# Voortgangsrapportage AVG

| Algemene gegevens | |
|---|---|
| Organisatie | Gemeente Woensdrecht |
| Registratienummer | FG 001058 |
| Datum | **27 november 2018** |
| Naam Functionaris Gegevensbescherming | |
| Verslagperiode | 2018 |

*De functionaris gegevensbescherming (FG) is een onafhankelijke toezichthouder (ex. art. 37 Algemene verordening gegevensbescherming (AVG), binnen de gemeente Woensdrecht op het gebied van privacy- en informatiebeveiliging. Op basis van art. 39 AVG zijn de FG taken toebedeeld. De FG informeert en adviseert de organisatie over de rustende verplichtingen op basis van de AVG. Voorts ziet de FG toe op naleving van de bepalingen uit de AVG. Tevens adviseert de FG over privacy onderzoeken. Tot slot treedt de FG op als contactpunt naar de landelijke toezichthouder in zaken die verband houden met de verwerking van persoonsgegevens.*

# Inhoud

Inleiding ..... 3

Hoofdstuk 1 Borging ..... 4

Hoofdstuk 2 Basis op orde ..... 5

Hoofdstuk 3 Verdieping ..... 6

Hoofdstuk 4 Beoordeling & risico's en advies ..... 7

Bijlage 1 : Beoordeling register van verwerkingsactiviteiten ..... 7

Bijlage 2: Register van datalekken ..... 8

## Inleiding

De Algemene Verordening Gegevensbescherming (AVG) is een nieuwe Europese wet die in 2016 is aangenomen en waarvan de implementatietermijn op 25 mei 2018 is afgelopen. Vanaf 25 mei 2018 is de AVG van toepassing en heeft hiermee de Wet bescherming persoonsgegevens vervangen. Omdat de AVG een verordening is, heeft deze directe werking in het Nederlandse recht en is omzetting van de AVG in nationale wetgeving niet nodig.

De AVG stelt nieuwe eisen aan het omgaan met en het verwerken van persoonsgegevens. Bestaande rechten en plichten van een betrokkene, maar ook van de verwerkingsverantwoordelijke, worden in de AVG uitgebreid. Tevens biedt de AVG nieuwe verplichtingen. Binnen gemeente Woensdrecht wordt veel gewerkt met persoonsgegevens van burgers, medewerkers en (keten)partners. Persoonsgegevens worden voornamelijk verzameld bij de burgers voor het goed uitvoeren van de gemeentelijke (wettelijke) taken. De burger moet erop kunnen vertrouwen dat gemeente Woensdrecht zorgvuldig en veilig met de persoonsgegevens omgaat.

Deze voortgangsrapportage is bedoeld om het college van B&W op de hoogte te stellen van de voortgang ten aanzien van de waarborging van de AVG.

Hierbij wordt in hoofdstuk 2 de structurele borging van privacy door gemeente Woensdrecht beschreven. Vervolgens wordt in hoofdstuk 3 de nakoming van de belangrijkste verplichtingen uit de AVG uiteengezet onder het mom van '*de basis op orde*'. In hoofdstuk 4 wordt verdiepend ingegaan op specifieke verplichtingen uit de AVG en de consequenties voor gemeente Woensdrecht. Deze voortgangsrapportage wordt in hoofdstuk 5 afgesloten met een beschrijving van, en een advies over, aanwezige risico's ten aanzien van de omgang met persoonsgegevens.

27 november 2018

Functionaris Gegevensbescherming

## Hoofdstuk 1 Borging

*1. Strategische borging*

Op strategisch niveau wordt vooral aandacht besteed aan de aandachtsgebieden: Strategie en Beleid.

*1.1. Strategie*

Vanaf 25 mei 2018 is de AVG van toepassing en heeft hiermee de Wet bescherming persoonsgegevens vervangen. De AVG stelt nieuwe eisen aan het omgaan met en het verwerken van persoonsgegevens. Bestaande rechten en plichten van een betrokkene, maar ook van de verwerkingsverantwoordelijke, worden in de AVG uitgebreid. De gemeente Woensdrecht heeft als doel de AVG juist te implementeren in de bedrijfsvoering. Met deze aanpak is de voor de buitenkant alles op orde.

*1.2. Beleid*

| **Vaststellingsproces privacybeleid** | |
|---|---|
| Akkoord MT | - Geen datum beschikbaar |
| Vaststelling college van B&W | - 6 februari 2018 |
| Bekendmaking | - 16 mei 2018 |
| Inwerkingtreding | - 25 mei 2018 |
| Evaluatie | - Op te pakken in 2019 |

*Tactische borging*

Op tactisch niveau wordt vooral aandacht besteed aan de aandachtsgebieden: inrichting van de organisatie, de inzet van medewerkers, de toewijzing van middelen.

*1.3. Inrichting organisatie en management van de uitvoeringsprocessen*

De gemeente Woensdrecht heeft in een vroegtijdig stadium de noodzaak erkend te anticiperen op de AVG. Deze wet werd van 25 mei 2018 van kracht. Kwartiermakers hebben het 10 stappenplan van de Autoriteit Persoonsgegevens geïmplementeerd. Daarmee was de gemeente in eerste instantie op orde.

Alle afdelingen hebben een bestand van gegevensverwerkingen opgeleverd. Het management is eigenaar van het bestand en zal dit met regelmaat aanvullen en actualiseren.

Daarnaast zijn er op de afdelingen bewustwordingsbijeenkomsten gehouden en is er een privacy en informatieveiligheidsmarkt georganiseerd.

*1.4. Inzet van medewerkers*

Per 1 april is er een Functionaris Gegevensbescherming (FG) benoemd. Deze is door middel van een aanwijzingsbesluit van College en Raad in uitvoering gezet. Er is een Privacy Team samengesteld. Daarnaast is een Privacy Beheerder benoemd als voorzitter van het privacy team. Het Privacy Team bevat vertegenwoordigers uit diverse geledingen van de organisatie. Het Privacy Team volgt een werkprogramma, op initiatief van de privacy beheerder en met instemming door het leidinggevend kader.

*1.5. Toewijzen van middelen*

Om de implementatie van de AVG op gang te brengen zijn er kwartiermakers aangesteld. De formatie is uitgebreid om daarmee de FG in dienst te laten treden. Tot slot is budget voor een Privacy Beheerder opgenomen in de formatie. Ook is er een budget toegekend aan de FG. Dit budget is bedoeld voor scholing, applicaties en andere acties om de kennis en het besef te vergroten.

## Hoofdstuk 2 Basis op orde

1. *Register van verwerkingsactiviteiten*
   Het register van gegevensverwerkingen is door de kwartiermakers Q2 2018 afgerond. Het register is een dynamisch product en mutaties dienen steeds opgenomen te worden in het register. Het lijn management is verantwoordelijk voor het bijhouden van het register. In Q4 2018 is de managers gevraagd het register een kwalitatieve- en kwantitatieve slag te geven. De verdieping in bestanden van applicaties uitgebreid naar fysieke bestanden. De oplevering zal nog doorlopen in Q1 2019. Per 2019 wordt ernaar gestreefd om per kwartaal actualisatie vast te leggen.

2. *Meldplicht datalekken en register van datalekken*
   Er is een register van datalekken opgesteld. Dit is een opsomming van historische gemelde datalekken. In 2018 is er één datalek gemeld.

3. *Functionaris gegevensbescherming*
   Per 1 april is de Functionaris Gegevensbescherming in dienst getreden. Hij is tevens als zodanig aangemeld bij de AP. De FG is bekend gemaakt op intranet voor medewerkers en op de website voor bewoners en derden. Daarnaast is er een stagiaire aangesteld voor 4 maanden die tijdelijk de functie vervult van Privacy Beheerder. Het privacy programma PRO! (Privacy Raakt Ons) gelanceerd. Tevens is de OR betrokken in deze organisatie verandering.

4. *Externe gegevensdeling*
   Er vindt externe gegevensdeling plaats met diverse partijen. De gemeente heeft een privacy beleid opgesteld en gepubliceerd. Daar waar dit verwerkers betreft is hiervoor een verwerkingsovereenkomst op te stellen. Als er sprake is van een gedeelde verwerkingsverantwoordelijkheid behoort privacy in een contract geregeld te worden. Voor de toetsing van de verwerkingsovereenkomsten is een medewerker met juridische achtergrond opgesteld. Momenteel vindt er een inhaalslag plaats op de toetsing van verwerkingsovereenkomsten.
   Daarnaast wordt gekeken of alle benodigde verwerkingsovereenkomsten aanwezig zijn. Ook bij het aangaan van nieuwe uitwisseling van persoonsgegevens zal er aandacht moeten zijn voor de contractuele vastlegging van afspraken omtrent de uitvoering van de AVG.

## Hoofdstuk 3 Verdieping

1. *Rechten van betrokkenen*

   De gemeente Woensdrecht is verplicht om uitvoering te geven aan de rechten van betrokkenen. Om de procesgang te borgen is een uitgebreid stilgestaan bij de wijze van aanpak. Q1 zal deze procesgang worden uitgerold. In 2018 is er 1 verzoek ontvangen met het recht op vergetelheid.

2. *DPIA*

   Er zijn een 2-tal DPIA's opgesteld. Te weten voor het Sociaal Domein, en Corsa.

   Deze DPIA's zijn gedeeld met verantwoordelijk management, welke aan de slag zijn gegaan met de verbetervoorstellen. In de loop van 2019 worden hiervan de resultaten verwacht.

   Mooi initiatief binnen het Sociaal Domein is dat er een verdiepingsslag gemaakt op het privacy beleid geënt op de specifieke werkzaamheden. Dit hulpmiddel word momenteel getoetst op juistheid.

3. *Privacy door ontwerp en standaard instelling*

   Er zijn diverse voorbeelden waarbij privacy door ontwerp is gehanteerd. Een voorbeeld is de kwaliteitstoetsing in de jeugdzorg. Gemeente Roosendaal heeft de FG's van de betrokken gemeenten meegenomen in de aanpak. Er zijn verbeter voorstellen gedaan en CJG is hiermee aan de slag gegaan. In Q1 2019 wordt de voorgestelde werkwijzen aan de betrokken gemeenten voorgelegd.

   Het is van belang dat de FG en CISO vaker eerder betrokken worden bij nieuwe ophanden zijnde processen, zodat privacy en informatieveiligheid in een vroegtijdig stadium de aandacht krijgen. Deze werkwijze begint zijn vruchten af te werpen.

4. *Beveiligingseisen*

   De gemeente dient passende maatregelen te nemen om de persoonsgegevens voldoende te beveiligen. Daartoe wordt bij vraagstukken omtrent beveiliging vroegtijdig de CISO ingeschakeld. De FG werkt intensief samen met de CISO. De rolverdeling tussen de FG, PB, CISO en eigenaar is in document vastgelegd.

5. *Verwerkingsbeginselen*

   De gemeente dient te voldoen aan de verwerkingsbeginselen. Om de persoonsgegevens te mogen verwerken zal één van de 6 grondslagen van toepassing verklaard moeten worden. Bij de gemeente is dit vaak de wettelijke verplichting. Maar ook algemeen belang en gerechtvaardigd belang komt voor. De grondslagen Overeenkomst, Vitaal belang en (zuivere) Toestemming komen nauwelijks voor.

   Vaak is de wijze van omgang met privacy al vastgelegd in de voorliggende wetten, zie bijvoorbeeld art 7 van de jeugdwet.

   De gemeente dient zich bij iedere verwerking van persoonsgegevens af te vragen uit hoofde van welke grondslag de verwerking plaatsvindt. Daarnaast is de doelbepaling van bepaling van belang. In relatie tot het doel dient de verwerking van persoonsgegevens proportioneel te zijn. (dataminimalisatie) Tot slot speelt de subsidiariteit een rol. Hiermee wordt bedoeld dat de minst ingrijpende manier om het doel te bereiken wordt gebruikt.

## Hoofdstuk 4 Beoordeling & risico's en advies

### Bijlage 1 : Beoordeling register van verwerkingsactiviteiten

| Beoordelingscriteria register van verwerkingsactiviteiten | | Toelichting |
|---|---|---|
| **Formele vereisten** | | |
| 1.1 | Naam en contactgegevens verwerkingsverantwoordelijke | Het verwerkingsregister is opgemaakt per afdeling. In de kop staat de verantwoordelijk manager als eigenaar benoemd. |
| 1.2 | Naam en contactgegevens FG | De FG is zichtbaar op de website |
| 1.3 | Naam en contactgegevens eventuele gezamenlijke verwerkingsverantwoordelijken en eventuele FG | De situatie waarin er sprake is van gezamenlijke verwerkingsverantwoordelijke heeft onvoldoende aandacht gehad. Door voortschrijdend inzicht heeft doen inzien dat deze vorm beter ingebed moet worden met afspraken en een verwerkingscontract. |
| 1.4 | Verwerkingsdoeleinden | De verwerkingsdoelen zijn bij iedere verwerking gedefinieerd. |
| 1.5 | Categorieën van betrokkenen | De categorieën van betrokkenen zijn steeds benoemd. |
| 1.6 | Ontvangers en derde partijen | Ontvangers zijn benoemd. Deze bevatten ook de derden partijen. |
| 1.7 | Beschrijving beveiligingsmaatregelen | Technische en organisatorische maatregelen zijn opgenomen. |
| 1.8 | Bewaar- en vernietigingstermijnen | Bewaartermijn is opgenomen. In de praktijk dienen de vernietigingstermijnen eerbiedigt te worden. |
| 1.9 | Doorgifte aan een derde land of internationale organisatie | Er is geen onderscheid gemaakt naar derde land of organisatie. Dit dient wel opgenomen te worden omdat er sterke banden zijn met Belgische gemeenten. |
| **Inhoudelijke vereisten** | | |
| 1.10 | Het register is in schriftelijke vorm, waaronder in elektronische vorm, opgesteld | Het register is opgesteld in Excel. |
| 1.11 | Het register is volledig | Het register is een eerste oplevering en verdieping en verbreding is noodzakelijk en is Q4 2018 uitgezet onder de managers (eigenaren) |
| 1.12 | Het register is actueel | Nee, het register is opgesteld in Q1 2018 door kwartiermakers. Er is onvoldoende bewustwording bij eigenaren dat dit een dynamisch document is. Hieraan wordt gewerkt door in Q4 een en ander opnieuw onder de aandacht te brengen van de eigenaren. |
| 1.13 | Het register is intern toegankelijk | Het register is niet intern toegankelijk. Uitsluitend voor medewerkers van privacy. Aan een ontsluiting wordt gewerkt. |
| 1.14 | Het register is voor de betrokkene toegankelijk | Ja, betrokkenen hebben toegang op een directory. Voor privacy. |

Toelichting:

Opmerkingen FG: Het verwerkingsregister is opgesteld door de kwartiermakers Q4 2017 en Q1 2018. De FG constateerde dat de beleving bij het dynamisch karakter van de registers onvoldoende is. Daartoe is er in Q4 een bewustwordingstraject gestart met de verantwoordelijke eigenaren (managers) De gelegenheid is gebruikt om meteen een kwalitatieve en kwantitatieve slag te maken. Tot slot is aangegeven dat de privacy beheerder steeds per kwartaal geactualiseerde lijsten zal opvragen. Al met al concludeert de FG dat we goed op weg zijn. Met een complexe organisatie als een gemeente is er echter ook nog veel op te pakken. Daartoe is er een werkplan gepresenteerd en gaat in 2019 en volgende uitgerold worden.

**Bijlage 2: register van datalekken**

| **Beoordelingscriteria register van datalekken** | | |
|---|---|---|
| 1.1 | Feiten omtrent de inbreuk in verband met persoonsgegevens | In 2018 is er slechts 1 inbreuk geregistreerd. Het lijkt erg onwaarschijnlijk dat er niet meer datalekken aan de orde zijn geweest. Verdere bewustwording tot het melden van incidenten is van belang. |
| 1.2 | De gevolgen van het datalek | Het betreft een verloren geraakt poststuk. Er is geen signaal gekomen van misbruik. |
| 1.3 | Genomen corrigerende maatregelen | Verzending heeft correct plaatsgevonden |
| 1.4 | Melding aan de betrokkene | Er is overleg geweest met de betrokkene |
| **Inhoudelijke vereisten** | | |
| 1.5 | Het register is volledig | Het lijkt erop dat er in de organisatie meer inbreuken bekend zouden moeten zijn. In 2019 wordt door middel van de leercirkel hier verder aandacht aan gegeven. |
| 1.6 | Het register is actueel | Ja, zodra een inbreuk zich voordoet en wordt gemeld, wordt dit in het register opgenomen en worden alle vragen in het sjabloon beantwoord. |

Opmerkingen FG:

| |
|---|
| Voor het register van datalekken geldt dat dit is opgesteld door de kwartiermakers. Dit register zal verder ontwikkeld gaan worden.<br>Het protocol data lekken is herschreven en zal Q1 2019 worden uitgerold. Daarnaast zal de leercirkel de awareness gemeente breed worden uitgerold.<br>Als deze activiteiten moeten er toe leiden dat er meer aandacht is voor datalekken en de correcte verwerking ervan. |