

**Algemene Verordening Gegevensbescherming**

# Stand van zaken en aanbevelingen

Naar aanleiding van de resultaten van de nulmeting van 25 oktober 2018

Mr. N. (Nadia) Benaissa, Functionaris Gegevensbescherming  
29-11-2018

## 1. Aanleiding

In september 2018 heeft Privacy Management Partners in opdracht van de functionaris gegevensbescherming een nulmeting verricht, waarbij onderzocht is wat binnen de Gemeente Breda de stand van zaken is met betrekking tot de implementatie van de AVG en welke uitdagingen nog voor ons liggen. Er is daarbij ook verzocht om aanbevelingen en verbeterpunten.

In november zijn de resultaten van de nulmeting opgeleverd (bijlage 1). In dit stuk wordt er ingegaan op de beoordelingen en verbeterpunten die door Privacy Management Partners zijn aangedragen en geeft de functionaris gegevensbescherming daar een reactie op. Daarnaast wordt er stil gestaan bij verbeterpunten naar inzicht van de functionaris gegevensbescherming en wordt er een voorstel gedaan voor een praktische, uitvoerbare en meetbare groei in effectieve bescherming van persoonsgegevens.

## 2. Resultaten nulmeting

De nulmeting heeft op 11 september 2018 plaatsgevonden, tijdens een bijeenkomst onder leiding van Privacy Management Partners. De CISO, afdelingshoofd ICO, teamleider iRegie en Communicatie, Concern Control, kwaliteitsmedewerker Sociaal Domein en de functionaris gegevensbescherming waren de aanwezigen. Er is eerst een presentatie gehouden over algemene aspecten van de AVG, vervolgens is de nulmeting uitgevoerd. De resultaten heeft de Gemeente Breda op 25 oktober 2018 ontvangen.

Het gehanteerde beoordelingskader richtte zich op een tiental prestatie-indicatoren. Aan de hand van de indicatoren zijn er 'goede punten' en 'verbeterpunten' beschreven. Hieronder worden zowel de goede als verbeterpunten kort beschreven. Voor een uitgebreide beschrijving wordt verwezen naar de resultaten van de nulmeting zoals beschreven in het document 'AVG: hoe nu verder? Stand van zaken en aanbevelingen', van Privacy Management Partners (bijlage 1).

### 1. Bestuurlijk beleid

De Gemeente Breda beschikt sinds 2016 over een privacybeleidskader. Dit beleidskader is echter niet bestuurlijk vastgesteld.

### 2. Regie en support

Er is een portefeuillehouder voor AVG-aangelegenheden. De functionaris gegevensbescherming en de portefeuillehouder voeren periodiek overleg. Daarnaast is er een ondersteuningsteam met (sinds kort) een privacy coördinator. Ook wordt er samengewerkt met privacy ambassadeurs binnen afdelingen. Als verbeterpunt wordt er meegegeven dat er aangesloten kan worden bij het bredere risicobeleid van de Gemeente Breda.

### 3. Toezicht

Er is een functionaris gegevensbescherming, maar is er nog onvoldoende scheiding tussen uitvoering en toezicht. Daarnaast dient er ruimte te zijn om als persoon en als positie te groeien.

### 4. Werkprogramma

Er is een implementatieplan dat uitgaat van de aanbevelingen vanuit de Autoriteit Persoonsgegevens en met aspecten voor verdere bewustwording. Het plan mist echter bestuurlijke en operationele risicosturing en verbinding met bestuurlijke verantwoording conform het privacybeleidskader. Geadviseerd wordt de aanbevelingen van de Autoriteit Persoonsgegevens te laten varen en het 'dashboard specifieke aandachtsgebieden', ontwikkeld door Privacy Management Partners, te hanteren en van daaruit de aandachtsgebieden te prioriteren.

### 5. Ketenregie

Dit onderdeel hangt samen met het hierboven beschreven dashboard specifieke aandachtsgebieden. Omdat de Gemeente Breda zich hier niet op deze wijze op gericht heeft, is dit punt niet beoordeeld.

### 6. Privacy by design

Privacy Management Partners beoordeelt privacy bij design op basis van privacy impact assessments. De Gemeente Breda gaat hier op een andere manier mee op. Ook dit onderdeel is niet beoordeeld.

### 7. Verzoeken, klachten en incidenten

De Gemeente Breda beschikt over een loket voor uitoefening van AVG-rechten door burgers en er wordt gewerkt aan een behandelprotocol voor een meer gestructureerde aanpak. Er wordt aangeraden te controleren op slagvaardigheid en kwaliteit.

### 8. Communicatie & training en opleiding

Er zijn initiatieven genomen op het gebied van bewustwording, maar het ontbreekt aan een opleidingsprogramma.

### 9. Informatiebeveiliging

De Gemeente Breda hanteert informatiebeveiligingsbeleid conform de richtsnoeren van de IBD en beschikt over een informatiebeveiligingcoördinator. De informatiebeveiliging sluit echter nog niet doelbewust aan op AVG-risico's.

### 10. Budget

Er is budget, maar nog geen budgettering. De AVG-aanpak dient vast onderdeel te zijn van de jaarlijkse begroting. Geadviseerd wordt om de kosten op basis van personele kosten en ambities volgens bovenstaande tien punten te begroten.

## 3. Reactie functionaris gegevensbescherming

Het doel van de nulmeting was om van een externe organisatie die ervaring heeft bij verschillende gemeenten een eerste indruk te krijgen hoe de Gemeente Breda ervoor staat. De nulmeting was derhalve geen diepgravend onderzoek, maar een manier om 'de temperatuur te meten' en de organisatie een spiegel voor te houden. Hebben we aandacht voor de juiste aspecten of missen we belangrijke zaken? Privacy Management Partners heeft zich daarover uitgesproken. Uitgaande van het overzicht onder 'goede punten' lijkt de Gemeente Breda gemiddeld te scoren. Er zijn nog veel verbeterpunten, maar er zijn ook al stappen gezet. De Gemeente Breda is nog volop in ontwikkeling en op het gebied van privacy een lerende organisatie. De verbeterpunten kunnen helpen richting te geven in die ontwikkeling. De functionaris gegevensbescherming onderschrijft veel van de aangedragen verbeterpunten. Zoals echter bij een niet-diepgravend onderzoek te verwachten is, ontbreekt het bij de beoordeling aan context. Daarnaast lijken bepaalde verbeterpunten gepaard te gaan met commerciële belangen die niet altijd in verhouding lijken te staan tot de organisatiebelangen en de belangen van betrokkenen. Hieronder wordt daarom door de functionaris gegevensbescherming ingegaan op de besproken punten en wordt haar visie, naast de visie van Privacy Management Partners gelegd.

### 1. Bestuurlijk beleid

Het privacybeleidskader is op initiatief van de voormalige functionaris gegevensbescherming tot stand gekomen met behulp van Privacy Management Partners. Onlangs ontving de huidige functionaris gegevensbescherming het bericht dat het privacybeleidskader niet bestuurlijk is vastgesteld. Dit dient alsnog zo spoedig mogelijk te worden gedaan. Het beleidskader dient als vertrekpunt voor de organisatie waarin de uitgangspunten met betrekking tot de bescherming van persoonsgegevens en de daarbij behorende verantwoordelijkheden verankerd worden. Nu er een privacybeleidskader is, kan dit bestuurlijk worden vastgesteld. Er kan echter ook voor gekozen worden het beleidskader op punten aan te passen. Er wordt nog gesproken in verouderde termen (Wet bescherming persoonsgegevens in plaats van Algemene Verordening Gegevensbescherming). Daarnaast sluit het model van Privacy Management Partners niet naadloos aan op de werkwijze van de Gemeente Breda. Bij voorkeur wordt het beleid herzien en op punten aangepast alvorens het bestuurlijk wordt vastgesteld. Dit dient echter met prioriteit te worden opgepakt om verdere vertraging te voorkomen en uiterlijk in Q1 2019 te worden aangeboden.

### 2. Regie en support

Op het onderdeel regie en support scoort de Gemeente Breda relatief hoog (2,5 van de 4 punten). Het onderwerp is onder de aandacht bij de portefeuille houdende wethouder en er is regelmatig overleg tussen de functionaris gegevensbescherming en de wethouder. Ook is bescherming van persoonsgegevens vast onderdeel geworden van het stafoverleg bedrijfsvoering. De functionaris gegevensbescherming is aangesloten bij afdeling concern control, waardoor de onafhankelijkheid beter geborgd wordt. Terecht wordt (onder punt 3 Toezicht) opgemerkt dat de functionaris gegevensbescherming nog verder in haar rol moet groeien. Het afgelopen jaar is er ruimte geweest voor opleiding en het opzetten van een netwerk. Daar is ook gebruik van gemaakt.

De functionaris gegevensbescherming heeft veel afdelingen bezocht in het kader van bewustwording en om op te halen waar medewerkers tegenaan lopen bij de bescherming van persoonsgegevens. Naar mate de bewustwording groter werd, steeg het aantal vragen binnen de organisatie. De functionaris gegevensbescherming heeft er steeds voor gewaarschuwd dat er onvoldoende medewerkers waren om aan de behoefte van de organisatie te voorzien. Dat bracht ook met zich mee dat de functionaris gegevensbescherming te veel betrokken werd bij de uitvoering. Hoewel zij steeds alert is geweest op haar rol en haar beperkte mogelijkheden bij advies (om daarna nog zuiver toezicht te kunnen houden), zijn er door de functionaris gegevensbescherming ook zaken opgepakt die elders belegd hadden moeten worden. Denk daarbij aan het implementatieplan, beantwoording van eerstelijns vragen, ontwikkeling van beleid en formats en bewustwording. Dat gaat ten kosten van de werkzaamheden die de functionaris gegevensbescherming zou moeten uitvoeren (met name toezicht) en vertroebelt de verschillen in rollen en functies die binnen een organisatie als de Gemeente Breda nodig zijn om persoonsgegevens van burgers afdoende te beschermen en gehoor te geven aan de vraag naar begeleiding en ondersteuning vanuit de organisatie, alsmede de behoefte vanuit het bestuur om in control te zijn.

Inmiddels zijn er naast de functionaris gegevensbescherming (parttime) privacy adviseurs en een privacy coördinator. De praktijk wijst echter uit dat dit onvoldoende is om de organisatie voldoende te begeleiden, waardoor zaken onnodig lang blijven liggen. Uiteraard heeft dit effect op de AVG-risico's, waaronder datalekken. De functionaris gegevensbescherming is dan ook van mening dat de Gemeente Breda nog onvoldoende scoort op het gebied van regie en support.

### 3. Toezicht

De functionaris gegevensbescherming informeert en te adviseert over AVG-verplichtingen en houdt toezicht op de naleving daarvan. Daarnaast werkt de functionaris gegevensbescherming samen met de Autoriteit Persoonsgegevens, waarvoor zij ook als contactpunt optreedt (art. 39 AVG). Daarvoor moet de functionaris gegevensbescherming "tijdig en naar behoren worden betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens" (art 38 AVG). De functionaris gegevensbescherming mag geen instructies ontvangen en legt rechtstreeks verantwoording af aan de hoogste leidinggevende.

Hoewel de rol en van functionaris gegevensbescherming relatief nieuw is, ervaart de functionaris gegevensbescherming dat binnen de organisatie, zowel op bestuurlijk als ambtelijk niveau, de onafhankelijkheid en autonomie voldoende gewaarborgd wordt. De functionaris gegevensbescherming wordt binnen alle hiërarchische lagen betrokken en mengt zich actief in aangelegenheden die de bescherming van persoonsgegevens betreffen. Daarvoor worden er contacten gelegd op uitvoeringsniveau, maar ook op management, directie en bestuurlijk niveau. Indien nodig zijn er mogelijkheden om risico's en aandachtspunten snel bij de juiste personen onder de aandacht te brengen.

De functionaris gegevensbescherming ervaart voldoende faciliteiten om verder te ontwikkelen, echter, door het tekort aan medewerkers op het gebied van privacy, te weinig ruimte om haar eigen taken naar behoren uit te kunnen voeren. Haar voornaamste zorg is dat er onvoldoende ruimte is voor proactieve toezicht in zaken er werkwijzen die niet door medewerkers binnen de organisatie onder haar aandacht worden gebracht.

### 4. Werkprogramma

Privacy Management Partners adviseert het stappenplan van de Autoriteit Persoonsgegevens los te laten en gebruik te maken van hun werkplan. Ook zou het huidige implementatieplan bestuurlijke en operationele risicosturing missen.

Het stappenplan van de Autoriteit Persoonsgegevens zijn 'harde' eisen waaraan organisaties moeten voldoen. Het zijn ook aspecten waar de Autoriteit Persoonsgegevens actief toezicht op houdt. Dit los laten zou een slecht idee zijn. In het implementatieplan van de functionaris gegevensbescherming wordt echter wel aangegeven dat het stappenplan van de Autoriteit Persoonsgegevens nog onvoldoende aandacht heeft voor hoe er inhoudelijk met persoonsgegevens wordt omgegaan. De waarnemingen van de functionaris gegevensbescherming waren in april 2018 dat er binnen de organisatie te weinig zicht is op de persoonsgegevens die verwerkt worden, met welk doel en met welke grondslag. Ook bleek er niet genoeg aandacht te zijn voor juiste autorisaties en het handhaven van bewaartermijnen. Op inzageverzoeken konden medewerkers moeilijk een antwoord formuleren door gebrek aan overzicht. Kortom er was een tekort aan gegevensmanagement. Gegevensmanagement is breder dan de bescherming van persoonsgegevens, maar zonder gegevensmanagement ontstaan er direct risico's op het gebied van bescherming van persoonsgegevens. Indien afdelingen te weinig zicht hebben op de processen waarin persoonsgegevens verwerkt worden en de medewerkers en samenwerkingspartners die hierbij betrokken zijn, is er ook te weinig zorg voor een juiste werkwijze. Andersom kan inzicht en overzicht bijdragen aan het in kaart brengen van risico's en aandachtspunten. Daarnaast kan gegevensmanagement dienen als fundament voor verdere (periodieke) onderzoeken naar compliance. Als de basis goed gelegd wordt, is het daarna een kwestie van bijhouden. Op dit moment ontbreekt het echter nog aan een solide basis. Nu dit voor een groot deel van de organisatie geldt, bestaat het implementatieplan uit een voorstel om hier met de belangrijkste afdelingen in groepsverband aan te werken. Met de overige afdelingen kan bilateraal worden gewerkt. De stappen worden binnen het groepsverband met de privacy ambassadeurs onder leiding van de privacy coördinator gelijktijdig gezet, zodat afdelingen samen kunnen optrekken, van elkaar kunnen leren en niet steeds zelf het wiel hoeven uit te vinden.

Er zijn gemeenten die kiezen voor de aanpak die door Privacy Management Partners wordt voorgesteld, waarbij geprioriteerd wordt in afdelingen, welke één voor één worden aangevlogen. Die prioritering kan nuttig zijn wanneer er ernstige risico's zijn binnen bepaalde afdelingen waarbij verbeteringen snel gewenst zijn. Daar staat tegenover dat andere afdelingen langer moeten wachten. De Gemeente Breda is een grote organisatie en de werkzaamheden die verricht dienen te worden om in de basis aan de AVG te voldoen zijn talrijk. Overigens worden er binnen de Gemeente Breda indien nodig uitzonderingen gemaakt. Met afdeling Jeugd wordt een versneld en individueel traject aangegaan.

### 5. Ketenregie

Dit onderdeel hangt samen met het werkprogramma. Omdat de Gemeente Breda een ander werkprogramma gebruikt, is dit onderdeel niet beoordeeld.

Een manier voor Privacy Management Partners om de risico's en verbeterpunten binnen ketens in te schatten is het uitvoeren van Privacy Impact Assessments (PIA's). Door middel van uitvoerige vragenlijsten worden verschillende aspecten die betrekking hebben op de bescherming van persoonsgegevens beoordeeld, waarna er aanbevelingen kunnen worden gedaan. PIA's zijn echter bedoeld (en verplicht) voor (waarschijnlijk) risicovolle verwerkingen die gelet op de technologieën, aard, omvang en doeleinden aandacht behoeven (art. 35 AVG). Een PIA dient dan ook verricht te worden vóór afgaand aan een verwerking en richt zich dus op nieuwe verwerkingen. Het uitvoeren van een PIA is arbeidsintensief en vraagt veel van medewerkers. De functionaris gegevensbescherming geeft daarom alleen opdracht tot het verrichten van een PIA indien dat noodzakelijk is op grond van de AVG.

De Gemeente Breda heeft een eigen gebruiksvriendelijke PIA ontwikkeld die medewerkers zelf kunnen uitvoeren met ondersteuning van privacy medewerkers en advies van de functionaris gegevensbescherming. Er zijn echter veel organisaties die dit onderdeel uitbesteden omdat zij niet de expertise, capaciteit en tools ter beschikking hebben. Privacy Management Partners is een organisatie die hierin ondersteunt

De functionaris gegevensbescherming is lid van het Nederlands Genootschap Functionarissen Gegevensbescherming, een beroepsvereniging waarbij regelmatig bijeenkomsten georganiseerd worden. Tijdens zo'n bijeenkomst werd afgeraden PIA's uit te voeren voor afdelingen en reguliere verwerkingen, omdat PIA's daar niet voor bedoeld zijn. De functionaris gegevensbescherming is ook van mening dat PIA's voor elke afdeling of keten een afschrikwekkend effect kunnen hebben op het concept. Daarnaast zijn er effectievere manieren te bedenken om de risico's binnen de organisatie in kaart te brengen. De functionaris gegevensbescherming is het afgelopen jaar in gesprek gegaan met verschillende teams om daar een indruk van te krijgen. Met het implementatieplan worden de belangrijkste risico's onder handen genomen.

### 6. Privacy by design

Ook bij dit onderdeel gaat het werkprogramma van Privacy Management Partners uit van resultaten uit PIA's, waar dat niet de bedoeling van de AVG lijkt te zijn. De AVG spreekt over technische en organisatorische maatregelen die getroffen worden om gegevensbeschermingsbeginselen op een doeltreffende manier uit te voeren en de nodige waarborgen in de verwerking in te bouwen ter bescherming van de rechten van betrokkenen (art. 25 AVG). Daarbij moet rekening gehouden worden met de stand van de techniek, uitvoeringskosten en de aard, omvang, context en het doel van de verwerking alsmede met de waarschijnlijkheid dat risico's zich voordoen.

Privacy by design komt dus neer op maatwerk. De Gemeente Breda maakt hierbij onderscheid tussen reguliere werkzaamheden en nieuwe projecten. Privacy by design bij reguliere werkzaamheden is de kerntaak van de privacy ambassadeurs, onder leiding van de privacy coördinator. Alle verwerkingen van persoonsgegevens dienen onder de loep genomen te worden en er moet worden vastgelegd hoe gegevens op een zorgvuldige en veilige manier verwerkt kunnen worden. Die afspraken dienen terug te komen in de privacyverklaringen. Autorisaties en het handhaven van bewaartermijnen dienen die afspraken te ondersteunen.

Bij nieuwe projecten dient er een privacy adviseur en de functionaris gegevensbescherming geraadpleegd te worden. Er wordt een verantwoordingsdocument ingevuld waarin wordt aangegeven welke persoonsgegevens er verwerkt worden, met welk doel en op basis van welke grondslag. Ook dient er worden ingegaan op de beveiligingsmaatregelen die genomen worden om de persoonsgegevens te beschermen. De privacy adviseur ondersteunt bij het invullen van het verantwoordingsdocument. De functionaris gegevensbescherming schat de risico's van de verwerking in en adviseert over verbeteringen en informeert de verwerkingsverantwoordelijke over mogelijke risico's. Indien op basis van het verantwoordingsdocument wordt ingeschat dat de verwerking mogelijk een hoog risico inhoudt, wordt er opdracht gegeven tot het verrichten van een PIA. Het doel daarvan is de risico's volledig in kaart te brengen en tot maatregelen te komen die de risico's uitsluiten of beperken.

Privacy by design is essentieel voor effectieve bescherming van persoonsgegevens. De verwerkingen van persoonsgegevens verschillen binnen de Gemeente Breda inhoudelijk erg veel van elkaar omdat de organisatie steeds met andere wetgeving te maken heeft. De doeleinden en de categorieën persoonsgegevens (van NAW-gegevens tot medische en strafrechtelijke gegevens) zijn uiteenlopend en vragen naast de algemene regels van de AVG om op maat ontworpen maatregelen. Te weinig aandacht op dit vlak verhoogt automatisch de risico's voor betrokkenen en daarmee voor de organisatie. Door middel van bewustwording en de privacy ambassadeurs wordt getracht het belang hiervan steeds onder de aandacht te brengen. De aanpak zou echter meer sluitend zijn als het ook een vast onderdeel wordt bij inkooptrajecten en collegebesluiten.

### 7. Verzoeken, klachten en incidenten

De Gemeente Breda scoort op dit vlak het hoogst volgens Privacy Management Partners. Het ontbreekt de Gemeente Breda echter nog aan een werkplan, hoewel deze wel in ontwikkeling is. De functionaris gegevensbescherming onderschrijft het advies van Privacy Management Partners om te controleren op slagvaardigheid en kwaliteit. De coördinatie van de AVG-verzoeken is onlangs verplaatst van publiekszaken naar de privacy coördinator. Het proces is



nog in ontwikkeling en er wordt nog erg gezocht naar een juiste afwikkeling van de verzoeken. De rechten van betrokkenen zijn onder de AVG sterk. Betrokkenen kunnen direct een klacht indienen bij de Autoriteit Persoonsgegevens indien niet of onvoldoende gehoor wordt gegeven aan een AVG-verzoek. De Autoriteit Persoonsgegevens heeft eerder dit jaar een dwangsom opgelegd nadat een organisatie niet volledig voldeed aan een inzageverzoek.<sup>1</sup> De ontwikkeling van de werkwijze dient daarom niet te lang op zich te laten wachten en bij voorkeur in Q1 2019 gereed te zijn.

### 8. Communicatie & training/opleiding

De Gemeente Breda heeft een privacy coördinator aangenomen om de bewustwording binnen de organisatie te verzorgen. Er is ook veel behoefte aan bewustwording, blijkt uit de uitnodigingen die de functionaris gegevensbescherming het afgelopen jaar heeft gekregen (en aangenomen). Medewerkers willen graag weten wat de nieuwe wetgeving voor hen betekent en hoe ze op een goede manier met persoonsgegevens om kunnen gaan. Medewerkers vrezen soms ook dat onder de AVG 'niets meer mag', waardoor hun werk erg ingewikkeld zou kunnen worden. Op basis van de ervaringen in het afgelopen jaar, waarbij de functionaris gegevensbescherming diverse teams bezocht heeft, adviseert zij persoonlijk contact met medewerkers waarbij bewustwordingsworkshops zowel een informerend als een interactief karakter hebben. Door middel van een presentatie kunnen medewerkers kennis maken met de AVG en met behulp van vragen en voorbeelden kunnen ze zelf nadenken over hoe zij vinden dat de wet een plek kan krijgen binnen hun werkzaamheden.

Bewustwording dient een terugkerend onderdeel te zijn om het bewustzijn hoog te houden. Daarnaast dient bewustwording in stappen doorlopen te worden. Na de basis kan er dieper worden ingegaan op bepaalde onderdelen, met aandacht voor de uitdagingen binnen de organisatie en de ontwikkelingen in de techniek en de maatschappij. Het onderdeel bewustwording is daarom nooit klaar.

### 9. Informatiebeveiliging

Zonder informatiebeveiliging is bescherming van persoonsgegevens niet mogelijk. Niet voor niets komen de termen 'passende technische en organisatorische maatregelen' veel voor in de AVG. Samenwerking tussen medewerkers van privacy en informatiebeveiliging is daarom erg belangrijk, zodat de onderwerpen elkaar aanvullen en niet los van elkaar worden gezien. Die samenwerking wordt vaak gezocht, maar komt niet altijd van de grond. Terecht merkt Privacy Management Partners op dat de informatiebeveiliging nog niet doelbewust aansluit op AVG-risico's. De AVG wordt nog te veel ervaren als een 'privacy kwestie' in plaats van een gemeenschappelijk belang. Daarin is nog veel winst te behalen. Zo zou informatiebeveiliging bijvoorbeeld een actievere rol kunnen spelen in de ontwikkeling van gegevensmanagement, waaraan wordt gewerkt met de privacy ambassadeurs. Ook is er bij nieuwe projecten behoefte aan integraal advies, vanuit privacy, informatiebeveiliging en andere expertises binnen de organisatie. Vanuit het team iRegie wordt het initiatief genomen om de integrale samenwerking vorm te geven.

### 10. Budget

De bescherming van persoonsgegevens blijft een belangrijk onderdeel voor de Gemeente Breda. De verwerking van persoonsgegevens is een kerntaak van de gemeente en om dat op een veilige, zorgvuldige en vooruitstrevende manier te doen, zijn er voldoende middelen nodig om dat mogelijk te maken. Qua kosten kan gedacht worden aan betrouwbare systemen, nieuwe technologieën, externe trainers voor themabijeenkomsten en capaciteit. Ook dient er gedacht te worden aan risico's die voort kunnen vloeien uit aansprakelijkheid.

---

<sup>1</sup> <https://autoriteitpersoonsgegevens.nl/nl/nieuws/tgb-betaalt-dwangsom-na-niet-voldoen-aan-inzageverzoek#subtopic-4542>

## 4. Op weg naar verbetering

De Gemeente Breda is een lerende organisatie en kan op veel onderdelen nog winst behalen. Dat is niet alleen wenselijk, maar noodzakelijk om voldoende aan de AVG-verplichtingen te kunnen voldoen. Als er op zoveel aspecten nog verbeteringen nodig zijn, waar beginnen we dan? De functionaris gegevensbescherming biedt, naar haar inzicht, een top drie aan om in 2019 tot de belangrijkste én realistische verbeteringen te komen.

### 1. De basis op orde

De grootste uitdaging ligt voor de Gemeente Breda in de ontwikkeling van gegevensmanagement. Doordat er nog onvoldoende zicht is op processen waarin persoonsgegevens verwerkt worden en dus ook een gebrek aan goede afspraken over de wijze waarop die gegevens verwerkt en beschermd worden, liggen er grote risico's voor de organisatie. Als blijkt dat gegevens onrechtmatig verwerkt worden, of voor andere doeleinden dan door de wetgever bedoeld is, is de Gemeente Breda al snel in overtreding en daarop aanspreekbaar door betrokkenen, de Autoriteit Persoonsgegevens en de rechter. Onvoldoende beveiliging of onzorgvuldig gedrag kan resulteren in datalekken met verstrekken gevolgen voor de rechten en vrijheden van betrokkenen én voor de Gemeente Breda (reputatieschade, aansprakelijkheid, enz.). Gebrek aan gegevensmanagement betekent dat de basis niet op orde is. Zonder dat fundament liggen er constant risico's op de loer en is de verwachting dat de organisatie achter incidenten blijft aanhollen. Daar staat tegenover dat een investering hierin z'n vruchten op korte en lange termijn zal afwerpen. Op korte termijn zal er duidelijkheid ontstaan over wat wel en niet kan met persoonsgegevens, zowel voor de ambtelijke en bestuurlijke organisatie als voor betrokkenen zelf. De Gemeente Breda heeft dan in de basis de verantwoording op orde. Op lange termijn kunnen wijzigingen en toevoegingen eenvoudig gedaan worden, denk bijvoorbeeld aan extra taken of nieuwe wetgeving. Daarnaast zorgt een goede basis ervoor dat de kwaliteit in stand gehouden kan worden door periodieke controles, denk aan juiste autorisaties en het handhaven van bewaartermijnen.

Bij gegevensmanagement wordt de hele organisatie betrokken bij de verantwoordelijkheid om persoonsgegevens te beschermen. Door dit zo collectief mogelijk aan te pakken, met de privacy ambassadeurs, ontstaat er kruisbestuiving tussen de verschillende afdelingen. Verwerkingen die afdeling-overstijgend zijn, kunnen op dezelfde wijze aangevlogen worden. Een afdeling die nieuwe technologieën gebruikt, kan een andere afdeling op weg helpen. Uitdagingen samen en tegelijk aangaan, zorgt voor kritische vragen en discussies die de aanpak scherper maken.

Gegevensmanagement is niet alleen de grootste uitdaging, maar vergt ook de meeste inspanning van medewerkers. Het is daarom belangrijk dat alle betrokken partijen de schouders eronder zetten om het tot een succes te maken:

- Directeuren en afdelingshoofden zijn verantwoordelijk voor juiste toepassing van de AVG binnen hun directies en afdelingen. De afdelingshoofden hebben privacy ambassadeurs aangedragen die voor hun afdeling de werkzaamheden zullen uitvoeren en/of coördineren. Het is ook aan de afdelingshoofden ervoor zorg te dragen dat de ambassadeurs voldoende ruimte hebben én ervaren om te doen wat van hen verwacht wordt. Ambassadeurs die afspraken niet nakomen worden door hun teamleider of afdelingshoofd aangesproken. Indien een medewerker niet meer als ambassadeur kan optreden, zorgt het afdelingshoofd voor vervanging.
- De privacy coördinator leidt en begeleidt de ambassadeurs. Hij verzorgt de maandelijkse trainingen, zodat de ambassadeurs worden meegenomen in de materie. Daarnaast zet hij de opdracht duidelijk uiteen, zodat de ambassadeurs weten wat er van hen verwacht wordt. De privacy coördinator is het aanspreekpunt voor de ambassadeurs bij vragen of andere zaken die betrekking hebben op de opdrachten. De privacy coördinator let op de planning en heeft aandacht voor de motivatie van de ambassadeurs en grijpt in wanneer hij merkt dat de motivatie afneemt of wanneer deadlines niet behaald worden. De privacy coördinator gaat ook trajecten aan met afdelingen waar geen privacy ambassadeur voor is. Dit kunnen verkorte trajecten zijn, maar komen zoveel mogelijk overeen met het traject van de afdelingen waar wel een ambassadeur voor is.
- De privacy ambassadeurs zijn aanwezig tijdens de maandelijkse bijeenkomsten. De bijeenkomsten en de daaruit voortvloeiende werkzaamheden hebben prioriteit. Indien de



ambassadeur daar onvoldoende ruimte voor ervaart, geeft hij/zij dat tijdig aan zodat er naar een oplossing gezocht kan worden. De ambassadeurs hoeven niet alle gegevens (processen, specifieke wetgeving, regels met betrekking tot autorisaties, contracten...) zelf te verzamelen, maar dienen de vraag uit te zetten bij de juiste mensen binnen de afdeling. Ook zijn de ambassadeurs het eerste aanspreekpunt binnen de afdeling indien er vragen zijn over de bescherming van persoonsgegevens. Indien de privacy ambassadeur er zelf niet uitkomt, neemt hij/zij contact op met de privacy coördinator.

- De functionaris gegevensbescherming heeft het implementatieplan bedacht, maar draagt de uitvoering en ontwikkeling van vervolgplannen over aan de privacy coördinator. De functionaris gegevensbescherming blijft als toezichthouder betrokken en controleert de afspraken die gemaakt worden. Zij let samen met de coördinator op de voortgang en rapporteert daarover aan de afdelingshoofden, directie en wethouder.

### 2. Bewustwording

De organisatie heeft behoefte aan bewustwording. Medewerkers uiten steeds opnieuw de wens te worden meegenomen in de nieuwe privacywetgeving en willen weten hoe ze hun werkzaamheden zo kunnen inrichten dat persoonsgegevens voldoende beschermd worden. Die vraag naar informatie is een belangrijk en positief signaal. De Gemeente Breda zou er dan ook goed aan doen daar gehoor aan te geven. Ook wanneer de (actieve) vraag naar bewustwording afneemt, dient het een vast onderdeel te blijven. Bewustwording zakt immers zo weer in wanneer er geen aandacht meer voor is. Voor een grote organisatie als de Gemeente Breda kost het tijd om teams af te gaan en alle medewerkers bewust te maken. Persoonlijke aandacht is echter wel waar medewerkers behoefte aan hebben om in gesprek te gaan en vragen te stellen. Die aandacht wordt door bijvoorbeeld e-learning modules niet geboden. Het is daarom belangrijk dat bewustwording tot de primaire taken van een privacy medewerker behoort. Momenteel is die taak toebedeeld aan de privacy coördinator.

De functionaris gegevensbescherming doet graag de volgende suggesties voor een effectieve bewustwordingscampagne die aansluit op de wensen en behoeften van de organisatie:

- Gebruik Q1 en Q2 van 2019 om voor alle teams (al dan niet gecombineerd) bewustwordingsworkshops te verzorgen. Maak die workshops zowel informatief als interactief. Het verdient de voorkeur de groepen niet te groot te maken, zodat er voldoende ruimte is voor interactie. Prioriteer bij het uitnodigen van teams in gevoeligheid van persoonsgegevens, beginnend bij het sociaal domein.
- Organiseer themabijeenkomsten waarbij van buiten naar binnen wordt gedacht. Hoe denken privacy organisaties, journalisten, schrijvers en technici over privacy? Nodig hen uit om hun verhaal te vertellen aan medewerkers van de Gemeente Breda, zodat de medewerkers het onderwerp ook van een andere kant kunnen bekijken. Gebruik daar het jaar 2019 voor, waarbij elk kwartaal of elke twee maanden iemand het woord krijgt.
- De AVG is jonge wetgeving en is met veel bombarie in werking getreden. Een hoge piek in aandacht wordt vaak gevolgd door een dieptepunt wanneer het nieuwe er van af is. Het is aan de organisatie om de aandacht er bij te houden. De week rondom 25 mei 2019 bestaat de AVG een jaar. Die week zou de week van privacy genoemd kunnen worden, waarbij activiteiten en bijeenkomsten georganiseerd worden over privacy.
- Zorg voor een gelaagde structuur in de bewustwordingsworkshops. Begin bij de basis en bouw het van daaruit verder op.
- Gebruik naast de workshops verschillende (ludieke) manieren om medewerkers aan de bescherming van persoonsgegevens te herinneren. Maak bijvoorbeeld gebruik van pip en spreekuren. Blijf zichtbaar voor medewerkers en wees creatief en origineel.

### 3. Evenwicht tussen beleid en uitvoering

Hoewel er een privacy beleid is, heeft het nog geen formele status. Daarnaast kan het privacy beleid een update gebruiken. Het privacy beleid dient als vertrekpunt, waaraan verdere beleidsstukken en werkwijzen nadere invulling kunnen geven. Zo is er bijvoorbeeld ook behoefte aan een datalekkenbeleid en een werkwijze AVG-verzoeken. Deze stukken zijn al in ontwikkeling en moeten Q1 2019 opgeleverd kunnen worden.

Voorts is het de vraag hoe de beleidsstukken op de juiste wijze, door de juiste mensen en op het juiste moment worden uitgevoerd. De concern controller merkt in zijn advies van 15 november 2018 terecht op dat er vaak goede adviezen liggen, maar een tekort aan doe-types. Advies en

beleid zonder uitvoering zet geen zoden aan de dijk. De concern controller stelt voor extern advies in te winnen voor een helder governance model. De functionaris gegevensbescherming sluit zich graag bij dat advies aan en doet een voorstel om de volgende vragen bij dat onderzoek te betrekken:

- De functionaris gegevensbescherming heeft het afgelopen jaar het initiatief genomen tot het schrijven van diverse formats, werkwijzen en beleidsstukken. Niet omdat dit haar rol was, maar omdat er gebrek aan capaciteit was. De functionaris gegevensbescherming dient eerder toezicht te houden op de inhoud en de naleving van de stukken. Inmiddels wordt de ontwikkeling van deze stukken belegd bij de privacy coördinator. Hoe wordt deze taak in andere organisaties belegd?
- De Gemeente Breda is van vrijwel geen capaciteit op het gebied van privacy gegaan naar een functionaris gegevensbescherming (1fte), een privacy coördinator (1fte), en twee privacy adviseurs (1,5 fte). Er wordt echter nog steeds een tekort ervaren doordat er niet tijdig gehoor gegeven kan worden aan de vragen die gesteld worden. Er ontstaat regelmatig een wachttijd van weken, waar dat niet altijd geoorloofd is. Bij incidenten of andere spoedeisende zaken loopt de wachttijd nog verder op. De Gemeente Breda is binnen de regio in verschillende hoedanigheden een opdrachtnemende partij. Diensten waarbij persoonsgegevens verwerkt worden, worden aan Breda uitbesteed. Ook is de Gemeente Breda vooruitstrevend en ambitieus waar het gaat om nieuwe projecten en technologieën. De Gemeente Breda investeert in diverse Big Data-projecten en loopt voorop in het tegengaan van ondermijning. Dergelijke opdrachten en projecten gaan gepaard met risico's waar aandacht voor vereist is. Wat is gelet op alle omstandigheden, waaronder de grootte van de organisatie, de opdrachten die aan de Gemeente Breda zijn uitbesteed, de lopende projecten en de ambities, realistisch ten aanzien van de capaciteit en welke rollen, met welke taken, zijn vereist?
- De bescherming van persoonsgegevens is een taak voor iedereen, maar wordt ervaren als een taak voor privacy medewerkers. Op welke wijze kan de verantwoordelijkheid op een juiste manier verdeeld worden onder de directeurs, afdelingshoofden en teamleiders? En hoe kan de kwaliteit geborgd worden?
- Hoe zorgen we ervoor dat verschillende met elkaar samenhangende expertises binnen de organisatie op een effectieve en efficiënte manier bij elkaar kunnen komen en integraal kunnen adviseren, waarbij ruimte blijft voor autonome overwegingen (bijvoorbeeld vanuit toezicht)? Welke samenwerkingen zijn vereist (bijvoorbeeld privacy en informatiebeveiliging)? Welke samenwerkingen zijn wenselijk (bijvoorbeeld privacy en smart city)? Wat mag wie op welk moment van elkaar verwachten, doelend op medewerkers onderling en het bestuur en de directie ten opzichte van medewerkers)?