting of the scene Camerahandhaving voetgangerszones
[5] Bijlage 2 van het beoordelingskader parket CVOM voor digitale handhaving bij geslotenverklaringen en voetgangersgebieden d.d. 18 april 2023, zie document: 51874664.

7. Als er sprake is van een overtreding, maakt de BOA de keuze voor het versturen van een waarschuwing of het opleggen van een boete. 8. BOA geeft (handmatig) besluit door aan: • Cannock Chase (waarschuwing) of • CJIB (boete). 9. Versturen waarschuwing (Cannock Chase) of boete (CJIB).	• Beoordelingskader Parket CVOM voor digitale handhaving bij geslotenverklaringen en voetgangersgebieden d.d. 18 april 2023, document: 51874664.

3. De verwerking van persoonsgegevens voor het verlenen van toegang.

Om toegang tot een autoluw gebied te reguleren is het noodzakelijk om persoonsgegevens te verwerken. Dit geldt voor zowel vaststelling achteraf (kentekentoegang) als bij toegangscontrole vooraf (pollerpalen).

3.1 Het doel kan op een minder ingrijpende wijze worden bereikt.

Zowel bij toegangscontrole vooraf als bij vaststelling achteraf worden persoonsgegevens verwerkt. De toegangscontrole vooraf is minder ingrijpend op de persoonlijke levenssfeer van betrokkenen. Dit terwijl ook met toegangscontrole vooraf het doel kan worden bereikt.

1. Ontheffinghouders:
Er is een registratie van ontheffinghouders nodig om de toegang te reguleren. De registratie van ontheffinghouders valt buiten scope van dit advies.

1. *Toegangscontrole vooraf* kan plaatsvinden met behulp van een middel waarover belanghebbende zelf beschikt (bv een pasje of een sleutel). Het is **niet** noodzakelijk dat dit middel persoonsgegevens bevat.
2. Om *vaststelling achteraf* mogelijk te maken is het **wel** noodzakelijk om persoonsgegevens te verwerken. Bij vaststelling achteraf worden namelijk elke keer wanneer een ontheffinghouder het gebied binnenrijdt een foto gemaakt en opgeslagen. Deze foto bevat:
   a. Het kenteken, zodat kan worden gecontroleerd of men een ontheffing heeft.
   b. Alle informatie die nodig is voor digitale handhaving[3].

Ad 2b: Omdat vooraf niet bekend is of een overtreding wordt begaan, worden bij inrijden van iedere bestuurder deze gegevens verwerkt. De gegevens worden vervolgens:

- Vernietigd als blijkt dat er geen overtreding is begaan
- Bewaard als blijkt dat er een overtreding is begaan.

Dit betekent dat er (tijdelijk) gegevens van de ontheffinghouders worden verwerkt waarvan pas achteraf wordt vastgesteld dat ze toch niet noodzakelijk zijn.

Derden (toevallige voorbijgangers, bestuurders of inzittenden):

1. Bij *Toegangscontrole vooraf* worden er **geen** persoonsgegevens van derden verwerkt.
2. Om *vaststelling achteraf* wordt er gebruik gemaakt van camera's, daarbij **bestaat het risico** dat er ook persoonsgegevens van derden worden verwerkt.

Ad 2: Er wordt gebruik gemaakt van camera's die zijn uitgerust met, kort gezegd, ANPR-techniek. De afkorting ANPR staat voor Automatic Number Plate Recognition (automatische kentekenplaatherkenning). ANPR-camera's zijn in staat om voertuigkentekens als zodanig te herkennen en hebben dan ook primair tot doel om in elk geval voertuigkentekens te fotograferen. De meeste foto's die met een ANPR-camera worden genomen zijn zogenoemde overzichtsfoto's. Dit zijn foto's waarop het voertuig te zien is plus een klein deel van de omgeving. Op een deel van die overzichtsfoto's is de bestuurder in beeld (en soms ook een of meer andere inzittenden). Een veel kleiner aandeel wordt gevormd door de foto's waarop deze personen (bestuurders en inzittenden)

herkenbaar voorkomen[6]. Deze foto's worden opgeslagen in een database en pas in de digitale handhavingsfase, wordt deze niet relevantie informatie op de foto's weggehaald door de BOA (door middel van blurring).

Bij vaststelling achteraf worden er dus meer persoonsgegevens van ontheffinghouders verwerkt dan bij toegangscontrole vooraf. Voor derden geldt dat er met de vaststelling achteraf een risico ontstaat dat er persoonsgegevens over hen worden verwerkt. Er is pas sprake van een persoonsgegeven indien betrokkenen ook daadwerkelijk worden geïdentificeerd. Het risico op identificatie is klein, omdat de foto's in principe niet worden bekeken in de eerste fase (toegangscontrole).

3.2 De extra gegevensverwerking is proportioneel mits zij beperkt blijft tot de noodzakelijke persoonsgegevens.

Het college heeft besloten om de toegangscontrole vooraf te vervangen door toegangscontrole achteraf. Men heeft hiervoor gekozen omdat een fysieke barrière met zich meebrengt dat:

- Er sprake is van aanrijdingen en (letsel)schade
- Hulpdiensten de autoluwe gebieden minder goed kunnen bereiken

Het college heeft deze belangen (kennelijk) zwaarder laten wegen dan de privacybelangen van de betrokken ontheffinghouders. Alhoewel het college haar afweging tussen deze belangen niet inzichtelijk heeft gemaakt in haar besluit vindt zij de toename van gegevensverwerkingen kennelijk proportioneel.

De FG volgt het college hierin, mits de verwerking van persoonsgegevens beperkt blijft tot datgene wat noodzakelijk is voor deze manier van reguleren van de toegang.

3.3 Het is niet noodzakelijk om na stap 3 nog persoonsgegevens te verwerken.

Zodra de kentekens zijn vergeleken met de inrijdrechten (stap 3) is er:

- Of sprake van een overtreding en zijn de gegevens niet langer persoonsgegevens maar politiegegevens.
- Of sprake van terechte toegang en is de verwerking van persoonsgegevens niet langer noodzakelijk. Dit betekent dat de verwerking op dat moment dient te stoppen, wat ook betekent dat de persoonsgegevens dienen te worden vernietigd.

Voor derden geldt dat er helemaal geen noodzaak bestaat om persoonsgegevens te verwerken. Dat betekent dat er maatregelen moeten worden getroffen om te voorkomen dat personen worden geïdentificeerd in de fase "toegangscontrole".
Dat kan worden bereikt door te zorgen dat:

- Foto's zo snel mogelijk worden verwijderd (als er geen sprake is van een overtreding) of worden overgedragen en behandeld als politiegegevens (als er wel sprake is van een overtreding);
- Niemand toegang heeft tot de foto's in de periode tussen maken van de opname en het verwijderen of overdragen van de foto.

4 De verwerking van politiegegevens voor het uitvoeren van digitale handhaving.

Digitaal handhaven is slechts mogelijk op overtreding van het RVV 1990 en na instemming van Parket Centrale Verwerking Openbaar Ministerie(CVOM)[7]. Om de kwaliteit van de digitale handhaving te borgen en een eenduidige toetsing op proportionaliteit mogelijk te maken heeft het Parket CVOM een beoordelingskader voor digitale handhaving bij geslotenverklaringen en voetgangersgebieden

[6] bron: Meer informatie ANPR-foto's | Publicatie | Openbaar Ministerie (om.nl)
[7] Onderdeel 10 van de bijlage bij de Regeling domeinlijsten Buitengewoon opsporingsambtenaar

opgesteld. Een aanvraag wordt in beginsel alleen toegewezen als aan de uitgangspunten van dit kader wordt voldaan[8].

Er is echter geen procesbeschrijving. Rollen zijn niet beschreven. Het ontbreken van een beschrijving van het proces en de rollen brengt het risico met zich mee dat er meer gegevens worden verwerkt dan noodzakelijk bijvoorbeeld omdat er onduidelijkheid bestaat over de rol of omdat het te lang duurt voordat foto's worden bekeken of geblurred. De genomen maatregelen om de verwerking van persoonsgegevens te beperken tot de ter zake dienende noodzakelijk gegevens zijn daarom niet toereikend.

[8] Het beoordelingskader parket CVOM voor digitale handhaving bij geslotenverklaringen en voetgangersgebieden d.d. 18 april 2023.

Bijlage

1. Toets van de risicoanalyse

Een risicoanalyse heeft betrekking op informatieveiligheid en privacy. Voor privacy geldt dat de AVG een aantal vereisten stelt aan de uit te voeren risicoanalyse. Dit zijn de volgende vereisten:

1. Een systematische beschrijving van de beoogde verwerking en de doeleinden;
2. Een beoordeling van de noodzaak en de evenredigheid;
3. Een beoordeling van de risico's voor de rechten en vrijheden van betrokkenen;
4. Een overzicht van beoogde maatregelen om deze risico's aan te pakken.

Ad 1 een systematische beschrijving

1	Omschrijving	Toelichting

1.1.	De risicoanalyse vermeldt: de persoonsgegevens die worden verwerkt	• De volgende persoonsgegevens worden verwerkt:
		  ○ Van de verkeersdeelnemer, die het gebied inrijdt:
		  - Beeldmateriaal;
		  - Contactgegevens;
		  - Identiteitsgegevens;
		  - Locatiegegevens;
		  - Persoonlijke gegevens.
		  ○ Van de toevallige voorbijganger en inzittenden (derden):
		  - Beeldmateriaal.
		• De volgende politiegegevens worden verwerkt:
		  ○ Van de overtreder
		  - Beeldmateriaal;
		  - Contactgegevens;
		  - Identiteitsgegevens;
		  - Locatiegegevens;
		  - Persoonlijke gegevens.

1.2	De risicoanalyse vermeldt: de ontvangers van deze persoonsgegevens	• Ontvangers van de Persoonsgegevens zijn:
		  - Niemand
		• Ontvangers van de Politiegegevens zijn:
		  - Cannock Chase
		  - CJIB
		
		(zie pagina 8 DPIA, document 51883287)

1.3.	De risicoanalyse vermeldt: de periode gedurende welke de persoonsgegevens worden bewaard	• Persoonsgegevens, AVG:
		  - De foto's worden na 72 uur verwijderd uit het systeem.
		
		Noot:
		  - dit is langer dan noodzakelijk.
		• Politiegegevens, Wpg:
		  - 5 jaar, de gemeente moet als opsporingsinstantie de digitale opnames gedurende een periode van 5 jaar bewaren (Beoordelingskader parket[2] en art. 8 Wpg).
		  - Verwijderde gegevens worden gedurende 5 jaar bewaard ten behoeve van klachten en verantwoording (artikel 14 lid 1 Wpg)
		  - Daarna (na 10 jaar dus) worden de gegevens definitief vernietigd (art. 14 lid 2 Wpg).
		
		(zie pagina 9 DPIA, document 51883287 voor een toelichting)

1.4.	De risicoanalyse bevat een functionele beschrijving van de verwerking	• AVG en Wpg Zie voor de levenscyclus: “Setting of the scene Camerahandhaving voetgangerszones”, Doc: 51841337 en de toelichting in dit document: “De levenscyclus en het relevante kader”. Noot: - Er bestaat risico op rolonduidelijkheid, omdat een procesbeschrijving van de huidige werkwijze ontbreekt. - Er bestaat daarom ook een risico dat persoonsgegevens en politiegegevens met elkaar vermengd raken.
1.5.	De risicoanalyse bevat de activa waarop persoonsgegevens steunen (hardware, software, netwerken, mensen, papier of papiertransmissiekanalen)	• AVG en Wpg Zie pagina 10 DPIA document 51883287, waar dit is beschreven aan de hand van het MAPGOOD principe. Het betreft hier een SAAS-applicatie waarbij het merendeel van de hardware en software wordt beheerd door de leverancier (Brickyard). Noot: - Een beschrijving van de organisatorische maatregelen ontbreekt.

Ad 2 De noodzaak en de evenredigheid wordt beoordeeld

Voldoet	Omschrijving	Toelichting
2.1.	De risicoanalyse vermeldt de grondslag en de doeleinden van de verwerking.	• Persoonsgegevens, AVG: - Grondslag: art. 6 lid 1 sub e AVG (taak van algemeen belang). Zie voor de relevante wetgeving paragraaf 2.1. De levenscyclus en het relevante kader. - Doel: Beïnvloeding van het gedrag van bestuurders, zodat de aangewezen gebieden daadwerkelijk, conform het gemeentelijke beleid, autoluw blijven. • Politiegegevens Wpg: - De gegevens zijn noodzakelijk voor de uitvoering van de dagelijkse politietaak (artikel 8 Wpg) Zie ook paragraaf 2.1 De levenscyclus en het relevante kader en paragraaf 4 De verwerking van politiegegevens voor het uitvoeren van digitale handhaving.
2.2.	De risicoanalyse vermeldt of er een minder ingrijpende gegevensverwerking mogelijk is het bereiken van dit doel	• Persoonsgegevens, AVG: Het gewenste doel kan ook worden bereikt door middel van Toegangscontrole vooraf. De verwerking van persoonsgegevens die samenhangt met toegangscontrole vooraf is minder ingrijpend voor de privacy van ontheffinghouders en derden (zie paragraaf 3.1.) • Politiegegevens, Wpg: Digitale handhaving is slechts mogelijk na instemming van het Parket Centrale Verwerking Openbaar Ministerie. Daarmee wordt geborgd dat digitale handhaving voldoet aan de wettelijke vereisten (zie paragraaf 4). De gemeente heeft instemming gekregen[9].
2.3.	De risicoanalyse vermeldt welke gegevens en verwerkingen proportioneel is voor het bereiken van dit doel	• Persoonsgegevens, AVG: De extra gegevensverwerking is proportioneel mits zij beperkt blijft tot de noodzakelijke persoonsgegevens (zie paragraaf 3.2 en onderdeel 2.4 van deze tabel.

[9] Het OM toetst de verwerking aan het Beoordelingskader parket CVOM voor digitale handhaving bij geslotenverklaringen en voetgangersgebieden

		• Politiegegevens, Wpg: Zie onderdeel 2.2. van deze tabel.
2.4.	De risicoanalyse bevat een omschrijving van de maatregelen die worden getroffen om de verwerking te beperken tot de ter zake dienende noodzakelijke gegevens	• Persoonsgegevens, AVG: ○ *Ontheffinghouders* Het is niet noodzakelijk en ter zake dienend om persoonsgegevens te verwerken van bestuurders die geen overtreding hebben begaan. Deze persoonsgegevens worden echter 72 uur bewaard. ○ *Toevallige voorbijgangers, bestuurders of inzittenden (derden).* Het is niet noodzakelijk persoonsgegevens te verwerken van derden. De maatregelen om de verwerking van persoonsgegevens te beperken tot de ter zake dienende noodzakelijk gegevens zijn niet toereikend. Er zijn aanvullende maatregelen nodig. (zie paragraaf 3.3.) Advies 1. Bewaar de persoonsgegevens zo kort mogelijk door ze ○ onmiddellijk te verwijderen na vaststelling dat er geen sprake is van een overtreding. ○ onmiddellijk over te dragen en te behandelen als politiegegevens na vaststelleing dat er sprake is van een overtreding. 2. Pas daarom de bewaartermijn van “niet-overtreders” aan van 72 uur naar 0 uur na vaststelling dat men terecht toegang heeft verkregen tot de autoluwe zone. 3. Richt autorisaties zodanig in, dat niemand toegang heeft tot de persoonsgegevens in de periode van vastleggen van de toegang tot de autoluwe zone, tot vernietiging of overdragen van deze gegevens. • Politiegegevens, Wpg: Zie bij 2.2. van deze tabel. Het ontbreken van een beschrijving van het proces en de rollen brengt het risico met zich mee dat er meer gegevens worden verwerkt dan noodzakelijk bijvoorbeeld omdat er onduidelijkheid bestaat over de rol of omdat het te lang duurt voordat foto’s worden bekeken of geblurrd. De maatregelen om de verwerking van persoonsgegevens te beperken tot de ter zake dienende noodzakelijk gegevens zijn daarom niet toereikend. Er zijn aanvullende maatregelen nodig. Advies 1. Werk conform het beoordelingskader parket[2] 2. Beschrijf de digitale handhavingsprocessen en leg ze vast in een procesplaat in Bizagi en publiceer deze op de Helmondse Processenpagina. 3. Beschrijf rollen, procedures en/of werkinstructies, om te borgen dat: ○ Er gewerkt wordt conform het beoordelingskader parket2 ○ Er alleen politiegegevens worden verwerkt om digitaal te kunnen handhaven. ○ Er geen bovenmatige politiegegevens worden verwerkt.

		○ Er geen vermenging ontstaat tussen persoonsgegevens en politiegegevens. 4. Periodiek controle's uit te voeren op doelbinding en noodzakelijkheid van de gegevensverwerking en hierover te rapporteren. 5. Een autorisatiematrix op te stellen (voor zover nog niet aanwezig) en te werken conform deze autorisatiematrix. 6. Periodiek controle's uit te voeren op accounts, rollen en rechten. 7. Aandacht te besteden aan bewustwording en de geheimhoudingsplicht met betrekking tot de verwerking. 8. Mocht PCH in de toekomst worden ingeschakeld om boa's te leveren, breng dan opnieuw de risico's en de noodzakelijke maatregelen in beeld en sluit een verwerkersovereenkomst af.
2.5.	De risicoanalyse bevat een omschrijving van de maatregelen die worden getroffen om te zorgen dat geen function creep[10] optreedt.	• Persoonsgegevens, AVG Er zijn geen maatregelen getroffen om te zorgen dat function creep niet optreedt • Politiegegevens, Wpg Enkel het blurren van foto's wordt genoemd als maatregel om function creep tegen te gaan. Dit is niet voldoende. Omdat een procesbeschrijving van de huidige verwerking ontbreekt, bestaat het risico dat persoonsgegevens en politiegegevens vermengd raken. Wat kan leiden tot function creep. • AVG en Wpg Er zijn aanvullende maatregelen nodig om function creep tegen te gaan. Maatregelen om te zorgen dat de gegevens veilig worden verwerkt en dat er niet meer gegevens worden verwerkt dan noodzakelijk zijn volstaan om hier aan te voldoen zie daarom onderdeel 2.4 van deze tabel.
2.6.	De risicoanalyse bevat een omschrijving van de maatregelen die worden getroffen om ervoor te zorgen dat gegevens niet langer dan noodzakelijk worden opgeslagen in een vorm die het mogelijk maakt om betrokkene te identificeren.	• Persoonsgegevens, AVG Bewaartermijnen zijn automatisch ingericht. 72 uur is echter te lang, de bewaartermijn dient aangepast te worden naar 0 uur. Zie onder 1.3 en 2.4. van deze tabel. • Politiegegevens, Wpg: Bewaartermijnen zijn automatisch ingericht. Zie onder 1.3.
2.7.	De risicoanalyse bevat een omschrijving van de wijze waarop betrokkene (toereikend) wordt geïnformeerd.	• AVG en Wpg: Betrokkenen worden geïnformeerd door middel van informatie op de website[11]. Er wordt daarbij wel aangegeven dat camera's de kentekens registreren bij binnenrijden. (pagina 13 DPIA)
2.8.	De risicoanalyse bevat een omschrijving van hoe betrokkenen hun rechten uit kunnen oefenen: a. rechten van inzage	• AVG en Wpg: De wijze waarop betrokkenen hun rechten kunnen uitoefenen is opgenomen in de algemene privacyverklaring van de gemeente. De informatie op de website (zie bij 2.7 van deze tabel) verwijst niet naar deze algemene informatie.

[10] function creep is wat er gebeurt als we technologie en systemen gebruiken op een andere manier dan in de eerste instantie eigenlijk bedoeld is, met name wanneer het nieuwe doel resulteert in een inbreuk op de privacy.

[11] Kentekentoegang | Gemeente Helmond

	b. recht op rectificatie en verwijdering c. recht op bezwaar d. recht op beperking van de verwerking	Noot: door op de website over kentekenregistratie te verwijzen naar de privacyverklaring, worden betrokkenen beter geïnformeerd over de wijze waarop zij hun rechten kunnen uitoefenen.
2.9.	De risicoanalyse beschrijft de relatie met verwerkers	• Persoonsgegevens AVG - Verwerkingsverantwoordelijke: college van B&W gemeente Helmond - Verwerker: Brickyard - Verstrekkers: Interne afdeling (parkeerbeheer) Er is een verwerkersovereenkomst getekend zie document 51841903; • WPG - Verwerkingsverantwoordelijke: college van B&W gemeente Helmond - Verwerker: Brickyard - Ontvangers: Cannock Chase en CJIB In de toekomst gaat PCH BOA's leveren om de camerabeelden te beoordelen. Op dat moment is de situatie als volgt: Verwerker: PCH - Subverwerker: Cannock Chase - Subverwerker: BLOXX - Subverwerker: CityPermit Noot: Er is nog geen verwerkersovereenkomst gesloten met PCH. Dat is tzt wel nodig.
2.10.	De risicoanalyse beschrijft de waarborgen omtrent internationale doorgifte	N.v.t. alle data blijft binnen de Europese Economische Ruimte.
2.11.	De risicoanalyse vermeldt of voorafgaande raadpleging nodig is.	N.v.t. er is geen hoog risico dat niet kan worden gemitigeerd.

Ad 3 de risico's voor de rechten en vrijheden van betrokkenen

	Omschrijving	Toelichting
	De risicoanalyse brengt de risico's voldoende in beeld.	.
3.1	De bedreigingen die kunnen leiden tot onrechtmatige toegang zijn benoemd. De mogelijke gevolgen voor de rechten en vrijheden van betrokkenen zijn geïdentificeerd. Ze zijn benoemd vanuit het perspectief van betrokkenen en er is daarbij ook gedacht aan de gevolgen die dit heeft op het recht op: • zelfstandigheid (bijvoorbeeld de mogelijkheid om bepaalde handelingen uit te voeren); • vrij blijven van stigmatisering (bijvoorbeeld	• Persoonsgegevens, AVG: Bij onrechtmatige toegang tot persoonsgegevens ontstaat het risico dat er meer persoonsgegevens worden verwerkt dan noodzakelijk. Bijvoorbeeld omdat personen kunnen worden geïdentificeerd Ook bestaat het risico dat function creep optreedt, omdat bijvoorbeeld kan worden gezien wie wanneer het gebied binnenreed en deze informatie voor andere doeleinden zou kunnen worden gebruikt Onrechtmatige toegang kan ook leiden tot manipulatie van het systeem, waardoor er bestuurders geen toegang hebben terwijl ze dat wel zouden moeten krijgen of andersom. Dit kan tot levensbedreigende situaties leiden indien dit de hulpdiensten betreft. Het risico op onrechtmatige toegang is groot omdat de gegevens te lang worden bewaard. Daarnaast is het risico groot bij een onjuiste inrichting van autorisaties. (zie onder 2.4 van deze tabel). • Politiegegevens, Wpg:

	niet op een bepaalde wijze behandeld worden op basis van bepaalde kenmerken); • gelijkheid (bijvoorbeeld het op dezelfde wijze benaderd worden als andere betrokkenen); • vrij blijven van manipulatie (bijvoorbeeld niet beïnvloed worden op gedrag op basis van een (afwijkend) levenspatroon); • integriteit (verlies van eigenheid, waardigheid en ongeschondenheid, niet jezelf kunnen zijn, je moeten aanpassen aan wat anderen vinden hoe je moet zijn); • ongestoord leven (waarbij het bijvoorbeeld kan gaan om identiteitsfraude of (onaangenaam) afbreken van rust en stilte). • eigenwaarde (bijvoorbeeld geen afbreuk aan persoonlijkheid). • autonomie (bijvoorbeeld geen beperking van de vrijheid om eigen regels te volgen) Vooral van zaken als stigmatisering, ongelijkheid, manipulatie en niet ongestoord kunnen leven kunnen betrokkenen last hebben. • Daarnaast zijn de risico's voor de organisatie benoemd.	Bij onrechtmatige toegang tot politiegegevens ontstaat het risico dat er meer politiegegevens worden verwerkt dan noodzakelijk en ontstaat het risico van function creep. Daarnaast kan onrechtmatige toegang leiden tot manipulatie van het systeem, waardoor de integriteit van de data wordt aangetast. wel Het risico is groot omdat het inzicht in de processen en de organisatorische maatregelen rondom het digitaal handhaven ontbreekt. Dit brengt het risico met zich met dat er onrechtmatige toegang tot gegevens wordt verkregen en/of er function creep ontstaat. Het risico wordt ingeperkt door te werken conform het beoordelingskader parket[2]. • AVG en Wpg: Onrechtmatige toegang heeft gevolgen voor de rechten en vrijheden van betrokkenen. Met name het recht op een ongestoord leven en integriteit. De organisatie loopt het risico dat de burgers het vertrouwen in de overheid verliest en het kan leiden tot imagoschade. Het risico tot onrechtmatige toegang door externe actoren wordt beperkt door de goede beveiliging van de saas oplossing.
3.2.	De waarschijnlijkheid en ernst zijn ingeschat.	• AVG en Wpg: Zie pagina 18 t/m 20 van de DPIA, en in de quickscan.
3.3.	De bedreigingen die kunnen leiden tot ongewenste wijziging zijn benoemd. De mogelijke gevolgen voor de rechten en vrijheden van betrokkenen zijn geïdentificeerd. Ze zijn benoemd vanuit het perspectief van betrokkenen en er is daarbij ook gedacht aan de bij het vorige punt genoemde gevolgen. Daarnaast zijn de risico's voor de organisatie benoemd	• Persoonsgegevens, AVG: Ongewenste wijzigingen kunnen er toe leiden dat bestuurders geen toegang hebben terwijl ze dat wel zouden moeten krijgen of andersom. Dit kan tot levensbedreigende situaties leiden indien dit de hulpdiensten betreft. • Politiegegevens, Wpg: Bij ongewenste wijzigingen kunnen betrokkenen ten onrechte en boete of een waarschuwing krijgen. Of andersom. • AVG en Wpg: Het risico hierop is klein, omdat de SAAS oplossing voldoende hiertegen is beveiligd.

3.4.	De waarschijnlijkheid en ernst zijn ingeschat.	• AVG en Wpg: Zie pagina 18 t/m 20 van de DPIA, en in de quickscan..
3.5.	De bedreigingen die kunnen leiden tot het niet beschikbaar zijn van gegevens zijn benoemd. De mogelijke gevolgen voor de rechten en vrijheden van betrokkenen zijn geïdentificeerd. Ze zijn benoemd vanuit het perspectief van betrokkenen en er is daarbij ook gedacht aan de bij het vorige punt genoemde gevolgen. Daarnaast zijn de risico's voor de organisatie benoemd	• Persoonsgegevens, AVG: Het niet beschikbaar zijn van persoonsgegevens kan er toe leiden dat bestuurders geen toegang hebben terwijl ze dat wel zouden moeten. Dit kan tot levensbedreigende situaties leiden indien dit de hulpdiensten betreft. • Politiegegevens, Wpg: Het niet beschikbaar zijn van gegevens heeft als risico dat betrokkenen ten onrechte een boete krijgen (wanneer ontheffingen niet beschikbaar zijn) Dat overtreders onbestraft blijven. Dat heeft als risico dat het doel niet wordt bereikt. • AVG en Wpg: Het risico hierop is klein, gelet op de SLA die is afgesloten.
3.6.	De waarschijnlijkheid en ernst zijn ingeschat.	• AVG en Wpg: Zie pagina 18 t/m 20 van de DPIA, en in de quickscan..

Ad 4 de maatregelen worden benoemd

	Omschrijving	Toelichting
4.1.	De beoogde maatregelen om de risico's aan te pakken worden bepaald en zijn voldoende.	• Persoonsgegevens AVG: Er zijn aanvullende maatregelen nodig om: - Toegang tot persoonsgegevens te borgen. - Persoonsgegevens niet langer te bewaren dan noodzakelijk. Zie onderdeel 2.4 van deze tabel. • Politiegegevens, wpg: Er zijn aanvullende organisatorische maatregelen nodig om: - Toegang tot politiegegevens te borgen - Te borgen dat de verwerking van politiegegevens toereikend, ter zake dienend en beperkt blijft tot wat noodzakelijk is om het doel te bereiken. - Te borgen dat politie- en persoonsgegevens niet met elkaar vermengd raken. - Handelen conform het beoordelingskader parket[2] te borgen Zie onderdeel 2.4 van deze tabel. • AVG en Wpg: Er zijn aanvullende maatregelen nodig om betrokkenen goed te informeren. Zie onder 2.8 van deze tabel. Door het Advies op te volgen worden alsnog voldoende maatregelen getroffen.

Bijlage

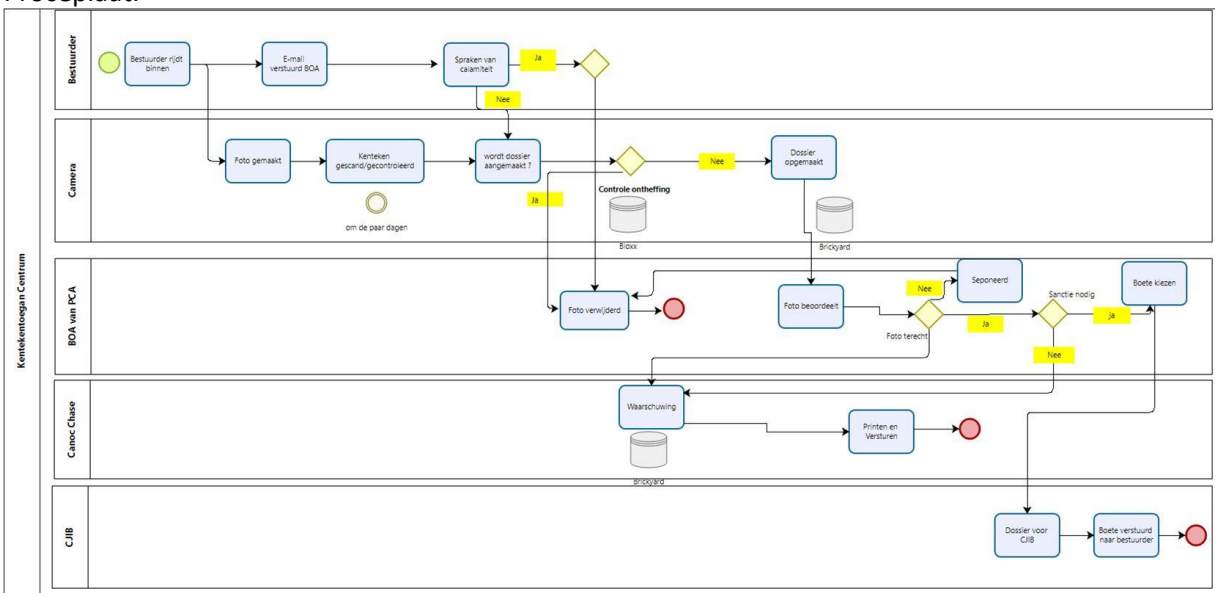
2. Terugkoppeling proceseigenaar

Onder deze kop heeft de proceseigenaar de gelegenheid om aan de FG/CISO terugkoppeling te verschaffen over de implementatie van het advies. Dit verloopt volgens het pas toe of leg uit principe (ptolu) waarbij de proceseigenaar de mogelijkheid heeft om het advies over te nemen, of nader te onderbouwen waarom het advies niet wordt overgenomen.

Reactietermijn proceseigenaar: nader te bepalen
1. Breng het register van verwerkingen in overeenstemming met de aangepaste manier van werken. Doe dit zowel voor wat betreft de Avg als de Wpg.
Reactie proceseigenaar: Dit is inmiddels gedaan door de DSPO' er in samenwerking met de SPO`er. Twee keer per jaar wordt dit opnieuw beoordeeld en evt. Aangepast.
2. Neem op de informatiepagina een verwijzing op naar de privacyverklaring van de gemeente Helmond.
Reactie proceseigenaar: Deze opdracht is op 28 november 2024 verstrekt aan webcare. Zal in de loop van de week worden aangepast.
Met betrekking tot de AVG
1. Bewaar de persoonsgegevens zo kort mogelijk door ze a. onmiddellijk te verwijderen na vaststelling dat er geen sprake is van een overtreding. b. onmiddellijk over te dragen en te behandelen als politiegegevens na vaststelling dat er sprake is van een overtreding.
Reactie proceseigenaar: 1a. Deze gegevens worden inderdaad z.s.m. verwijderd na de constatering dat er geen sprake is van een overtreding. 1b. De overtredingen die leiden tot een waarschuwing worden dagelijke doorgezet naar de partij die de waarschuwingen verstuurd. De overtredingen die leiden tot een boete worden 3 tot 4 keer per week overgedragen aan het CJIB. Hierbij worden alleen de kentekens verzonden. De verrijking van de gegevens vindt bij een derde/ CJIB plaats.
2. Pas daarom de bewaartermijn van "niet-overtreders" aan van 72 uur naar 0 uur na vaststelling dat men terecht toegang heeft verkregen tot de autoluwe zone.
Reactie proceseigenaar: De beelden van de niet overtreders worden z.s.m. bekeken, beoordeeld en vernietigd. Achter kan dit niet terug naar 0 uur. O.b.v. de foto herkent de software het kenteken. Vervolgens zal deze een bevraging moeten doen op de Parkeerrechtendatabase van BLOXX om vervolgens te constateren dat het betreffende voertuig een ontheffing heeft. Voor controledoeleinden wordt dit gegeven enkele uren (maximaal 72 uren) bewaart en daarna vernietigd. Voor overtreders is het niet mogelijk die naar 0 uur bij te stellen. In het beleidsdocument van het CVOM is aangegeven dat de beelden binnen 72 uur moeten worden beoordeeld anders moeten ze worden vernietigd. De beelden mogen hierbij niet worden beoordeeld door een computer, maar alleen door een BOA. Meestal gebeurt dat de volgende dag. Maar de beelden van het weekend worden pas op maandag uitgekeken.

3. Richt autorisaties zodanig in, dat niemand toegang heeft tot de persoonsgegevens in de periode van vastleggen van de toegang tot de autoluwe zone, tot vernietiging of overdragen van deze gegevens.
Met betrekking tot de Wbp
Reactie proceseigenaar: In het softwarepakket wordt alleen het kenteken vastgelegd. Alleen de BOA heeft toegang tot de registraties.
1. Werk conform het beoordelingskader parket[2]
Reactie proceseigenaar: Er wordt gewerkt conform het beoordelingskader van het CVOM. Dit is vooraf en tijdens het project ook met het CVOM afgestemd.
2. Beschrijf de digitale handhavingsprocessen en leg ze vast in een procesplaat in Bizagi en publiceer deze op de Helmondse Processenpagina.
Reactie proceseigenaar: Dit is tijdens het project gedaan. Onder aan deze vragenlijst is de proceplaat toegevoegd.
3. Beschrijf rollen, procedures en/of werkinstructies, om te borgen dat: e. Er gewerkt wordt conform het beoordelingskader parket[2] f. Er alleen politiegegevens worden verwerkt om digitaal te kunnen handhaven. g. Er geen bovenmatige politiegegevens worden verwerkt. h. Er geen vermenging ontstaat tussen persoonsgegevens en politiegegevens.
Reactie proceseigenaar: Tijdens het project is er een handhaafstrategie opgesteld om de bovenstaande punten te waarborgen. Deze handhaafstrategie is toegevoegd aan de zaak (51834053).
4. Voer Periodiek controle's uit op doelbinding en noodzakelijkheid van de gegevensverwerking en rapporteer hierover.
Reactie proceseigenaar: Dit wordt 2x per jaar gedaan bij het updaten van alle verwerkingen van de betreffende afdeling.
5. Stel een autorisatiematrix op (voor zover nog niet aanwezig) en werk conform deze autorisatiematrix.
Reactie proceseigenaar: Er is maar 1 persoon bevoegd en dat is de BOA.
6. Voer periodiek controles uit op accounts, rollen en rechten.
Reactie proceseigenaar: Dit zal worden belegd bij de systeembeheerder (5.1.2e / 5.1.2e)
7. Besteedt aandacht aan bewustwording en de geheimhoudingsplicht met betrekking tot de verwerking van politiegegevens.
Reactie proceseigenaar: Dit zal worden gedaan.
8. Mocht PCH in de toekomst worden ingeschakeld om boa's te leveren, breng dan opnieuw de risico's en de noodzakelijke maatregelen in beeld en sluit een verwerkersovereenkomst af.
Reactie proceseigenaar: Deze overeenkomst is een onderdeel van een al bestaande overeenkomst met PCH. Hiervoor is reeds een verwerkersovereenkomst opgesteld.

Proceplaat:


Kentekentoegan Centrum
Bestuurder
Camera
BOA van PCA
Canoc Chase
CJIB
Bestuurder rijdt binnen
E-mail verstuurd BOA
Spraken van calamiteit
Ja
Nee
Foto gemaakt
Kenteken gescand/gecontroleerd
om de paar dagen
wordt dossier aangemaakt ?
Ja
Controle ontheffing
Bloxx
Nee
Dossier opgemaakt
Brickyard
Foto verwijderd
Foto beoordeelt
Nee
Seponeerd
Foto terecht
Ja
Sanctie nodig
Ja
Nee
Boete kiezen
Waarschuwing
Brickyard
Printen en Versturen
Dossier voor CJIB
Boete verstuurd naar bestuurder

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	16

From: "5.1.2e " <5.1.2e @helmond.nl>
Sent: 4/17/2025 3:11:26 PM
To: "5.1.2e " <5.1.2e 5.1.2e @helmond.nl>
Cc: "5.1.2e " <5.1.2e 5.1.2e @helmond.nl>
Subject: FW: Vraag rondom gebruik van Mailchimp

Hallo 5.1.2e,

Advies
Ik adviseer om een risico analyse uit te voeren op het gebruik van Mailchimp, zodat op basis van een risico analyse een afgewogen keuze kan worden gemaakt. En ik een goed inhoudelijk advies kan geven

Voor de duidelijkheid
Ciso en FG adviseren niet: Ga geen contractuele verplichtingen aan met Amerikaanse bedrijven.
Zij adviseren wel: Maak een goede afweging op basis van de risico's maar hou daarbij rekening met het hogere risico van dit moment. Dit betekent ook dat de afweging veel sneller (dan voorheen) zal moeten leiden tot een keuze voor een andere oplossing. Het heeft inmiddels de voorkeur om niet in zee te gaan met een Amerikaans bedrijf.

Toelichting
Het feit dat Mailchimp een Amerikaans bedrijf is, is inderdaad een risico. Dat houdt echter niet automatisch in dat je geen contractuele verplichtingen kunt aangaan met een Amerikaans bedrijf.
Hoe groot dit risico is hangt van verschillende factoren af zoals:

1. De huidige politieke situatie in Amerika (die invloed heeft op de kans dat een risico zich voordoet)
2. De aard van de informatie die wordt verwerkt via Mailchimp (die invloed heeft op de impact)
    a. Hoe erg is het als de Amerikaanse overheid toegang krijgt tot deze informatie
    b. Hoe erg is het als de informatie helemaal niet meer beschikbaar is (bv omdat de toegang tot de informatie onmogelijk wordt gemaakt)
3. De mogelijke maatregelen om het risico of de impact te verkleinen

Of het risico kan worden geaccepteerd (oftewel of je contractuele verplichtingen met Mailchimp kunt aangaan) is afhankelijk van:

1. Hoe groot zijn de risico's ? (waaronder, maar niet enkel, het risico dat Mailchimp een Amerikaans bedrijf is)
2. Welke alternatieven zijn er voor handen? (en wat zijn de risico's van deze alternatieven).

Inhoudelijk in deze case

- Het EU-US Data Privacy Framework (EU-US DPF) geldt nog en Mailchimp geeft aan hier aan te voldoen. Er is geen sprake van een verbod op doorgifte
- Desondanks bestaat het risico dat de Amerikaanse overheid toegang krijgt tot informatie die door Mailchimp wordt verwerkt, of dat de informatie op enig moment niet meer toegankelijk is.
- Ik begrijp dat mailchimp wordt gebruikt om nieuwsbrieven naar zakelijke mailadressen te sturen.
    - Zakelijke mailadressen kunnen (in bepaalde gevallen) te herleiden zijn naar natuurlijke personen, er kan dus niet worden uitgesloten dat er sprake is van persoonsgegevens
    - Bij het gebruik van zakelijke mailadressen loop je minder privacy risico's dan bij het gebruik van persoonlijke mailadressen
    - Er kunnen wel informatiebeveiligingsrisico's voor de betrokken bedrijven ontstaan
    - Ook van de gebruikers van mailchimp worden persoonsgegevens verwerkt (tbv het account bv)
    - De risico's hangen daarbij af van de aard van de gegevens die van de gebruikers worden verwerkt
    - De aard van de (informatie in de) nieuwsbrieven zijn van invloed op het risico.

Kun je verder zo?

Met vriendelijke groet,

Gemeente Helmond

5.1.2e
Functionaris voor de gegevensbescherming

Afdeling Concern control
Postbus 950, 5700 AZ, Helmond
Telefoonnummer 5.1.2e

Kom bij ons werken! Kijk eens op www.helmond.nl/werkenbij.

Van: 5.1.2e <5.1.2e 5.1.2e @helmond.nl>
Verzonden: donderdag 17 april 2025 08:47
Aan: 5.1.2e <5.1.2e @helmond.nl>
Onderwerp: RE: Vraag rondom gebruik van Mailchimp

Dag 5.1.2e,

Team Ondernemen & Cultuur (Stedelijk Beleid) wil via een externe communicatiepartner Mailchimp gebruiken voor het versturen van mailinglijsten naar startende ondernemers als onderdeel van het Helmond Start programma. Aanmelding gebeurt via een opt-in.

De persoonsgegevens die verwerkt worden zijn beperkt tot naam en zakelijk e-mailadres. Een beperkte risicoanalyse en verwerkersovereenkomst leken aanvankelijk voldoende. Door drukte bij het SPO-team heeft dit vraagstuk vertraging opgelopen. Ondertussen wordt de GDPR-compliancy in twijfel getrokken door recente bewegingen van Trump.

5.1.2e adviseert om ook advies in te winnen bij de FG.
Indien meer context nodig is, kan ik dit toelichten.

Met vriendelijke groet,

Gemeente Helmond

5.1.2e
Informatie Adviseur

Afdeling Informatievoorziening en Automatisering (IVA)
Telefoonnummer 5.1.2e

Kom bij ons werken! Kijk eens op www.helmond.nl/werkenbij.

Van: 5.1.2e <5.1.2e 5.1.2e @helmond.nl>
Verzonden: woensdag 16 april 2025 17:15

Aan: 5.1.2e <5.1.2e 5.1.2e @helmond.nl>
CC: 5.1.2e <5.1.2e 5.1.2e @helmond.nl>; 5.1.2e <5.1.2e @helmond.nl>
Onderwerp: Vraag rondom gebruik van Mailchimp

Hoi 5.1.2e,

Vanuit het SPO-team ben ik bezig geweest met de vraag rondom Communiteers en het gebruik van Mailchimp. Door onvoorziene omstandigheden (o.a. datalekken met hogere prioriteit) is het dossier nu een aantal keer overgegaan naar een andere collega binnen het SPO-team. Dat is niet handig, maar helaas is het niet anders.

De vraag is om een advies te geven inzake het gebruik van Mailchimp als mogelijke oplossing voor het versturen van emails voor Helmond Start.
Mailchimp heeft op dit moment de volgende verklaring online staan: How Mailchimp is GDPR Compliant in the EU | Mailchimp

“The establishment of the EU-US Data Privacy Framework (EU-US DPF) in July 2023 changed the dynamic of personal data transfers, allowing personal data to flow seamlessly across the Atlantic. The EU-US DPF serves as a mechanism for lawfully transferring personal data from the EU to Mailchimp in the US, and indicates that we meet high standards for data transfers. This enables you to focus on growing your business and connecting with your audience, confident that your data privacy needs are addressed.”

Dit heb ik ook besproken met 5.1.2e. Op zich zou de EU-US DPF afspraken eventuele privacy risico’s afvangen. Echter, heeft Trump de hele afdeling van de Amerikaanse overheid ontslagen die hierop toezicht moet uitoefenen.
Het risicoprofiel ten opzichte van de digitale soevereiniteit is daarmee wereldwijd aan het veranderen.

Als CISO adviseert 5.1.2e op dit moment niet om een contractuele verplichting aan te gaan met een Amerikaanse partij. De risico’s zijn niet stabiel en daarmee niet goed (genoeg) in te schatten.
Zoals besproken, zouden 5.1.2e en ik willen adviseren om ook advies in te winnen bij onze Functionaris Gegevensbescherming.

Tot slot: zowel CISO als FG kunnen op dit onderwerp een advies geven.
Als proceseigenaar mag je natuurlijk, mits onderbouwd, afwijken van gegeven adviezen. Daarmee zul je risico’s accepteren als proceseigenaar.
Er zijn ook alternatieve oplossingen van partijen die mailinglijsten ondersteunen en wél direct voldoen aan de AVG. Ik wil natuurlijk graag mee blijven denken hierin.

Met vriendelijke groet,

Gemeente Helmond

5.1.2e
Security & Privacy Officer

Afdeling IVA, Team Regie
Postbus 950, 5700 AZ, Helmond
Telefoonnummer 5.1.2e

Kom bij ons werken! Kijk eens op www.helmond.nl/werkenbij.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	1, 2, 3

Gemeente Helmond

Voorblad **DT (directie) op donderdag**		**Datum: 29/8/2024**
Onderwerp	Toezichtrapportage van de FG.	
Vertrouwelijk	Maak een keuze: nee	
Opsteller/afdeling	5.1.2e	Functionaris voor de gegevensbescherming
Behandelwijze	Ter informatie én besluitvormend	
Eerdere besluitvorming	De gemeente Helmond wil een betrouwbare stad zijn. Inwoners en medewerkers moeten erop kunnen vertrouwen dat er zorgvuldig met hun gegevens wordt omgegaan. Het college heeft daarom de ambitie om zo snel mogelijk te groeien naar een volwassen organisatie op het gebied van privacy (zie collegebesluit 8 maart 2019 documentnummer 50000374). De directie heeft prioritering aangebracht in de voor deze groei noodzakelijke maatregelen (zie directiebesluit van 28 maart 2024). Zij heeft in ieder geval besloten om: - De actualisatie van de kernregistratie processen (verder kernregistratie) de allerhoogste prioriteit te geven (Einddatum Q2). - De actualisatie van het register van verwerkingen (verder register) de allerhoogste prioriteit te geven (Einddatum Q2). - De 10 meest risicovolle processen te benoemen (Einddatum Q2), deze processen te beschrijven of te verbeteren én op deze processen in 2024 een risico-analyse uit te voeren (Einddatum Q4). Daarnaast heeft de directie op 21 december 2023 besloten om akkoord te gaan met de huidige koppeling met de Arbodienstverlener en zo snel mogelijk een koppeling te realiseren die privacy-proof is.	
Aanleiding agendering en toelichting	De Functionaris voor Gegevensbescherming (FG) is de interne privacy toezichthouder. Zij ziet bij de gemeente Helmond toe op de naleving van de wet- en regelgeving rond de bescherming van persoonsgegevens en politiegegevens. De FG heeft in haar Toezichtplan 2024 aangegeven op welke wijze zij in 2024 haar werkzaamheden vormgeeft. Zij heeft een onderzoek uitgevoerd en haar bevindingen vastgelegd in een rapportage (zie bijlage). Het onderzoek is uitgevoerd voor 1 juli 2024 en heeft dus betrekking op de situatie van voor de organisatiewijziging. Het onderwerp is geagendeerd om u op de hoogte te stellen van deze rapportage. **Conclusie van de FG:** Er is onvoldoende opvolging gegeven aan de besluiten van de directie. Voor alle afdelingen, behalve concerncontrol, geldt dat er nog veel werk te doen is (zie ook de mangementsamenvatting in bijlage 2) Bij een ongewijzigde aanpak zal de organisatie zich niet significant verbeteren, en is zij niet in staat om te voldoen aan de ambities van het college. De gemeente Helmond toont zich geen betrouwbare overheid. Zij loopt bovendien het risico dat een boete wordt	

	opgelegd of dat zij onderwerp wordt van geïntensiveerd toezicht (zie gemeente Eindhoven). De FG heeft daarom een aantal adviezen voor het management. Deze adviezen heeft zij in de vorm van beslispunten opgenomen in dit voorstel. De adviezen aan de afdelingshoofden zijn als beslispunten in het DT/MT voorstel opgenomen.
Voorgestelde beslispunten	1. Afdelingsmanagers aan te spreken op hun verantwoordelijkheid om te zorgen voor **actualisatie van de kernregistratie en het register**. 2. Dit te doen door: a) Elke manager de opdracht te geven om te komen met een plan van aanpak. b) Met elke manager een voortgangsgesprek te voeren over de uitvoering van het plan aanpak kernregistratie en register. 3. De 10 **(**meest risicovolle) **processen vast te stellen.** 4. Dit te doen door: a) De vaststelling (op korte termijn) te agenderen op een DT/MT vergadering. b) Elke afdelingsmanagers de opdracht te geven om hiervoor een advies aan et leveren: Het advies bevat: • Minimaal 2 processen. • Een onderbouwing van de keuze en een planning (wanneer is hier capaciteit voor beschikbaar). c) De volgende adviseurs uit te nodigen voor deze DT/MT vergadering: • FG en CISO, om te adviseren over de risico's. • Coördinator of teammanager SPO team, om te adviseren over de haalbaarheid van de planning. (De afdelingsmanager BO doet dit voor de procesadviseurs). 5. Een planning vast te stellen voor de uitwerking van de aangewezen **processen.** De uitwerking heeft betrekking op het beschrijving/verbeteren van het proces en het uitvoeren van een risico analyse. *Door de directie is aan het actualiseren van kernregistratie, het register en de uitwerking van de meest risico volle processen de allerhoogste prioriteit gegeven. Mocht uit de diverse planningen blijken dat een en ander niet kan worden gerealiseerd in 2024, dan betekent dat, dat in de praktijk aan andere zaken een hogere prioriteit wordt gegeven.* 6. Te zorgen dat dit inzichtelijk wordt voor management en bestuur en dit te doen door: a) De gewijzigde prioriteit vast te stellen. b) Het college te informeren over deze wijziging in prioriteit en de gevolgen daarvan voor de groei van de organisatie op het gebied van privacy. 7. De stand van zaken rondom een koppeling met de **Arbodienstverlener** op te vragen bij de projectgroep "Koppeling Bloeij". 8. Medewerkers te informeren over de huidige bovenmatige verwerking door de Arbodienstverlener.
Vergaderduur (beoogd)	10 minuten
Genodigden bij onderwerp	5.1.2e
Presentatie	Vul in Nee
Procedurestappen, bij het onderwerp behorende (eerdere) betrokken medewerkers en verdere planning	De rapportage is besproken met de Gemeentesecretaris. Het is aan de directie om vervolgstappen af te spreken.

Financiële consequenties (en dekking)	Het is aan het management om de financiële consequenties in beeld te brengen, bij de door hen te maken planningen.
Personele consequenties	Het is aan het management om de personele consequenties in beeld te brengen bij de door hen te maken planningen.
Communicatie	Via deze vergadering heeft de FG gecommuniceerd met directie.

Bijlagen:

1. Rapportage Onderzoek FG Q1 en Q2.
2. Rapportage Stand van Zaken Register van verwerkingen.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens geanonimiseerd op grond van:

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

From: "5.1.2e " <5.1.2e @helmond.nl>
Sent: 4/18/2023 2:03:41 PM
To: "5.1.2e " <5.1.2e @helmond.nl>
Cc:
Subject: Advies: omzetten e-formulieren kodision --> Djuma

Hallo 5.1.2e,

Je vraagt ons advies over het overbrengen van e-formulieren kodision naar de formulierenmodule van Djuma.

We begrijpen dat de formulierenmodule onderdeel is van de Djuma functionaliteit.
De functionaliteit van Djuma die we op dit moment in gebruik hebben is toereikend beveiligd. De autorisaties zijn gebaseerd op het zaaktype en we begrijpen dat de e- formulieren in Djuma direct aan een zaaktype worden gekoppeld waardoor ook een juiste autorisatie is geborgd.

We adviseren daarom om
- Zo veel mogelijk formulieren via Djuma te ontsluiten.
- Formulieren (ongeveer 14) die nu niet via Djuma worden ontsloten maar via "Web" en "mail" alsnog over te brengen naar Djuma.
- Voor de formulieren die niet worden overgebracht naar Djuma:
Te motiveren waarom overbrengen naar Djuma niet mogelijk is.
In beeld te brengen wat de (technische) route is van deze formulieren en de data daarin en hoe de autorisaties zijn geregeld.
In beeld te brengen of dit extra risico's met zich meebrengt en welke mitigerende maatregelen er worden getroffen.

Overigens adviseren we de proceseigenaar van Djuma om het uitvoeren van een risico analyse op Djuma als geheel in te plannen.

Met vriendelijke groet,
5.1.2e en 5.1.2e

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens geanonimiseerd op grond van:

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

Afdeling/Programma: Transactionele Dienstverlening/ Ambtenaar van de burgerlijke stand.

Onderwerp: Ontsluiten gedigitaliseerde akten van de burgerlijke stand met iDocumenten

Datum: 28-6-2023, AL

Aanleiding

Dit advies betreft de volgende fase in het project 'Digitalisering akten burgerlijke stand' en is een vervolg op het advies van 15 februari 2023. Bij mail van 28 februari 2023 is door 5.1.2e gemotiveerd aangegeven van dit eerdere advies af te wijken en het traject om akten van de burgerlijke stand te digitaliseren doorgezet.

In scope voor dit advies is *het in iBrondocumenten ontsluiten en verder verwerken van de digitale akten burgerlijke stand* (hierna: BS). Het betreft scans (images), bijbehorende metadata en rapportage. Het omvat ruim 250.000 bestaande fysieke (originele) BS akten t/m 2023 die door een externe partij gedigitaliseerd zijn/worden. Na deze conversie zal de gemeente Helmond de volgende mogelijkheden van iBrondocumenten gebruiken:

- Opslag digitale BS akten
- Ontsluiting digitale BS akten
- Raadpleging (inzage) digitale BS akten
- Verstrekking digitale BS akten
- Vernietiging digitale BS akten na wettelijke bewaartermijnen.

iBrondocumenten is een module van het bij gemeente Helmond in gebruik zijnde systeem iBurgerzaken. Leverancier hiervan is Pink Roccade Local Government. In 2020 is bij gemeente Helmond een project gestart om iBrondocumenten in gebruik te nemen. Dat is niet doorgezet en ook is nog geen risicoanalyse op de ingebruikname van iBrondocumenten en de bijbehorende processen uitgevoerd. Nu wordt iBrondocumenten dus deels in gebruik genomen voor de in de vorige alinea genoemde processen/verwerkingen.

Expliciet buiten scope voor dit advies zijn gebruik van iBrondocumenten bij alle andere processen en verwerkingen, zoals:

- het zelf direct digitaliseren van BS akten
- verwerking van latere vermeldingen
- digitaliseren, opslag, ontsluiting, raadpleging, verstrekking en vernietiging van andere (bron)documenten dan BS akten

Conclusie

Niet alle risico's voor de privacy van betrokkenen zijn afgedekt. Als laatste onderdeel van het advies van 15-2-2023 is geadviseerd om alle nog te implementeren maatregelen over te nemen in een plan van aanpak en de implementatie daarvan te bewaken. Zoals hierboven aangegeven is echter vanuit de proceseigenaar gemotiveerd aangegeven niet alle adviezen van 15-2-2023 over te nemen.

Voor de processen en verwerkingen die nu in scope zijn dienen passende technische en organisatorische maatregelen te worden getroffen, om de persoonsgegevens te beschermen tegen onrechtmatige verwerking en inbreuken op de beschikbaarheid, integriteit en vertrouwelijkheid. Aanvullende maatregelen, zeker ten aanzien van de bescherming van de invoerbestanden (gescande akten BS en metadata) die leverancier Pink Roccade in iBrondocumenten importeert, zijn noodzakelijk om de restrisico's terug te brengen naar een acceptabel niveau.

Gezien de impact die de nog aanwezige risico's kunnen hebben op onze inwoners en onze dienstverlening, adviseert de CISO daarom om de onderstaande maatregelen te implementeren Het niet opvolgen van dit advies en het inrichten van deze maatregelen betekent dat de privacy risico's voor betrokkenen hoog zijn en dat proceseigenaar en de gemeente tot het moment van implementatie een risico loopt.

Advies

De CISO adviseert om:

1. Het project 'implementatie iBrondocumenten' nieuw leven in te blazen
2. Op de implementatie van iBrondocumenten en de daarmee ondersteunde/te ondersteunen processen en verwerkingen een risico analyse uit te voeren zodat de te implementeren maatregelen steeds als onderdeel van het project kunnen worden meegenomen
3. De volgende, voor de huidige risico analyse in scope zijnde, processen uit te werken in een procesbeschrijving:
    a. De opslag van digitale BS akten
    b. De ontsluiting digitale BS akten
    c. De raadpleging (inzage) van digitale BS akten
    d. De verstrekking digitale BS akten
    e. De vernietiging van digitale BS akten na verstrijken van de wettelijke bewaartermijnen en overdracht van de fysieke akten naar het regionaal archief
4. de verwerkingen die in scope zijn op te nemen in het register van verwerkingen, dan wel de in het register van verwerkingen opgenomen verwerking zo nodig aan te passen
5. Een duidelijk *testplan* op te stellen voor de technische en functionele tests in het kader van de conversie én voor de ingebruikname van de functionaliteit van iBrondocumenten voor de in scope zijnde processen.
6. Een duidelijk *implementatieplan* op te stellen voor de conversie in de productieomgeving van iBrondocumenten,
7. Zoals eerder is geadviseerd in het advies van 15-2-2023: over het volgende afspraken vast te leggen met Pink Roccade:
    a. over de beschikbaarheid van iBurgerzaken tijdens de conversie/overzetting van de digitale akten.
    b. Over wat te doen bij (onherstelbare) afwijkingen/verstoringen/fouten? Wie is waarvoor verantwoordelijk? Wie lost de afwijking/verstoring/fout op? Binnen welke termijn moet een afwijking/verstoring/fout opgelost worden?
    c. Aanvullend: over het bewaren en de vernietiging van de invoerbestanden (scans, metadata en rapportage).
8. Alle nog te implementeren maatregelen over te nemen in een plan van aanpak, voeg dit plan van aanpak toe aan de projectadministratie en bewaak de implementatie hiervan.
9. De risico analyse op iBrondocumenten te herhalen over drie jaar, of bij wijzigingen van het proces of de gebruikte systemen

Toelichting

In bijlage 1 vindt u de volledige beoordeling van de risico analyse

Toelichting risicomanagement

Risicomanagement is het proces dat organisaties uitvoeren waarbij risico's worden geïdentificeerd en gekwantificeerd gevolgd door vaststelling en uitvoering van beheersmaatregelen. Met beheersmaatregelen worden activiteiten bedoeld waarmee de kans van optreden of de gevolgen van risico's positief worden beïnvloed. Tot slot wordt dit gehele proces continu gemonitord en wordt over het risicomanagement verantwoording afgelegd aan belanghebbenden.

In de kern is een risico analyse een document, waarin X de risico's van de gegevensverwerking inventariseert, vanuit het perspectief van de mensen van wie de persoonsgegevens worden verwerkt (de "betrokkenen") en vanuit het perspectief van de organisatie.

Doel van de uitgevoerde risico analyse is om tegenover de risico's maatregelen te zetten. Het is daarnaast een belangrijk proces om te beoordelen of de verwerking van persoonsgegevens rechtmatig en behoorlijk is. Het is óók een document waarmee het college intern én extern verantwoording aflegt over de gemaakte keuzes bij de gegevensverwerking.

De AVG schrijft voor dat bij iedere uitgevoerde risico analyse een advies wordt gevraagd aan de Functionaris Gegevensbescherming (FG), de onafhankelijk toezichthouder op de naleving van de AVG. Onder de AVG is een FG advies geen dwingend advies, maar een zwaarwegend advies. Dat houdt in dat afgeweken kan worden van het advies, mits dit beargumenteerd wordt vastgelegd.

Bijlagen

1 Toets van de risico analyse

Een risico analyse heeft betrekking op informatieveiligheid en privacy. Voor privacy geldt dat de AVG een aantal vereisten stelt aan de uit te voeren risico analyse: Dit zijn de volgende vereisten:

1. Een systematische beschrijving van de beoogde verwerking en de doeleinden;
2. Een beoordeling van de noodzaak en de evenredigheid;
3. Een beoordeling van de risico's voor de rechten en vrijheden van betrokkenen:
4. Een overzicht van beoogde maatregelen om deze risico's aan te pakken.

Ad 1 een systematische beschrijving

	omschrijving	Toelichting
a.	De risico analyse vermeldt: de persoonsgegevens die worden verwerkt	Ja, staat vermeld in document 'Sessie 2 oriëntatie privacy DEFINITIEF', privacyvragen pré DPIA 6 t/m 9
b.	De risico analyse vermeldt: de ontvangers van deze persoonsgegevens	Ja, staat vermeld in document 'Sessie 2 oriëntatie privacy DEFINITIEF', privacyvraag pré DPIA 10
c.	De risico analyse vermeldt: de periode gedurende welke de persoonsgegevens worden bewaard	Ja, staat vermeld in document 'Sessie 2 oriëntatie privacy DEFINITIEF', privacyvraag pré DPIA 12. Aandachtspunt: In iBrondocumenten staan bewaartermijnen default op onbeperkt (*niet privacy by default*) dus de bewaartermijnen moet vóór in productie name correct worden gevuld.
d.	De risico analyse bevat een functionele beschrijving van de verwerking	Ja, staat vermeld in document 'Sessie 2 oriëntatie privacy DEFINITIEF', privacyvraag pré DPIA 3.
e.	De risico analyse bevat de activa waarop persoonsgegevens steunen (hardware, software, netwerken, mensen, papier of papiertransmissiekanalen)	Dit is beschreven in het document 'Sessie 1 verkenning proces en applicatie DEFINITIEF' vanaf pagina 3, het onderdeel '2. Verkenning proces: overzetten digitale akten in iBrondocumenten'. Overigens begrijpen we dat niet gekozen is voor USB-opslag van de te importeren/converteren bestanden, maar gekozen is voor cloud-opslag.

Ad 2 De noodzaak en de evenredigheid wordt beoordeeld

	omschrijving	Toelichting
a.	De risico analyse vermeldt de grondslag en de doeleinden van de verwerking	Ja, staat vermeld in document 'Sessie 2 oriëntatie privacy DEFINITIEF', privacyvragen pré DPIA 4 en 5 en privacyvraag DPIA 8. Zie echter ook opmerking hierover in vorig advies (15-2-2023): *Het terugdringen van inktvraat is een gerechtvaardigd doel voor 3% van de aangeboden akten (9.100 van de 270.000 akten[1]).* *De Grondslag voor deze verwerking is: artikel 6 lid 1 sub e van de AVG.* *Voor de overige 97% geldt dat het doel van de verwerking bestaat uit een efficiënte bedrijfsvoering en dienstverlening is. Er kan niet worden vastgesteld of er sprake is van een gerechtvaardigd doel (zie toelichting).*
b.	De risico analyse vermeldt welke gegevens en verwerkingen er	Ja, staat vermeld in document 'Sessie 2 oriëntatie privacy DEFINITIEF', privacyvragen DPIA 8 en 9.

[1] Bron Concept Programma van Eisen.

	noodzakelijk zijn voor het bereiken van dit doel	
c.	De risico analyse vermeldt of er een minder ingrijpende gegevensverwerking mogelijk is	Ja, in document 'Sessie 2 oriëntatie privacy DEFINITIEF', privacyvragen DPIA 8 en 9. Waarom niet is gekozen voor een minder ingrijpende verwerking is niet (en ook niet in de eerste) risico analyse vermeld: *Met betrekking tot **subsidiariteit** kan het doel, op een andere, voor betrokkene minder nadelige wijze, worden bereikt. Immers blijft de gemeente (ABS) wettelijk verplicht de fysieke (originele) BS akten en latere vermeldingen te bewaren (archiveren). Deze gegevensverwerking voldoet daarom niet aan eisen van **dataminimalisatie**.* Echter, in de reactie op het eerder advies die door 5.1.2e op 28-2-2023 is aangeleverd is gemotiveerd waarom er toch voor digitalisering is gekozen.
d	De risico analyse bevat een omschrijving van de maatregelen die worden getroffen om de verwerking te beperken tot de ter zake dienende noodzakelijke gegevens	Zie ook advies van 15-2-2023: *Omdat de noodzaak van de gekozen werkwijze niet is onderbouwd en alternatieven met een afweging over de gemaakte keuze ontbreken kan niet worden vastgesteld dat er maatregelen zijn getroffen om de verwerking te beperken tot de terzake dienende noodzakelijke gegevens.* Daarom zijn in dat advies voor dit punt diverse aanvullende maatregelen opgenomen. Voor hetgeen nu in scope is, willen we daaraan vast blijven houden.
e.	De risico analyse bevat een omschrijving van de maatregelen die worden getroffen om te zorgen dat geen function creep[2] optreedt.	In het advies van 25-2-2023 is aangegeven dat dit een aandachtspunt is voor het gebruik van iBrondocumenten. Op de implementatie van iBrondocumenten zelf is (nog) geen risico analyse uitgevoerd. Ons dringend advies blijft om dat alsnog te doen.
f.	De risico analyse bevat een omschrijving van de maatregelen die worden getroffen om ervoor te zorgen dat gegevens niet langer dan noodzakelijk worden opgeslagen in een vorm die het mogelijk maakt om betrokkene te identificeren.	Voor deze risico analyse ziet dit op: 1. De invoerbestanden (gescande akten BS en metadata) die leverancier Pink Roccade in iBrondocumenten importeert 2. De informatie in iBrondocumenten zelf (nadat de invoerbestanden in iBrondocumenten zijn geïmporteerd). Niet duidelijk is hoe lang de invoerbestanden bewaard blijven. Voor de gegevens in iBrondocumenten dienen vooraf de bewaartermijnen goed in iBrondocumenten ingesteld te worden.
g.	De risico analyse bevat een omschrijving van de wijze waarop betrokkene (toereikend) wordt geïnformeerd.	Betrokkenen worden niet specifiek geïnformeerd over het digitaliseren, zie document 'Sessie 2 oriëntatie privacy DEFINITIEF', privacyvraag DPIA 10.
h.	de risico analyse bevat een omschrijving van hoe betrokkenen hun rechten uit kunnen oefenen: a. rechten van inzage b. recht op rectificatie en verwijdering c. recht op overdraagbaarheid van gegevens d. recht op bezwaar	Dit is toereikend beschreven in document 'Sessie 2 oriëntatie privacy DEFINITIEF', privacyvraag DPIA 11.

[2] function creep is wat er gebeurt als we technologie en systemen gebruiken op een andere manier dan in de eerste instantie eigenlijk bedoeld is, met name wanneer het nieuwe doel resulteert in een inbreuk op de privacy.

	e. recht op beperking van de verwerking	
i.	de risico analyse beschrijft de relatie met verwerkers	Dit is beschreven in document 'Sessie 2 oriëntatie privacy DEFINITIEF', privacyvraag DPIA 12. Met verwerker Pink Roccade is een (raam)verwerkersovereenkomst afgesloten.
j.	De risico analyse beschrijft de waarborgen omtrent internationale doorgifte	Dit is beschreven in document 'Sessie 2 oriëntatie privacy DEFINITIEF', aanvullende vraag bij privacyvraag DPIA 12: *De opslag van data in iBrondocumenten vindt plaats in Amsterdam in een Azure (Microsoft) omgeving. Dit kan nadelig zijn, als evt. USA instanties zoals CIA, FBI enz. de gegevens opvragen bij Microsoft. In dat geval is Microsoft wettelijk verplicht om de gegevens te overhandigen aan de USA instanties. PinkRoccade geeft in ieder geval aan dat zij van plan zijn om te veranderen van deze omgeving.* Zie ook artikel 4.3 van de (raam)verwerkersovereenkomst.
k.	de risico analyse vermeldt of voorafgaande raadpleging nodig is	Niet van toepassing.

Ad 3 de risico's voor de rechten en vrijheden van betrokkenen

	omschrijving	Toelichting
a.	de risico analyse brengt de risico's voldoende in beeld.	Zie ook de toelichting op dit punt in het advies van 15-2-2023. Voor de huidige scope zijn In de IRPA-documenten dpiadefault en risicoanalysedefault zijn risico's benoemd. Daarnaast is Pink Roccade ISO 27001 gecertificeerd. **Risico's voor de organisatie**: Een inbreuk op beschikbaarheid, integriteit of vertrouwelijkheid van de akten van de burgerlijke stand kan leiden tot de verstoring van de dienstverlening, imagoverlies en financiële schade.
b.	De bedreigingen die kunnen leiden tot onrechtmatige toegang zijn benoemd.	**Conclusie CISO:** Voor deze risico analyse ziet dit op de mogelijkheid van onrechtmatige toegang tot: 1. De invoerbestanden (gescande akten BS en metadata) die leverancier Pink Roccade in iBrondocumenten importeert 2. De informatie in iBrondocumenten zelf (nadat de invoerbestanden in iBrondocumenten zijn geïmporteerd).
c.	De waarschijnlijkheid en ernst zijn ingeschat.	**Conclusie CISO:** Vanwege de aard van de gegevens leidt onrechtmatige toegang tot de akten tot ernstige gevolgen voor betrokkenen. Aanvullende maatregelen, zeker ten aanzien van de invoerbestanden (gescande akten BS en metadata) die leverancier Pink Roccade in iBrondocumenten importeert, zijn noodzakelijk om de restrisico's terug te brengen naar een acceptabel niveau.
d.	De bedreigingen die kunnen leiden tot ongewenste wijziging zijn benoemd.	**Conclusie CISO:** De import van de gescande akten BS en metadata in iBrondocumenten brengt extra verwerkingen met zich mee en daarmee extra risico dat er (onbedoelde) verschillen ontstaan tussen wat ter import is aangeboden en wat in iBrondocumenten wordt opgeslagen. Dit kan ontstaan doordat: - er fouten ontstaan bij het importeren (converteren) van de bestanden in iBrondocumenten;

		- onbevoegden toegang krijgen tot de gegevens en wijzigingen aanbrengt in de data.
e.	De waarschijnlijkheid en ernst zijn ingeschat.	**Conclusie CISO:** Vanwege het feit dat een akte van de burgerlijke stand een brondocument is, leiden onjuiste gegevens tot zeer ernstige gevolgen voor betrokkenen. Aangegeven is, dat er weinig ervaring is met het in deze grote aantallen converteren/importeren van digitale akten in iBrondocumenten. Er is nog geen volledig plan van aanpak en testplan voor deze conversie. We hebben begrepen dat in een testomgeving gestart wordt met een technische test op een populatie van 2.000 gescande akten. Nog niet duidelijk is hoe en of er een gebruikersacceptatietest plaatsvindt. Welke aanpak bij de conversie/import in de productie omgeving wordt gebruikt is nog niet duidelijk. Zolang hierover geen duidelijkheid bestaat moet de kans dat er iets mis kan gaan bij de conversie als groot worden ingeschat. Aanvullende maatregelen zijn noodzakelijk om de restrisico's terug te brengen naar een acceptabel niveau.
f.	De bedreigingen die kunnen leiden tot het niet beschikbaar zijn van gegevens zijn benoemd.	**Conclusie CISO:** De import van de gescande akten BS en metadata in iBrondocumenten) brengt extra verwerkingen met zich mee met zich mee en daarmee zijn er extra risico's op tijdelijk verlies van gegevens. Dit kan ontstaan doordat: - er iets mis gaat in het proces waardoor gedigitaliseerde akten en/of metadata kwijt raken of verloren gaan; - tijdens het in de productieomgeving importeren/converteren van de digitale akten, er iets mis gaat (bijvoorbeeld met de performance van iBurgerzaken) en iBurgerzaken niet beschikbaar is.
g.	De waarschijnlijkheid en ernst zijn ingeschat.	**Conclusie FG en CISO:** Voor de beschikbaarheid van iBurgerzaken dienen tijdens het importeren/converteren van de digitale akten in de productieomgeving aanvullende maatregelen te worden getroffen.

Ad 4 de maatregelen worden benoemd

	omschrijving	Toelichting
a.	de beoogde maatregelen om de risico's aan te pakken worden bepaald en zijn voldoende.	De noodzakelijke maatregelen zijn terug te vinden in dit advies.

2 Geraadpleegde documenten

De FG en de CISO hebben het advies gebaseerd op de documenten in de map ‘P:\DSPO\Uitgevoerde risico analyses en DPIA 2023\Transactionele Dienstverlening\1. Risico-analyse en DPIA\5 - Project digitaliseren akten BS - opslag in iBrondocumenten - afgerond’ en dan met name de volgende documenten:

- Vorig advies ‘Digitalisering akten van de burgerlijke stand’ van 15-2-2023
- Reactie op dit advies d.d. 28-2-2023
- Startnotitie digitaliseren akten BS
- Sessie 1 verkenning proces en applicatie DEFINITIEF
- Sessie 2 oriëntatie privacy DEFINITIEF
- Architectuurdocument d.d. 12-4-2023
- Toelichting architectuurplaat d.d. 13-4-2023
- Akkoord iBrondocumenten d.d. 17-4-2023
- Documenten uit de IRPA tool

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	1, 5

Inhoudsopgave

1. Aanleiding 2
2. Scope 2
3. Conclusie 2
4. Advies 3
5. Toelichting 3
5.1. Actoren PIT-team binnen de gemeente Helmond 3
5.2. Betrokken adviseurs en documenten 4
6. Bijlage 1 Adviezen 5
6.1. Zaakgericht werken in één systeem 5
6.1.1. Eisen aan het zaaksysteem en de inrichting: 5
6.1.2. Label de Informatie o.b.v. een procedure met een classificatieschema 7
6.2. Verwerkingen ten behoeve coördinatie PIT 7
6.2.1. Werkwijze 7
6.2.2. Stel procedures en instructies op en voer ze uit. 8
6.2.3. Instellingen ICT componenten 9
6.3. Het PIT convenant 10
6.3.1. Convenant herzien 10
6.3.2. Opstellen extra overeenkomsten. 11
7 Bijlage 2: visuele weergave PIT-proces (IST/Huidige situatie) 12
8. Bijlage 3: Toets van de risico analyse 13

Afdeling:	Veiligheid en Naleving (V&N)
Onderwerp:	Risico Analyse gemeente Helmond op het PIT-Convenant (Peelland Interventie Team)
Datum:	24 mei 2024

1. Aanleiding

Gemeente Helmond is partner binnen het convenant van het Peelland Interventie Team (PIT). Het PIT voert acties uit op locaties met een sterk vermoeden van misstanden. De PIT-samenwerking heeft als focus de handhaving van bestuurlijke wet- en regelgeving, het voorkomen en signaleren van strafbare feiten en het handhaven van de openbare orde en veiligheid. Hierbij moet er altijd sprake zijn van een multidisciplinaire aanpak, want anders kan de gemeente zelf actie voeren.

De wettelijke bevoegdheden en verantwoordelijkheden van iedere partner vormen in deze samenwerking de basis. Via het PIT-convenant is beschreven op welke manier het mogelijk is om vanuit die bevoegdheden en verantwoordelijkheden een gezamenlijke handhavingsaanpak toe te kunnen/mogen passen op de onderliggende problematiek.

Vanwege de periodieke doorontwikkeling van het PIT-convenant (het nieuwe convenant is geldig van 2022-2025) is er binnen de gemeente Helmond een risicoanalyse uitgevoerd op het proces hier omheen.

2. Scope

Dit advies beperkt zich tot de verwerkingen die plaatsvinden onder de gezamenlijke verantwoordelijkheid van alle PIT-partners. Dit zijn de verwerkingen die plaatsvinden ten behoeve van het PIT- coördinatorschap en het convenant (zie toelichting).

De inhoudelijke verantwoording van de coördinator PIT is buiten scope gehouden, omdat deze valt onder de verantwoordelijkheid van een andere convenantpartner.

3. Conclusie

De privacy risico’s voor betrokkenen zijn groot. Enerzijds door de soort verwerkingen en anderzijds door gebrek aan overzicht in en/of het missen van (technische en organisatorische) maatregelen op het gebied van informatiebeveiliging en privacy. Dit wordt mede veroorzaakt door het ontbreken van een standaard werkwijze en het ontbreken van een specifieke vak-applicatie. Naast het coördinatorschap voor de PIT verwerkingen is de gemeente Helmond zelf ook convenantpartner. Het ontbreken van een strakke functiescheiding tussen dat PIT coördinatorschap en de eigen verantwoordelijkheden als convenantpartner is ook een belangrijke risicofactor.

Zonder het daadwerkelijk treffen van de geadviseerde maatregelen zijn de restrisico's voor betrokkenen groot. Gezien de impact die de nog aanwezige risico's kunnen hebben op onze inwoners en onze dienstverlening, adviseren de FG en de CISO daarom om vóór de ingebruikname van een gezamenlijk zaaksysteem de onderstaande maatregelen te implementeren. We adviseren bovendien om nieuwe procedures en afspraken, die voortkomen uit dit advies over te nemen in een aangepast convenant.

Het niet opvolgen van dit advies betekent dat de privacy risico's voor betrokkenen onacceptabel hoog blijven en dat proceseigenaar, PIT-partners en de gemeente Helmond tot het moment van implementatie diverse risico's lopen.

4. Advies

1. Ga samen met de andere partners zaakgericht werken in één systeem
2. Label de informatie en leg de classificatie vast.
3. Leg de uitgevoerde DPIA voor aan de FG van de partners. Stuur dit advies mee.
4. Voer een aanvullende risico analyse uit op de processen binnen de gemeente Helmond, als PIT convenantpartner. Gelet op de risico's die optreden bij samenwerking wordt geadviseerd om hier prio aan te geven (zie toelichting en bijlage 3 onder 2a).
5. Pas de in het register van verwerkingen opgenomen verwerkingen zodanig aan dat, daar waar van toepassing, PIT is opgenomen als ontvanger van gegevens.
6. Besluit van alle in de bijlage 3 opgenomen adviezen of de adviezen worden overgenomen.
7. Neem alle overgenomen adviezen op in een plan van aanpak. Voeg dit plan van aanpak toe aan de projectadministratie en bewaak de implementatie hiervan.
8. Motiveer van de niet overgenomen adviezen waarom het advies niet wordt overgenomen.
9. Zorg dat nieuwe procedures en afspraken, die vanuit dit advies gezamenlijk worden overgenomen, terugkomen in het convenant.
10. Informeer alle FG's en CISO's over het besluit.

5. Toelichting

Het is van belang dat de gemeente optreedt tegen misstanden, strafbare feiten worden voorkomen of gesignaleerd en dat de openbare orde en veiligheid wordt gehandhaafd. Er moet voor worden gewaakt dat de gemeente daarbij de grondrechten van de mensen die het betreft niet schendt. In het huidige verharde politieke en maatschappelijke klimaat dient de gemeente hier extra aandacht voor te hebben[1]. Dit onderstreept het belang van de zorgvuldige omgang met gegevens en het treffen van de geadviseerde maatregelen.

5.1. Actoren PIT-team binnen de gemeente Helmond

PIT-team coördinatie

De coördinator PIT heeft de beschikking over een fysieke werkruimte en digitale werkplek binnen de gemeente Helmond. Daarbij wordt gebruik gemaakt van de technische infrastructuur, communicatiemiddelen en opslagtechnieken van de gemeente Helmond. Iedere PIT-partner heeft zo haar eigen maatregelen te realiseren met betrekking tot informatiebeveiliging en privacy. Zowel voor een eigen PIT-proces als de eigen (digitale) werkplek.

De gegevens die ten behoeve van de PIT-team coördinatie worden verwerkt, vallen onder de gezamenlijke verantwoordelijkheid van alle PIT-partners. Over de onderlinge verantwoordelijkheden zijn afspraken gemaakt in een convenant. Aangezien er sprake is van een gezamenlijke verantwoordelijkheid is er ook een advies van de FG's van de PIT partners noodzakelijk.

Dit advies heeft enkel betrekking op deze verwerkingen en het convenant.

Inrichting PIT-handhavingstaken gemeente Helmond

Binnen de gemeente Helmond is de toezichthouder bouwen en wonen het eerste aanspreekpunt voor het PIT-team (verder: vertegenwoordiger PIT). Hij neemt ook deel aan de PIT-overleggen. Ook is

[1] Er moet fundamenteel anders naar de grondrechten van mensen worden gekeken" Uit "Blind voor Mens en Recht van de Parlementaire enquêtecommissie Fraudebeleid

binnen de gemeente Helmond een informatie coördinator aangesteld binnen de afdeling Veiligheid en Naleving. Zie bijlage 2 waar dit visueel wordt weergegeven.

De gegevens die ten behoeve van deze taken worden verwerkt, vallen onder verantwoordelijkheid van de gemeente Helmond. Voor zover deze medewerkers gegevens delen met de PIT-coördinator, doet de gemeente Helmond dit als convenant-partner. Voor deze verwerkingen is een aparte risico-analyse nodig. Expliciet buiten scope van deze risicoanalyse zijn dan ook gehouden:

- Het valideren, verrijken van signalen ten behoeve van een PIT actie. Ook voor zover dit gezamenlijk wordt uitgevoerd door de PIT-partners tijdens het tweewekelijkse PIT-overleg.
- De inhoudelijke werkzaamheden bij het toezichthouden/handhaven van toezichthouders die betrokken worden bij acties van het PIT. Dit is namelijk het standaard toezicht- en handhavingsproces. Sommige geadviseerde maatregelen hebben hier wel invloed op.
- De werkzaamheden en inrichting van PIT processen bij de overige partners.

Vooruitlopend op deze risico-analyse heeft het SPO team al een aantal adviezen gegeven, om handvatten te geven voor de aanpak (zie SPO adviesdocument: PIT team Helmond als convenantpartner).

5.2. Betrokken adviseurs en documenten

Dit advies is opgesteld door de Functionaris Gegevensbescherming (FG) en Chief Information Security Officer (CISO) van de gemeente Helmond. De risico analyse is uitgevoerd in samenwerking tussen de coördinator PIT, toezichthouder PIT, notulist, de gemeentelijke informatiecoördinator van afdeling Veiligheid en Naleving (VN) en het Security en Privacy Officer-team van de gemeente Helmond.

De FG en de CISO hebben het advies gebaseerd op de volgende documenten:

- PIT Convenant 2022-2025.
- DPIA “Risico Analyse Samenwerkingsconvenant”.
- Rapportage “Risico Analyse Samenwerkingsconvenant”.
- Informatiestromen “PIT-proces” (zie bijlage2).

Aanvullende (te verstrekken) stukken:

- Het SPO advies, PIT team Helmond als convenantpartner.
- Tactisch kader voor Logging en Monitoring v1.0.

6. Bijlage 1 Adviezen

6.1. Zaakgericht werken in één systeem

Om een gezamenlijke aanpak beter te kunnen ondersteunen en waar mogelijke standaardisatie te faciliteren worden de PIT-partners geadviseerd om in één systeem te gaan werken.
Dit brengt echter enkele risico's met zich mee:

- Andere PIT-partners houden zich niet aan de afspraken die gericht zijn op informatiebeveiliging (de zwakste schakel in de informatieketen bepaalt mede het dreigingsniveau).
- Het gebruikmaken van één systeem leidt ook tot een potentieel "Single Point of Failure".
    - Indien er verkeerde keuzes gemaakt worden bij het implementeren van voorgestelde maatregelen rondom een dergelijk systeem, kan dit juist tot extra risico leiden, omdat alle betrokken PIT-partners geheel of gedeeltelijk toegang krijgen tot het systeem.
    - Voor een kwaadwillende is het gedeelde systeem een mogelijk gewild 'target'.
- Het niet goed inrichten van een mogelijke vakspecifieke applicatie en gezamenlijk afspraken binnen het PIT-convenant maakt de uitvoering van werkzaamheden kwetsbaarder voor dreigingen.

6.1.1. Eisen aan het zaaksysteem en de inrichting:

1. Algemene eisen aan het zaaksysteem:
    a. Het systeem moet minimaal voldoen aan BBN2 niveau en gemeentelijke inkoopvereisten[2].
    b. Het systeem moet voldoen aan privacy by design en privacy by default (conform Programma van Eisen 'PvE').
    c. Bij het PIT betrokken externe PIT-partners (o.a. de andere gemeenten) moeten ook gebruik kunnen maken van het zaaksysteem.
    d. Bij het verkrijgen van de autorisatie tot het gezamenlijke zaaksysteem, wordt duidelijk kenbaar gemaakt aan de gebruiker onder welke voorwaarden van het zaaksysteem gebruik kan worden gemaakt (SLA, Gegevensleverovereenkomst(en), verwerkersovereenkomst(en), PIT-convenant) en op welke manier het gebruik van de gegevens in het systeem worden gelogd en hoe hier monitoring op plaats vindt.
    e. Bewaartermijnen moeten goed in het systeem automatisch ingeregeld worden. Persoonsgegevens worden verwijderd of geanonimiseerd in overeenstemming met de termijnen uit de Selectielijst 2020[3].
    f. Het moet mogelijk zijn om vernietigingslijsten te genereren ter verificatie en bevestigingslijsten na vernietiging.
    g. Bij het ontwerp of de aanschaf van het nieuwe systeem moet de mogelijkheid voor betrokkenen om hun rechten op grond van de AVG uit te oefenen als criterium worden meegenomen.
    h. Kies voor het meest veilige en privacy vriendelijke systeem. Zorg dat dit in de gunningscriteria tot uiting komt.
    i. Het zaaksysteem moet in staat zijn om functiescheiding toe te passen. Zodat er een duidelijk onderscheid wordt gemaakt tussen de activiteiten waar de partners gezamenlijk verantwoordelijk zijn (de expliciete PIT werkzaamheden) en de werkzaamheden waar de partners zelf verantwoordelijkheid dragen.
    j. Neem bij de aanbesteding als wens mee dat documenten kunnen worden opgesteld en bewerkt in het systeem zelf door meerdere mensen tegelijk;

[2] Conform GIBIT 2020: Hierin wordt verwezen naar de gemeentelijke ICT kwaliteitsnormen (waartoe onder andere de normen van de BIO en wettelijke AVG-vereisten behoren)
[3] Link naar de website met de selectielijst Selectielijst 2020 vastgesteld | VNG

2. Logging en monitoring implementeren (in nieuwe systeem/nieuw proces):
   a. Logging en monitoring moet in eigen beheer kunnen worden uitgevoerd conform aanbestedingsafspraken die we hiervoor hebben en dient daarom onder andere in lijn te zijn met het binnen de gemeente Helmond geldende “Tactisch kader voor Logging en Monitoring v1.0”.
   b. Bij aankoop of aanbesteding van een nieuw systeem zijn in ieder geval onderstaande voorwaarden om onderzoek te kunnen uitvoeren vastgesteld:
      - Er is bepaald welke gebruikershandelingen, systeemactiviteiten, gebeurtenissen en/of beheeractiviteiten vastgelegd kunnen worden.
      - Er is vastgelegd waar en hoe centralisering van logging is ingericht (inclusief configuratie-instellingen).
      - Er is een plan met daarin activiteiten die worden uitgevoerd indien logrecords op kwaadwillend misbruik duiden, geïmplementeerde maatregelen niet aan de gestelde eisen en/of verwachtingen hebben voldaan of tekortkomingen hebben opgeleverd.
      - De systemen zijn zodanig geconfigureerd dat interne systeemklokken automatisch gesynchroniseerd worden.
      - Er is bepaald wat te doen bij het uitvallen van logmechanismen (alternatieve paden).
      - Er zijn bewaartermijnen vastgesteld voor de loginformatie.
      - De loggegevens zijn beveiligd tegen achteraf wijzigen/verwijderen door onbevoegden.
   c. ICT-systemen leggen ten minste de in paragraaf 3 van het “Tactisch kader voor Logging en Monitoring v1.0” opgenomen basisset loggegevens vast.
   d. Zorg ervoor dat er steekproeven worden ingepland ter monitoring op applicatieniveau (zie blz 5 van het “Tactisch kader voor Logging en Monitoring v1.0”).
   e. Leg activiteiten van gebruikers waarbij persoonsgegevens worden verwerkt vast in audit-logbestanden. En controleer ze periodiek (minimaal 2x per jaar).
   f. De beschikbaarheid van loginformatie met persoonsgegevens is gegarandeerd totdat de voor de verschillende logging vastgestelde bewaartermijnen zijn verlopen. Verwijder daarna de loginformatie.
   g. De toegang tot loginstellingen, - bestanden en -rapportages is ingericht conform paragraaf 5.4. van het “Tactisch kader voor Logging en Monitoring v1.0”
3. Ingebruikname van nieuwe informatiesystemen, of wijzigingen van bestaande informatiesystemen:
   a. Stel een business impact analyse op bij ingebruikname van nieuwe informatiesystemen
   b. Stel een business impact analyse op bij het aanbrengen van wijzigingen, updates, upgrades en/of patches op bestaande informatiesystemen.
   c. Stel een testplan op.
   d. Gebruik voor acceptatietesten, afhankelijk van de impact en omvang van de wijziging, gestructureerde testmethodieken. Bij voorkeur het geautomatiseerd uitvoeren van testen.

   Omdat de facilitering van het nieuwe systeem en de implementatie ervan binnen de gemeente Helmond plaatsvindt, zijn hierbij de volgende organisatorische maatregelen van toepassing voor het project ingebruikname nieuw informatiesysteem:
   a. Betrek bij de aanbesteding ook de i-adviseur, de architect, functioneel beheerder en de service manager.
   b. Betrek daarnaast de (D)SPO aangezien er koppelingen nodig zijn met persoonsgegevens.
   c. Zorg ervoor dat er een verwerkersovereenkomst wordt gesloten met de leverancier van een systeem.

d. PIT-partners voldoen aan de beveiligingseisen van de gemeente Helmond. Hier mag niet van afgeweken worden om (hoge) risico's op kwetsbaarheden in de infrastructuur, informatievoorziening en overige automatisering van de gemeente Helmond te vermijden.
e. Stel een autorisatiematrix op voor alle interne en externe medewerkers die bij het PIT-convenant betrokken zijn.
f. Zorg dat de autorisatiematrix actueel gehouden wordt en aantoonbaar periodiek (minimaal half-jaarlijks) door verantwoordelijke managers (per gebruikersorganisatie) wordt gereviewd en goedgekeurd.

6.1.2. Label de Informatie o.b.v. een procedure met een classificatieschema.

Binnen deze risicoanalyse op het PIT-convenant zijn door ons onder andere het gebruik van de volgende typen documentatie vastgesteld:

- Vastlegging signaal.
- Draaiboek, verslaglegging.
- Voortgangsdocumentatie.
- Opvolging.
- Communicatie naar burgemeester(s) en/of andere convenant partners.

1. Ken een label toe per documentatie.
2. Bepaal op basis van documentatie type én casuïstiek per informatiestuk:
   a. Hoe lang de informatie bewaard mag worden.
   b. Op welke manier daarbij treffende informatiebeveiligingsmaatregelen genomen dienen te worden (per label zijn mogelijk andere maatregelen nodig).
   c. Documenteer deze maatregelen per label in een dataclassificatieschema.

Per casuïstiek kan ook bepaalde wetgeving van toepassing zijn die bijdraagt in het (mede) bepalen van het vertrouwelijkheidsniveau en de lengte van de bewaartermijn van persoonsgegevens. Daardoor kan het label per type document ook nog verschillen.

6.2. Verwerkingen ten behoeve coördinatie PIT.

Onderstaande adviezen gelden zowel voor de huidige situatie als in de situatie waarbij met een zaaksysteem wordt gewerkt.

6.2.1. Werkwijze

1. Mail alleen met behulp van een veilig mailen tool; beveilig de bestanden door encryptie mét een wachtwoord en deel dit wachtwoord via een ander medium.
   a. Zodra zaaksysteem uitgerold is, verwijs naar zaken. Rondmailen van (gevoelige)informatie is dan niet meer nodig.
2. Gegevensminimalisatie
   a. Werk conform een vastgestelde en uniforme werkwijze (zie adviezen over procedures) .
   b. Gebruik standaard rapportageformulieren/sjablonen met standaard vragen en invulvelden.
   c. Wijs iemand aan die steekproefsgewijs controleert of de gegevensverwerkingen samenhangen met het doel, of er rekening wordt gehouden met dataminimalisatie en of een minder ingrijpende manier mogelijk was geweest om een signaal in kaart te brengen en/of af te handelen.
   d. Voer deze controle minimaal tweemaal per jaar uit en leg de uitkomst vast.
3. Gebruik zo min mogelijk fysieke documenten.
   Zijn fysieke documenten toch nodig: Print dan alleen op een werklocatie en niet thuis of op een openbare locatie. Betreffende documentatie bevat namelijk (bijna) altijd gevoelige persoonsgegevens.

4. Vernietig de ingeleverde draaiboeken direct en leg vast dat dit is gebeurd. Leg minimaal vast hoeveel draaiboeken er zijn uitgereikt, de datum waarop ze zijn ingeleverd en de datum van vernietiging. Hierdoor reduceer je het risico dat draaiboeken op een plek komen waar ze niet thuishoren en daarmee een datalek kunnen veroorzaken.
5. Richt functiescheiding in. Niet alleen in het zaaksysteem maar ook in de huidige situatie en huidige opslaglocaties. Zorg dat de taken die worden uitgevoerd als convenantpartner gescheiden zijn en blijven van de taken die samenhangen met het PIT proces. Richt de autorisaties ook zodanig in. Dit betekent concreet dat de huidige autorisaties op de p-schijf dienen te worden aangepast, aangezien de informatie coördinator te veel informatie kan zien (zie bijlage 2 onderdeel 2 e).
6. Zorg ervoor dat iedereen zich bewust is van de soort persoonsgegevens die zij verwerken en dat zij zich bewust zijn van de risico's die hierbij komen kijken.
7. Deel het advies van deze risicoanalyse met de betrokken medewerkers.

6.2.2. Stel procedures en instructies op en voer ze uit.

Werkprocessen, procedures en instructies zorgen voor een gestandaardiseerde werkwijze. Daarmee worden steeds dezelfde afwegingen gemaakt die bovendien reproduceerbaar zijn. Dit geldt voor zowel de huidige situatie als de (toekomstige) situatie waarbij gebruik wordt gemaakt van een zaaksysteem.

1. Maak afspraken over het downloaden van bestanden ("need-of-use" en o.a. encryptie, beveiligde verbinding, autorisaties, etc.).
2. Stel een procedure op voor het verwijderen van tijdelijke bestanden die zijn aangemaakt als gevolg van de verwerking van persoonsgegevens. Concreet:
    a. Zodra er gewerkt wordt met een systeem: wanneer je een bestand opstelt.
    b. Zodra toegevoegd aan (zaak)systeem, op andere plekken verwijderen.
    c. Wanneer een actie is afgerond: check of alle documentatie met persoonsgegevens op andere locaties dan het (zaak)systeem verwijderd is.
3. Standaardiseer de werkwijze binnen de PIT processen Er worden in ieder geval de volgende documenten geadviseerd.
    a. Werkinstructie/keuzeboom coördinator PIT. Dit document beschrijft wanneer het signaal door het PIT wordt opgepakt of bij VN/extern.
    b. Werkinstructie/keuzeboom huisbezoek, waarbij wordt uitgewerkt op welke wijze de deelnemers de woning mogen betreden. Er wordt per taak specifiek aangegeven of de machtiging tot binnentreden van toepassing is en op welke wijze er per taak informed consent wordt toegepast. Daarnaast beschrijft de instructie op welke wijze er voor wordt gezorgd dat er geen informatie wordt gedeeld tussen de partners waarvoor de machtiging tot binnentreden wel geldt en voor de partners die alleen op basis van toestemming van de bewoner de woning mogen betreden. Dit is van belang om huisvredebreuk of lokaalvredebreuk te voorkomen.
    c. Werkinstructie keuzeboom opvragen politie informatie in verband met de veiligheid van het PIT-team.
    d. Een instructie over het identificeren van betrokkenen. De instructie beschrijft in welke gevallen op welke wijze betrokkenen worden geïdentificeerd.
    e. Een instructie of formulieren die borgen dat het PIT-Dossier enkel de afspraken omtrent de opvolging bevat en geen inhoudelijke informatie.
    f. Een instructie over de afweging en de vastlegging van de gemaakte afwegingen, indien tijdens een actie zaken worden gezien waar de actie niet op gericht was.
4. Stel een procedure op voor het opslaan van informatie: wat sla je op, waar mag je het opslaan, wie mag er wel/niet bij.

5. Stel een procedure op voor het vernietigen van informatie. Stel daarvoor vast welke gegevens hoe lang worden bewaard ten behoeve van de PIT coördinatie. Doe dit voor de verschillende situaties en pas daarbij dataminimalisatie toe. Dat betekent dat gegevens niet langer worden bewaard dan noodzakelijk en er is onderbouwd waarom dit noodzakelijk is.
6. Stel een procedure op voor het ontsluiten van informatie: met wie mag er wat gedeeld worden. Het is zowel intern als extern van belang dat dit wordt afgewogen per situatie en via welke techniek(en) dit gebeurt (vastlegging en reproduceerbaarheid).
7. Stel een procedure op voor het verlenen van autorisaties. Dit geldt voor de locatie waar alle informatie staat opgeslagen en/of voor het te gebruiken zaaksysteem.
8. Leg de rollen en verantwoordelijkheden voor alle binnen de gemeente Helmond bij het PIT-team betrokken functionarissen vast en zorg dat ze duidelijk terugkomen in de processen en procedures.
9. Richt de toegang tot informatie zodanig in dat er een duidelijke scheiding is tussen PIT-verwerkingen en overige verwerking door de gemeente Helmond als convenantpartner.
10. Stel een autorisatiematrix op.
11. Zorg ervoor en leg vast dat draaiboeken verplicht moeten worden ingeleverd bij de coördinator.
12. Zorg ervoor en leg vast dat de coördinator PIT na elke actie controleert of hij alle draaiboeken heeft ontvangen.
13. Documenteer opgezette en vastgestelde processen in Bizagi. Onderhoud de processen door te monitoren op werkbaarheid, correctheid en actualiteit van processen. Je kan hiervoor ondersteuning vragen bij het proces verbeterteam (PVT).

6.2.3. Rechten van betrokkenen

1. Richt de PIT-processen zodanig in dat ze voldoen aan de rechten van betrokkene (AVG) en artikel 24 van het convenant.
2. Informeer betrokkenen over de gegevens die over hen worden verwerkt binnen het PIT. Wijk alleen af op individueel niveau en doe dit gemotiveerd, i.v.m. noodzakelijkheid en op proportionele wijze. Leg deze motivatie vast. Doe dit op twee momenten binnen het proces:
    a. Tijdens een lopend onderzoek.
    b. Na afronding van een onderzoek.

6.2.3. Instellingen ICT componenten

1. Stel vast welke autorisaties en (applicatie)functies nodig zijn en schakel alle andere functies uit (principe van minste functionaliteit).
2. Deactiveer of verwijder (deïnstallatie) alle functies, protocollen, services en accounts op een ICT-component als die niet noodzakelijk zijn.
3. Toets periodiek (eventueel automatisch) of de in productie zijnde ICT-componenten niet meer dan de vastgestelde noodzakelijke functies bieden (momentopname) en de geconstateerde afwijkingen worden hersteld. Doe dit minstens tweemaal per jaar.
4. Maak een overzicht van alle gebruikte apps en geef aan welke medewerkers deze wel/niet mogen gebruiken. Pas periodieke logging toe op gebruikersaccounts. Doe dit bv iedere maand, maar in ieder geval tweemaal per jaar.

6.2.4. Verantwoordelijkheden

Zorg ervoor dat de verantwoordelijkheden bij het lijnmanagement benoemd, belegd en vastgelegd worden op het gebied van privacy en informatiebeveiliging. Daarmee ook het wel/niet implementeren van deze in dit advies voorgestelde maatregelen.

1. Zorg ervoor dat de betrokken proceseigenaren bekend zijn met wat er in het convenant staat, waar zij voor tekenen en zich aan moeten houden.
2. Per PIT-partner bewaakt de proceseigenaar de voortgang van de implementatie van de maatregelen. De risico's en verbetervoorstellen van deze risico analyse moeten daarom bekend zijn bij die proceseigenaar.
3. Afwijkingen van de BIO (O-maatregelen) zijn uitsluitend toegestaan indien de proceseigenaar hiervoor toestemming heeft verleend. Deze toestemming wordt verleend uitsluitend nadat een formele risicoafweging heeft aangetoond dat (bijvoorbeeld met vervangende maatregelen) het beveiligingsrisico als gevolg van de niet-naleving niet is toegenomen. Deze afwijking wordt gedocumenteerd en moet periodiek gevalideerd worden om vast te stellen of het risico nog steeds bestaat en of er aanvullende maatregelen nodig zijn om de risico's (verder) te verlagen.

6.3. Het PIT convenant

Het PIT convenant loopt tot 2025. De aanschaf van een zaaksysteem en het invoeren van maatregelen heeft effect op het convenant. Daarnaast zijn aanvullende afspraken nodig. We adviseren het convenant aan te passen en aanvullende afspraken te maken in de loop van 2024 en daarmee rekening te houden met onderstaande adviezen.

6.3.1. Convenant herzien

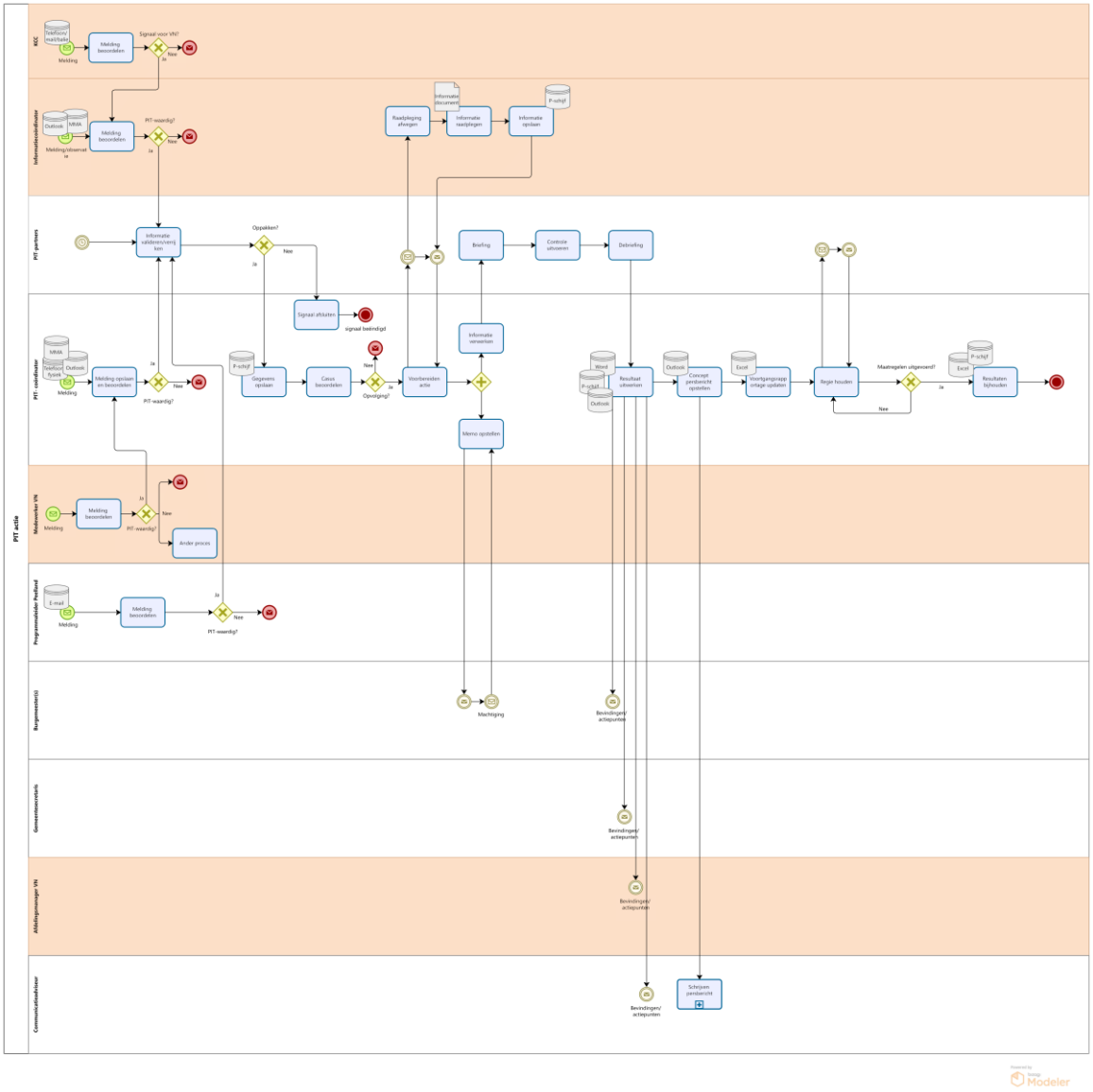
1. Zorg dat nieuwe procedures en afspraken, die vanuit dit advies gezamenlijk worden overgenomen, terugkomen in het convenant. Spreek daarbij ook af dat er niet wordt afgeweken van deze procedures en afspraken.
2. Leg duidelijk in het convenant vast dat het herzien van het convenant noodzakelijk is wanneer er nieuwe afspraken gemaakt (moeten) worden bij doorontwikkelingen en/of wijziging(en) van onderliggende procedures, wetten, applicatie(s) en/of gemeentelijke verantwoordelijkheden c.q. de invulling daarvan.
3. Maak bij iedereen duidelijk: indien je het convenant tekent, werk je ook conform het convenant en wijk je hier niet van af. Is het toch nodig om af te wijken, leg dit dan gezamenlijk vast in het convenant.
4. Richt de processen daarom zo in dat het overeenkomt met de afspraken in het convenant.
5. Leg duidelijk vast in het convenant dat iedere PIT-partner naast de maatregelen ook haar eigen verantwoordelijkheid heeft voor het up-to-date hebben en houden van persoonsgegevens.
6. Stel een procedure op voor het (periodiek) controleren op privacyaspecten binnen de uitvoering van de PIT-processen door bijvoorbeeld (D)SPO/PO/FG met als doel: het vaststellen dat de afspraken binnen het PIT-convenant worden nageleefd. (Deze maatregel is nodig om te voldoen aan artikel 20 lid 2 van het huidige convenant).
7. Voer de onder het vorige punt opstelde procedure uit en controleer minimaal 2x per jaar.
8. Indien de gemeente Helmond een vakspecifieke applicatie gaat aanbieden om te gebruiken voor partners buiten de gemeente Helmond, is het noodzakelijk afspraken en onderliggende taken over het gebruik hiervan (denk bv. aan wachtwoordbeleid) ook vast te leggen in het convenant.
9. Indien de gemeente Helmond een vakspecifieke applicatie gaat aanbieden om te gebruiken voor partners buiten de gemeente Helmond, is het noodzakelijk om vast te leggen in het convenant dat hier alleen gegevens verwerkt mogen worden die noodzakelijk zijn voor het doel van de aanschaf van deze applicatie binnen het PIT. Dit gaat concreet over gegevens waarvan verwacht wordt dat de coördinator PIT hier kennis van neemt.

10. Breng in kaart in welke mate leveranciers van digitale ondersteunende technieken voor het PIT de hierbij verwerkte informatie op buitenlandse server(s) opslaan/verwerken of via eventuele subverwerkers (deels) via buitenlandse diensten/producten worden verwerkt. En tref bijbehorende passende maatregelen.

6.3.2. Opstellen extra overeenkomsten.

a. Stel een overeenkomst gezamenlijke verantwoordelijkheid persoonsgegevensverwerkingen op en Gegevens Lever Overeenkomsten (GLO) tussen PIT-partners (delen van informatie).
b. Verwerkersovereenkomst tussen de PIT-convenantpartners en de leverancier van een zaaksysteem of andere gedeelde informatiesystemen.
c. Service Level Agreement tussen PIT-convenantpartners en de gemeente Helmond (voor het beschikbaar stellen van informatiediensten en applicatiediensten m.b.t. het zaaksysteem en de werkplek voor de Coördinator PIT)

7 Bijlage 2: visuele weergave PIT-proces (IST/Huidige situatie)



Belangrijk: *dit is een conceptversie en is niet formeel vastgelegd als proces – rechtermuisklik koppeling openen geeft een betere weergave*

8. Bijlage 3: Toets van de risico analyse

Een risico analyse heeft betrekking op informatieveiligheid en privacy. Voor privacy geldt dat de AVG een aantal vereisten stelt aan de uit te voeren risico analyse: Dit zijn de volgende vereisten:

1. Een systematische beschrijving van de beoogde verwerking en de doeleinden.
2. Een beoordeling van de noodzaak en de evenredigheid.
3. Een beoordeling van de risico's voor de rechten en vrijheden van betrokkenen.
4. Een overzicht van beoogde maatregelen om deze risico's aan te pakken.

Ad 1 een systematische beschrijving

Voldoet	omschrijving	Toelichting
a.	De risico analyse vermeldt: de persoonsgegevens die worden verwerkt in het Pit.	Blz. 8, 9, 10, 11 en 12 van het DPIA document beschrijven deze in detail. Samengevat: **Draaiboek** - Signaal/de aanleiding(en) die tot een PIT-actie/taak leiden; - adres/locatie(s) van de actie; - samenstelling ingeschrevene(n) (aantallen); Formulier met tabel waarop (aanvullend) genoteerd kan worden: - Naam; - Geboortedatum; - Pas/ID kaartnr. en land (worden zelden uitgevraagd, denk aan maandelijkse prostitutiecontroles); - bijzonderheden (wie gesproken, wat vastgesteld, etc.) - Datum + tijdstip start actie + tijdstip einde actie Bijzondere persoonsgegevens, zoals gegevens over gezondheid of seksueel gedrag. - Coördinator-PIT heeft aanvullend ook naam ingeschrevene(n) van een locatie (om te verifiëren of de eigenaar van de locatie aanwezig is) **Huisbezoek** Tijdens een PIT-actie vindt een huisbezoek plaats. **Verslaglegging PIT-coördinator:** De verslaglegging van de PIT-coördinator zal de hoog-over gegevens omvatten van alle partners: omtrent vastgestelde situatie(s)/constatering(en), wel/geen medewerking verkregen, overige bevindingen, opvolging nodig, eventuele vervolgstappen, etc. **Verslaglegging van iedere Partner** De verslaglegging van een specifieke PIT-partner zal aanvullende/detail gegevens omvatten: omtrent vastgestelde situatie(s)/constatering(en), aanvullende persoonlijke gegevens van betrokkene(n), specifiek voor dat deel van de casuïstiek waar de PIT-partner verantwoordelijk voor is. Deze verslaglegging is geen onderdeel van de uitgevoerde risico-analyse en dit advies. **Voorbereiding** De informatiecoördinator van een partner (waaronder die van de gemeente Helmond) zal op basis van een eigen signaal of besproken signaal vanuit het PIT-team aanvullende informatie verzamelen/vastleggen vanuit de verschillende bronsystemen, voor zover dat binnen wettelijke bevoegdheden en verantwoordelijkheden van betreffende partner is toegestaan Deze voorbereiding is geen onderdeel van de uitgevoerde risico-analyse en dit advies. Dit geldt

		ook voor de werkzaamheden die de (informatie coördinator) gemeente Helmond in die rol uitvoert. Bij al deze verwerkingen worden mogelijk ook bijzondere en/of anderszins gevoelige persoonsgegevens verwerkt. Denk bijvoorbeeld gegevens over verslaving of gegevens over seksuele geaardheid bij de maandelijkse prostitutiecontroles. Bovendien kunnen er gegevens worden verwerkt over kwetsbare groepen. **Maandelijkse prostitutiecontroles (gemeentelijke taak)** Op basis van maandelijkse prostitutiecontroles kunnen ook bijzondere persoonsgegevens worden verwerkt (o.a. seksuele geaardheid, afbeeldingen, type dienstverlening, communicatie, etniciteit). Het betreft dan persoonsgegevens van de kwetsbare beroepsgroep prostitutie. **Zeer Incidenteel** (Casuïstiek specifiek) Ad hoc een mondeling door politie gedeeld met Coördinator PIT: antecedenten/aanvullende gegevens rondom locatie van actie(s) indien dit impact heeft op risico's van deelnemende PIT-teamleden. Een vastgestelde werkwijze en vastlegging zijn noodzakelijk om per casus te kunnen aantonen met welke informatie wordt verzameld en op grond waarvan
b.	De risico analyse vermeldt: de ontvangers van deze persoonsgegevens	Dit verschilt sterk per casuïstiek en per functie binnen het PIT-team. Convenant- en netwerkpartners zijn bekend. Daar kan op casusniveau informatie mee worden gedeeld. Structureel met de politie, VRBZO, Senzer, belastingsamenwerking, ODZOB, coördinator PIT, notulist en vertegenwoordigers per gemeente (Asten, Deurne, Gemert-Bakel, Helmond, Laarbeek en Someren) tijdens het tweewekelijkse PIT-overleg. Het gaat daarbij ook om het delen van informatie intern. Denk bijvoorbeeld aan het delen van informatie tussen de toezichthouder omgevingswet en degene die is belast met adresonderzoek. Binnen de taken en bevoegdheden van iedere partner (zowel intern als extern) zullen bepaalde persoonsgegevens wel/niet gedeeld mogen worden. Bovendien worden bevindingen teruggekoppeld naar Coördinator-PIT om voortgang te bewaken van eventuele opvolgacties én om op hoofdlijnen de bevindingen te kunnen delen met burgemeester(s). Een vastgestelde werkwijze en vastlegging zijn noodzakelijk om per casus te kunnen aantonen met wie informatie is gedeeld en op grond waarvan.
c.	De risico analyse vermeldt: de periode gedurende welke de persoonsgegevens worden bewaard	Op dit moment is er geen/geen gezamenlijk beleid op de bewaartermijnen. Iedere PIT-partner heeft volgens het PIT-convenant zijn eigen verantwoordelijkheid en werkwijze. Voor de informatie die met de PIT partners wordt gedeeld ten behoeve van de uitoefening van hun taken geldt de bij deze (toezichthoudende) taak behorende bewaartermijn. Dit geldt echter niet voor de bewaartermijnen van de gegevens die betrekking hebben op de PIT coördinatie. Omdat de Coördinator PIT binnen de gemeente Helmond is gesitueerd, deelt deze gegevens (intern) op een gezamenlijke netwerkschijf van de netwerkinfrastructuur van de gemeente Helmond. Met de externe partners deelt hij informatie via mail. Aan de gebruikte opslag zijn (momenteel) geen bewaartermijnen

		gekoppeld. Het periodiek en/of binnen bepaalde termijnen vernietigen van informatie wordt ook niet handmatig uitgevoerd. Daarnaast zijn er geen afspraken gemaakt over het bewaren en vernietigen van informatie in de mailfunctie en fysieke informatie. Er bestaat behoefte om de gegevens te bewaren, omdat Casuïstiek het niet beschikbaar zijn van bepaalde gegevens ook negatieve gevolgen kan hebben op lopende (lange termijn) interventies. Te lang bewaren van gegevens (voor het geval dat) is in strijd met het beginsel van onschuldpresumptie. Zie maatregel nummer 21 in het DPIA document bijlage E maatregel voor de bewaartermijnen. Of zie paragraaf 6.2.2. advies 5.
d.	De risico analyse bevat een functionele beschrijving van de verwerking	Op pagina 8 van de DPIA is toegelicht dat het PIT op dit moment (nog) niet met een specifieke (vak)applicatie werkt. In de huidige situatie worden alle voorbereidingen, bevindingen, actiepunten, gevolgen, enz. uitgetypt in Word en Excel: rapportages, verslagen, overzichten en actiepunten. De correspondentie hierover gaat via overleggen, mails en telefonisch. Tijdens de uitvoering van controles wordt gebruik gemaakt van draaiboeken. Deze worden na afloop vernietigd via shredder/blauwe bakken of opgeslagen in een afgesloten ruimte op Boscotondo. Zie voor de beschrijving van de verwerking ook het proces. Een technische oplossing in de vorm van een applicatie biedt waarschijnlijk uitkomst om veiliger, effectiever en efficiënter te werk te gaan. Ook kunnen autorisaties daarin een hele belangrijke ondersteunende rol spelen.
e.	De risico analyse bevat de activa waarop persoonsgegevens (in Helmond)steunen (hardware, software, netwerken, mensen, papier of papiertransmissiekanalen)	Mens: PIT-coördinator, informatiecoördinator, notulist, Afdelingsmanager VN, Burgemeester, PIT-partners Apparatuur: laptops werken on premise en met SAAS-applicaties (in de cloud), smartphones en vaste lijn voor meldingen per telefoon Programmatuur: MSO365 systemen, MS Office systemen, opslagsysteem is de P-schijf (migratie naar Sharepoint?) Organisatie: veiligheid en naleving Omgeving: kantoorruimte in Boscotondo is belangrijk, is afgesloten ruimte (eigen fysieke toegangsmaatregel) waar in de kasten documenten met persoonsgegevens die onderdeel van het proces zijn bewaard worden. Diensten: alle applicaties die de informatiecoördinator o.b.v. casuïstiek raadpleegt (zie blz. 23 + 24 DPIA document). Advies is om over te gaan op een zaaksysteem als opslagplaats voor de documenten, zie maatregelnummer 1 bijlage E van het DPIA document. Zie ook paragraaf 6.1 van dit document.

Ad 2 De noodzaak en de evenredigheid wordt beoordeeld

Voldoet	omschrijving	Toelichting
a.	De risico analyse vermeldt de grondslag en de doeleinden van de verwerking	Blz. 13, 15, 16, 17 en 25 van het DPIA document beschrijven dit in detail. <u>Daarnaast van belang:</u>

		Art. 19 PIT-convenant: Per partner is het doel van de gegevensverwerking beschreven. Art. 20 PIT-convenant: Per partner staat gegevensuitwisseling beschreven. Voor de verwerkingen ten behoeve van de voorbereiding en de uitwerking van een PIT actie is iedere deelnemer zelf verwerkersverantwoordelijk. Voor de verwerkingen ten behoeve van PIT is er sprake van gezamenlijke verwerkingsverantwoordelijkheid. Er is geen grondslag aanwezig voor een gezamenlijke aanpak. Gegevens worden verwerkt op grond van een specifieke overheidstaak. De grondslag voor de verwerking van persoonsgegevens is gelegen in deze individuele verwerking. Dit betekent dat per individuele verwerking moet worden beoordeeld of er een grondslag is en met wie gegevens mogen worden gedeeld. Deze beoordeling moet door iedere convenantpartner afzonderlijk worden gemaakt. De uitgevoerde risico analyse heeft hier geen betrekking op.. Het risico bestaat dat de PIT coördinator gegevens krijgt waarvoor geen grondslag bestaat. Het is daarom van belang dat op deze processen wel een risico analyse wordt uitgevoerd en dat er gemeenschappelijke afspraken over worden gemaakt. Daarnaast heeft de gezamenlijke aanpak als risico dat er te veel gegevens worden gedeeld tussen diverse overheidstaken. Dit kan gebeuren omdat men informatie meekrijgt tijdens een actie, (bijvoorbeeld, de toezichthouder in het kader van de omgevingsvergunning, krijgt mee dat een betrokkene bekende is bij verslavingszorg). Ook is van belang dat er bij een PIT actie een huisbezoek of locatiebezoek plaatsvindt. Een PIT actie wordt uitgevoerd met een multi-disciplinair team waarbij elke deelnemer een ander juridisch kader (en daarmee grondslag) kan hebben voor het huisbezoek. Er bestaat een risico dat tijdens een huisbezoek informatie wordt verkregen waarvoor een grondslag ontbreekt (omdat men zich niet heeft bediend van het juiste juridische kader). In dat geval is er sprake van huisvredebreuk of lokaalvredebreuk. Bovendien heeft men de informatie onrechtmatig verkregen. Het is belangrijk hier meer transparantie en een vastgestelde werkwijze in te verkrijgen, Daarbij dient ook te worden uitgewerkt op welke wijze de deelnemers een woning of een locatie mogen betreden. Zie ook paragraaf 6.2.2 van dit document.
b.	De risico analyse vermeldt welke gegevens en verwerkingen er noodzakelijk zijn voor het bereiken van dit doel	De verwerkingen zijn sterk signaal afhankelijk. Op blz. 15, 16 en 17 is er geprobeerd te schetsen op basis van welk signaal (kan ook als het doel gezien worden in deze context) er op basis van welke wetgeving persoonsgegevens verwerkt kunnen worden. Echter, bij een actie kan het gegeven signaal ook leiden tot bevindingen waarop andere wetgeving van toepassing is dan verwacht. Ook kan het voorkomen dat de actie (tijdelijk) stilgelegd moet worden wanneer blijkt dat de politie of de BOA strafrechtelijke taken moet uitvoeren. Bij een actie/taak van het PIT-team kan iedere hierbij betrokken partner op basis van zijn eigen wetgeving(en) specifieke doelen en dus

		noodzaak voor verwerkingen van (persoons)gegevens hebben. Het risico bestaat dat er meer gegevens worden verwerkt dan noodzakelijk is. Zie ook de gemaakte opmerkingen bij “doel en grondslag van de verwerking”. Op grond van de voorbeelden kan verder worden vastgesteld dat in het PIT dossier de bevindingen te uitgebreid worden beschreven. De inhoudelijke bevindingen horen thuis in de specifieke rapportage niet in het PIT dossier. Voor het PIT dossier volstaan de gemaakte afspraken voor opvolging. Bovendien worden de PIT dossiers dubbel opgeslagen, terwijl niet is gemotiveerd waarom dit nodig is. Bovendien maakt het ontbreken van bewaartermijn en afspraken rondom het gebruiken, bewaren en vernietigen van (PIT) gegevens het risico groter dat er meer en langer gegevens worden verwerkt dan noodzakelijk. Tot slot worden er soms gegevens bij de politie opgevraagd en worden soms id bewijzen gevraagd ter identificatie van betrokkenen die tijdens de uitvoering van een actie op perceel aanwezig zijn. Ook hiervoor ontbreekt een instructie, afwegingskader en vastlegging waardoor het risico bestaat dat er meer gegevens worden verwerkt dan noodzakelijk. Het is belangrijk hier meer transparantie en een vastgestelde werkwijze in te verkrijgen, zie hiervoor maatregel 31 bijlage E van het DPIA document. Zie ook paragraaf 6.2.2.van dit document. De verwerkingen die door de informatiecoördinator worden uitgevoerd en de handhavingsprocessen zijn **geen** onderdeel van de uitgevoerde risico analyse Het uitvoeren van een DPIA op deze verwerkingen is noodzakelijk. Gelet op de extra risico’s die optreden bij samenwerking wordt geadviseerd om hier prio aan te geven. Ook de overige convenantpartners zouden hier aandacht aan moeten besteden. Een technische oplossing, kan het risico met betrekking tot het hergebruiken, bewaren en vernietigen van (PIT) gegevens verkleinen.
c.	De risico analyse vermeldt of er een minder ingrijpende gegevensverwerking mogelijk is	Blz. 25 en 26 van het DPIA document. Per PIT-actie wordt signaalgericht gewerkt. Enkel noodzakelijk geachte convenant-partners en/of incidentele partners worden bij een actie betrokken indien het signaal besproken is binnen het PIT-team en daarvoor aanleiding geeft vanwege de specifieke (wettelijke) bevoegdheden/verantwoordelijkheden van de betreffende partner(s). Indien toch (ook) andere feiten worden vastgesteld die binnen bevoegdheden van andere partner(s) vallen, worden deze partners op dat moment door Coördinator PIT geïnformeerd. Die partner(s) overwegen op dat moment wel/niet direct of op een later tijdstip een eigen actie uit te voeren. De inzet van een multi-disciplinair team is ingrijpender dan wanneer er een “solo” handhavingsactie wordt uitgevoerd. Meldingen komen op veel verschillende plekken binnen. Bovendien zijn er veel mensen die een afweging kunnen maken of iets een PIT zaak is. Het risico dat een verkeerde afweging wordt gemaakt is groter naarmate er meer mensen bij zijn betrokken. Daarmee is ook de kans groter dat er meer informatie wordt gedeeld dan noodzakelijk is. Er is geen methodiek

		noch vastlegging over de wijze waarop wordt getoetst of een zaak PIT-waardig is. Om te onderzoeken of er meer zaken spelen, moet informatie worden gedeeld met (in en of externe) partners. Deze afweging wordt niet vastgelegd. Er ontbreekt bovendien een instructie. Het risico bestaat dat teveel informatie wordt gedeeld met partners. Dat geldt zowel extern als intern (verschillende domeinen). Het is belangrijk hier meer transparantie en een vastgestelde werkwijze in te verkrijgen, zie hiervoor maatregel 31 bijlage E van het DPIA document. Zie ook paragraaf 6.2.2. van dit document.
d.	De risico analyse bevat een omschrijving van de maatregelen die worden getroffen om de verwerking te beperken tot de ter zake dienende noodzakelijke gegevens	De maatregelen uit de risico analyse zijn tot stand gekomen op basis van de Data Protectie Impact Analyse (DPIA) die wij in de IRPA-tool hebben uitgevoerd. Daarnaast hebben wij maatregelen beschreven op basis van de verschillende interviews, gesprekken en documentatieonderzoeken. De maatregelen zijn beschreven in bijlage E van het DPIA document of blz. 4 t/m 11 van dit document.
E.	De risico analyse bevat een omschrijving van de maatregelen die worden getroffen om te zorgen dat geen function creep[4] optreedt.	**Function Creep** Er is sprake van function creep als er informatie wordt verwerkt voor andere doeleinden dan waarvoor de gegevens oorspronkelijk werden verwerkt. Omdat voor het PIT zelf geen grondslag bestaat. Elke gegevensverwerking binnen het PIT moet worden gebaseerd op de grondslag en het doel van een individuele verwerking. De multi-disciplinaire aanpak vergroot het risico dat men informatie verkrijgt waarvoor geen grondslag bestaat en die niet past binnen het oorspronkelijke doel van de individuele verwerking. Dit geldt in het bijzonder voor huisbezoeken waar toezichthoudende taken waarvoor een machtiging tot binnentreden geldt worden gecombineerd met taken waarvoor informed consent geldt. De maatregelen waarnaar wordt verwezen bij a,b,c en d van deze bijlage (zie hierboven) dragen bij aan het tegengaan van function creep. Bijlage E van het DPIA document bevat ook de maatregelen die noodzakelijk zijn om de risico's op het gebied van function creep te reduceren. De FG en CISO van de gemeente Helmond kunnen slechts adviseren over de in Helmond (als convenantpartner uitgevoerde werkzaamheden). Binnen het PIT zijn de partners gezamenlijk verwerkingsverantwoordelijke wat betekent dat ook aan de FG's en CISO's van alle convenantpartners advies moet worden gevraagd. Een andere mogelijkheid is dat PIT-partners het advies door FG en CISO van de gemeente Helmond accepteren en opvolgen. **Alle Convenant-partners** Er wordt aangegeven dat Function creep in principe wordt voorkomen wanneer iedere partner van het PIT-convenant enkel binnen haar eigen wettelijke bevoegdheden en/of expertise een deel van de PIT-actie(s) op zich neemt (functiescheiding). Iedere convenant partner is hierbij zelf verantwoordelijk voor de ondersteunende werkwijze(n) en daarbij te gebruiken applicatie(s) om de gegevens te verwerken die binnen de wettelijke

[4] function creep is wat er gebeurt als we technologie en systemen gebruiken op een andere manier dan in de eerste instantie eigenlijk bedoeld is, met name wanneer het nieuwe doel resulteert in een inbreuk op de privacy.

		bevoegdheden/verantwoordelijkheden van haar taken in het PIT-team vallen. Partners slaan ieder hun eigen detail informatie op en informeren Coördinator-PIT hoog-over inzake de aangetroffen situatie, eventueel geconstateerde feiten, bevindingen en/of misstanden. Zoals eerder aangegeven, vallen maatregelen die partners zelf nemen, niet binnen de scope van dit advies. **Gemeente Helmond Specifiek** Op dit moment werken de coördinator-PIT en de informatiecoördinator van de gemeente Helmond vanuit dezelfde P:-schijf. Dit betekent dat binnen Helmond de functie-scheiding niet in voldoende mate is aangebracht. Dat dient als maatregelen nog te gebeuren. Beiden krijgen enkel autorisaties via een digitale werkplek van de gemeente Helmond en daarbij tot applicaties die uit hoofde van hun functie aan hun beschikbaar worden gesteld. Hierdoor kunnen beiden bij alle zaakinformatie in die folder, dus ook die van de andere convenant partners. **Specifiek voor Informatiecoördinator PIT** Binnen de gemeente Helmond heeft de informatiecoördinator PIT de bevoegdheden om vanuit haar taken/verantwoordelijkheden als toezichthouder VN én als informatiecoördinator PIT (namens gemeente Helmond) diverse systemen te raadplegen. Deze risico analyse heeft geen betrekking op de door de informatie-coördinator uitgevoerde handelingen als toezichthouder VN. De hierbij verrichtte werkzaamheden zijn niet als PIT medewerker, niet als convenantparter. Wij adviseren hiervoor een aparte risico analyse uit te voeren voor wat betreft inhoud, verantwoordelijkheden, bevoegdheden en taken. Er dienen duidelijk functiescheidingen inzichtelijk te worden gemaakt met daarbij beschrijving van welke toegangsrechten en informatiestromen wel/niet mogen worden gebruikt per functie. **Specifiek voor Coördinator PIT** Uit principe legt de coördinator PIT geen detailbevindingen vast over vastgestelde misstanden. Dat doet iedere convenant partner zelf binnen haar taken en verantwoordelijkheden. Ze rapporteren op hoofdlijnen en dusdanig niveau aan de coördinator-PIT om eventuele te adviseren maatregelen voor een gemeente voldoende te kunnen onderbouwen. Ook voert de coördinator-PIT de voortgangsbewaking-taken uit die ertoe moeten bijdragen dat lopende zaken (tijdig) worden afgerond. Er is op dit moment geen vak-applicatie beschikbaar, wat resulteert in de situatie dat de Coördinator-PIT altijd telefonisch en/of via de mail/MS-Teams met convenant partners moet communiceren over de voortgang, opvolging en/of casuïstiek specifieke openstaande vragen die (tijdige) opvolging behoeven. Dat is niet efficiënt en in sommige situaties ook niet effectief. Een vakspecifieke applicatie kan hierin beter ondersteuning bieden, mits deze applicatie er met name toe bijdraagt dat informatiedeling op een veilige wijze kan plaatsvinden én autorisaties per casus (of deel van een casus) aan specifieke convenant partners ingeregeld kunnen

		worden. Daarnaast zal een vakspecifieke applicatie de follow-up van lopende zaken voor en door de Coördinator-PIT véél efficiënter maken en ook voor makkelijk te genereren managementrapportages kunnen zorgen.
f.	De risico analyse bevat een omschrijving van de maatregelen die worden getroffen om ervoor te zorgen dat gegevens niet langer dan noodzakelijk worden opgeslagen in een vorm die het mogelijk maakt om betrokkene te identificeren.	Bewaartermijnen zijn onbekend. Hier moet dus 1. Bekendheid over zijn, hoe lang mag wat bewaard worden en 2. Automatisch ingeregeld worden bij het (zaak)systeem dat gekozen wordt. Er wordt geadviseerd om de bewaartermijnen vast te stellen en ze automatisch goed in te laten regelen. Nu is dat namelijk niet het geval, doordat informatie op de P-schijf wordt opgeslagen. Zie daarnaast ook de opmerkingen bij noodzakelijkheid. Zie maatregelnummer 20, 21 en 22 in bijlage E van het DPIA document. Of zie paragraaf 6.2.2. advies 5.
g.	De risico analyse bevat een omschrijving van de wijze waarop betrokkene (toereikend) wordt geïnformeerd.	Op dit moment gebeurt dit niet op een gestructureerde wijze. Betrokkenen worden op locatie door coördinator-PIT mondeling geïnformeerd over bevindingen van de betrokken partners. Betrokkenen die zijn onderzocht en waarbij het niet tot een PIT actie komt, worden niet geïnformeerd. Daarnaast vindt er tijdens een PIT-actie een huis- of lokaalbezoek bezoek plaats. Bij een multidisciplinaire aanpak heeft een dergelijk bezoek verschillende doelen. Bovendien kunnen de bevoegdheden van de aanwezigen verschillen. Het risico bestaat dat betrokkenen hier niet goed over worden geïnformeerd. Of dat de informatie voor hem onvoldoende duidelijk is. Het risico bestaat dat er niet wordt voldaan aan het principe van informed consent. De risicoanalyse bevat daarom een maatregel op welke wijze dit (structureel) gedaan moet worden, of in ieder geval rekening mee moet worden gehouden (maatregelnummer 13 in bijlage E van het DPIA document). Zie ook paragraaf 6.2.2 van dit document.
h.	de risico analyse bevat een omschrijving van hoe betrokkenen hun rechten uit kunnen oefenen: a. rechten van inzage b. recht op rectificatie en verwijdering c. recht op overdraagbaarheid van gegevens d. recht op bezwaar e. recht op beperking van de verwerking	Blz. 26 en 27 van het DPIA document beschrijft dit in detail. De informatieplicht vanuit het PIT-convenant is vastgelegd in Artikel 26. In Artikel 24 van het PIT-convenant is aangegeven hoe betrokkene bij de individuele PIT-partners een verzoek kan indienen. Deze dienen dit zelf binnen hun eigen privacy regime op te pakken. Indien het (deels) ook politiegegevens zou betrekken, dient de betreffende partner dit bij Politie neer te leggen ter afhandeling van haar deel.
i.	de risico analyse beschrijft de relatie met verwerkers	In het PIT convenant 2022-2025 is vastgelegd dat iedere convenantpartner zelf verantwoordelijk is voor de verwerking van gegevens. Voor het vastleggen van gezamenlijk verwerkte persoonsgegevens is de gemeente Helmond verantwoordelijk om passende (beveiligings)maatregelen te nemen, omdat het daar wordt vastgelegd. Dat komt omdat dit valt onder de bevoegdheden van verantwoordelijkheden van de Coördinator-PIT en deze qua werkplek is gesitueerd binnen de gemeente Helmond. Daarnaast zijn de relaties en verantwoordelijkheden voor de

		aangesloten convenantpartners vastgelegd in het convenant zelf. Om te borgen dat convenantpartners handelen conform convenant worden hier enkele adviezen over gegeven in bijlage E van het DPIA document, nummer 5 en 6. Of zie hoofdstuk 6.3. van dit document..
j.	De risico analyse beschrijft de waarborgen omtrent internationale doorgifte	Er is geen sprake van een directe gegevensoverdracht buiten de EER, zie PIT convenant 2022-2025 artikel 23 lid 3. Wel wordt er gebruik gemaakt van MS365 (o.a. MS Outlook), waardoor er op die manier een vorm van internationale gegevensoverdracht plaatsvindt. Microsoft werkt daarom voor Europese klanten zo veel mogelijk via datacentra binnen de EU (resp. Dublin en Amsterdam). Daarmee kan echter niet worden voorkomen dat de Amerikaanse overheid de gegevens kan vorderen en dus kan meekijken[5]. De huidige Amerikaanse wetgeving om data op te vragen heeft specifiek betrekking op uitzonderlijke omstandigheden waarin een vermoeden van een ernstig misdrijf wordt vastgesteld. Microsoft geeft aan dat zij zich daar "waar mogelijk" zal verzetten tegen het leveren van gegevens. Daarnaast werkt Microsoft ook met subverwerkers en die zijn niet allemaal gevestigd in Europa. Een deel van de gegevens kunnen mogelijk gedeeld worden (binnen de GDPR) met deze subverwerkers. Dit geldt mogelijk voor iedere partner, maar ook voor andere leveranciers van bij die partner gebruikte systemen ter ondersteuning van hun PIT-convenant gerelateerde taken. Daarom wordt geadviseerd om het in kaart te brengen, maatregelnummer 32 van het DPIA document in bijlage E. Of zie hoofdstuk 6.3. van dit document maatregel 10.
k.	de risico analyse vermeldt of voorafgaande raadpleging nodig is	Omdat de gemeente Helmond bereid is een eventueel gezamenlijk zaaksysteem te faciliteren, bestaat binnen de gemeente Helmond wél een voorwaardelijke situatie, opdat het gebruik van een door de gemeente Helmond gefaciliteerd zaaksysteem, waaraan tot externe gebruikers toegang tot (een deel van) de netwerkinfrastructuur gegeven gaat worden, een aantal verplichtte maatregelen zal behoren. (Denk aan multi factor authenticatie en vooraf te volgen (veiligheids)instructies en/of systeemconfiguraties). Om te bepalen of een voorafgaande raadpleging nodig is, zijn er meerdere opties mogelijk. Het is niet aan de FG/CISO van de gemeente Helmond om per PIT-partner te bepalen hier mee om te gaan. Een eenduidige werkwijze en interpretatie van de vastgestelde risico's en bijbehorende beheersmaatregelen wordt wel als gewenst beschouwd. Optie 1: Iedere betrokken Functionaris Gegevensbescherming (FG) vooraf betrekken om op basis van deze risico analyse een afweging te maken of voorafgaande raadpleging nodig is op basis van de risico's en geadviseerde maatregelen die uit deze risico analyse voortkomen. Zie advies van de FG en CISO.

[5] Rapport van Clingendael: "Too late to act? Europe's quest for cloud sovereignty

Ad 3 de risico's voor de rechten en vrijheden van betrokkenen

Voldoet	omschrijving	Toelichting
a.	de risico analyse brengt de risico's voldoende in beeld.	Deel 1 de risico's die vanuit de IRPA-tool komen en deel 2 nog risico's naast de IRPA-tool of die extra benadrukt worden (bijlage E van het document DPIA vanaf blz. 61), omdat er meer maatregelen mogelijk zijn.
b.	De bedreigingen die kunnen leiden tot **onrechtmatige toegang** zijn benoemd. De mogelijke gevolgen voor de rechten en vrijheden van betrokkenen zijn geïdentificeerd. Ze zijn benoemd vanuit het perspectief van betrokkenen en er is daarbij ook gedacht aan de gevolgen die dit heeft op het recht op : • zelfstandigheid (bijvoorbeeld de mogelijkheid om bepaalde handelingen uit te voeren); • vrij blijven van stigmatisering (bijvoorbeeld niet op een bepaalde wijze behandeld worden op basis van bepaalde kenmerken); • gelijkheid (bijvoorbeeld het op de zelfde wijze benaderd worden als andere betrokkenen); • vrij blijven van manipulatie (bijvoorbeeld niet beïnvloed worden op gedrag op basis van een (afwijkend) levenspatroon); • integriteit (verlies van eigenheid, waardigheid en ongeschondenheid, niet jezelf kunnen zijn , je moeten aanpassen aan wat anderen vinden hoe je moet zijn); • ongestoord leven (waarbij het bijvoorbeeld kan gaan om identiteitsfraude of (onaangenaam) afbreken van rust en stilte). • eigenwaarde (bijvoorbeeld geen afbreuk aan persoonlijkheid). • autonomie (bijvoorbeeld geen beperking van de vrijheid om eigen regels te volgen) Vooral van zaken als stigmatisering, ongelijkheid, manipulatie en niet ongestoord kunnen leven kunnen betrokkenen last hebben.	*Wat zijn de risicobronnen? Genoemd zijn:* Alles: Partner/contractor; werknemer met veel rechten; cybercriminelen; cyberterroristen; hacktivisten; werknemer; script kiddies Meer specifiek: - Binnen de gemeente Helmond: beheerders met hoge toegangsrechten tot de opgeslagen gegevens waar Coördinator PIT, Informatiecoördinator gemeente Helmond en/of andere specifiek binnen de gemeente Helmond bij PIT-team betrokken functionarissen met rechten tot deze gegevens. - Binnen de gemeente Helmond: onvoldoende bewustzijn over de verschillende rollen en processen. - Voor iedere Convenant-partner: beheerders met hoge toegangsrechten tot de opgeslagen gegevens waar bij het PIT-team betrokken medewerkers en/of andere specifiek binnen de convenant-partner bij PIT-team betrokken functionarissen met rechten tot deze gegevens. - Voor iedere Convenant-partner: onvoldoende bewustzijn bij medewerkers over grondslagen, doelbinding, te maken afwegingen en het feit dat niet alle verkregen informatie ook mag worden gebruikt. - *Wat zijn de belangrijkste dreigingen (50+) die tot het risico kunnen leiden? Genoemd zijn:* - Exporteren van persoonsgegevens is te gemakkelijk. - Gebruik onveilige e-mail. - Persoonsgegevens worden heimelijk verwerkt. - Data wat management ontvangt is herleidbaar naar adressen en/of personen. - Onduidelijkheid over grondslag gegevensdeling. - Personen worden onnodig gevolgd. - Onvoldoende afspraken over gegevensuitwisseling. - Onvoldoende inzicht in (sub)verwerkers. - Onvoldoende inzicht in verwerking door derden. - Te lang bewaren van gegevens. - Te veel gegevens verwerkt. - Te veel toegang tot gegevens (+ Ongeautoriseerde toegang tot opgeslagen persoonsgevoelige gegevens, verkeerd autorisatiebeleid, te veel informatie die me meekrijgt bij een multi disciplinaire aanpak.). - Verwerking bijzondere persoonsgegevens zonder grondslag. - Verwerking in derde landen zonder aanvullende afspraken hierover. - Verwerking zonder grondslag. - *Onrbreken van autorisatiebeleid.*

	• Daarnaast zijn de risico's voor de organisatie benoemd.	- *Logging en monitoring is niet mogelijk op P-schijf* Op deze punten is de focus gelegd bij het voorleggen van maatregelen waar de IRPA-tool te kort komt. Gezien de situatie: eerst voor verbetering gaan en dan pas naar perfectie streven. *Wat zijn de kwetsbaarheden?* *Genoemd worden de volgende kwetsbaarheden:* Mens, apparatuur, programmatuur, organisatie, omgeving en diensten. Onderstreept zijn het meest kwetsbaar. Zie blz. 32, 33 en 34 van het DPIA document. **De kwetsbaarheid zit hem, naast de hierboven opgestelde opsomming met name in:** - Het ontbreken van de basis, doordat de P-schijf als opslaglocatie wordt gebruikt. Hierdoor ben je kwetsbaar op veel gebieden, omdat logging en monitoring niet voldoende mogelijk is, er zijn geen geautomatiseerde bewaartermijnen (bewaartermijnen zijn ook niet bekend), actualiteit van informatie is niet (automatisch) gewaarborgd. Zie maatregel 1 en 2 van bijlage E DPIA document. - Er is niet eenduidig binnen het PIT-convenant een afgestemde aanpak en werkmethodiek rondom het identificeren, registreren, verwerken en uitvoeren van acties en bijbehorende (gevoelige) persoonsgegevens (standaardisatie), geen enkele controle op verder verspreiden van informatie. Ook de gemeente Helmond zelf heeft geen vastgestelde werkmethodiek. De kans dat er onrechtmatig gegevens worden verwerkt (opgezocht, gedeeld, bewaard) of dat de verwerkingen onevenredig zijn is daarom groot. → hier wordt daarom op geadviseerd, zie maatregelnummer 8.2.2.2 in bijlage A en 12 van bijlage E van het DPIA document. *Wat kunnen de belangrijkste gevolgen voor de betrokkenen zijn als het risico zou optreden?* Zie bijlage D van DPIA document. Onterechte inbreuk op persoonsgegevens van subjecten . Hierdoor verliezen zij het recht op een ongestoord leven, Dit kan leiden tot een inbreuk op hun recht om eigen keuzes te maken (autonomie) . Bovendien kan dit tot wantrouwen leiden. Zie ook blz. 28 voor max. bruto schade voor betrokkenen op het gebied van beschikbaarheid, integriteit en vertrouwelijkheid. **Risico's voor betrokkene – concreter** - Het onrechtmatig onderwerp worden van een onderzoek - Het worden gestigmatiseerd, omdat men niet uitgaat van onschuldpresumptie. - Een inbreuk op het huiselijk leven, omdat er niet onder het juiste juridische kader wordt gehandeld. (misbruik van de machtiging, of het ontbreken van informed consent) - Discriminatie, omdat kaders en richtlijnen ontbreken is de kans groot dat een individuele medewerker eventuele persoonlijke vooroordelen mee laat wegen bij het maken van de afweging of iets een PIT zaak is, dan wel bij het opzoeken van extra informatie.

		- Het publiekelijk worden van signaalinformatie (wanneer nog geen mogelijke misstanden zijn vastgesteld) maar een betrokkene wel schade kan ondervinden wanneer deze uit zijn verband kunnen worden getrokken en/of al vooraf tot nadelige gevolgen voor betrokkene(n) kunnen leiden - Het publiekelijk worden van gevoelige persoonsgegevens die zijn vastgesteld tijdens een actie (wanneer gedrag van betrokkene(n) of bijzondere persoonsgegevens zijn vastgesteld) en/of bevindingen die bij de actie(s) zijn vastgesteld door PIT-partner(s) - Het onterecht toekennen van bevinding(en) aan betrokkene(n) omdat PIT-partner(s) onjuiste/niet volledige/niet tijdige locatie-specifieke informatie als basis hebben genomen tijdens de voorbereiding(en) van PIT-acties **Risico's voor de organisatie** - Te ruime bevoegdheden/autorisaties voor individuele medewerkers waardoor onrechtmatig, te veel of te gevoelige persoonlijke gegevens kunnen worden verwerkt rondom aan PIT-team gerelateerde werkzaamheden; - Te weinig kennis van wetgeving en hieraan toegekende taken en bevoegdheden voor PIT-teamleden en/of betrokken convenant-partner(s) waardoor verwerking van persoonsgegevens niet overeenkomstig wet- en/of regelgeving plaatsvindt; - Het indirecte risico op de aanwezigheid/infiltratie van een 'mol' in één van de bij het PIT-convenant aangesloten organisaties waardoor successen van een mogelijke acties daarmee kunnen worden verkleind (en getroffen maatregelen worden omzeild of kwaadwillende(n) vooraf kunnen worden geïnformeerd).
c.	De waarschijnlijkheid en ernst zijn ingeschat.	Netto kans en netto schade is in kaart gebracht tijdens het uitvoeren van de risico analyse. Zie bijlage D van het DPIA document en de prioritering die bij Ad. 3 b. van dit document wordt gesteld. BIV-classificatie beoordeling komt terug in de quickscan.
d.	De bedreigingen die kunnen leiden tot **ongewenste wijziging** zijn benoemd. De mogelijke gevolgen voor de rechten en vrijheden van betrokkenen zijn geïdentificeerd. Ze zijn benoemd vanuit het perspectief van betrokkenen en er is daarbij ook gedacht aan de bij het vorige punt genoemde gevolgen. Daarnaast zijn de risico's voor de organisatie benoemd	*Wat zijn de risicobronnen? Genoemd zijn:* Alles: Partner/contractor; werknemer met veel rechten; cybercriminelen; cyberterroristen; hacktivisten; werknemer; script kiddies *Wat zijn de belangrijkste dreigingen (50+) die tot het risico kunnen leiden? Genoemd zijn:* - Data moeilijk corrigeerbaar: pg zijn niet of slechts met onevenredige inspanningen corrigeerbaar. - Exporteren van persoonsgegevens is te gemakkelijk. - Onvoldoende afspraken over gegevensuitwisseling. - Onvoldoende inzicht in verwerking door derden. - Onvolledige dossiers, of dossiers met te veel informatie . - Te veel toegang tot gegevens (+ Ongeautoriseerde toegang tot opgeslagen persoonsgevoelige gegevens, verkeerd autorisatiebeleid). - Er is geen werkinstructie/standaardisatie, waardoor ongewenste wijzigingen sneller doorgevoerd kunnen worden. *Wat zijn de kwetsbaarheden?* *Genoemd worden de volgende kwetsbaarheden:*

		Met name mens, apparatuur en organisatie. Doordat er niet in een zaaksysteem wordt gewerkt, maar veel op de P-schijf en via de mail. Iedereen met autorisatie tot de map op de P-schijf kan dingen wijzigen/verwijderen, zonder dat dit wordt gelogd. Hierdoor ben je kwetsbaar voor ongewenste wijzigingen en je kunt achteraf niet vaststellen wie ze (al dan niet terecht) heeft uitgevoerd. *Wat kunnen de belangrijkste gevolgen voor de betrokkenen zijn als het risico zou optreden?* Onbekend of en welke gegevens er verwerkt worden van de betrokkene. Of de gegevens kloppen. Op een later moment kan de betrokkene erachter komen doordat er wel interventie plaatsvindt, dit kan wantrouwen opwekken. Je kan als organisatie niet goed transparant zijn richting betrokkene. Betrokkene wordt in de basis ook niet geïnformeerd over verwerking, daardoor kunnen zij geen gebruik maken van hun rechten. Dit betekent dat zij ook niet weten of besluiten zijn gebaseerd op onjuiste informatie. Dit geldt zeker voor het besluit om een casus al dan niet in PIT verband op te pakken en de informatie die is opgeslagen in het PIT dossier. Betrokkenen kunnen daardoor knel komen te zitten. In bepaalde specifieke gevallen kan weliswaar worden afgeweken van de informatieplicht. De afweging of er van een dergelijke uitzondering sprake is wordt nu niet gemaakt. Ook kan een betrokkene door ongewenste wijzigingen en onjuiste conclusies benadeeld worden door de gemeente (handhavings-/sanctiegevolgen) en daarmee beperkt worden in zijn/haar rechten en vrijheden. Een betrokkene kan daardoor in de knel komen te zitten.
e.	De waarschijnlijkheid en ernst zijn ingeschat.	Netto kans en netto schade is in kaart gebracht tijdens het uitvoeren van de risico analyse. Zie bijlage D van het DPIA document en de prioritering die bij Ad. 3 d. van dit document wordt gesteld (de punten in de opsomming zijn in ieder geval realistisch). BIV-classificatie beoordeling komt terug in de quickscan.
f.	De bedreigingen die kunnen leiden tot het **niet beschikbaar** zijn van gegevens zijn benoemd. De mogelijke gevolgen voor de rechten en vrijheden van betrokkenen zijn geïdentificeerd. Ze zijn benoemd vanuit het perspectief van betrokkenen en er is daarbij ook gedacht aan de bij het vorige punt genoemde gevolgen. Daarnaast zijn de risico's voor de organisatie benoemd	*Wat zijn de risicobronnen? Genoemd zijn:* Alles: Partner/contractor; werknemer met veel rechten; cybercriminelen; cyberterroristen; hacktivisten; werknemer; script kiddies *Wat zijn de belangrijkste dreigingen (50+) die tot het risico kunnen leiden? Genoemd zijn:* - Betrokkene niet goed geïnformeerd over verwerking van zijn persoonsgegevens. - Binnen de organisatie is het lastig rechten van betrokkene verzoeken af te handelen door het gebruik van P-schijf en veelvuldig gebruik van e-mail. - Onvoldoende afspraken over gegevensuitwisseling. - Onvoldoende inzicht in (sub)verwerkers. - Onvoldoende inzicht in verwerking door derden. - Onvolledige dossiers. - Te veel toegang tot gegevens (+ Ongeautoriseerde toegang tot opgeslagen persoonsgevoelige gegevens, verkeerd autorisatiebeleid, waardoor ze verwijderd kunnen worden).

		- Gegevens op de P-schijf worden per ongeluk of bewust verwijderd (in een zaaksysteem kan dat niet zomaar). *Wat zijn de kwetsbaarheden?* *Genoemd worden de volgende kwetsbaarheden:* De gegevens op de P:-schijf kunnen per (sub)map in een paar klikken verwijderd worden van de schijf. Daarom komen we ook hier weer terug op dat het werken in een zaaksysteem zo belangrijk is. *Wat kunnen de belangrijkste gevolgen voor de betrokkenen zijn als het risico zou optreden?* **Risico's voor betrokkene** Er kan niet achterhaald worden of en wat er is verwerkt van een eventuele betrokkene. Verzoeken m.b.t. rechten van betrokkene kunnen niet in behandeling worden genomen. **Risico's voor de organisatie** De aanpak van openbare orde problemen kunnen niet goed multidisciplinair opgepakt worden. Mogelijk is er als gevolg hiervan meer sprake van overlast voor burgers en ontstaat er (meer) wantrouwen in de gemeente. Bijkomstig gevolg van het niet beschikbaar zijn van informatie is het mogelijk niet kunnen sturen van de Coördinator-PIT op het tijdig afronden van PIT-acties of opvolging ervan.
g.	De waarschijnlijkheid en ernst zijn ingeschat.	Netto kans en netto schade is in kaart gebracht tijdens het uitvoeren van de risico analyse. Hier is wel naar gekeken. Zie bijlage D van het DPIA document en de prioritering die bij Ad. 3 f. van dit document wordt gesteld (de punten in de opsomming zijn in ieder geval realistisch). BIV-classificatie beoordeling komt terug in de quickscan.

Ad 4 de maatregelen worden benoemd

Voldoet	omschrijving	Toelichting
a.	de beoogde maatregelen om de risico's aan te pakken worden bepaald en zijn voldoende.	Zie bijlage A en E van het DPIA document. Het betreft BIO-maatregelen, PNG-maatregelen, IBD-maatregelen en aanvullende maatregelen vanuit onze expertise.

Programma:	Jeugd
Onderwerp:	Preventie met gezag
Datum:	29 januari 2025
Djuma:	52373526
Aantal blz:	3

Inleiding

Preventie met Gezag (PvG) is onderdeel van het meerjarenprogramma Jeugd en is gericht op het voorkomen van jeugdcriminaliteit en het bieden van perspectief aan risicojongeren, door middel van jeugdhulpverlening, onderwijs, werk en inkomen, en handhaving van de openbare orde. Om uitvoering aan dit programma te kunnen geven worden er persoonsgegevens verwerkt. De gemeente Helmond en partners willen zorgvuldig te werk gaan. De wens is om een optimale balans te vinden tussen het delen van informatie en privacybescherming. Men heeft daarom Privacy Management Partners (PMP) gevraagd om hen daarbij te helpen.

Op 17 september 2024 heeft de stuurgroep besloten om de samenwerking met PMP te beëindigen en al werkenderwijs een DPIA uit te voeren. Op 4 februari 2025 behandelt de stuurgroep een voorstel over de inrichting van de signaaloverleggen (zie voor concept voorstel document 52373539 en 52373533). Na besluitvorming wil de gemeente Helmond daadwerkelijk starten met de organisatie van deze signaaloverleggen.

Advies

Aan de directeur Sociaal Domein en Veligheid en Naleving (vertegenwoordiger van de gemeente in de stuurgroep)

- Start pas met de signaaloverleggen **nadat,** het proces (de processen) en de informatiestromen goed in beeld zijn gebracht. Er daarnaast een risico-analyse (waaronder een DPIA)[1] is uitgevoerd, alle privacy en informatiebeveiligingsrisico's zijn herkend en erkend en er passende maatregelen zijn getroffen.
- Start pas met het delen van informatie met de andere deelnemers als zij kunnen aantonen dat ook zij passende maatregelen hebben getroffen. Vraag als bewijs het FG advies van de partners op de door hen uitgevoerde DPIA.
- Voor zover het advies niet wordt overgenomen:
    - Neem hierover (expliciet) een besluit en onderbouw de afwijking, informeer de FG en leg het besluit vast in het zaaksysteem.
    - Realiseer je dat betrokkenen grote privacyrisico's lopen en dat zij hierdoor nadelige gevolgen kunnen ondervinden die haaks staan op de doelen die met dit project worden beoogd.
    - Realiseer je dat er niet kan worden aangetoond dat er een goede afweging is gemaakt tussen de privacyrechten van betrokkenen en andere belangen.
    - Realiseer je dat je handelt in strijd met de Algemene verordening gegevensbescherming en mogelijk ook de Wet politiegegevens. Hiervoor kan de Autoriteit Persoonsgegevens een boete opleggen.
    - Neem, in ieder geval een besluit over het (z.s.m.) alsnog uitvoeren van een Risico-analyse (RA). Leg in het besluit concreet vast wanneer de risico analsye zal zijn uitgevoerd en stuur hier daadwerkelijk op. Zorg ook dat er voldoende capaciteit beschikbaar is voor het uitvoeren van deze RA. Dit kan betekenen dat er moet worden geprioriteerd.

  Voor zover het advies niet wordt overgenomen en de partners niet in staat zijn om een FG advies te overleggen:

[1] *De termen Risico analyse en DPIA worden door elkaar gebruikt. Een DPIA is in deze casus, gelet op de hoge risico's, verplicht op grond van de AVG. Met een DPIA worden de privacyrisico's voor betrokkenen in beeld gebracht. De term Risico analyse is breder, er wordt niet alleen een DPIA uitgevoerd maar ook worden de risico's voor de organisatie in beeld gebracht. De gemeente Helmond heeft als afspraak dat er bij het uitvoeren van een DPIA altijd de brede Risico analyse wordt uitgevoerd.*

  - Spreek in ieder geval af wanneer zij (uiterlijk) een FG advies overleggen en stuur hier op.
  - Leg deze afspraak schriftelijk vast en informeer de FG.

- Deel met de stuurgroep dit advies én het genomen besluit.

Toelichting

Om een goede afweging te kunnen maken tussen de individuele rechten en vrijheden (zoals het recht op privacy) en de rechten en vrijheden van anderen is het nodig om goed in beeld te brengen welke informatie er door wie wordt verwerkt. Door daarnaast in beeld te brengen welke risico's er worden gelopen kunnen maatregelen worden getroffen om de risico's terug te brengen tot een aanvaardbaar niveau. De AVG vereist dat dit gebeurt voordat je start met het verwerken van de gegevens.

Met de maatregelen wil je voorkomen dat de doelgroep van het project onbedoelde nadelige gevolgen ondervindt. Gevolgen die haaks kunnen staan op het doel van het project.
Denk aan:

- Het op een onveilige manier delen van informatie als gevolg waarvan informatie in handen valt van kwaadwillenden en de jongere bijvoorbeeld juist extra vatbaar wordt voor de invloed van criminele activiteiten, omdat men "iets weet" van de jongere.
- Het dubbel opslaan van gegevens, waardoor het risico bestaat dat (onjuiste) gegevens, in een voorkomend geval, niet op alle plekken worden verwijderd of aangepast, waardoor niet de juiste hulp wordt geboden.
- Het stigmatiseren van de jongeren die behoren tot de doelgroep als "risico jongere" wat een negatieve invloed op hun perspectief kan hebben. Bijvoorbeeld wanneer dit stigma aan hen blijft plakken terwijl de jongere niet langer tot de doelgroep behoort omdat de aanpak succesvol was.

Het is ook van belang voor het slagen van het project dat er grip te krijgen op de risico's ze in kaart te brengen en passende maatregelen te treffen.

Tijdlijn

Het is te begrijpen dat men wil starten met de uitvoering en dat verdere vertraging niet gewenst is. Het is echter al een jaar bekend dat het uitvoeren van een RA noodzakelijk is om afgewogen en met respect voor alle betrokkenen te kunnen starten met het project. Men is hier weliswaar mee gestart, maar dit is niet afgemaakt. Door het ontbreken van voortgang is de situatie ontstaan dat men nu wil starten met de uitvoering terwijl de RA nog niet is uitgevoerd.

- Op 15 januari 2024 heb ik geadviseerd om een **RA** uit te voeren.
- De organisatie heeft hier vervolgens PMP gevraagd om mee te denken vanuit de wettelijke kaders en een RA uit te voeren.
- PMP heeft in het voorjaar van 2024 in een beleidsanalyse op hoofdlijnen (verder beleidsanalyse) het antwoord gegeven op de vraag waar de balans ligt tussen privacybescherming en informatiedeling binnen het jeugdteam uit het programma Preventie met Gezag. (zie document 52373540).
- De beleidsanalyse is intern met mij besproken. Mijn reactie: Op zichzelf klopt het dat er binnen de diverse wetten ruimte is om te delen mits het goed is ingeregeld. Hoe je het goed inregelt moet uit de nog uit te voeren RA blijken. Deze **RA** is daarom belangrijk.
- De beleidsanalyse is op 14 mei 2024 besproken met de privacyadviseurs en/of FG's van de verschillende partners.
- Naar aanleiding van deze bijeenkomst heeft er op 7 augustus 2025 een aanvullend gesprek plaatsgevonden met politie en Openbaar Ministerie.
- De programmamanager is uitgevallen.
- De stuurgroep heeft op 17 september 2024 besloten om:
  - De samenwerking met PMP partners stop te zetten.
  - Privacy by design toe te passen, wat betekent dat al werkenderwijs een DPIA zal worden uitgevoerd.
- De gemeente Helmond heeft mij niet betrokken bij dit besluit (zie artikel 38 lid 1 van de AVG). Met het besluit om al werkenderwijs een DPIA uit te voeren (wat overigens het tegenovergestelde is van Privacy by Design toepassen) heeft de gemeente Helmond mijn eerdere adviezen niet opgevolgd.

- PMP heeft door de beëindiging van de samenwerking geen RA meer opgeleverd.
- Op 1 november 2024 is een nieuwe programmamanager gestart.
- De projectorganisatie heeft zich geconcentreerd op de uitvoering, concreet betekent dit dat er geen voortgang is geweest op het uitvoeren van een RA. Daarmee is de situatie ontstaan dat de projectorganisatie wil starten met het proces (de uitvoering) en dat hiervoor een besluit van de stuurgroep nodig is.
- De projectorganisatie heeft deze situatie is op 13 november 2024 besproken met mij (zie document 52374545). Ik heb aangegeven dat er pas kan worden gestart met de verwerking als er voldoende maatregelen zijn getroffen om veilig en verantwoord met de gegevens om te kunnen gaan. Er dient eerst **een RA** te worden uitgevoerd. Concreet is tijdens dit gesprek afgesproken dat het advies aan de stuurgroep is voorzien
    - Van de (privacy en informatiebeveiligings) risico's die de projectleider nu al ziet en de maatregelen om deze risico's te mitigeren.
    - Een concreet plan voor het vervolg om te komen tot een uitgebreide risico analyse op gebied van privacy en IB. Onderdeel van dit plan is de capaciteitsraming
    - Een advies van de FG van de gemeente Helmond.
- Op 8 januari 2025 ben ik mondeling op de hoogte gesteld van het voorstel om met Preventie met gezag aan te sluiten bij een bestaande overlegstructuur. De wens bestaat om te starten, en gelijktijdig (en niet voorafgaand) een RA uit te voeren. Die RA heeft niet alleen betrekking op Preventie met gezag als op de bestaande overlegstructuur.
- Op 23 januari 2025 heb ik het voorstel voor de stuurgroep ontvangen en ben ik in de gelegenheid gesteld om dit advies op te stellen.

Belangrijkste adviezen van PMP (zie document 52373540):

- Voor het voorzien in rechtswaarborgen is het wezenlijk dat de partners een gezamenlijke regieregeling treffen over de onderlinge verdeling van rollen, verantwoordelijkheden, aansprakelijkheidsrisico's.
- Naast de gezamenlijke regieregeling is een AVG-conforme dataprotectie impact assessment vereist. Een goede DPIA maakt inzichtelijk waar in de praktijk precies de valkuilen en kwetsbaarheden liggen. Op deze manier ontstaat ook inzicht in de mate waarin het samenwerkingsverband Preventie met Gezag al met passende waarborgen is omkleed. Naar AVG-maatstaven heeft de aanpak per definitie een hoog risicoprofiel. Dat is op zich niet problematisch maar noodzaakt tot extra degelijkheid.

Afdeling/Programma: Sociaal Domein

Onderwerp: Schuldenknooppunt.

Aanleiding

De Nederlandse Vereniging voor Volkskrediet (NVVK) en Vereniging Nederlandse Gemeenten (VNG) hebben een Schuldenknooppunt geïnitieerd om het berichtenverkeer in de schuldhulpverlening te vereenvoudigen en te versnellen. De gemeente Helmond is op dit Schuldenknooppunt aangesloten en heeft op 31 januari 2023 besloten om de aansluitovereenkomst te tekenen. De afdeling Sociaal Domein heeft een risico-analyse[1] uitgevoerd om de risico's in het gebruik van het Schuldenknooppunt in kaart te brengen, zodat passende maatregelen kunnen worden getroffen.

Conclusie

Het Schuldenknooppunt bevat gevoelige gegevens. Het risico voor de privacy van betrokkene is groot. Met het Schuldenknooppunt wordt een al bestaande gegevensuitwisseling tussen schuldhulpverleners en schuldeisers gedigitaliseerd en geüniformeerd. Deze gegevensuitwisseling is daarmee veiliger geworden. Dat neemt niet weg dat ook deze gegevensuitwisseling risico's met zich mee brengt. Deze risico's kunnen worden teruggebracht tot een aanvaardbaar risico door het advies van de FG en CISO op te volgen.

De gegevensuitwisseling in het Schuldenknooppunt is een processtap (of zijn meerdere processtap) van de schuldhulpverleningsprocessen. Dit advies heeft daarmee slechts betrekking op een (zeer) klein onderdeel van de schuldhulpverleningsprocessen. Om een veilige verwerking van (persoons)gegevens binnen de (volledige) processen te borgen is het noodzakelijk om ook op deze volledige processen een risico analyse uit te voeren.

Advies

De FG en CISO adviseren om:

- De in het register van verwerkingen opgenomen verwerking aan te passen en daar bij de diverse processen op te nemen dat het Schuldenknooppunt wordt geraadpleegd.
- Alle in de risico analyse opgenomen aanbevelingen over te nemen in een plan van aanpak.
- Naast de in de risico analyse aanbevolen werkinstructies, werkinstructies op te stellen voor:
    - Het versturen van berichten door de (3) geautoriseerde medewerkers en de wijze waarop zij het signaal ontvangen dat een bericht moet worden verstuurd.
    - De bezetting en de verdeling van de werkzaamheden van de geautoriseerde medewerkers, zodanig dat de bedrijfscontinuïteit is gewaarborgd. De instructie gaat in op het verbod om wachtwoorden te delen.
- Het opstellen van deze werkinstructies ook over te nemen in het op te stellen plan van aanpak.
- Het plan van aanpak vast te stellen. Daarbij van aanbevelingen die niet worden overgenomen expliciet vast te stellen dat ze niet worden overgenomen met een motivering.
- Het plan van aanpak toe te voegen aan Djuma zaaknummer 51729141
- De implementatie van het plan van aanpak te bewaken.

[1] Data Protection Impact Assessment Sociaal Domein, Gegevens vanuit het Schuldenknooppunt, d.d. 31-10-2023. (verder: risico analyse).

- Een risico analyse uit te voeren op alle schuldhulpverleningsprocessen en hier een concrete planning voor te maken. Betrek hierbij ook OnView. Neem dit mee in het project basis op orde SDV.
- Een nieuwe risico analyse uit te voeren voordat de koppeling met OnView in gebruik wordt genomen. Bij het maken van een planning rekening te houden met de capaciteit en de tijd die het maken van een dergelijke analyse kost.

De FG en de CISO hebben het advies gebaseerd op de volgende documenten:
- Data Protection Impact Assessment Sociaal Domein, Gegevens vanuit het Schuldenknooppunt, d.d. 31-10-2023. (verder: risico analyse).
- Advies van de FG d.d. 3-1-2023 (document 51337441)

Toelichting

Met het Schuldenknooppunt wordt een al bestaande gegevensuitwisseling tussen schuldhulpverleners en schuldeisers gedigitaliseerd en geüniformeerd. Deze gegevensuitwisseling betreft een (of meerdere) processtap(pen) binnen de volgende processen (verder hoofdprocessen genoemd):
- Hoofdproces SDV
- Aanmelden SDV
- Uitvoeren intake
- Vroegsignalering.

Om deze processen goed te kunnen uitvoeren is het noodzakelijk om gegevens uit te wisselen met schuldeisers. Met de aansluiting op het Schuldenknooppunt kan de communicatie met de (aangesloten) schuldeisers via dit portaal lopen in plaats van via (bv) de (digitale) post. Dit is in principe veiliger. De uitgevoerde risico analyse brengt duidelijk de risico's in beeld en beschrijft een aantal maatregelen om de risico's te maatregelen. Hierna volgt enige verduidelijking.

De uitgevoerde risico analyse heeft alleen betrekking op de (interne) processen om het schuldenknooppunt te gebruiken[2]. Het heeft geen betrekking op de hoofdprocessen ten behoeve waarvan deze gegevens worden verwerkt. De grondslag, noodzaak en proportionaliteit van de gegevensuitwisseling wordt wel bepaald door deze hoofdprocessen. Om een volledig inzicht te krijgen in risico's en noodzakelijke maatregelen is het daarom noodzakelijk om ook op deze hoofdprocessen een risico analyse uit te voeren.

De uitgevoerde risico analyse heeft wel betrekking op de processen die samenhangen met het uitwisselen van de gegevens in het schuldenknooppunt. De uitwisseling heeft betrekking op:
1. Het versturen van gegevens (berichten)[3]
2. Het ophalen van gegevens (berichten)

1. <u>Het versturen van berichten.</u>

Het initiërend bericht voor de gegevensuitwisseling is het bericht van de schuldhulpverlener dat een klant zich heeft gemeld voor schuldhulpverlening[3].
Daarnaast versturen zij berichten zoals:
- Saldoverzoek
- Betaalvoorstel

[2] De uitgevoerde risico analyse wekt soms een andere indruk.
[3] Het handboek schuldenknooppunt webportaal beschrijft welke berichten er kunnen worden opgehaald.

Deze berichten worden verstuurd door de tot het Schuldenknooppunt geautoriseerde medewerkers. Zij moeten op een of andere manier een signaal krijgen dat een bericht moet worden verstuurd. Het is niet duidelijk geworden hoe zij dit signaal ontvangen.

2. Het ophalen van berichten.

- Door de geautoriseerde medewerkers worden berichten gedownload in csv of pdf formaat.
- Deze berichten zijn een reactie op de opgevraagde informatie (verstuurde berichten[3]).
- Deze bestanden worden automatisch door de computers opgeslagen op de lokale schijf. Uit de uitgevoerde risico analyse blijkt dat het voorkomt dat deze gegevens te lang in de downloadfolder worden opgeslagen. De risico analyse bevat aanbevelingen om dit risico te verkleinen.
- De gegevens uit het Schuldenknooppunt worden (door dezelfde medewerkers) handmatig opgeslagen op dossierniveau in OnView. Deze applicatie ondersteunt de hoofdprocessen. OnView had daarom buiten scope van deze risico analyse mogen worden gehouden. Er zijn wel risico's bij het gebruik van OnView gedetecteerd en verbetervoorstellen gedaan. Omdat de hoofdprocessen niet zijn onderzocht, moet er rekening mee worden gehouden dat de gedetecteerde risico's niet volledig zijn.

De toegang tot het schuldenknooppunt is beperkt tot 3 accounts, toegang vindt plaats middels eHerkenning. Logische toegangsbeleid is (volgens de uitgevoerde risico analyse) ingeregeld.
De 3 medewerkers met een account zijn verantwoordelijk voor het versturen van berichten en voor het integer overzetten van de gegevens van het Schuldenknooppunt naar de interne applicatie OnView.

De beperking van het aantal accounts is een maatregel om onrechtmatige toegang te voorkomen. Het is echter ook een risico. Het versturen van berichten en het ophalen van de informatie en het verwerken van de informatie in Onview is immers beperkt tot 3 personen. Wanneer dit onvoldoende blijkt bestaat het risico dat:

- Berichten niet op tijd worden verstuurd of opgehaald. Waardoor:
    - De gegevens niet beschikbaar zijn op de juiste momenten
    - De gegevens niet juist zijn (want niet op tijd overgenomen in OnView)
    - Account gegevens worden gedeeld, om bij onvoldoende bezetting medewerkers te kunnen vervangen.

Het is daarom van belang dat er ook werkinstructies worden opgesteld over:

- Het versturen van berichten door de (3) geautoriseerde medewerkers en de wijze waarop zij het signaal ontvangen dat een bericht moet worden verstuurd.
- De bezetting en de verdeling van de werkzaamheden van de geautoriseerde medewerkers, zodanig dat de bedrijfscontinuïteit is gewaarborgd. De instructie gaat in op het verbod om wachtwoorden te delen.

Begin 2023 is aan het college voorgesteld om de aansluitovereenkomst van het schuldenknooppunt te tekenen. De FG heeft ten behoeve van dit voorstel het onderstaande advies uitgebracht (zie ook document 51337441). Hierna volgt een beoordeling of het advies is opgevolgd.

	Advies	*Beoordeling*	*Aanvullende maatregel.*
1	Ook op de interne processen een risico analyse uit te voeren en passende maatregelen te treffen. Door dit uit te voeren, voordat er daadwerkelijk gebruik wordt gemaakt van het schuldenknooppunt, wordt voorkomen dat achteraf herstelmaatregelen moeten worden getroffen. Ook vermindert daarmee de kans dat de schuldenaars onbedoeld nadelige gevolgen ondervinden van de gegevensuitwisseling.	De uitgevoerde risico analyse heeft alleen betrekking op de (interne) processen om het schuldenknooppunt te gebruiken[4]. Het heeft geen betrekking op de hoofdprocessen ten behoeve waarvan deze gegevens worden verwerkt. De grondslag, noodzaak en proportionaliteit van de gegevensuitwisseling wordt wel bepaald door deze hoofdprocessen. Om een volledig inzicht te krijgen in risico's en noodzakelijke maatregelen is het daarom noodzakelijk om ook op deze hoofdprocessen een risico analyse uit te voeren.	Een risico analyse uit te voeren op alle schuldhulpverleningsprocessen en hier een concrete planning voor te maken. Betrek hierbij ook On View. Neem dit mee in het project basis op orde SDV.
2	In ieder geval maatregelen te treffen om met voldoende zekerheid te waarborgen dat toegang tot de via het Schuldenknooppunt verkregen gegevens per dossier beperkt blijft tot medewerkers voor wie dat op grond van hun taak noodzakelijk is.	✓	
3	De verdere verwerking van de gedownloade bestanden en berichten te beschrijven.	Een beschrijving van de werkwijze bij het versturen van berichten ontbreekt. Voor het overige: ✓	Een werkinstructie op te stellen voor: Het versturen van berichten door de (3) geautoriseerde medewerkers en de wijze waarop zij het signaal ontvangen dat een bericht moet worden verstuurd.
4a	Te beschrijven welke bedreigingen (bij deze verdere verwerking) kunnen leiden tot: onrechtmatige toegang (bv omdat de gedownloade bestanden op een niet veilige plek worden opgeslagen);	Met maar 3 accounts bestaat het risico dat wachtwoorden worden uitgeleend. Voor het overige: ✓	Een werkinstructies op te stellen voor: De bezetting en de verdeling van de werkzaamheden van de geautoriseerde medewerkers, zodanig dat de bedrijfscontinuïteit is gewaarborgd. De instructie gaat in op het verbod om wachtwoorden te delen
4b	ongewenste wijziging van gegevens (bv omdat de gegevens niet juist worden overgenomen);	✓	

[4] De uitgevoerde risico analyse wekt soms een andere indruk.

4c	het niet beschikbaar zijn van gegevens (bv omdat het schuldenknooppunt geen database bevat waarin berichten worden bewaard). En te bepalen welke maatregelen er nodig zijn om deze (onder 4a,4b en 4c genoemde risico's te verminderen.	✓	
5	In ieder geval te beschrijven welke maatregelen er worden getroffen om te zorgen dat de gedownloade bestanden en berichten niet langer dan noodzakelijk worden opgeslagen in een vorm die het mogelijk maakt om betrokkenen te identificeren.	✓	
6	Een nieuwe risico analyse uit te voeren voordat de koppeling met ON View in gebruik wordt genomen.	Niet van toepassing, advies blijft van kracht.	Een nieuwe risico analyse uit te voeren voordat de koppeling met ON View in gebruik wordt genomen.

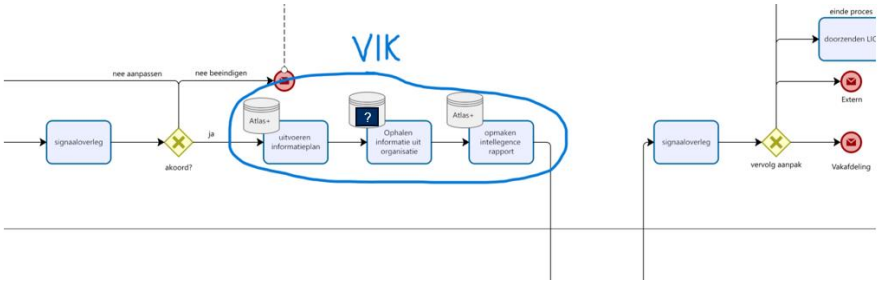
Advies van de FG en CISO

Afdeling/Programma:	Veiligheid & Naleving (VN)
Onderwerp:	Veiligheid Informatie Knooppunt (VIK)
Datum:	11 september 2024

Aanleiding

De afdeling VN wil binnen het proces binnengemeentelijke aanpak van ondermijning (verder de aanpak ondermijning) gebruik maken van een systeem dat dit proces mede ondersteunt. Dit wordt het Veiligheid Informatieknooppunt (VIK) genoemd. Hiervoor is een project gestart. Het VIK betreft het deel in de blauwe cirkel te zien in figuur 1. Dit is ook de scope van de uitgevoerde risicoanalyse en dit advies.

Binnen het proces van het VIK, gaat het om het raadplegen van registraties. Er is op basis van een voor- en nadelen analyse en advies vanuit SPO door de proceseigenaar besloten om hiervoor Analyse studio in te zetten[1]. Analysis Studio is de licentienaam. Dit betekent dat Analysis Studio op de plaats komt van het vraagteken in de afbeelding hieronder.



Figuur 1 Proces binnengemeentelijke aanpak ondermijning ingezoomd op het VIK-proces

Analysis Studio bestaat uit een server (i2 Analyze), waarmee (via een koppeling) verbinding wordt gemaakt met de basisregistraties[2]. De opgehaalde informatie wordt door Analysis Notebook omgezet in een tekening. Deze tekening wordt vervolgens geplakt in een rapportage (Word document), waar de analyse verder op wordt uitgevoerd. Het uiteindelijke bestand wordt in de applicatie Atlas+[3] opgeslagen. In i2 Analysize en Notebook vindt geen opslag plaats.

Er is een risico analyse uitgevoerd op (dit onderdeel van de aanpak ondermijning, het VIK) om in beeld te brengen wat de bij deze verwerking passende maatregelen zijn. Dit is noodzakelijk om te voldoen aan de privacywetgeving en informatiebeveiligingseisen.

De FG en de CISO hebben het advies gebaseerd op de volgende documenten:

- 1. DPIA uitwerking VIK

[1] Zie hiervoor zaak 52003151 in Djuma.
[2] Basisregistratie Adressen en Gebouwen (BAG), Handelsregister (NHR), Basisregistratie Kadaster (BKR) en Basisregistratie Personen (BRP).
[3] Dit is het binnen het proces “Bjnnengemeentelijke aanpak van ondermijning” gebruikte casemanagementsysteem

- 2. quickscan_privacy_en_beveiliging_VIK

Conclusie

Het risico voor de privacy van betrokkenen is groot. De aanpak ondermijning, brengt een gegevensverwerking met zich mee die een grote inbreuk maakt op de persoonlijke levenssfeer en de grondrechten van betrokkenen.

Er dienen aanvullende technische en organisatorische maatregelen te worden getroffen, om de persoonsgegevens te beschermen tegen onrechtmatige verwerking en inbreuken op de beschikbaarheid, integriteit en vertrouwelijkheid. Dit geldt voor de gehele aanpak ondermijning en niet alleen voor het onderdeel waar dit advies betrekking op heeft (het VIK).

Door de geadviseerde maatregelen over te nemen, kan gestart worden met het inrichten van het VIK en de bijbehorende applicatie. Met de uitvoering kan echter nog niet worden gestart. De rest-risico's voor betrokkenen zijn namelijk nog te hoog. Dit is omdat nog niet kan worden aangetoond dat in eerdere en latere fases van de aanpak ondermijning sprake is van een passende bescherming. Het ontbreken van een passende bescherming in deze andere fases heeft namelijk direct gevolgen voor de risico's die betrokkenen in deze fase (VIK) lopen.

Vanwege de hoge rest-riscio's voor betrokkenen dient vóór ingebruikname van het VIK:

- (in ieder geval) Alsnog te worden aangetoond dat ook in de eerdere en latere fases passende maatregelen zijn getroffen, of
- Voorafgaande raadpleging te worden aangevraagd bij de Autoriteit Persoonsgegevens.

Advies

De FG en CISO adviseren om, voordat er wordt gestart met de uitvoering van het VIK proces:

1. De / de in het register van verwerkingen opgenomen verwerkingen aan te passen en aanpak ondermijning, toe te voegen als ontvanger en verstrekker, daarnaast de BRP, BAG, NHR en BRK als verstrekker toe te voegen aan deze verwerkingen en tot slot i2 Analyze en Atlas+ als applicatie toe te voegen.
2. de BIV classificatie op te nemen in het register van verwerkingen.
3. Alle nog, in Excel bijlage 5: "Risico's vs maatregelen[4] " te implementeren maatregelen over te nemen in een plan van aanpak.
4. De implementatie van het plan van aanpak te bewaken.
5. Het plan van aanpak, dit advies en de administratie rondom de implementatie te archiveren.
6. Alle onderdelen van het proces 'aanpak ondermijning' te beschrijven. een risico-analyse uit te voeren op al deze onderdelen en de daarbij behorende passende maatregelen te treffen.
7. Het opgestelde privacy-protocol[5] aan te passen conform het door de FG gegeven[6] advies, en de bij 3 en 6 genoemde maatregelen.
8. De risico analyse te herhalen over drie jaar, of bij wijzigingen van het proces of de gebruikte systemen.

Voor zover de organisatie wil starten met de uitvoering van het VIK, voordat er kan worden aangetoond dat ook in de andere fases van de aanpak voldoende passende maatregelen zijn getroffen:

9. Vraag een voorafgaande raadpleging aan bij de Autoriteit Persoonsgegevens.

[4] Djuma documentnummer 52128863
[5] Djuma zaaknummer 51780294.
[6] Djuma Document 51832097

Advies van de FG en CISO

In bijlage 1 vindt u de volledige beoordeling van de risico analyse

Bijlagen

1 Toets van de risico analyse

Een risico analyse heeft betrekking op informatieveiligheid en privacy. Voor privacy geldt dat de AVG een aantal vereisten stelt aan de uit te voeren risico analyse: Dit zijn de volgende vereisten:

1. Een systematische beschrijving van de beoogde verwerking en de doeleinden;
2. Een beoordeling van de noodzaak en de evenredigheid;
3. Een beoordeling van de risico's voor de rechten en vrijheden van betrokkenen:
4. Een overzicht van beoogde maatregelen om deze risico's aan te pakken.

Ad 1 een systematische beschrijving

	omschrijving	Toelichting
1.1	De risico analyse vermeldt: de persoonsgegevens die worden verwerkt	Blz. 8, en 11 van de DPIA en bijlage 3 vermeldt de Persoonsgegevens die worden verwerkt in het VIK: *Persoonsgegevens opsomming uit BRP, BAG, NHR, BRK.*
1.2	De risico analyse vermeldt: de ontvangers van deze persoonsgegevens	Blz. 9 van de DPIA: vermeldt de Functionarissen die toegang krijgen tot de persoonsgegevens in het VIK. Dit zijn: 2 Data-Analisten informatieknooppunt. Deze functies vallen, zodra hiermee aan de slag wordt gegaan, binnen het VIK-proces onder het VIK-team. Deze twee personen voeren allebei dezelfde werkzaamheden voor het VIK uit. Daarom komt het onder de noemer VIK-team terug in de procesplaat. Eén van deze twee medewerkers heeft echter een extra functie en is naast VIK-team medewerker VIK coördinator.
1.3	De risico analyse vermeldt: de periode gedurende welke de persoonsgegevens worden bewaard	De periode gedurende welke persoonsgegeven worden bewaard komen niet terug in de DPIA. Gegevens worden niet bewaard in i2 Analyze of Notebook. Er wordt wel een word document opgesteld. Er bestaat geen noodzaak om het Word document te bewaren, anders dan in Atlas+ Atlas + bevat wel bewaartermijnen. Atlas+ is echter geen onderdeel van het VIK maar onderdeel van het vervolg. Het is daarom geen onderdeel van deze risico- analyse en dit advies. Zie verder onder 2.4
1.4	De risico analyse bevat een functionele beschrijving van de verwerking	Zie voor de setting of the scene het in kaart gebrachte proces en omschrijving op blz. 8 DPIA. Daarnaast op blz. 9 DPIA het kopje informatie over de software.
1.5	De risico analyse bevat de activa waarop persoonsgegevens steunen (hardware, software, netwerken, mensen, papier of papiertransmissiekanalen)	Zie blz. 7 t/m 10 DPIA

Formatted: English (United States)

Ad 2 De noodzaak en de evenredigheid wordt beoordeeld

Voldoet	omschrijving	Toelichting
2.1	De risico analyse vermeldt de grondslag en de doeleinden van de verwerking	Doeleinden: De inzet van bestuurlijke handhavingsinstrumenten om een Effectieve aanpak van ondermijnende activiteiten mogelijk te maken en de openbare ruimte veiliger te maken. Het VIK heeft als doel de casuïstiek sneller en beter in beeld krijgen (zie ook blz 9 DPIA) Grondslag: De aanpak van ondermijning heeft geen zelfstandige grondslag. De gemeente heeft wel een grondslag om bestuurlijke instrumenten in te zetten.

		Er is slechts een grondslag voor verwerkingen (en daarom ook voor raadplegingen) binnen het VIK, indien een grondslag gevonden kan worden bij de inzet van één of meerdere bestuurlijke instrumenten. Er bestaat daarom een risico dat er persoonsgegevens worden verwerkt zonder dat hiervoor een grondslag is. Er zijn daarom aanvullende maatregelen nodig, zie: 2.4
2.2	De risico analyse vermeldt welke gegevens en verwerkingen er noodzakelijk zijn voor het bereiken van dit doel	Voor de aanpak ondermijning verwerkt de gemeente gegevens naast de (klassieke) inzet door politie en justitie. Zij hebben voor het aanpakken van min of meer dezelfde problematiek ingrijpende wettelijke mogelijkheden beschikbaar. Deze wettelijke mogelijkheden bevatten waarborgen om de verwerkingen (en gegevensdeling) te toetsen op noodzaak en een disbalans in de bescherming van de burger te voorkomen. Anders dan bij de inzet door politie en justitie, wordt de door de gemeente uitgevoerde analyse niet gedekt door een concrete verdenking en er vindt geen preventieve onafhankelijke toets plaats over de inzet van bepaalde middelen. Er bestaat daarom een risico dat de gemeente informatie verzamelt waar politie en justitie geen toegang toe hebben, omdat zij wel gehouden zijn aan dergelijke waarborgen. Dit betekent ook dat er een risico bestaat dat er meer gegevens worden verwerkt dan noodzakelijk is voor de bestuurlijke aanpak. Er zijn daarom aanvullende maatregelen nodig, zie: 2.4.
2.3	De risico analyse vermeldt of er een minder ingrijpende gegevensverwerking mogelijk is	<u>Voor het VIK</u>: Zie alle opmerkingen die zijn gemaakt bij 2.1. en 2.2. Er zijn aanvullende maatregelen nodig, zie: 2.4 <u>Voor de keuze om een applicatie in te zetten:</u> Analysis studio, vervangt de handmatige raadpleging, het doel hiervan is om casuïstiek sneller en beter in beeld te krijgen In Notebook worden gegevens met elkaar in verbinding gebracht. De verwachting is dat er een beter beeld ontstaat en daarmee is de raadpleging via een systeem ook ingrijpendere dan de handmatige raadplegingen Anderzijds is minder kans op fouten omdat er een rechtstreekse koppeling is tot actuele gegevens. Er is bovendien een kans dat de verwachtingen te hoog gespannen zijn, aangezien er niet meer gegevens mogen worden verwerkt dan noodzakelijk. Het is denkbaar dat het maken van verbindingen minder vaak mogelijk is dan gedacht. Dit is ook door het SPO team aangegeven in de uitgevoerde voor- en nadelen analyse. De proceseigenaar heeft toch gekozen voor inzet van analysis Studio[1]. De wens om het systeem volwaardig in te kunnen zetten heeft het riscio in zich dat dit leidt tot onrechtmatige verwerkingen. Er zijn daarom aanvullende maatregelen nodig. zie 2.4.
2.4.	De risico analyse bevat een omschrijving van de maatregelen die worden getroffen om de verwerking te beperken tot de ter zake dienende noodzakelijke gegevens	De risico analyse bevat onvoldoende maatregelen om te borgen dat de verwerking zich beperkt tot de ter zake dienende noodzakelijk gegevens. Er bestaat een risico dat er gegevens worden verwerkt zonder grondslag of dat er meer gegevens worden verwerkt dan noodzakelijk voor het te bereiken doel. (zie ook 2.2.)_ Om dit risico terug te brengen tot een acceptabel niveau zijn aanvullende maatregelen nodig. Deze maatregelen zijn ook noodzakelijk om te zorgen dat function creep niet optreedt. Zie de Excel bijlage 5: Risico's vs maatregelen[4] voor de noodzakelijke maatregelen.

		Met het treffen van deze maatregelen worden risico's binnen het VIK proces gemitigeerd. Er kan echter nog niet worden vastgesteld dat er sprake is van een passende bescherming. kan nog niet worden aangetoond dat er sprake is van een passende bescherming. 1. De rechtmatigheid van de verwerking is met name afhankelijk van de vraag of in de eerdere fase rechtmatig gegevens worden verwerkt. Om te voorkomen dat elke inwoner het onderwerp kan worden van een onderzoek naar ondermijning, en daarmee van een verwerking van gegevens binnen het VIK, is er namelijk een duidelijk en objectief startpunt noodzakelijk. De andere fases in het proces aanpak ondermijning zijn echter geen onderwerp van deze risico analyse. 2. Het is nog onduidelijk of het in dit deelproces op te stellen Word document direct in Atlas+ worden opgeslagen of dat er nog opslag plaatsvindt op andere locaties (zoals one drive). Er bestaat echter geen noodzaak om het Word document te bewaren, anders dan in Atlas+. Indien de opslag niet beperkt wordt tot Atlas+ worden er meer gegevens verwerkt dan noodzakelijk. De andere fases in het proces aanpak ondermijning zijn echter geen onderwerp van deze risico analyse 3. De gemeente heeft een privacy protocol[5] opgesteld. In dit protocol beschrijft zij een stapsgewijze aanpak. Een privacy protocol is een goede maatregel die kan bijdragen aan rechtmatig gebruik. Het privacy protocol is geen onderwerp van deze risico analyse. De FG heeft op 2 januari 2024 wel geadviseerd over een concept protocol[6]. Het is daarom noodzakelijk dat (naast al genoemde maatregelen): 1. Ook in de voorfase voldoende maatregelen zijn getroffen om risico's op onrechtmatige verwerking te mitigeren. Om dit te kunnen vaststellen is er een beschrijving van het proces en een risico analyse nodig. 2. Een privacy protocol wordt vastgesteld conform advies van de FG d.d. 2 januari 2024[6]. Waarbij ook alle noodzakelijke maatregelen uit dit en toekomstige adviezen worden betrokken.
	De risico analyse bevat een omschrijving van de maatregelen die worden getroffen om te zorgen dat geen function creep[7] optreedt.	De verwerkingen binnen het VIK bevatten het risico op function creep. Er worden namelijk gegevens geraadpleegd (en anderszins verwerkt) die voor andere doelen zijn verzameld. Het risico bestaat dat de verwerking binnen het VIK niet past bij de oorspronkelijke bedoeling van de verwerking. Er zijn daarom aanvullende maatregelen nodig om te zorgen dat function creep niet optreedt: zie voor de maatregelen onder 2.4. Daarnaast is bij een verandering in de verwerking, (bv. het toevoegen van basisregistraties) een nieuwe afweging nodig. Het is daarom noodzakelijk dat de risico analyse wordt herhaald bij wijzigingen en in ieder geval over drie jaar.
	De risico analyse bevat een omschrijving van de maatregelen	De DPIA bevat geen maatregelen om te voorkomen dat gegevens langer dan noodzakelijk worden opgeslagen.

[7] function creep is wat er gebeurt als we technologie en systemen gebruiken op een andere manier dan in de eerste instantie eigenlijk bedoeld is, met name wanneer het nieuwe doel resulteert in een inbreuk op de privacy.

	die worden getroffen om ervoor te zorgen dat gegevens niet langer dan noodzakelijk worden opgeslagen in een vorm die het mogelijk maakt om betrokkene te identificeren.	Het is nog onduidelijk of dit document direct in Atlas+ worden opgeslagen of dat er nog opslag plaatsvindt op andere locaties (zoals one drive). Dit betekent dat het risico bestaat dat gegevens te lang worden bewaard. Atlas+ is geen onderwerp van deze risico-analyse en advies. Dit betekent dat (on)mogelijkheden, risico's en noodzakelijke maatregelen nog niet in beeld zijn. Er zijn daarom aanvullende maatregelen nodig. zie 2.4.
	De risico analyse bevat een omschrijving van de wijze waarop betrokkene (toereikend) wordt geïnformeerd.	Wanneer een signaal mono- of interdisciplinair wordt afgerond, ontvangt betrokkene informatie conform de wet- of regelgeving die van toepassing is. Er is niet opgenomen op welke wijze betrokkenen worden geïnformeerd indien een signaal niet wordt opgepakt. In de basis bestaat er een informatieplicht richting betrokkenen. Echter zijn er ook uitzonderingen mogelijk: UAVG art. 41 lid c. Daarom mag er voor de openbare veiligheid worden afgeweken, mits dit gemotiveerd gebeurt , i.v.m. noodzakelijkheid en op proportionaliteit. Zie Excel bijlage 5: Risico's vs maatregelen[4].
	de risico analyse bevat een omschrijving van hoe betrokkenen hun rechten uit kunnen oefenen: a. rechten van inzage b. recht op rectificatie en verwijdering c. recht op overdraagbaarheid van gegevens d. recht op bezwaar e. recht op beperking van de verwerking	Verwijzing naar de privacyverklaring op de website van de gemeente Helmond.
	de risico analyse beschrijft de relatie met verwerkers	Met Atlas+ is een verwerkersovereenkomst opgesteld. Voor Analysis Studio en Notebook is dit nog niet geregeld. Komt wel terug in de maatregelen dat dit uitgezocht moet worden, zie Excel bijlage 5: Risico's vs maatregelen[4].
	De risico analyse beschrijft de waarborgen omtrent internationale doorgifte	Er is geen sprake van internationale doorgifte.
	de risico analyse vermeldt of voorafgaande raadpleging nodig is	De verwerking binnen de aanpak levert hoge privacy risico's op. Deze risico's kunnen worden beperkt door de geadviseerde maatregelen op te volgen. Indien de organisatie besluit het advies niet of slechts deels op te volgen dan worden de risicos' onvoldoende beperkt en is voorafgaande raadpleging noodzakelijk.

Ad 3 de risico's voor de rechten en vrijheden van betrokkenen

Voldoet	omschrijving	Toelichting
	de risico analyse brengt de risico's voldoende in beeld.	Zie bijlage Excelbestand Risico's vs maatregelen[4].

Ad 4 de maatregelen worden benoemd

Voldoet	omschrijving	Toelichting

	de beoogde maatregelen om de risico's aan te pakken worden bepaald en zijn voldoende.	Hiervoor verwijs ik graag naar het Excelbestand Risico's vs maatregelen[4].

Afdeling	IVA
Onderwerp:	Meten van drukte in de binnenstad
Datum:	18 april 2024

Aanleiding

De uitspraak van de Rechtbank over de aan gemeente Enschede door de Autoriteit Persoonsgegevens opgelegde boete.

Sinds 2014 wordt het aantal bezoekers in het Helmondse centrum in opdracht van de gemeente door RMC geteld. De gemeente heeft op 11 mei 20211 besloten om te stoppen met deze manier van tellen. De reden hiervoor was een aan de gemeente Enschede opgelegde boete. De boete is door de Autoriteit Persoonsgegevens opgelegd, vanwege onrechtmatige verwerking van persoonsgegevens. Omdat de gemeente Helmond op dezelfde wijze de bezoekers telt, zou ook de verwerking van de gemeente Helmond onrechtmatig zijn.
De gemeente Helmond Enschede heeft beroep aangetekend tegen de opgelegde boete. Op 2 februari 2024 heeft de Rechtbank Zwolle het beroep van de gemeente Enschede gegrond verklaard.

Conclusie

- De gemeente ontvangt geen persoonsgegevens.
- Ook de leverancier verwerkt geen persoonsgegevens bij de meting. Bij de beschreven werkwijze (waarbij ook geen camera's worden gebruikt) is de informatie voldoende beschermd tegen re-identificatie.
- De AVG is van toepassing op persoonsgegevens. Omdat er geen persoonsgegevens worden verwerkt is er ook geen sprake van strijdigheid met de AVG.

Noot:
Gewijzigde technieken kunnen tot andere conclusies leiden.
Niet is onderzocht of er sprake is van verwerking van persoonsgegevens in het geval er wel camera's worden gebruikt.

Analyse

De kern van de discussie draait om de vraag of er bij de meting persoonsgegevens worden verwerkt.

Boetebesluit[2]:

Er worden de volgende gegevens verwerkt op de volgende momenten:
1. MAC adres en locatiegegevens op de sensor.
2. gehasht (gepseudonimiseerd) mac adres en locatiegegevens tijdens de verzending.
3. gepseudonimiseerd en afgeknipt mac adres en locatiegegevens op de server van PFM.

De Autoriteit Persoonsgegevens is van mening dat er sprake is van persoonsgegevens. De identiteit volgt weliswaar niet direct uit de (onder 1 t/m 3 genoemde) gegevens, maar de natuurlijke persoon is op basis van deze gegevens wel (alsnog) te identificeren is en dat deze identificatie geen

[1] Djuma zaaknummer: 50564108
[2] Duma, documentnummer: 51991718

onevenredige inspanning vergt. Hierbij gaat de AP er vanuit dat een medewerker ter plaatse de identiteit van een gebruiker van een mobiel apparaat met het blote oog kan achterhalen.

Uitspraak Rechtbank Zwolle

De rechtbank Zwolle is van oordeel dat de Autoriteit Persoonsgegevens onvoldoende heeft onderzocht of het redelijkerwijs te verwachten is dat de genoemde middelen worden gebruikt om de natuurlijke persoon direct of indirect te identificeren. Daarbij had men de kosten en de benodigde tijd voor identificatie met in achtneming van de beschikbare technologie betrokken moeten worden. De rechtbank meent dan ook dat de Autoriteit Persoonsgegevens niet heeft bewezen dat er persoonsgegevens worden verwerkt bij de meting.

Analyse FG Helmond

De uitspraak sluit niet uit dat de Autoriteit Persoonsgegevens in de toekomst alsnog bewijst dat er persoonsgegevens worden verwerkt bij de meting. Daarvoor zou zij moeten onderzoeken en onderbouwen dat het redelijkerwijs kan worden verwacht dat medewerkers de straat op gaan om betrokkenen ter plekke te identificeren. De FG acht het vergezocht dat op deze wijze re-identificatie van de gepseudonimiseerde data zal plaatsvinden.

Gewijzigde techniek

Door aanpassing van het besturingssysteem (Android en IOS) op de mobiele randapparatuur functioneert het Wifi protocol anders. Niet het daadwerkelijke MAC-adres wordt uitgezonden, maar bij elk probe request (een verzoek aan nabijgelegen WiFi acces points om informatie op te vragen van het netwerk) wordt een nieuw willekeurig Mac-adres gegenereerd[3]. Hierdoor wordt het moeilijker om de pseudonimisering ongedaan te maken.

Ook de leverancier heeft aanvullende maatregelen getroffen om de gegevens te beschermen tegen re-indentificatie[4].
De scanners vangen probe request, die een Mac-adres bevatten, op en deze worden geaggregeerd tot half uur niveaus. Deze verzamelde deels indirecte persoonsgegevens worden door middel van een one way hash en door verkorting teruggebracht tot het aantal randapparatuur. Deze verkorting vindt plaats door zes karakters van de individuele hash af te halen (ten tijde van het onderzoek ging het om drie karakters). Hierdoor kan alleen het aantal randapparatuur worden geteld na verkorting van de hashcode en niet meer het Mac-adres.
Op basis van de aantal wifi-signalen (gerandomiseerde en niet-gerandomiseerde) bepaalt CityTraffic het aantal passanten per half uur binnen zone. De methode waarop dit automatisch wordt gedaan is als volgt: de ruwe tellingen worden verwerkt tot passantenaantallen per half uur per locatie door de aantallen te verhogen/verlagen met lokale statistische coëfficiënten die het wifi-gebruik symboliseren. Daarna wordt er centraal gevalideerd per week met andere telgegevens, die beschikbaar zijn als stereoscopie-metingen van telsensoren, gps metingen van Google, bezoekersgegevens van andere onderzoeksbureaus (indien voorhanden). De ijking van de gegevens hoeft niet via camera's. Ook zonder camera's levert de telling een goed beeld op.

Informatie die de gemeente ontvangt

De data wordt door de leverancier aangeboden in rapporten en in dashboards. Het betreft statistische informatie er worden geen persoonsgegevens in aangetroffen.

[3] Zie blz 7 en verder van de door de leverancier uitgevoerde DPIA, documentnummer 51991886
[4] Zie blz 12 en verder van de door de leverancier uitgevoerde DPIA, documentnummer 51991886

De statistische informatie die de gemeente Helmond krijgt (het aantal bezoekers per tijdseenheid in het centrum) wordt gebruikt als beleidsinformatie en informatie voor de partijen die in het centrum actief (willen) zijn.

Afdeling:	Sociaal Domein
Onderwerp:	Zorgned
Datum:	27 juni 2024

Aanleiding

Het contract met de huidige leverancier van het processysteem Suite4Sociaal Domein loopt af. Afdeling Sociaal Domein heeft een aanbestedingsprocedure uitgevoerd en de opdracht gegund aan leverancier ZorgNed. Het processysteem Suite4SociaalDomein wordt vervangen door het processysteem met de naam ZorgNed.

De FG en de CISO hebben het advies gebaseerd op de volgende documenten en nadere afstemming hierover met DSPO 5.1.2e van afdeling Sociaal Domein:

- DPIAdefault (documentnummer 52064085 bij zaak nummer 51979585)
- Baseline toets (documentnummer 52064082 bij zaak nummer 51979585)
- Maatregelenoverzicht GAP-P voor DPIA Zorgned (uit de mail van 5.1.2e d.d. 10 juni 2024)

Conclusie

Met het ZorgNed systeem worden veel processen ondersteund met, vanwege de aard van deze processen, risicovolle verwerkingen. Van deze bestaande processen zijn de risico's niet in beeld. Daarom is het niet mogelijk om te komen tot een volledig overzicht van de maatregelen die noodzakelijk zijn om de risico's voor betrokkenen en de organisatie te mitigeren tot een aanvaardbaar risico. Het advies (en de uitgevoerde risico analyse) heeft daarom alleen betrekking op de privacy eisen die aan het systeem kunnen worden gesteld en een aantal te nemen informatiebeveiligingsmaatregelen. Er moet rekening mee gehouden worden dat een (noodzakelijke) analyse van de processen leidt tot aanvullende maatregelen met mogelijk extra kosten, bijvoorbeeld omdat het systeem hier niet (standaard) aan kan voldoen.

Advies

De FG en CISO adviseren om:

- een (meerjaren) planning te maken voor het maken van een analyse op alle processen en de gegevens die worden verwerkt. En op basis van deze analyses passende maatregelen te treffen.
- de BIV classificatie BBN2 op te nemen in Blue Dolphin
- Alle nog te implementeren maatregelen uit de bijlage 2 over te nemen in een plan van aanpak, voeg dit plan van aanpak toe aan de projectadministratie en bewaak de implementatie hiervan.
- De risico analyse te herhalen over drie jaar, of bij wijzigingen van het proces of de gebruikte systemen.

Bijlagen:

1. Toets van de risico analyse, is hierna in dit document opgenomen.
2. Te implementeren maatregelen. Dit is een aparte bijlage, Djuma documentnummer 52084800. Op het tabblad "Maatregelenlijst" in kolom A (Project) bevatten de te implementeren maatregelen de waarde "P".

Bijlagen

1 Toets van de risico analyse

Een risico analyse heeft betrekking op informatieveiligheid en privacy. Voor privacy geldt dat de AVG een aantal vereisten stelt aan de uit te voeren risico analyse: Dit zijn de volgende vereisten:

1. Een systematische beschrijving van de beoogde verwerking en de doeleinden;
2. Een beoordeling van de noodzaak en de evenredigheid;
3. Een beoordeling van de risico's voor de rechten en vrijheden van betrokkenen:
4. Een overzicht van beoogde maatregelen om deze risico's aan te pakken.

Ad 1 een systematische beschrijving

1	omschrijving	Toelichting
1.1	De risico analyse vermeldt: de persoonsgegevens die worden verwerkt	De risico analyse geeft dit in hoofdlijnen aan, aangezien het systeem diverse processen met persoonsgegevens ondersteunt. Het systeem bevat ook bijzondere persoonsgegevens van kwetsbare personen. Voor een volledig overzicht is een analyse op de diverse processen en de verwerkingen binnen deze processen nodig.
1.2	De risico analyse vermeldt: de ontvangers van deze persoonsgegevens	De risico analyse geeft niet aan wie de ontvangers zijn. Dit is ook moeilijk in te vullen aangezien het systeem diverse processen met persoonsgegevens ondersteunt. Voor een goede invulling van de ontvangers is een analyse op de diverse processen en de verwerkingen binnen deze processen nodig.
1.3	De risico analyse vermeldt: de periode gedurende welke de persoonsgegevens worden bewaard	De bewaartermijn is gekoppeld aan de diverse processen. Dit betekent ook dat er verschillende bewaartermijnen zijn. Advies: Het systeem dient geautomatiseerd te verwijderen na afloop van de bewaartermijn. Het systeem moet dit kunnen Van belang is dat het systeem vernietigingsljisten kan overleggen (zie maatregel 20.2.5.1).
1.4	De risico analyse bevat een functionele beschrijving van de verwerking	Een architectuur is beschreven in Djuma document 52064236
1.5	De risico analyse bevat de activa waarop persoonsgegevens steunen (hardware, software, netwerken, mensen, papier of papiertransmissiekanalen)	De risico analyse heeft enkel betrekking op het systeem.

Ad 2 De noodzaak en de evenredigheid wordt beoordeeld

2	omschrijving	Toelichting
2.1	De risico analyse vermeldt de grondslag en de doeleinden van de verwerking	De risico analyse geeft dit in hoofdlijnen aan, aangezien het systeem diverse processen met persoonsgegevens ondersteunt. Deze processen ondersteunen de uitvoering van aan de gemeente uitgevoerde taken (Artikel 6 lid 1 sub e).
2.2.	De risico analyse vermeldt welke gegevens en verwerkingen er noodzakelijk zijn voor het bereiken van dit doel	De risico analyse gaat hier niet op in. Dat is ook niet mogelijk omdat de analyse alleen betrekking heeft op het systeem. Voor een volledig overzicht is een analyse op de diverse processen en de verwerkingen binnen deze processen nodig.
2.3	De risico analyse vermeldt of er een minder ingrijpende gegevensverwerking mogelijk is	De risico analyse gaat hier niet op in. Dat is ook niet mogelijk omdat de analyse alleen betrekking heeft op het systeem. Voor een volledig overzicht is een analyse op de diverse processen en de verwerkingen binnen deze processen nodig.

2.4	De risico analyse bevat een omschrijving van de maatregelen die worden getroffen om de verwerking te beperken tot de ter zake dienende noodzakelijke gegevens	De risico analyse gaat hier niet op in. Dat is ook niet mogelijk omdat de analyse alleen betrekking heeft op het systeem. Voor een volledig overzicht is een analyse op de diverse processen en de verwerkingen binnen deze processen nodig.
2.5	De risico analyse bevat een omschrijving van de maatregelen die worden getroffen om te zorgen dat geen function creep[1] optreedt.	De risico analyse gaat hier niet op in. Dat is ook niet mogelijk omdat de analyse alleen betrekking heeft op het systeem. Voor een volledig overzicht is een analyse op de diverse processen en de verwerkingen binnen deze processen nodig.
2.6	De risico analyse bevat een omschrijving van de maatregelen die worden getroffen om ervoor te zorgen dat gegevens niet langer dan noodzakelijk worden opgeslagen in een vorm die het mogelijk maakt om betrokkene te identificeren.	Zie 1.3.
2.7	De risico analyse bevat een omschrijving van de wijze waarop betrokkene (toereikend) wordt geïnformeerd.	De verwerking volgt uit de wettelijke taken en de daarbij behorende processen. Binnen deze processen dienen betrokkenen te worden geïnformeerd. Er is een analyse op de diverse processen en de verwerkingen binnen deze processen nodig om een antwoord te kunnen geven op deze vragen.
2.8.	de risico analyse bevat een omschrijving van hoe betrokkenen hun rechten uit kunnen oefenen: a. rechten van inzage b. recht op rectificatie en verwijdering c. recht op overdraagbaarheid van gegevens d. recht op bezwaar e. recht op beperking van de verwerking	Dit zijn algemene procedures. De risico analyse verwijst naar deze procedures.
2.9.	de risico analyse beschrijft de relatie met verwerkers	De gemeente Helmond is verantwoordelijk voor de uitvoering van de diverse processen. Zorgned is verwerker. De verwerkersovereenkomst is getekend. Er ontbreekt echter 1 subverwerker (GoBIT) in de verwerkersovereenkomst. Deze actie komt terug als maatregel.
2.10.	De risico analyse beschrijft de waarborgen omtrent internationale doorgifte	Uit aanvullende vragen is duidelijk geworden dat Zorgned geen gegevens buiten Europa verwerkt. Dit is aldus ook opgenomen in de verwerkersovereenkomst.
2.11	de risico analyse vermeldt of voorafgaande raadpleging nodig is	n.v.t

Ad 3 de risico's voor de rechten en vrijheden van betrokkenen

Voldoet	omschrijving	Toelichting

[1] function creep is wat er gebeurt als we technologie en systemen gebruiken op een andere manier dan in de eerste instantie eigenlijk bedoeld is, met name wanneer het nieuwe doel resulteert in een inbreuk op de privacy.

	de risico analyse brengt de risico's voldoende in beeld.	Het systeem ondersteunt diverse processen. Het is niet mogelijk om alle risico's in beeld te brengen zonder ook alle risico's van deze processen in beeld te brengen.
	De bedreigingen die kunnen leiden tot onrechtmatige toegang zijn benoemd. De mogelijke gevolgen voor de rechten en vrijheden van betrokkenen zijn geïdentificeerd. Daarnaast zijn de risico's voor de organisatie benoemd. De waarschijnlijkheid en ernst zijn ingeschat.	Gelet op de aard van de gegevens zijn de mogelijke risico's voor betrokkenen ernstig. (blz 11 DPIA Djuma document 52064085). De impact voor de organisatie is Midden (baseline toets Djuma document 52064082
	De bedreigingen die kunnen leiden tot ongewenste wijziging zijn benoemd. De mogelijke gevolgen voor de rechten en vrijheden van betrokkenen zijn geïdentificeerd. Daarnaast zijn de risico's voor de organisatie benoemd. De waarschijnlijkheid en ernst zijn ingeschat.	Gelet op de aard van de gegevens zijn de mogelijke risico's voor betrokkenen ernstig. (blz 11 DPIA Djuma document 52064085). De impact voor de organisatie is Midden (baseline toets Djuma document 52064082
	De bedreigingen die kunnen leiden tot het niet beschikbaar zijn van gegevens zijn benoemd. De mogelijke gevolgen voor de rechten en vrijheden van betrokkenen zijn geïdentificeerd. Daarnaast zijn de risico's voor de organisatie benoemd. De waarschijnlijkheid en ernst zijn ingeschat.	Gelet op de aard van de gegevens zijn de mogelijke risico's voor betrokkenen aanzienlijk. (blz 11 DPIA Djuma document 52064085). De impact voor de organisatie is Midden (baseline toets Djuma document 52064082

Ad 4 de maatregelen worden benoemd

Voldoet	omschrijving	Toelichting
	de beoogde maatregelen om de risico's aan te pakken worden bepaald en zijn voldoende.	Zie bijlage.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens geanonimiseerd op grond van:

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

Kaders	Actiehouder
Implementeer het monitoring en loggingsbeleid.	SPO team
Stel een kader op wat proceseigenaren helpt bij het maken van een keuze over de wijze waarop betrokkenen worden geïnformeerd.	SPO team
Stel een informatiebeveiligings en privacy beleid 2024-2028 op en vast en neem de volgende wijzigingen mee: a. Wpg b. SPO organisatie c. Processenlandschap d. Wijziging RASCI: leg vast wie keuzes mag maken op het gebied van (rest)risico's, zoals accepteren of mitigeren	FG CISO
Beschrijf een procedure: verwijderen tijdelijke bestanden.	Adviseur informatiebeheer
Definieer de principes voor een verantwoord gebruik van data-analyse en/of zelflerende logica.	SPO team Project Digitale Stad
Definieer privacycriteria en vertaal ze naar een systeemeisenset met specifieke maatregelen, ontwerppatronen of functionaliteiten.	SPO team
Implementeer het proces incidentele gegevensverstrekking.	Projectleider gegevensmanagement
Onderzoek of opbouw met beleid en reglement in stand moet blijven.	FG CISO
Stel een informatiebeheerplan op.	Adviseur informatiebeheer
Stel een kader dataclassificatie op.	FG CISO
Stel een kader vast voor het uitvoeren van een Impact Assessment Mensenrechten en Algoritmes (IAMA) voorafgaand aan de inzet van algoritmen.	SPO team Project Digitale Stad
Stel een procedure op om partijen met wie gegevens worden gedeeld op te hoogte te brengen van wijzigingen.	Projectleider gegevensmanagement
Stel een sensorregister op en een afwegingskader.	
Stel een strategisch en tactisch kader Business Continuity Management (BCM) vast.	Projectleider BCM
Stel op basis van het vastgestelde kader (informeren betrokkenen) domeinspecifieke documenten, zoals een domeinspecifieke privacyverklaring, op.	SPO team
Stel uitgangspunten voor verantwoord gebruik van logaritme vast.	SPO team Project Digitale Stad
Stel vast wanneer en hoe uitgevoerde risico-analyses en de bijbehorende adviezen worden bekendgemaakt.	SPO team
Veranker de principes gebruik data analyse en zelflerende logica als onderdeel van een data- en analyticsstrategie.	SPO team Project Digitale Stad
Vertaal de principes verantwoord gebruik data-analyse en zelflerende logica naar praktische richtlijnen.	SPO team Project Digitale Stad
Werk een tactisch kader delen van informatie uit.	SPO team
Procesverbetering	**Actiehouder**
Zorg voor afstemming tussen SPO team en procesadviseurs over: a. aansluiten SPO, zodat risico's voor informatiebeveiliging en privacy worden meegenomen; b. prioriteren van procesverbetering.	SPO team
Zorg voor eenduidig overzicht van processen en register van verwerkingen	SPO team
Leg een relatie tussen processen, verwerkingen en applicaties.	Architecten
Zorg voor afstemming tussen SPO team en procesadviseurs over: a. aansluiten SPO, zodat risico's voor informatiebeveiliging en privacy worden meegenomen; b. prioriteren van procesverbetering.	Procesadviseur
Zorg voor eenduidig overzicht van processen en register van verwerkingen	Procesadviseur
Leg het verbetervoorstel procesmatig werken aan MT voor en geef de uitvoering prioriteit.	Procesadviseur
Herhaal de meting procesmatig werken, om groei te kunnen meten.	Procesadviseur
Voeg ook inhoudelijke kenmerken, waaronder persoonsgegevens die binnen het proces worden verwerkt toe aan de procesbeschrijvingen.	Procesadviseur
Pas het proces "aanbieden stukken ondernemingsraad" aan, door toe te voegen of de FG is betrokken.	Ondernemingsraad.
Architectuur	**Actiehouder**

Zorg dat je de domein architectuur informatiebeveliging en privacy hebt vastgesteld.	Architecten
Zorg dat je de data architectuur vastgesteld hebt.	Procesadviseur
Ontwikkel processen onder architectuur.	Procesadviseur
Zorg dat je een vastgestelde enterprise architectuur hebt.	Architecten
Maak de architectuurkaders leidend bij alle veranderingen binnen de organisatie met impact op de organisatie of de informatievoorziening	Architecten
Register van Verwerkingen	**Actiehouder**
Geef actualisering van het register de hoogste prioriteit geven en zorg voor afronding in Q1.	SPO team
Stel een register op voor de rol van verwerker.	SPO team
Ontwikkel het register verder door: a. Maak het toegankelijk voor proceseigenaar, medewerker en inwoner b. Stel een proces voor onderhoud en actualisatie vast. c. Stel een proces voor het doorgeven van wijzigingen en nieuwe verwerkingen vast. d. Stel een proces vast dat het mogelijk maakt om te monitoren of er sprake is van een regelmatige stroom van gewijzigde verwerkingen en nieuwe verwerkingen. e. Verwerkingen te classificeren en te benoemen welke verwerkingen een hoog risico inhouden, zodat een plan kan worden opgesteld voor het uitvoeren van risico analyses op bestaande processen.	SPO team
Vul het register aan met: a. De niet verplichte gegevens. b. De vindplaats DPIA zodat er overzicht ontstaat c. Samenwerkende partijen (leveranciers en ketenpartners).	SPO team
DSPO organisatie	**Actiehouder**
Stel vast dat binnen de afdeling blijvend inzet nodig is op de thema's privacy en informatieveiligheid.	DT/MT
Stel de taakverdeling vast. De inzet van de afdeling bestaat in ieder geval uit: a. Adviesvragen, risico analyses,tactische kaders, incidenten, register van verwerkingen, rechten van betrokkenen: optreden als -materiedeskundige; -procesdeskundige; -applicatiedeskundige (functioneel beheer). b. Verantwoording: -(mede) beantwoorden vragen privacy en informatiebeveiliging; -verzamelen bewijslast (kwaliteitsmonitor) hele jaar door. c. Doorontwikkelplannen/plan van aanpak nav risico analyse: -opstellen, uitvoeren, controleren en bijstellen (PDCA). d. Bewustwording: -ondersteunen gemeentebrede acties zoals "clear desk & clear screen"; -ogen en oren binnen domein; -actieve vertegenwoordiger.	DT/MT
Spreek afdelingsmanagers aan op de verantwoordelijkheid om privacy en informatieveiligheid te borgen binnen de processen en hiervoor de benodigde capaciteit vrij te maken.	Directie
Begroot bij nieuwe projecten ook capaciteit (binnen de afdeling) voor borging van privacy en informatieveiligheid binnen het project.	DT/MT
Stuur op daadwerkelijke levering van capaciteit.	Directie
Positionering FG	**Actiehouder**
Stel ee toezichtsplan/jaarplan op, neem in het plan de volgende controles op: a. Actualiteit register van verwerkingen. b. Actualiteit uitgevoerde risico-analyses. c. Rechtmatigheid van verwerkingen.	FG CISO
Herpostioneer de Functionaris voor de gegevensbescherming (FG), bij voorkeur rechtstreeks onder en bij de directie.	FG CISO
Breng de Functionaris voor de gegevensbescherming beter in positie door: a. Het bestuurlijk behandelproces aan te passen; b. Een proces in te richten om afwijkingen op het advies van de FG voor te leggen aan directie.	FG CISO
Gegevensmanagement	**Actiehouder**
Stel de architectuurprincipes voor gegevensmanagement vast.	Architecten

Breng het gegevenslandschap in beeld.	Architecten
Breng de relatie tussen processen, verwerkingen en applicaties in beeld.	Architecten Procesadviseurs Projectleider Gegevensmanagement Adviseur Informatiebeheer
Voer het projectplan gegevensmanagement uit.	Projectleider Gegevensmanagement
Toets gebruik van basis- en kerngegevens in bedrijfsprocessen en vakapplicaties, door: a. Periodiek te meten of gegevens volledig en actueel zijn. b. Kwaliteit gegevens en gegevensgebruik in beeld te brengen (dashboard). c. Een verbeterplan gegevenskwaliteit afnemers op te stellen. d. Losse lijstjes te onderzoeken.	Projectleider Gegevensmanagement
Stel een gegevenscatalogus, met gegevenswoordenboeken op die organisatiebreed het kader vormen.	Projectleider Gegevensmanagement
Breng het gegevenslandschap in beeld.	Projectleider Gegevensmanagement
Breng de informatie op netwerkschijven in Teams in beeld.	Projectleider Gegevensmanagement Adviseur Informatiebeheer
Risico management	**Actiehouder**
Pas het proces en de handreiking/het beleid aan, aan de huidige situatie met een centraal spo team	SPO team
Voorzie het proces van ondersteunende documenten. a. Betere rapportage. b. Betere ondersteuning bij beschrijving "setting of the scene'. c. Eenvoudige analyse voor eenvoudige zaken. d. Vastlegging hoe kan worden geleerd van eerdere adviezen en risico-analyses. e. Vastlegging vaste evaluatiemomenten gebruikte tools en proces. f. Toets of de ondernemingsraad om instemming of advies gevraagd moet worden.	SPO team
Leg rapportages en adviezen vast in het zaaksyteem.	SPO team
Leg vast: a. Op welke wijze keuzes op gebeid van (rest)risico's worden vastgelegd b. Hoe en waar afwijkingen op het advies worden vastgelegd. c. Hoe en waar een gemaakte belangenafweging moet worden vastl	SPO team
Zorg voor aansluiting tussen het uitvoeren van een Risico analsye Informatiebeveiliging, een Data protection impact assessment (DPIA) en een IAMA.	SPO team Project Digitale Stad
Ontwikkeling SPO Team	**Actiehouder**
Neem een besluit over de organisatorische inbedding van het SPO team.	SPO team
Leg de werkwijze van het SPO team vast (Way of working). a. leg het intakeproces vast.	SPO team
Werk de verdeling van de SPO's over de domeinen verder uit, formaliseer deze verdeling en deel het met de organisatie.	SPO team
Werk uit op welke wijze adviezen worden opgevolgd.	SPO team
Monitor de opvolging van adviezen.	SPO team
Organiseer kennisuitwisseling tussen SPO-team en OR.	SPO team
Stel een jaarplan op voor het SPO team. Onderdeel van dit jaarplan is: 1. een goed overzicht van uit te voeren acties en werkvooraad. 2. de doorontwikkeling van het SPO team qua: a. producten (werk en ontwikkel). b. kennis, waaronder: * Kennis en kunde over het uitvoeren van een risico analyse. * Kennis en kunde over algoritme/AI, geautomatiseerde besluitvorming en profilering. * Kennis over cookies en de daarover ingenomen standpunten van de toezichthouders.	SPO team
Neem een besluit over de organisatorische inbedding van het SPO team.	DT/MT
Leveranciersmanagement	**Actiehouder**
Onderzoek of SCC moeten worden toegepast of aangepast.	SPO team
Stel standaard overeenkomsten op voor partijen waarmee gegevens worden uitgewisseld (anders dan in de rol als verwerker).	SPO team

Neem in de te ontwikkelen lange termijn inkoop strategie en de te ontwikkelen domein architectuur informatiebeveiliging enprivacy maatregelen op die borgen dat: a. Afdelingen bij zelfstandig aanschaf van producten zich houden aan de Helmondse afspraken; b. De technische, architecturele, privacy en veiligheidseisen en/of wensen bij het maken van een keuze een doorslaggevende rol krijgen.	Architecten Adviseur informatiemanagement en beleid Team inkoop Service manager
Neem in de te ontwikkelen domein architectuur informatiebeveiliging enprivacy maatregelen op die borgen dat de mate waarin de leverancier privacy by design en privacy by default heeft toegepast.	Architecten
Zorg dat de te ontwikkelen cloud- en sourcingsstrategie(zie jaarplan IVA) ook waarborgen bevat dat de gegevens van de burgers veilig zijn. Neem de door de door de Europese privacytoezichthouders opgestelde aanbevelingen over in deze strategie.	Architecten Team inkoop Service manager
Neem in de te ontwikkelen lange termijn inkoop strategie maatregelen op die borgen dat de mate waarin de leverancier: a. privacy by design en privacy by default heeft toegepast ; b. de mogelijkheid tot logging standaard; c. maatregelen 20.4.6.1. tot en met 20.4.6.6 van het borgingsprodcut heeft toegepast een significante factor is bij het maken van een keuze.	Team inkoop Service manager
Controleer periodiek of de afspraken op papier in de praktijk worden nagekomen.	Service en contract manager Team verbonden partijen
Laat het samenwerkingsverband niet alleen verantwoording afleggen over de doelen en de middelen, maar ook over informatiebeveiliging en privacy	Service en contract manager
Onderzoek of contractmanagement centraal dient te worden belegd.	DT/MT
Bewustwording	**Actiehouder**
Evalueer het huidige bewustwordingsprogramma (van Brooklyn).	FG CISO SPO Team
Verleng, bij voorkeur, het contract met Brooklyn. (vanwege de continuïteit).	FG CISO SPO Team
Start een nieuwe aanbestedingsprocedure indien uit de evaluatie blijkt dat de kwaliteit zodanig was dat de continuïteit niet zwaarder moet wegen.	FG CISO SPO Team
Voer het bewustwordingsprogramma uit volgens plan van aanpak en zet daarbij in op cultuurverandering.	SPO team
Meet jaarlijks de mate van bewustwording van de organisatie.	SPO team
Breidt het bewustwordingsprogramma uit met domeinspecifieke bewustwordingsactiviteiten.	SPO team
Stel een communicatieplan op om: a. De processen rechten betrokkenen meer bekendheid te geven. b. De vereisten van toestemming meer bekendheid te geven. c. Het beleid meer bekendheid te geven binnen en buiten de organisatie.	SPO team
Stel een communicatieplan op om: om het proces incidentele gegevensverstrekking bekend te maken binnen de organisatie.	Projectleider Gegevensmanagement
Informeren betrokkenen	**Actiehouder**
Zorg dat de landelijk beschikbare kaders gemakkelijk vindbaar en toegankelijk zijn voor de medewerkers in de organisatie.	SPO team
Voeg aan de privacyverklaring op de website een link toe naar het privacybeleid en het privacyreglement.	SPO team
Breng alle websites waar de gemeente voor verantwoordelijk is in kaart.	SPO team
Onderzoek welke cookies op deze websites worden verzameld.	SPO team
Onderzoek actualiteit en toegankelijkheid van de cookieverklaring en toets aan het gewijzigd advies van de AP.	SPO team
Richt een proces in om privacy- en cookieverklaringen te actualiseren.	SPO team
Breng in kaart welke in gebruikzijnde systemen tot doel hebben pesoonsgegevens te laten vastleggen door betrokkenen (klantportaal).	SPO team
Stel op basis van het vastgestelde kader domeinspecifieke documenten, zoals een domeinspecifieke privacyverklaring, op.	SPO team
Breng in kaart welke in gebruikzijnde systemen tot doel hebben pesoonsgegevens te laten vastleggen door betrokkenen (klantportaal).	SPO team

(AOG) Stel een interne privacyverklaring op.	AOG
(AOG) Publiceer de privacyverklaring op intranet en in het personeelsportaal.	AOG
Stel op basis van het vastgestelde kader domeinspecifieke documenten, zoals een domeinspecifieke privacyverklaring, op.	Proceseigenaren
Zorg dat er een omnichanel strategie komt.	DT/MT
Richt een klantportaal in en zorg dat een inwoner daarbij verdergaande mogelijkheden tot zijn beschikking krijgt om zijn rechten uit te oefenen.	DT/MT
Rechten van betrokkenen	**Actiehouder**
Verbeter het proces rechten van betrokkenen: a. Stel een digitaal aanvraagformulier beschikbaar. b. Maak aanvragen via Digid mogelijk. c. Onderzoek door wie de verzoeken het beste kunnen worden afgehandeld SPO/DSPO. d. Onderzoek op welke wijze toegang tot documenten het beste kan worden geregeld. e. Stel een standaard SLA op en sluit deze SLA af met vakafdelingen.	SPO team
2. Implementeer het proces rechten van betrokkenen: a. Regel de juiste autorisaties. b. Regel het juiste mandaat. c. Communiceer de processen, zodat bij iedereen in de organisatie de werkwijze bekend is.	SPO team
Ethiek	**Actiehouder**
Borg de samenwerking tussen FG en ethische commissie.	FG CISO
Werk uit wat er wordt verstaan onder algoritme/AI, geautomatiseerde besluitvorming en profilering.	SPO team Project Digitale Stad
Houdt een logaritme register bij	SPO team Project Digitale Stad
Houdt een register bij van systemen waar geautomatiseerde besluitvorming plaatsvindt.	SPO team Project Digitale Stad
Benoem een ethische commissie	Project Digitale Stad
Stel de werkwijze van de ethische commissie vast.	Project Digitale Stad
Borg de samenwerking tussen FG en ethische commissie.	Project Digitale Stad FG
Implementeer data-ethiek in de organisatie en geef uitvoering aan de agenda Digitale grondrechten en ethiek 2022-2024.	Project Digitale Stad
Informatiebeveiliging	**Actiehouder**
Richt IT-service management in en richt het proces incidentemanagement in, waaronder a. het melden van datalekken. b. de positie van de FG binnen het crisisteam (bij incidenten) c. aanpassen mandaatregeling.	FG CISO SPO team Service- en contractmanager
Richt de TOPdesk applicatie in voor het melden van incidenten.	SPO team Service- en contractmanager
Implementeer IT-service management.	SPO team Service- en contractmanager
Ontwikkel managementinformatie IT servicemanagement.	SPO team Service- en contractmanager
Classificeer data.	SPO team
Richt een crisis organisatie in.	Projectleider BCM
Voer per afdeling een impact analyse uit en formuleer de continuïteitseisen met bijbehorende maatregelen.	Projectleider BCM
monitor op naleving van het proces:"eenmalige gegevensverstrekking".	Proceseigenaar
Verantwoording	**Actiehouder**
Verbeter het Information Security Management System (ISMS).	FG CISO
Publiceer het jaarverslag op een gemakkelijk vindbare plaats op de gemeentelijke website en op intranet.	FG CISO
Leg over alle processen verantwoording af op naleving van de BIO.	Proceseigenaar
Werk verantwoording privacy op afdelingsniveau verder uit.	SPO team

Maak een doorontwikkelplan waarin is op opgenomen welke acties en maatregelen er worden getroffen naar aanleiding van de aanbevelingen van de Functionaris voor de gegevensbescherming om de privacybescherming naar een hoger niveau te brengen en neem deze vervolgstappen op in de jaarplannen van de afdelingen.	SPO team
Ontwikkelen een dashboard "Stand van zaken privacy".	SPO team
Onderzoek op welke wijze kan worden samengewerkt met concern control.	SPO team
Monitor op naleving van het vastgestelde proces eenmalige gegevensverstrekking.	Projectleider Gegevensmanagement
Controleer auditlogbestanden.	Proceseigenaar
Monitor op toegang tot applicaties.	Proceseigenaar
Leg door het jaar heen verantwoording af over de stand van zaken.	Proceseigenaar
Stel vast of betrokkenen conform vastgestelde kader worden geïnformeerd.	Proceseigenaar
Neem in de jaarplannen van de afdeling een paragraaf op over informatiebeveiliging en privacy.	Proceseigenaar
Huis van de Stad	**Actiehouder**
Tref aanvullende maatregelen om de infrastuctuur en informatie te beschermen.	Programma Huis voor de Stad
Stel leidende uitgangspunten voor het hybride werken op.	AOG
WPG	**Actiehouder**
Stuur de rapportage van de interne audit naar de FG zodat zij kan vast stellen of zij een extra controle op naleving van de Wpg opneemt in haar toezichtsplan.	SPO team
Algemeen	**Actiehouder**
Het ambitieniveau is, gelet op de huidige groei, erg ambitieus. Realistischer is het om uit te gaan van een volwassenheidsniveau van 3 in de loop van 2024.	DT/MT
Zie de thema's privacy en informatieveiligheid worden gezien als een kwaltieitsaspect van de dienstverlening. Door de thema's te borgen in de processen en er in de planning rekening mee te houden dat hier tijd en capaciteit mee is gemoeid, zullen de thema's minder als belemmerend worden ervaren. De FG is het met de rekenkamer eens dat het management het beleid nog niet voldoende actief uitdraagt.	DT/MT
Draag het beleid actiever uit.	DT/MT
Stel een informatiebeleidsplan op dat overkoepelend vorm zal geven aan de ontwikkeling van de informatievoorziening.	Architectuur

Proces-eigenaar	DT/MT
	x
	x
	x
	x
	x
	x

Proces eigenaar	DT/MT
	x
x	

Proces eigenaar	DT/MT

	x
	x
Proces eigenaar	**DT/MT**
x	
Proces eigenaar	**DT/MT**
	x
	x
	x
	x
	x
	x
Proces eigenaar	**DT/MT**
	x
	x
Proces eigenaar	**DT/MT**

	x
Proces eigenaar	**DT/MT**
Proces eigenaar	**DT/MT**
	x
Proces eigenaar	**DT/MT**

x	x
x	
x	

Proces eigenaar	DT/MT

Proces eigenaar	DT/MT
x	

x	
x	
x	
	x
	x

Proces eigenaar	DT/MT

Proces eigenaar	DT/MT
x	
x	
	x
	x

Proces eigenaar	DT/MT
x	
x	
	x
x	
x	

Proces eigenaar	DT/MT
x	

x	
x	
x	
x	
x	
x	
x	
Proces eigenaar	**DT/MT**
	x
x	
Proces eigenaar	**DT/MT**
Proces eigenaar	**DT/MT**
	x
x	x
x	x

Algemene bevinding met betrekking tot Privacy by design en Privacy bij default.
De auditor (geeft in navolging van de externe auditor) aan dat niet volledig wordt voldaan aan de normen met betrekking tot gegevensbescherming door standaardinstellingen. (norm 7). De reden hiervoor is dat in het privacybeleid beperkt maatregelen zijn opgenomen omtrent privacy by design en privacy by default. De FG is het niet eens met deze conclusie.
Privacy by design en privacy by default zijn wel vastgelegd in Helmonds beleid. Daarvoor is het relevant dat:

- Privacy by default kan worden gezien als een onderdeel van privacy by design. Privacy by default vereist dat de standaardinstellingen altijd zo privacy-vriendelijk moeten zijn.
- Privacy by desing betekent dat je in een vroeg stadium een zorgvuldige omgang met persoonsgegevens wordt afgedwongen. Dit doe je door zo vroeg mogelijk in het proces de bij de risico's passende maatregelen te treffen.

In het (onderstaande) beleid is vastgelegd op welke wijze er vorm wordt gegeven aan privacy by design (en daarmee ook aan privacy by design):
1. Architectuurafspraken:

- Op 12 september 2022 heeft het MT/DT de visie werken onder architectuur vastgesteld. Grote en complexe veranderingen vinden onder architectuur plaats.
- Op 17 april 2023 heeft het DT/MT de richtinggevende principes vastgesteld. Eén van deze principes is: "We benutten kansen en en sturen op risico's".

2. Privacybeleid

- In paragraaf 4 van het privacybeleid is beschreven dat er bij nieuwe en veranderende processen diensten, producten en informatiesystemen een risico analyse wordt uitgevoerd. Daarbij wordt verwezen naar de Handreiking risicomanagement. Ook bij verwerkingen met een laag privacy risico moeten privacy en beveiligingsrisico's inzichtelijk zijn en passende maatregelen worden getroffen. (zie ook RM.02.02 Workingpaper risico analyses.docx

	Thema		Control	Vraag	Audit
norm 2	**Rechtmatig heid**	Art 3 lid 1, 3 en 4 Art 8 lid 1 Art 9 lid 1 en 2 Art 11 (m.u.v. lid 2) Art 13	Politiegegevens worden alleen verwerkt als dat nodig is voor de in de wet genoemde doeleinden. Geborgd is dat bij het verwerken van politiegegevens altijd sprake is van **doelbinding** en dat de gegevens niet op een onrechtmatige wijze, worden verwerkt.	Wordt er gewerkt conform procedures en werkinstructies. Worden er regelmatig deelwaarnemingen gedaan om de doelbinding vast te stellen?	nvt, wel is er met betrekking tot de verwerking van bijzondere categorieën van bijzondere gegevens opgehaald dat er in enkele gevallen bijzondere categoriën worden vastgelegd
norm 3		Art 3 lid 2 en 5	Er wordt geborgd dat de Politie- gegevens daartoe toereikend, ter zake dienend en beperkt zijn tot wat noodzakelijk is (niet bovenmatig) en dat de herkomst van gegevens voor art 9 verwerkingen wordt vermeld	Worden er regelmatig deelwaarnemingen gedaan om de noodzakelijkheid van de verwerking en de herkomst van gegevens vast te stellen? (denk ook aan verstrekkingen)	nvt
norm 4			Er zijn controles op de kwaliteit ingericht.		

	Juistheid en volledigheid	Art 4 lid 1	Er zijn procedures opgesteld voor het vernietigen en rectificeren van gegevens.	Hoe wordt de juistheid van gegevens gecontroleerd?	Er is een document opgesteld met maatregelen om de juistheid en volledigheid van politiegegevens te borgen. Deze maatregelen zijn echter nog nietgeïmplementeerd in 2022. (bron externe audit)
norm 6 en 8	**Privacy by design**	art 4a lid 1 t/m 5 en art 4c	Er zijn (aantoonbaar) risicoanalyses uitgevoerd waaruit het risiconiveau blijkt. De mitigerende maatregelen worden doorgevoerd. Evaluaties vinden plaatsen en maatregelen worden aangepast daar waar nodig,	Zijn er risico analyses uitgevoerd? Is er gecontroleerd of de maatregelen zijn uitgevoerd? Wordt de effectiviteit van de maatregelen getest? Is vastgesteld op welke processen nog een risico analyse moet worden uitgevoerd?	Er wordt voldaan aan de norm aangezien er een DPIA is uitgevoerd over BRS. Deze is echter niet beoordeeld door verwerkingsverantwoordleijke.
norm 10	**Autorisaties**	art 6 lid 2	Politiegegevens worden slechts verwerkt door ambtenaren van politie die voor deze taken zijn geautoriseerd.	Is er tweemaal per jaar een controle uitgevoerd op de toegekende autorisaties?	Er wordt nagenoeg volledig aan de eisen uit de norm voldaan. De auditor doet een aantal aanbevelingen
norm 26	**Register**	Art 31d lid 1 en 2	De organisatie heeft een verwerkingenregister dat de in de Wpg opgenomen gegevens bevat.	Zijn alle processen waarbij persoonsgegevens worden verwerkt vastgelegd in het register en is het register volledig gevuld? Is er een proces dat het actueel houden van het register borgt?	nvt.
norm 28	**Audits**	Art 33	Er wordt uitvoering gegeven aan de eisen zoals gesteld in de Regeling Periodieke Audit politiegegevens.	Is er een planning voor het uitvoeren van in- en externe audits. Is er (indien van toepassing) een verbeterplan opgesteld?	voldoet

Bewustwording		Wordt er aandacht besteedt aan bewustwording van de BOA's? Is daarbij specifiek aandacht voor de geheimhoudingsplicht en het verbod op het gebruik van profilering die leidt tot discriminatie?	is er een bewustwordingsplan?	nvt.

Domein I (openbare ruimte)		
Bevindingen FG	**Adviezen FG**	**extra onderzoek in 2025**
Binnen VN is een medewerker aangesteld om twee keer per jaar steekproeven uit te voeren op doelbinding noodzakelijkheid en herkomst van gegevens. In 2024 is eenmaal een deelwaarneming gedaan. De twee momenten voor 2025 staan we al in de agenda. Verwerking van bijzondere categoriën kunnen alleen onder voorwaarden plaatsvinden. In het kader van de interne audit is geadviseerd om steekproeven uit te voeren op de vastlegging van de bijzondere categoriën gegevens.	volg het advies van de interne auditor op en voer in 2025 steekproeven uit op de vastlegging van de bijzondere categoriën gegevens.	Aanvullend onderzoek in 2025: Opvragen van de steekproeven op de vastlegging van bijzondere categorieën gegevens, om vast te stellen dat wordt voldaan aan de wet.
		Er is reden voor een nader onderzoek.

In juli en in oktober 2024 heb ik een overzicht van de geïmplementeerde maatregelen opgevraagd. Deze heb ik niet ontvangen.	.	Het overzicht is opnieuw opgevraagd.
Mijn Advies van 2023: Stel vast op welke interne processen een risico analyse noodzakelijk is. Onderbouw waarom een risico-analyse niet noodzakelijk wordt geacht en vraag advies aan de FG. Neem het uitvoeren van risico analyses op in het afdelingsplan. Aan dit advies is geen opvolging gegeven.	Volg alsnog het advies uit 2023 op: : Stel vast op welke interne processen een risico analyse noodzakelijk is. Onderbouw waarom een risico-analyse niet noodzakelijk wordt geacht en vraag advies aan de FG. Neem het uitvoeren van risico analyses op in het afdelingsplan.	Er is reden voor een nader onderzoek Bij de proceseigenaar opvragen van besluit op dit advies.
Ik sluit me aan bij deze bevindingen.	Volg de aanbevelinggen van de interne auditor op.	Er is reden voor een nader onderzoek. Dit onderzoek richt zich op de vraag of de aanbevelingen zijn overgenomen.
Bij de laatste externe audit werd voldaan aan deze norm.		Er is geen reden voor een nader onderzoek
Er wordt voldaan aan de norm. Zie De FG heeft verder op 13 februari 2025 vastgesteld dat er een interne audit wordt uitgevoerd over het jaar 2024 en dat er een externe audit is ingepland (start juni 2025)		Er is geen reden voor een nader onderzoek

De FG heeft in 2024 geadviseerd om controle op deelname aan bewustwordingsactiviteiten uit te voeren. De afdeling geeft aan dat deelname aan activiteiten sinds 2025 wordt vastgelegd		Er is geen reden voor een nader onderzoek

	Thema		Control	Vraag	Audit
norm 2	**Rechtmatig heid**	Art 3 lid 1, 3 en 4 Art 8 lid 1 Art 9 lid 1 en 2 Art 11 (m.u.v. lid 2) Art 13	Politiegegevens worden alleen verwerkt als dat nodig is voor de in de wet genoemde doeleinden. Geborgd is dat bij het verwerken van politiegegevens altijd sprake is van **doelbinding** en dat de gegevens niet op een onrechtmatige wijze, worden verwerkt.	Wordt er gewerkt conform procedures en werkinstructies. Worden er regelmatig deelwaarnemingen gedaan om de doelbinding vast te stellen?	nvt, wel is er met betrekking tot de verwerking van bijzondere categorieën van bijzondere gegevens opgehaald dat er in enkele gevallen bijzondere categoriën worden vastgelegd
norm 3		Art 3 lid 2 en 5	Er wordt geborgd dat de Politie- gegevens daartoe toereikend, ter zake dienend en beperkt zijn tot wat noodzakelijk is (niet bovenmatig) en dat de herkomst van gegevens voor art 9 verwerkingen wordt vermeld	Worden er regelmatig deelwaarnemingen gedaan om de noodzakelijkheid van de verwerking en de herkomst van gegevens vast te stellen? (denk ook aan verstrekkingen)	nvt
norm 4			Er zijn controles op de kwaliteit ingericht.		

	Juistheid en volledigheid	Art 4 lid 1	Er zijn procedures opgesteld voor het vernietigen en rectificeren van gegevens.	Hoe wordt de juistheid van gegevens gecontroleerd?	Er is een document opgesteld met maatregelen om de juistheid en volledigheid van politiegegevens te borgen. Deze maatregelen zijn echter nog nietgeïmplementeerd in 2022. (bron externe audit)
norm 6 en 8	**Privacy by design**	art 4a lid 1 t/m 5 en art 4c	Er zijn (aantoonbaar) risicoanalyses uitgevoerd waaruit het risiconiveau blijkt. De mitigerende maatregelen worden doorgevoerd. Evaluaties vinden plaatsen en maatregelen worden aangepast daar waar nodig,	Zijn er risico analyses uitgevoerd? Is er gecontroleerd of de maatregelen zijn uitgevoerd? Wordt de effectiviteit van de maatregelen getest? Is vastgesteld op welke processen nog een risico analyse moet worden uitgevoerd?	Er wordt voldaan aan de norm aangezien er een DPIA is uitgevoerd over BRS. Deze is echter niet beoordeeld door verwerkingsverantwoordleijke.
norm 10	**Autorisaties**	art 6 lid 2	Politiegegevens worden slechts verwerkt door ambtenaren van politie die voor deze taken zijn geautoriseerd.	Is er tweemaal per jaar een controle uitgevoerd op de toegekende autorisaties?	Er wordt nagenoeg volledig aan de eisen uit de norm voldaan. De auditor doet een aantal aanbevelingen
norm 26	**Register**	Art 31d lid 1 en 2	De organisatie heeft een verwerkingenregister dat de in de Wpg opgenomen gegevens bevat.	Zijn alle processen waarbij persoonsgegevens worden verwerkt vastgelegd in het register en is het register volledig gevuld? Is er een proces dat het actueel houden van het register borgt?	nvt.
norm 28	**Audits**	Art 33	Er wordt uitvoering gegeven aan de eisen zoals gesteld in de Regeling Periodieke Audit politiegegevens.	Is er een planning voor het uitvoeren van in- en externe audits. Is er (indien van toepassing) een verbeterplan opgesteld?	voldoet

Bewustwording		Wordt er aandacht besteedt aan bewustwording van de BOA's? Is daarbij specifiek aandacht voor de geheimhoudingsplicht en het verbod op het gebruik van profilering die leidt tot discriminatie?	is er een bewustwordingsplan?	nvt.

Algemene bevinding met betrekking tot Privacy by design en Privacy bij default.
De auditor (geeft in navolging van de externe auditor) aan dat niet volledig wordt voldaan aan de normen met betrekking tot gegevensbescherming door standaardinstellingen. (norm 7). De reden hiervoor is dat in het privacybeleid beperkt maatregelen zijn opgenomen omtrent privacy by design en privacy by default. De FG is het niet eens met deze conclusie.
Privacy by design en privacy by default zijn wel vastgelegd in Helmonds beleid. Daarvoor is het relevant dat:

- Privacy by default kan worden gezien als een onderdeel van privacy by design. Privacy by default vereist dat de standaardinstellingen altijd zo privacy-vriendelijk moeten zijn.
- Privacy by desing betekent dat je in een vroeg stadium een zorgvuldige omgang met persoonsgegevens wordt afgedwongen. Dit doe je door zo vroeg mogelijk in het proces de bij de risico's passende maatregelen te treffen.

In het (onderstaande) beleid is vastgelegd op welke wijze er vorm wordt gegeven aan privacy by design (en daarmee ook aan privacy by design):
1. Architectuurafspraken:

- Op 12 september 2022 heeft het MT/DT de visie werken onder architectuur vastgesteld. Grote en complexe veranderingen vinden onder architectuur plaats.
- Op 17 april 2023 heeft het DT/MT de richtinggevende principes vastgesteld. Eén van deze principes is: "We benutten kansen en en sturen op risico's".

2. Privacybeleid

	Domein III (onderwijs)
Audit	**Bevindingen FG**
Verantwoordelijkheden t.a.v. de werkzaamheden rondom de Wpg zijn niet belegd binnen de afdeling.	De gemeente Helmond heeft de leerplichttaak gedelegeerd aan de GGD. De BOA's die in dienst zijn van de gemeente Helmond voeren de taken in mandaat uit. Op grond van artikel 1 onder c van de Bpg boa, is de gemeente Helmond als werkgever verwerkersverantwoordelijke voor de BOA taken. Voor zover de leerplichtambtenaren gegevens verwerken waar de AVG op van toepassing is, is de gemeente Helmond een verwerker en is de GGD verwerkersverantwoordelijke. Dit is, voor zover bekend bij de FG, niet opgenomen in het beleid/procedures. Er worden geen deelwaarnemingen gedaan. De auditrapportage geeft geen antwoord op de vraag of de herkomst van gegevens wordt vastgesteld. Er zijn geen deelwaarnemingen ontvangen op mijn verzoek om die te verstrekken. Ook de opgevraagde beleid en procedures zijn niet ontvangen.
Verantwoordelijkheden t.a.v. de werkzaamheden rondom de Wpg zijn niet belegd binnen de afdeling.	

Verantwoordelijkheden t.a.v. de werkzaamheden rondom de Wpg zijn niet belegd binnen de afdeling. Er is niet of nauwelijks opvolging gegeven aan bevindingen uit eerdere audits.	Op 10 juni 2024 heb ik een overzicht van de geïmplementeerde maatregelen opgevraagd. Deze heb ik niet ontvangen.
In de beleidsdocumentatie m.b.t. privacy zijn slechts in beperkte mate maatregelen omtrent Privacy by Design en Privacy by Default opgenomen; - Er is geen bewijslast m.b.t. DPIA's opgeleverd. Zodoende hebben wij niet kunnen vaststellen dat er DPIA's zijn uitgevoerd over verwerkingen van politiegegevens; Er is geen verwerkersovereenkosmt aanwezig tussen de gemeente Helmond en de externe partij Metaobjects.	Er zou in 2018 een PIA zijn uitgevoerd door een werkgroep onder leiding van de functionaris gegevensbescherming van de GGD BZO. De PIA rapportage zou zijn opgeleverd aan de sectormanager van GGD BZO. (zie mailtje in map P:\DSPO\Verantwoording Privacy en informatiebeveiliging 2023\Verantwoording Privacy 2023\bewijslast\Wpg\domeinIII) De leerplichttaak is naar de GGD gedelegeerd om een probleem rondom toegang tot de BRP op te lossen. Hierdoor is de gemeente Helmond niet verantwoordleijk voor de contracten met de leverancier. Die verantwoordelijkheid ligt bij de GGD. De GGD heeft de gemeente Eindhoven ingeschakeld als verwerker, die vervolgens weer afspraken heeft gemaakt met de leverancier. (zie ook analyse in map P:\DSPO\Verantwoording Privacy en informatiebeveiliging 2023\Verantwoording Privacy 2023\bewijslast\Wpg\domeinIII). Er zijn geen risico analyses uitgevoerd op alle processen waarvoor JVS wordt gebruikt. Gelet op de ingewikkelde construcite is er wel aanleiding om risico analyses uit tevoeren. Mijn advies over 2024 was: Vraag bij GGD BZO de uitvoerde PIA rapportage en het advies van de FG van de GGD op
Bestan en werking worden niet aangetoond, Verantwoordelijkheden t.a.v. de werkzaamheden rondom de Wpg zijn niet belegd binnen de afdeling.	Er zijn geen deelwaarnemingen ontvangen op mijn verzoek om die te verstrekken
Er is geen procedure aanwezig voor het beheren en onderhouden van het verwerkingsregister. Ook vind er geen controle op het verwerkingsregister plaats.	Geen aaanvullende bevindingen
	Er wordt voldaan aan de norm. Zie De FG heeft verder op 31 maart 2025 vastgesteld dat er een interne audit wordt uitgevoerd over het jaar 2024 en dat er een externe audit is ingepland (start juni 2025)

Er is geen bewijslast opgeleverd waaruit blijkt dat alle nieuwe medewerkers verplicht een bewustwordingscursus hebben gevolgen;	Geen aanvullende bevindingen.

Adviezen FG	extra onderzoek in 2025
Wijs iemand aan die deelwaarneming doet om doelbinding, noodzakelijkheid en herkomst van gegevens vast te stellen. Doe minimaal tweemaal per jaar deelwaarnemingen en leg de uitkomst vast. Leg de onderlinge verhoudingen vast in een beleid en procedures.	Aanvuillend onderzoek in 2025: Opvragen van de steekproeven op de vastlegging van bijzondere categorieën gegevens, en opvragen beleid en procedures.
	Aanvullend onderzoek:

Beleg de verantwoordelijkheden t.a.v. de werkzaamheden rondom de Wpg binnen de afdeling. Volg als nog de bevindingen uit eerdere audits op en implementeer de maatregelen.	Opvragen of de werkzaamheden zijn belegd en opvragen van een overzicht van geïmplementeerde maatregelen.
Volg alsnog het advies uit 2023 op: Vraag bij GGD BZO de uitvoerde PIA rapportage en het advies van de FG van de GGD op. Stel vast op welke interne processen een risico analyse noodzakelijk is. Onderbouw waarom een risico-analyse niet noodzakelijk wordt geacht en vraag advies aan de FG. Neem het uitvoeren van risico analyses op in het afdelingsplan.	Aanvullend onderzoek Opvragen stand van zaken
Volg de aanbevelingen van de interne auditor op.	Aanvullend onderzoek: Opvragen van de periodieke controles
	Er is geen reden voor een nader onderzoek

Bespreek in de personeelsgesprekken met medewerkers of er wordt deelgenomen aan bewustwordingsactiviteiten en leg deelname vast in het personeelsdossier.	Aanvullend onderzoek: opvragen van uitgevoerde controles op deelname aan bewustwordingsactiviteiten door nieuwe medewerkers.

Gemeente Helmond

Jaarverslag 2022

Privacy

1 maart 2023

5.1.2e

Inhoud

1. Managementsamenvatting
2. Inleiding
3. Resultaten van het afgelopen jaar
   - Beleid
   - Processen
   - Organisatorische inbedding
   - Rechten van betrokkene
   - Samenwerking
   - Beveiliging
   - Verantwoording
   - Wet Politiegegevens
4. Vooruitblik

Managementsamenvatting

Bevindingen

De organisatie is nog niet volwassen.

De organisatie kan nog niet aantonen dat de persoonsgegevens van haar inwoners en medewerkers verantwoord worden gebruikt en veilig zijn. Daarvoor is minimaal een volwassenheidsniveau van 3 nodig en daar is de organisatie nog niet.

Helmond is gegroeid.

Afgelopen jaar is Helmond gegroeid van 1,7 naar 2,1. Ze neemt privacy en informatiebeveiliging serieus en wil z.s.m. doorgroeien naar 3. Om dit te bereiken is een centraal team met Security en Privacy officers (SPO team) aangesteld.

De basis voor versnelling is gelegd.

Met het SPO team is er extra capaciteit en kennis in de organisatie gekomen om de proceseigenaar te ondersteunen bij privacy en informatiebeveiligingsvraagstukken. Daarnaast is in 2022 het aangekochte bewustwordingsprogramma live gegaan. Metingen tonen aan dat het bewustzijn bij medewerkers is toegenomen.

Adviezen

Zorg voor inzicht in de persoonsgegevens die worden verwerkt binnen processen.

Breng het gegevenslandschap in beeld, waarbij een relatie wordt gelegd tussen processen, verwerkingen en applicaties. Zorg dat het register van verwerkingen volledig en actueel is en blijft en benoem de meest risicovolle processen. Daarmee verkrijgt de organisatie beter inzicht in de persoonsgegevens die zij verwerkt. Waardoor ze ook beter kunnen worden beschermd.

Pas risicomanagement toe

Zorg dat risicomanagement de basis wordt van Privacy en informatiebeveiliging. Zo kunnen de risico's teruggebracht worden naar een acceptabel niveau voor de organisatie en voor betrokkenen. Het zal hierdoor gemakkelijker worden om zicht te krijgen op de bedreigingen. Ook de naleving van de acties die hieruit voortvloeien zal gemakkelijker worden.

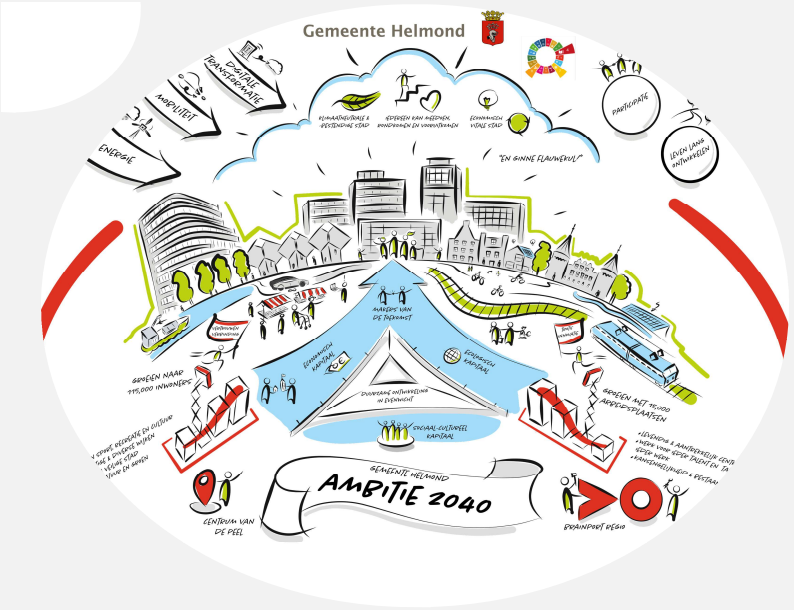
Onderzoek daarnaast ook voor alle bestaande processen de privacyrisico's en de noodzakelijke maatregelen. Begin bij de meest risicovolle processen.

Draag het privacy en IB beleid actiever uit.

Zie informatiebeveiliging en privacy, net als financiën en personeel, als een integrale managementtaak en maak ook op de werkvloer capaciteit vrij voor deze thema's. Draag als management uit dat privacy en informatiebeveiliging **de kwaliteit van de dienstverlening verbeteren**.

Inleiding

- De ambities in de stad Helmond zijn groot. Ze wil een klimaatneutrale bestendige en vitale stad zijn waar iedereen kan meedoen, rondkomen en vooruitkomen. Dit doet zij vanuit haar kernwaarden: trots, verbinding, vertrouwen en innovatie.
- Daarbij heeft ze te maken met de digitale transformatie. De razendsnel groeiende digitale wereld geeft mogelijkheden waar de stad gebruik van wil maken. Zowel de inwoners als de medewerkers moeten er op kunnen vertrouwen dat dit veilig gebeurt en met respect voor hun privacy.
- Dit jaarverslag geeft inzicht in waar de organisatie staat op het gebied van de veilige verwerking van persoons- en politiegegevens. Naast het geven van inzicht bevat dit jaarverslag aanbevelingen om verder te groeien, zodat Helmond haar inwoners en medewerkers kan laten zien:
  - wat er met hun gegevens gebeurt;
  - dat hun gegevens goed zijn beschermd en op een veilige wijze worden verwerkt.
- Dit jaarverslag is opgesteld door 5.1.2e . 5.1.2e is aangesteld als Functionaris voor de Gegevensbescherming (FG) en ziet toe op de naleving van de Algemene verordening gegevensbescherming (AVG) en de Wet politiegegevens (Wpg).
- Leeswijzer: Allereerst vindt u de samenvatting van de bevindingen en aanbevelingen van de FG over de naleving van de AVG en de Wpg. Daarna ziet u de volwassenheid van de organisatie. Vervolgens leest u per thema de bevindingen van de FG en haar advies. Tot slot kijkt de FG vooruit. In de bijlagen vindt u een infograhpic, met een overzicht van het jaarverslag.
- Dit jaarverslag bevat een samenvatting van de bevindingen en de adviezen van de FG. In bijlage 1 vindt u de uitgevoerde analyse. Zie Bijlage 1 Gap analyse privacy 2022.xlsx. In bijlage 2 vindt u alle adviezen van de FG. Zie bijlage 2 Adviezen FG .xlsx.



Volwassenheid

- Het volwassenheidsniveau Privacy van de gemeente is 2,1 op een schaal van 5. Dit is gelijk aan het volwassenheidsniveau informatiebeveiliging

- De gemeente Helmond groeit met kleine stappen. Eind 2020 was het volwassenheidsniveau 1,4. Met dit tempo duurt het te lang voordat de gemeente Helmond kan aantonen dat de gegevens van haar inwoners volledig zijn beschermd.

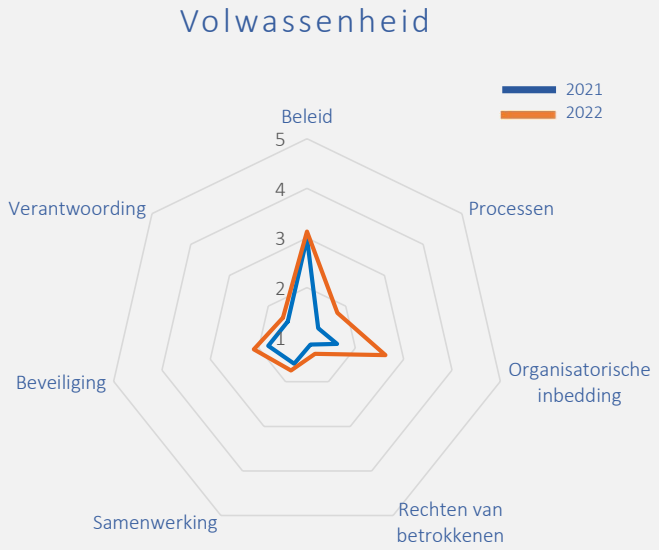
- De gemeente heeft dit onderkend en heeft daarom in 2022
  - Een privacy team (het SPO team) gevormd;
  - Een bewustwordingsprogramma ingekocht.

  Deze twee elementen hebben een bijdrage geleverd aan de groei in volwassenheid maar hebben nog niet gezorgd voor een significante versnelling.

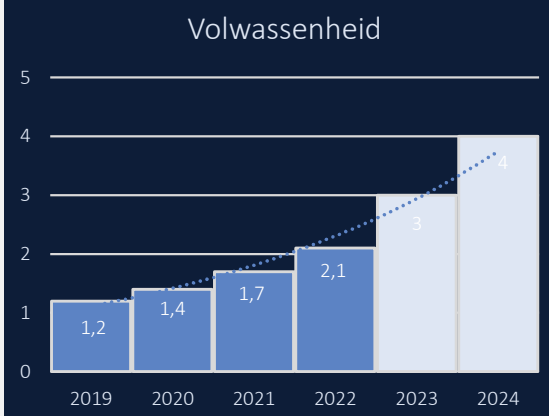
- Om een veilige verwerking van persoonsgegevens te kunnen realiseren is het essentieel dat er een stevig IT-fundament komt. Voor dit fundament is het essentieel dat procesmatig werken wordt verbeterd, functioneel en applicatiebeheer verder worden geprofessionaliseerd en dat ook het werken onder architectuur verder wordt geïmplementeerd. Tot slot zijn de inrichting van IT-servicemanagement en gegevensmanagement noodzakelijk.

- Daarnaast is een juiste houding ten opzichte van de thema's Informatiebeveiliging en privacy nodig. Het omarmen van de thema's als onderwerpen die de kwaliteit van de dienstverlening verbeteren en ze te zien als een integrale management taak is essentieel voor een groei in volwassenheid.

- De volwassenheid wordt beoordeeld op 7 thema's. Hiervoor is, gebruik gemaakt van het borgingsproduct van VNG Informatiebeveiligingsdienst (VNG IBD).



Noot: De laagste score bepaalt de volwassenheid van de organisatie. Om inzicht te geven in de groei is hier niet van uitgegaan, maar is er uitgegaan van de gemiddelde score per thema.



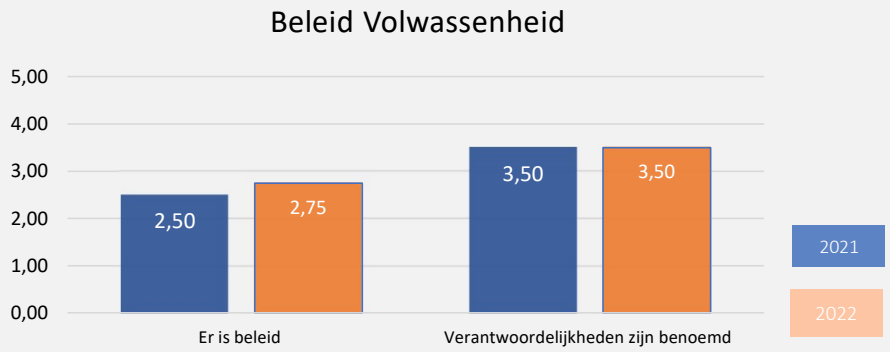
De gemeente Helmond heeft de ambitie om te groeien naar een volwassenheidsniveau van 3 in 2023 en niveau 4 eind 2024 .

Advies:
Het ambitieniveau is, gelet op de huidige groei, erg ambitieus. Realistischer is het om uit te gaan van een volwassenheidsniveau van 3 in de loop van 2024.

Beleid

Het privacybeleid beschrijft hoe de organisatie invulling geeft aan de veilige verwerking van persoonsgegevens.

- Op 10 november 2020 is het privacybeleid 2020-2024 vastgesteld. Dit beleid is compleet en er is samenhang met het informatiebeveiligingsbeleid. Hoewel het privacybeleid is gepubliceerd, is het nog niet bij iedereen bekend. In 2023 wordt een nieuw beleid opgesteld.
- Verantwoordelijkheden met betrekking tot de veilige verwerking van persoonsgegevens zijn vastgelegd en worden opgepakt, dit gebeurt echter nog niet structureel. Het is afhankelijk van de proceseigenaar of hij binnen zijn afdeling capaciteit vrijmaakt voor de thema's privacy en informatiebeveiliging.



Advies

Voor niveau 2:

- Stel een informatiebeveiliging en privacy beleid 2024-2028 op en vast.

Voor niveau 3:

- Stel een communicatieplan op, om het beleid meer bekendheid te geven binnen en buiten de organisatie.

Processen

Om haar inwoners en medewerkers goed van dienst te kunnen zijn worden binnen de processen persoonsgegevens gebruikt. Om dit zorgvuldig te kunnen doen is inzicht nodig in de processen. Daarnaast is inzicht nodig in de persoonsgegevens, die in de processen worden gebruikt. Tot slot is het nodig dat bekend is op welke wijze gegevens worden verwerkt en verstrekt.

❖ *Processen, instructies en register*

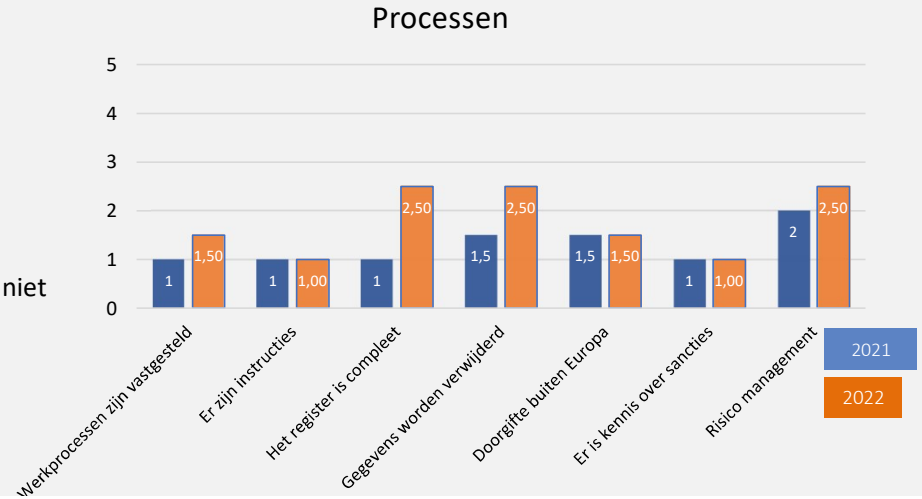
- Er is procesbeleid en een procesverbeterteam; werkprocessen worden conform het beleid gemodelleerd en geoptimaliseerd.
- De gemeentelijke organisatie is echter nog niet georganiseerd op het faciliteren van verandering, het denken in processen en het werken over ketens heen, zeker niet gezien vanuit een privacy perspectief. Een verbetering van het procesmatig werken zal bijdragen aan een beter inzicht in werkprocessen waarin persoonsgegevens worden verwerkt.
- Nog niet alle werkprocessen zijn beschreven en ze bevatten niet altijd een instructie hoe om te gaan met persoonsgegevens. Op dit moment verloopt proces optimalisatie en het ontwerp van processen nog buiten architectuur om.
- Het register van verwerkingen (RvV) is in 2022 verder gecompleteerd, het is echter nog altijd niet volledig.
- Verantwoordelijkheden voor het bijhouden van het RvV zijn onvolledig belegd.
- Er is daardoor geen volledig en actueel inzicht in de persoonsgegevens die worden verwerkt binnen de diverse werkprocessen.

❖ *Verwijderen*

- Verwijdering van gegevens in het zaaksysteem gebeurt automatisch en tijdig. Gegevens worden echter ook op andere plekken (persoonlijke schijven, MS Teams, mail) opgeslagen. Hierdoor is het niet vast te stellen dat in alle gevallen aan de wettelijke eisen rondom bewaren en vernietigen wordt voldaan.

❖ *Doorgifte en sancties*

- De standaard inkoopvoorwaarden en de standaard verwerkersovereenkomst bevatten bepalingen over de bescherming van de persoonsgegevens bij doorgifte naar landen buiten de EU.
- Afdelingen zijn echter gerechtigd zelfstandig producten (software en diensten) aan te schaffen. Zij zijn zich daarbij niet altijd bewust van de Helmondse afspraken en standaarddocumenten.



Advies

Voor niveau 2:

- Zorg voor een actueel register van verwerkingen dat aansluit op procesmatig werken en geef de actualisering de allerhoogste prioriteit.
- Voer het verbetervoorstel procesmatig werken uit en herhaal de meting.
- Zorg dat de domeinarchitectuur informatiebeveiliging en privacy worden uitgewerkt.
- Ontwikkel processen onder architectuur.
- Stel een cloud-en sourcingsstrategie op en neem de aanbevelingen van de privacytoezichthouder over.

Voor niveau 2,5:

- Betrek bij de prioritering van procesverbetering, de privacy risico's.
- Zorg dat in ieder geval de processen met een hoog privacy risico zijn beschreven.
- Zorg dat de verantwoordelijkheid voor het bijhouden van het RvV is belegd en wordt uitgevoerd, zodat het altijd actueel is.
- Stel een inkoopstrategie op, die faciliteert dat er wordt gekozen voor de meest privacyvriendelijke en veilige optie en dat afdelingen zich, bij zelfstandige aanschaf van producten of het aangaan van verplichtingen, houden aan de Helmondse afspraken en standaarden.

Voor niveau 3:

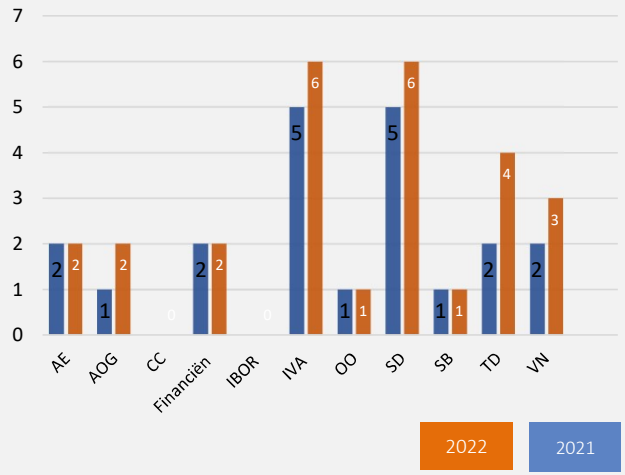
- Zorg dat voor alle processen bovengenoemde maatregelen zijn uitgevoerd.
- Stel een informatiebeheerplan op.
- Breng alle applicaties met een archieffunctie en alternatieve opslaglocaties (zoals teams) in beeld.
- Beschrijf een procedure voor het verwijderen van tijdelijke bestanden.
- Zorg dat er een volledig inzicht is in leveranciers die gegevens doorgeven buiten de EER en dat de transfermechanismen zijn getoetst.

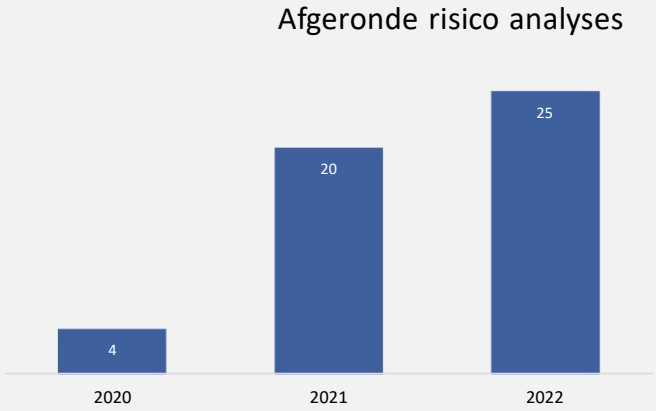
Processen

❖ Risicomanagement

Door in een vroeg stadium na te denken over de risico's, die het gebruik van persoonsgegevens met zich meebrengen, kunnen de juiste maatregelen worden getroffen. Risicomanagement zorgt hier voor.

- In 2022 zijn er meer risicoanalyses uitgevoerd dan in 2020 en 2021. De organisatie pakt steeds vaker deze taak actief op. Dit gebeurt echter nog niet structureel en het vastgestelde proces wordt niet altijd gevolgd. Niet altijd wordt het uitvoeren van een risico analyse als helpend ervaren.
- De uitgevoerde risicoanalyses en het uitgebrachte advies van FG en CISO over de uitgevoerde risicoanalyses worden gedocumenteerd. Mitigerende maatregelen worden niet consistent uitgevoerd en gedocumenteerd.





Advies

Voor niveau 2:

- Zorg voor verdere doorontwikkeling van het risicomanagement.
- Stimuleer een risicogerichte denkwijze en breng het risicomanagement (blijvend) onder de aandacht van het management.
- Benoem de meest risicovolle processen.

Voor niveau 2,5:

- Zorg dat in ieder geval voor de meest risico volle processen een risico analyse is uitgevoerd en dat mitigerende maatregelen zijn doorgevoerd. Zodat bij veranderingen slechts de risico's van de verandering in beeld hoeft te worden gebracht.

Voor niveau 3:

- Zorg dat in alle gevallen een risico analyse is uitgevoerd en dat mitigerende maatregelen zijn doorgevoerd. Zodat bij veranderingen slechts de risico's van de verandering in beeld hoeft te worden gebracht.

Organisatorische inbedding

Om daadwerkelijk invulling te geven aan de bescherming van privacy, moeten de taken organisatorisch zijn ingebed. Dit wordt bereikt met een goede taakverdeling en voldoende middelen

❖ Functionaris gegevensbescherming

- Rol, taken en de autonome positie van de FG zijn vastgelegd in het privacybeleid.
- In de praktijk komt haar autonome, onafhankelijke rol, waarbij rechtstreeks wordt gerapporteerd aan het hoogste bestuurlijke niveau, niet volledig tot zijn recht. Toegang tot het hoogste bestuurlijke niveau loopt via het afdelingshoofd IVA en binnen het bestuurlijk behandelproces is de FG niet gepositioneerd. Advies van de FG wordt niet afgedwongen en er wordt niet vastgelegd of adviezen van de FG worden opgevolgd dan wel waarom er van wordt afgeweken.

❖ Privacy team

- Er is in 2022 een centraal team van Security en privacy offiers benoemd. Daarmee heeft de organisatie haar slagkracht in potentie vergroot. Naast het centrale team, wat voor versnelling moet zorgen is er capaciteit in de afdeling nodig. Er is (nog) geen organisatiebreed commitment over deze afdelingstaken. Daardoor verschilt de inzet van de afdeling en de samenwerking met het SPO team en is die niet overal even effectief. Hierdoor blijft de versnelling achter.

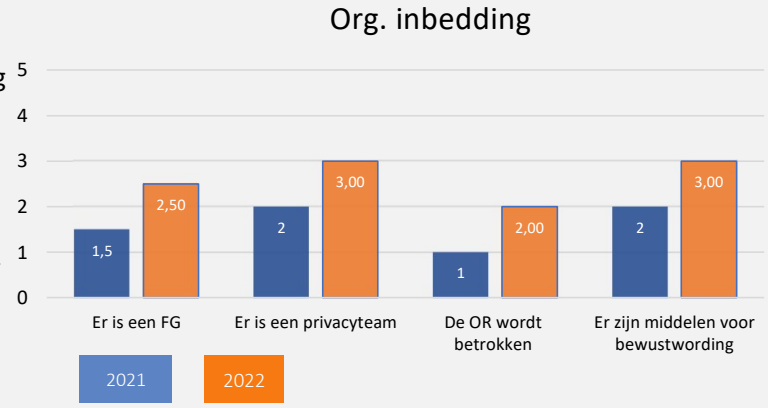
- Het zal bijdragen aan de verdere groei in volwassenheid, wanneer de thema's privacy en informatiebeveiliging worden gezien als een kwaliteitsaspect van de dienstverlening. Door de thema's te borgen in de processen en er in de planning rekening mee te houden dat hier tijd en capaciteit mee is gemoeid, zullen de thema's minder als belemmerend worden ervaren. De FG is het met de rekenkamer eens dat het management het beleid nog niet voldoende actief uitdraagt.

❖ Ondernemingsraad (OR)

- De ondernemingsraad wordt, daar waar nodig, om instemming gevraagd. Ze wordt echter niet gestructureerd betrokkene bij onderwerpen over de bescherming van persoonsgegevens.

❖ Bewustwording

- Om de noodzakelijke cultuurverandering te bereiken is in 2022 het bewustwordingsprogramma 'Helmond ben ik, veiligheid ben ik' opgezet. Metingen tonen aan dat het bewustzijn bij medewerkers is toegenomen.



Advies

Voor niveau 2:

- Spreek afdelingsmanagers aan op hun verantwoordelijkheid om privacy en informatiebeveiliging te borgen binnen de processen en hiervoor de benodigde capaciteit vrij te maken.
- Zorg voor duidelijkheid over inrichting en rolverdeling van het centrale team van security en privacy officers en de taken van de afdeling zelf.
- Voer het bewustwordingsprogramma uit volgens plan van aanpak en zet daarbij in op cultuurverandering.

Voor niveau 2,5:

- Richt een proces in om afwijkingen op het advies van de FG voor te leggen aan stuurgroep/gemeentesecretaris en/of college.
- Pas het bestuurlijk behandelproces aan.
- Zorg, voor (verdere) opbouw en doorontwikkeling van het SPO team.
- Voer het bewustwordingsprogramma uit volgens plan van aanpak, waarbij ook aandacht wordt besteed aan specifieke domeinen.

Voor niveau 3:

- Onderzoek de mogelijkheden om de FG rechtstreekst onder de Gemeentesecretaris te positioneren.
- Ontwikkel een dashboard "Stand van zaken privacy".
- Neem een besluit over de organieke inbedding van het SPO team en hef de projectorganisatie op.
- Stel een communicatieplan op, om meer bekendheid te geven aan:
  a. het privacybeleid;
  b. de processen rechten betrokkenen;
  c. Risicomanagement.

Bewustwording in 2022

E-learning

Nieuwe medewerkers volgen bij indiensttreding een E-learning en maken hierbij een kennistest.

Bewustwordingsworkshop

Er is een workshop in de vorm van een pubquiz “digitale veiligheid” ontwikkeld. Deze workshop is onderdeel geworden van het onboarding programma voor nieuwe medewerkers en kan ook op verzoek worden afgenomen.

Continue leren

Medewerkers ontvangen periodiek korte berichten (nano learnings) in hun inbox. In dit bericht wordt een onderwerp aan de orde gesteld, om betrokkenen te informeren en te motiveren om veilig te handelen om zo continue bewustwording rondom informatiebeveiliging en privacy te stimuleren.

Nieuwsberichten

Er is een site “Veilig werken” ingericht. Deze site bevat richtlijnen om digitaal veilig te werken. Daarnaast worden er
regelmatig nieuwsberichten gepubliceerd op het Knaal.

Mystery guest

Met deze test is heeft een medewerker van het ingehuurde bedrijf geprobeerd of hij toegang kon krijgen tot onze gebouwen en informatie. Van de actie is een video gemaakt die wordt ingezet voor bewustwordingsactiviteiten.

Social Hack training:

Tijdens de Social Hack training, hebben de medewerkers van de klantcontactcentra geleerd hoe ze een social hack kunnen herkennen. De training is ook tijdens de “Helmond ben ik dag” aangeboden.

Landelijke cyberoefening

In oktober is tijdens de cyber security week deelgenomen aan de landelijke cyberoefening. Doel van deze cyberoefening was om beter voorbereid te zijn, mocht zich in Helmond een cyberaanval voordoen. Verder werd inzicht gegeven in de bestuurlijke gevolgen van een cybercrisis.

Phishing competitie

Door middel van een phishing campagne en cultuurvideo’s werden medewerkers getraind om phishing mails te herkennen en adequaat te handelen.

Cyberbarometer:

In 2022 is gemeten hoe bewust onze organisatie is van de risico’s.
Deze meting toont aan dat het bewustzijn bij medewerkers is toegenomen.

Rechten van betrokkene

Inwoners en andere betrokkenen hebben het recht op informatie en inzage. Zo kunnen ze controleren of er op een juiste wijze wordt omgegaan met hun gegevens. Ze hebben het recht om aanpassing van de gegevens te vragen of een klacht in te dienen bij de FG. Ook hebben ze het recht op menselijke tussenkomst, bij geautomatiseerde besluiten.

❖ Klachten

- In 2021 heeft de FG 1 klacht behandeld. De inwoner meende dat de organisatie teveel informatie van hem had gevraagd. Zijn klacht was ongegrond.

❖ Processen

- Er zijn processen en procedures opgesteld om uitvoering te geven aan de rechten van betrokkenen. Deze processen zijn nog niet bij iedereen bekend, waardoor er nog geen sprake is van een uniforme benadering. Standaarddocumenten ontbreken nog.

❖ Geautomatiseerde besluitvorming

- Digitalisering neemt toe en daarmee ook de hoeveelheid data. Het is de ambitie van de gemeente Helmond om de data(stromen) te gebruiken om enerzijds te komen tot nieuwe inzichten en opgaven uit de stad en anderzijds slimme (geautomatiseerde) beslissingen te nemen.
- De gemeente maakt daarbij (nog) geen gebruik van geautomatiseerde (bestuursrechtelijke) besluitvorming, er is in die gevallen nog altijd sprake van “menselijke tussenkomst."
- Momenteel bestaat er echter onvoldoende inzicht in het gebruik van automatisch verwerkte persoonsgegevens of algoritmes.

Advies

Voor niveau 2:

- Zorg voor inzicht het gebruik van data-analyse, statistiek en/of zelflerende logica om te komen tot geautomatiseerde feitelijke besluitvorming en leg dit vast in een register.

Voor niveau 2.5:

- Stel standaardbeschikkingen op voor het afhandelen van verzoeken.
- Definieer de principes voor een verantwoord gebruik van data-analyse en/of zelflerende logica.
- Vertaal deze principes naar praktische richtlijnen.
- Veranker deze principes als onderdeel van een data- en analyticsstrategie.

Voor niveau 3:

- Stel een communicatieplan op om bekendheid te geven aan:
  a) het privacybeleid;
  b) de processen rechten betrokkenen;
  c) risicomanagement.
- Implementeer data-ethiek in de organisatie en betrek daarbij de agenda Digitale grondrechten en ethiek 2022-2024.

Rechten van betrokkene

❖ Informatieplicht en Communicatieplan

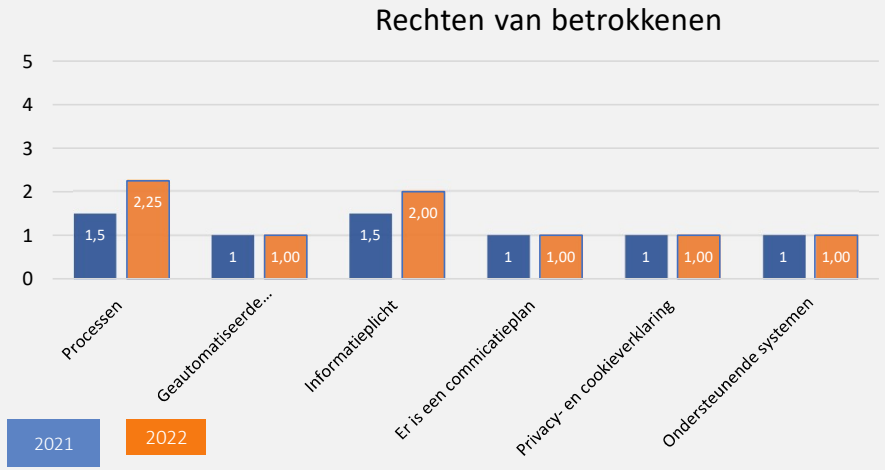
- De organisatie heeft (in het algemeen) een passieve houding voor wat betreft het informeren van betrokkenen. Betrokkenen worden via de privacyverklaring op de website geïnformeerd over hoe de gemeente Helmond omgaat met hun persoonsgegevens. Naaste deze algemene privacy verklaring zijn er geen of weinig (domein) specifieke documenten. Een privacyverklaring voor medewerkers ontbreekt.
- De organisatie ontwikkelt samen met de provincie en andere gemeenten een sensorenregister met bijbehorend kader, zodat betrokkenen kunnen opzoeken waar sensoren hangen en welke informatie er wordt verzameld.

❖ Privacy- en cookieverklaring

- De cookieverklaring van de website "Helmond.nl" informeert over het gebruik van cookies op deze site. Er worden alleen analytische cookies geplaatst, daarvoor wordt Google Analytics gebruikt.
- De gemeente Helmond participeert in verschillende websites. Het inzicht in het gebruik van cookies of andere persoonsgegevens op deze websites en de verantwoordelijkheid voor deze verwerkingen is onvolledig.

❖ Ondersteunende systemen

- De gemeente maakt niet of nauwelijks gebruik van verdergaande mogelijkheden om invulling te geven aan rechten van betrokkenen, zoals een klantportaal. Onderdeel van een op te stellen Omnichanel strategie is de inrichting van een klantportaal.



Advies

Voor niveau 2:

- Stel een privacyverklaring op over de verwerking van persoonsgegevens van het personeel en publiceer dit op intranet.
- Informeer het personeel over de gegevens die over hen worden verwerkt in het kader van logging en monitoring.
- Breng alle websites waar de gemeente voor verantwoordelijk is in kaart en onderzoek of betrokkenen juist worden geïnformeerd.

Voor niveau 2,5:

- Stel een kader vast, wat helpt bij het maken van een keuze over de wijze waarop betrokkenen worden geïnformeerd.
- Stel domeinspecifieke privacyverklaringen op, conform dit kader.
- Pas de geplaatste cookies en privacyverklaringen daar waar nodig aan.

Voor niveau 3:

- Stel vast dat betrokkenen in alle gevallen conform het vastgestelde kader worden geïnformeerd.
- Richt een proces in om privacy- en cookieverklaringen te actualiseren.
- Zorg dat er een omnichanel strategie komt.
- Richt een klantportaal in en zorg dat een inwoner daarbij verdergaande mogelijkheden tot zijn beschikking krijgt om zijn rechten uit te oefenen.
- Stel een sensorregister op en een afwegingskader.

Samenwerking

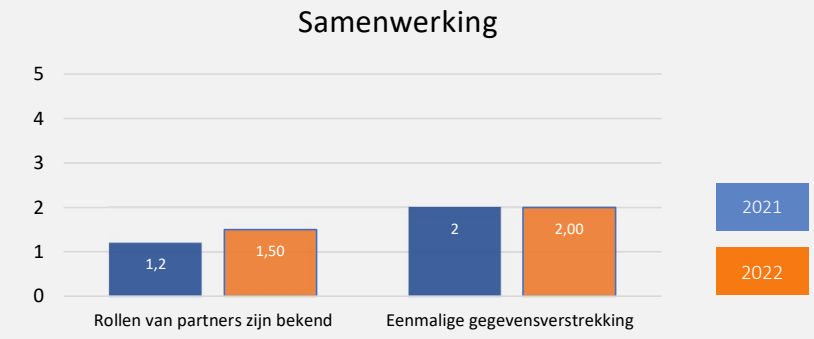
Met haar partners deelt de gemeente Helmond gegevens. Betrokkenen moeten er op kunnen vertrouwen dat dit zorgvuldig en veilig gebeurt. Eenmalige verstrekkingen moeten daarom worden getoetst en bij meer structurele verstrekkingen moeten er goede afspraken gemaakt worden. Voor het maken van deze afspraken is het belangrijk om te weten welke rol een partner inneemt.

❖ Rollen van partners

- Bij aanbestedingen door de afdeling inkoop, wordt er standaard uitvraag gedaan naar de rol die de partner heeft. Dit geldt niet voor aanbestedingen onder de drempel. In dat geval zijn afdelingen gerechtigd om zelfstandig producten aan te schaffen. Ook bij het aangaan van samenwerkingsverbanden wordt niet altijd uitvraag gedaan naar de rol van de partner.
- Er zijn een aantal standaardovereenkomsten beschikbaar, op afdelingsniveau is echter niet altijd inzichtelijk welke afspraken er moeten worden gemaakt en of deze afspraken passen bij de rol die een partij inneemt. Als gevolg hiervan gebeurt het dat contracten niet voldoen aan de eisen van de gemeente Helmond of van de AVG.

❖ Eenmalige Gegevensverstrekking

In 2022 is een nulmeting tactisch gegevensmanagement uitgevoerd. Uit deze meting blijkt dat de verantwoordelijkheid voor beheer en gebruik van gegevens in Helmond niet eenduidig is belegd. Ook ontbreekt beleid en een duidelijke roadmap. Het project gegevensmanagement moet hier in gaan voorzien. Onderdeel van het project gegevensmanagement is de inrichting van het proces "incidentele gegevensverstrekking". Dit proces is begin 2023 opgeleverd.



Advies

Voor niveau 2:

- Vul het register van verwerkingen aan met leverancier, ketenpartners en de vindplaats van de gemaakte afspraken.
- Voer bij aanbestedingen altijd een risico analyse uit.
- Stel standaard overeenkomsten op voor partijen waarmee gegevens worden uitgewisseld (anders dan in de rol als verwerker).

Voor niveau 2,5:

- Stel een inkoopstrategie op, die faciliteert dat er wordt gekozen voor de meest privacyvriendelijke en veilige optie en afdelingen zich, bij zelfstandige aanschaf van producten of het aangaan van verplichtingen, houden aan de Helmondse afspraken.
- Zorg dat in ieder geval voor de processen met hoge risico's voor de privacy van betrokkenen:
- - in beeld is welk rol partners innemen.
- - er afspraken met hen zijn gemaakt over de omgang met persoonsgegevens.
- - er periodiek wordt gecontroleerd of de afspraken op papier in de praktijk worden nagekomen.
- Laat het samenwerkingsverband niet alleen verantwoording afleggen over de doelen en de middelen, maar ook over informatiebeveiliging en privacy.
- Werk een tactisch kader delen van informatie uit.
- Implementeer het proces incidentele gegevensverstrekking, en monitor de naleving bij verwerkingen met hoge privacy risico's.

Voor niveau 3:

- Zorg dat het voor alle processen duidelijk is welke rol partners innemen en dat afspraken zijn gemaakt over de omgang met persoonsgegevens door deze partners.
- Monitor de naleving van het proces incidentele gegevensverstrekking, bij alle verwerkingen.
- Stel een communicatieplan op om het proces incidentele gegevensverstrekking bekend te maken binnen de organisatie.

Beveiliging

De inwoner en medewerker moeten er op kunnen vertrouwen dat hun persoonsgegevens passend zijn beveiligd, zodat hun gegevens niet kunnen worden misbruikt. Dit betekent ook dat de inwoner en de medewerker kunnen rekenen op goede dienstverlening, omdat de juiste persoonsgegevens op het juiste moment voor de juiste mensen beschikbaar zijn

- De gemeente legt via ENSIA verantwoording af. Uit deze verantwoording blijkt dat het volwassenheidsniveau van informatiebeveiliging van de gemeente Helmond 2.1 op een schaal van 5. Dit niveau houdt mede in dat het afhankelijk is van de deskundigheid en inzet van individuele personen of de gegevens van onze inwoners en medewerkers passend zijn beveiligd.
- De organisatie is bezig met de ontwikkeling van een enterprise architectuur, eind 2022 is men hiervoor gestart met het opstellen van richtinggevende principes. Deze principes zijn richtinggevend bij alle veranderingen binnen de organisatie die impact hebben op de organisatie en de informatievoorziening. De enterprise architectuur moet in de loop van 2023 vertaald worden in een domein architectuur informatiebeveiliging en privacy. Dan ontstaan er gedocumenteerde eisen om privacy risico's in de ontwerpfase voor processen en systemen mee te nemen. Bovendien is dit richtinggevend voor de inrichting van de organisatie en informatievoorziening van alle organisatiedomeinen. Hiervoor zal in 2024 architectuur worden opgesteld.

Slordig	Aanval van buitenaf	Overig	Totaal	
3	0	2	5	Gemeld bij de AP
68	1	14	83	Geen melding
71	1	16	88	Totaal

- Er zijn in 2022 88 datalekken gemeld. Een eenduidig proces om privacy incidenten te identificeren en beheren is echter niet aanwezig.
- Er worden nauwelijks aanvallen van buitenaf gemeld. Overige incidenten worden vaak gemeld. Er kan daarom worden vastgesteld dat het personeel adequaat reageert, ondanks het ontbreken van een eenduidig proces.
- Incidenten kunnen leiden tot een verstoring van de bedrijfsvoering. Het is daarom van belang dat er Bedrijfscontinuïteitsmanagement (BCM) is in ingericht. Hier is in 2022 mee gestart. In 2023 wordt BCM verder projectmatig opgepakt.

Advies

Voor niveau 2:

- Implementeer IT-Servicemanagement.
- Stel het strategisch en tactisch kader Business Continuity Management (BCM) vast.
- Zorg dat je een vastgestelde enterprise architectuur hebt.
- Zorg dat je de domein architectuur informatiebeveiliging en privacy hebt.
- Zorg dat je de data architectuur vastgesteld hebt.
- Ontwikkel processen onder architectuur.
- Maak de architectuurkaders leidend bij alle veranderingen binnen de organisatie.

Voor niveau 2,5:

- Richt een crisis organisatie in.
- Voer per afdeling een impact analyse uit en formuleer de continuïteitseisen met bijbehorende maatregelen.
- Werk per organisatiedomein een domeinarchitectuur uit. Zorg dat daarbij de domeinarchitectuur informatiebeveiliging en privacy leidend is.
- Stel een doorontwikkelplan op om de informatiebeveiliging naar volwassenheidsniveau 2,5 te brengen en voer dit plan uit.

Voor niveau 3:

- Ontwikkel managementinformatie IT servicemanagement.
- Stuur op basis van managementinformatie.
- Stel een doorontwikkelplan op om de informatiebeveiliging naar volwassenheidsniveau 3 te brengen en voer dit plan uit.

Verantwoording

De AVG vereist dat de organisatie kan aantonen dat er zorgvuldig wordt omgegaan met de gegevens van betrokkenen en dat de AVG wordt nageleefd. Met een GAP analyse kan worden vastgesteld waar de gemeente voldoet aan de privacywetgeving en waar in de toekomst nog aan gewerkt moet worden.

❖ Aantonen naleving en GAP analyse

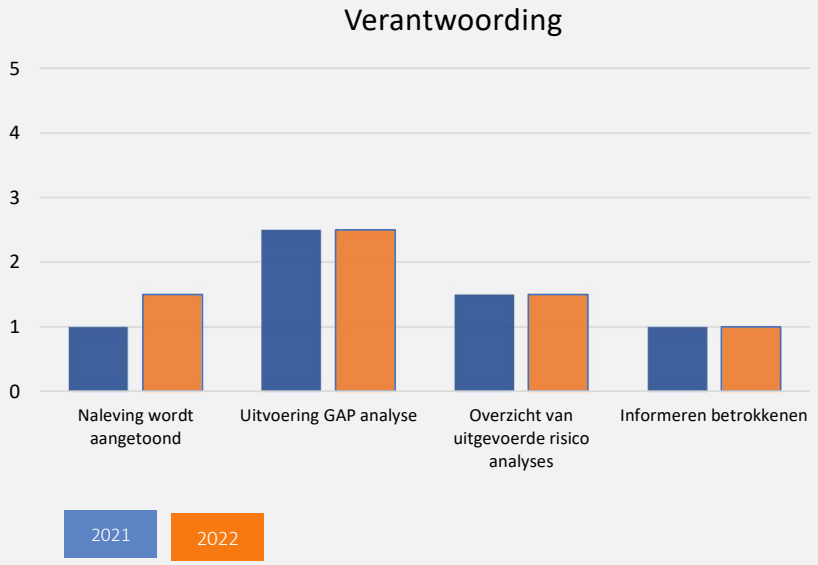
- Er vindt op afdelingsniveau nauwelijks toezicht plaats op de rechtmatigheid van de verwerking van persoonsgegevens. Er wordt niet over gerapporteerd.
- Gegevensmanagement is nog niet ingericht, hiervoor is inmiddels wel en project gestart. Daarmee zal meer grip op de kwaliteit van gegevens ontstaan.

❖ Overzicht uitgevoerde risico analyses

- Er is een fragmentarisch beeld van verwerkingen met een hoog risico en uitgevoerde risico analyses.

❖ Informeren betrokkenen

- Betrokkenen worden vooral reactief, naar aanleiding van vragen, klachten en datalekken, geïnformeerd over de omgang met hun persoonsgegevens.



Advies

Voor niveau 2:

- Toets het gebruik van basis- en kerngegevens in bedrijfsprocessen en vakapplicaties.
- Stel een gegevenscatalogus, met gegevenswoordenboeken op die organisatiebreed het kader vormen. .
- Stimuleer een risicogerichte denkwijze en breng het risicomanagement (blijvend) onder de aandacht van het management.

Voor niveau 2,5:

- Werk de rollen voor gegevensmanagement uit en implementeer ze.
- Leg het eigenaarschap van gegevensbronnen vast (waaronder basis- en kernregistraties).
- Breng het gegevenslandschap in beeld.
- Stel de architectuurprincipes voor gegevensmanagement vast.

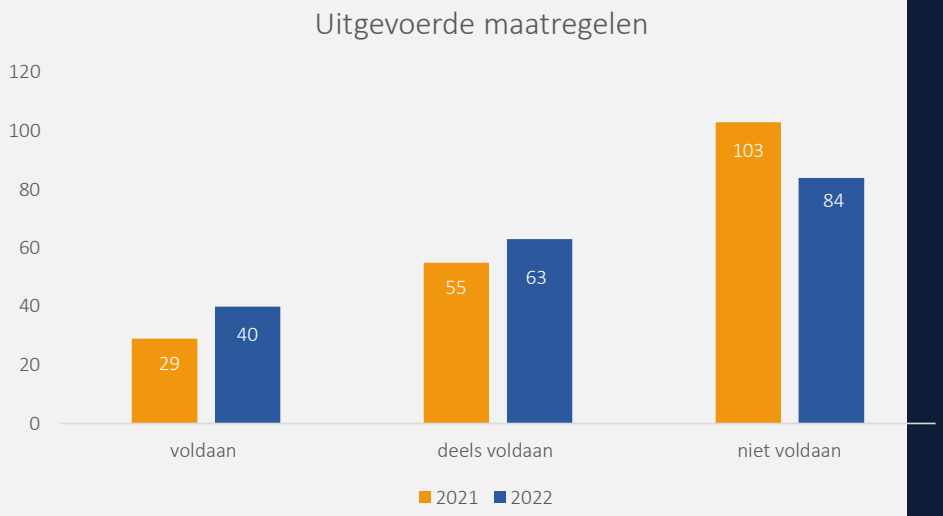
Voor niveau 3:

- Zorg dat voor alle processen adequate logging en monitoring plaatsvindt.
- Richt gegevensmanagement in.

Verantwoording

❖ Aantonen naleving en GAP analyse

- Er vindt jaarlijks een GAP analyse, op basis van het VNG/IBD privacy normenkader, plaats op organisatie niveau. De FG baseert hier het jaarverslag op en maakt daarmee inzichtelijk hoe de organisatie staat op het gebied van privacy.
- Het normenkader 187 maatregelen. Door het implementeren van deze maatregelen groeit de organisatie in volwassenheid.
- Het aantal geïmplementeerde maatregelen is in 2022 toegenomen.
- Het uitvoeren van de GAP analyse is onderdeel van een PDCA-cyclus. De directie ontvangt het jaarverslag en ze heeft in 2021 een handelingsperspectief opgesteld. Het belangrijkste advies: “versterken van de DSPO organisatie” is overgenomen.
- Gemeenteraad en college ontvangen het jaarverslag. Het jaarverslag is openbaar, maar werd in 2021 niet actief bekend gemaakt.



Advies

Voor niveau 3:

- Stel een toezichtsplan voor de FG op.
- Voer periodiek een GAP analyse en/of een volwassenheidsmeting op afdelingsniveau uit.
- Neem in de jaarplannen van de afdeling een paragraaf op over informatiebeveiliging en privacy
- Maak een doorontwikkelplan waarin is op opgenomen welke acties en maatregelen er worden getroffen naar aanleiding van de aanbevelingen van de Functionaris voor de gegevensbescherming om de privacybescherming naar een hoger niveau te brengen en neem deze vervolgstappen op in de jaarplannen van de afdelingen.

WPG voor Boa’s

Sinds begin 2019 is de Wet politiegegevens (Wpg) ook van kracht voor bijzonder opsporingsambtenaren (boa's). Om aan te tonen dat de gemeente Helmond compliant is aan de Wpg moet jaarlijks een interne audit en eens in de vier jaar, een externe audit worden uitgevoerd.

- Er is een externe audit uitgevoerd over 2021. De rapportage van de externe audit is in december 2022 aangeboden aan de toezichthouder.
- Er wordt, conform wettelijke verplichting, een interne audit over 2022 uitgevoerd, deze is nog niet afgerond.
- De organisatie heeft een verbeterplan opgesteld en uitgevoerd. Ze heeft instructies en procedures opgesteld.
- Daarnaast heeft ze een applicatie voor het verwerken van politiegegevens aangeschaft. Hierdoor kunnen politiegegevens gescheiden van andere gegevens worden opgeslagen en verwerkt. De applicatie moet nog worden geïmplementeerd.

Advies:
Stuur de rapportage van de interne audit naar de FG zodat zij kan vast stellen of zij een extra controle op naleving van de Wpg opneemt in haar toezichtsplan.

Vooruitblik

❖ Huis van de Stad

- In 2023 verhuizen we naar het Huis van de Stad. Het Huis van de Stad heeft een open karakter, dit heeft effect op de beveiliging van onze infrastructuur en informatie. Het open karakter, de flexibele werkplekken en het hybride werken vergroten de kans op meeluisteren of meekijken.

Advies:

- Tref aanvullende maatregelen om de infrastuctuur en informatie te beschermen.
- Stel leidende uitgangspunten voor het hybride werken op.

❖ Dienstverlening

- Wetgeving

Dienstverlening is en wordt steeds verder gedigitaliseerd. De hoeveelheid data en (digitale) informatie groeit razendsnel en daarmee ook de mogelijkheden en de risico's. Er zal daarom blijvend veel aandacht (nodig) zijn voor privacy en gegevensbescherming. Zowel Europees als landelijk is die aandacht terug te zien in wetgeving (in voorbereiding) zoals de "E-privacy verordening", "Wet Digitale Overheid (Wdo)" en de "Wet modernisering elektronisch bestuurlijk verkeer (Wmebv)". Daarnaast treedt op 24 september 2023 de "Data Governance Act" in werking. Deze verordening faciliteert hergebruik van overheidsinformatie en de data. Dit maakt het ook nodig om te kijken naar de inrichting van onze informatievoorziening en informatiehuishouding.

- Omnichanel

Bewoners, ondernemers en instellingen die contact hebben met hun gemeente doen dit via verschillende interactiekanalen. Denk aan het raadplegen van informatie via een mobiele app, online formulieren of een persoonlijk gesprek aan de balie. Die variëteit aan kanalen heeft voordelen: gericht een bepaald kanaal inzetten voor een bepaalde dienst voor een bepaalde doelgroep. Daarmee wordt het contact effectiever en efficiënter. Tegelijkertijd zijn er uitdagingen. Zo kunnen burgers het gevoel krijgen van het kastje naar de muur te worden gestuurd door de complexiteit en diversiteit van kanalen. In 2023 ontwikkelt de gemeente een Omnichanel aanpak die dit moet voorkomen.

Advies:

Geef de uitwerking van de Omnichanel aanpak prioriteit.
Stel een informatiebeleidsplan op dat overkoepelend vorm zal geven aan de ontwikkeling van de informatievoorziening.

Vooruitblik

- Ethiek
  - Digitale vernieuwingen zullen de komende jaren veel teweeg gaan brengen en grote alertheid vragen. Het is aan de overheid om hiervoor goede kaders te stellen. De “Agenda Digitale Grondrechten en Ethiek 2022-2026” geeft de gemeenten daar instrumenten voor.

    Deze agenda vormt het fundament om de komende jaren te werken aan het beschermen van grondrechten en het borgen van publieke waarden bij de inzet van digitale technologieën.

- Algoritme

Regie op je digitale leven betekent onder meer dat je erop kan vertrouwen dat digitale systemen, waaronder algoritmes, aan publieke waarden voldoen en dat je begrijpt hoe deze werken. Bij bedrijven en de overheid is dit op het moment geen gegeven.
In Europa wordt gewerkt aan een AI verordening, (EU Artificial Intelligence (AI) Act) omdat men vindt dat de huidige Europese regelgeving de (toekomstige) risico’s van AI onvoldoende adresseren. De EU streeft ernaar om in het najaar van 2023 een definitief akkoord te bereiken. Vanaf 1 januari 2023 is de Autoriteit Persoonsgegevens aangewezen als algoritme toezichthouder. Verder heeft de Tweede Kamer heeft een motie aangenomen om gebruik van een algoritmeregister algemeen verplicht te stellen voor overheidsorganisaties. Het ministerie heeft ook aangekondigd dat ze werkt aan een richtlijn ‘inzet van algoritmeś voor het Rijk en andere overheden. Het uitvoeren van een IAMA wordt hier een integraal onderdeel van. Een IAMA is een Impact Assessment Mensenrechten en Algoritmes.

Advies:
Implementeer data-ethiek in de organisatie en geef uitvoering aan de agenda Digitale grondrechten en ethiek 2022-2024.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	1, 4

Gemeente Helmond

Jaarverslag 2023

Privacy

1 maart 2024

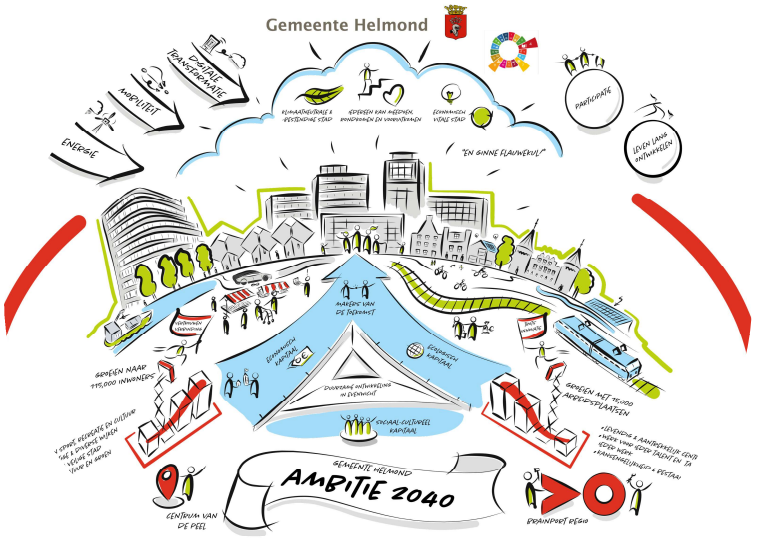
5.1.2e

Inhoud

1. Managementsamenvatting
2. Inleiding
3. Resultaten van het afgelopen jaar
   - Beleid
   - Processen
   - Organisatorische inbedding
   - Rechten van betrokkene
   - Samenwerking
   - Beveiliging
   - Verantwoording
   - Wet Politiegegevens
4. Vooruitblik
5. Adviezen
   - Randvoorwaardelijk
   - Maatregelen
   - Monitoring

Inleiding

- De ambities in de stad Helmond zijn groot. Ze wil een klimaatneutrale bestendige en vitale stad zijn waar iedereen kan meedoen, rondkomen en vooruitkomen. Dit doet zij vanuit haar kernwaarden: trots, verbinding, vertrouwen en innovatie.
- Daarbij heeft ze te maken met de digitale transformatie. De razendsnel groeiende digitale wereld geeft mogelijkheden waar de stad gebruik van wil maken. Zowel de inwoners als de medewerkers moeten er op kunnen vertrouwen dat dit veilig gebeurt en met respect voor hun privacy.
- Om de ambities van de stad te verwezenlijken en daarnaast het vertrouwen van de inwoners en de medewerkers te behouden is er een solide inrichting van informatiebeveiliging en privacy nodig. De organisatie is zich hier van bewust en heeft de ambitie om van sturen op processen, door te groeien naar sturing op resultaten (volwassenheidsniveau 3).
- Dit jaarverslag geeft inzicht in waar de organisatie staat op het gebied van de veilige verwerking van persoons- en politiegegevens. Naast het geven van inzicht bevat dit jaarverslag aanbevelingen om verder te groeien, zodat Helmond haar inwoners en medewerkers kan laten zien:
  - wat er met hun gegevens gebeurt;
  - dat hun gegevens goed zijn beschermd en op een veilige wijze worden verwerkt.
- Dit jaarverslag is opgesteld door 5.1.2e . 5.1.2e is aangesteld als Functionaris voor de Gegevensbescherming (FG) en ziet toe op de naleving van de Algemene verordening gegevensbescherming (AVG) en de Wet politiegegevens (Wpg).
- Leeswijzer: Allereerst vindt u de samenvatting van de bevindingen en aanbevelingen van de FG over de naleving van de AVG en de Wpg. Daarna ziet u de volwassenheid van de organisatie. Vervolgens leest u per thema de bevindingen van de Fg. Ook kijkt de FG vooruit. Tot slot vindt u de adviezen van de FG.
- Dit jaarverslag bevat een samenvatting van de bevindingen en de belangrijkste adviezen van de FG. In bijlage 1 vindt u de door de FG uitgevoerde analyse, met alle bevindingen. Bijlage 2 bevat alle adviezen per manager op het gebied van privacy én informatiebeveiliging. Deze adviezen zijn tot stand gekomen samen met de CISO en worden mondeling besproken met betrokken manager. Tot slot vindt u in bijlage 3 de samenvatting van dit jaarverslag in de vorm van een infographic. Deze infographic wordt gedeeld met de gemeenteraad en gepubliceerd.



Managementsamenvatting

Bevindingen

De organisatie is nog niet volwassen t.a.v. privacy.

De organisatie kan nog niet aantonen dat de persoonsgegevens van haar inwoners en medewerkers verantwoord worden gebruikt en veilig zijn. Daarvoor is een volwassenheidsniveau van 3 nodig en daar is de organisatie nog niet.

Groei volwassenheid privacy blijft nog achter

Afgelopen jaar is Helmond gegroeid van niveau 2,1 naar 2,2. De groei gaat langzamer dan verwacht. Dit terwijl er wel diverse maatregelen zijn getroffen in 2023. De groei in volwassenheid op het thema privacy kan echter niet los worden gezien van de volwassenheid van de organisatie op andere thema's. Zoals werken onder architectuur, procesgericht werken en risico management.

Een doorbraak is uitgebleven.

Met het SPO team is er extra capaciteit en kennis in de organisatie gekomen om de proceseigenaar te ondersteunen. De verwachte versnelling bij privacy en informatiebeveiligings- vraagstukken is echter achtergebleven. Dat heeft niet alleen te maken met de hierboven geschetste volwassenheid op andere thema's. Voor een doorbraak is meer eigenaarschap en sturing op deze thema's nodig.

Adviezen

Zorg voor inzicht in de persoonsgegevens die worden verwerkt binnen processen.

Een compleet register van verwerkingen geeft de organisatie een beter inzicht in de persoonsgegevens die zij verwerkt binnen haar processen. De gegevens kunnen daardoor beter worden beschermd. Omdat dit een cruciale stap is om te groeien in volwassenheid dient het actualiseren van het register van verwerkingen de allerhoogste prioriteit te krijgen. Randvoorwaarde is een volledige kernregistratie processen. Dit betekent dat ook hier prioriteit aan gegeven dient te worden én dat dit dient te gebeuren in samenhang met het register van verwerkingen.

Stuur op kansen en risico's

Zorg dat risicomanagement de basis wordt van Privacy en informatiebeveiliging. Zo kunnen de risico's teruggebracht worden naar een acceptabel niveau voor de organisatie en voor betrokkenen. Het zal hierdoor gemakkelijker worden om zicht te krijgen op de bedreigingen. Ook de naleving van de acties die hieruit voortvloeien zal gemakkelijker worden. Onderzoek daarnaast ook voor alle bestaande processen de privacyrisico's en de noodzakelijke maatregelen. Begin bij de 10 meest risicovolle processen.

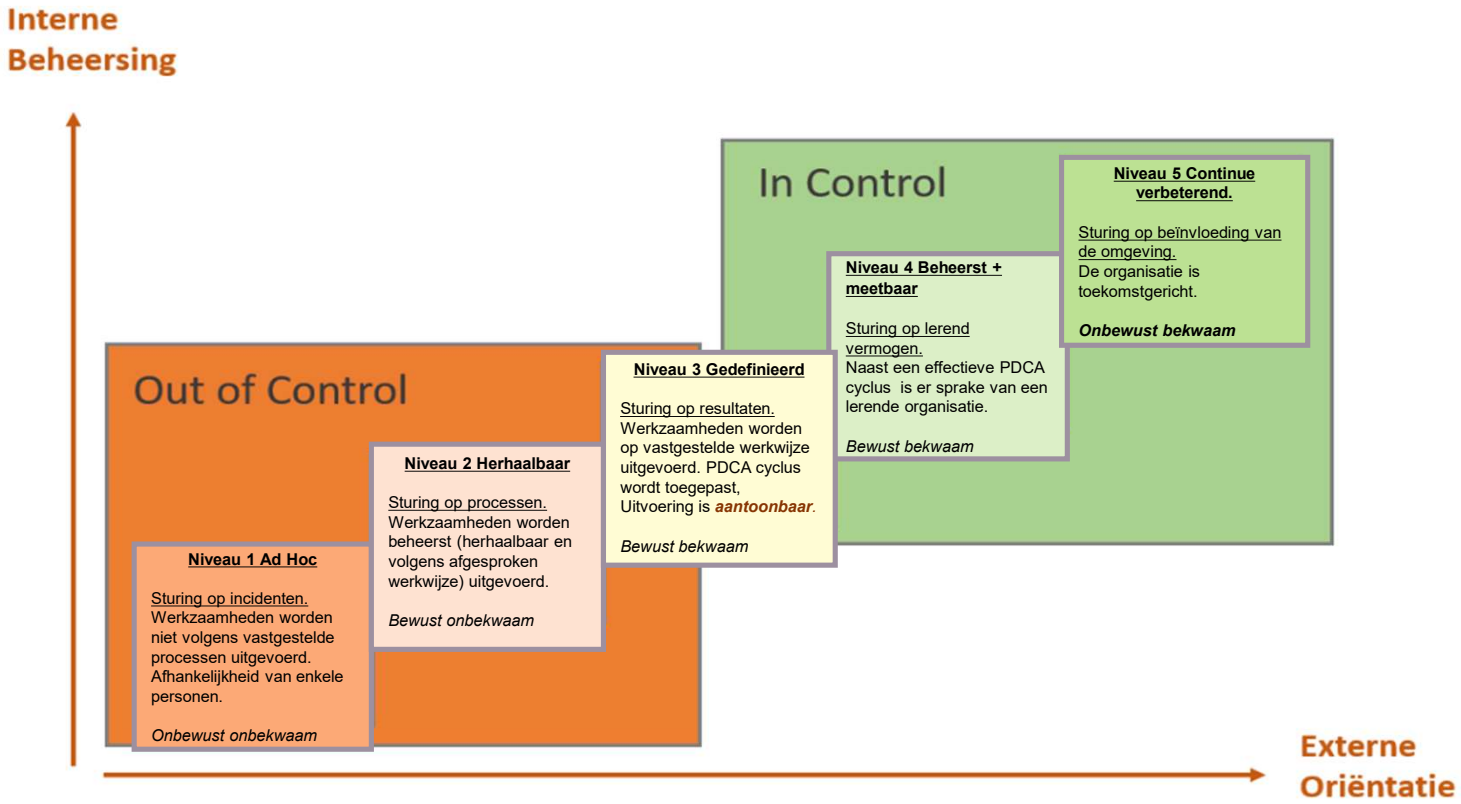
Veranderen van houding en gedrag.

Beschouw informatiebeveiliging en privacy, net als financiën en personeel, als een integrale managementtaak en maak ook op de werkvloer capaciteit vrij voor deze thema's. Draag als management uit dat privacy en informatiebeveiliging **de kwaliteit van de dienstverlening verbeteren**. Stuur op prioriteiten en pas de PDCA cyclus toe. Dat betekent dat informatiebeveiliging en privacy onderdeel horen te zijn van afdelingsplannen, projecten en veranderingen. Bovendien dient er te worden gestuurd op resultaat op deze thema's, binnen deze plannen en projecten.

Volwassenheid

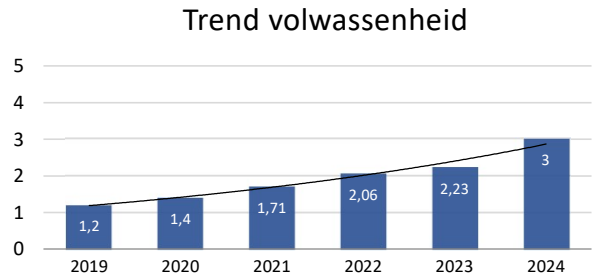
Een volwassen organisatie is in staat om aan te tonen dat er zorgvuldig om wordt gegaan met de gegevens van onze inwoners. Daarvoor heeft de organisatie inzicht nodig en moet ze in staat zijn om risico's en onzekerheden te beheersen. De organisatie voert de juiste discussies, op het juiste niveau, zodat (indien nodig) bijgestuurd kan worden om zo de doelstellingen te realiseren. Een volwassen organisatie is in control.

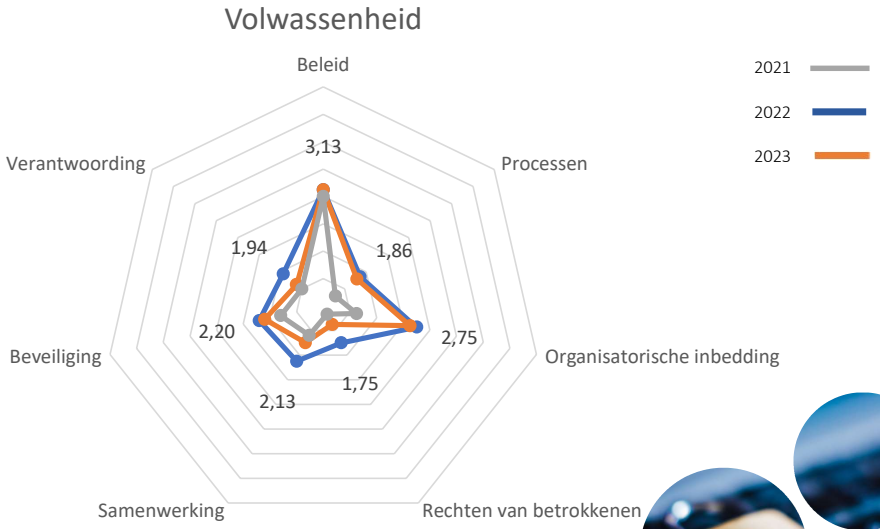
- De AVG kent een aantoonplicht. Dit betekent dat de gemeente moet kunnen aantonen welke persoonsgegevens ze waarvoor gebruikt. Daarnaast moet ze kunnen aantonen dat zij passende maatregelen heeft genomen om deze gegevens te beschermen.
- De gemeente heeft de ambitie om z.s.m. te groeien naar een volwassenheid van 3 voor de thema's privacy en informatiebeveiliging.
- De groei in volwassenheid voor de thema's privacy en informatiebeveiliging kan niet los worden gezien van de organisatieontwikkeling die de gehele organisatie meer in control moet brengen.
- Inmiddels vormen informatiebeveiliging en privacy een vast onderdeel van het concernplan en de jaarplannen. Daarmee is een belangrijke eerste stap gezet om te komen tot een PDCA cyclus.



Volwassenheid

- Het volwassenheidsniveau Privacy van de gemeente is 2,2 op een schaal van 5. Dit is gelijk aan het volwassenheidsniveau informatiebeveiliging
- De gemeente Helmond groeit met kleine stappen. Eind 2021 was het volwassenheidsniveau 1,7 en eind 2022 was dit 2,1. Met dit tempo duurt het te lang voordat de gemeente Helmond kan aantonen dat de gegevens van haar inwoners volledig zijn beschermd.
- De gemeente heeft dit onderkend en heeft daarom in 2022 een privacy team (het SPO team) gevormd en een (meerjarig) bewustwordingsprogramma ingekocht. Daarmee is de organisatorische inbedding verbeterd.
- Het privacy-team en het bewustwordingsprogramma hebben echter niet gezorgd voor versnelling in 2023. Voor een echte doorbraak is er een verandering in houding en gedrag nodig. Het omarmen van de thema's als onderwerpen die de kwaliteit van de dienstverlening verbeteren en ze te zien als een integrale management taak is essentieel voor een groei in volwassenheid.
- Daarnaast is een verdere ontwikkeling van de PDCA cyclus en verbetering van prestatiemanagement van belang. Ook sturing op prioriteiten en een ontwikkeling van risicomanagement is nodig om stappen te kunnen zetten.
- Om een veilige verwerking van persoonsgegevens te kunnen realiseren is het verder essentieel dat er een stevig IT-fundament komt. Voor dit fundament is het essentieel dat procesmatig werken wordt verbeterd, functioneel en applicatiebeheer verder worden geprofessionaliseerd en dat ook het werken onder architectuur verder wordt geïmplementeerd. Tot slot zijn de inrichting van IT-servicemanagement, gegevens- en datamanagement noodzakelijk.
- De volwassenheid wordt beoordeeld op 7 thema's Hiervoor is gebruik gemaakt van het borgingsproduct van de VNG Informatiebeveiligingsdienst. (VNG IBD)



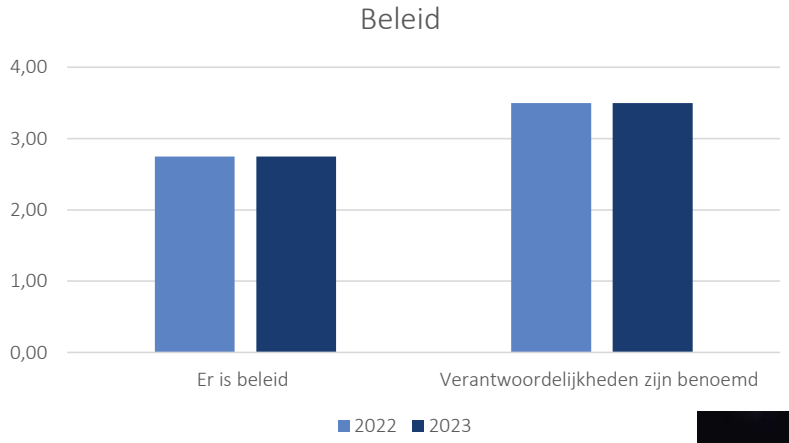


Noot: De laagste score bepaalt de volwassenheid van de organisatie. Om inzicht te geven in de groei is hier niet van uitgegaan, maar is er uitgegaan van de gemiddelde score per thema.

Beleid

Het privacybeleid beschrijft hoe de organisatie invulling geeft aan de veilige verwerking van persoonsgegevens.

- Op het onderdeel beleid scoort de organisatie goed.
- Op 10 november 2020 is het privacybeleid 2020-2024 vastgesteld. Dit beleid is compleet en er is samenhang met het informatiebeveiligingsbeleid. Hoewel het privacybeleid is gepubliceerd, is het nog niet bij iedereen bekend. In 2024 wordt een nieuw beleid opgesteld.
- Het management is verantwoordelijk voor de veilige verwerking van persoonsgegevens. Dit is vastgelegd in het beleid en het management ziet het belang in van de bescherming van persoonsgegevens. Hier daadwerkelijk uitvoering aangeven wordt nog als lastig ervaren.



Processen

Om haar inwoners en medewerkers goed van dienst te kunnen zijn worden binnen de processen persoonsgegevens gebruikt. Om dit zorgvuldig te kunnen doen is inzicht nodig in de processen. Daarnaast is inzicht nodig in de persoonsgegevens, die in deze processen worden gebruikt. Tot slot is het nodig dat bekend is op welke wijze gegevens worden verstrekt.

❖ *Processen, instructies en register*

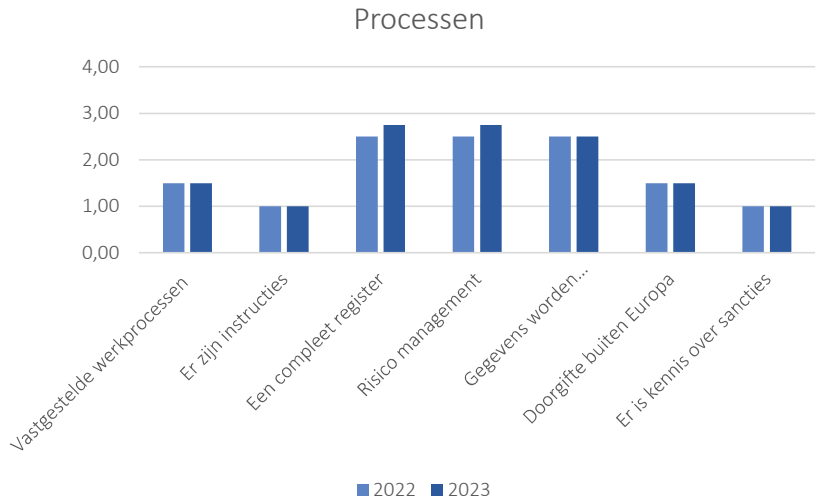
- Proces en ketengericht werken, de (volledige)kernregistratie processen, een procesbeleid dat een multi-disciplinaire aanpak bevat en een compleet register van verwerkingen (RvV) zijn essentieel om aan te kunnen tonen dat privacy is geborgd binnen onze processen.
- Er is procesbeleid en een procesverbeterteam; werkprocessen worden conform het beleid gemodelleerd en geoptimaliseerd.
- Er is een kernregistratie processen vastgesteld. Deze kernregistratie is nog niet volledig, de organisatie heeft daardoor nog geen volledig inzicht in al haar werkprocessen.
- In 2023 is het register van verwerkingen (RvV) geactualiseerd, op basis van deze kernregistratie processen. Omdat de kernregistratie processen nog niet compleet is, is er ook nog geen compleet RvV. Omdat een compleet RvV randvoorwaardelijk is om te voldoen aan de privacyregels, dient actualisatie van de kernregistratie processen en het RvV de allerhoogste prioriteit te krijgen.
- In 2023 zijn de verantwoordelijkheden voor het bijhouden van het RvV belegd.

❖ *Verwijderen*

- De Archiefwet is van toepassing. Om de naleving van de Archiefwet te borgen, heeft de gemeente beleidsstukken opgesteld en vinden er audits plaats. Analoge informatie en informatie in het zaaksysteem wordt volgens gedocumenteerde procedures geautomatiseerd vernietigd. De gemeente beschikt (nog) niet over een integraal overzicht van archiefbescheiden in taakspecifieke applicaties. Hierdoor is het niet vast te stellen dat in alle gevallen aan de wettelijke eisen rondom bewaren en vernietigen wordt voldaan.

❖ *Doorgifte en sancties*

- De standaard inkoopvoorwaarden en de standaard verwerkersovereenkomst bevatten bepalingen over de bescherming van de persoonsgegevens bij doorgifte naar landen buiten de EU.
- Afdelingen schaffen nog zelfstandig producten (software en diensten) aan zonder dit vooraf integraal met IVA af te stemmen. Zij zijn zich daarbij niet altijd bewust van de Helmondse afspraken en standaarddocumenten.

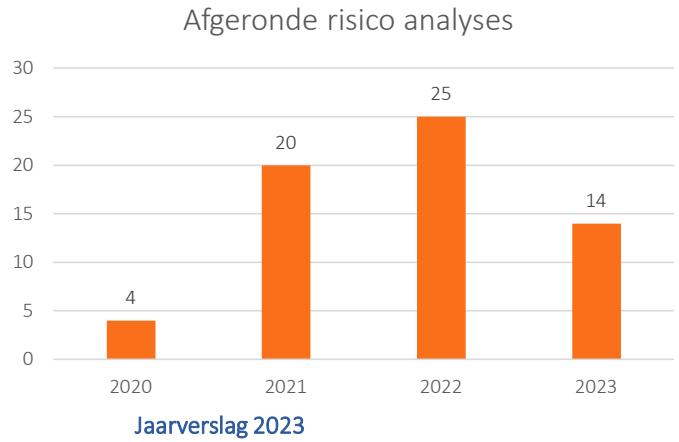


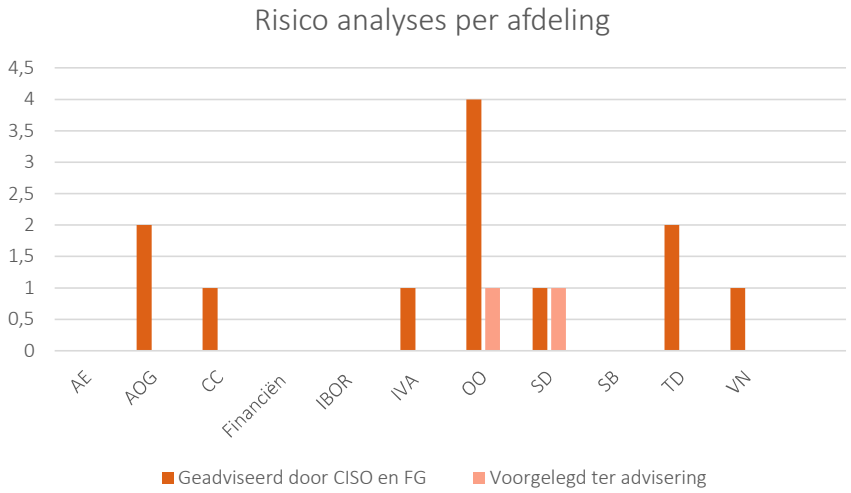
Processen

❖ Risicomanagement

Door in een vroeg stadium na te denken over de risico's, die het gebruik van persoonsgegevens met zich meebrengen, kunnen de juiste maatregelen worden getroffen. Risicomanagement zorgt hier voor. Daarmee wordt dan ook voldaan aan het principe van "Privacy by design"

- De uitgevoerde risicoanalyses en het uitgebrachte advies van FG en CISO worden gedocumenteerd in het zaaksysteem.
- Afwijkingen van het advies van de FG en de CISO worden niet consistent gemotiveerd vastgelegd noch, indien nodig, bekrachtigd door de directie.
- In 2023 zijn er minder risico analyses uitgevoerd en afgerond dan in 2022 en 2021. Er zijn geen risicoanalyses uitgevoerd op bestaande processen. Alle analyses hadden betrekking op een verandering.
- Risicoanalyses worden uitgevoerd op vraag en niet op basis van prioriteit.
- Er wordt in projecten te weinig tijd (in capaciteit en/of in doorlooptijd) geraamd voor het uitvoeren van een risico analyse op het gebied van privacy en informatieveiligheid.
- Niet altijd wordt het uitvoeren van een risico analyse als helpend ervaren.
- Mitigerende maatregelen worden niet consistent opgenomen in een (jaar)planning en uitgevoerd.





Organisatorische inbedding

Om daadwerkelijk invulling te geven aan de bescherming van privacy, moeten de taken organisatorisch zijn ingebed. Dit wordt bereikt met een goede taakverdeling en voldoende middelen

❖ Functionaris gegevensbescherming

- De FG bewaakt en bevordert dat de organisatie zich aan de privacyregels houdt. Ze bevordert de naleving door te adviseren over de wijze waarop het bestuur en management aan haar verplichtingen kan voldoen.
- Rol, taken en de autonome positie van de FG zijn in 2023 verbeterd. In het “Verhaal van de organisatie” wordt de FG-rol aangemerkt als een staf-functie en wordt ze geplaatst in de unit Concern Control. Dat past beter bij haar onafhankelijke rol.
- Voor 2024 heeft de FG een toezichtplan opgesteld, dit plan beschrijft op welke wijze de FG de naleving van de privacyregels bewaakt.
- De organisatie kan de positie van de FG verder verbeteren door afwijkingen van haar advies gemotiveerd vast te leggen. Daarnaast kan ze meer worden betrokken bij besluitvorming, bijvoorbeeld door haar als adviseur uit te nodigen bij vergaderingen van het management.

❖ Privacy team

- Er is een centraal team van Security en privacy officers benoemd. Naast het centrale team is er capaciteit in de afdeling nodig, omdat de medewerkers in de afdeling materie- proces- en applicatiedeskundige zijn. In 2023 heeft de directie alle afdelingshoofden hier op aangesproken. Het commitment hiervoor neemt toe.

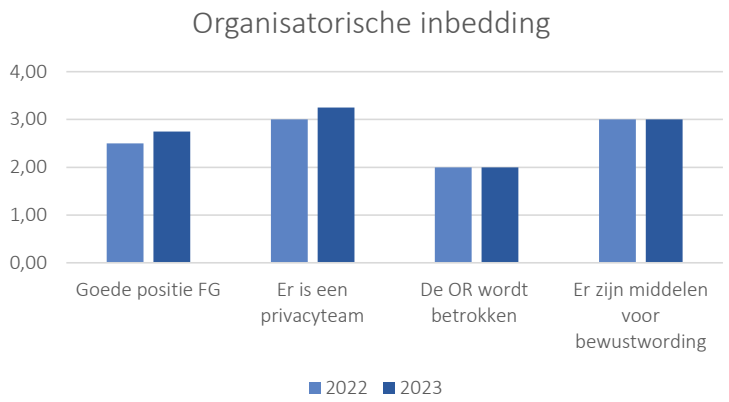
- Het zal bijdragen aan de verdere groei in volwassenheid, wanneer de thema’s privacy en informatiebeveiliging worden gezien als een kwaliteitsaspect van de dienstverlening. Door de thema’s te borgen in de processen en er in de planning rekening mee te houden dat hier tijd en capaciteit mee is gemoeid, zullen de thema’s minder als belemmerend worden ervaren.
- Het privacyteam werkt in opdracht van en ondersteunt het management bij het uitvoeren van de taken en de inbedding van de maatregelen in de organisatie als het gaat om de bescherming van persoonsgegevens.

❖ Ondernemingsraad (OR)

- De ondernemingsraad wordt, daar waar nodig, om instemming gevraagd. Ze wordt echter niet gestructureerd betrokken bij onderwerpen over de bescherming van persoonsgegevens van de medewerkers.

❖ Bewustwording

- Om de noodzakelijke cultuurverandering te bereiken is in 2022 het bewustwordingsprogramma ‘Helmond ben ik, veiligheid ben ik’ opgezet. Dit programma is in 2023 voortgezet. Metingen tonen aan dat het bewustzijn bij medewerkers sinds de start van het programma is toegenomen. Naast het aangekochte programma, organiseert het SPO team ook zelfstandig bewustwordingsactiviteiten.



Bewustwording in 2023

Onboarding

Nieuwe medewerkers volgen bij indiensttreding een E-learning en maken hierbij een kennistest. Er is een workshop in de vorm van een pubquiz “digitale veiligheid” ontwikkeld. Deze workshop is onderdeel geworden van het onboarding programma voor nieuwe medewerkers en kan ook op verzoek worden afgenomen.

Continu leren

Medewerkers ontvangen periodiek korte berichten (nano learnings) in hun inbox. In dit bericht wordt een onderwerp aan de orde gesteld. Hiermee worden betrokkenen geïnformeerd en gemotiveerd om veilig te handelen. Daarmee wordt continue bewust handelen rondom informatiebeveiliging en privacy gestimuleerd.

Workshops

Tijdens het Festival van de Weerbaarheid konden collega’s deelnemen aan workshops die betrekking hadden op informatiebeveiliging en privacy. Op de “Helmond ben ik dag” konden medewerkers meedoen aan het Helmondse Datalekkenspel.

Management en Bestuur

Eind 2023 zijn er bewustwordingssessies gehouden met het management en met het college. Deze sessies hadden tot doel het verantwoordelijkheids-gevoel voor informatiebeveiliging en privacy te vergroten.

Nieuwsberichten

Er is een site “Veilig werken” ingericht. Deze site bevat richtlijnen om digitaal veilig te werken. Daarnaast worden er
regelmatig nieuwsberichten gepubliceerd op het Knaal.

Clear desk clear screen

Met deze actie is er aandacht gevraagd voor het vergrendelen van de werkplek en het netjes achterlaten van de werkplek. Daarmee wordt voorkomen dat anderen de informatie, waarmee wordt gewerkt, kunnen inzien.

Pas op meelopers

Alle toegangsdeuren tot de beveiligde zones bevatten stickers: “Pas op meelopers”. Hiermee worden medewerkers geactiveerd om meelopers aan te spreken: “Hoor je hier wel thuis”. Zeker in het Huis voor de stad, waar ook mensen van buiten de organisatie kunnen werken is dit belangrijk.

Landelijke cyberoefening

In oktober is tijdens de cyber security week deelgenomen aan de landelijke cyberoefening. Doel van deze cyberoefening was om beter voorbereid te zijn, mocht zich in Helmond een cyberaanval voordoen. Verder werd inzicht gegeven in de bestuurlijke gevolgen van een cybercrisis.

Phishing competitie

Door middel van een phishing campagne en cultuurvideo’s werden medewerkers getraind om phishing mails te herkennen en adequaat te handelen.

Cyberbarometer:

In 2023 is gemeten hoe bewust onze organisatie is van de risico’s. De uitkomsten van deze meting worden gebruikt bij het opstellen van het meerjarig bewustwordingsprogramma 2024-2027.

Rechten van betrokkene

Inwoners en andere betrokkenen hebben het recht op informatie en inzage. Zo kunnen ze controleren of er op een juiste wijze wordt omgegaan met hun gegevens. Ze hebben het recht om aanpassing van de gegevens te vragen of een klacht in te dienen bij de FG. Ook hebben ze het recht op menselijke tussenkomst, bij geautomatiseerde besluiten.

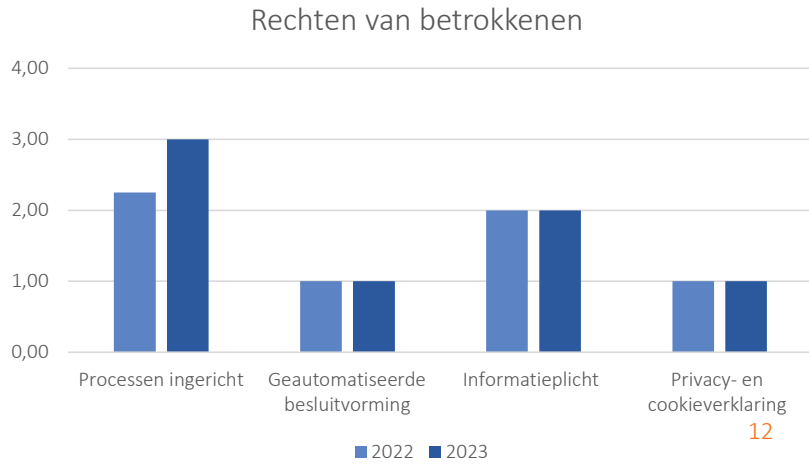
- Klachten
  - In 2023 heeft de FG geen klachten ontvangen.

- Processen
  - Er zijn processen en procedures opgesteld om uitvoering te geven aan de rechten van betrokkenen. Ook zijn er standaarddocumenten beschikbaar. Deze documenten zijn goed toegankelijk voor het privacy-team. Verzoeken komen echter ook op andere plekken in de organisatie binnen. Hierdoor is er nog geen sprake van een volledig uniforme benadering.

- Geautomatiseerde besluitvorming
  - Digitalisering neemt toe en daarmee ook de hoeveelheid data. Het is de ambitie van de gemeente Helmond om de data(stromen) te gebruiken om enerzijds te komen tot nieuwe inzichten en opgaven uit de stad en anderzijds slimme (geautomatiseerde) beslissingen te nemen. De gemeente maakt daarbij (nog) geen gebruik van geautomatiseerde (bestuursrechtelijke) besluitvorming, er is in die gevallen nog altijd sprake van “menselijke tussenkomst."
  - Momenteel bestaat er echter onvoldoende inzicht in het gebruik van automatisch verwerkte persoonsgegevens of algoritmes.

- Informatieplicht en Communicatieplan
  - De organisatie heeft (in het algemeen) een passieve houding voor wat betreft het informeren van betrokkenen. Betrokkenen worden via de privacyverklaring op de website geïnformeerd over hoe de gemeente Helmond omgaat met hun persoonsgegevens. Naaste deze algemene privacy verklaring zijn er weinig (domein) specifieke documenten. Een privacyverklaring voor medewerkers ontbreekt.
  - De organisatie ontwikkelt samen met de provincie en andere gemeenten een sensorenregister met bijbehorend kader, zodat betrokkenen kunnen opzoeken waar sensoren hangen en welke informatie er wordt verzameld.

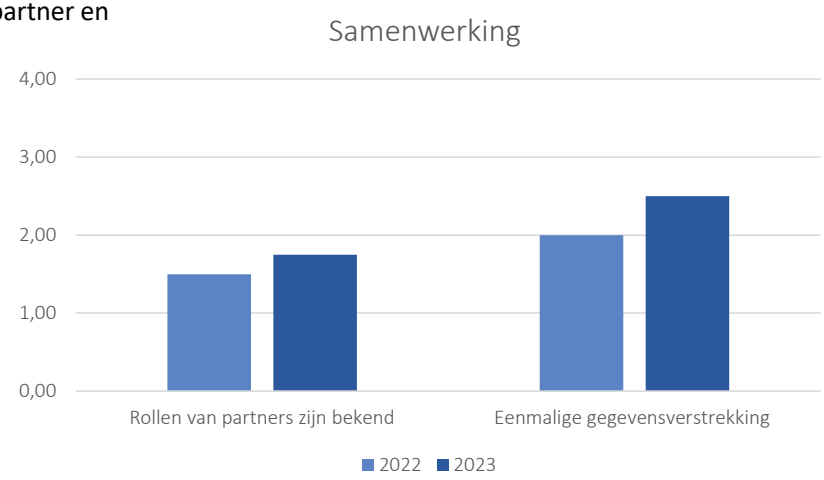
- Privacy- en cookieverklaring
  - De privacy-verklaring op de website “Helmond.nl”, voldoet aan de transparantieverplichting.
  - De cookieverklaring van de website "Helmond.nl" informeert over het gebruik van cookies op deze site. Er worden alleen analytische cookies geplaatst, daarvoor wordt Google Analytics gebruikt.
  - De gemeente Helmond participeert in verschillende websites. Het inzicht in het gebruik van cookies of andere persoonsgegevens op deze websites en de verantwoordelijkheid voor deze verwerkingen is onvolledig.



Samenwerking

Met haar partners deelt de gemeente Helmond gegevens. Betrokkenen moeten er op kunnen vertrouwen dat dit zorgvuldig en veilig gebeurt. Eenmalige verstrekkingen moeten daarom worden getoetst en bij meer structurele verstrekkingen moeten er goede afspraken gemaakt worden. Voor het maken van deze afspraken is het belangrijk om te weten welke rol een partner inneemt.

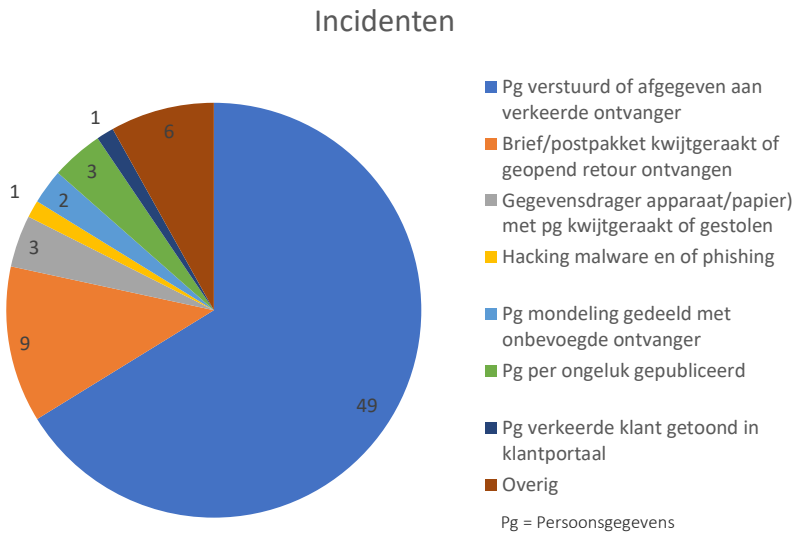
- Rollen van partners
  - Bij aanbestedingen door de afdeling inkoop, wordt er standaard uitvraag gedaan naar de rol die de partner heeft. Dit geldt niet voor aanbestedingen onder de drempel. In dat geval zijn afdelingen gerechtigd om zelfstandig producten aan te schaffen.
  - Er zijn een aantal standaardovereenkomsten beschikbaar, op afdelingsniveau is echter niet altijd inzichtelijk welke afspraken er moeten worden gemaakt en of deze afspraken passen bij de rol die een partij inneemt. Als gevolg hiervan gebeurt het dat contracten niet voldoen aan de eisen van de gemeente Helmond of van de AVG.
  - Ook bij het aangaan van samenwerkingsverbanden wordt niet altijd uitvraag gedaan naar de rol van de partner en worden afspraken rondom informatiebeveiliging en privacy niet goed vastgelegd.
- Gegevensverstrekking
  - De organisatie heeft in 2023 een proces incidentele gegevensverstrekkingen opgesteld.
  - Binnen dit proces is geborgd dat interne incidentele leveringen via de gegevensmakelaar worden getoetst aan de privacyregels en dat afspraken worden vastgelegd. Leveringen rechtstreeks uit een applicatie kunnen echter nog worden gemist.
  - Structurele en incidentele externe gegevensleveringen zijn nog niet in beeld.
  - Structurele gegevensleveringen worden in 2024 in kaart gebracht.

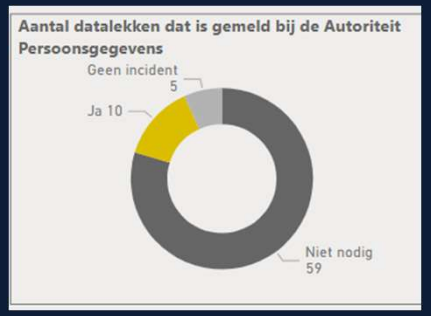


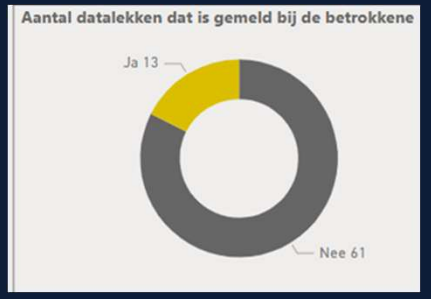
Beveiliging

De inwoner en medewerker moeten er op kunnen vertrouwen dat hun persoonsgegevens passend zijn beveiligd, zodat hun gegevens niet kunnen worden misbruikt. Dit betekent ook dat de inwoner en de medewerker kunnen rekenen op goede dienstverlening, omdat de juiste persoonsgegevens op het juiste moment voor de juiste mensen beschikbaar zijn

- De gemeente legt via ENSIA verantwoording af. Uit deze verantwoording blijkt dat het volwassenheidsniveau van informatiebeveiliging van de gemeente Helmond 2.2 op een schaal van 5. Dit niveau houdt mede in dat het afhankelijk is van de deskundigheid en inzet van individuele personen of de gegevens van onze inwoners en medewerkers passend zijn beveiligd.
- De organisatie is bezig met de ontwikkeling van een enterprise architectuur. In 2023 zijn richtinggevende principes opgesteld. Deze principes zijn richtinggevend bij alle veranderingen binnen de organisatie die impact hebben op de organisatie en de informatievoorziening. De enterprise architectuur moet in de loop van 2024 vertaald worden in een domein architectuur informatiebeveiliging en privacy. Op dat moment ontstaan er gedocumenteerde eisen om privacy risico's in de ontwerpfase voor processen en systemen mee te nemen. Bovendien is dit richtinggevend voor de inrichting van de organisatie en informatievoorziening van alle organisatiedomeinen.
- In 2023 is de organisatie gestart met ITSM. Daarmee krijgt de organisatie een eenduidig proces om privacy incidenten te identificeren en beheren.
- Er zijn in 2023 74 incidenten gemeld. Uiteindelijk bleek er in 69 gevallen sprake te zijn van een datalek.
- Er worden nauwelijks aanvallen van buitenaf gemeld. Overige incidenten worden vaak gemeld. Er kan daarom worden vastgesteld dat het personeel adequaat reageert, ondanks het ontbreken van een eenduidig proces.
- Incidenten kunnen leiden tot een verstoring van de bedrijfsvoering. Het is daarom van belang dat er Bedrijfscontinuïteitsmanagement (BCM) is in ingericht. Hier is in 2023 mee gestart. In 2024 wordt BCM verder projectmatig opgepakt.





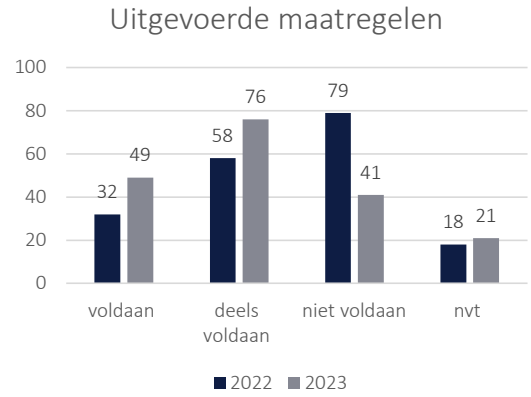


Verantwoording

De AVG vereist dat de organisatie kan aantonen dat er zorgvuldig wordt omgegaan met de gegevens van betrokkenen en dat de AVG wordt nageleefd. Met een GAP analyse kan worden vastgesteld waar de gemeente voldoet aan de privacywetgeving en waar in de toekomst nog aan gewerkt moet worden.

❖ Aantonen naleving en GAP analyse

- Er vindt jaarlijks een GAP analyse, op basis van het VNG/IBD privacy normenkader, plaats op organisatie niveau. De FG baseert hier het jaarverslag op en maakt daarmee inzichtelijk hoe de organisatie staat op het gebied van privacy.
- Het normenkader bevat 164 maatregelen die van toepassing zijn. Door het implementeren van deze maatregelen groeit de organisatie in volwassenheid.
- Het aantal geïmplementeerde maatregelen is in 2023 toegenomen.
- Er vindt op afdelingsniveau echter nauwelijks toezicht plaats op de rechtmatigheid van de verwerking van persoonsgegevens. Er wordt door hen niet over gerapporteerd.
- Het uitvoeren van de GAP analyse is onderdeel van een PDCA-cyclus. De directie ontvangt het jaarverslag en naar aanleiding van het jaarverslag 2022 heeft ze in het concernplan en de afdelingsplannen verbetermaatregelen privacy en informatiebeveiliging opgenomen
- Gemeenteraad en college ontvangen het jaarverslag. Het jaarverslag is openbaar, en werd in 2022 actief bekend gemaakt.
- De FG heeft voor 2024 een Toezichtplan opgesteld. Op basis van dit plan ziet ze in 2024 toe op de naleving van de privacyregels.
- Er is een project Gegevensmanagement gestart, dit project zorgt ervoor dat voor alle aspecten van goed gebruik van gegevens organisatie-breed afspraken zijn gemaakt. Er is een instrumentarium ontwikkeld, een roadmap en een actieplan opgesteld.

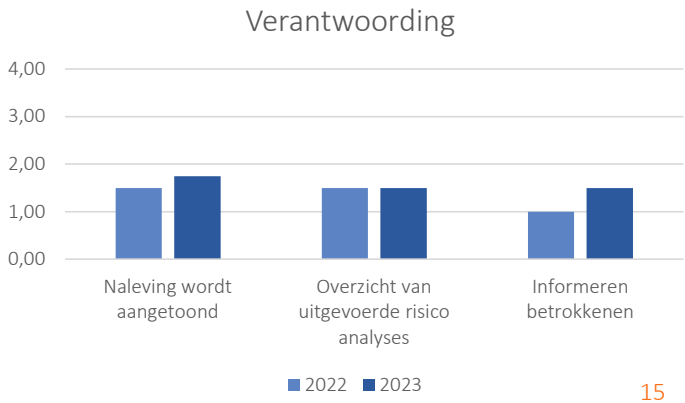


❖ Overzicht uitgevoerde risico analyses

- Er is een fragmentarisch beeld van verwerkingen met een hoog risico en uitgevoerde risico analyses.
- De risico's en de plannen met te nemen maatregelen worden niet formeel vastgesteld en de te nemen maatregelen worden niet planmatig opgepakt.

❖ Informeren betrokkenen

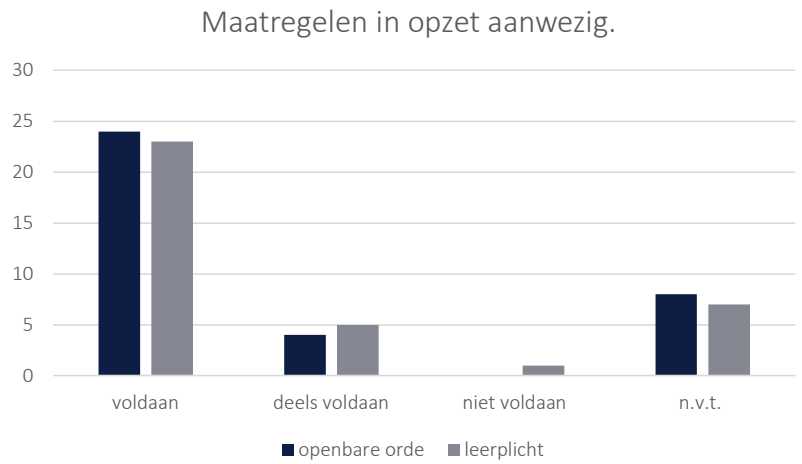
- Bestuurders worden jaarlijks geïnformeerd over de omgang met persoonsgegevens door middel van het jaarverslag van de FG. Dit jaarverslag is openbaar en wordt op de website gepubliceerd.
- Betrokkenen worden vooral reactief, naar aanleiding van vragen, klachten en datalekken, geïnformeerd over de omgang met hun persoonsgegevens.



WPG voor Boa's

Sinds begin 2019 is de Wet politiegegevens (Wpg) ook van kracht voor bijzonder opsporingsambtenaren (Boa's). Bij de afdeling Veiligheid & Naleving (openbare orde) en bij het Sociaal Domein (leerplicht) werken Boa's. Om aan te tonen dat de gemeente Helmond compliant is aan de Wpg moet jaarlijks een interne audit en eens in de vier jaar, een externe audit worden uitgevoerd.

- In 2022 is een externe audit uitgevoerd. De gemeente voldeed toen niet aan haar verplichtingen. In 2023 is daarom een hercontrole uitgevoerd door een externe auditor. De beide afdelingen hebben een verbeterplan opgesteld.
- Naar aanleiding van de hercontrole heeft de externe auditor een auditrapportage opgesteld. Deze rapportage is begin 2024 aangeboden aan het college.
- De gemeente heeft de in het verbeterplan opgenomen maatregelen uitgevoerd. Er zijn o.a. instructies en protocollen opgesteld. Hierdoor kan worden vastgesteld dat bijna alle noodzakelijke maatregelen volledig in opzet aanwezig zijn.
- Er is nog niet aangetoond dat ook gewerkt volgens afspraak. Daarvoor is het nodig dat hier ook gedurende het jaar op wordt gemonitord door de afdeling.
- De FG heeft geen aanvullend onderzoek uitgevoerd. De uitkomsten uit de hercontrole geven hier geen aanleiding toe.
- In 2024 vindt er wel een interne audit plaats. Bovendien heeft de FG toezicht op de Wpg opgenomen in het toezichtplan.



Vooruitblik

❖ Huis voor de Stad
- In 2024 verhuizen we naar het Huis voor de Stad. Het Huis voor de Stad heeft een open karakter, dit heeft effect op de beveiliging van onze infrastructuur en informatie. Het open karakter, de flexibele werkplekken en het hybride werken vergroten de kans op meeluisteren of meekijken. De FG zal in 2024 onderzoeken of er voldoende maatregelen zijn getroffen om meeluisteren of meekijken te voorkomen.

❖ Ethiek
- Digitale vernieuwingen zullen de komende jaren veel teweeg gaan brengen en grote alertheid vragen. Het is aan de overheid om hiervoor goede kaders te stellen. De “Agenda Digitale Grondrechten en Ethiek 2022-2026” geeft de gemeenten daar instrumenten voor.

❖ Algoritme

Regie op je digitale leven betekent onder meer dat je erop kan vertrouwen dat digitale systemen, waaronder algoritmes, aan publieke waarden voldoen en dat je begrijpt hoe deze werken. Bij bedrijven en de overheid is dit op het moment geen gegeven.
In Europa wordt gewerkt aan een AI verordening, (EU Artificial Intelligence (AI) Act) omdat men vindt dat de huidige Europese regelgeving de (toekomstige) risico’s van AI onvoldoende adresseren. De Autoriteit Persoonsgegevens (AP) is sinds 2023 coördinerend toezichthouder op algoritmes en AI die risico’s met zich meebrengen voor publieke waarden en grondrechten. De AP publiceert elk half jaar een Rapportage AI- & algoritmerisico’s Nederland (RAN), om daarmee een beeld te geven van recente ontwikkelingen, actuele risico’s en bijbehorende uitdagingen. Op 9 december is op Europees niveau een politiek akkoord gesloten over de AI-verordening. De komende maanden worden details verder uitgewerkt om de verordening medio 2024 in werking te laten treden, met daaropvolgend een overgangsperiode alvorens regels van toepassing worden. Daarmee is een belangrijke stap gezet die zal bijdragen aan de beheersing en controle van AI. De praktijk zal moeten uitwijzen of de verordening een adequate basis gaat vormen voor veilige algoritmes en AI.




Vooruitblik

Dienstverlening is en wordt steeds verder gedigitaliseerd. De hoeveelheid data en (digitale) informatie groeit razendsnel en daarmee ook de mogelijkheden en de risico's. Er zal daarom blijvend veel aandacht (nodig) zijn voor privacy en gegevensbescherming. Zowel Europees als landelijk is die aandacht terug te zien in wetgeving (in voorbereiding). De tabel hiernaast bevat een overzicht van digitale wetgeving met een inschatting van de datum waarop de wet in werking treedt. Daarnaast bevat de tabel een grove indicatie van de impact/ benodigd werk voor de gemeente Helmond.

Naam	Beoogde datum in werking v.d. wet	Impact	loopt al	2024	2025	2026	2027
Wet Open Overheid (Woo)	reeds	hoog	X	X	X	X	X
Wet Modernisering Elektronisch Bestuurlijk Verkeer (Wmebv)	1-jan-25	middel		X	X		
Archiefwet 202X (Aw)	1-jan-25	middel			X	X	
Single Digital Gateway: Annex 2/OOTS (SDG)	"2023"	middel			X	X	
Wet Digitale Overheid: Stelsel Toegang en eIDAS2.0 (Wdo)	2024-2026	laag			X	X	
Algemene Informatiewet	n.t.b.	n.t.b.					
Netwerk en informatiesystemen richtlijn (NIS2/NIB2)	17-okt-24	hoog		X	X		
Cyberbeveiligingsverordening / Cyber Security Act	reeds	middel				X	
Cyberweerbaarheidsverordening / Cyber Resilience Act	n.t.b.	n.t.b.				X	X
Critical Entities Resilience	17-okt-24	n.t.b.				X	X
ePrivacy verordening	n.t.b.	n.t.b.					
Digital Services Act (DSA)	reeds	zeer laag	X				
Digital Markets Act (DMA)	reeds	zeer laag	X				
Data Act	sep-23	n.t.b.					
Data Governance Act	n.t.b.	n.t.b.					
Open data richtlijn	n.t.b.	n.t.b.					
AI Act	~2026	middel				X	X
Urban Air Mobility	2023/2024	zeer laag					

Adviezen

Randvoorwaardelijk

De groei in volwassenheid op het thema privacy kan niet los worden gezien van de volwassenheid van de organisatie op andere thema's. Opvolging van onderstaande adviezen is randvoorwaardelijk om daadwerkelijke groei te bereiken.

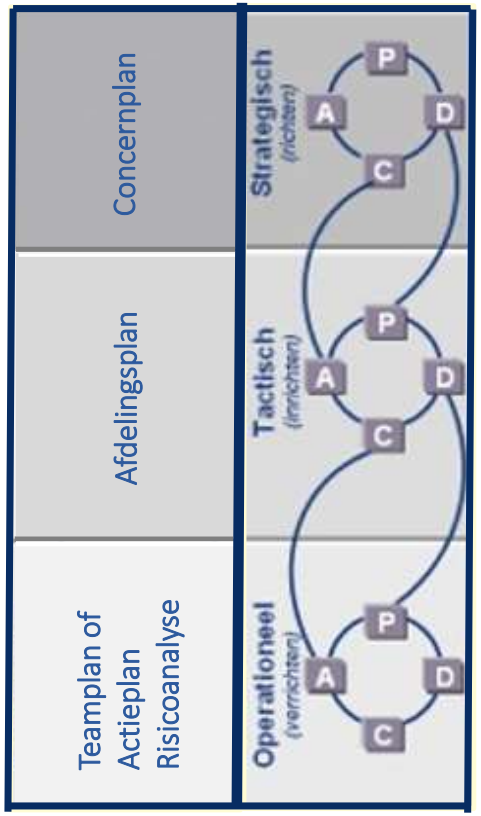
Advies	Prioriteit	Accountable Directie	Accountable Afdelingshoof	Responsible	Thema waaraan wordt bijgedragen:
Doe mee aan bewustwordingsactiviteiten.	Randvoorwaardelijk	Directeur bedrijfsvoering	Allen	SPO team en Helmond academie	Alle thema's
Betrek de FG actiever bij aangelegenheden die de privacy van inwoners of medewerkers kunnen raken.	Randvoorwaardelijk	Directeur bedrijfsvoering	Allen	Management	Alle thema's
Werk onder architectuur, zodat in samenhang de organisatiedoelen worden gehaald.	Randvoorwaardelijk	Directeur bedrijfsvoering	Allen	CIO office	Alle thema's
Werk proces- en ketengericht.	Randvoorwaardelijk	Directeur bedrijfsvoering	Allen	Procesadviseurs	Alle thema's
Werk zaakgericht.	Randvoorwaardelijk	Directeur bedrijfsvoering	Allen	Informatiediensten	Alle thema's
Hou je ook bij de zelfstandige aanschaf van producten aan de Helmondse afspraken.	Randvoorwaardelijk	Directeur bedrijfsvoering	Allen	Inkoop	Alle thema's
Pas risico management toe.	Randvoorwaardelijk	Directeur bedrijfsvoering	Allen	CC	Alle thema's
Pas de gemaakte afspraken rondom gegevensgebruik en de kwaliteit hiervan toe.	Randvoorwaardelijk	Directeur bedrijfsvoering	Allen	Informatiediensten	Alle thema's

Adviezen

Maatregelen

Om te groeien in volwassenheid is het nodig dat (verbeter)acties uit beleid, adviezen en verantwoordingstrajecten daadwerkelijk worden opgepakt en uitgevoerd en dat het resultaat wordt geborgd. Een inbedding van privacy in de PDCA cycli leidt tot grip op verbetering en groei op de thema's privacy en informatiebeveiliging.

Advies	Prio	Klaar	Accountable Directie	Accountable Afd. hoofd	Responsible	Supporting	Thema waaraan wordt bijgedragen:
Actualiseer de kernregistratie processen	1	Q2	Bedrijfsvoering	IVA *	Procesadviseurs		Processen
Actualiseer het register van verwerkingen.	1	Q2	Bedrijfsvoering	Allen	Management	SPO team	Processen
Benoem de 10 processen met de meeste privacyrisico's voor betr.	2	Q2	Bedrijfsvoering	CC	CC	SPO team	Processen
Beschrijf of verbeter het proces van deze 10 processen	2	Q4	Bedrijfsvoering	IVA *	Procesadviseurs		Processen
Voer een risico-analyse uit op deze 10 processen	2	Q4	Bedrijfsvoering	Allen	Management	SPO team	Processen
Het volgende beleid uit te werken en vast te stellen:							
Een visie op informatievoorziening en een informatiebeleid.	3	Q4	Bedrijfsvoering	IVA	CIO office		Beleid
Informatiebeveiligings- en privacybeleid.	2	Q4	Bedrijfsvoering	Ciso en IVA	Adviseur IB en architectuur		Beleid
Integraal risicomanagement.	3	Q4	Bedrijfsvoering	CC	CC		Procesen
Visie op bewustwording.	2	Q2	Bedrijfsvoering	IVA en AOG*	SPO + Helmond academie		Org. inbedding
Procesbeleid.	3	Q4	Bedrijfsvoering	IVA *	Procesadviseurs		Processen
AI en Algoritme beleid	3	Q4	Bedrijfsvoering	IVA	CIO office		Rechten betr.
Architectuur te ontwikkelen en vast te stellen:							
Enterprise architectuur als kader voor grote veranderopgaven.	2	Q4	Bedrijfsvoering	IVA	CIO office		Alle thema's
Domeinarchitectuur informatiebeveiliging en privacy.	3	Q4	Bedrijfsvoering	IVA	Adviseur IB en architectuur		Alle thema's
IT-servicemanagement in te richten.	1	Q2	Bedrijfsvoering	IVA	Regisseur FB en AB		Beveiliging
Te monitoren op toegang van applicaties.	2	Q2	Bedrijfsvoering	Allen	Functioneel beheerders		Beveiliging
Binnen het progr. Altijd Verbonden prioriteit te geven aan de thema's:							
Implementatie monitoring en logging beleid.	1	Q2	Bedrijfsvoering Dienstverlening	Stuurgroep	Progr.manager Altijd Verbonden		Beveiliging
Informatiebeheer.	1	Q4	Bedrijfsvoering Dienstverlening	Stuurgroep	Progr.manager Altijd Verbonden		Processen



* In de toekomst SB

Met betrekking tot alle niet geprioriteerde maatregelen adviseert de FG het management persoonlijk en mondeling. Hierbij worden ook de adviezen van de CISO op het gebied van informatiebeveiliging meegenomen. Deze (aanvullende) adviezen zijn ook te vinden in bijlage 2.

Adviezen

Monitoring

Door ook privacy onderwerp te maken van de sturingsgesprekken, op elk niveau, wordt opvolging gemonitord en wordt privacy steeds meer ingebed in een PDCA cyclus en ontstaat er verbinding met de P&C Cyclus.

Advies	Prioriteit	Accountable	Accountable Afdelingshoofd	Responsible	Supporting	Thema waaraan
Periodiek verantwoording af te leggen over het uitvoeren van maatregelen op het gebied van privacy en informatiebeveiliging.	Continue monitoring	Directeur bedrijfsvoering	Allen	Management	SPO team	PDCA cyclus
Te sturen op blijvende inzet binnen afdelingen en teams op de thema's privacy en informatiebeveiliging.	Continue monitoring	Directeur bedrijfsvoering	Allen	Management	SPO team	Alle thema's
Medewerkers aan te spreken op deelname aan bewustwordingsactiviteiten.	Continue monitoring	Directeur bedrijfsvoering	Allen	Management	AOG	Alle thema's

De FG adviseert het management mondeling over de wijze waarop zij hier uitvoering aan kunnen geven. Deze adviezen worden gecombineerd met de adviezen van de CISO en ze zijn ook te vinden in bijlage 2.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	1, 3

Gemeente Helmond

Jaarverslag 2024

Privacy

1 maart 2025

5.1.2e

Inhoud

- Managementsamenvatting
- Inleiding
- Uitgevoerd toezicht
- Bewustwording
- Bewaken
  - Register van verwerkingen
  - Risico- analyses
  - Thema-onderzoeken en klachten
  - Borging gegevensbescherming
    - Volwassenheid van de organisatie
    - Beleid
    - Processen
    - Organisatorische inbedding
    - Rechten van betrokkene
    - Samenwerking
    - Gegevensbescherming
    - Verantwoording
    - Wet Politiegegevens
- Vooruitblik
- Adviezen

Voorwoord

De gemeente Helmond heeft één Functionaris voor de gegevensbescherming. (FG). Zij ziet toe op de naleving van de Algemene verordening gegevensbescherming (AVG) en de Wet Politiegegevens (WPG).

Volgens de wet heeft de FG verschillende taken:

- Informeren en adviseren over de verwerking van persoons- en politiegegevens.
- Controleren of de verwerking van persoons- en politiegegevens netjes en transparant gebeurt.
- Er op toezien dat mensen binnen en buiten de gemeente hun privacyrechten kunnen uitoefenen.
- Toezien op de juiste afhandeling van datalekken.
- Behandelen van klachten over de verwerking van persoons- en politiegegevens.

In dit jaarverslag rapporteer ik als FG aan bestuur en directie over mijn werkzaamheden en bevindingen. Dit gaat over hoe de gemeente Helmond in 2024 de privacyregels en haar eigen beleid heeft nageleefd.

5.1.2e

Functionaris voor de gegevensbescherming.

Managementsamenvatting

Bevindingen

Een lagere volwassenheid dan in 2023

De organisatie kan niet aantonen dat de persoonsgegevens van haar inwoners en medewerkers verantwoord worden gebruikt en veilig zijn.
Bij een volwassenheidsniveau van 3 is de basis op orde. Pas dan zijn de randvoorwaarden gecreëerd die nodig zijn om zich betrouwbaar te kunnen tonen. Voor een verantwoorde inzet van digitale innovaties is een hoger volwassenheidsniveau nodig.
De organisatie heeft een volwassenheidsniveau van 2,1, dit is lager dan in 2023 (2,2).

Ook op andere thema's is groei nodig.

De groei in volwassenheid op het thema privacy draagt bij aan het toegroeien naar het in control zijn van de organisatie. Het is één van de relevante onderwerpen van een in control statement.
Bovendien is privacy geen losstaand onderwerp. Om te kunnen groeien op het gebied privacy is ook groei nodig op thema's zoals: werken onder architectuur, informatiebeveiliging, informatiebeheer, proces- en zaakgericht werken en risico management.

Adviezen

Geef prioriteit aan het verkrijgen van overzicht.

Een volwassen organisatie heeft grip op de risico's die zij loopt. Hiervoor is het noodzakelijk dat de organisatie overzicht en inzicht krijgt in de aanwezige informatie en de ondersteunende applicaties. Dit overzicht en inzicht ontbreekt, het verkrijgen van dit overzicht zou de allerhoogste prioriteit moeten krijgen.
Ik adviseer daarom om de kernregistratie processen, het verwerkingenregister en de CMDB in 2025 te actualiseren, zodat zij zo snel mogelijk maar in ieder geval voor de tweede helft van 2025 allen actueel en accuraat zijn. Daarmee heeft de organisatie inzichtelijk wat ze in huis heeft.
Breng vervolgens in beeld waar betrokkenen en de organisatie risico's lopen en waar aanvullende maatregelen nodig zijn. Ik adviseer om minimaal 10 bestaande processen, te beschrijven/verbeteren en een risico analyse uit te voeren op deze processen. Zodat eind 2025 van deze 10 processen de noodzakelijke risico mitigerende maatregelen zijn getroffen. (zie blz 24 en verder voor het volledige advies).

Eigenaarschap en sturing

Om te kunnen groeien in volwassenheid is het nodig dat adviezen en (verbeter)acties uit beleid en verantwoordingstrajecten daadwerkelijk worden opgepakt en uitgevoerd. Hiervoor is het noodzakelijk dat het management, onder regie van de gemeentesecretaris, meer eigenaarschap toont en dat er in 2025 daadwerkelijk wordt gestuurd, op de thema's informatiebeveiliging en privacy. Bij een ongewijzigde aanpak zal de organisatie zich niet significant verbeteren.
Ik adviseer om de Galan groep de opdracht te geven om dit mee te nemen in het management developmentprogramma en hen dit jaarverslag te verstrekken.

Inleiding

- De gemeente Helmond werkt hard aan haar visie voor de toekomst. Het realiseren van brede welvaart, een energietransitie richting klimaatneutraal en via de schaalsprong een sterkere stad voor iedereen. Om dit te bereiken worden opgaven, strategische visies en beleid vertaald naar programma's en projecten om verandering te realiseren. In het zoeken naar oplossingen spelen technologische innovaties en ICT een belangrijke rol, zoals het toepassen van sensoren en van kunstmatige intelligentie. Data en documenten stromen volop tussen afdelingen en ketenpartners. Daarnaast verandert de samenleving als geheel door de groeiende digitalisering.
- Om deze ambities waar te maken is het essentieel dat de gemeente digitale technologie verantwoord inzet en goede dienstverlening aanbiedt aan burgers en ondernemers. Dit vraagt om proactief handelen, regie nemen en prioriteiten stellen. Welke kansen wil de organisatie pakken en waar moet er worden ingegrepen om risico's te verkleinen. Wat kan nu en wat kan later. En hoe houden ze daarbij rekening met de privacy van haar inwoners en medewerkers.
- De ontwikkeling van kunstmatige intelligentie (AI) ging in 2024 sneller dan ooit. Generatieve AI, zoals Chat GPT en Copilot, is nog krachtiger geworden waardoor het breder ingezet wordt. Het wordt steeds moeilijker om te onderscheiden wat echt of nep is. Bovendien zijn AI- tools zijn beter toegankelijk en eenvoudiger in gebruik. De drempel om AI te gebruiken wordt dan ook steeds lager. Dit terwijl de toegenomen mogelijkheden zorgen voor complexiteit, wat beheersing lastiger maakt en het onderwerp relevanter. Zeker in relatie tot de menselijke waarden.
- Deze ontwikkelingen maken een robuuste privacy organisatie noodzakelijk. Door middel van toezichtonderzoeken, documenten en waarnemingen genereer ik een beeld van de organisatie en de naleving van de wet- en regelgeving rond de bescherming van persoonsgegevens. U leest in dit jaarverslag op welke wijze ik toezicht heb gehouden. Tot slot kijk ik vooruit en vindt u mijn adviezen.

Uitgevoerd Toezicht

Toezicht door de FG bestaat uit bevorderen en bewaken. Bevorderen dat de gemeente haar verantwoordelijkheid neemt bij de naleving van de privacyregels, door bestuur en het management te informeren en te adviseren over de verplichtingen die gemeente heeft. Daarnaast bewaak ik de naleving van de privacyregels door hier onderzoek naar te doen. Om daarbij de juiste problemen aan te pakken hou ik risico gestuurd onderzoek. In het toezichtplan[1] leg ik jaarlijks vast waar ik komend jaar aandacht aan zal besteden.

Bevorderen

Met bewustwordingsactiviteiten heb ik de organisatie geïnformeerd over haar verplichtingen. (zie blz 7). Daarnaast heb ik in 2024 het bestuur en het management onder andere geadviseerd over de volgende onderwerpen:

- De inrichting van Mobile device management.
- Het Zorg en Veiligheidshuis.
- Veilig mailen.
- Wifi tracking in de binnenstad.
- Preventie met gezag.
- Het delen van gegevens met de arbodienstverlener.
- Zorgned (applicatie Sociaal Domein).
- Strategie verkeersveiligheid Helmond.
- Digitaal ondertekenen.
- Kentekentoezicht.
- Cameratoezicht Huis voor de stad.

Bewaken

Ik heb in 2024 de naleving van de privacy bewaakt door de volgende onderzoeken uit te voeren:

1. Onderzoek naar de volledigheid van het register van verwerkingsactiviteiten.
2. De uitvoering van risico- analyses.
3. Thema onderzoeken en klachten.
4. Onderzoek naar de borging van de gegevensbescherming binnen de organisatie.

Een toelichting volgt vanaf blz 8

[1] zie Toezichtplan FG 2024 Djuma: 51890882.

Bevorderen

Bewustwording

Continu leren

Medewerkers ontvangen periodiek korte berichten (nano learnings) in hun inbox. In dit bericht wordt een onderwerp aan de orde gesteld. Hiermee worden betrokkenen geïnformeerd en gemotiveerd om veilig te handelen. Daarmee wordt continue bewust handelen rondom informatiebeveiliging en privacy gestimuleerd.

Onboarding

Nieuwe medewerkers volgen bij indiensttreding een E-learning en maken hierbij een kennistest. Er is een workshop in de vorm van een pubquiz “digitale veiligheid” ontwikkeld. Deze workshop is onderdeel geworden van het onboarding programma voor nieuwe medewerkers en kan ook op verzoek worden afgenomen.

Huis voor de stad

Bij de opening van het huis voor de stad was er een informatiestand. Medewerkers konden hier terecht met vragen over veilig werken in het gebouw. Deze informatie is ook te vinden in het handboek “Zo werken we in het huis voor de stad”.

Nieuwsberichten

Er is een site “Veilig werken” ingericht. Deze site bevat richtlijnen om digitaal veilig te werken. Daarnaast worden er regelmatig nieuwsberichten gepubliceerd op het Knaal.

Clear desk clear screen

Met een schouw is er aandacht gevraagd voor het vergrendelen van de werkplek en het netjes achterlaten van de werkplek. Daarmee wordt voorkomen dat anderen de informatie, waarmee wordt gewerkt, kunnen inzien.

Cyberbarometer:

In september is onderzocht hoe het bewustzijn van informatiebeveiliging en privacy is gegroeid sinds de vorige meting. De bewustwording is s op bijna alle thema’s gelijk gebleven. Er is ook gekeken welke acties er nog nodig zijn om de kennis en weerbaarheid van de organisatie verder te verbeteren. De resultaten van deze acties en metingen zijn gebruikt om de jaarplanning voor bewustwording in 2025 op te stellen.

Phishing actie

Het incident rondom de fraudefactuur, die via phishing bij een externe leverancier was verkregen, benadrukt het belang van bewustzijn qua houding en gedrag. Het incident is daarom gebruikt om de medewerkers hier op te wijzen. Daarnaast is er in 2024 een phishing actie uitgevoerd.

Afdelingsactiviteiten:

Tijdens afdelingsoverleggen zijn, voor die afdeling van belang zijnde onderwerpen op het vlak van informatiebeveiliging en privacy, gepresenteerd en besproken.

Bewaken

1. Register van verwerkingsactiviteiten

Om haar inwoners en medewerkers goed van dienst te kunnen zijn worden binnen de processen persoonsgegevens gebruikt. Om dit zorgvuldig en veilig te kunnen doen is inzicht nodig in de processen en de persoonsgegevens die daarbij worden gebruikt. Het gebruik van persoonsgegevens moet worden vastgelegd in een register van verwerkingsactiviteiten (verwerkingsregister). Een randvoorwaarde voor dit register is een actuele en accurate registratie van alle processen die de gemeente uitvoert.

Toezicht

Omdat een compleet register een cruciale stap is om te kunnen voldoen aan de privacywetgeving, heeft de directie op 28 maart 2024 besloten om zowel het actualiseren van de kernregistratie processen als het actualiseren van het verwerkingsregister de allerhoogste prioriteit te geven, met als einddatum 1 juli 2024. Mijn toezicht heeft zich geconcentreerd op de vraag of er opvolging is gegeven aan het directiebesluit. Ik heb hierover gerapporteerd op 22 juli 2024. In december 2024 heb ik opnieuw de stand van zaken beoordeeld, en de bevindingen opgenomen in dit jaarverslag.

Conclusies

❖ 22 juli 2024:
- Zowel kernregistratie processen als het verwerkingsregister van verwerkingsactiviteiten zijn niet actueel en compleet.
- Er is onvoldoende eigenaarschap en er is onvoldoende gestuurd op opvolging van het directiebesluit.
- Bij een ongewijzigde aanpak zal de organisatie zich niet significant verbeteren.

❖ 31 december 2024:
- Zowel kernregistratie processen als register van verwerkingsactiviteiten zijn niet actueel en compleet.
- Er is onvoldoende eigenaarschap en er is onvoldoende gestuurd op opvolging van het directiebesluit.
- Bij een ongewijzigde aanpak zal de organisatie zich niet significant verbeteren.

Toelichting Conclusies

Als reactie op de rapportage van 22 juli 2024 heeft de directie op 19 november 2024 een 2 uur durende thema workshop met directie en (afdelings)managers georganiseerd. Deze workshop stond in het teken van de actualisatie van de kernregistratie processen, de benoeming van de 10 meest risicovolle processen en het maken van vervolgafspraken zodat vóór eind november het verwerkingsregister zou zijn geactualiseerd. Omdat de geformuleerde doelen niet zijn bereikt is er een vervolgsessie gepland in januari 2025.

De actualisatie van de kernregistratie processen en het register van verwerkingsregister zijn echter nog steeds niet afgerond, dat betekent dat feitelijk andere activiteiten een hogere prioriteit hebben gekregen. Hier kunnen goede redenen voor zijn, er ontbreekt echter een expliciet besluit met een nieuwe planning. Er is onvoldoende eigenaarschap en er is onvoldoende gestuurd op opvolging van het directiebesluit.

Bewaken

2 Risico-analyses

Door in een vroeg stadium na te denken over de risico's, die het gebruik van persoonsgegevens met zich meebrengen, kunnen de juiste maatregelen worden getroffen. Risicomanagement zorgt hier voor. Daarmee wordt dan ook voldaan aan het principe van "Privacy by design".

Toezicht:

Om aan te kunnen tonen dat er passende maatregelen zijn getroffen is een risico analyse nodig. De gemeente heeft als beleid dat er bij verandering en/of vernieuwing van processen een risico analyse zal worden uitgevoerd, voordat de verandering of vernieuwing wordt uitgevoerd. Daarnaast heb ik 2024 geadviseerd om een risico analyse uit te voeren op de 10 meest risico volle bestaande processen. De directie heeft op 28 maart 2024 besloten om dit advies over te nemen. Mijn toezicht heeft zich geconcentreerd op de vraag of er opvolging is gegeven aan het directiebesluit. Ik heb hierover gerapporteerd op 22 juli 2024. In december 2024 heb ik opnieuw de stand van zaken beoordeeld, en heb ik onderzocht of de gemeente zich heeft gehouden aan haar eigen beleid. De bevindingen zijn opgenomen in een workingpaper[1] en in dit jaarverslag.

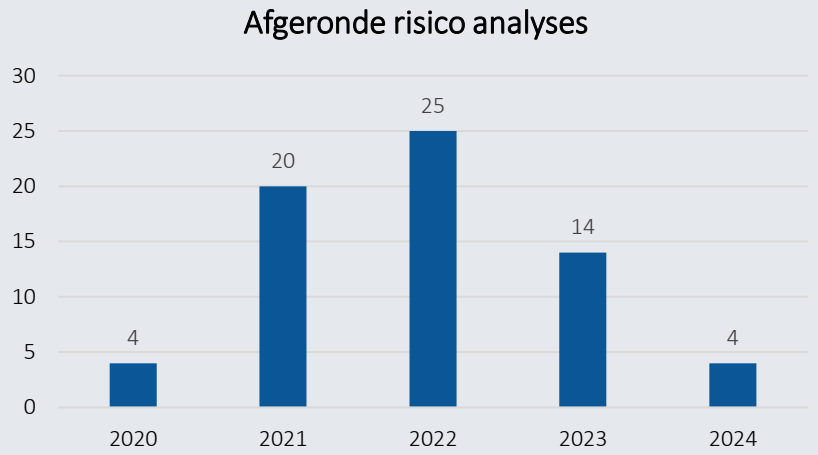
Conclusies

❖ 22 juli 2024:

- Er zijn geen processen benoemd, er is daarmee ook geen planning voor het uitvoeren van risico analyses op deze processen. Het wordt daarom moeilijk om voldoende capaciteit vrij te maken om daadwerkelijk in 2024 een risico analyse uit te voeren op 10 aangewezen processen.
- Er is onvoldoende eigenaarschap en er is onvoldoende gestuurd op opvolging van het directiebesluit.

❖ 31 december 2024:

- In 2024 zijn er minder risico analyses uitgevoerd en afgerond dan in 2023 en eerdere jaren.
- Er zijn geen risicoanalyses uitgevoerd op bestaande processen. Alle analyses hadden betrekking op een verandering.
- Risicoanalyses worden uitgevoerd op vraag en niet op basis van prioriteit.
- Er wordt in projecten te weinig tijd (in capaciteit en/of in doorlooptijd) geraamd voor het uitvoeren van een risico analyse op het gebied van privacy en informatieveiligheid.
- Het uitveren van een risico analyse en de uitvoering van mitigerende maatregelen worden niet consistent opgenomen in een (jaar)planning.



[1] zie RA.02.01 Overzicht uitgevoerde risico analyses.docx

Bewaken

3. Thema onderzoeken en klachten

Op basis van ontwikkelingen binnen de gemeente vindt thematisch onderzoek plaats. Daarnaast vormen jn klachten van inwoners of medewerkers een signaal om een onderzoek in te stellen.

Klachten

In 2024 heb ik twee klachten van inwoners behandeld.

- Een inwoner vond dat de gemeente geen adresgegevens uit de Basisregistratie personen (BRP) aan de GGD had mogen verstrekken. Zijn klacht was ongegrond. De gemeente Helmond had deze gegevens namelijk niet verstrekt. De GGD beschikt zelf over toegang tot de BRP en heeft de gegevens zelf opgezocht. Samen met de FG van de GGD heb ik de klacht beantwoordt en de inwoner geïnformeerd.

- De andere klacht had betrekking op het vragen van persoonsgegevens bij het doen van een telefonische melding. De melding had betrekking op een probleem in de openbare ruimte. Deze inwoner had gelijk, voor het doen van een dergelijke melding zijn geen persoonsgegevens nodig.

Thema onderzoeken

- Arbodienstverlener

Met ingang van 1 januari 2024 heeft de gemeente een nieuwe Arbodienstverlener. Ik heb eind 2023 geadviseerd om minder persoonsgegevens met hen te delen. Bovendien heb ik geadviseerd om medewerkers te informeren over de verstrekte persoonsgegevens. In 2024 heb ik onderzocht of dit advies is overgenomen. Ik heb vastgesteld dat dit niet het geval is.

- Huis voor de stad

In 2024 is de gemeente verhuisd naar het Huis voor de Stad. Het open karakter van het gebouw, brengt extra privacyrisico's met zich mee. Eind 2024 ben ik gestart met een onderzoek naar de naleving van de AVG en de gemeentelijke beleidsregels, dit onderzoek is nog niet afgerond.

Bewaken

4. Borging Gegevensbescherming

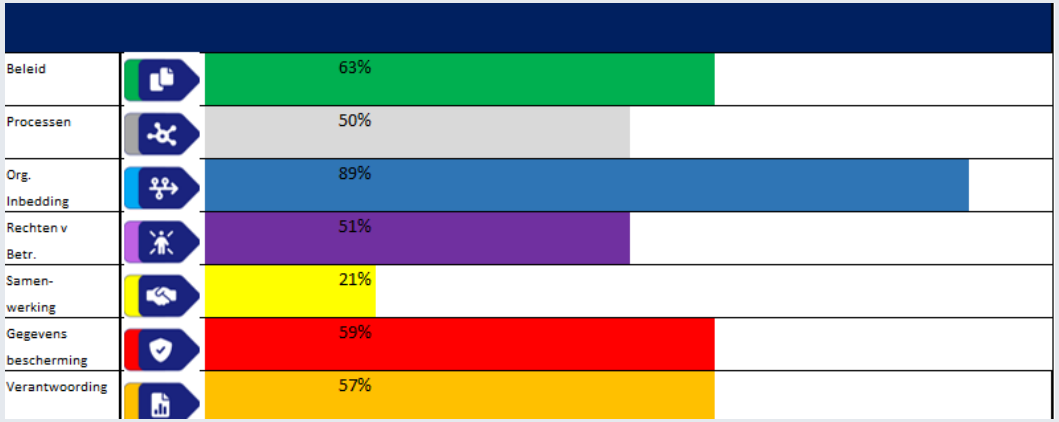
Jaarlijks meet ik in hoeverre de gemeente de naleving van de privacywetgeving heeft geborgd binnen haar processen. Dat doe ik door te toetsen in hoeverre de gemeente voldoet aan een baseline.

Wet politiegegevens (Wpg)

- De buitengewone opsporingsambtenaren bij Veiligheid en Naleving en de leerplichtambtenaren, verwerken (ook) politiegegevens. Op deze verwerking is de Wpg van toepassing. Norea heeft een normenkader opgesteld, waarmee gemeten kan worden in hoeverre de gemeente voldoet aan de Wet politiegegevens. Jaarlijks toets ik de stand van zaken aan de hand van dit normenkader en de uitgevoerde audits. Op blz 21 vindt u mijn bevindingen.

Algemene verordening gegevensbescherming (AVG)

- De Informatiebeveiligingsdienst (IBD) heeft een toetsingskader opgesteld. Met dit kader wil de IBD een eenduidige baseline geven voor wat gemeenten moeten doen om aan de AVG te voldoen. Jaarlijks toets ik aan de hand van deze baseline in hoeverre de organisatie doorlopend in staat is om de naleving van de AVG te waarborgen. De baseline is vastgelegd in het "Borgingsproduct AVG". Eind 2024 heb ik opnieuw deze meting uitgevoerd. Voor de eerste keer was dat aan de hand van het borgingsproduct 3.0[1]. Het borgingsprodcuct bestaat uit zeven thema's . In de grafiek hiernaast ziet u de score per thema. Hierna vindt u eerst het volwassenheidsniveau van de organisatie en daarna een toelichting per thema.

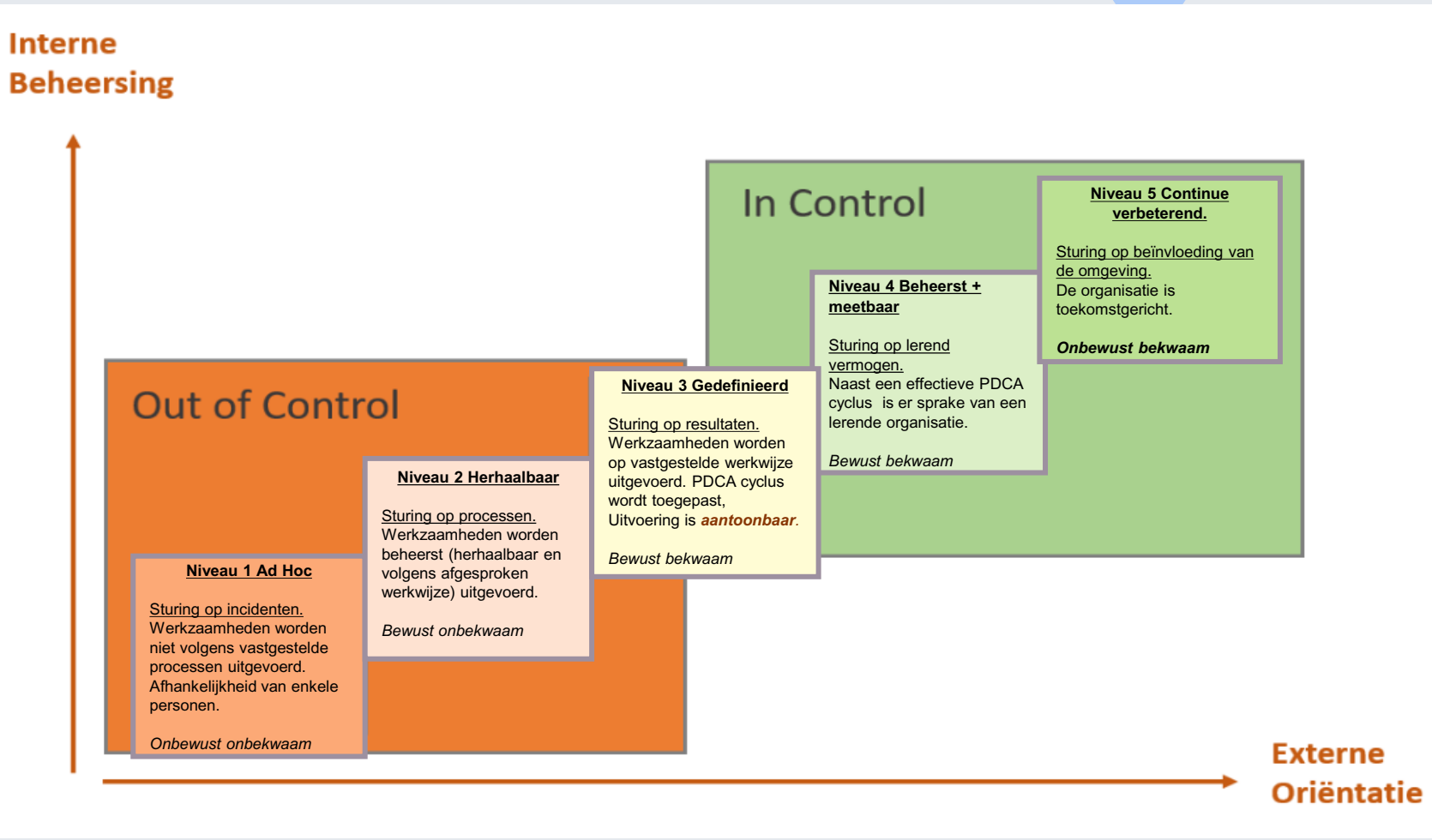


[1] T/m 2023 heb ik het Borgingsproduct 2.0 gebruikt.

Volwassenheid

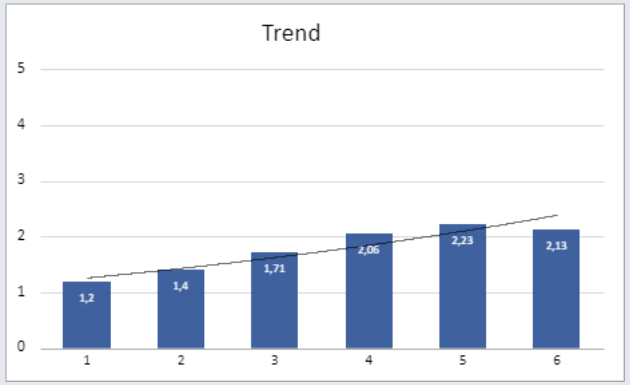
Een volwassen organisatie is in staat om aan te tonen dat er zorgvuldig om wordt gegaan met de gegevens van onze inwoners. Daarvoor heeft de organisatie inzicht nodig en moet ze in staat zijn om risico's en onzekerheden te beheersen. De organisatie voert de juiste discussies, op het juiste niveau, zodat (indien nodig) bijgestuurd kan worden om zo de doelstellingen te realiseren. Een volwassen organisatie is in control. Volwassenheid op het gebied va privacy is een onderdeel voor groei naar een in control statement (ICS)

- De organisatie heeft als doelstelling om te groeien naar een "In control Statement"(ICS) Met een ICS verklaren bestuur en management dat de interne beheersings- en controlesystemen van een gemeente adequaat en efficiënt zijn. Het in control zijn op het gebied van privacy is een van de relevante onderdelen.
- De AVG kent een aantoonplicht. Dit betekent dat de gemeente moet kunnen aantonen welke persoonsgegevens ze waarvoor gebruikt. Daarnaast moet ze kunnen aantonen dat zij passende maatregelen heeft genomen om deze gegevens te beschermen.
- De gemeente heeft de ambitie om z.s.m. te groeien naar een volwassenheid van 3 voor de thema's privacy en informatiebeveiliging.
- Pas bij een volwassenheid van 3 is de organisatie in Control (op het gebied van privacy) en kan zij voldoen aan de aantoonplicht.
- De groei in volwassenheid voor de thema's privacy en informatiebeveiliging kan niet los worden gezien van andere ontwikkelingen om de organisatie meer in control te brengen.



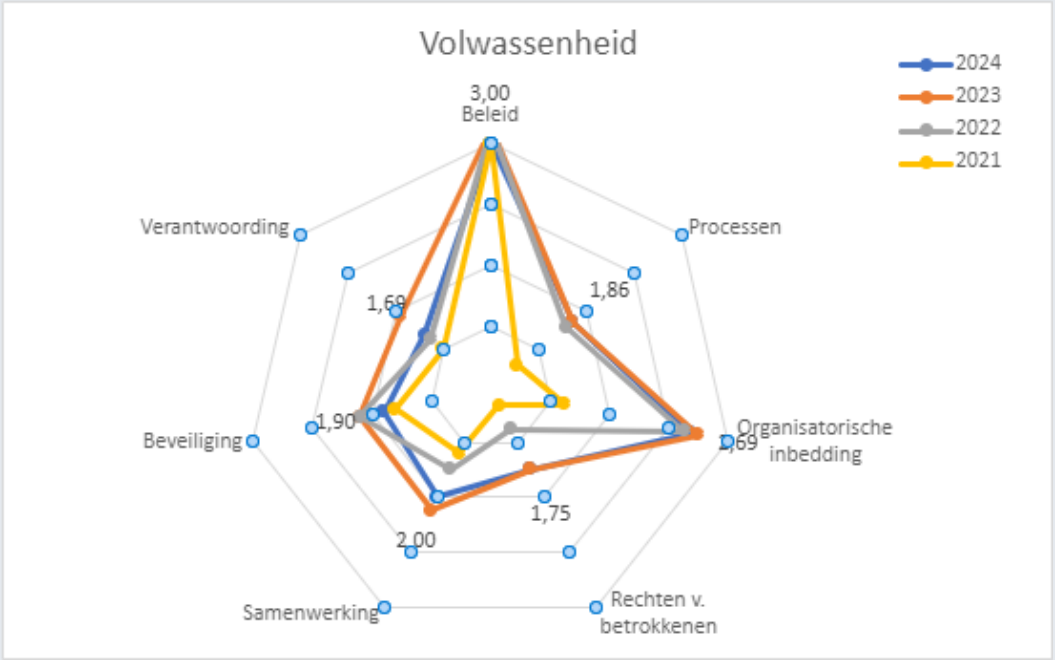
Noot: De gepresenteerde grafiek is qua gedachtegoed gelijk aan de gepresenteerde visie om toe te groeien naar een in control statement (ICS). Datum college 19 maart 2024

Volwassenheid



Het volwassenheidsniveau op het gebied van privacy van de gemeente is 2,1 (2,2 in 2023) op een schaal van 5. Het volwassenheidsniveau informatiebeveiliging is 1,9 (2,2 in 2023). Voor het eerst sinds 2019 heeft de gemeente Helmond geen groei laten zien. De volwassenheid is zelfs licht gedaald.

- De organisatie is onvoldoende in staat om haar risico's op de gegevensbescherming te beheersen omdat zij geen volledig overzicht heeft van de informatie en de ondersteunende applicaties die zij in huis heeft. Er is meer inzicht en grip nodig.
- Om te komen tot een significante verbetering is er daarnaast meer eigenaarschap en sturing nodig. Om hierin stappen te kunnen zetten is het in ieder geval noodzakelijk dat in 2025:
  - de PDCA cyclus verder wordt ontwikkeld;
  - Informatiebeveiliging en privacy worden opgenomen in de jaarplannen;
  - het verantwoordingstraject wordt vereenvoudigd en
  - er een strategisch IB en P overleg wordt ingericht.
- De FG constateert dat de organisatie zich op deze punten niet heeft verbeterd ten opzichte van vorig jaar. Verwachtingen zijn niet waargemaakt, waardoor de volwassenheid van de organisatie is gedaald.



Noot: De laagste score bepaalt de volwassenheid van de organisatie. Om inzicht te geven in de groei is hier niet van uitgegaan, maar is er uitgegaan van de gemiddelde score per thema.

Beleid

Volwassenheid	Groei	Toetsingskader
Gedefinieerd	**Achteruitgang**	**AVG 3.0**
●●●○○	↘	**63%**

Het privacybeleid beschrijft hoe de organisatie invulling geeft aan de veilige verwerking van persoonsgegevens.

- *Beleid vaststellen*
  - Het organisatiebrede geldende beleid, procedures en besluiten zijn moeilijk vindbaar. Het ontbreekt de organisatie aan overzicht. Dit is een algemeen beeld en heeft niet specifiek betrekking op privacybeleid.
- *Privacybeleid*
  - Op het onderdeel privacybeleid scoort de organisatie goed.
  - Op 10 november 2020 is het privacybeleid 2020-2024 vastgesteld. Dit beleid is compleet en er is samenhang met het informatiebeveiligingsbeleid. Beleidsdocumenten over andere onderwerpen zijn niet altijd in lijn met het privacybeleid.
  - De organisatie heeft geen domeinspecifieke uitwerkingen van het privacybeleid.
  - Het organisatiebrede geldende beleid, procedures en besluiten zijn moeilijk vindbaar. Het ontbreekt de organisatie aan overzicht. Dit is een algemeen beeld en heeft niet specifiek betrekking op privacybeleid.
- *Verantwoordelijkheden.*
  - Het management is verantwoordelijk voor de veilige verwerking van persoonsgegevens. Dit is vastgelegd in het beleid en het management en zegt het belang van de bescherming van persoonsgegevens in te zien. Er zijn echter niet daadwerkelijk stappen gezet om hier uitvoering aan te geven. Er is sprake van achteruitgang in de groei omdat de verwachtingen niet zijn waargemaakt.

Processen

Volwassenheid	Stilstand	Toetsingskader
Herhaalbaar		**AVG 3.0**
●●○○○	...	**50%**

Om haar inwoners en medewerkers goed van dienst te kunnen zijn worden binnen de processen persoonsgegevens gebruikt. Om dit zorgvuldig te kunnen doen is inzicht nodig in de processen. Daarnaast is inzicht nodig in de persoonsgegevens, die in deze processen worden gebruikt en bewaard. Door de bij de risico's passende maatregelen te treffen en dit vast te leggen kan de gemeente aan haar inwoners en medewerkers laten zien dat zij betrouwbaar is en verantwoord met hun gegevens om gaat.

- *Verantwoordelijkheden*
  - Verantwoordelijkheden zijn goed vastgelegd in het privacybeleid.
  - Het management kan beroep doen op een centraal privacy team maar heeft moeite met het vrijmaken van capaciteit binnen de eigen afdeling.
  - Privacy is bij enkele afdelingen onderwerp van hun jaarplan.
- *Werkprocessen*
  - Er is procesbeleid en een procesverbeterteam.
  - Er is een kernregistratie processen vastgesteld. Deze kernregistratie is nog niet actueel en volledig. De organisatie heeft daardoor nog geen volledig inzicht in al haar werkprocessen en de verantwoordelijke proceseigenaren.
  - Werkprocessen worden conform het procesbeleid gemodelleerd en geoptimaliseerd. Ze worden eenduidig vastgelegd in de gemeentelijke processen registratie. De registratie is echter niet in lijn met de kernregistratie: "i-navigator". De herkenbaarheid kan dan ook beter.
- *Verwerkingsregister*
  - Het verwerkingsregister voldoet in opzet aan de wettelijke vereisten.
  - Het verwerkingsregister is niet volledig en actueel.
  - De verantwoordelijkheden voor het bijhouden van het verwerkingsregister zijn belegd. Procedures zijn opgesteld maar niet vastgesteld.
- *Bewaren en vernietigen*
  - De Archiefwet is van toepassing. Om de naleving van de Archiefwet te borgen, heeft de gemeente beleidsstukken opgesteld. Er vinden jaarlijks interne dan wel externe controles plaats. Uit de externe controle van 2024 blijkt dat de gemeente in grote lijnen voldoet. De gesignaleerde verbeterpunten worden in 2025 opgepakt.
  - De gemeente is gestart met opstellen van een informatiebeheerplan, zodat informatie- en kwaliteitszorg worden ingericht
  - Analoge informatie en informatie in het zaaksysteem wordt volgens gedocumenteerde procedures automatisch vernietigd. Toch is niet vast te stellen dat in alle gevallen aan de wettelijke eisen rondom bewaren en vernietigen wordt voldaan. Dit komt omdat er nog geen afspraken zijn gemaakt over bewaartermijnen in taakspecifieke applicaties. Bovendien worden er ook gegevens op andere plaatsten opgeslagen zoals bijvoorbeeld in mailboxen.
- *Risico analyses*
  - In beleid en procedures is vastgelegd wanneer een risico analyse dient te worden uitgevoerd. Er zijn procedures en werksinstructies vastgesteld.
  - De organisatie kan een beroep doen op het SPO team voor ondersteuning bij het uitvoeren van een risico analyses.
  - De uitgevoerde risicoanalyses en het uitgebrachte advies van FG en CISO worden gedocumenteerd in het zaaksysteem. Geïdentificeerde risico's en te implementeren maatregelen worden niet op een centrale plaats opgeslagen
  - Extra aandacht behoeft het documenteren van de bewuste keuze om (deels) af te wijken van het ontvangen advies.
  - Er is niet vastgelegd wie beslissingsbevoegd is ten aanzien van de afwijking van een het advies van de FG en CISO.

Organisatorische inbedding

Volwassenheid	Groei	Toetsingskader
Gedefinieerd	**Achteruitgang**	**AVG 3.0**
●●●○○	↘	**89%**

Om daadwerkelijk invulling te geven aan de bescherming van privacy, moeten de taken organisatorisch zijn ingebed. Dit wordt bereikt met een goede taakverdeling en voldoende middelen. Het is daarbij belangrijk dat ook de ondernemingsraad in staat wordt gesteld haar bevoegdheden met betrekking tot de privacy van de medewerkers uit te oefenen.

❖ *Functionaris gegevensbescherming*

- Ik ben benoemd als de FG voor de AVG en de Wpg. Ik heb hiervoor de benodigde bevoegdheden en deskundigheid.
- Ik heb een onafhankelijke rol, die is gewaarborgd door middel van een rechtstreekse lijn met de Gemeentesecretraris. Ik ben gepostioneerd in de unit Concern Control, maar wordt niet inhoudelijk aangestuurd door de Concern Controller.
- Rol, taken en bevoegdheden zijn vastgelegd in het privacybeleid en de conctactgegevens van de FG zijn in- en extern bekendgemaakt.
- De organisatie kan de positie van de FG verder verbeteren door afwijkingen van haar advies gemotiveerd vast te leggen.

❖ *Privacy team*

- Er is een centraal team van Security en privacy officers. Dit team werkt voor het management en helpt hen bij het uitvoeren van taken en het implementeren van maatregelen om persoonsgegevens te beschermen. De afdelingen beschikken nog niet over een vast contactpersoon binnen dit team (businesspartnerrol).
- Naast het centrale team is er ook capaciteit binnen de afdeling nodig, maar dit is niet altijd goed georganiseerd. Vaak wordt er in projecten of afdelings- en teamplannen geen capaciteit gereserveerd voor informatiebeveiliging en privacy. Daarnaast heeft de afdeling niet altijd een vaste contactpersoon (DSPO). Hun inzet is echter cruciaal, omdat zij de kennis hebben over de processen, producten en applicaties van de afdeling.
- Er is (nog) geen rol beschreven voor een privacy-officer die verantwoordelijk is voor de privacystrategie.
- De PDCA cyclus is niet ingericht. Ik heb niet kunnen vaststellen dat informatiebeveiliging en privacy zijn opgenomen in alle jaarplannen. Er kan daarnaast worden vastgesteld dat er geen opvolging is gegeven aan het directiebesluit met betrekking tot de uitvoering van (een aantal geprioriteerde) verbeteracties. Er is sprake van achteruitgang in de groei omdat de verwachtingen niet zijn waargemaakt.

❖ *Ondernemingsraad (OR)*

- De OR wordt om instemming gevraagd. Een overzicht van alle interne regelingen ontbreekt, waardoor het moeilijk is om vast te stellen of de OR, in voorkomende gevallen, altijd om instemming is gevraagd.
- De OR wordt in de meeste gevallen actief geïnformeerd over privacy en gegevensbescherming van het personeel.

❖ *Bewustwording*

- De gemeente heeft een bewustwordingsplan 2024-2027, dit plan beschrijft op welke wijze medewerker doorlopend bewust worden gemaakt van de risico's en randvoorwaarden bij de omgang met persoonsgegevens.
- Nieuwe medewerker volgen heen onboardingsprogramma.
- Jaarlijks wordt er een bewustwordingsprogramma vastgesteld. De effectiviteit van het programma wordt gemeten en het programma wordt aangepast aan de hand van deze meting. De organisatie wordt bij de uitvoering van het programma ondersteunt door een externe partij.

Rechten van betrokkenen

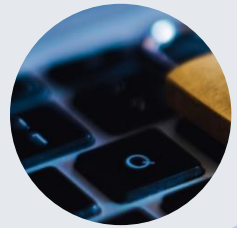
Volwassenheid
Herhaalbaar

Groei
Stilstand

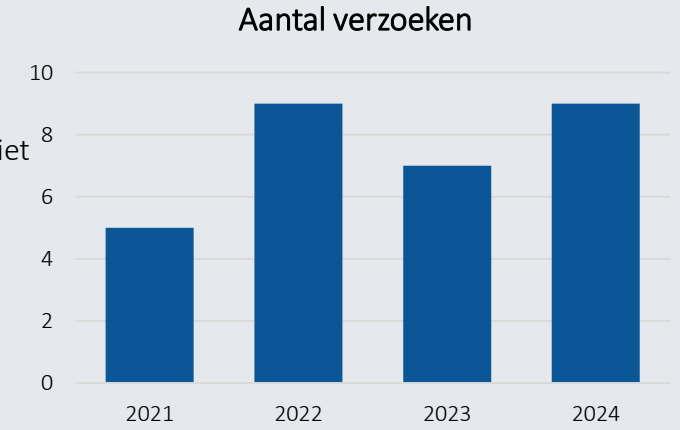
Toetsingskader
AVG 3.0

51%

Inwoners en andere betrokkenen hebben het recht op informatie en inzage. Zo kunnen ze controleren of er op een juiste wijze wordt omgegaan met hun gegevens. Ze hebben het recht om aanpassing van de gegevens te vragen of een klacht in te dienen bij de FG. Ook hebben ze het recht op menselijke tussenkomst, bij geautomatiseerde besluiten.



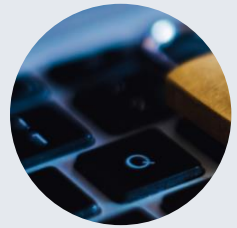
- *Recht op informatie*
- Betrokkenen worden via de privacyverklaring op de website geïnformeerd over hoe de gemeente Helmond omgaat met hun persoonsgegevens. Deze privacyverklaring voldoet aan de transparantieverplichting.
- Naast deze algemene privacy verklaring zijn er weinig (domein) specifieke documenten. Een privacyverklaring voor medewerkers ontbreekt.
- Er is een wildgroei aan websites en apps waarin de gemeente Helmond participeert. Het inzicht in het gebruik van cookies of andere persoonsgegevens op deze websites en de verantwoordelijkheid voor deze verwerkingen is onvolledig.
- Het is niet bekend of verwerkingen van persoonsgegevens die zijn gebaseerd op toestemming voldoen aan de wet. Dit is niet bekend vanwege het gebrek van inzicht in de verwerking van persoonsgegevens op de websites en apps.
- De wel bij mij bekende en onderzochte websites en apps bevatten niet allemaal informatie over de verwerking van persoonsgegevens.
- *Rechten van betrokkenen*
- Er zijn processen en procedures opgesteld om uitvoering te geven aan de rechten van betrokkenen. Ook zijn er standaarddocumenten beschikbaar.
- Deze documenten zijn goed toegankelijk voor het privacy-team. Verzoeken komen echter ook op andere plekken in de organisatie binnen. Hierdoor is er nog geen sprake van een volledig uniforme benadering.
- *Geautomatiseerde besluitvorming*
- Digitalisering neemt toe en daarmee ook de hoeveelheid data. Het is de ambitie van de gemeente Helmond om de data(stromen) te gebruiken om enerzijds te komen tot nieuwe inzichten en opgaven uit de stad en anderzijds slimme (geautomatiseerde) beslissingen te nemen. De gemeente heeft echter geen maatregelen getroffen die passen bij deze ambitie.
- De gemeente Helmond heeft namelijk geen register waarin wordt bijgehouden in welke informatiesystemen geautomatiseerde individuele besluitvorming wordt toegepast.
- Bij geautomatiseerde besluitvorming worden vaak algoritmes gebruikt, de gemeente Helmond heeft ook het landelijke algoritmeregister nog niet gevuld en heeft de verantwoordelijkheid voor het vullen van dit register niet georganiseerd.
- De gemeente heeft de uitvoering van de AI-act nog niet belegd.
- De gemeente heeft wel een ethisch waardenkader vastgesteld, in dit waardenkader is Algoritmegedreven besluitvorming opgenomen



Samenwerking

Volwassenheid	Groei	Toetsingskader
Gedefinieerd	**Achteruitgang**	**AVG 3.0**
●●○○○	↘	**21%**

Met haar partners deelt de gemeente Helmond gegevens. Betrokkenen moeten er op kunnen vertrouwen dat dit zorgvuldig en veilig gebeurt. Eenmalige verstrekkingen moeten daarom worden getoetst en bij meer structurele verstrekkingen moeten er goede afspraken gemaakt worden. Voor het maken van deze afspraken is het belangrijk om te weten welke rol een partner inneemt.



- *Rollen van partners*
  - Bij aanbestedingen door de afdeling inkoop, wordt er standaard uitvraag gedaan naar de rol die de partner heeft. Dit geldt niet voor aanbestedingen onder de drempel. In dat geval zijn afdelingen gerechtigd om zelfstandig producten aan te schaffen. n dat geval mogen afdelingen zelfstandig producten aanschaffen, waardoor het niet gegarandeerd is dat de gemeentelijke inkoopvoorwaarden worden gevolgd.
  - Er zijn een aantal standaardovereenkomsten beschikbaar, op afdelingsniveau is echter niet altijd inzichtelijk welke afspraken er moeten worden gemaakt en of deze afspraken passen bij de rol die een partij inneemt. Als gevolg hiervan gebeurt het dat contracten niet voldoen aan de eisen van de gemeente Helmond of de AVG.
  - Ook bij het aangaan van samenwerkingsverbanden wordt niet altijd uitvraag gedaan naar de rol van de partner en worden afspraken rondom informatiebeveiliging en privacy niet goed vastgelegd.
  - Er wordt niet of nauwelijks gecontroleerd of persoonsgegevens worden verwerkt buiten Europa en of er in dat geval wordt voldaan aan de wettelijke vereisten voor internationale doorgifte. (denk bv bij de keuze voor een internationale organisatie met een moederbedrijf in de VS)
  - Controle op naleving vindt slechts gedeeltelijk plaats. De FG heeft de indruk dat controle op naleving van de afspraken, en borging van naleving van de afspraken door de gemeente zelf, onvoldoende aandacht krijgt.
- *Gegevensverstrekking*
  - De organisatie heeft in 2023 een proces incidentele gegevensverstrekkingen opgesteld.
  - Binnen dit proces is geborgd dat interne incidentele leveringen via de gegevensmakelaar worden getoetst aan de privacyregels en dat afspraken worden vastgelegd. Leveringen rechtstreeks uit een applicatie kunnen echter nog worden gemist.
  - Structurele en incidentele externe gegevensleveringen zijn buiten scope.
  - Structurele interne gegevensleveringen zijn deels in beeld. Afspraken rondom deze leveringen worden nog niet vastgelegd.
  - De gemeente heeft een data-architectuur vastgesteld, daarmee heeft zij ook de wijze waarop Helmond met koppelingen en gegevensuitwisselingen tussen applicaties omgaat vastgesteld.
  - In 2023 heeft het project gegevensmanagement diverse verbeterpunten opgepakt. Het project is in 2024 opgeleverd. De governance voor gegevensmanagement/datamanagement is nog niet ingericht.

Gegevensbescherming

Volwassenheid
Gedefinieerd

Groei
Achteruitgang

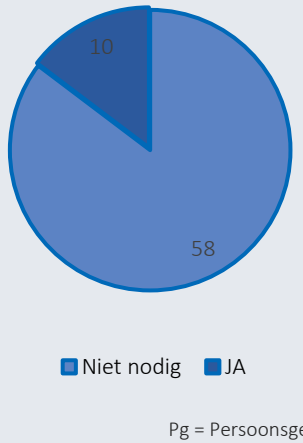
Toetsingskader
AVG 3.0

59%

De inwoner en medewerker moeten er op kunnen vertrouwen dat hun persoonsgegevens passend zijn beveiligd, zodat hun gegevens niet kunnen worden misbruikt. Dit betekent ook dat de inwoner en de medewerker kunnen rekenen op goede dienstverlening, omdat de juiste persoonsgegevens op het juiste moment voor de juiste mensen beschikbaar zijn

- *Gegevensbescherming door ontwerp en standaardinstellingen*
  - De organisatie is bezig met de ontwikkeling van een enterprise architectuur. In 2023 zijn richtinggevende principes opgesteld. Deze principes zijn richtinggevend bij alle veranderingen binnen de organisatie die impact hebben op de organisatie en de informatievoorziening.
  - De enterprise architectuur moet in de loop van 2025 vertaald worden in een domein architectuur informatiebeveiliging en privacy. Op dat moment ontstaan er gedocumenteerde eisen om privacy risico's in de ontwerpfase voor processen en systemen mee te nemen. Bovendien is dit richtinggevend voor de inrichting van de organisatie en informatievoorziening van alle organisatiedomeinen.
- *Informatiebeveiliging*
  - De gemeente legt via ENSIA verantwoording af. Uit deze verantwoording blijkt dat het volwassenheidsniveau van informatiebeveiliging van de gemeente Helmond is gedaald van 2,2 naar 1,9 op een schaal van 5. Dit niveau houdt in dat het afhankelijk is van de deskundigheid en inzet van individuele personen of de gegevens van onze inwoners en medewerkers passend zijn beveiligd.
  - Proceseigenaren geven onvoldoende uitvoering geven aan hun verantwoordelijkheid om een toereikend stelsel van maatregelen te implementeren voor de systemen, applicaties en processen waarvoor zij verantwoordelijk zijn.
- *Privacy incidenten en datalekken*
  - Er zijn standaardprocedures en rapportages
  - Er is een apart proces voor het melden van (potentiële datalekken en/of security incidenten ingericht in een meldloket (Topdesk).
  - zijn
  - Er zijn in 2024 83 incidenten gemeld. Uiteindelijk bleek er in 68 gevallen sprake te zijn van een datalek.
  - Incidenten kunnen leiden tot een verstoring van de bedrijfsvoering. Het is daarom van belang dat er Bedrijfscontinuïteitsmanagement (BCM) is in ingericht. Hier is in 2023 mee gestart. In 2024 is dit niet echt van de grond gekomen.

Aantal datalekken gemeld bij de AP



Pg = Persoonsgegevens

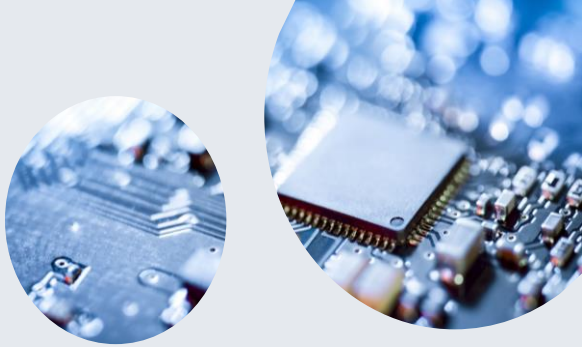
Verantwoording

Volwassenheid	Groei	Toetsingskader
Herhaalbaar	**Achteruitgang**	**AVG 3.0**
●●○○○	↘	**60%**

Met het inrichten van een PDCA cyclus op het thema privacy, is de organisatie in staat om de naleving van de privacywetgeving te beoordelen en daar waar nodig te verbeteren.

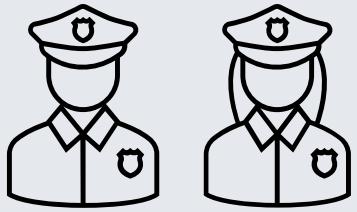
- *Evaluatie naleving AVG*
- Het management heeft de verantwoordelijkheid voor de gegevensbescherming bij de uitvoering van de processen waarvoor zij eigenaar is. Daarom is het van belang dat het management zich zelf een beeld vormt van de mate waarin de privacywetgeving wordt nageleefd. Daarmee toont men eigenaarschap. Deze evaluaties vinden echter niet plaats
- Ik heb als FG een toezichtplan. In deze rapportage is te lezen op welke wijze ik in 2024 de organisatie heb gecontroleerd op de naleving van de AVG en de Wpg.
- De PDCA cyclus is niet ingericht. Ik heb niet kunnen vaststellen dat informatiebeveiliging en privacy zijn opgenomen in alle jaarplannen. Er kan daarnaast worden vastgesteld dat er geen opvolging is gegeven aan het directiebesluit met betrekking tot de uitvoering van (een aantal geprioriteerde) verbeteracties.
- *Evaluatie naleving informatiebeveiliging*
- De uitvoering van het informatiebeveiligingsbeleid wordt jaarlijks geëvalueerd middels Ensia.
- Hierover wordt gerapporteerd door de Ciso in de rapportage digitale weerbaarheid.
- Door het gebruikte Excel-raamwerk te vervangen door (GRC/ISMS)-tooling wordt de verantwoording gemakkelijker, inzichtelijker en beter beheersbaar.

WPG voor Boa's



Sinds begin 2019 is de Wet politiegegevens (Wpg) ook van kracht voor bijzonder opsporingsambtenaren (Boa's). Bij de afdeling Veiligheid & Naleving (openbare orde) en bij het Sociaal Domein (leerplicht) werken Boa's. Om aan te tonen dat de gemeente Helmond compliant is aan de Wpg moet jaarlijks een interne audit en eens in de vier jaar, een externe audit worden uitgevoerd.

- *De audits*
  - In 2022 is een externe audit uitgevoerd. De gemeente voldeed toen niet aan haar verplichtingen. De beide afdelingen hebben een verbeterplan opgesteld.
  - In 2023 is een hercontrole uitgevoerd door een externe auditor. Deze rapportage is begin 2024 aangeboden aan het college.
  - De gemeente heeft in 2024 een interne audit uitgevoerd. Deze is nog niet afgerond.
- *Onderzoek door de FG*
  - De organisatie heeft instructies en protocollen opgesteld om te borgen dat de Wpg wordt nageleefd.
  - Er kan niet worden aangetoond dat gedurende heel 2024 ook volgens deze instructies en protocollen is gewerkt. Daarvoor is het nodig dat hier ook gedurende het jaar op wordt gemonitord door de afdeling.
  - Veiligheid en Naleving is eind 2024 gestart met monitoring.
  - Bij het Sociaal Domein was de uitvoering van de verbetermaatregelen, monitoring en het afleggen van verantwoording (in 2024) niet belegd bij een (vaste) medewerker.
  - Er zijn geen incidenten geweest en ook zijn er geen betrokkenen die gebruik hebben gemaakt van hun rechten.
  - De organisatiebrede regels voor het uitvoeren van een riscioanalyse gelden ook voor de verwerkingen van politiegegevens. Er zijn in 2024 geen risico analyses uitgevoerd terwijl ik wel risico's zie:
    - Risico's hangen niet alleen samen met de gebruikte applicaties maar ook met de onderliggende processen. Op processen zijn nog geen risico analyses uitgevoerd.
    - De ingewikkelde constructie die de gemeente heeft ingericht voor de uitvoering van de leerplichtwet brengt extra risico's met zich mee. De gemeente heeft namelijk de uitvoering van de leerplicht gedelegeerd aan de GGD, waarna de GGD de taken weer heeft gemandateerd aan de leerplichtambtenaren in dienst van de gemeente Helmond.



Vooruitblik

❖ *De wet- en regelgeving op het gebied van digitalisering ontwikkelt zich enorm. Ook dit jaar zullen nieuwe Europese wetten van toepassing worden die relevant zijn voor de gemeente. In de Digiflyer 2025 van Kenniscentrum Europa Decentraal is een selectie gemaakt van de Europese wetgeving die impact kan hebben.*

- Interoperabiliteit gaat over de mogelijkheden om onderling via netwerken en informatiesystemen gegevens uit te wisselen
- De toegankelijkheidsrichtlijn heeft als doel om diensten en producten toegankelijk te maken voor mensen met een beperking.
- De dataverordening regelt de toegang tot dat.a
- Om te zorgen dat AI op een verantwoorde manier wordt uitgerold is de AI verordening (de AI act) opgesteld.

❖ *De gemeente is voor haar digitale infra-structuur voor een groot deel afhankelijk van Amerikaanse techgiganten zoals Microsoft. Deze afhankelijkheid is een veiligheidsrisico nu de VS niet langer de zekere bondgenoot is die ze ooit waren.*

Vooruitblik

Ik zie een aantal ontwikkelingen met extra risico's voor betrokkenen. In 2025 zal ik daarom extra aandacht besteden aan onderstaande onderwerpen. Dit wordt verder uitgewerkt in mijn toezichtplan.

- *Huis voor de Stad*
  - In 2024 heeft de verhuizing naar het Huis voor de Stad plaatsgevonden. Het Huis voor de Stad heeft een open karakter, dit heeft effect op de beveiliging van onze infrastructuur en informatie. Het open karakter, de flexibele werkplekken en het hybride werken vergroten de kans op meeluisteren of meekijken. Ik ben daarom in 2025 gestart met een onderzoek dat ik zal afronden in 2025. Ik onderzoek of de gemeente haar eigen beleid goed toepast en of er voldoende maatregelen zijn getroffen om meeluisteren of meekijken te voorkomen.
- *Preventie met gezag.*
  - Preventie met Gezag (PvG) is onderdeel van het meerjarenprogramma Jeugd en is gericht op het voorkomen van jeugdcriminaliteit en het bieden van perspectief aan risicojongeren. Om uitvoering aan dit programma te kunnen geven worden er persoonsgegevens verwerkt met hoge privacy risico's voor betrokkenen. De organisatie start in 2025 met de uitvoering, terwijl zij nog niet weet welke wat er nodig is om de privacy risico's voor betrokkenen te verminderen. Dit betekent dat de doelgroep onbedoeld nadelige gevolgen kan ondervinden.
- *Kunstmatige intelligentie (AI)*
  - AI kan worden ingezet om efficiënter te werken, kosten te besparen of tijdrovende taken te automatiseren. Om op een verantwoorde wijze gebruik te maken van AI is het o.a. van belang dat AI-systemen eerlijk transparant en betrouwbaar zijn. Dit betekent dat er ondermeer rekening gehouden moet worden met veiligheid en privacy. Daarnaast dient AI menselijke waarden te respecteren, en maatschappelijke impact te overwegen. De organisatie heeft nog geen AI-governance ingericht terwijl er wel een groeiende behoefte bestaat om AI in te zetten. De toegankelijkheid en het eenvoudige gebruik brengen het risico met zich mee dat AI tools worden gebruikt zonder dat de vraag wordt gesteld of dit verantwoord kan.

Adviezen

Overzicht krijgen

Een volwassen organisatie heeft grip op de risico's die zij loopt. Bovendien kan zij aantonen dat zij voldoet aan de BIO en de privacywetgeving. Hiervoor is het noodzakelijk dat de organisatie overzicht en inzicht krijgt in haar informatie en de ondersteunende applicatie. De FG en CISO adviseren daarom om prioriteit te geven aan het verkrijgen van overzicht. Wat hebben we in huis en waar lopen we risico's.

Advies	Prio	Responsible	Supporting
Actualiseer de kernregistratie processen.	1	Alle Afdelingsmanagers (proceseigenaar)	Procesadviseurs
Actualiseer het register van verwerkingen.	2	Alle Afdelingsmanagers (proceseigenaar)	SPO team
Actualiseer de CMDB.	3	Alle Afdelingsmanagers (proceseigenaar)	FB AB
Kies (organisatiebreed) 10 processen.	3	Alle Afdelingsmanagers (proceseigenaar)	SPO team en CC
Beschrijf en verbeter 10 bestaande processen en voer hier een risico analyse op uit.	4	De desbetreffende Afdelingsmanager (proceseigenaar)	SPO team en CC

Adviezen

Sturing

Om te kunnen groeien in volwassenheid is het nodig dat adviezen en (verbeter)acties uit beleid en verantwoordingstrajecten daadwerkelijk worden opgepakt en uitgevoerd. Hiervoor is het noodzakelijk dat het management meer eigenaarschap toont en dat er daadwerkelijk wordt gestuurd op de thema's informatiebeveiliging en privacy. De FG en Ciso adivseren om dit mee te nemen in het Management ontwikkelprogramma.

Advies	Prio	Responsible	Supporting
Inbedding van privacy en informatiebeveiliging in de PDCA cyclus.	2	Alle directieleden, afdelingsmanagers en teamleiders	Financiën
IB en P onderdeel van de jaarplannen en sturing op uitvoering.	1	Alle directieleden, afdelingsmanagers en teamleiders	Bestuur en Organisatie
Vereenvoudiging van het verantwoordingstraject.	1	Teamleider Regie	Coördinator verantwoording BIO, Wpg en AVG en CC
Invoering businesspartner rol SPO team.	1	Teamleider Regie en alle afdelingshoofden	
Informatiebeveiliging en privacy vast onderdeel van het goede gesprek.	3	Alle directieleden, afdelingsmanagers en teamleiders	Teamleider Mens en Organsiatie
Inrichting strategisch overleg IB en P.	4	FG en Ciso	SPO team
Verbetering positie FG en Ciso, opstellen reglement.	4	FG en Ciso	

Adviezen

Beleid en regelgeving

Beleid en regelgeving geven de kaders aan. De FG en Ciso adviseren om aan de volgende beleidsonderwerpen prioriteit te geven. Zij adviseren om het beleid op te stellen, vast te stellen en te implementeren in 2025.

Advies	Prio	Responsible	Supporting
Informatiebeleid.	1	Cio office	Beleidsmederwerker
Strategisch informatiebeveiliging- en privacybeleid.	1	Ciso en IVA	SPO team
Business continuïteit implementeren.	2	Alle Afdelingsmanagers (proceseigenaar)	BCM
IDU en rolgebaseerde autorisaties implementeren.	2	Programma manager altijd verbonden	
Logging en monitoring implementeren.	4	Programma manager altijd verbonden	
AI en Algoritmebeleid.	4	Cio office	Beleidsmedewerker

Adviezen

SPO team als businesspartner

Het SPO team helpt de organisatie bij het borgen van informatiebeveiliging en privacy. Zij spelen dus een belangrijke rol bij het realiseren van de gestelde doelen. De FG en Ciso hebben daarom een advies over de wijze waarop de businesspartnerrol wordt ingevuld en de wijze waarop het SPO team het verantwoordingstraject inricht.

Implementeren businesspartner rol
Leg vast dat periodiek (minstens 4x per jaar) een gesprek plaatsvindt met afdelingsmanager en DSPO.

Bespreek in de periodieke gesprekken met de afdelingsmanagers in ieder geval:
1. De stand van zaken met betrekking tot:
    1. Informatie en beveiliging van de afdeling en de in de teamplannen opgenomen werkzaamheden.
    2. De actualiteit van het register van verwerkingen.
    3. De uitgevoerde en uit te voeren risico analyses.
    4. Of de afdeling iemand heeft die zorgt voor dossieropbouw gedurende het jaar. (zie punt 3 bij verantwoording).
    5. Of er daadwerkelijk regelmatig vastlegging plaatsvindt (zie punt 3 bij verantwoording).
2. De aankomende ontwikkelingen binnen het betreffende domein.
3. De gevraagde capaciteit van het SPO team.
4. Aanbevelingen van het SPO team ter verbetering.

Adviezen

SPO team en het verantwoordingstraject.

Het SPO team helpt de organisatie bij het borgen van informatiebeveiliging en privacy. Zij spelen dus een belangrijke rol bij het realiseren van de gestelde doelen. De FG en Ciso hebben daarom een advies over de wijze waarop de businesspartnerrol wordt ingevuld en de wijze waarop het SPO team het verantwoordingstraject inricht.

Vereenvoudigen verantwoordingstraject
1. Stel vast dat het SPO team verantwoordelijk is voor de coördinatie van en het brengen van samenhang in de verantwoording van: AVG, WPG, BIO, Ensia, Suwinet, Digid en de basisregistraties.
2. Stel vast dat de Coördinator(en) verantwoordelijk is/zijn voor: a. Het opstellen van standaard vooringevulde Workingpapers met verwijzing naar de normen. b. Het maken van een standaard vooringevuld bewijsdossier. c. Een dossieropzet die een dossieropbouw gedurende het gehele jaar faciliteert.
3. Met betrekking tot punt 2: a. Stel geen extra vragen, maar houd je aan de norm. b. Betrek FG, CISO en IT auditor bij het opstellen van de standaarden. c. Gebruik de over 2024 opgeleverde documenten om de standaarden op te stellen. d. Bekijk welke (generieke) bewijslast workingpapers door een SPO-er kunnen worden gevuld en bijgehouden. e. Zorg dat de medewerkers in de lijn enkel de aanvullingen hoeven te doen die betrekking hebben op bestaan en werking. Medewerkers in de lijn zijn enkel verantwoordelijk voor de workingpapers en bewijslast met betrekking tot de opzet als zij ook verantwoordelijk zijn voor het opstellen van deze stukken.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	1, 3

Afdeling:	Organisatiebreed
Onderwerp:	Thema onderzoek onrechtmatige inzage persoonsgegevens
Datum:	1 mei 2024

Aanleiding

RTL heeft een artikel geschreven over de integriteit van ambtenaren. (Hiervoor zijn ambtenaren in jouw gemeente op de vingers getikt | RTL Nieuws). Het artikel is gebaseerd op (oa) informatie die gemeente Helmond openbaar heeft gemaakt naar aanleiding van een WOO onderzoek van RTL. (zie document: 52009579).

Dit artikel is voor de Autoriteit Persoonsgegevens (AP)aanleiding geweest om een themaonderzoek te doen naar datalekken door onrechtmatige inzage in persoonsgegevens door ambtenaren. De Autoriteit Persoonsgegevens heeft daarom de FG gevraagd om een onderzoek uit te voeren en een aantal vragen te beantwoorden.

Scope

De AP vraagt om van de onderstaande integriteitsschendingen te onderzoeken of er sprake is geweest van ongeoorloofde toegang tot persoonsgegevens:

1. *"Overig: uitlezen systeem."*
2. *"Overig: druk uitgeoefend t.b.v. aanpassingen in systeem."*
3. *"Ongeoorloofde inzage in documenten."*

Onderzoek

1. Overig uitlezen systeem.

Er is sprake van persoonsgegevens.

Bij deze kwestie gaat het om het onbevoegd uitlezen van een (voordeur)camera.

Beschrijving situatie

De gemeentelijke camera's worden uitgelezen bij de Stichting bedrijventerrein Helmond. De voordeurcamera is van de Stichting bedrijventerrein (en niet van de gemeente Helmond) en de betrokken medewerker was niet bevoegd om deze camera uit te lezen.

Er zijn maatregelen getroffen om herhaling te voorkomen.

Wachtwoorden zijn bv aangepast. De betrokken medewerker had nl toegang tot deze camera omdat de wachtwoorden gelijk waren.

Er is sprake van een datalek.

De medewerker had de camera niet mogen gebruiken. De melding is gedaan, omdat uit de loggegevens een ongebruikelijke aanmelding bleek. Enkel gedurende de (beperkte) periode dat de medewerker ingelogd is geweest heeft hij kunnen zien of er iemand voor de voordeur stond ervoor langsliep. Hij keek of zijn collega er al was. Mogelijk zijn er in die periode ook andere bezoekers geweest of mensen langs de voordeur gelopen. Voor zover de medewerker bezoekers of passanten kon identificeren, had hij in dat geval enkel kunnen vaststellen dat betrokkene op dat moment de Stichting bedrijventerrein bezocht of hier langskwam. Het risico voor betrokkene(n) is verwaarloosbaar. Een melding is niet nodig. Het datalek had wel gemeld en geregistreerd moeten

worden. Het datalek is naar aanleiding van dit onderzoek alsnog geregistreerd (in 2024) met de (4 jaar later) nog beschikbare gegevens.

2. Druk uitgeoefend.

Er is geen sprake van persoonsgegevens.

Bij deze kwestie gaat het om het onheus bejegenen van een medewerker.

Beschrijving situatie

In het personeelssysteem zat een bug. Een medewerker heeft de nodige actie ondernomen om deze bug te verhelpen. De wijze waarop hij daarbij door een medewerker werd bejegend, was de reden voor een melding.

3. Ongeoorloofde inzage in documenten

Er is wel sprake van persoonsgegevens.

Bij deze kwestie gaat het om het onbevoegd opzoeken van een eigen verkeersboete.

Beschrijving situatie.

Een medewerker heeft vanuit 5.1.2e functie toegang tot opgelegde verkeersboetes. 5.1.2e heeft zelf een verkeersboete gekregen en deze boete opgezocht in het systeem.

Er zijn maatregelen getroffen om herhaling te voorkomen.

De autorisaties zijn bv aangepast

Er is sprake van een datalek.

De medewerker heeft onbevoegd kennis genomen van 5.1.2e eigen gegevens. De melding is gedaan, omdat uit de loggegevens een ongebruikelijke aanmelding bleek.
Aangezien er sprake is van ongeoorloofde toegang is er wel sprake van een datalek. De medewerker heeft daarbij kennis genomen van (5.1.2e eigen) contactgegevens en financiële gegevens (informatie over de boete). Het risico voor betrokkene is nihil, aangezien het 5.1.2e eigen gegevens betreft. Een melding is niet nodig. Het datalek had wel gemeld en geregistreerd moeten worden. Het datalek is naar aanleiding van dit onderzoek alsnog geregistreerd (in 2024) met de (4 jaar later) nog beschikbare gegevens.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens geanonimiseerd op grond van:

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