

|                         |                                                  |                         |
|-------------------------|--------------------------------------------------|-------------------------|
| Afdeling                | : INF - Privacy                                  | B&W-voorstel:           |
| Naam opsteller voorstel | : Roger Coenen<br>r.coenen@weert.nl, 0495-575581 | DJ-2449417              |
| Portefeuillehouder      | : mr. R.J.H. (Raymond) Vlecken CBM               | Zaaknummer:<br>2449290  |
|                         |                                                  | Publicatie:<br>Openbaar |

**Onderwerp**

Jaarverantwoordingsrapportage FG 2023 terugblik |2024 vooruitblik (AVG/Wpg)

**Voorstel**

1. De jaarverantwoordingsrapportage FG 2023 terugblik |2024 vooruitblik (AVG/Wpg) vast te stellen.

**Inleiding**

Het is de taak van de Functionaris Gegevensbescherming (FG) om toe te zien op de naleving door de gemeente van de wet- en regelgeving op het gebied van gegevensbescherming. De FG brengt jaarlijks verslag uit aan het college, de burgemeester en de gemeenteraad. Voor de duidelijkheid en voor het verkrijgen van een "overall" beeld heeft de FG ervoor gekozen om geen onderscheid te maken tussen de voornoemde organen en één FG-jaarverantwoordingsrapportage gegevensbescherming met zowel een terugblik op 2023 als een vooruitblik op 2024 voor de geldende privacy wet- en regelgeving AVG/Wpg te distribueren.

**Doel(en)**

Een hoog niveau van privacy door bescherming van (bijzondere) persoonsgegevens van burgers, ondernemers, gelieerde maatschappelijke instellingen) draagt bij aan een betrouwbare, integere en professionele gemeente in lijn met de doelen zoals vermeld in de gemeentelijke kadernota 2024.

Doel is eveneens om via de jaarlijkse PDCA-verbetercyclus (Plan Do Check Act) stap voor stap als gemeente Weert aan de AVG en Wpg verantwoordingsplicht incl. documentatieplicht (lees: bewijslast) te voldoen ten behoeve van privacy compliance (voldoen aan de privacy wet- en regelgeving).

**Resultaten**

De FG-jaarverantwoordingsrapportage gegevensbescherming is een jaarlijkse verantwoordingsrapportage vanuit de FG als onafhankelijk intern toezichthouder voor de gemeentelijke privacy wet- en regelgeving Algemene Verordening Gegevensbescherming –

|                        |    |           |    |      |     |    |    |    |
|------------------------|----|-----------|----|------|-----|----|----|----|
| Weert,<br>8 april 2024 | S  |           | B  | W    | W   | W  | W  | W  |
|                        | AV |           | RV | MvdH | TvG | SW | LS | MF |
|                        |    | akkoord   |    |      |     |    |    |    |
|                        |    | bespreken |    |      |     |    |    |    |

Soort besluit: Besluit college

**In te vullen door het B&W secretariaat:**

- ☒ Akkoord  
☐ Akkoord met tekstuele aanpassing door portefeuillehouder  
☐ Anders, nl.:

- ☐ Niet akkoord  
☐ Gewijzigde versie

Beslissing d.d.: 21 mei 2024

Nummer:

6

De secretaris

AVG en Wet Politiegegevens - Wpg en privacy ontwikkelingen ten behoeve van de hoogste leidinggevende, bestuursorganen Burgemeester, College en Raad. In deze FG-verantwoordingsrapportage (zie Bijlage 1) staat welke onderwerpen reeds grotendeels voldoen aan de geldende privacy wet- en regelgeving en welke hoofdaandachtspunten /aanbevelingen aandacht vereist van management voor komend jaar 2024 en vervolgjaren.

#### Stand van zaken AVG:

| Thema:                                                                                                              | 2023                                                                                | 2024      | 2024                                                                                  |
|---------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-----------|---------------------------------------------------------------------------------------|
| Borging AVG                                                                                                         | Jaarverslag                                                                         | Resultaat | Verwacht                                                                              |
|  <b>Beleid</b>                     |    |           |    |
|  <b>Processen</b>                  |    |           |    |
|  <b>Organisatorische inbedding</b> |    |           |    |
|  <b>Rechten van betrokkenen</b>    |    |           |    |
|  <b>Samenwerking</b>              |   |           |   |
|  <b>Gegevensbescherming</b>      |  |           |  |
|  <b>Verantwoording</b>           |  |           |  |

#### Legenda:

|                                                                                     |                                 |
|-------------------------------------------------------------------------------------|---------------------------------|
|  | AANDACHT VEREIST VAN MANAGEMENT |
|  | IN TE HALEN ACHTERSTAND         |
|  | OP SCHEMA                       |

## Stand van zaken Wpg:

| Thema:                           | 2023        | 2024      | 2024     |
|----------------------------------|-------------|-----------|----------|
| Borging WPG                      | Jaarverslag | Resultaat | Verwacht |
| Beleid                           | ●           |           | ●        |
| Bewustwording                    | ●           |           | ●        |
| Autorisatieproces                | ●           |           | ○        |
| Bewaartermijnen                  | ○           |           | ○        |
| Verstrekken van persoonsgegevens | ●           |           | ○        |
| DPIA                             | ●           |           | ●        |
| Register van verwerkingen        | ●           |           | ○        |
| Auditverplichting                | ●           |           | ●        |
| (.....)                          | ●           |           | ●        |

### Legenda:

|   |                                 |
|---|---------------------------------|
| ● | AANDACHT VEREIST VAN MANAGEMENT |
| ○ | IN TE HALEN ACHTERSTAND         |
| ● | OP SCHEMA                       |

## Activiteiten

De beoogde activiteiten hiervoor in het kader van het gegevensbeschermingsrecht worden uitgevoerd conform het uitvoeringsplan c.q. Afdelingsplan Informatie 2024 versiedatum d.d. 18-12-2023.

## Argumenten

### 1.1 Opvolging FG aanbevelingen- Hoofd Aandachts Punten (HAP's) voor 2024

In de FG-jaarverantwoordingsrapportage 2023 Terugblik | 2024 Vooruitblik zijn door de FG aanbevelingen- Hoofd Aandachts Punten benoemd die management aandacht vereisen voor 2024.

#### 1.1.1 DPIA's voor hoog risicovolle persoonsgegevensverwerkingen zijn verplicht vanuit de AVG en Wpg.

DPIA's vallen onder het thema AVG borging-Processen. Voor de Wpg borging geldt er een separaat thema DPIA. In de 2e helft van 2024 is gepland om nieuwe DPIA's voor nieuwe processen uit te voeren en ontstane DPIA-achterstanden in te lopen voor bestaande c.q. generieke gemeentelijke en ook specifieke gemeentelijke processen-gegevensverwerkingen.

#### 1.1.2 Management Control systeem-proces vanuit verantwoordingsplicht en documentatieplicht voor o.a. AVG en Wpg.

Om de gemeentelijke verantwoordingsplicht incl. bewijslast eenvoudiger te kunnen monitoren en rapporteren is er een Privacy Management Systeem (PMS) nodig voor de privacy normenkaders AVG en Wpg ter ondersteuning van de jaarlijkse verantwoordingscyclus. Hierbij wordt gebruik gemaakt van de Plan-Do-Check-Act (PDCA) cyclus. Een Privacy Informatie Management Systeem (PIMS) is hierbij ondersteunend echter zonder zo'n systeem is het risico om zaken te vergeten groot en is er een aanzienlijke kans dat de gemeente Weert niet 'privacy compliant' is.

## **Kanttekeningen en risico's**

### **1.1.1**

*In geval van het niet uitvoeren van verplichte DPIA's vanuit AVG/Wpg wet- en regelgeving loopt het Bestuur vanuit bestuursverantwoordelijkheid risico's o.a.:*

- Media-aandacht voor gemeente Weert, afbreukrisico, imagoschade, negatief in de pers, onder verscherpt toezicht van de Autoriteit Persoonsgegevens (AP) zoals in maart 2023 is gebeurd bij gemeente Eindhoven.
- Kritische adviezen vanuit diverse toezichthouders (o.a. externe auditor (-s), interimcontrole via externe accountant, Autoriteit Persoonsgegevens (AP) richting bestuur zijn mogelijk.
- De AP kan nader onderzoek instellen naar verwerkingen van persoonsgegevens bij en door gemeente Weert in het kader van de AVG of Wpg indien zij daar aanleiding toe ziet, bijvoorbeeld als de AP-klachten of andere signalen over een verwerking krijgt.
- Boetebedrag voorbeeld zoals opgelegd vanuit de AP voor het niet uitgevoerd hebben van een verplichte DPIA a € 150K.
- Slechts enkele DPIA's op de hoog risicoverwerkingen van persoonsgegevens zijn uitgevoerd in de afgelopen jaren vanaf de startdatum van de AVG op 25 mei 2018.
- Minimaal XX-processen zijn niet gevalideerd conform AVG en Wpg. Dus het is op dit moment onbekend hoeveel risico we als gemeente lopen met mogelijk onnodige financiële kosten.
- Processen lopen gemiddeld XX maanden/Y jaren vertraging op.
- Er zijn geen accurate cijfers voor het bestuur om op te sturen.
- Geen focus op beheersing en control van risico's vanwege het niet uitvoeren van DPIA's in het kader van data- en gegevensbeheer v.w.b. aard (persoons-) gegevens, omvang gegevens, noodzakelijkheid/ dataminimalisatie, proportionaliteit, subsidiariteit en rechtmatigheid.

### **1.1.2**

*Management Control systeem-proces vanuit verantwoordingsplicht en documentatieplicht voor o.a. AVG en Wpg.*

Zonder Management Control systeem-proces ook wel genaamd GRC (Governance, Risk, Compliance) tool is het risico om zaken te vergeten groot en is er een aanzienlijke kans dat de gemeente Weert niet 'privacy compliant' is.

## **Financiële, personele en juridische gevolgen**

### **1.1 Opvolging FG aanbevelingen- Hoofd Aandachts Punten (HAP's) voor 2024**

*1.1.1 DPIA's voor hoog risicovolle persoonsgegevensverwerkingen zijn verplicht vanuit de AVG en Wpg.*

#### **Personele gevolgen:**

Vanuit de afdeling Informatie zal afdoende Privacy Officer (PO) capaciteit t.z.t. aanwezig moeten zijn uiteraard afhankelijk van het aantal te prioriteren verplichte DPIA's voor 2024. Intern zullen medewerkers uit de lijn ook tijd moeten investeren. Per DPIA zullen de lijn-vak afdelingen gemiddeld 16-24 uur nodig hebben initieel gedurende komend jaar 2024.

#### **Financiële gevolgen:**

Verder is door de FG geadviseerd om een DPIA-training (eenduidige methodiek) extern/incompany te gaan volgen voor een nader vast te stellen doelgroep binnen gemeente Weert. Deze opleiding zal worden bekostigd uit het budget Vorming & Opleiding van de directie.

### *1.1.2 Management Control systeem-proces vanuit verantwoordingsplicht en documentatieplicht voor o.a. AVG en Wpg.*

#### Personele gevolgen:

Initieel zullen de privacy ambassadeurs per afdeling voor de projectimplementatie beperkt betrokken zijn. De leverancier zal het grootste gedeelte van de realisatie en implementatie/nazorg voor zijn rekening nemen. Vanuit de lijn-vak afdelingen waar uiteraard persoonsgegevens van toepassing zijn is in de reguliere fase de privacy contactpersoon voor het Privacy Management Control systeem structureel gemiddeld 2 uur per week nodig.

#### Financiële gevolgen:

Aanschaf van de Privacy Management Control modules ofwel normenkaders zal bekostigd worden vanuit het afdelingsbudget Informatie 2024 voor de eenmalige kosten (voor de projectimplementatie) en de jaarlijks terugkerende (structurele) kosten voor het beheer en gebruik.

#### Juridische gevolgen:

Met de leverancier van het nieuwe Management Control systeem dient een AVG/Wpg verwerkersovereenkomst als onderdeel van de implementatie te worden gesloten voorafgaande aan de productie ingebruikname datum.

### **Overleg gevoerd met**

#### *Intern:*

- Janine Wolters (Privacy Officer, afdeling Informatie)
- Bart Lurken (CISO, afdeling Informatie)
- Ron Meerts (Afdelingshoofd Informatie)
- Anne-Marie Vrijenhoek (Algemeen directeur/ Gemeentesecretaris)
- CMT

#### *Extern:*

- Niet van toepassing.

### **Participatie**

Er is voor bijgaand B&W voorstel geen sprake van burgerparticipatie.

### **Communicatie**

Gemeenteraad informeren via TILS-lijst digitaal, TILS als Ter Inzage Liggende Stukken voor de Raad.

### **Planning**

#### *1.1.1 DPIA's voor hoog risicovolle persoonsgegevensverwerkingen zijn verplicht vanuit de AVG en Wpg.*

De planning is dat het opstellen van DPIA's (wegwerken van opgelopen achterstanden) voor geprioriteerde bestaande hoog risicovolle persoonsgegevens verwerkingen van start gaat in de 2e helft van 2024. DPIA's maken voor nieuwe hoog risicovolle persoonsgegevensverwerkingen geldt ook voor nieuwe processen en nieuwe initiatieven in het kader van het coalitieprogramma 2022-2026 waarbij privacy in overweging moet worden genomen in de eerste ontwerpfasen en gedurende het volledige ontwikkelingsproces van nieuwe producten, processen of diensten waarbij persoonsgegevens worden verwerkt.

### *1.1.2 Management Control systeem-proces vanuit verantwoordingsplicht en documentatieplicht voor o.a. AVG en Wpg.*

De implementatie van het Management Control systeem voor AVG/Wpg zal gaan plaats vinden als project in de 2e helft van 2024 na selectie en aanschaf. Dit in samenspraak met de leverancier.

#### **Evaluatie**

Het privacy jaarwerkprogramma wordt ambtelijk periodiek geëvalueerd. Evaluatie vindt ook plaats via de jaarlijkse verantwoordingsrapportage van de FG (zie Bijlage 1) aan het College.

#### **Bijlage(n)**

- Bijlage 1 – Jaarverantwoordingsrapportage FG 2023 terugblik | 2024 vooruitblik (AVG/Wpg)
- Bijlage 1A – Datalekken overzicht 2023
- Bijlage 1B - Overzicht (pré) - DPIA's

# **Jaarverantwoordingsrapportage FG**

## **2023 terugblik 2024 vooruitblik**

Maart-April 2024

Auteur: Roger Coenen,  
Functionaris Gegevensbescherming  
(FG)

# Managementsamenvatting

Naast de wettelijke verplichting vanuit de Europese Algemene verordening gegevensbescherming (AVG) is de bescherming van persoonsgegevens essentieel voor het vertrouwen van de inwoners van Weert in de overheid. In een vrije, democratische samenleving moeten mensen erop kunnen vertrouwen dat de gemeente zorgvuldig omgaat met hun gegevens. Anders kan dit grote gevolgen hebben voor de inwoners die het betreft. Denk bijvoorbeeld aan identiteitsfraude, reputatieschade, discriminatie en financiële schade. Digitalisering en technologische ontwikkelingen hebben vanzelfsprekend een steeds grotere impact op de maatschappij en daarmee op iedereen die woont en werkt in gemeente Weert. Als gegevens op plekken komen waar ze niet horen te zijn, leidt dat tot situaties die juist niet mensgericht zijn. Een incident met (persoons-) data kan ook grote impact hebben voor de gemeente zelf. Het kan de interne bedrijfsvoering en externe publieke dienstverlening richting de burgers en ondernemers stil leggen. Het digitale dreigingsbeeld voor gemeenten is mede door de in 2022 ontstane oorlog in Oekraïne eveneens sterk toegenomen.

De Europese Verordening AVG is op 24 mei 2016 in werking getreden en sinds 25 mei 2018 van toepassing zo ook voor gemeenten. De Autoriteit Persoonsgegevens (AP) is in Nederland de privacy toezichthouder sedert 25 mei 2018 voor de AVG, sedert 2022 voor de landelijke Wet Politiegegevens (Wpg) – Bpgboa (Besluit politiegegevens voor BOA's) en sedert 2023 ook als Algoritme Autoriteit vanuit Artificial Intelligence (AI) ofwel kunstmatige intelligentie (KI) & Algoritmen.

Wij als gemeente Weert zien de privacy wetgeving niet als een 'kan niet / mag niet-wetgeving', maar een wetgeving die ons kaders en ruimte biedt. Ruimte om zaken mogelijk te maken die bijdragen aan het goede leven in Weert. De huidige AVG en Wpg/Bpgboa bieden ons als gemeente handvatten om dit op een zorgvuldige manier te doen zodat we ongewenste situaties voorkomen in de omgang met en het verwerken van persoonsgegevens. Zorgvuldig omgaan met persoonsgegevens is een continu proces en zal dan ook aandacht blijven vergen van zowel bestuur, management als medewerkers. De verantwoordelijkheden voor gemeente Weert voor het verwerken van persoonsgegevens van burgers liggen in hoofdlijnen bij de drie bestuursorganen: het college van B&W, de burgemeester en de gemeenteraad. Het college is verantwoordelijk voor het merendeel van de verwerkingen van persoonsgegevens in onze gemeente. Deze verantwoordelijkheid brengt verplichtingen met zich mee.

Vanuit de privacy jaarwerkprogramma's voor zowel AVG als Wpg is in Weert afgelopen jaar 2023 opnieuw veel werk verzet op het gebied van gegevensbescherming/privacy om de gezamenlijke gemeentelijke business- en informatie doelen te verwezenlijken. Dit omvat o.a. privacybeleid, privacy governance inrichting, training en privacy bewustwording via o.a. E-learning en blogs op het Intranet, contracten of overeenkomsten afsluiten met verwerkers, gezamenlijke- en zelfstandige verwerkingsverantwoordelijken, datalekken management en mitigatie maatregelen treffen, informeren van betrokkenen en het correct en tijdig afhandelen van ontvangen rechten van betrokkenen.

In 2024 gaat de gemeente Weert verder met vergroten van de privacy bewustwording / bewustzijn en kennisdeling op het gebied van AVG, Wpg en AI met zowel medewerkers als bestuur. Daarnaast is het FG advies om de aantoonbaarheid van privacy compliance per afdeling (verantwoordingsplicht en documentatieplicht) te gaan borgen via een privacy informatie management control systeem. Bescherming van persoonsgegevens is een teamsport, waarbij de privacy adviseurs gezamenlijk met de vak afdelingen invulling geven aan het gemeentelijke programma en de business-informatie doelen. De vak afdelingen zijn daarbij de processysteemdata eigenaren en verwerkingsverantwoordelijken voor hun eigen gegevensverwerkingen.

# FG aanbevelingen voor 2024

## **Verplichte DPIA's:**

- Zorg dat het uitvoeren van een verplichte DPIA risicotoeets voor hoog risicovolle persoons gegevensverwerkingen een gestandaardiseerd en eenduidig proces wordt. Dit bevordert eveneens het DPIA bewustzijn van de vak afdelingen c.q. verwerkingsverantwoordelijken. Daarnaast voorkomt het uitvoeren van een verplichte DPIA via een gestandaardiseerd/eenduidig DPIA proces boetes/sancties zoals eerder is opgelegd door de AP (NL Autoriteit Persoonsgegevens) a € 150.000 euro vanwege het ontbreken van een verplichte DPIA.
- Zorg dat werkprocessen / bedrijfsprocessen zoals beschreven actueel blijven en overeenkomen met het werken in de praktijk. Dit in lijn met de jaarlijkse financiële rechtmatigheidsverantwoording vanuit de gemeente met de focus op alle hoog risicovolle processen met een hoog afbreukrisico voor gemeente Weert. De organisatie evalueert periodiek of de beschrijvingen van werkprocessen aansluiten bij de praktijk. Wanneer de procesbeschrijvingen niet actueel zijn, kan de organisatie niet aantonen dat de verwerkingen van persoonsgegevens in overeenstemming met de AVG worden uitgevoerd (art. 24 lid 1 AVG). Daarnaast gaat het her beoordelen van de eigen hoog risicovolle processen (bijvoorbeeld a.h.v. van een Lean management methodiek) leiden tot een hogere effectiviteit en meer efficiency.
- Zorg voor een externe of incompany DPIA training voor een nader vast te stellen doelgroep binnen gemeente Weert.
- Zorg voor afdoende resourcecapaciteit en middelen voor en het uitvoeren van DPIA's op nieuwe processen en tevens voor het wegwerken van de opgelopen achterstanden voor verplichte DPIA's bij alle bestaande hoog risicovolle gegevensverwerkingen van persoonsgegevens.

## **Management Control systeem:**

- De FG adviseert om z.s.m. in 2024 gebruik te gaan maken van een management control systeem voor Governance Risk Compliance (GRC) waarmee aantoonbaar de jaarlijkse PDCA – Plan Do Check Act verbetercyclus op gestructureerde wijze wordt afgedekt ook voor wat betreft de bescherming van persoonsgegevens. Een management control systeem maakt onderdeel uit van de jaarplannen 2024 (van afdelingen Concerncontrol, Interne Controle en Informatie) voor de jaarlijkse financiële rechtmatigheidsverantwoording, privacy wet- en regelgeving, informatieveiligheid en Informatiebeheer. Het risico dat we als gemeente Weert iets (per ongeluk/onbewust) vergeten of over het hoofd zien is met een Management Control systeem niet meer aan de orde. Verantwoordingsplicht en documentatieplicht (bewijslast) op ieder willekeurig tijdstip t.b.v. de PDCA cyclus en compliance doeleinden (voldoen aan de geldende privacy wet- en regelgeving AVG, Wpg etc.) wordt daarmee geborgd voor de toekomst.
- De implementatie van voornoemde management control systeem vereist per afdeling privacy ambassadeurs. Deze privacy ambassadeurs zijn aanspreekpunt binnen de eigen afdeling voor de collega's en aanspreekpunt voor de privacy officer en applicatiebeheerders van de afdeling Informatie en zijn tevens verantwoordelijke voor het actueel houden van het Weertse AVG/Wpg en mogelijk toekomstige AI register van verwerkingen in opdracht van de proceseigenaar c.q. het afdelingshoofd.
- Zorg dat er op afdelingen meer tijd en budget vrij wordt gemaakt voor het uitvoeren van compliance taken.

# Inhoud

|                                                                        |    |
|------------------------------------------------------------------------|----|
| Inleiding.....                                                         | 5  |
| Leeswijzer .....                                                       | 6  |
| 1. AVG - Terugblik op 2023 .....                                       | 7  |
| 1.1 Beleid .....                                                       | 7  |
| 1.2 Processen .....                                                    | 7  |
| 1.3 Organisatorische inbedding .....                                   | 8  |
| 1.4 Rechten van betrokkenen .....                                      | 9  |
| 1.5 Samenwerking .....                                                 | 9  |
| 1.6 Gegevensbescherming .....                                          | 10 |
| 1.7 Verantwoording .....                                               | 10 |
| 2. AVG – Vooruitblik naar 2024 .....                                   | 12 |
| 2.1 Beleid .....                                                       | 12 |
| 2.2 Processen .....                                                    | 12 |
| 2.3 Organisatorische inbedding .....                                   | 15 |
| 2.4 Rechten van betrokkenen .....                                      | 16 |
| 2.5 Samenwerking .....                                                 | 17 |
| 2.6 Gegevensbescherming .....                                          | 17 |
| 2.7 Verantwoording .....                                               | 20 |
| 3. Wpg (Wet Politie Gegevens) .....                                    | 21 |
| 3.1 Terugblik op 2023 .....                                            | 21 |
| 3.2 Vooruitblik naar 2024 .....                                        | 22 |
| 4. AI - Artificial Intelligence   KI - Kunstmatige Intelligentie ..... | 23 |
| 4.1 Vooruitblik naar 2024 .....                                        | 23 |
| Bijlage A: Datalekken overzicht .....                                  | 23 |
| Bijlage B: (Pré-) DPIA overzicht .....                                 | 23 |

# Inleiding

De gemeente Weert verwerkt bij de uitoefening van haar taken veel (gevoelige) gegevens van (kwetsbare) burgers in verschillende domeinen. Daarnaast verwerkt de gemeente persoonsgegevens van o.a. medewerkers, bestuurders, externen, etc.

De EU-AVG geeft regels voor het verwerken van persoonsgegevens. Zo moet de gemeente transparant zijn over welke persoonsgegevens zij verwerkt, voor welk doel en op basis van welke grondslag. Persoonsgegevens mogen niet zomaar voor een ander doel worden verwerkt, moeten goed worden beveiligd en moeten zodra ze niet meer nodig zijn voor het doel worden vernietigd of geanonimiseerd. Ook voor sectorspecifieke wetten gelden er privacyregels. De gemeente moet zich hiervan bewust zijn en daarmee bij de inrichting van haar processen en systemen rekening houden.

Onder de verantwoordelijkheid van zowel het college van B&W als de burgemeester en de gemeenteraad vindt een groot aantal verwerkingen van persoonsgegevens plaats. De AVG bepaalt dat daar extern en intern toezicht op moet plaatsvinden. De Autoriteit Persoonsgegevens (AP) houdt extern toezicht op de naleving van de privacyregels in Nederland. Daarnaast is de gemeente verplicht te beschikken over een interne privacy toezichthouder: de Functionaris Gegevensbescherming (FG). Roger Coenen vervult sedert 1 november 2023 de functie als FG voor de gemeente Weert.

De FG ziet erop toe dat de privacywetgeving wordt nageleefd en dient als onafhankelijk intern toezichthouder hierover te informeren/adviseren, monitoren en rapporteren. Het college, respectievelijk de burgemeester en de gemeenteraad dient erop toe te zien dat de FG naar behoren en tijdig wordt betrokken bij alle gelegenheden die verband houden met de bescherming van persoonsgegevens. Daarnaast dient de FG ondersteund te worden door hem/haar toegang te verschaffen tot persoonsgegevens en verwerkingen daarvan en de benodigde middelen ter beschikking te stellen voor het vervullen van de taak en het in standhouden van de FG deskundigheid.

## Leeswijzer

Bijgaande jaarrapportage bestaat uit meerdere onderdelen. Allereerst wordt teruggekeken naar afgelopen jaar 2023 v.w.b. de AVG. Wat heeft de gemeente Weert bereikt op het gebied van gegevensbescherming? Welke maatregelen zijn er genomen om blijvend te voldoen aan de AVG? Aansluitend worden aanbevelingen gedaan om gegevensbescherming en privacy in het komende jaar 2024 naar een hoger niveau te tillen. Hierbij wordt waar nodig tevens aandacht geschonken aan de technische en organisatorische middelen die nodig zijn om dit hogere niveau te bereiken.

Om een gemotiveerd oordeel te kunnen geven over wat de gemeente heeft bereikt en waar zij "staat" in het implementatieproces van de AVG, maakt de FG voor bijgaande jaarverantwoordingsrapportage 2023 gebruik van het AVG borgingsproduct 3.0 van de Informatiebeveiligingsdienst (IBD) <sup>1</sup>. Daarin worden zeven thema's onderscheiden:

1. Beleid
2. Processen
3. Organisatorische inbedding
4. Rechten van betrokkenen
5. Samenwerking
6. Gegevensbescherming
7. Verantwoording

Per thema worden in het AVG borgingsproduct criteria en maatregelen omschreven die de AVG vertalen naar een kwaliteitscyclus voor gegevensbescherming/privacy voor gemeentelijke processen.

Ook voor de Wpg (Wet Politiegegevens) verantwoording volgt een terugblik op 2023 en een vooruitblik naar 2024. Door de Wpg auditor Koenen & Co is een separaat Assurance rapport 2023 / (her-) audit rapportage aangeleverd met daarin benoemd de vereiste PDCA maatregelen en verbeteracties om als gemeente Weert Wpg compliant te worden.

De nieuwe Eu verordening AI act v.w.b. AI – Artificial Intelligence c.q. KI – Kunstmatige Intelligentie komt er ook aan in 2024. Voor AI & Algoritmen (hieronder valt o.a. ChatGPT of Co-pilot als AI tool) volgt een vooruitblik naar de AI/KI hoofdaandachtspunten van belang voor gemeentelijke overheden.

<sup>1</sup> <https://www.informatiebeveiligingsdienst.nl/product/avg-borgingsproduct-3-0-toetsingskader/>

# 1. AVG - Terugblik op 2023

Ook het afgelopen jaar 2023 stond in het teken van het verder implementeren van de AVG en het continueren van de bewustwording op het gebied van en gegevensbescherming en informatieveiligheid. In dit deel van de rapportage zal worden teruggeblikt op hetgeen de gemeente in 2023 heeft bereikt en welke werkzaamheden zijn verricht.

## 1.1 Beleid

Het privacy beleid omschrijft hoe gemeente Weert invulling geeft aan de privacy wet- en regelgeving Europese Algemene Verordening Gegevensbescherming (EU-AVG) en landelijke Wet Politiegegevens (Wpg) / Besluit politiegegevens voor Boa's (bpgboa). Het nieuwe privacy beleid 2023-2026 is op 21 maart 2023 jl. vastgesteld door college B&W voor de gehele organisatie.

Het is van belang dat de organisatie periodiek heroverweegt of het privacy beleid nog aansluit bij interne en externe ontwikkelingen. Het privacy beleid wordt periodiek, maar ten minste eenmaal per 36 maanden, herzien. Bij een herziening is het niet altijd noodzakelijk om wijzigingen door te voeren. Het is wel van belang dat de organisatie periodiek heroverweegt of het beleid nog aansluit bij interne en externe ontwikkelingen.

Privacy kent overlap of aanknopingspunten met de organisatievisie, kernwaarden van gemeente Weert en ander beleid in de organisatie. Denk bijvoorbeeld aan het informatiebeveiligingsbeleid, archiefbeleid en personeelsbeleid. Dit beleid moet op elkaar aansluiten en waar nodig naar elkaar verwijzen.

Management is verantwoordelijk voor het realiseren van de doelstellingen van het nieuwe privacy beleid 2023-2026 van gemeente Weert.

De gemeente voldoet wat betreft dit thema voor een groot deel aan de AVG. 😊

## 1.2 Processen

De verwerkingen van persoonsgegevens van gemeente Weert dienen te voldoen aan de AVG. Dit houdt in dat de werkprocessen die persoonsgegevens bevatten getoetst en ingericht moeten worden volgens de volgende AVG beginselen: behoorlijkheid, transparantie, doelbinding, dataminimalisatie, opslagbeperking, juistheid, integriteit en vertrouwelijkheid.

### **DPIA's:**

Daarnaast kan de gemeente in gevallen verplicht zijn om een GEB – gegevensbeschermings-effectbeoordeling (afkorting DPIA<sup>2</sup>) uit te voeren. Voorts heeft de gemeente afgelopen jaar 2023 DPIA's uitgevoerd bij nieuwe of gewijzigde verwerkingen van persoonsgegevens.

In bijlage B is een overzicht opgenomen van DPIA's opgestart/onderhanden/afgerond in 2023 en ook nieuwe verplichte DPIA's voor 2024.

Constatering van de FG is dat het aantal DPIA's fors achterblijft ten opzichte van het aantal DPIA's dat gehouden zou moeten worden. Vanuit de FG-rol wordt aangedrongen op het opstellen van een overzicht inzake de noodzakelijke DPIA's (voor welke nieuwe en bestaande hoog risicovolle verwerkingen zijn ze nodig) alsook een DPIA planning verdeeld over geheel 2024. Een DPIA dient eens per 3 jaar te worden gehouden (conform advies vanuit de AP). De AVG is al vanaf mei 2018 van kracht dus dit zou met zich meebrengen dat voor de meeste verwerkingen waar dit nodig is er al een DPIA gehouden zou moeten zijn. Het is zaak om voor 2024 goed zicht hierop te krijgen voor alle gemeentelijke processen (Weertse - specifieke lokale (maatwerk-) processen ofwel eigen processen en de landelijke - generieke ofwel gemeenschappelijke processen) allen met hoog risicovolle persoonsgegevensverwerkingen.

<sup>2</sup> De gegevensbeschermingseffectbeoordeling wordt ook wel afgekort tot DPIA naar de Engelse term Data Protection Impact Assessment.

Ieder afdelingshoofd is verantwoordelijk dat een DPIA risico analyse tijdig wordt uitgevoerd. Hij/zij kan dit zelf doen maar ook een ander de opdracht hiervoor geven, bijvoorbeeld aan een projectleider of beleidsadviseur van de eigen vak afdeling of van afdeling Informatie. En deze hoeft dit niet alleen te doen! Geadviseerd wordt om ondersteuning te vragen aan de privacy officer. Privacy officer formeert een multidisciplinair team bestaande uit afdelingsverantwoordelijke (-n) mogelijk de beleidsadviseur, informatieveiligheid adviseur/CISO, applicatiebeheerder, procesmanager etc. De FG geeft voor elke uitgevoerde DPIA een eindoordeel/advies maar ook vooraf of de vak afdeling de DPIA zelf uitvoert of afhankelijk van het onderwerp hiervoor beter een gespecialiseerd extern bureau inschakelt. Het afdelingshoofd vermeld ook schriftelijk in de DPIA wat er gebeurt als er afgeweken wordt van het FG advies. Het afdelingshoofd is uiteindelijk met het resultaat van de DPIA in staat om te beslissen welke risico's bewust genomen worden en welke risico's geminimaliseerd worden door de benodigde acties uit te zetten om de maatregelen/afspraken te regelen.

#### **Register van verwerkingen (RVV):**

De gemeente heeft het afgelopen jaar 2023 het bestaande register van verwerkingen van persoonsgegevens opnieuw geactualiseerd maar op dit tijdstip 2024Q1 nog niet gepubliceerd op de externe c.q. publieke gemeentelijke website. De FG acht dit laatste wel wenselijk mede vanuit transparantie richting burgers en omdat gemeente Weert een open overheid is zo ook vanuit de Wet Open Overheid (WOO). Register van verwerkingen volgt als output uit de verplicht uit te voeren DPIA 's voor alle hoog risico verwerkingen. De verwerkingen van persoonsgegevens ofwel (persoons-) gegevensuitwisseling incl. geldende AVG grondslag maakt onderdeel uit van af te sluiten verwerkersovereenkomsten persoonsgegevens tussen afdelingsverantwoordelijke/verwerkingsverantwoordelijke (Vv) en verwerkers (V) o.a. (IT-) leveranciers en via de overeenkomsten van gezamenlijke- of zelfstandige verwerkingsverantwoordelijken met andere gemeenten, samenwerking- of private organisaties gebaseerd op de hiervoor genoemde AVG beginselen.

#### **Rechtmatigheids- en efficiency check:**

Daarnaast voert de gemeente Weert - Interne Control een rechtmatigheids- en efficiency check uit op alle financieel risicovolle processen zoals bijvoorbeeld Inkopen en aanbestedingen en Sociaal Domein: WMO (Wet Maatschappelijke Ondersteuning), jeugdzorg, participatiewet (excl. verbonden partijen). Financiële rechtmatigheidsverantwoording is onderdeel van de jaarrekening.

#### **Bewaar- en vernietigingsbeleid:**

Persoonsgegevens worden tijdig verwijderd of geanonimiseerd. De selectielijst is van toepassing op papieren en digitale gegevens. Papieren documenten zijn onderhevig aan de AVG als ze opgenomen zijn (of bestemd zijn om opgenomen te worden in) in een bestand. Persoonsgegevens worden verwijderd of geanonimiseerd in overeenstemming met de Selectielijst 2020. Voor dit onderwerp wordt verwezen naar het jaarverslag 2023 van de gemeentearchivaris voor gemeente Weert.

## **1.3 Organisatorische inbedding**

Voor een goede en juiste uitvoering is het van belang dat eenieder binnen de organisatie op de hoogte is van de beginselen van de AVG en het belang van privacy. Organisatorische inbedding betekent het toewijzen van taken, verantwoordelijkheden en bevoegdheden en bewustzijn creëren. De gemeente heeft de rollen, taken en verantwoordelijkheden op het gebied van gegevensbescherming in haar privacy beleid in de organisatie belegd. Binnen de organisatie wordt iedereen bewust gemaakt van de verantwoordelijkheden die hij heeft op dat gebied heeft. Er zijn middelen beschikbaar voor algemene, organisatie brede opleidingen op het gebied van bewustwording en de verdere doorontwikkeling van gegevensbescherming.

### **Privacy bewustwording – bewustzijn vergroten:**

Er zijn middelen beschikbaar voor algemene, organisatie brede opleidingen op het gebied van bewustwording en de verdere doorontwikkeling van gegevensbescherming. Gemeente Weert maakt gebruik van een laagdrempelige online E-learning tool voor de periodieke bewustwording van zowel privacy als informatieveiligheid. Het 5 jaar bestaan van de AVG op 25 mei 2023 jl. is niet onopgemerkt voorbijgegaan maar met een Hoera Hoera en AVG tompoezen voor alle kantoormedewerkers gevierd.

### **Privacy governance:**

M.i.v. 1 november 2023 is er een nieuwe Functionaris Gegevensbescherming (FG) 0,5 fte aangesteld. Voor gemeenten geldt dat de burgemeester, B&W en de raad allen een FG dienen aan te wijzen. De gemeente Weert heeft één FG aangewezen die zowel toezichthouder is op grond van de AVG als op grond van de Wpg/Wjsg. Dit overeenkomstig het nieuwe aanstellingsbesluit zoals jl. 8-11-2023 ontvangen vanuit de AP (Autoriteit Persoonsgegevens) n.a.v. de gewijzigde FG aanmelding voor gemeente Weert.

Daarnaast is er voor gemeente Weert een Privacy Officer (PO) werkzaam met een privacy beschikbaarheid van 0,5 fte. De uitvoerende privacy taken liggen bij de Privacy Officer (PO) dicht tegen de uitvoeringsorganisatie c.q. vak afdelingen aan. Bij diverse Limburgse gemeenten met zelfs minder inwoners en gelijke privacy uitdagingen zijn privacy officers voor zowel AVG als Wpg/Wjsg fulltime aangesteld voor 36 uur per week - 1 fte.

Taken, verantwoordelijkheden en bevoegdheden voor de FG en PO staan eveneens vermeld in het gegevensbescherming- privacy beleid 2023-2026.

Vanuit privacy governance is er minimaal 4x per jaar met de gemeentesecretaris (GS) een privacy prioriteiten overleg gepland. Daarnaast is er een regionaal privacy overleg voor Midden Limburg (RPO-ML) en optioneel Zuid-Limburg (RPO-ZL) 1x per maand waarbij afstemming plaats vindt over de gemeente overstijgende privacy projecten, issues en gezamenlijke standpunten.

De gemeente voldoet wat betreft dit thema voor een groot deel aan de AVG. 😊

## **1.4 Rechten van betrokkenen**

De gemeente dient degene van wie zij de persoonsgegevens verwerkt (betrokkene) zowel actief als passief te informeren over het verwerken, de wijze van het verwerken, de grondslag en de maatregelen die zij neemt om onrechtmatige toegang en - verwerking te voorkomen. Daarnaast stelt de AVG betrokkenen in staat om door middel van een aantal rechten controle en invloed uit te oefenen over hun persoonsgegevens.

In 2023 is slechts incidenteel gebruik gemaakt door betrokkenen (burgers of ondernemers) van de rechten als volgt:

- Recht op inzage verzoek AVG in 2023:1 (2022:3)
- Recht op verwijdering verzoek AVG in 2023:1 (2022:2)
  
- Recht op correctie verzoek AVG in 2023: 0 (2022:?)
- Recht op beperking verzoek AVG in 2023: 0 (2022:?)
- Recht op data portabiliteit verzoek AVG in 2023: 0 (2022:?)
- Recht op bezwaar verzoek AVG in 2023: 0 (2022:?)

De gemeente voldoet wat betreft dit thema voor een groot deel aan de AVG. 😊

## **1.5 Samenwerking**

De gemeente Weert werkt op meerdere beleidsterreinen, in verschillende bedrijfsfuncties, in diverse rollen en hoedanigheden samen met (mede) overheden en private organisaties. In veelvoorkomende gevallen zal er sprake zijn van een verwerking van persoonsgegevens tussen

partijen: ontvangen van persoonsgegevens, verzenden van persoonsgegevens, maar ook het opslaan van en inzage hebben in persoonsgegevens valt onder dit begrip. Deze verwerkingen dienen dan ook te voldoen aan de AVG. De gemeente moet daarover afspraken maken met de partijen waarmee zij samenwerkt.

Ook het afgelopen jaar heeft de gemeente veel schriftelijke afspraken gemaakt. Dit betreft afspraken met externe partijen die of verwerker zijn (via de meest recente versie van de VNG standaard verwerkersovereenkomst) of als zelfstandig verwerkingsverantwoordelijke (via de modelgegevensleveringsovereenkomst-voor-zelfstandige-verwerkingsverantwoordelijken) of als gezamenlijke verwerkingsverantwoordelijken (via de Model-Overeenkomst-Gezamenlijke-Verwerkingsverantwoordelijken ook wel Convenant genaamd) zijn te beschouwen.

## 1.6 Gegevensbescherming

Vanuit het algemene behoorlijkheidsbeginsel, het integriteitsbeginsel en het vertrouwelijkheidsbeginsel is het essentieel dat de gemeente Weert passende technische en organisatorische maatregelen neemt ter beveiliging van persoonsgegevens.

### **Datalekken <sup>3</sup>:**

Daarnaast geldt er onder de AVG een meldplicht datalekken. Dit houdt in dat incidenten – waaronder inbreuken – op de beveiliging onder omstandigheden gemeld dienen te worden aan de AP en/of de betrokkene(n). Voor wat betreft het thema beveiliging is er sprake van een overlap tussen het vakgebied informatiebeveiliging en gegevensbescherming. De gemeentelijke Chief Information Security Officer (CISO), privacy officer (PO) en de Functionaris Gegevensbescherming (FG) en overige AVG teamleden werken daarop samen. Ook is stevig ingezet op het verder creëren van bewustwording op het gebied van datalekken en beveiligingsincidenten. Dit heeft ertoe geleid dat ook het afgelopen jaar meerdere datalekken zijn gemeld. Het is van belang binnen de organisatie aandacht te blijven besteden aan zowel het melden van datalekken alsook het treffen van treffende risicobeheersmaatregelen n.a.v. een datalek in geval van lekken persoonsgegevens en / of een informatiebeveiliging incident zonder het lekken van persoonsgegevens. Datalekken management procedure is beschikbaar.

### **Enkele doelen bereikt in 2023 voor dit thema:**

- Voor de ENSIA audit (zelfevaluatie van de gemeente op basis van het huidige normenkader BIO – Baseline Informatieveiligheid Overheid is gemeente Weert wederom succesvol geslaagd. Voor een externe digid aansluiting is een aansluit audit uitgevoerd door de CISO.
- MFA (Multi Factor Authenticatie) voor MS Office 365 incl. Teams is gemeente breed ingevoerd.
- Applicatiekeuze en het wel of niet aansluiten op SIEM SOC<sup>4</sup> de bestaande ICT voorkeursleverancier is gestart in 2023 en ook nog onderhanden in 2024.

De gemeente voldoet wat betreft dit thema voor een groot deel aan de AVG. 😊

## 1.7 Verantwoording

De AVG en externe toezichthouder AP leggen de verantwoordelijkheid bij de organisatie zelf om aantoonbaar te maken dat deze voldoet aan de privacyregels. Door te voldoen aan de verantwoordingsplicht, levert de organisatie een belangrijke bijdrage aan de bescherming van het grondrecht van mensen op privacy.

Dit betekent dat het college van B&W te allen tijde aan moet kunnen tonen dat de verwerkingen van persoonsgegevens voldoen aan de beginselen van de AVG en sectorale wet- en regelgeving.

<sup>3</sup> In bijlage 1A is een overzicht opgenomen van het aantal datalekken in 2023 voor gemeente Weert.

<sup>4</sup> Security Information and Event Management, oftewel SIEM, is een oplossing die organisaties helpt bedreigingen te detecteren, te analyseren en erop te reageren voordat ze bedrijfsactiviteiten schade berokkenen zoals dit continueren van de gemeentelijke dienstverlening.

In de praktijk monitort een SOC - Security Operations Centre de computer- en netwerkactiviteiten in een organisatie. Log-informatie van applicaties en apparaten in het bedrijfsnetwerk wordt verzameld en onderzocht op afwijkende zaken.

Tenslotte wordt het college, de burgemeester en de gemeenteraad als verantwoordelijke bestuursorganen door de FG mede door middel van deze jaarrapportage periodiek geïnformeerd over de omgang met persoonsgegevens en de naleving van de AVG.

## 2. AVG – Vooruitblik naar 2024

### 2.1 Beleid

Het privacy beleid 2023-2026 is beschikbaar. Management is verantwoordelijk voor het realiseren van de doelstellingen van het gegevensbescherming- privacy beleid van de gemeente Weert. De Privacy Officer biedt hulp en advies aan management c.q. afdelingsverantwoordelijken bij het uitvoeren van het gegevensbescherming- privacy beleid.

FG advies: inventariseer in 2024 of en zo ja, voor welke domeinen/afdelingen het noodzakelijk is om over domein specifieke uitwerkingen van het privacy beleid te beschikken om correcte omgang met persoonsgegevens binnen het desbetreffende domein te verzekeren. Focus hierbij uitsluitend op de hoog risicovolle persoonsgegevensverwerkingen. Denk hierbij ook aan een privacy protocol c.q. privacy reglement ten behoeve van ondermijning.

### 2.2 Processen

#### **DPIA's:**

Uitvoeren van de verplichte DPIA zorgt ervoor dat de privacy c.q. bescherming van persoonsgegevens (van burgers en /of werknemers) op de juiste wijze wordt geborgd. Door het uitvoeren van een DPIA wordt helder welke risico- beheersmaatregelen bijdragen aan de privacy borging.

DPIA's voor hoog risicovolle persoonsgegevensverwerkingen zijn verplicht vanuit de AVG. Begin februari '24 is gestart met het opnieuw inventariseren van onze hoog risicovolle persoonsgegevensverwerkingen via alle afdelingsmanagers. Dit heet een pré -DPIA waaruit volgt of er een DPIA vereist is ja of nee. De afdelingsmanagers zijn hierbij in termen van de AVG verwerkingsverantwoordelijken en tevens processysteemdata eigenaren van de eigen data c.q. (persoons-) gegevensverwerkingen.

De inventarisatie gaat middels het invullen van dit DPIA uitvraag formulier:

<https://forms.office.com/e/15hT2XQCjh> in te vullen door de specialisten van alle genoemde vak afdelingen.

De materie specialisten van de vak afdelingen voeren de DPIA's uit. De huidige privacy officer (PO) en / of tijdelijke inhuur van een DPIA expert/specialist leveren hierbij de ondersteuning aan de materiespecialisten van de vak afdelingen.

FG geeft na oplevering van de DPIA door de privacy officer (PO) een onafhankelijk advies met de focus op DPIA kwaliteit, volledigheid en aanbevolen privacy risico-beheersmaatregelen om mogelijke risico's voor de betrokkenen te mitigeren.

CISO geeft een onafhankelijk advies met focus op mensgerichte- technische- en organisatorische risico-beheersmaatregelen gebaseerd op betrouwbaarheid, integriteit, vertrouwelijkheid ten behoeve van de gemeentelijke informatieveiligheid.

Hoe zorg we als gemeente Weert dat DPIA's een succes worden?

Het uitvoeren van een DPIA (een privacytoets op een hoog risico proces) kan een flinke uitdaging zijn. Enkele uitdagingen om succesvol aan te pakken:

- Er zijn zoveel hoog risico processen waarop een DPIA moet worden gedaan, dat de organisatie amper weet waar ze moet beginnen 🤖
- Medewerkers hebben geen tijd of zin om mee te werken aan een DPIA, waardoor het werk bij de privacy officer komt te liggen 🧑🏻💻
- Als het lukt om de DPIA tot een succesvol einde te brengen, worden de maatregelen niet opgevolgd 📄

Het is dus zaak om DPIA's succesvol te organiseren. In gezamenlijk overleg met het CMT wordt er bepaald welke DPIA's worden gestart op basis van prioriteit, urgentie en wet- en regelgeving.

Een DPIA is verplicht voor verwerkingen met een hoog privacy risico. De verwerkingsverantwoordelijke moet bij de uitvoering van een DPIA advies vragen van de FG (art. 35 lid 2 AVG). Bij deze advisering kan het gaan om:

- of er al dan niet een DPIA moet worden uitgevoerd;
- welke methodologie moet worden uitgevoerd;
- of de DPIA intern kan worden uitgevoerd, of zou moeten worden uitbesteed;
- welke waarborgen (waaronder technische en organisatorische maatregelen) moeten worden toegepast om eventuele risico's voor de rechten en belangen van de betrokkenen te beperken;
- of de DPIA al dan niet correct is uitgevoerd en of de conclusies (de verwerking al dan niet uitvoeren en welke waarborgen toepassen) al dan niet in overeenstemming zijn met de AVG.

De FG is in principe niet betrokken bij de uitvoering van een DPIA, zodat de FG vrij is om onafhankelijk te adviseren over de uitkomsten daarvan. De FG moet toezien op de uitvoering van zijn advies (art. 39 lid 1 sub c AVG). Als een verwerkingsverantwoordelijke het advies van de FG niet opvolgt, moet de besluitvorming hierover worden gemotiveerd en worden vastgelegd.

#### **Huidige risico's voor bestuur vanwege het ontbreken van verplichte DPIA's zijn:**

- Minimaal XX processen zijn niet gevalideerd conform AVG en Wpg. Dus het is op dit moment onbekend hoeveel risico we als gemeente lopen met mogelijke onnodige financiële kosten.
- Slechts enkele afgeronde DPIA's op hoog risico verwerkingen zijn uitgevoerd in de afgelopen jaren vanaf mei 2018.
- Processen lopen gemiddeld XX maanden c.q. Y jaren vertraging op.
- Er zijn geen accurate cijfers voor het bestuur om op te sturen.
- Media aandacht voor gemeente Weert, afbreukrisico, imagoschade, negatief in de pers, onder verscherpt toezicht van de Autoriteit Persoonsgegevens (AP) zoals bijvoorbeeld in maart 2023 is gebeurd bij gemeente Eindhoven.
- Geen focus op beheersing en control van risico's vanwege het niet uitvoeren van DPIA's in het kader van data- en gegevensbeheer v.w.b. aard (persoons-) gegevens, omvang gegevens, noodzakelijkheid/ dataminimalisatie, proportionaliteit, alternatieve oplossingen/subsidiariteit en rechtmatigheid.
- Diverse kritische adviezen vanuit diverse toezichthouders (externe auditors, interim controle externe accountant, Autoriteit Persoonsgegevens (AP) ) richting bestuur zijn mogelijk.
- De AP kan nader onderzoek instellen naar verwerkingen van persoonsgegevens door gemeente Weert in het kader van de AVG of Wpg indien zij daar aanleiding toe ziet, bijvoorbeeld als de AP klachten of andere signalen over een verwerking krijgt.
- Boetebedrag zoals eerder opgelegd vanuit de AP voor het niet uitgevoerd hebben van een verplichte DPIA a € 150K.

#### **FG advies/aanbevelingen m.b.t. DPIA's:**

- Zorg dat de privacy ambassadeurs / materie specialisten van de vak afdelingen / beleidsadviseurs / collega's AVG overleg / Informatiespecialisten - Projectleiders... een specifieke gemeentelijke doelgroep een DPIA training kunnen volgen voor het succesvol uitvoeren van DPIA's.
- Zorg voor een eenduidige DPIA procesbeschrijving en uniforme DPIA aanpak. Kies bij de aanpak voor de juiste methodiek voor het uitvoeren van DPIA's.
- Zorg dat in 2024/2025 zoveel mogelijk wettelijk verplichte DPIA's uitgevoerd gaan worden om deze verwerkingen alsnog te kunnen toetsen op de AVG en privacy impact. Hierbij ligt de prioriteit bij de hoog risicovolle verwerkingen. Op die manier krijgen we als gemeente Weert meer grip op onze risicovolle processen (o.a. Jeugd, WMO, participatie, ondermijning, publieke dienstverlening/Burgerzaken, HRM, Toezicht & Handhaving , cameratoezicht voor de Openbare Orde & Veiligheid en private camerabewaking op gemeentelijke eigendommen) en welke maatregelen nodig zijn voor de mitigatie ervan.

- Zorg voor afdoende capaciteit van o.a. de privacy officer (DPIA adviseur – procesbegeleider) en procesmanager voor het uitvoeren van het aantal geprioriteerde/geplande aantal DPIA's voor 2024/2025. Ook om de ontstane DPIA achterstanden weg te werken.
- Zorg voor voldoende DPIA expertise/kennis en kunde voor het uitvoeren van DPIA's in multidisciplinair verband samen met de collega- vak afdeling specialisten.

### **Register van verwerkingen:**

Nieuwe of gewijzigde verwerkingen van persoonsgegevens dienen tijdig te worden gemeld. Niet alleen om het register actueel te houden, maar ook zodat, waar dit wettelijk is vereist, tijdig een DPIA kan worden uitgevoerd. Aangezien de procesverantwoordelijken (leidinggevend) niet altijd gedetailleerd kennis hebben van de verwerkingen van persoonsgegevens waarvoor zij verantwoordelijk zijn en de proceseigenaren niet altijd de vereiste privacy kennis, is de aanbeveling van de FG aan om zogenaamde privacy-ambassadeurs aan te stellen op iedere afdeling, die de proceseigenaren hierbij kunnen ondersteunen.

Nog niet alle verwerkingen die risicovol zijn, zijn op dit meetmoment 2024Q1 in beeld. Er kan niet aangetoond worden of er aan de AVG/Wpg voldaan wordt en daardoor onduidelijk is of er passende maatregelen zijn genomen. Dit geldt voor zowel de generieke gemeentelijke processen evenals de lokale ofwel specifieke gemeentelijke processen voortvloeiend uit diverse samenwerkingsovereenkomsten in de regio Noord- en Midden Limburg (NML). Het register van verwerkingen is het fundament van de gemeente m.b.t de AVG/Wpg. Niet alleen voor verantwoording, maar ook voor toezicht en sturing. Het is daarom belangrijk dat het register van verwerkingen (AVG/Wpg) volledig en actueel is en blijft.

Een volledig en gevalideerd overzicht van alle hoog risicovolle gemeentelijke processen met de gegevensstromen met persoonsgegevens met een verplichte DPIA vanuit AVG/Wpg is ook goud waard voor nieuwe projecten. Inzicht = tijdsbesparing = kostenbesparing. Zonder inzag in de hoog risico processen en gegevensstromen met persoonsgegevens bestaat de kans dat er middelen ingezet worden op de verkeerde prioriteiten.

### **Bewaar- en vernietigingsbeleid:**

Voor de laatste stand van zaken m.b.t. het bewaar- en vernietigingsbeleid voor zowel AVG als Wpg wordt verwezen naar de door college eerder vastgestelde stukken:

- Verbeterplan Informatiebeheer 2023-2024 Gemeente Weert
- Horizontaal toezichtrapportage Informatiebeheer
- Project Weert Beter Actiever Digitaal met de daaraan gerelateerde deelonderwerpen Email en Whatsapp archivering stakeholders, anonimisering (integratie-) tool als voortvloeisel uit de landelijke wet- en regelgeving Wet Open Overheid – WOO, Wet Elektronische Publicaties – WEP, Wet modernisering elektronisch bestuurlijk verkeer - Wmebv.

### **FG advies/aanbevelingen:**

- FG adviseert om het register van verwerkingen (RVV) op alle wettelijk verplichte onderdelen aan te vullen en alle hoog risicovolle processen met persoonsgegevensverwerkingen voor 80-90% gevalideerd te hebben in 2024. In samenwerking met de stakeholders wordt dit geprioriteerd opgepakt. Verbetering en valideren van het register is een continue taak en zal periodiek geëvalueerd en gecontroleerd worden, waarna aanpassingen en aanvullingen worden uitgevoerd. Het register is geen statisch maar een dynamische bron van processen dat met de dynamiek van de gemeente meebeweegt en continu aandacht moet blijven krijgen.
- zorg voor een instructie hoe het Register van Verwerkingen (RVV) voor AVG/Wpg wordt beheerd, geactualiseerd en gepubliceerd op de publieke website (minimaal 1, maximaal 2x per jaar) en hoe het Register van Verwerkingen (RVV) door de collega's van de vak afdelingen in overleg met de privacy ambassadeur op de eigen afdeling wordt geverifieerd.
- Focus op registers (inzicht): Een actueel, compleet en juist verwerkingsregister, DPIA register en datalekken register. Nauwkeuriger en beter gestructureerde gegevens resulteren

- in efficiëntere rapportages voor management en bestuur en dito besluitvorming (Meten = Weten = Sturen).
- Zorg voor bijwerken van achterstanden (DPIA's, (verwerkers-) overeenkomsten/contractmanagement, bewaar- en vernietigingstermijnen conform het archiefbeleid).

## 2.3 Organisatorische inbedding

### **Privacy governance:**

Voor gemeenten geldt dat de burgemeester, B&W en de raad allen een FG dienen aan te wijzen. Ook dient een functionaris aanwezig te zijn die verantwoordelijk is voor het tijdig inschatten van de gevolgen voor de organisatie van nieuwe ontwikkelingen op het gebied van privacywetgeving.

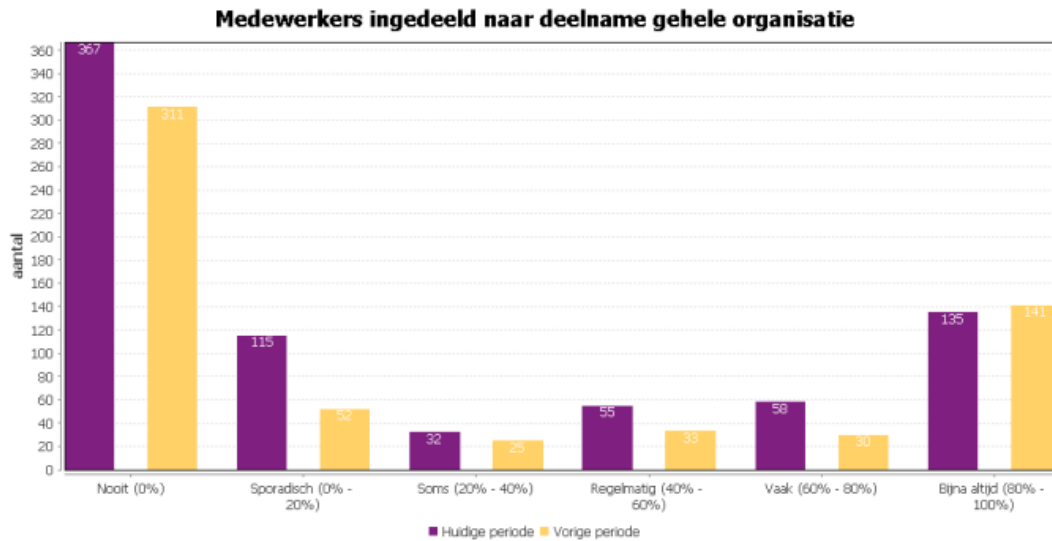
De OR en WOR bestuurder (gemeentesecretaris) worden ook door PO/FG actief geïnformeerd over privacy en gegevensbescherming specifiek voor wat betreft het eigen personeel.

De FG heeft een onafhankelijke, gemeente brede monitoring en toezichtrol (als privacy controller) en een informerende- adviserende rol m.b.t. gegevensbescherming en privacy. Om de onafhankelijkheid van de FG te waarborgen en de schijn van afhankelijkheid te voorkomen is het advies vanuit de AVG en dus ook vanuit de AP als toezichthouder om de rol van de FG onder te brengen bij die organisatieonderdelen die nu al een adviserende en/of toezichthoudende rol hebben (anders dan gegevensbescherming).

### **Privacy bewustwording – bewustzijn vergroten:**

Privacy bewustzijn vergroten van medewerkers en bestuur door training en opleiding kan op verschillende manieren. Naast de reeds bestaande e-learning tool Sir Ask e Lot van leverancier Recourse voor online bewustwording op de gebieden privacy/informatieveiligheid is ook de vraag binnengekomen voor het verzorgen van een (fysieke) introductie workshop privacy / informatieveiligheid bij de onboarding voor alle nieuwkomers/contractanten werkzaam voor gemeente Weert. Nieuwe medewerkers attenderen we al bij hun onboarding op de privacyaspecten van hun werk bij de gemeente Weert. Daarnaast worden ook op het Intranet ("Octo") zogenaamde blogs geplaatst om de privacy bewustwording aan te scherpen c.q. het privacy bewustzijn te vergroten van de medewerkers/werknemers.

## Deelname binnen de gehele organisatie



|                           | 2023-1 t/m 2023-52 |            | 2022-1 t/m 2022-52 |            |
|---------------------------|--------------------|------------|--------------------|------------|
| Deelname                  | Aantal deelnemers  | Percentage | Aantal deelnemers  | Percentage |
| Bijna altijd (80% - 100%) | 135                | 18         | 141                | 24         |
| Vaak (60% - 80%)          | 58                 | 8          | 30                 | 5          |
| Regelmatig (40 - 60%)     | 55                 | 7          | 33                 | 6          |
| Soms (20% - 40%)          | 32                 | 4          | 25                 | 4          |
| Sporadisch (0%- 20%)      | 115                | 15         | 52                 | 9          |
| Nooit (0%)                | 367                | 48         | 311                | 53         |
| Totaal                    | 762                |            | 592                |            |

Uit bovenstaand schema is zichtbaar dat het aantal deelnemers/werknemers dat nooit de één minuut privacy of informatieveiligheid vraag of een 5 minuten minileertaak periodiek beantwoord totaal 367 personen bedraagt voor 2023 op een totaal van 762 kortom rond de 50%. FG adviseert het afdelingsmanagement om de werknemers te vragen om het op een passend tijdstip alsnog zelfstandig af te ronden. Wellicht een idee om de gemeentelijke afdeling die het hoogste scoort (meetindicator: aantal afgerond door genodigden gedeeld door het aantal genodigden op kwartaalbasis en/of jaarbasis) te belonen met een leuke privacy gadget, iets lekkers of een privacy boek ter waardering van veilig gedrag en inzet.

100% betaald hebben voor een laagdrempelige online bewustwording tool met slechts een gebruik van 50% is een te lage opbrengst.

### **privacy ambassadeur (privacy contactpersoon) per afdeling**

Geadviseerd wordt om in 2024 uiterlijk bij de implementatie van het management control systeem privacy ambassadeurs binnen alle gemeentelijke vak afdelingen aan te stellen. Zij kunnen voor hun afdeling en de collega's fungeren als privacy contact / vraagbaak bij sectorspecifieke privacy kwesties (waarbij zij uiteraard altijd de mogelijkheid moeten hebben om te overleggen met de privacy adviseurs de Privacy Officer PO en / of de Functionaris Gegevensbescherming FG) en kunnen ook namens de procesverantwoordelijken de (persoons-) gegevensverwerkingen in het register van verwerkingen actueel houden.

## 2.4 Rechten van betrokkenen

De procedures / instructies m.b.t. de rechten van betrokkenen zijn geactualiseerd op het Intranet (Octo) van gemeente Weert en de externe publieke website voor zowel AVG als Wpg.

De Europese privacy toezichthouders gaan inzage procedures van organisaties nader onderzoeken. 🛡️ De gemeente Weert kan in 2024 mogelijk een vragenlijst ontvangen van de NL privacy toezichthouder (AP) om de kwaliteit van de inzage procedure te laten controleren. Reden is dat nog altijd teveel organisaties te laat of zelfs helemaal niet reageren op een inzageverzoek. Dat terwijl dit wel nodig is voor mensen om inzicht te krijgen om vervolgens mogelijk acties te ondernemen wanneer bijvoorbeeld iets niet klopt met de persoonsgegevens.

## 2.5 Samenwerking

Het advies van de FG is om naast het afsluiten van verwerkersovereenkomsten met verwerkers en de overeenkomsten opgesteld als gezamenlijke verwerkingsverantwoordelijken ook de overeenkomsten van zelfstandige verwerkingsverantwoordelijken met samenwerkende organisaties uit te laten wisselen. Het is zaak om de verstrekking van persoonsgegevens vanuit gemeente Weert aan een zelfstandig verwerkingsverantwoordelijke schriftelijk vastgelegd in een zelfstandige verwerkingsverantwoordelijke overeenkomst met elkaar te delen. In de zelfstandige verwerkingsverantwoordelijke overeenkomst is o.a. vastgelegd welke persoonsgegevens worden er vanuit gemeente verstrekt aan deze private organisatie (-s) en op welke AVG grondslag, wat te doen bij een datalek ofwel een hack bij de zelfstandig verwerkingsverantwoordelijke op de (bijzondere-) persoonsgegevens van cliënten van gemeente Weert. Het is zaak om controle door toezicht vanuit gemeente Weert op zowel privacy als informatieveiligheid bij en alle verwerkers en zelfstandig verwerkingsverantwoordelijken aan te scherpen met als eindconclusie OK of Niet OK. Niet OK kan betekenen dat gemeente Weert vanwege de bestuursverantwoordelijkheid (tijdelijk) afscheid moet nemen van deze zelfstandig verwerkingsverantwoordelijke c.q. private organisatie of verwerker ten faveure van een ander.

Zorg ervoor dat alle getekende verwerkersovereenkomsten en overeenkomsten gezamenlijke verwerkingsverantwoordelijken zijn en worden opgeslagen in een contractmanagement systeem bij financiële verplichtingen en / of in het gemeentelijke zaakstelsel zodat er een vindplaats in het verwerkingsregister wordt genoteerd waar de overeenkomst en e.g. einddatum van de overeenkomst eenvoudig in te zien is wanneer nodig.

## 2.6 Gegevensbescherming

Focus in 2024 ligt op de nieuwe EU NIS2 richtlijn en BIO 2.0 waaraan gemeenten moeten gaan voldoen. NIS2 betekent een wettelijke verplichting voor gemeenten om passende en evenredige maatregelen te nemen om de digitale weerbaarheid te verhogen en cyberbeveiligingsrisico's te beheersen. Aansprakelijkheidsrisico en (financiële) verantwoordelijkheid komt onder NIS2 bij gemeente bestuur te liggen ook wat betreft kosten van incidenten bij en veroorzaakt door ketenleveranciers.

Ook komt er vanuit de AP meer toezicht op de cookie compliance. AP pakt misleidende banners op websites aan. Samen met het team Communicatie zullen de websites van gemeente Weert getoetst worden aan de E-privacy richtlijn.

In 2024 wordt extra aandacht gevraagd voor (controles op) autorisaties en logging en het uitgevoerd hebben van informatie-data classificaties voor alle hoog risicovolle verwerkingen op beschikbaarheid, integriteit, vertrouwelijkheid en privacy.

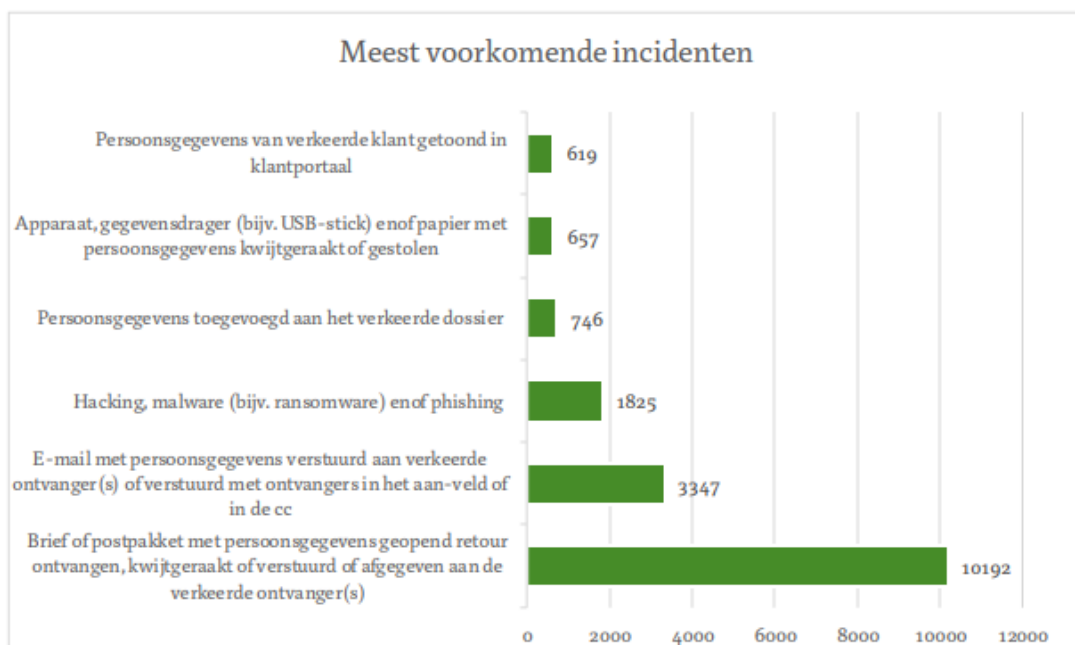
### **Datalekken in NL (overzicht AP):**

Onderstaand de NL datalekken rapportage over 2022 en 2023 van de Autoriteit Persoonsgegevens (AP). E-mail met persoonsgegevens verstuurd aan verkeerde ontvanger(s) of verstuurd met ontvangers in het aan-veld of in de cc (aantallen: 3347) &

Brief of postpakket met persoonsgegevens geopend retour ontvangen, kwijtgeraakt of verstuurd of afgegeven aan de verkeerde ontvanger(s) (aantallen: 10192) gelden als meest voorkomende incidenten.



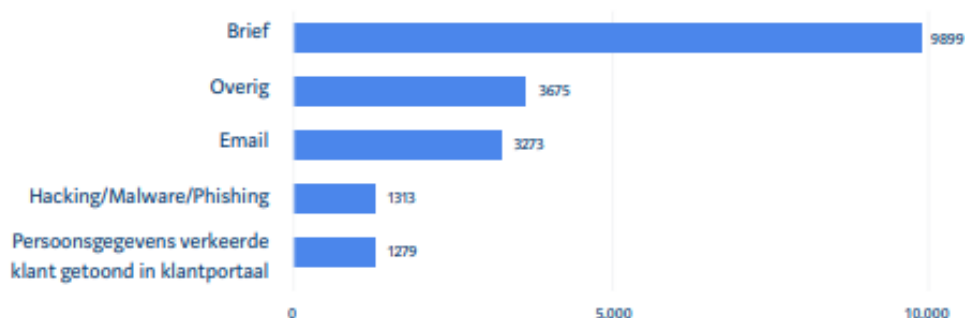
Verder ziet de AP een grote stijging van 65% van het aantal meldingen waarbij autorisaties van medewerkers te breed waren ingesteld. Als gevolg van dit type datalek kunnen medewerkers van organisaties persoonsgegevens inzien die ze voor hun werkzaamheden niet nodig hebben.



Bronvermelding: [AP Rapportage datalekken 2022.pdf \(autoriteitpersoonsgegevens.nl\)](#)

## Verkeerd verzonden brieven het meest gemeld

MEEST GEMELDE CATEGORIEËN VAN DATALEKKEN - TOP 5



Net als voorgaande jaren ontving de AP in 2023 de meeste meldingen over een verkeerd verzonden brief met daarin persoonsgegevens (9.899 meldingen). Alleen als sprake is van een ernstig privacy inbreuk moet dit type datalek gemeld worden aan de AP.

Meldingen in de categorie 'overig' bestonden uit de volgende typen datalekken:

- overig (79,6%), bijvoorbeeld: inzage door geautoriseerd persoon maar zonder geldige reden, of: meer persoonsgegevens doorgestuurd dan nodig;
- persoonsgegevens per ongeluk gepubliceerd (11,6%);
- netwerkmap of locatie verkeerd ingesteld (7,2%);
- persoonsgegevens tijdelijk niet beschikbaar door storing (0,9%);
- documenten met persoonsgegevens bij oud papier gezet (0,6%).

Bronvermelding: [AP Rapportage datalekken 2023.pdf](#)

## 2.7 Verantwoording

### **Privacy Management Systeem (PMS) / Privacy Informatie Management Systeem (PIMS)**

De verantwoordingsplicht incl. documentatieplicht in de Europese Algemene Verordening Gegevensbescherming (AVG) is een belangrijk onderdeel. Deze verantwoordingsplicht en documentatieplicht geldt ook vanuit de regeling voor onze boa's. Om de gemeentelijke verantwoordingsplicht incl. bewijslast eenvoudiger te kunnen monitoren en rapporteren is er een Privacy Management Systeem (PMS) nodig voor de privacy normenkaders AVG en Wpg ter ondersteuning van de jaarlijkse verantwoordingscyclus. Hierbij wordt gebruik gemaakt van de Plan-Do-Check-Act (PDCA) cyclus. Een Privacy Informatie Management Systeem (PIMS) is hierbij ondersteunend echter zonder zo'n systeem is het risico om zaken te vergeten groot en is er een aanzienlijke kans dat de gemeente Weert niet 'privacy compliant' is.

#### **Vervolgacties voor 2024:**

- FG toezichtplan t.b.v. AVG/Wpg;
- Auditplan 2024 t.b.v. AVG/Wpg;
- Voorstel: Onderzoek doen naar AVG certificeringsstandaard en -criteria BC 5701 (NL) in 2024.

Doel: Onderhoud certificaten en accreditaties voor het aan de Autoriteit Persoonsgegevens (AP) of andere externe toezichthouders kunnen aantonen dat de AVG wordt nageleefd. AVG Certificeringsstandaard en -criteria BC 5701 (NL) biedt een raamwerk waarmee organisaties op systematische wijze invulling kunnen geven aan de eisen van de AVG en de daarbij horende verantwoordingsplicht. Na implementatie van de Brand Compliance - BC 5701 is certificering mogelijk, waarmee organisaties kunnen aantonen aan de eisen te voldoen. De AVG Certificeringsstandaard en -criteria BC 5701 is ontwikkeld om organisaties te kunnen certificeren waarbij het object van de certificering een specifiek proces is van de verwerking van persoonsgegevens. De Raad voor Accreditatie heeft Brand Compliance BV accreditatie verleend voor certificering van de ISO 27701, de norm voor een Privacy Information Management System (PIMS).

## 3. Wpg (Wet Politie Gegevens)

### 3.1 Terugblik op 2023

De gemeente Weert heeft voor toezicht en handhaving een aantal buitengewoon opsporingsambtenaren (BOA's) in dienst. Deze BOA's werkzaam voor gemeente Weert zijn in 3 van de 5 Wpg domeinen actief te weten:

Domein 1: Handhaving Openbare Orde en Veiligheid, digitaal uitschrijven van Procesverbalen - Pv's, afdeling VTH (Vergunningen Toezicht & Handhaving).

Domein 3: Leerplichtadministratie in het kader van de Leerplicht, afdeling WIZ (Werk Inkomen en Zorg).

Domein 5: Sociale Recherche in het kader van sociale uitkeringen, afdeling WIZ (Werk Inkomen en Zorg).

Bij de uitoefening van hun toezichthoudende taken hebben de BOA's te maken met de AVG en bestuursrechtelijke persoonsgegevens. Voor hun handhavingstaken hebben zij echter te maken sedert 2019 met de Wet politiegegevens (Wpg) incl. Besluit Politie Gegevens (Bpg/boa) en strafrechtelijke persoonsgegevens.

De Wpg schrijft voor dat de verwerkingsverantwoordelijke (de gemeente Weert) bij het verwerken van persoonsgegevens een FG moet aanwijzen. De gemeente Weert heeft één FG (0.5 fte) aangewezen die zowel toezichthouder is op grond van de AVG als op grond van de Wpg - Wet politiegegevens /Wjsg – Wet justitiële en strafvorderlijke gegevens.

De Wpg schrijft, in tegenstelling tot de AVG, voor dat de gemeente jaarlijks een interne audit moet uitvoeren op de verwerking van persoonsgegevens en een vierjaarlijkse Wpg externe privacy audit. Een externe registrauditor (RE - Register EDP auditor) voerde in 2022 met 1 jaar uitstel vanuit de AP (Autoriteit Persoonsgegevens) de externe audit uit voor de Wpg periode 2019-2020-2021. De audit bevindingen leverden input voor het Wpg verbeterplan voor 2023 en ook voor het uitvoeren van de Wpg (her-) audit over 2023 door auditor Koenen & Co. Tijdens de audit zijn enkel de normen getoetst uit het verbeterplan welke is opgesteld naar aanleiding van de initiële WPG-audit uit 2022. De controle periode betreft 1-1-2023 t/m 31-12-2023. Gezien deze audit een her-audit betreft, is hier enkel op opzet en bestaan getoetst.

De Wpg Assurance rapportage over 2023 dient na vaststelling door college B&W (horizontale verantwoordingsplicht) te zijn aangeleverd vóór 1-3-2024 bij de AP (Autoriteit Persoonsgegevens) vanuit de verticale verantwoordingsplicht.

Uit genoemde Wpg (her-) audit 2023 volgt dat gemeente Weert voldoet aan de Wpg Informatieverstrekking vanuit gemeente Weert en bestaan aantonen van procedures voor het afhandelen van een verzoek tot inzage, rectificatie of verwijdering ingediend door een betrokkene. Voor de Wpg zijn in 2023 geen verzoeken ontvangen voor het uitoefenen van Wpg rechten door betrokkenen.

## 3.2 Vooruitblik naar 2024

Uit de Wpg (her-) audit 2023 komen enkele zaken naar voren die (nog) niet in orde zijn en dus actie vereisen. Het Wpg register van gegevensverwerkingen ontbreekt. Een andere is dat de vorige FG onvoldoende Wpg toezicht heeft gehouden. Wpg toezichtstaken die door de FG zouden moeten worden uitgevoerd in de controleperiode 2023 zijn niet uitgevoerd. De belanghebbenden c.q. lijnafdelingen met BOA's moeten nog taken uitvoeren voor de Wpg.

Focus voor de 3 Wpg domeinen komend jaar 2024 op de volgende bevindingen:

- Domein 1: Richten op app leverancier Citycontrol en de inrichting daarvan in relatie tot gemeente Nederweert.
- Domein 3: Inzicht krijgen over de mogelijkheden en inrichting van het JVS (Jeugd Volg Systeem) en de werkwijze van delen van persoonsgegevens met bureau Halt.
- Domein 5: Leverancier Blinqt vragen om mee te bewegen richting WPG TPM (Third Party Maintenance) verklaring en de mogelijkheden om de systeeminrichting conform de Wpg eisen technisch in te richten.

### **Verstrekkings van politiegegevens aan anderen dan politie en Koninklijke marechaussee:**

Vanuit het Wpg domein 1 - Openbare Ruimte worden er via de app/applicatie op het mobiele device van de BOA's politiegegevens PV's digitaal doorgestuurd naar het CJIB (Centraal Justitieel Incassoburo).

Ook vanuit het Wpg domein 3 – Leerplicht worden er politiegegevens met Bureau Halt gedeeld. Vanuit het Wpg domein 5 – Sociale Recherche afdeling Werk, Inkomen en Zorg (WIZ) zijn zowel in 2022 als in 2023 geen politiegegevens verstrekt aan derden.

### **FG advies:**

- FG adviseert om voor de Wpg verwerkingen van zowel domein 1 als domein 3 een DPIA uit te voeren in 2024 tijdig voor de deadline van de vervolg (her-) audit over 2024.
- FG adviseert om z.s.m. in 2024 ook de wettelijk verplichte Wpg functionaris c.q. privacy officer Wpg (PO Wpg) te laten vaststellen door College B&W en Raad. Een collegevoorstel en raadsinformatiebrief kan worden opgesteld in onderling overleg tussen de PO Wpg en het afdelingshoofd Informatie.

### **Vervolgacties voor 2024:**

- Afronding proces externe Wpg audit 2023.
- Verbeterplan Wpg 2024 opstellen, coördinatie en advies.
- Uitvoeringsplan Wpg 2024 (Plan van uitvoering) opstellen, coördinatie en advies.
- Dit plan van uitvoering afstemmen met de belanghebbenden van de vak afdelingen.
- Hercontrole / (her-) audit plannen voor 2024Q4.
- Opzetten en inrichten nieuwe Wpg compliant processen / Afstemmen met de belanghebbenden
- Opstellen (intern) auditplan Wpg

Voor het uitvoeren van bovenstaande taken dien je voldoende inhoudelijke kennis te hebben (of te verkrijgen middels educatie) van de geldende wetgeving Wpg/Bpgboa.

## 4. AI - Artificial Intelligence | KI - Kunstmatige Intelligentie

### 4.1 Vooruitblik naar 2024

Alle NL gemeenten evenals Gemeente Weert zijn in afwachting van de definitieve vaststelling naar verwachting in maart 2024 van de nieuwe wettekst van de EU-verordening AI (governance) act (Artificial Intelligence) / KI (Kunstmatige Intelligentie). Alle Tech giganten zijn al volop bezig met de (door-) ontwikkeling van diverse AI-Tool (-s) ofwel Chatbots/Bot/Robot zo ook ChatGPT (OpenAI), Copilot (Microsoft), Bard (Google) etc. Alle AI-tools dienen te gaan voldoen aan de wettelijke normen voor informatieveiligheid, opslag en privacy die overeenkomen met deze Europese regelgeving.

ChatGPT of Co-pilot zijn 2 voorbeelden van nieuwe AI/KI tools, robots die werken op basis van algoritmen. AI tools (eigen of derden Chatbots, Anonimiseringstools, iBurgerzaken e-diensten) en algoritmen worden vanuit transparantie oogpunt richting de burgers/ondernemers vastgelegd in Het Algoritmeregister van de Nederlandse overheid, zie voor de laatste stand van zaken hiervoor <https://algoritmes.overheid.nl>

Overheid wil discriminatie en profilering (cf. toeslagenaffaire Belastingdienst) vanwege geautomatiseerde besluitvorming via algoritmes in systemen/applicaties ook bij gemeentelijke overheidsorganisaties in de toekomst zien te voorkomen.

Zie voor een nadere AI toelichting onderstaande link:

<https://www.ictrecht.nl/hubfs/Marketing%20bestanden/AI/ICTRecht%20Cheat%20Sheet%20AI%20Act.pdf>

bronvermelding/auteursrecht: ICT recht

#### **Vervolgacties voor 2024:**

- Opstellen AI richtlijnen / AI principes in afwachting op addendum AI beleid 2024-2026 voor gemeente Weert op basis van de definitieve wettekst AI (governance) act;
- Algoritmeregister vullen voor gemeente Weert (zie jaarplan Informatie 2024 reeds geprioriteerd);
- AI-tools (vragen beantwoorden specifiek over ChatGPT via de gemeenteraadsfractie DUS Weert n.a.v. een TV uitzending van EenVandaag)
- Integrale (risico-) analyse uitvoeren vanuit meerdere invalshoeken met multidisciplinair team (o.a. applicatiebeheer t.b.v. IT leveranciers, Business Intelligence – Data Science / Data Impact Team - DIT, Privacy & Informatieveiligheid, beleidsadviseurs vakafdelingen, ....).
- Onderzoek doen naar nieuwe ISO 42001 standaard voor een verantwoorde inzet van AI. Na instemming met de Raad voor Accreditatie behoort AI certificering tegen deze standaard tot de mogelijkheden.

## Bijlage 1A: Datalekken overzicht 2023

## Bijlage 1B: (Pré-) DPIA overzicht



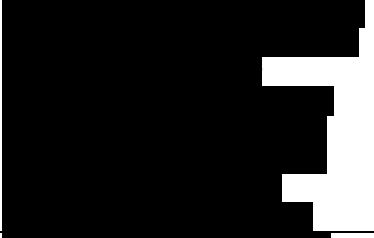
Postbus 950  
6000 AZ Weert  
[www.weert.nl](http://www.weert.nl)

| <b>Bijlage 1A: Overzicht van 21 datalekken in 2023 (2022:16)</b> |                                                                |                                                               |                        |                         |
|------------------------------------------------------------------|----------------------------------------------------------------|---------------------------------------------------------------|------------------------|-------------------------|
| Aantal                                                           | Datalek                                                        | Gemeld aan AP                                                 | Gemeld aan betrokkenen | Mitigerende maatregelen |
| 1                                                                | 2270374 - Incident HS webshop                                  | Nee                                                           | Nee                    |                         |
| 2                                                                | 2296737 - Persoonsverwisseling twee medewerkers gemeente Weert | Ja, door De BP als verwerkings-verantwoordelijke              | Ja                     |                         |
| 3                                                                | 2293592 - Foutief gestuurde mail 05-12                         | Nee                                                           | Ja                     |                         |
| 4                                                                | 2290707 - Foutief gestuurde mail 04-12                         | Ja                                                            | Ja                     |                         |
| 5                                                                | 2202673 - Verkeerd verzonden e-mail                            | Nee                                                           | Nee                    |                         |
| 6                                                                | 2265587 - Kwetsbaarheid Visma Idella                           | Ja, voorlopige melding bij AP                                 | Nee                    |                         |
| 7                                                                | 2108609 - ICT NML; server                                      | Nee                                                           | Nee                    |                         |
| 8                                                                | 2089473 - Ter kennisgeving: datalek CJG                        | Ja door CJGML als (zelfstandig) verwerkings-verantwoordelijke | Ja                     |                         |

**Bijlage 1A: Overzicht van 21 datalekken in 2023 (2022:16)**

|    |                                                           |     |                                                                                                                                                                                                                                                                                                                                                        |  |
|----|-----------------------------------------------------------|-----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| 9  | 2092467 - Novea bewind                                    | Ja  | Ja,<br>In dit geval zijn er twee opties: de gemeente stuurt rechtstreeks de informatiebrief naar de client of de gemeente stuurt de informatiebrief via de bewindvoerder naar de client. Uiteraard moet dan wel afgesproken zijn met de bewindvoerder dat hij/zij de brief (eventueel met uitleg van bewindvoerder) doorgeeft/doorneemt met de client. |  |
| 10 | 2177955 - Verkeerd verzonden e-mail                       | Nee | Nee                                                                                                                                                                                                                                                                                                                                                    |  |
| 11 | 2001032 - Alle documenten iot Djuma worden in PIP getoond | Nee | Nee                                                                                                                                                                                                                                                                                                                                                    |  |
| 12 | 2261727 - Datalek externe partner                         | Nee | Nee                                                                                                                                                                                                                                                                                                                                                    |  |

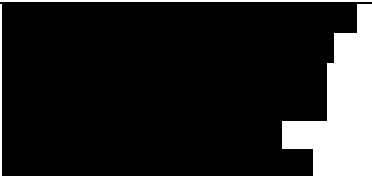
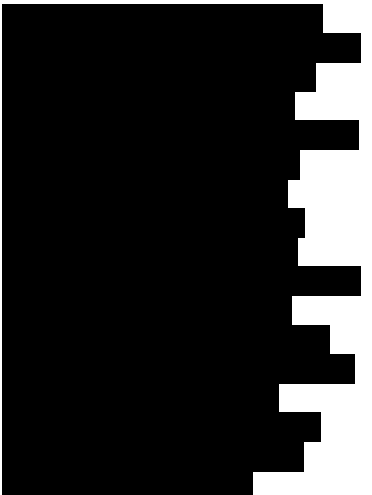
**Bijlage 1A: Overzicht van 21 datalekken in 2023 (2022:16)**

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |     |     |                                                                                      |
|----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|-----|--------------------------------------------------------------------------------------|
| 13 | 2307141 - Datalek melding                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Nee | Nee |   |
| 14 | 2311847 - Datalek melding<br>Max. 5 uur geen anonieme gegevens van betrokken ambtenaren gemeente Weert op de openbare publieke website gemeente Weert                                                                                                                                                                                                                                                                                                                                                                      | Nee | Nee |   |
| 15 | 2187983 - Datalek melding                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Nee | Nee |   |
| 16 | 2279381 - Datalek melding<br>Datalek gemeld bij de gemeente Weert. Er is een brief verstuurd naar het oude woonadres van het gezin (het gezin woont hier al 2 jaar niet meer). Nieuwe bewoners van het huis hebben de brief ontvangen en de oude bewoners op de hoogte gebracht.<br>In de verkeerd verzonden brief wordt aangegeven dat bij de gemeente niet bekend bij welke school het kind ingeschreven staat. De volgende persoonsgegevens staan beschreven in de brief: Voornamen kind, achternaam en oude woonadres. | Nee | Nee |  |

**Bijlage 1A: Overzicht van 21 datalekken in 2023 (2022:16)**

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |     |     |  |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|-----|--|
| 17 | 2262939 - Datalek melding<br>Er is in het verleden een fout gemaakt bij de conversie van de PK (persoonskaart) naar de PL (persoonslijst GBA/BRP). Deze conversie vond plaats in 1989. De betrokkene meldde per mail bij de gemeente dat hij op overheid.nl zag dat bij zijn oudergegevens niet de juiste moeder stond vermeld.                                                                                                                                                                                                                                                                        | Nee | Nee |  |
| 18 | 2094008 - datalek CISO vraagt aan verwerker medewerkers onderzoek hoeveel zakelijke e-mailadressen van medewerkers van gemeente Weert betrokken zijn bij dit incident. Het gaat om 1 e-mailadres.                                                                                                                                                                                                                                                                                                                                                                                                      | Nee | Nee |  |
| 19 | 2148056 - Datalek melding<br>Er is zojuist een datalek gemeld bij het datalekkenteam. Weert heeft in de productieomgeving van de applicatie X-works een testklant opgevoerd. Aan deze testklant is een ad-random BSN gekoppeld, welke bepaald is door testnummers.nl. Er zijn diverse testen uitgevoerd op deze testklant. Nu is gebleken dat dit BSN een daadwerkelijk uitgereikte BSN is, waardoor een natuurlijk persoon een dubbele registratie op haar naam heeft staan. Het gevolg hiervan is dat verschillende instanties (zoals Belastingdienst) geautomatiseerd een melding hebben ontvangen. | Ja  | Ja  |  |

**Bijlage 1A: Overzicht van 21 datalekken in 2023 (2022:16)**

|    |                                                                                                                                                                                                                                                                                                                                                                                 |     |     |                                                                                                                                                                            |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|-----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 20 | <p>2187660 - Datalek melding<br/>1<sup>e</sup> lek betreft dus enkel de zakelijke e-mailadressen van gemeentelijke collega's.</p> <p>2e lek Aan de melder van het datalek is verzocht om de doorgescheurde kopie ID-bewijs in een afgesloten prullenbak weg te gooien.</p>                                                                                                      | Nee | Nee | <br> |
| 21 | <p>2197725 - Datalek melding<br/>besluit tot vestiging van voorkeursrecht gemeenten een bijlage gevoegd waarop de NAW-gegevens van de eigenaren, wie eigenaar en wie half eigenaar is en kadastrale gegevens staan. Kadastrale gegevens zijn op aanvraag en tegen betaling op te vragen bij het kadaster. Daarnaast hebben de burens alleen elkaars NAW-gegevens ontvangen.</p> | Nee | Nee |                                                                                        |

## Bijlage 1B: overzicht (pré) DPIA's

| Onderwerp pré DPIA                                  | Afd, gemeente Weert | Datum | Conclusie: |
|-----------------------------------------------------|---------------------|-------|------------|
| Checklist DPIA Djuma klantcontact (AVG)             |                     | 2020  | ?          |
| Checklist DPIA Sociaal Recherche (AVG/Wpg)          |                     | 2020  | ?          |
| Checklist DPIA Djuma klantcontact Servicepunt (AVG) |                     | 2020  | ?          |

| Onderwerp DPIA                                                                                                                     | Afd, gemeente Weert                     | Datum                                                  | Status                              |
|------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------|--------------------------------------------------------|-------------------------------------|
| DPIA veiligstellen vertrouwelijke gegevens n.a.v. WOB verzoek (AVG)                                                                |                                         | 2020                                                   | Afgerond                            |
| DPIA SQUIT2020 (AVG)                                                                                                               | VTH                                     | 2020                                                   | Afgerond                            |
| X-Works (AVG)                                                                                                                      | Sociaal domein                          | 2021, versie 0.2 opgeleverd door leverancier Blinqt BV | Afgerond                            |
| Pilot Jongeren in Beeld (AVG)                                                                                                      | OCSW - Zorg & Participatie              | 2023                                                   | Afgerond                            |
| Woonkans (AVG)                                                                                                                     | OCSW via beleidsadviseur Sociaal Domein | 2023/2024                                              | Afgerond                            |
| Wams – Wet aanpak meervoudige problematiek Sociaal domein (nieuwe w&r)                                                             |                                         |                                                        | Te prioriteren na voorstel PO/FG/CJ |
| WGS (Wet gegevensverwerking door samenwerkingsverbanden) (nieuwe w&r)                                                              |                                         |                                                        | Te prioriteren na voorstel PO/FG/CJ |
| E-HRM: E-learning en game incl. nieuw platform trainingen Weert een lerende organisatie; nieuwe Personeel Informatie Systeem (PIS) |                                         |                                                        | Te prioriteren na voorstel PO/FG/CJ |

| Onderwerp DPIA                              | Afd, gemeente<br>Weert | Datum | Status                                                                                                            |
|---------------------------------------------|------------------------|-------|-------------------------------------------------------------------------------------------------------------------|
| Makelaar applicatie in de cloud             |                        |       | Te prioriteren na voorstel PO/FG/CJ                                                                               |
| MS Office 365 / Exchange Online in de cloud |                        |       | Te prioriteren na voorstel PO/FG/CJ                                                                               |
|                                             |                        |       |                                                                                                                   |
|                                             |                        |       |                                                                                                                   |
|                                             |                        |       | Te prioriteren na voorstel PO/FG/CJ /<br>In behandeling / Afgerond / Wacht op goedkeuring PO / Wacht op advies FG |