



Gemeente Breda

# AVG JAARRAPPORTAGE 2019

COLLEGE VAN BURGEMEESTER & WETHOUDERS

MR. N (NADIA) BENAÏSSA, FUNCTIONARIS GEGEVENSBECHERMING

GEMEENTE BREDA

## Inhoudsopgave

Inleiding	2
Leeswijzer	2
Samenvatting en conclusie	3
1. De basis op orde	5
2. Bewustwording	8
3. Organisatorische inbedding	11
4. Rechten van betrokkenen	14
5. Evenwicht tussen beleid en uitvoering	16
6. Samenwerking	19
7. Datalekken	22
8. Netwerk	25
9. Verantwoording van verwerkingen	26
10. Verantwoording van de functionaris gegevensbescherming	28

## Inleiding

De Gemeente Breda is verantwoordelijk voor de verwerking van persoonsgegevens van burgers. Van de wieg tot het graf worden belangrijke gebeurtenissen geregistreerd, worden er diensten verleend en wordt er hulp geboden als mensen dat nodig hebben. Bij de verwerking van al die gegevens dient de Gemeente Breda het fundamentele recht op bescherming van de persoonlijke levenssfeer in acht te nemen en te voldoen aan de verplichtingen die voortvloeien uit de Algemene Verordening Gegevensbescherming (AVG).

Op grond van artikel 38 lid 3 AVG brengt de functionaris gegevensbescherming jaarlijks verslag uit aan de gemeentesecretaris en het College van Burgemeester en Wethouders. Voor u ligt de AVG jaarrapportage 2019. In deze rapportage beschrijft de functionaris gegevensbescherming de stand van zaken op het gebied van de implementatie van de AVG binnen de Gemeente Breda en de wijze waarop persoonsgegevens beschermd worden.

## Leeswijzer

Deze rapportage richt zich op de belangrijkste aspecten van de AVG. Daarbij is ook aangesloten bij de onderwerpen die VNG Realisatie (IBD) van belang acht in de jaarrapportage van de functionaris gegevensbescherming.<sup>1</sup> Op de volgende pagina staat een samenvatting van de bevindingen.

De opbouw van de hoofdstukken 1 tot en met 8 is bepaald aan de hand van prioritering op basis van de risico's voor betrokkenen en de organisatie, te beginnen met de hoogste prioriteit. In deze hoofdstukken wordt steeds het onderwerp en het belang daarvan geïntroduceerd, het risico beschreven, teruggeblikt naar de afgelopen periode en vooruit gekeken naar komend jaar. In elk hoofdstuk staan concrete en praktische aanbevelingen die aansluiten bij het volwassenheidsniveau van de organisatie. De hoofdstukken worden afgesloten met een kader waarin de samenvatting wordt weergegeven.

Hoofdstukken 8 en 9 bevatten aanvullende informatie en hebben daarom een andere opbouw. In deze hoofdstukken wordt ingegaan op het netwerk van medewerkers die zich richten op de bescherming van persoonsgegevens en op de wijze waarop verwerkingen van persoonsgegevens geregistreerd en beoordeeld worden.

---

<sup>1</sup> FG Jaarrapportage College van Burgemeester en Wethouders, IBD.

## Samenvatting en conclusie

### ALGEMEEN BEELD

De Gemeente Breda is een ambitieuze organisatie en toont lef en liefde. In het belang van betrokkenen en/of de organisatie wordt er geëxperimenteerd met nieuwe datatechnieken. Er wordt niet voor terug gedeinsd het voortouw te nemen en mogelijkheden te verkennen. Samenwerkingen worden geïnitieerd en gefaciliteerd om belangen samen te brengen. Vooruitstrevend en vastberaden om zaken beter te organiseren en uitdagingen bij de horens te pakken. De AVG biedt daar ruimte toe. De belangrijkste voorwaarde is echter dat er vooraf goed wordt nagedacht over het beschermen van fundamentele rechten van mensen.

Medewerkers vanuit de hele organisatie wisten het privacyteam en de security adviseur te vinden om verwerkingen van persoonsgegevens, ook bij nieuwe verwerkingen, veilig in te richten. De organisatie doet dankbaar beroep op hun expertise, maar de vraag is groter dan de kleine groep medewerkers aan kunnen. De beperkte capaciteit resulteerde in onvoldoende bescherming van persoonsgegevens – een grondrecht waarvan de overheid de borging moet garanderen aan haar burgers. Ondanks dat de ernst van dit probleem herhaaldelijk is aangekaart, is er te afwachtend op gereageerd. Hoewel plannen worden ontwikkeld en adviezen worden ingewonnen, is een concrete oplossing nog niet bereikt. De Gemeente Breda zal hier in het jaar 2020 verder mee aan de slag gaan.

De Gemeente Breda staat voor de uitdaging om Europese wetgeving in een data-gedreven wereld, lokaal toe te passen. Waar de afgelopen twee jaar in het teken stond van implementatie en praktische toepassing van de AVG, vraagt de komende periode om visie en strategie. Technieken en mogelijkheden volgen elkaar in rap tempo op en biedt ook kansen voor de Gemeente Breda. Om tot successen te komen dient goed nagedacht te worden over juridische, technische, maatschappelijke en ethische aspecten. De directeur bedrijfsvoering heeft het afgelopen jaar de tijd genomen om mogelijkheden in kaart te brengen en is voornemens in 2020 te organiseren vanuit de basis, te beginnen met een strategisch beleid gegevensbescherming.

Tegelijkertijd heeft de Gemeente Breda nog een lange weg te gaan om te kunnen voldoen aan de basisvereisten van de AVG. In 2018 kende de Gemeente Breda een vliegende start. In rap tempo wist de Gemeente Breda te voldoen aan de meeste vereisten van het tienstappenplan van de Autoriteit Persoonsgegevens. In 2019 is de Gemeente Breda echter achter gaan lopen in het realiseren van de eigen ambities. Het ontbreekt de Gemeente Breda niet aan talent of goede plannen. De realisering en uitvoering blijkt echter nog vaak een stap te ver. Daarbij is het belangrijkste aandachtspunt dat het de Gemeente Breda ontbreekt aan een basis gegevensmanagement. Binnen veel afdelingen is nog onduidelijk welke gegevens met welk doel en op welke wijze verwerkt worden. Indien het overzicht en de structuur daarin ontbreekt kunnen risico's niet gedetecteerd worden en is het onmogelijk om in control te komen. Dat heeft tot gevolg dat de organisatie achter incidenten blijft aanhollen. Incidenten die soms verstrekken gevolgen hebben voor betrokkenen en de organisatie. Om dit te voorkomen dient er een structurele oplossing te komen: de basis moet op orde.

### BELANGRIJKSTE RESULTATEN 2019

- Vanuit het plan 'De basis op orde' zijn er belangrijke stappen gezet om het verwerkingenregister te completeren. Hier is aan gewerkt door de privacy ambassadeurs die vanuit afdelingen zijn aangesteld en de privacy adviseur die hen begeleidt. Op basis van dit overzicht is er een risicoanalyse gedaan.
- Om de bewustwording van medewerkers te vergroten zijn e-learning modules doorlopen op het gebied van informatiebeveiliging en datalekken. Ook zijn er diverse AVG-trainingen verzorgd voor medewerkers en het College van B&W. Daarnaast is er op het intranet Pip een tegel ontwikkeld waar medewerkers informatie en adviezen kunnen terugvinden met betrekking tot privacy en veilig werken.



- In 2019 is een datalekkenprotocol ontwikkeld en vastgesteld, inclusief een draaiboek en een meldings- en beoordelingsformulier.
- Nieuwe verwerkingen van persoonsgegevens worden beoordeeld aan de hand van verantwoordingsdocumenten en DPIA's (Data Protection Impact Assessments).
- Er is een proces voor AVG-verzoeken ontwikkeld, ook kunnen betrokkenen een verzoek via de website indienen.

#### GROOTSTE UITDAGINGEN VOOR 2020

- De basis moet op orde. Zolang er geen overzicht is in de gegevens die verwerkt worden en de wijze waarop dat gebeurt, is het onmogelijk een gedegen risico-inschatting te maken en de rechten van betrokkenen beter en naar behoren te borgen.
- Vanuit de organisatie wordt regelmatig aangegeven dat er veel behoefte is aan bewustwording. Medewerkers willen graag weten wat de AVG voor hun werkzaamheden betekent. Op maat gemaakte bewustwordingssessies zijn van belang om medewerkers hierin mee te nemen.
- Zonder expertise op het gebied van gegevensbescherming kan de Gemeente Breda persoonsgegevens onvoldoende beschermen. De Gemeente Breda dient over voldoende capaciteit te beschikken om aan de vraag vanuit de organisatie te voldoen.
- De Gemeente Breda dient over te gaan van implementatie naar vaste inbedding en strategie, waarbij meer betrokkenheid en eigenaarschap van de directie en het management vereist is.
- Het ontbreekt nog te veel een helder beleid, waardoor het voor medewerkers niet duidelijk is wat van hen verwacht wordt.
- Betere leiding en sturing is nodig om zicht te krijgen op de werkzaamheden en om plannen daadwerkelijk tot uitvoering te brengen.

#### AANBEVELINGEN EN ACTIEPUNTEN

- Zorg voor een goed plan van aanpak en een gedetailleerde, realistische planning om de basis op orde te krijgen. Faciliteer de medewerkers die met deze taak belast zijn voldoende en rapporteer periodiek over de voortgang aan de directeur bedrijfsvoering en functionaris gegevensbescherming.
- Organiseer informatieve en interactieve workshops voor medewerkers waarin de AVG vertaald wordt naar dagelijkse werkzaamheden. Maak een planning zodat medewerkers weten wanneer hun team aan bod komt en het management de voortgang in de gaten kan houden.
- Organisatorische inbedding vraagt meer betrokkenheid van de directie en het management, waarbij rekening wordt gehouden met de vraag van de organisatie dat vertaald wordt naar capaciteit dat voldoende is om rechten van betrokkenen te borgen. Zorg voor goed zicht op de werkzaamheden, de werkdruk en het functioneren van medewerkers.
- Om AVG-verzoeken goed in behandeling te nemen is een goed proces dat technisch ondersteund wordt noodzakelijk. Daarnaast dienen medewerkers opgeleid te worden en voldoende tijd ter beschikking te hebben om verzoeken naar behoren te verwerken.
- De directie is aan zet om te bepalen hoe de komende periode wordt overgegaan van implementatie naar strategie. Begin het jaar 2020 met een sessie, begeleid door een expert, om tot concrete beslissingen te komen.

## 1. De basis op orde

### AANLEIDING

In april 2018 constateerde de functionaris gegevensbescherming dat het binnen de Gemeente Breda ontbrak aan basis gegevensmanagement. Er was onvoldoende zicht op processen en de inrichting daarvan. Afdelingen hadden niet in beeld welke gegevens door wie en voor welk doel werden verwerkt. Dat maakte het onmogelijk om de verwerkingen van (persoons)gegevens beheersbaar te houden, risico's in beeld te krijgen of maatregelen te nemen om (persoons)gegevens afdoende te beschermen. Ook in de nulmeting dat eind 2018 door Privacy Management Partners verricht is, wordt de ontwikkeling van gegevensmanagement de grootste uitdaging voor de Gemeente Breda genoemd.

### Risico's

Uit de evaluatie van verschillende datalekken bleek dat er fouten en onrechtmatige verwerkingen ontstaan, doordat processen niet op orde zijn. Enkele gevallen waren zeer schrijnend, met aanzienlijke risico's voor betrokkenen. Denk hierbij aan werkzaamheden van medewerkers die niet voldoende in beeld zijn bij leidinggevenden. [REDACTED] het verstrekken van bijzondere persoonsgegevens met gedetailleerde dossierinformatie via email, of het publiceren van gegevens waarvan onvoldoende wordt afgevraagd of er een verplichting tot publiceren of anonimiseren is. Hierbij is vaak sprake van structurele gebreken in het proces, waardoor er niet van incidenten gesproken kan worden. Dergelijke situaties kunnen niet alleen ernstige gevolgen hebben voor betrokkenen, maar ook voor de Gemeente Breda als verwerkingsverantwoordelijke, of andere gemeenten en organisaties waarvoor de Gemeente Breda persoonsgegevens verwerkt. De Gemeente Breda wordt geacht de basis op orde te hebben. Burgers mogen er op vertrouwen dat de overheid betrouwbaar met gegevens omgaat, zeker nu burgers vaak verplicht zijn hun persoonsgegevens te delen met de overheid.

### TERUGBLIK

De functionaris gegevensbescherming adviseerde in 2018 prioriteit te geven aan het leggen van een basis voor gegevensmanagement: 'De basis op orde'. Daarbij dient aandacht te zijn voor verplichtingen die rechtstreeks voortvloeien uit de AVG, zoals het verwerkingenregister, privacyverklaringen, verwerkersovereenkomsten, correcte archivering en autorisaties, en bewustwording. Om dit te bewerkstelligen zijn er in 2018 binnen de meeste afdelingen privacy ambassadeurs aangesteld die naast de vakinhoudelijke kennis van de werkzaamheden en geldende wetgeving, opgeleid werden in de AVG. Afdelingen zijn immers zelf verantwoordelijk voor juiste toepassing van de AVG binnen hun verwerkingen van persoonsgegevens. Deze werkwijze wordt ook gehanteerd in andere gemeenten en ligt ook in lijn met het meerjarenverbeterplan. Daarnaast is er een privacy coördinator aangesteld om de ambassadeurs te begeleiden en aan te sturen. De functionaris gegevensbescherming heeft een planning voor 2018 en 2019 opgesteld en deze overhandigd aan de privacy coördinator. In september zijn de ambassadeurs onder begeleiding van de coördinator vol goede moed van start gegaan.

Vrij snel werd er van de planning afgeweken, helaas zonder dat er een nieuwe planning voor in de plaats kwam. Met als resultaat dat maanden elkaar opvolgden zonder dat voortgang geboekt werd. Ambassadeurs gaven terug dat het ontbrak aan heldere taken, formats en goede begeleiding. Gaandeweg haakten steeds meer ambassadeurs af en werd aangegeven geen prioriteit te kunnen geven aan de taken die zij als ambassadeurs hadden, omdat zij dit naast andere werkzaamheden deden.

In het voorjaar van 2019 heeft een privacy adviseur de begeleiding van de ambassadeurs overgenomen en is er prioriteit gesteld op het completeren van het verwerkingenregister. Er werden formats ontwikkeld om voor uniformiteit te zorgen en er werden individuele afspraken ingepland met de ambassadeurs om hen persoonlijk te begeleiden. Daarnaast werd er een planning ontwikkeld



en werden ambassadeurs aangesproken op deadlines. Op basis van het verwerkingenregister is er een risicoanalyse gedaan om vanaf 2020 risico gestuurd te kunnen werken.

#### BLIK VOORUIT

Na een moeilijke start zijn vervolgens wel belangrijke stappen gezet met het verwerkingenregister. Er zijn echter nog veel onderdelen die nog aan bod moeten komen om van een basisgegevensmanagement te kunnen spreken. Van de vijf onderdelen die aanvankelijk op de planning stonden om tussen september 2018 tot december 2019 te realiseren, is slechts één onderdeel daadwerkelijk (bijna) gerealiseerd. Voorlopig behoeft het dus nog veel aandacht en middelen om hier verdere stappen in te zetten.

Omdat er binnen de Gemeente Breda meerdere trajecten lopen om verbeteringen te bewerkstelligen in het organiseren van de basis, zijn er contacten gezocht om het 'AVG-traject' af te stemmen met andere disciplines. Zo wordt er aangesloten bij het meerjarenverbeterplan van concern control. Ook is er op verzoek van wethouder Adank en advies van de concern controller in november 2018 opdracht gegeven tot het uitvoeren van een governance onderzoek. Dit onderzoek wordt sinds juli 2019 uitgevoerd door Verdonck, Klooster & Associates (hierna: VKA).

Uit deze opdrachten zijn een concept 'Strategisch beleid voor gegevensbescherming' en een 'Plan van aanpak certificering ISO27001/NEN7510 (BIO) voortgekomen.<sup>2</sup> Met het strategisch beleid worden de rollen, taken en verantwoordelijkheden beter belegd en worden er mogelijkheden geboden om de samenwerking tussen privacy, informatiebeveiliging en dataverwerking te bevorderen en te zien als één geheel: gegevensbescherming. Er wordt voorgesteld om meer risico gebaseerd te werken. In het plan van aanpak wordt de nadruk gelegd op het voldoen aan de bovengenoemde informatiebeveiliging normenkaders, maar wordt daarnaast gezocht naar aansluiting met de bescherming van persoonsgegevens. Er is eveneens aandacht voor het op orde krijgen van de processen en het beleggen van verantwoordelijkheden binnen de afdelingen. Ook dit plan gaat uit van een werkwijze waarin de privacy ambassadeurs vanuit de afdelingen een belangrijke taak hebben om de basis op orde te krijgen.

#### AANBEVELINGEN

- Zorg voor een goed plan van aanpak en een voldoende gedetailleerde en realistische planning waarmee voor de ambassadeurs, de afdelingen, de directie en de functionaris gegevensbescherming duidelijk wordt waar naartoe gewerkt wordt en welke aspecten wanneer aan bod komen.
- Zorg voor goede begeleiding van de ambassadeurs en afdelingen, waarbij pro actief tijd gemaakt wordt om uitvoerders een hand toe te reiken. Faciliteer daarnaast door middel van heldere opdrachtbeschrijvingen en formats voor een uniforme en efficiënte werkwijze.
- Motiveer de ambassadeurs om aanwezig te zijn bij bijeenkomsten en de afgesproken deadlines te behalen. Geef ze voldoende bagage mee om de opdrachten binnen de afdelingen uit te voeren en ga in gesprek met het afdelingshoofd wanneer er een ambassadeur te weinig ruimte krijgt binnen de afdeling of er onvoldoende commitment wordt ervaren.
- Zorg voor goede sturing op de voortgang van het traject door het management en de directie.

<sup>2</sup> Ten tijde van het schrijven van deze rapportage waren beide stukken nog in concept, versie 0.95

- Neem de afdelingshoofden en de directie periodiek mee in de voortgang en zorg voor bewustwording.
- Rapporteer periodiek over de voortgang aan de CIO en de functionaris gegevensbescherming.

De grootste uitdaging voor de Gemeente Breda op het gebied van gegevensbescherming is het organiseren van gegevensmanagement. Welke gegevens verwerken we, met welk doel en op welke wijze. Om de basis op orde te krijgen dienen er belangrijke stappen gezet te worden. De organisatie heeft, na een moeilijke start, veel processen in beeld gebracht in het verwerkingenregister. Daar is vanuit afdelingen samen met een privacy adviseur hard aan gewerkt.

Komend jaar dient er echter nog veel gedaan te worden. De functionaris gegevensbescherming adviseert hier topprioriteit aan te geven en er vanuit de directie op te sturen dat de benodigde commitment bestaat bij afdelingen. Daarnaast dient de voortgang nauwlettend in de gaten gehouden te worden. Zorg voor periodieke rapportages die gedeeld worden met de directie en de functionaris gegevensbescherming.



## 2. Bewustwording

### AANLEIDING

Bewustwording omtrent de werking van de AVG en de verplichtingen die daaruit voortvloeien, is onmisbaar binnen een organisatie waarin persoonsgegevens verwerkt worden. De bescherming van persoonsgegevens valt of staat immers met het bewust en zorgvuldig handelen van medewerkers en faciliteiten die daartoe worden geboden door het management. Medewerkers hebben regelmatig de wens geuit meegenomen te worden in de (relatief nieuwe) privacywetgeving. Ze willen graag weten hoe ze hun werkzaamheden zo kunnen inrichten dat persoonsgegevens voldoende beschermd worden én efficiënt en effectief kunnen blijven werken. Ook is er behoefte aan praktisch advies met betrekking tot de beveiliging van informatie.

Binnen de Gemeente Breda staat de AVG vrijwel nooit op zichzelf, maar altijd in relatie tot specifieke wet- en regelgeving, zoals de Gemeentewet, de Jeugdwet of de Afvalstoffenverordening. Binnen die wetgeving staat vaak voorgeschreven welke persoonsgegevens met welk doel verwerkt moeten worden. De AVG hangt daar als een paraplu met algemene spelregels boven. Daarom is het niet voldoende medewerkers enkel mee te nemen in die algemene spelregels, maar dienen zij meegenomen te worden in wat de AVG met de specifieke wet- en regelgeving verbindt en wat dat betekent voor hun dagelijkse werkzaamheden.

### Risico's

Medewerkers die niet meegenomen worden in de betekenis van de AVG in relatie tot eigen werkzaamheden, missen de bagage om alert te kunnen zijn en zorgvuldig te handelen. Onbewust en met de beste bedoelingen worden privacygevoelige persoonsgegevens opgeslagen of doorgestuurd zonder dat er wordt nagedacht over juiste beveiliging, of überhaupt een grondslag om de gegevens te mogen verwerken. Het komt te vaak voor dat e-mails met BSN's en gedetailleerde casuïstiek vol informatie over de gezinssituatie, gezondheid, financiële situatie, etc. worden doorgestuurd naar allerlei medewerkers en partijen die in bepaalde mate betrokken zijn bij een casus. Bij het overgrote deel van de datalekken is er sprake van het uitlekken van gevoelige informatie. Vaak gebeurt dat per e-mail. Denk daarbij aan verkeerde geadresseerden of het toevoegen van verkeerde bijlagen. Individueel gezien lijken dat menselijke fouten die niet altijd voorkomen kunnen worden, maar in de breedte gezien is dit een te vaak voorkomend probleem waar door middel van bewustwording winst behaald kan worden. Met begrip over de AVG kan men kritischer beoordelen hoe en door wie persoonsgegevens verwerkt mogen worden.

### TERUGBLIK

Eind 2018 en begin 2019 hebben alle medewerkers e-learning modules doorlopen op het gebied van informatiebeveiliging en datalekken. Medewerkers volgden een online cursus en legden vervolgens een toets af waar een certificaat voor behaald moest worden. Voorafgaand aan de modules zijn er ook workshops geweest. De campagne heeft veel steun gehad en had een groot bereik. Een mooie prestatie!

In 2019 is er ook een privacy en veiligwerken-tegel geplaatst op Pip. Via deze tegel op Zelf Regelen kunnen medewerkers uitleg vinden over diverse onderwerpen gerelateerd aan gegevensbescherming en kunnen medewerkers eenvoudig een datalek of beveiligingsincident melden.

In de zomer en in het najaar van 2019 zijn er daarnaast een aantal AVG-trainingen verzorgd door Considerati. De AVG basis en basis plus werd gegeven aan de privacy en security adviseur, de privacy ambassadeurs, juridische zaken, advies en projecten en onderzoek en inzicht. Ook is er met Considerati een bewustwordingssessie georganiseerd voor het College van B&W.

De e-learning en de trainingen van Considerati hebben bijgedragen aan meer bewustwording binnen de organisatie. Ook is er twee keer getoetst middels 'phishings acties'. Medewerkers geven echter aan dat er nog veel behoefte is aan kennis en praktische tips om zorgvuldig om te kunnen gaan met gegevens. De bereidheid om het goed te doen is er, de faciliteiten ontbreken nog te veel, volgens medewerkers. Dat is een gemiste kans. De functionaris gegevensbescherming heeft daarom ook regelmatig in haar rapportages aan de directie het belang van bewustwording aangekaart en praktische adviezen gegeven om beter aan te sluiten op de behoefte vanuit de organisatie. Zo is er bijvoorbeeld geadviseerd om praktische informatie te delen via nieuwsberichtjes op pip, bewustwordingsfilmpjes te laten maken, een week van de privacy te organiseren en/ of sprekers van buiten uit te nodigen. Ook is er geadviseerd informatieve en interactieve workshops te organiseren op teamniveau, zodat medewerkers de ruimte krijgen concreet na te denken over de toepassing van de AVG binnen de dagelijkse werkzaamheden. Deze workshops kunnen vanuit de basis worden opgebouwd en in de loop der tijd gedetailleerder worden, naar gelang de behoefte vanuit de organisatie.

Het afdelingshoofd ICO heeft opdracht gegeven tot het ontwikkelen van een bewustwordingsprogramma en verschillende goede ideeën hebben het afgelopen jaar de revue gepasseerd. Zo werd er gesproken over trainingen aan nieuwe medewerkers waarin privacy, informatieveiligheid en integriteit gecombineerd werden, trainingen over veilig e-mailen en mogelijkheden binnen Office en Outlook om medewerkers praktische tips te geven om het aantal datalekken op dat vlak terug te dringen. Het komt echter geregeld voor dat dergelijke plannen te lang op de plank blijven liggen. Vooralsnog ontbreekt het aan een concreet programma met een planning waardoor de uitvoering op zich laat wachten.

#### **BLIK VOORUIT**

Komend jaar staan er nog een aantal AVG-trainingen van Considerati op de agenda. Ook staat er in het concept plan van aanpak van VKA dat er een bewustzijnsplan/communicatieplan opgesteld moet worden waarin wordt ingegaan op bewustwordingssessies, het aanbieden van training, coaching en begeleiding van gegevensbeschermingsspecialisten, en het begeleiden van het management in sturing op gegevensbescherming.

#### **AANBEVELINGEN**

- Zorg voor een goed bewustwordingsprogramma waarin gerelateerde onderwerpen (zoals gegevensbescherming in de breedte en integriteit) samen komen en vertaal dat in een planning. Communiceer de planning aan de organisatie, zodat medewerkers en het management weten wanneer zij aan de beurt komen.
- Bewaak periodiek de planning en voorkom vertraging in de uitvoering.
- Zorg voor informatieve en interactieve workshops voor alle teams die persoonsgegevens verwerken.
- Zorg voor een gelaagde structuur in de bewustwordingssessies. Begin bij de basis en bouw het van daaruit verder op.
- 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 medewerkers het onderwerp ook van een andere kant kunnen bekijken.
- Gebruik naast de workshops verschillende (ludieke) manieren om medewerkers aan de bescherming van persoonsgegevens te herinneren. Blijf zichtbaar en toegankelijk voor medewerkers en wees creatief en origineel.

In 2019 zijn medewerkers meegenomen in het onderwerp gegevensbescherming door middel van e-learning modules, informatie op Pip en de mogelijkheid zelf eenvoudig datalekken en beveiligingsincidenten te melden. Ook zijn trainingen en bewustwordingsworkshops georganiseerd voor verschillende teams en het College van B&W.

Vanuit de organisatie komen er regelmatig signalen dat er behoefte is aan informatieve en interactieve AVG-workshops, afgestemd op de dagelijkse werkzaamheden. Medewerkers zijn gebaat bij praktische tips om hun werkzaamheden effectief uit te kunnen voeren met aandacht voor de bescherming van persoonsgegevens. Hier valt nog veel winst te behalen. Zorg daarom voor een goed programma met een jaarplanning om de bewustwording in 2020 naar een hoger niveau te tillen. De bescherming van persoonsgegevens valt of staat immers met het bewust en zorgvuldig handelen van medewerkers en faciliteiten die daartoe worden geboden door het management.



### 3. Organisatorische inbedding

#### AANLEIDING

De Gemeente Breda draagt zorg voor de persoonsgegevens van 186.000 inwoners van Breda én in voorkomende gevallen voor de persoonsgegevens van de inwoners van omliggende gemeenten. De Gemeente Breda vervult de rol van centrumgemeente binnen de regio en is samenwerkingspartner van publieke en private partijen. Vol enthousiasme en ambitie wordt er buiten de box gedacht over nieuwe datatechnieken, zoals big data, kunstmatige intelligentie, domeinoverstijgend werken en smart city. Geheel in lijn met de kerngedachte van het huidige bestuursakkoord Lef & Liefde.

Maar hoe zorgt de Gemeente Breda ervoor dat ambitieuze dromen werkelijkheid worden en niet overslaan tot een nachtmerrie voor betrokkenen of de organisatie? Nieuwe technieken creëren mogelijkheden, maar dwingen tot 'denken voor doen' en zorgvuldig handelen. Dat is tevens de essentie van de AVG: verwerkingsverantwoordelijken krijgen veel ruimte om datamogelijkheden te verkennen, mits ze er vooraf goed over nadenken door risico's in kaart te brengen en maatregelen te nemen om risico's te beperken. Om dat te borgen is het noodzakelijk rollen en verantwoordelijkheden goed te beleggen en voldoende expertise in huis te hebben.

#### RISICO'S

De bescherming van persoonsgegevens is een verantwoordelijkheid van iedereen die persoonsgegevens verwerkt. Directies en afdelingen dienen zich bewust te zijn van die verantwoordelijkheid en medewerkers te faciliteren in juiste en zorgvuldige omgang met persoonsgegevens. Dat kunnen zij echter niet alleen. Er is expertise nodig om de organisatie op weg te helpen om te kunnen voldoen aan de verplichtingen die voortvloeien uit de AVG en het volwassenheidsniveau naar een hoger niveau te tillen. Onvoldoende expertise leidt ertoe dat afdelingen en projecten onvoldoende geadviseerd kunnen worden in de juiste toepassing van de AVG. Dat resulteert in onvoldoende bescherming van persoonsgegevens – een grondrecht waarvan de overheid de borging moet garanderen aan haar burgers.

Wat de risico's van het beperken van grondrechten zijn, wordt pas duidelijk als het recht geschonden wordt. Als je niet meer vrijuit kunt spreken, voel je het belang van vrijheid van meningsuiting. Als je een baan geweigerd wordt omdat je de verkeerde afkomst hebt, begrijp je het verbod op discriminatie. Wanneer de gegevens over je gezondheid of financiën op straat liggen, realiseer je je dat je toch iets te verbergen hebt. Schendingen van het recht op privacy kunnen een enorme impact hebben op het leven van mensen, met verstrekende gevolgen. De AVG is in werking getreden met veel bombarie over de hoogte van boetes die kunnen oplopen tot twintig miljoen. Een motivatie voor organisaties om aan de regels te voldoen. Maar hoeveel is een mensenleven waard? Dat vragen we ons af wanneer we er de verantwoordelijkheid voor dragen dat we de gegevens van een persoon hebben laten lekken die zo gevoelig van aard zijn dat het de persoon in kwestie tot wanhoop drijft.

#### TERUGBLIK

Begin 2019 waren er vier medewerkers (3,5 fte) die zich bezighielden met AVG-vraagstukken: een privacy coördinator die zich richtte op 'De basis op orde' en bewustwording en drie privacy adviseurs om de vragen vanuit de organisatie te beantwoorden. De functionaris gegevensbescherming houdt toezicht op de naleving van de AVG en adviseert daaromtrent. Daarnaast is er op het vlak van informatiebeveiliging een CISO (Concern Information Security Officer) en een informatiebeveiligingsadviseur. Informatiebeveiliging en bescherming van persoonsgegevens zijn nauw met elkaar verbonden. Samenwerking is dan ook van cruciaal belang om de organisatie op weg te helpen, te begeleiden naar een goed resultaat en om dit resultaat ook te borgen. Om de samenwerking te faciliteren heeft de functionaris gegevensbescherming wekelijkse overleggen geïnitieerd om lopende zaken met elkaar te bespreken en tijdig de juiste expertise aan te laten



haken. Deze overleggen hebben echter niet voldoende bijgedragen aan adequate sturing en borging van resultaten.

Eind 2018 is op verzoek van wethouder en op advies van de concern controller opdracht gegeven tot het uitvoeren van een governance onderzoek dat sinds juli 2019 door VKA wordt gedaan. Een belangrijke stap om de organisatorische inbedding nader en beter vorm te geven in een structuur die recht doet aan de rollen, taken en verantwoordelijkheden.<sup>3</sup>

Met een redelijke capaciteit en de uitgezette opdracht tot het governance onderzoek is de Gemeente Breda het jaar 2019 goed van start gegaan. Uitdagingen volgden elkaar echter al snel op. In februari 2019 heeft de functionaris gegevensbescherming aandacht gevraagd voor de informele opbouw van het privacyteam dat bestond uit de privacy coördinator en de privacy adviseurs. De vier medewerkers waren gepositioneerd bij drie verschillende teamleiders en geen van de teamleiders had zicht op de werkzaamheden, het functioneren of de werkdruk. Bovendien ontbrak het aan persoonlijke aandacht en coaching waar medewerkers, zeker in een pioniersrol, behoefte aan hebben. In deze context werd de functionaris gegevensbescherming al snel als (informeel) leidinggevende beschouwd. Zij heeft deze situatie bij de directie gesignaleerd en aangegeven dat een nauwe samenwerking tussen de functionaris gegevensbescherming en het team noodzakelijk is, maar dat zij vanuit hun eigen rol en deskundigheid de organisatie moeten kunnen adviseren en daarover van inzicht moeten kunnen verschillen. Bovendien achtte de functionaris gegevensbescherming de positie als (informeel) leidinggevende onverenigbaar met haar rol als toezichthouder. In afwachting van de resultaten van het governance-onderzoek is één van de teamleiders vanuit de afdeling ICO aangewezen als overkoepelend leidinggevende.

De volgende uitdaging die zich voordeed was uitval en vertrek van verschillende medewerkers, waardoor de capaciteit werd teruggebracht van 3,5 naar 1,5 fte. Al snel bleek dat het met deze capaciteit onmogelijk werd te voldoen aan de vraag vanuit de organisatie en om adequaat om te gaan met gesignaleerde risico's. Adviesvragen werden niet tijdig beantwoord, contracten werden incompleet gesloten, aanbestedingen liepen vertraging op, en de bereidheid vanuit de organisatie om advies te vragen nam sterk af, juist nu er in de afgelopen jaren is geïnvesteerd in bewustwording en toegankelijkheid. Door deze gang van zaken werd ook de functionaris gegevensbescherming niet tijdig en naar behoren betrokken. Daarnaast bleven andere onderdelen die in deze implementatiefase aandacht behoeven liggen, zoals het op orde krijgen van gegevensmanagement, bewustwording, het kunnen voldoen aan AVG-verzoeken, het opstellen van beleid, enzovoorts. Kortom, de organisatie was met deze beperkte capaciteit niet in staat de persoonsgegevens van betrokkenen te beschermen.

De functionaris gegevensbescherming heeft diverse gesprekken gevoerd met de directie en het management om het capaciteitsprobleem aan de orde te stellen en te adviseren in oplossingen. Hoewel het probleem werd ingezien, moet de functionaris gegevensbescherming constateren dat er niet tijdig en onvoldoende adequaat geageerd is om de organisatie en de betrokken medewerkers een passende oplossing te bieden. Dit heeft ertoe bijgedragen dat het probleem in omvang en ernst toenam, met alle risico's van dien.

#### **BLIK VOORUIT**

Waar de nadruk twee jaar geleden lag op de implementatie van de AVG, is het nu tijd over te gaan tot een volgende fase waarin de bescherming van persoonsgegevens een plek dient te krijgen in de organisatie dat past bij het belang en noodzaak van het onderwerp. Het thema kan en mag geen onderwerp meer zijn van een klein groepje professionals, maar dient in breder verband getrokken te

<sup>3</sup> Ten tijde van het schrijven van deze rapportage was het governance-advies nog in concept, versie 0.95

worden. Dat vraagt een actievere rol van de directie. Waar wil de directie zelf in prioriteren, welke doelen worden er gesteld en welke middelen worden daar voor vrij gemaakt?

Begin 2020 wordt er een Chief Privacy Officer (CPO) aangesteld vanuit VKA om het team beter in positie te begeleiden en een betere samenwerking tussen privacy en informatiebeveiliging te bewerkstellingen. Ook is het voornemen uitgesproken om er een interne strategische opgave van te maken.

#### AANBEVELINGEN

- Organisatorische inbedding van gegevensbescherming vraagt betrokkenheid en bewustzijn binnen alle lagen binnen de organisatie:
  - Het onderwerp vereist permanente aandacht van het College van B&W, de directie en het management;
  - Afdelingen zijn zelf verantwoordelijk voor adequate bescherming van persoonsgegevens en dienen maatregelen te treffen om goede bescherming te bieden;
  - Expertise op het gebied van gegevensbescherming is een vereiste om de organisatie te adviseren over en te begeleiden in goede gegevensbescherming.
- Let bij de aanstelling van specialisten op het gebied van gegevensbescherming op juridische en/of technische deskundigheid. Gegevensbescherming is een breed en dynamisch onderwerp dat zich snel ontwikkelt. Kundige expertise vraagt om kennis, ervaring, begrip en know how.
- Zorg voor goed zicht op de werkzaamheden, de werkdruk en het functioneren van medewerkers.
- Neem het onderwerp gegevensbescherming mee in de begroting en houdt rekening met de uitdagingen die er nog liggen.

Het onderwerp gegevensbescherming staat binnen de organisatie nog in de startblokken als het om adequate toepassing en borging van de AVG gaat, maar is tegelijkertijd al een onderwerp waar men niet omheen kan. Om te kunnen voldoen aan de vraag vanuit de organisatie en voortgang te krijgen in de implementatie van de AVG, is er expertise nodig: kennis van de AVG en informatiebeveiliging.

Om de rollen, taken en verantwoordelijkheden goed in te richten, wordt er een governance onderzoek gedaan. In de tussentijd dient er voldoende capaciteit beschikbaar te zijn. De functionaris gegevensbescherming is van mening dat daar de afgelopen periode niet voldoende zorg voor gedragen is, wat risico's voor betrokkenen en de organisatie met zich mee brengt.



## 4. Rechten van betrokkenen

### AANLEIDING

Het fundamentele recht op eerbiediging van de persoonlijke levenssfeer<sup>4</sup> dient betrokkenen in staat te stellen te controleren of gegevens juist en rechtmatig worden verwerkt. Daarnaast mogen betrokkenen verzoeken minder gegevens te verwerken of gegevens te verwijderen. De rechten van betrokkenen die hen meer controle mogelijkheden en zeggenschap geven, zijn vastgelegd in de AVG.<sup>5</sup> Deze 'AVG-rechten van betrokkenen' zijn sterke rechten die slechts beperkt mogen worden indien de reden tot weigering in de wet staat vastgelegd. De Gemeente Breda dient als verwerkingsverantwoordelijke verzoeken van betrokkenen die voortvloeien uit deze rechten, in behandeling te nemen.

### Risico's

De gemeente verwerkt van het wieg tot het graf gegevens van burgers, die zij vaak verplicht zijn te delen met de overheid. Doen burgers dat niet tijdig of op de juiste manier, dan lopen ze het risico daarop aangesproken of zelfs gesanctioneerd te worden. Dat brengt gemeenten in een machtige positie, en burgers in een afhankelijke positie. Het recht op gegevensbescherming en de daaruit voortvloeiende AVG-rechten van betrokkenen herstelt de asymmetrische verhouding deels en dwingt de overheid tot transparantie. Het voornaamste risico dat kan voortvloeien uit het niet (kunnen) voldoen aan verzoeken van burgers is dan ook dat het vertrouwen van burgers wordt aangetast en dat de Gemeente Breda imago schade oploopt.

Verondersteld wordt dat geen enkele gemeente in verband gebracht wil worden met de ondoorgroondelijke bureaucratie zoals in 'Het Proces' beschreven wordt door Franz Kafka. Verwerkingsverantwoordelijken worden door de AVG ook excentriek gemotiveerd: het niet kunnen voldoen aan AVG-verzoeken kan door de Autoriteit Persoonsgegevens worden bestraft met boetes die kunnen oplopen tot twintig miljoen euro, de maximale boete die op grond van de AVG gegeven kan worden. De Autoriteit Persoonsgegevens heeft op dit vlak al handhavend opgetreden bij andere organisaties. In 2018 heeft de toezichthouder een dwangsom ingevorderd van € 48.000 bij een bank omdat er niet volledig voldaan kon worden aan een verzoek tot inzage.<sup>6</sup> Daarnaast kunnen burgers zelf dwangsommen vorderen en rechtszaken aanspannen om hun rechten op te eisen.

### TERUGBLIK

De Gemeente Breda heeft sinds de inwerkingtreding van de AVG een aantal AVG-verzoeken ontvangen. De behandeling van deze verzoeken verliep uiterst moeizaam. Na verschillende signalen hiervan heeft de functionaris gegevensbescherming in september 2019 een evaluatie gedaan op de behandeling van de verzoeken. Hieruit bleek dat er in 2018 negen verzoeken waren gedaan en in 2019 vier verzoeken, echter met de kanttekening dat het precieze aantal onbekend is omdat er niet centraal en gestructureerd gedocumenteerd wordt. Naast het gebrek aan documentatie bleek dat verzoeken in de meeste gevallen niet tijdig werden afgerond en dat termijnen zonder gegronde

<sup>4</sup> Art. 8 EVRM

<sup>5</sup> In de artikelen 12 tot en met 22 in de AVG:

- Het recht op informatie (art. 12 t/m 14 AVG)
- Het recht op inzage (art. 15 AVG)
- Het recht op rectificatie (art. 16 AVG)
- Het recht op gegevenswissing (art. 17 AVG)
- Het recht op beperking van de verwerking (art. 18 AVG)
- Het recht op kennisgeving bij rectificatie, verwijdering of beperking (art. 19 AVG)
- Het recht op overdraagbaarheid van de gegevens (art. 20 AVG)
- Het recht op bezwaar (art. 21 AVG)
- Het recht niet te worden onderworpen aan geautomatiseerde individuele besluitvorming (art. 22 AVG)

<sup>6</sup> <https://autoriteitpersoonsgegevens.nl/nl/nieuws/tgb-betaalt-dwangsom-na-niet-voldoen-aan-inzageverzoek#subtopic-4542>

redenen overschreden werden. Het ontbrak aan een proces en aan technische ondersteuning om het proces te borgen. Ook de communicatie met betrokkenen verliep moeizaam.

In de zomer van 2018 is er een begin gemaakt aan het schrijven van een proces en zijn er rollen en taken belegd. De sturing hierop ontbrak echter. De functionaris gegevensbescherming heeft ook in eerdere rapportages gewezen op gebreken en daarover geadviseerd.

#### **BLIK VOORUIT**

De evaluatie op de AVG-verzoeken is besproken met de gemeentesecretaris en CIO (directeur bedrijfsvoering). Beiden gaven aan het onderwerp belangrijk te vinden en het hoog op de agenda te zetten. De CIO heeft opdracht gegeven tot het ontwikkelen van het proces en de technische ondersteuning daarvan en dit uiterlijk eind 2019 af te ronden. De Gemeente Breda is hier ook in geslaagd. Komend jaar zal getest en geëvalueerd moeten worden of deze nieuwe werkwijze voldoet.

#### **AANBEVELINGEN**

- Leidt medewerkers die verzoeken in behandeling nemen goed op. Zorg voor voldoende bewustwording, niet alleen op het gebied van de AVG, maar ook in relatie tot de algemene beginselen van behoorlijk bestuur en integriteit.
- Zorg ervoor dat het proces en de werkwijze niet afhankelijk is van één persoon want dit maakt de organisatie onnodig kwetsbaar.
- Voer een aantal testcases uit om de effectiviteit te beoordelen en tref indien nodig maatregelen om de werkwijze te verbeteren. Let daarbij op binnenkomst van het verzoek, de behandeltijd, de communicatie naar de betrokkene, de inhoudelijke kwaliteit en de registratie.
- Vraag om advies aan de functionaris gegevensbescherming en/of andere gemeenten.
- Zorg voor voldoende sturing en periodieke evaluatie en rapporteer hierover aan de CIO en functionaris gegevensbescherming.

De AVG-rechten van betrokkenen stelt burgers in staat meer controle uit te oefenen op de verwerking van hun gegevens. Het dwingt de verwerkingsverantwoordelijken tot transparantie. Dit zijn dan ook sterke rechten waar betrokkenen zonder verdere toelichting een beroep op mogen doen.

Het niet kunnen voldoen aan AVG-verzoeken kan lijden tot aantasting van het vertrouwen en imagoschade. Daarnaast kan de Autoriteit Persoonsgegevens de hoogste categorie boetes opleggen indien niet voldaan wordt aan de verplichtingen op dit vlak.

Uit een evaluatie van de functionaris gegevensbescherming is gebleken dat de Gemeente Breda nog veel stappen te zetten heeft om AVG-verzoeken naar behoren op te kunnen pakken. De gemeentesecretaris en CIO hebben dit hoog op de agenda gezet en hebben er zorg voor gedragen dat dit eind 2019 gerealiseerd werd.



## 5. Evenwicht tussen beleid en uitvoering

### AANLEIDING

Bij de inwerkingtreding van de AVG kwam voor veel gemeenten, zo ook voor de Gemeente Breda, de prioriteit te liggen bij de implementatie, toepassing en naleving van praktische zaken. De Autoriteit Persoonsgegevens stuurde daarop met een tienstappenplan waar organisaties direct mee aan de slag konden: een functionaris gegevensbescherming in dienst nemen, een verwerkersovereenkomst ontwikkelen en gebruiken, een verwerkingenregister vullen, et cetera.

De AVG moedigt verwerkingsverantwoordelijken echter vooral aan om goed na te denken over de verwerkingen van persoonsgegevens die uitgevoerd worden om dat achteraf te kunnen verantwoorden. Niet alleen ten opzichte van specifieke verwerkingen, maar ook op macroniveau. In een data-gedreven wereld is het aan de Gemeente Breda om Europese wetgeving vorm te geven op lokaal niveau. Een uitdaging die niet onderschat kan worden. Om dit te realiseren is noodzakelijk om van implementatie over te gaan tot strategie. Hierbij dient niet alleen rekening gehouden te worden met rechtmatigheid en begrotingen, maar ook met principiële en ethische kwesties. Bij het maken van dergelijke keuzes is de directie en het bestuur aan zet.

### Risico's

Datatechnieken en -toepassingen zijn continu in ontwikkeling. De Gemeente Breda is ambitieus in het verkennen en benutten van nieuwe mogelijkheden. De impact op de privacy van betrokkenen wordt echter ook steeds groter. Bij het in kaart brengen van kwetsbaren groepen in wijken bestaat het risico op stigmatisering van wijkbewoners. Pro actieve benadering vanuit de schuldhulpverlening bij mensen die mogelijk betaalproblemen hebben, kunnen betrokkenen een bespied gevoel geven. Datzelfde gevoel kan worden veroorzaakt door passanten te volgen in de binnenstad door middel van wifitracking of slimme camera's.

Maatschappelijke, organisatorische en individuele belangen dienen tegen elkaar opgewogen te worden. De Gemeente Breda dient hierin niet alleen projectmatig standpunten in te nemen. Een visie waarin kaders geboden worden en sturing concreet wordt, biedt de organisatie de ruimte om tijd en middelen effectief en efficiënt te benutten. Bij gebrek daaraan schieten enthousiaste ideeën als paddenstoelen uit de grond, zonder dat dit tot realistische resultaten leidt en tijd en middelen verloren gaan.

### TERUGBLIK

In 2017 is er een privacybeleid ontwikkeld voor het College van B&W als verwerkingsverantwoordelijke, maar niet vastgesteld. In het afgelopen jaar is het privacybeleid herzien en uitgebreid naar de burgemeester en de gemeenteraad als verwerkingsverantwoordelijken. Dit beleid is in concept in de afrondende fase. Ook is er een datalekkenprotocol ontwikkeld en bestuurlijk vastgesteld. Er is eveneens een informatiebeveiligingsbeleid, maar dat is gedateerd en niet tijdig herzien conform de Baseline Informatiebeveiliging Gemeenten (BIG). In 2018 is de i-Strategie ontwikkeld, waarin zeven wegen benoemd worden naar een digitaal Breda. De i-Strategie gaat over 2018 tot 2020. In het concept Strategisch Beleid voor Gegevensbescherming Gemeente Breda worden de onderwerpen privacy en informatiebeveiliging integraal opgenomen en worden de rollen, taken en verantwoordelijkheden belegd.<sup>7</sup>

Het ontbreekt binnen de Gemeente Breda aan een concreet uitgewerkt beleid waarin bepaald wordt wie toegang geeft of krijgt tot bepaalde informatie (autorisatiebeleid) en hoe er wordt omgegaan met het ontsluiten van informatie in spoedeisende gevallen. Ook is het medewerkers onduidelijk op

<sup>7</sup> Ten tijde van het schrijven van deze rapportage was het beleid nog in concept, versie 0.95

welke wijze bedrijfsmiddelen zoals telefoons en laptops gebruikt mogen worden. Privégebruik al dan niet toestaan, wordt niet beschreven. Bovendien is niet vastgesteld waar leidinggevendenden op mogen controleren en op basis van welke voorwaarden een controle geschied. Gebrek aan dergelijk beleid zorgt te vaak voor tijdrovende situaties waarbij wet- en regelgeving praktische mogelijkheden en voor de hand liggende oplossingen blokkeren. Zo is het bijvoorbeeld toegestaan medewerkers te controleren en indien noodzakelijk toegang te verkrijgen tot mailboxen, mits het proces vooraf is vastgesteld en gecommuniceerd is met medewerkers. Neemt de organisatie niet de moeite om dergelijke zaken vooraf goed te regelen, dan is het heel moeilijk (en vaak onrechtmatig) om adequaat te kunnen handelen wanneer een situatie dat vereist.

### **BLIK VOORUIT**

Er dient nog veel te gebeuren in de ontwikkeling van beleid, maar ook in de praktische uitvoering daarvan. Om te organisatie op weg te helpen is er eerst meer betrokkenheid en eigenaarschap vanuit de directie en het bestuur vereist. Er dient een visie ontwikkeld te worden omtrent datagebruik waarin maatschappelijke, organisatorische, juridische, financiële en ethische aspecten betrokken worden. Zonder een dergelijke visie blijft het voor de organisatie onduidelijk wat van hen verwacht wordt en welke middelen daarvoor beschikbaar gesteld worden.

Vervolgens is het van belang dat rollen, taken en verantwoordelijkheden (beter) belegd worden. Er wordt nog niet goed gestuurd op werkzaamheden gerelateerd aan gegevensbescherming. Dat draagt er in bij dat het te vaak voorkomt dat projecten sneuvelen alvorens de eindstreep bereikt te hebben. Het Strategisch Beleid voor Gegevensbescherming (dat nog moet worden vastgesteld) kan bijdragen in een oplossing hiervoor. Naast beleid is er een praktische vertaalslag nodig om het papier tot leven te laten komen.

### **AANBEVELINGEN**

- Begin het jaar 2020 met een sessie voor de directie om de mogelijkheden van dataverwerking te verkennen, begeleid door een expert. Betrek hierbij de functionaris gegevensbescherming en verzoek haar de directie te adviseren alvorens tot een concrete visie te komen.
- Benut het eerste half jaar van 2020 voor het opstellen van een helder beleid. Neem het tweede deel van het jaar om stap voor stap de beleidsstukken die nog ontbreken te ontwikkelen en vast te stellen.
- Zorg ervoor dat er eind 2020 minimaal een visie, een vastgesteld gegevensbeschermingsbeleid (inclusief een privacybeleid en informatiebeveiligingsbeleid) en een beleid rondom het gebruik en beheer van bedrijfsmiddelen ligt.
- Zorg voor sturing waarbij niet alleen opdrachten worden verstrekt, maar ook de resultaten in beeld worden gebracht.
- Koppel aan elk beleidsstuk een PDCA-cyclus waarmee de opvolging en uitvoering van het beleid geborgd wordt.
- Communiceer visie en beleid met de organisatie om bewustwording te creëren.

De AVG moedigt verwerkingsverantwoordelijken aan om vooral goed na te denken over de verwerkingen van persoonsgegevens om dat achteraf te kunnen verantwoorden. De Gemeente Breda staat voor de grote uitdaging om in een data-gedreven wereld die aan veel ontwikkeling en verandering onderhevig is, Europese wetgeving lokaal toe te passen. Daarbij dient zij niet alleen oog te hebben voor juridische en financiële aspecten, maar ook voor ethische aspecten. De directie en het bestuur zijn hiervoor aan zet.

Het ontbreekt binnen de organisatie nog te veel aan beleid waarin is vastgesteld wat van het management en medewerkers verwacht wordt. Daardoor worden er te vaak ad hoc beslissingen genomen die niet goed geborgd zijn en soms onrechtmatig zijn. Dat kan voorkomen worden door vooraf strategisch te denken en processen vast te leggen. Benut het jaar 2020 om hier een goede basis in te leggen.



## 6. Samenwerking

### AANLEIDING

'Breda brengt het samen' luidt het motto van de Gemeente Breda. Daad wordt bij woord gevoegd door de samenwerking te initiëren. Binnen de organisatie wordt er keten-overstijgend gewerkt. Als centrumgemeente pakt te Gemeente Breda een regierol in samenwerkingsverbanden met publieke partners. Ook wordt er samengewerkt met private partijen. De Gemeente Breda faciliteert en levert diensten als uitvoerende partij, waarbij persoonsgegevens van andere verwerkingsverantwoordelijken verwerkt worden. Op haar beurt doet de Gemeente Breda als verwerkingsverantwoordelijke beroep op leveranciers en uitvoerders aan wie persoonsgegevens worden toevertrouwd.

De Gemeente Breda staat voor grote uitdagingen. Van het organiseren van jeugdzorg binnen de regio tot het terugdringen van misbruik van overheidsmiddelen. Taken met stevige verantwoordelijkheden en zwaarwegende belangen. Waarbij ook de bescherming van persoonsgegevens geborgd dient te worden.

### Risico's

De samenwerking opzoeken en informatie uitwisselen brengt vele voordelen met zich mee. Organisaties kunnen zoals sneller en effectiever werken. Betrokkenen hoeven niet bij elk loket hetzelfde verhaal te vertellen. Het uitbesteden van verwerkingen van persoonsgegevens zorgt ervoor dat niet elke organisatie dezelfde expertise in huis hoeft te hebben. Het samenbrengen van persoonsgegevens vormt echter ook risico's voor betrokkenen. Het verhaal dat een betrokkene deelt met een regievoerder, is wellicht niet ook (in detail) bestemd voor een andere klantmanager of maatschappelijk werker. En als de ene medewerker een indruk deelt dat zonder opzet en met de beste bedoelingen toch erg gekleurd is, gaat een andere medewerker vaak uit van de professionaliteit van zijn collega. Het kan burgers in een nog afhankelijkere positie brengen, omdat de gegevens die zij verplicht zijn te delen met de overheid, nu ook intern en extern met andere partijen worden gedeeld. Vaak zonder dat een betrokkene daar zelf iets over te zeggen heeft. Bovendien wordt het moeilijker AVG-rechten uit te oefenen. Want het controleren van de juistheid van de gegevens wordt erg ingewikkeld als het verwerkt wordt door verschillende partijen, evenals het laten corrigeren ervan.

Ook voor organisaties brengt samenwerking risico's met zich mee. Zo dragen samenwerkingspartners in sommige gevallen gezamenlijke verantwoordelijkheid waardoor ze niet alleen voor het eigen handelen, maar ook voor het handelen van de ander verantwoordelijk zijn. Indien er beroep wordt gedaan op verwerkers die in opdracht van de verantwoordelijke partij persoonsgegevens verwerken, is de verantwoordelijke partij verplicht er op toe te zien dat de verwerker voldoet aan de wetgeving en passende bescherming biedt. Het is dan ook zaak naast de voordelen, ook de risico's scherp te hebben en de samenwerking goed en consistent vorm te geven.

### TERUGBLIK

Bij samenwerkingen waarbij verwerkingsverantwoordelijken een beroep doen op een partij om gegevens te verwerken, is een verwerkersovereenkomst verplicht. Hierin wordt vastgelegd hoe partijen omgaan met persoonsgegevens en hoe de gegevens beschermd dienen te worden. In 2017 heeft de functionaris gegevensbescherming samen met een privacy adviseur een verwerkersovereenkomst ontwikkeld en deze afgestemd met informatiebeveiliging. Deze overeenkomst is in 2018 herzien, waarna er ook een handleiding geschreven is voor medewerkers. De verwerkersovereenkomsten kunnen centraal worden opgeslagen door contractmanagement, waar deze gekoppeld worden aan de hoofdovereenkomst. Momenteel staan er veertig verwerkersovereenkomsten geregistreerd. Naar waarschijnlijkheid zijn er echter meer verwerkersovereenkomsten gesloten, maar zijn ze niet allemaal centraal geregistreerd. Bij het



privacy advies-team komen geregeld vragen binnen over het sluiten van verwerkersovereenkomsten. Vaak wordt er door partijen onderhandeld over clausules, waardoor maatwerk vereist is.

In het afgelopen jaar bleek een partij die zeer gevoelige en bijzondere persoonsgegevens verwerkt niet te voldoen aan de standaard beveiligingseisen die de Gemeente Breda aan haar verwerkers stelt. Gezien de hoge risico's voor betrokkenen en de organisaties (Breda handelde mede namens gemeenten binnen de regio), heeft de functionaris gegevensbescherming de verwerker verzocht aantoonbaar te maken wat het beveiligingsniveau was van de organisatie. Vervolgens zijn er afspraken gemaakt tussen de verwerker en de Gemeente Breda om passende maatregelen te treffen in de periode waarin de verwerker nog niet aan de vereisten voldoet. Inmiddels doorloopt de verwerker een certificeringstraject om aantoonbaar aan de internationale beveiligingsnormen te voldoen.

Alertheid bij het sluiten van overeenkomsten waarbij persoonsgegevens verwerkt worden, is zeer belangrijk. De Gemeente Breda mag alleen een beroep doen op verwerkers die afdoende garanties bieden door middel van passende technische en organisatorische maatregelen om de gegevens te beschermen. Het privacy advies-team begeleidt afdelingen hier vakkundig in.

De Gemeente Breda heeft in het afgelopen jaar een aantal convenanten gesloten met samenwerkende partijen. Voor deze vorm wordt meestal gekozen als er een gezamenlijke verantwoordelijkheid is. De convenanten worden op nationaal niveau ontwikkeld, zodat gemeenten en andere samenwerkingspartners daar in het hele land gebruik van kunnen maken. De noodzaak tot een convenant vloeit vaak voort uit gebrek aan passende wetgeving waarin de uitwisseling van persoonsgegevens wordt geregeld. Met een convenant wordt getracht de uitwisseling zo goed en veilig mogelijk in te richten. Daarbij moet echter wel gemeld worden dat convenanten geen oplossing bieden voor het gebrek aan een rechtmatige grondslag.

#### **BLIK VOORUIT**

Vanaf 2020 worden gemeenten geacht de modelverwerkersovereenkomst van de VNG te gebruiken. Dit kan voordelen bieden omdat het een landelijk model is dat ook door veel verwerkers gedragen wordt. De verwachting is dat dit een deel van het werk weg zal nemen, omdat er minder discussie over clausules zal zijn. Met dit model is het echter de bedoeling dat er meer geregeld wordt in de hoofdovereenkomst en de bijlagen. Denk bijvoorbeeld aan aansprakelijkheidsclausules en beveiligingsmaatregelen. Om te voorkomen dat contracten inhoudelijk incompleet worden gesloten, of dat er willekeur ontstaat in de eisen die de Gemeente Breda stelt aan haar partners, is het van belang dat er goede standaarden ontwikkeld worden waar alle betrokken medewerkers mee kunnen werken. Samenwerking tussen inkoop, juridische zaken, informatiebeveiliging en privacy is noodzakelijk. Daarnaast dient er gezorgd te worden voor bewustwording bij de afdelingen.

Naast de verwerkersovereenkomsten dient er ook goed in beeld gebracht te worden met welke partijen de Gemeente Breda zaken doet, waarbij persoonsgegevens verwerkt worden. Momenteel ontbreekt dat overzicht, waardoor het onmogelijk te bepalen is of de samenwerkingen correct zijn vormgegeven en voldoen aan toepasselijke wet- en regelgeving. Dit kan met name binnen het Sociaal Domein en het Veiligheidsdomein tot hoge risico's leiden voor betrokkenen en de organisaties.

#### **AANBEVELINGEN**

- Breng bij (het aangaan van) samenwerkingen, naast de voordelen, ook de specifieke risico's in beeld voor betrokkenen en de organisaties ten aanzien van gegevensverwerking. Tref maatregelen om de risico's zo veel mogelijk uit te sluiten en/of te beperken. Betrek de functionaris gegevensbescherming daarbij en vraag om advies.
- Convenanten helpen de samenwerking goed vorm te geven, maar scheppen geen grondslagen voor rechtmatige gegevensverwerking. Betrek altijd eerst de functionaris

gegevensbescherming alvorens een besluit te laten nemen door het College van B&W, zodat haar advies bij het besluit betrokken kan worden.

- Bereid de overgang van de verwerkersovereenkomst naar het model van de VNG goed voor. Zorg ervoor dat inkoop, juridische zaken, informatiebeveiliging en privacy aan tafel zitten zodat met alle noodzakelijke disciplines wordt afgestemd waar de contracten en standaarden aan moeten voldoen. Zorg daarnaast voor bewustwording bij afdelingen zodat de contracten correct gesloten worden.
- Breng in kaart welke samenwerkingen er zijn en hoe deze zijn vormgegeven. Dit dient onderdeel te zijn van 'De basis op orde'.

Breda brengt het samen en dat biedt veel kansen, intern en extern. Naast de vele voordelen zijn er echter ook risico's waar aan de ontwerptafel rekening mee gehouden moet worden. Het laten meedenken vanuit de juiste expertise is dan ook cruciaal om de samenwerking goed vorm te geven. Convenanten, samenwerkingsovereenkomsten en verwerkersovereenkomsten zijn middelen die daarvoor ingezet kunnen worden, maar dienen wel op de juiste manier gebruikt te worden.

## 7. Datalekken

### AANLEIDING

De AVG spreekt van een datalek wanneer een inbreuk op de beveiliging leidt tot toegang, vernietiging, wijziging of vrijkomen van persoonsgegevens, zonder dat dit de bedoeling van de organisatie is of wettelijk toegestaan is. Datalekken dienen door de organisatie worden bijgehouden in een register en in sommige gevallen gemeld te worden aan de Autoriteit Persoonsgegevens en de betrokkene.

Geen enkele organisatie is vrij van fouten. Datalekken helpen in beeld te brengen welke menselijke en technische kwetsbaarheden er zijn binnen de organisatie. De Gemeente Breda heeft er dan ook belang bij dat zoveel mogelijk datalekken gemeld worden, zodat daar lering uit getrokken kan worden.

### Risico's

Het grootste risico voor de organisatie is dat datalekken niet gemeld worden waar dat wel verplicht is. Zonder de meldingsbereidheid van medewerkers en leidinggevenden kan de Gemeente Breda niet voldoen aan haar plicht om datalekken te registreren en maatregelen te treffen om de datalekken te dichten en te voorkomen. Van belang is dan ook dat de mogelijkheid om te melden laagdrempelig is en dat medewerkers niet meteen worden berispt, maar een helpende hand wordt uitgereikt en in oplossingen wordt gedacht.

Voor betrokkenen kunnen datalekken een enorme impact hebben. Het risico daarop wordt groter naar mate de gegevens bij een datalek privacygevoeliger zijn. Denk daarbij aan bijzondere persoonsgegevens, zoals gegevens over de gezondheid, etniciteit, religie of geaardheid. Ook financiële, strafrechtelijke gegevens of gegevens van kwetsbare groepen zoals kinderen of mensen die niet zelfredzaam zijn, verhogen de impact voor betrokkenen. Betrokkenen wiens gegevens openbaar zijn gemaakt, kunnen daar voor de rest van hun leven last van ondervinden. In zeer schrijnende gevallen kunnen betrokkenen dermate tot wanhoop gedreven worden dat ze het leven niet meer zien zitten. Ook de Gemeente Breda verwerkt gegevens die enorm privacygevoelig zijn. Hoewel datalekken helaas nooit volledig uitgesloten kunnen worden, dient er zorg voor gedragen te worden dat er organisatorisch en technisch voldoende maatregelen getroffen worden om persoonsgegevens zo adequaat mogelijk te beschermen.

### TERUGBLIK

In 2019 is er op verzoek van wethouder Adank en de gemeentesecretaris/ interim CIO door de functionaris gegevensbescherming en het privacy advies-team een datalekkenprotocol opgesteld, inclusief een draaiboek waarin beschreven staat hoe er met datalekken omgegaan moet worden en wie daarbij vanuit de organisatie betrokken moeten worden (variërend in impact van het datalek). Ook is het datalekkenformulier aangepast en is er een beoordelingsformulier ontwikkeld. Volgens een vast stramien worden datalekken gemeld, beoordeeld en geregistreerd. Bij de beoordeling van het datalek wordt door het privacy advies-team en de functionaris gegevensbescherming de ernst en impact ingeschat aan de hand van wettelijk bepaalde factoren. Aan de hand daarvan wordt bepaald welke oplossingen en maatregelen getroffen dienen te worden.

De e-learning bevatte één module over datalekken. In de periode die volgde op de training was er ten opzichte van het jaar daarop voorafgaand een forse stijging van het aantal meldingen. In de maanden januari en februari zijn er in 2019 zestien dataleken gemeld, in 2018 waren dat er drie. Uit het type meldingen en de gesprekken die erover gevoerd werden, bleek dat de e-learning had bijgedragen in de bewustwording.



In 2019 zijn er in totaal vierenzestig datalekken gemeld. In de meeste gevallen is er sprake van het uitlekken van gevoelige informatie, waarbij e-mails (of brieven) verkeerd geadresseerd werden. Dit komt overeen met de landelijke trend. De Autoriteit Persoonsgegevens heeft gepubliceerd dat in het eerste half jaar van 2019 in 63% van de datalekken sprake was van het versturen of afgeven van persoonsgegevens aan de verkeerde ontvanger.<sup>8</sup> In een aantal gevallen bleken datalekken veroorzaakt te worden door systeemtechnische problemen, waarbij gegevens niet of onvoldoende werden afgeschermd en onbevoegden toegang verkregen tot de informatie.

### **BLIK VOORUIT**

Het onderwerp datalekken dient blijvend onder de aandacht gebracht te worden bij medewerkers en het management. Het datalekkenprotocol bevat veel nuttige informatie en wordt op verzoek van de functionaris gegevensbescherming daarom vertaald naar een tweetal digitale flyers: één voor het management met tips over hoe een datalek voorkomen kan worden, en één voor de gehele organisatie met een stappenplan die doorlopen kan worden ingeval van een datalek. Ook wordt er een kort filmpje ontwikkeld waarin medewerkers worden geïnformeerd over de inhoud van het datalekkenprotocol.

Alleen bewustwording is echter niet voldoende. Medewerkers dienen gefaciliteerd te worden om datalekken te voorkomen. De organisatie dient er zorg voor te dragen dat medewerkers er op mogen vertrouwen dat de apparatuur waarmee ze werken veilig is, evenals de systemen waarin ze werken. Daar zijn het afgelopen jaar belangrijke stappen in gezet, door de apparatuur te beveiligen. Ook is het mogelijk op afstand gegevens te wissen indien sprake is van diefstal of verlies. Praktische tips en workshops over veilig e-mailgebruik kunnen eveneens helpen. De plannen hiervoor zijn er al, maar blijven helaas vaak te lang op de plank liggen. Goede sturing is dan ook nodig om plannen ook daadwerkelijk tot uitvoer te laten brengen.

Grotere datalekken die veroorzaakt worden door systeemtechnische fouten lossen zichzelf niet op. In dergelijke gevallen dienen er dan ook passende maatregelen getroffen te worden om de lekken te dichten. Aanpassingen dienen in voorkomende gevallen door leveranciers verricht te worden. Van de Gemeente Breda mag als verwerkingsverantwoordelijke partij verwacht worden dat zij leveranciers er op aanspreekt dat ook zij gebonden zijn aan de AVG.

### **AANBEVELINGEN**

- Indien datalekken niet gemeld worden, lopen betrokkenen én de organisatie risico's. Blijf dan ook investeren in bewustwording om de meldingsbereidheid van medewerkers hoog te houden. Zorg daarbij voor voldoende sturing zodat plannen ook daadwerkelijk tot uitvoering komen.
- Pak systeemtechnische problemen aan en spreek leveranciers aan op hun verantwoordelijkheden.
- Zorg ervoor dat er passende beveiligingsmaatregelen worden getroffen die voldoen aan de stand van techniek. De informatiebeveiligingsdienst en de Autoriteit Persoonsgegevens publiceren regelmatig waar organisaties aan moeten worden. Controleer periodiek of de Gemeente Breda daar voldoende in mee gaat.

<sup>8</sup>[https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/meldplicht\\_datalekken\\_feiten\\_en\\_cijfers\\_1e\\_half\\_2019.pdf](https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/meldplicht_datalekken_feiten_en_cijfers_1e_half_2019.pdf)

In 2019 zijn er e-learning modules geweest waarmee de bewustwording rondom datalekken vergroot is. Het is van belang het bewustzijn onder medewerkers en het management op peil te houden. Betrokkenen en de organisatie lopen risico's indien datalekken niet gemeld worden.

De Gemeente Breda heeft in 2019 een datalekkenprotocol ontwikkeld, inclusief een draaiboek, een meldings- en beoordelingsformulier. Dit protocol is bestuurlijk vastgesteld en zal komend jaar onder de aandacht gebracht worden bij medewerkers en het management.

In 2019 zijn er 40 datalekken gemeld, waarbij in het gros van de gevallen sprake was van het uitlekken van gevoelige informatie.

## 8. Netwerk

De AVG is relatief nieuwe wetgeving en vraagt om verandering in het werken. Gemeenten en ook andere organisaties proberen elkaar te vinden tijdens bijeenkomsten en overleggen, zodat niet ieder voor zich het wiel hoeft uit te vinden. Dat wordt gefaciliteerd door verenigingen zoals de VNG, IBD en het Nationaal Genootschap Functionarissen Gegevensbescherming (NGFG). Functionarissen gegevensbescherming en privacy adviseurs initiëren ook zelf overleggen om ervaringen met elkaar uit te wisselen en te overleggen over de interpretatie en toepassing van wetgeving.

De privacy adviseurs en de functionaris gegevensbescherming zijn aangesloten bij een regionaal overleg waarbij casuïstiek met elkaar besproken wordt. Daarnaast is de functionaris gegevensbescherming onderdeel van een intervisiegroep met functionarissen gegevensbescherming van grote en middelgrote gemeenten (waaronder Tilburg, Eindhoven, Rotterdam, Den Haag en Drechtsteden). In deze netwerkgroepen wordt informatie met elkaar uitgewisseld en worden er stukken gedeeld die voor deelnemende gemeenten van nut kunnen zijn. Daarbij wordt uiteraard rekening gehouden met bedrijfsgevoelige informatie. De overleggen zijn daarnaast goed om de werkzaamheden en het eigen functioneren te spiegelen aan dat van collega's in andere gemeenten.

Naast de periodieke overleggen worden er ook regelmatig gesprekken gevoerd met andere organisaties. Zo is er in het afgelopen jaar gesproken met lokale collega's van Zorg voor Elkaar, het CJG en de GGD, maar bijvoorbeeld ook landelijke spelers. Verschillende perspectieven helpen in kaart te brengen wat de verwachtingen zijn van organisaties ten opzichte van de overheid.



## 9. Verantwoording van verwerkingen

### VERWERKINGENREGISTER

Sinds de inwerkingtreding van de AVG zijn verwerkingsverantwoordelijken verplicht zelf een overzicht bij te houden van de verwerkingen van persoonsgegevens. De Gemeente Breda beschikt over een standaard verwerkingenregister. Daarin staan de verwerkingen die voor de meeste gemeenten gelden op grond van de gemeentelijke taken. In het najaar van 2018 zijn de privacy ambassadeurs de standaardverwerkingen gaan vergelijken met de verwerkingen die in de praktijk worden uitgevoerd binnen de afdelingen, als onderdeel van 'De basis op orde'. Ondanks een moeilijke start is er in het tweede half jaar van 2019 voortgang gekomen in het traject. Veel afdelingen waar een ambassadeur voor is, voltooien in 2019 hun onderdeel van het register.

### VERANTWOORDINGSDOCUMENTEN

Nieuwe en risicovolle verwerkingen worden overlegd met het privacyteam, informatiebeveiliging en de functionaris gegevensbescherming. Daarbij wordt onderzocht welke gegevens met welk doel en op basis van welke grondslag verwerkt zullen worden. Dit wordt in kaart gebracht middels een verantwoordingsdocument waarin de belangrijkste vragen door de afdeling of projectgroep (met behulp van het privacyteam en informatiebeveiliging) beantwoord worden. Na de beantwoording wordt de verwerking voorgelegd aan de functionaris gegevensbescherming. Zij voorziet de verantwoordelijken van een advies. In 2019 zijn er 25 verantwoordingsdocumenten beoordeeld.

### DPIA's

In sommige gevallen ontstaat een vermoeden van een verwerking met een hoog risico. Daarvan kan bijvoorbeeld sprake zijn als er gebruik wordt gemaakt van nieuwe technologieën, profilering, monitoring of in geval van verwerking van bijzondere persoonsgegevens. De Gemeente Breda is dan verplicht een DPIA (Data Protection Impact Assessment) uit te voeren om de risico's in kaart te brengen en maatregelen te treffen om de risico's uit te sluiten of te beperken. De functionaris gegevensbescherming heeft samen met een privacy adviseur een gebruiksvriendelijke DPIA ontwikkeld waarmee medewerkers zelf aan de slag kunnen indien een DPIA verplicht is. Het privacyteam en informatiebeveiligingsadviseur ondersteunen bij het invullen van de DPIA en geven eerstelijns advies aan de afdeling of projectgroep en aan de functionaris gegevensbescherming. Vervolgens beoordeeld de functionaris gegevensbescherming de verwerking en geeft een eindadvies aan de verantwoordelijken. In 2019 zijn er 9 DPIA's uitgevoerd.

## 10. Verantwoording van de functionaris gegevensbescherming

In deze rapportage is uitgegaan van de belangrijkste verplichtingen van verwerkingsverantwoordelijken die in de AVG en de checklist 'Houd grip op gegevens' van de Autoriteit Persoonsgegevens worden genoemd. Daarnaast zijn de aanbevolen onderwerpen uit het format 'FG Jaarrapportage College van Burgemeester en Wethouders, IBD' verwerkt.

Voorafgaand aan deze rapportage zijn verschillende metingen en evaluatiemomenten geweest. In het najaar van 2018 is er een nulmeting verricht door Privacy Management Partners. Naar aanleiding van deze nulmeting heeft de functionaris gegevensbescherming een stand van zaken rapport opgesteld waarin de belangrijkste uitdagingen geprioriteerd werden. Uitgaande van het volwassenheidsniveau van de organisatie zijn er praktische en haalbare aanbevelingen gedaan om in 2019 tot verbeteringen te komen.

In mei 2019 heeft de functionaris gegevensbescherming een tussenrapportage geschreven en deze gericht tot de directie en het management. Reden hiervoor was dat de functionaris gegevensbescherming niet voldoende voortgang constateerde om de bescherming van persoonsgegevens in 2019 tot een hoger en passend niveau te brengen. Dit werd besproken met het management en directie, waarbij tevens is aangegeven dat de benoemde aandachtspunten in de tussenrapportage zouden terugkeren in de jaarrapportage. Vervolgens is er op een aantal vlakken hard gewerkt en dat heeft tot positieve resultaten geleidt. Ook aanbevelingen naar aanleiding van de evaluatie op AVG-verzoeken zijn hoog geprioriteerd, waardoor het vastleggen van het proces en het inregelen van technische ondersteuning voor het eind van 2019 gerealiseerd zijn.

Het afdelingshoofd ICO, de Ciso en het privacy adviesteam zijn uitgenodigd informatie aan te leveren die zij voor deze rapportage relevant achtten. Ook is de conceptversie voorgelegd aan de directeur bedrijfsvoering, het afdelingshoofd ICO, de teamleider van het privacyteam en de Ciso. Reacties en suggesties zijn verwerkt voor zover deze aantoonbaar gemaakt konden worden.

De functionaris gegevensbescherming is regelmatig in gesprek gegaan met de wethouder, directie, het management en de uitvoering om de voortgang te bespreken en te adviseren. Zowel de portefeuille houdende wethouder als de gemeentesecretaris hebben herhaaldelijk aangetoond de bescherming van persoonsgegevens hoog te prioriteren. Dit heeft bijgedragen in bewustwording, het agenderen van verbeterpunten en het behalen van resultaten.