Gemeente Scherpenzeel

Jaarverslag

Functionaris Gegevensbescherming 2019

Jaarverslag

Functionaris Gegevensbescherming 2019

Opdrachtgever:	gemeente Scherpenzeel Afdeling Bedrijfsvoering
Auteur:	Sascha Beekman, FG
Datum:	27 januari 2020

Inhoud

MANAGEMENTSAMENVATTING

Dit verslag betreft de periode van 1 januari 2019 tot en met 31 december 2019. In deze verslagperiode is het volgende gerealiseerd:

- Het Jaarverslag FG over 2017-2018 is in februari 2019 vastgesteld, deze is geplaatst op de website van de gemeente.
- Met alle verwerkers zijn verwerkersovereenkomsten afgesloten; dit overzicht wordt actueel gehouden. Bij nieuw af te sluiten overeenkomsten wordt (indien nodig) gelijk een verwerkersovereenkomst afgesloten.
- In de zomer is het register geactualiseerd, maar een nieuw register komt er nu nog niet. Er zijn hooguit een paar kleine punten die intern opgepakt zijn om nog beter aan de AVG te voldoen, maar die de in het register opgenomen verwerkingen niet wijzigen. In 2020 zal weer een controle op actualisatie van het register gedaan worden.
- Er zijn toestemmingsformulieren voor Sociaal Domein gemaakt en de klantmanagers gebruiken deze ook. Folders/brochures Sociaal Domein zijn ook aangepast aan AVG.
- De in 2017/2018 uitgevoerde Privacy Impact Analyses (PIA's) zijn nagelopen op wijzigingen en in 2020 en 2021 worden de vakgebieden waarvoor een PIA is uitgevoerd herzien/opnieuw beoordeeld worden. Iedere 3 jaar moet een PIA herzien worden, dus dan liggen we goed op schema. Voor nieuw aan te schaffen of in gebruik te nemen (gewijzigde) software wordt standaard een PIA uitgevoerd.
- Er is een (interne) procedure / werkinstructie opgesteld hoe een verzoek ten aanzien van de rechten van betrokkenen behandeld moet worden. Er is een algemene procedure en een aanvullende procedure voor het Sociaal Domein.
- Om het bewustzijn over het veilig en zorgvuldig werken met persoonsgegevens vast te houden en te verbeteren, is er in het voorjaar van 2019 een medewerkersbijeenkomst gehouden over dit onderwerp en is er in het najaar van 2019 een start gemaakt met het inrichten van een bewustwordingsactie waarbij korte e-learning modules worden ingezet. Door met regelmaat de onderwerpen "Informatieveiligheid" en "Privacy" onder de aandacht te brengen, beklijft dit beter. Deze e-learning zal in Q1 2020 aanvangen.
- Thuiswerken/telewerken wordt al langere tijd gefaciliteerd, maar sinds december 2018 is daarvoor een Telewerkregeling vastgesteld. Vervolgens is in het voorjaar van 2019 tijdens de gesprekscyclus met alle medewerkers een telewerkovereenkomst voor incidenteel of structureel telewerken afgesloten.

In de vorige verslagperiode, van 1 oktober 2017 tot en met 31 december 2018 is hard gewerkt om aan alle vereisten van de AVG te voldoen. In het jaarverslag 2017-2018 is al aangegeven dat er continue aandacht besteed dient te worden aan privacy van burgers, bedrijven en medewerkers, waarbij een zorgvuldige verwerking en de bescherming daarvan steeds gewaarborgd moeten zijn. Daarbij is het belangrijk het bewustzijn van dit belang goed tussen de oren te hebben en te houden. In de huidige verslagperiode, het jaar 2019, zijn al stappen gezet om de privacy en de bescherming van persoonsgegevens te borgen.

2. GOVERNANCE

○ 2.1 Governance algemeen

Er is een duidelijke structuur aangaande de governance aanwezig wat betreft de uitvoering van de AVG. Er zijn met ingang van 1 oktober 2017 een Chief Information Security Officer (CISO) en een Functionaris Gegevensbescherming (FG) aangewezen door het college bij besluit van 5 september 2017 alsook een beschrijving van de onderlinge relaties en verantwoordingen. Deze onderlinge relaties en verantwoordingen blijken uit het op 13 februari 2018 door het college vastgestelde Privacybeleid. Hiermee wordt voldaan aan artikel 5 lid 2 van de AVG dat bepaalt dat een organisatie dient aan te kunnen tonen 'in control' te zijn aangaande de uitvoering van de AVG.

○ 2.2 Verantwoording Functionaris gegevensbescherming

Op 5 maart 2019 is er een medewerkersbijeenkomst gehouden, waarbij de onderwerpen "privacy" en "informatiebeveiliging" onder de aandacht zijn gebracht om het bewustzijn bij de medewerkers te verhogen en vast te houden.

In 2019 zijn er nog een tiental verwerkersovereenkomsten afgesloten of vernieuwd, zodat inmiddels met alle verwerkers een overeenkomst is afgesloten. In geval van nieuwe overeenkomsten voor werken, leveringen of diensten wordt gelijktijdig een verwerkersovereenkomst afgesloten. Zo is de standaard-verwerkersovereenkomst bijvoorbeeld ook meegenomen als een van de vereisten waaraan een deelnemende partij moest voldoen in het aanbestedingstraject voor jobcoaching.

Verder zijn er in 2019 nog een paar PIA's uitgevoerd vanwege nieuwe soorten verwerkingen of nieuw aan te schaffen applicaties.

De VNG heeft medio 2019 een borgingsdocument opgeleverd, waarmee is aan te tonen hoe ver een organisatie staat met het borgen van de privacy en de bescherming van de persoonsgegevens. In het borgingsdocument zijn zowel AVG-vragen als Informatieveiligheidsvragen (veelal afkomstig van de BIO) opgenomen, zodat een mooi totaalbeeld te verkrijgen is bij het invullen daarvan. De Gemeente Scherpenzeel heeft een mooie score behaald, waaruit blijkt dat de gemeente zich goed bewust is en voldoende doordrongen is van het feit dat een gemeente veel persoonsgegevens, inclusief gevoelige en bijzondere persoonsgegevens verwerkt, en dat daar bewust en zorgvuldig mee omgegaan wordt. Ook de informatiebeveiliging is goed op orde.

○ 2.3 Verantwoording Privacy Officer

De gemeente Scherpenzeel werd, evenals in 2018 en 2017, ook in 2019 ondersteund door een externe privacy officer. Door deze privacy officer zijn op verschillende terreinen werkzaamheden verricht.

Sociaal domein
De informatieverstrekking in het sociaal domein is door de privacy officer getoetst en waar nodig verbeterd. Hiervoor zijn de gebruikte formulieren en brochures waar nodig aangepast. Ook is beschreven in welke gevallen de gemeente toestemming nodig heeft voor het delen van gegevens. Daarnaast is door de externe privacy officer een model opgesteld voor een convenant voor multidisciplinaire overleggen. Dit convenant kan als basis dienen voor de gegevensuitwisseling met externe partijen in het sociaal domein.

Overzicht partijen die persoonsgegevens ontvangen
Daarnaast is door de privacy officer een overzicht gemaakt van de partijen die gegevens ontvangen van de gemeente Scherpenzeel. Samen met de Functionaris gegevensbescherming is getoetst met welke partijen een overeenkomst moet worden gesloten over het uitwisselen van gegevens. Door de privacy officer is hiervoor een modelovereenkomst opgesteld. In 2020 wordt de overeenkomst aan partijen voorgelegd.

Toetsingskader verwerkers
In 2018 zijn door de Functionaris gegevensbescherming de meeste verwerkersovereenkomsten afgesloten. In deze overeenkomsten staan een groot aantal verplichtingen voor verwerkers. Om te toetsen of deze verwerkers voldoen aan de afspraken, is door de privacy officer een toetsingskader opgesteld. In 2020 zal deze toetsing uitgevoerd worden.

Overzicht DPIA's
De privacy officer heeft in het register van verwerkingen een kolom toegevoegd. Bij iedere verwerking uit het register is beoordeeld of een DPIA noodzakelijk is en of deze reeds is uitgevoerd. Dit overzicht zal in 2020 gebruikt worden bij de actualisatie van de DPIA's.

○ 2.4 Verantwoording CISO

In regionaal verband is er regulier CISO overleg waarbij zaken zoals informatiebeveiliging, samenwerking mbt ENSIA en de invoering van de BIO (Baseline Informatiebeveiliging Overheden). 2020 wordt gezien als een overgangsjaar waarin de BIG wordt vervangen door de BIO. Om de implementatie van deze BIO normen te verwezenlijken blijft goede samenwerking noodzakelijk.

Op 27 februari 2018 heeft het college het gemeente brede Informatieveiligheidsbeleid vastgesteld en in juli 2018 heeft het college het Informatieveiligheidsplan vastgesteld. In dit beleid en plan is vanuit verschillende wettelijke kaders, w.o. de AVG, aandacht gevraagd voor de verplichtingen waaraan voldaan moet worden bij de inrichting van de ICT-infrastructuur van de gemeentelijke organisatie. Tijdens de ICT migratie is hier aan voldaan.

De CISO heeft de coördinatie over ENSIA, waarvoor o.a. van de FG input ontvangen is voor de vragen over de AVG.

Alle benodigde informatie welke nodig is voor de ENSIA verantwoording is op tijd geleverd, zodat ruim voor de aangegeven einddatum de verantwoording in ENSIA heeft

plaatsgevonden. Ook met betrekking de verplichte SUWI-audit is de bewijslast tijdig en volledig aangeleverd zodat gemeente Scherpenzeel op alle gestelde normen voldoet.

Beveiligingsmeldingen worden conform de Procedure Meldplicht datalekken geanalyseerd en afgehandeld. Zie verder bij 3.3.

3. WERKZAAMHEDEN EN BEVINDINGEN

3.1 Privacybeleid

Op 13 februari 2018 is het Privacybeleid door het college vastgesteld.
In dit beleid zijn de taken, rollen en verantwoordelijkheden van de FG en CISO opgenomen, evenals de procedures rondom datalekken en toezicht. Zaken zoals big data, tracking etc. zijn ook opgenomen in dit beleid, zodat het voor de inwoners van de gemeente Scherpenzeel inzichtelijk is welke gegevens de gemeente verzameld en wat de gemeente met de gegevens doet. Dit is in het beleid opgenomen, omdat het college het belangrijk vindt dat de inwoners (burgers en bedrijven) erop kunnen vertrouwen dat de bescherming van de door hen aan de gemeente toevertrouwde gegevens gewaarborgd is.

In 2019 is het beleid beoordeeld op actualiteit en het beleid voldoet nog en hoeft nog niet herzien te worden. In 2020 wordt het beleid opnieuw beoordeeld en indien nodig geactualiseerd en herzien.

Met de komst van de Wet normalisering rechtspositie ambtenaren en de CAO gemeenten per 1 januari 2020 zijn in 2019 alle personeelsregelingen zijn doorgenomen en opgenomen in het Personeelshandboek. Onder andere het privacyreglement e-mail en internetgebruik, het privacyreglement personeel, de verzuimregeling en beoordelingsregeling zijn herzien en aangepast, waardoor ook deze regelingen voldoen aan de AVG.

3.2 Register van verwerkingen

Het register van verwerkingen is door het college vastgesteld op 17 juli 2018. Het register is openbaar gemaakt door plaatsing op de gemeentelijke website. Aan het register is in 2019 een kolom toegevoegd waarin bij iedere verwerking is opgenomen of het verplicht is om een DPIA uit te voeren en wanneer deze is gedaan. In 2020 zal het register geactualiseerd worden. Daarbij zal ook (opnieuw) een toets worden gedaan aan de beginselen van de AVG, zoals proportionaliteit en subsidiariteit.

3.3 Meldingen datalekken

Op 5 september 2017 heeft het college de geactualiseerde procedure meldplicht datalekken vastgesteld. Er wordt een register bijgehouden, waarin alle beveiligingsincidenten opgenomen worden. In dat register, waarvoor alleen de FG en CISO geautoriseerd zijn, wordt vermeld welke beveiligingsincidenten voorgekomen zijn, welke daarvan aangemerkt zijn als datalek, of deze gemeld zijn aan de Autoriteit Persoonsgegevens en/of betrokkenen en of er (technische of organisatorische) maatregelen getroffen zijn.

In 2019 hebben 11 beveiligingsincidenten plaatsgevonden, waarvan er 5 zijn aangemerkt als meldenswaardig datalek. Deze zijn gemeld bij de AP. Van deze gemelde datalekken zijn er 3 meldingen gedaan aan betrokkenen, waarbij in een van de gevallen de gemeente was aan te merken als betrokkene. De veroorzakende partij heeft melding van een datalek aan de gemeente gedaan, waarna de gemeente het datalek gemeld heeft aan de AP. In dit geval

betrof het een technisch probleem dat de veroorzakende partij door een aanpassing in de software heeft opgelost.

○ 3.4 Rechten van betrokkenen

Er is een overzicht gemaakt van de rechten die betrokkenen hebben, waarbij is aangegeven welke rechten zij al onder de Wet bescherming persoonsgegevens hadden en welke rechten daar bij gekomen zijn met de inwerkingtreding van de AVG. Ook is daarbij vermeld hoe een verzoek ingediend kan worden door betrokkenen om deze rechten in te roepen. In maart 2018 is dit overzicht openbaar gemaakt en op de gemeentelijke website geplaatst. Er is door betrokkenen in de verslagperiode geen gebruik gemaakt van de mogelijkheden om hun rechten in te roepen. In 2019 zijn een standaardprocedure rechten van betrokkenen en een aanvullende procedure rechten van betrokkenen voor het Sociaal Domein opgesteld en op intranet geplaatst. Hierdoor kunnen alle medewerkers op de hoogte zijn en gebruik maken van deze procesbeschrijvingen.

○ 3.5 Bewaartermijnen

De bewaartermijnen die gelden voor de verwerkingen die door de gemeente Scherpenzeel worden uitgevoerd, staan vermeld in het register van verwerkingen. Hierin zijn ten opzichte van 2018 geen wijzigingen doorgevoerd. Niet in alle systemen en applicaties is het technisch mogelijk om automatisch na ommekomst van de bewaartermijn de gegevens en documenten te verwijderen. In een aantal systemen en applicaties werkt dit wel automatisch, maar in enkele andere wordt hierover met de leverancier naar een oplossing gezocht, zodat dit wel automatisch of na een signaal gedaan kan worden. Met de applicatiebeheerder van Suite voor Sociaal Domein zijn de besprekingen daarover gaande en worden de bewaartermijnen in 2020 ingeregeld.

Daarnaast is het van belang dat de medewerkers ook in eigen mappen de betreffende gegevens verwijderen en vernietigen na afloop van de bewaartermijnen. In 2019 en ook in 2020 zal hierop toegezien worden, waarbij vooral de eigen mappen van de medewerkers de aandacht verdienen. In veel systemen zit namelijk een signaal dat aangeeft dat de bewaartermijn bijna is verstreken. Wel zal nagegaan worden of dat in ieder systeem zo is of dat daar ook actie op ondernomen moet worden. Momenteel lopen er onderhandelingen met enkele softwareleveranciers.

In 2018 zijn de gegevens en documenten die te lang bewaard werden bij de financiële administratie (debiteuren en crediteuren) al opgeschoond en verwijderd. Vanaf 2019 is dit ingeregeld in de Planning & Control-cyclus, zodat na ommekomst van de bewaartermijnen de documenten en gegevens automatisch op de lijst met te verwijderen gegevens en documenten komen, zodat deze na een laatste controle (bijvoorbeeld betaling in later boekjaar waardoor de bewaartermijn een jaar later afloopt) verwijderd kunnen worden. Op dezelfde wijze zijn de bewaartermijnen ingeregeld in het interne controleproces.

Ook in de personeelsdossiers zijn in 2018 al veel gegevens en documenten opgeschoond en verwijderd. Met de komst van de Wet normalisering rechtspositie ambtenaren en de CAO gemeenten per 1 januari 2020 zijn in 2019 alle personeelsdossiers nogmaals doorgenomen

en opgeschoond, omdat de aanstellingsbesluiten omgezet moesten worden naar arbeidsovereenkomsten.

○ 3.6 Verwerkers en verwerkersovereenkomsten

Bij het aangaan van een samenwerkings- of uitvoeringsovereenkomst komt bij de meeste partijen direct de vraag op of er ook een verwerkersovereenkomst afgesloten moet worden. Het bewustzijn is groot, zodat er nauwelijks discussies zijn waar geen oplossing voor gevonden wordt. Ook worden oude overeenkomsten met regelmaat vernieuwd en geactualiseerd om beter te voldoen aan de AVG.
Het overzicht wordt consequent bijgehouden. In totaal zijn er 69 partijen beoordeeld, waarbij met 62 partijen een verwerkersovereenkomst afgesloten is. Daarvan is er nog 1 in behandeling, maar die partij – die maar een zeer beperkte hoeveelheid gegevens verwerkt – heeft al sinds begin 2018 meerdere reminders gehad en reageert nergens op. Nog meer reminders sturen, is zinloos, maar dit is genoteerd als aandachtspunt.

○ 3.7 Privacy in het Sociaal Domein

Binnen het Sociaal Domein zijn de aanmeld-/aanvraag- en toestemmingsformulieren tegen het licht gehouden en waar nodig aangepast aan de AVG. Dit is in een werkoverleg met de collega's van het Sociaal Domein nader toegelicht om het belang van het gebruik van de vernieuwde formulieren en de vraag om toestemming voor het delen van gegevens, in gevallen dat dit niet rechtstreeks voortvloeit uit de publiekrechtelijke taak of wettelijke grondslag, te benadrukken. De informatieverstrekking in het sociaal domein is getoetst en waar nodig verbeterd. Hiervoor zijn de gebruikte formulieren en brochures waar nodig aangepast. Ook is beschreven in welke gevallen de gemeente toestemming nodig heeft voor het delen van gegevens. Daarnaast is een model opgesteld voor een convenant voor multidisciplinaire overleggen. Dit convenant kan als basis dienen voor de gegevensuitwisseling met externe partijen in het sociaal domein.

Daarnaast is er in regionaal verband (Foodvalley) een vernieuwd privacyprotocol en een convenant voor gegevensdeling opgesteld.
De Adviesraad Sociaal Domein heeft de gemeente vanaf het begin van de implementatie van de AVG op de voet gevolgd. Door als FG meerdere keren per jaar aan te sluiten bij een vergadering van de adviesraad of door de Adviesraad via hun secretaris met enige regelmaat de stand van zaken door te geven, is het draagvlak groot en zijn zij continue op de hoogte gehouden van de vorderingen.

○ 3.8 Informatieveiligheid

Informatieveiligheid is een continu proces. Met regelmaat worden bij IBD aangesloten gemeenten geïnformeerd over (mogelijke) beveiligingsdreigingen. Wat betreft het aantal meldingen van incidenten is voor 2019 een forse stijging te zien ten opzichte van het jaar 2018.

De Informatiebeveiligingsdienst voor gemeenten (IBD) heeft op 15 januari 2020 haar jaarcijfers gepubliceerd.

"Het jaar in cijfers

De IBD ontving in 2019 3044 vragen en meldingen over privacy en informatiebeveiliging en de IBD CERT stuurde maar liefst 1751 kwetsbaarheidsmeldingen uit, waarvan 23 zeer ernstige, dat wil zeggen met een hoge kans op en hoge waarschijnlijkheid van misbruik. Tweemaal werd hiervoor ook een waarschuwings-sms gestuurd aan de contactpersonen, waarvan 1 op kerstavond in verband met een ernstige kwetsbaarheid in Citrix. De IBD ontving 14 onderzoekswaardige responsible disclosure meldingen, de melders hebben een kleine attentie ontvangen voor de moeite en zijn vermeld in de hall of fame. De website van de IBD werd 112.716 maal bezocht met gemiddeld 3 pagina's per bezoek. In totaal zijn 88.615 documenten gedownload. De meest gedownloade documenten waren de BIO (3662 unieke downloads) en de standaardverwerkersovereenkomst (2803 unieke downloads). Het websitebezoek is ten opzichte van 2018 bijna verdubbeld. De IBD registreerde 144 informatiebeveiligingsincidenten met een hulpvraag van gemeenten. Hierbij verleende de IBD op afstand assistentie in de vorm van bijvoorbeeld analyse van logbestanden, woordvoerings- en communicatieadvies en advies over aanvullende maatregelen om herhaling van incidenten
te voorkomen. Eén maal is de hulp van andere gemeenten ingeroepen om een gemeente bij te staan na een incident. Deze vorm van gemeentelijke bijstand bleek zeer goed te werken en de IBD noemt dit voortaan het gemeentelijk responsnetwerk (GRN)".

Uit het jaarbericht van IBD blijkt dat er het afgelopen jaar veel beveiligingsincidenten zijn geweest. Dat zijn landelijke cijfers. Hieronder volgen de cijfers voor de Gemeente Scherpenzeel.

Ook Scherpenzeel heeft te maken gehad met datalekken. Zie ook paragraaf 3.3. De impact van deze meldingen was laag. De meeste meldingen worden onbewust veroorzaakt door medewerkers. Daarom zijn voorbereidingen gestart om de bewustwording te vergroten. Door complexiteit van systemen neemt de dreiging gehacked te worden toe. Informatiebeveiliging is niet alleen een ICT aangelegenheid, het is van ons allemaal.

○ 3.9 Data Protection Impact Assessments

In 2019 zijn er DPIA's uitgevoerd op de volgende vakgebieden:

- Nieuw zaaksysteem Djuma ter vervanging van Verseon, voorafgaande aan de contractondertekening in februari 2019 is in december 2018 een PIA uitgevoerd.
- Diftar. Wegens in werking treding van het systeem en de koppeling van gegevens is een (verkorte) PIA uitgevoerd.
- Voorbereiding Belastingsamenwerking Veenendaal en Woudenberg. Hiervoor is door de gemeente Veenendaal een voorafgaande PIA uitgevoerd, waarvan medegedeeld is dat de samenwerking en de daarvoor benodigde bestandoverdracht aan de AVG voldoet. Voor deze samenwerking en voor de gegevensverstrekking en de bestandsoverdracht zijn meerdere verwerkersovereenkomsten afgesloten. Ten tijde

van afronding van de verslagperiode is een Samenwerkingsovereenkomst met daarbij horende Service Level Agreement(s) in concept nagenoeg gereed. De belastingsamenwerking gaat echter niet op 1 januari 2020 in, maar vermoedelijk op 1 juli 2020.

- Per 1 januari 2020 treedt de Wet Verplichte Geestelijke Gezondheidszorg in werking. De uitvoering van deze wet zal in regionaal verband binnen de Veiligheids- en Gezondheidsregio Gelderland-Midden gedaan worden, zodat een convenant met alle deelnemende gemeenten en ketenpartners is afgesloten in december 2019. De VNG heeft een PIA uitgevoerd die alle gemeenten over kunnen nemen en waarvan slechts op enkele punten lokale invulling dient plaats te vinden. Deze lokale invulling wordt voor de Gemeente Scherpenzeel gedaan door de VGGM.

○ 3.10 Bewustwording

In maart 2019 is een medewerkersbijeenkomst georganiseerd over privacy en informatiebeveiliging.

Met alle medewerkers is in het voorjaar een Telewerkovereenkomst (voor incidenteel of structureel telewerken) afgesloten tijdens de gesprekscyclus.

Per 1 augustus 2019 is het niet meer toegestaan om op privéapparaten (telefoon, tablet) werkmail en werkdocumenten te hebben, zonder dat daarvoor gebruik gemaakt wordt van een beveiligde inlog (MDM/Maas360/Horizon VMWare). Bij nieuwe medewerkers is meteen geregeld dat zij alleen via een beveiligde inlog op verstrekte iPads en eventueel iPhones kunnen werken. Door middel van steekproef vindt hier controle op plaats.

In het najaar zijn CISO en FG gestart met de ontwikkeling van een e-learning module voor privacy en een module voor informatiebeveiliging in samenwerking met Junglemap. Deze zogenoemde nanolearning zal in begin 2020 uitgerold worden en bestaan uit korte e-learning lessen die per e-mail worden verstuurd en enkele minuten per keer duren. Er zijn zo'n 30-32 lessen ontwikkeld die van begin februari tot medio september 2020 elke week gestuurd kunnen worden. Door de grote regelmaat van deze korte lessen over beide onderwerpen en het steeds terug kunnen kijken van eerder gestuurde lessen wordt het bewustzijn verhoogd en blijft dit tussen de oren zitten.

Daarnaast krijgt iedere nieuwe (tijdelijke en vaste) medewerker een introductieprogramma, waarbij aandacht gevraagd wordt voor de omgang met persoonsgegevens en waarbij de informatieveiligheidsaspecten besproken worden.

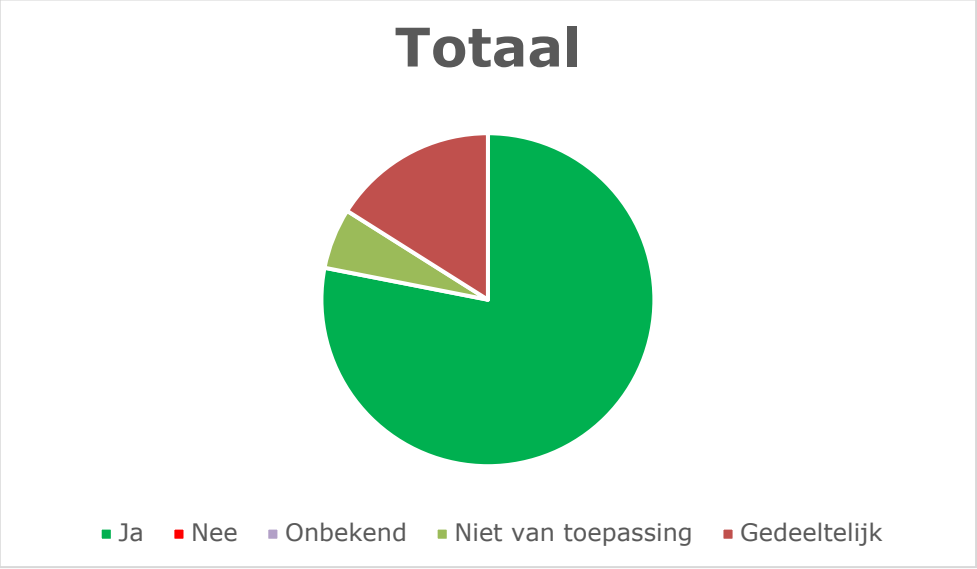
○ 3.11 Borging

De VNG en IBD hebben samen een borgingsdocument opgesteld, waarin circa 190 vragen zijn opgenomen die zowel op de AVG betrekking hebben als op de maatregelen die de BIO (voorheen BIG) voorschrijft, onderverdeeld naar aandachtsgebieden beleid, processen, organisatorische inbedding, rechten van betrokkenen, samenwerking, beveiliging en verantwoording.

In onderstaande tabel is de score per onderdeel weergegeven:

Score per onderdeel	Ja	Nee	Onbekend	N.v.t.	Gedeeltelijk
Beleid	12	0	0	2	0
Processen	28	0	0	0	6
Organisatorische Inbedding	35	0	0	6	6
Rechten van betrokkenen	27	0	0	3	3
Samenwerking	12	0	0	2	5
Beveiliging	16	0	0	0	5
Verantwoording	16	0	0	0	5

Dit levert de volgende cirkeldiagram op van de totaalscore.



Hieruit is af te leiden dat de Gemeente Scherpenzeel goed in zicht heeft op wat wel, niet of deels geregeld is en waar nog aandacht aan besteed moet worden. Bij zaken die de score gedeeltelijk hebben gekregen, is de betreffende zaak veelal wel goed ingeregeld, maar ontbreekt een (werk)procesbeschrijving. Dat zijn actiepunten voor 2020 en volgende jaren. Overigens wordt hier geen risico gelopen, aangezien het de borging betreft.

4. AANBEVELINGEN

Belang: het is belangrijk om het bewustzijn over het belang van het zorgvuldig omgaan met en verwerken van persoonsgegevens tussen de oren te krijgen en te houden bij de medewerkers. Daarbij is het van belang om te weten op welk moment toestemming gevraagd dient te worden om gegevens te mogen verwerken of te delen en wanneer dat niet nodig is, omdat de verwerking of deling van gegevens voortvloeit uit een wettelijke verplichting of de uitvoering van een publiekrechtelijke taak.

Aanbeveling: door met enige regelmaat de medewerkers hierop te attenderen en daarover te informeren door een berichtje op intranet of door het houden van een medewerkersbijeenkomst wordt het bewustzijn hoog gehouden. Een combinatie van de onderwerpen privacy en informatieveiligheid kan dit beeld versterken en het belang verduidelijken.
Begin 2020 wordt gestart met een "Nano" e-learning die bestaat uit korte lessen van een paar minuten die elke week gedurende 7,5 maand per e-mail gestuurd worden.
Er zal een checklist over toestemming in het Sociaal Domein opgesteld gaan worden, zodat snel inzichtelijk is wanneer expliciet toestemming (d.m.v. toestemmingsformulier) gevraagd moet worden en waar dit wettelijk geregeld is.

Belang: bij aanschaf van nieuwe of bij verlenging van diensten en leveringen zoals bijvoorbeeld een softwarepakket, de uitbesteding van salarisverwerking, een inwonersenquête of een chatfunctie op de website moet niet alleen een overeenkomst van opdracht/levering afgesloten worden, maar ook een verwerkersovereenkomst.

Aanbeveling: nog beter en blijvend onder de aandacht brengen bij de medewerkers dat deze twee soorten overeenkomsten onlosmakelijk met elkaar verbonden zijn en dat deze voorafgaand aan de levering of uitvoering van de dienst afgesloten moeten zijn. Om dit beter inzichtelijk te maken, kan hiervoor een werkproces ontwikkeld worden door de projectgroep dienstverlening (processen en innovatie). Ook kan in bestaande of reeds beschreven werkprocessen opgenomen wanneer een verwerkersovereenkomst nodig is, zodat dit tijdens het werkproces al onder de aandacht gebracht wordt.

Belang: niet meer persoonsgegevens en documenten dan noodzakelijk bewaren en de gegevens en documenten niet langer dan nodig bewaren. Voor alle soorten persoonsgegevens en documenten bestaan wettelijke bewaartermijnen die per soort gegeven of document kunnen verschillen. Sommige gegevens mogen maar enkele weken worden bewaard, maar andere gegevens worden tientallen jaren of zelfs eeuwig bewaard. In het register van verwerkingen is per gegeven aangegeven wat daarvan de bewaartermijn is. Behalve in de gebruikte systemen en applicaties worden ook schaduwbestanden bijgehouden en zitten er documenten in e-mails. Dit is een blijvend punt van aandacht.

Aanbeveling: jaarlijkse opschoonactie om te controleren of niet te veel gegevens en documenten bewaard worden en dat deze niet te lang bewaard worden. Daarbij moet niet

alleen naar de systemen en applicaties gekeken worden, maar dan moet ook aandacht gevraagd worden voor het opschonen van de schaduwbestanden en e-mailboxen.

5. ACTIES 2019

In de hoofdstukken 2 en 3 is aangegeven welke werkzaamheden in 2019 zijn uitgevoerd en in hoofdstuk 4 worden de aanbevelingen genoemd. In dit laatste hoofdstuk wordt nader ingegaan op de acties die al kort genoemd zijn in de voorgaande hoofdstukken. In 2020 worden de onderstaande acties opgepakt, waarover in het Jaarverslag FG 2020 gerapporteerd zal worden.

- Actualiseren en waar nodig herzien van het Register van verwerkingen.
- Actualisatie en waar nodig herzien van de Data Protection Impact Assessments;
- Toetsing en waar nodig actualisatie van het privacybeleid.
- Het afsluiten van overeenkomsten gegevensuitwisseling met partijen die persoonsgegevens van de gemeente Scherpenzeel ontvangen.
- Toetsen of verwerkers de afspraken uit de verwerkersovereenkomsten naleven.
- Afsluiten convenanten indien de multidisciplinaire overleggen weer opgestart gaan worden.
- Opstellen checklist wanneer in het Sociaal Domein gebruik gemaakt moet worden van het expliciet vragen om toestemming (d.m.v. toestemmingsformulier) of waar dit al wettelijk geregeld is.
- Handhaving van de bewaartermijn en toezien op de juiste wijze van verwijdering van gegevens na het verstrijken van de bewaartermijn, waarbij vooral aandacht wordt besteed aan de persoonlijke mappen van medewerkers en op afdelingsschijven en e-mailbestanden.
- Actiepunten / aandachtspunten voortkomend uit borgingsdocument oppakken en uitvoeren, zoals het opstellen van (werk)procesbeschrijvingen, protocollen etc.
- Plaatsen van een Nieuwsbericht in Scherpenzeelse Krant of in de Gemeentegids over een AVG-onderwerp voor burgers over bijvoorbeeld, recht van inzage etc.

BIJLAGE WETTELIJK KADER

○ AVG Algemeen

In de Algemene Verordening Gegevensbescherming (AVG) zijn regels vastgelegd voor het verwerken van persoonsgegevens. Deze verordening voor de verwerking van persoonsgegevens kent een rechtstreekse werking voor de lidstaten van de Europese Unie. In de AVG worden de rechten van burgers versterkt en de AVG legt de nadruk op de eigen verantwoordingsplicht van organisaties die persoonsgegevens verwerken. Dit betekent dat organisaties bijvoorbeeld goed moeten vastleggen welke gegevens zij verwerken, met welk doel, hoe lang zij die gegevens bewaren, dat zij de gegevens goed beveiligen en met wie ze gegevens delen. De rechtstreekse werking van de AVG zorgt ervoor dat de regels voor bescherming van persoonsgegevens uniform zijn binnen de Europese Unie.

De AVG geeft een overkoepelend kader voor het verwerken van persoonsgegevens en is nader uitgewerkt in de Nederlandse Uitvoeringswet AVG. Daarnaast zijn er in materiewetgeving, zoals de Jeugdwet, de Wet maatschappelijke ondersteuning, de Wet Basisregistratie personen specifieke regels te vinden voor het verwerken van persoonsgegevens. De AVG hangt daar altijd als een paraplu boven. Dat betekent dat als persoonsgegevens verwerkt mogen worden op grond van de materiewetgeving, de bepalingen van de AVG daar boven blijven hangen. Er moet bijvoorbeeld altijd een rechtmatige grondslag zijn voor het verwerken van persoonsgegevens en persoonsgegevens mogen alleen worden verwerkt voor het doel waarvoor ze zijn verzameld.

○ Specifieke wetgevende ontwikkelingen en jurisprudentie

Door de Autoriteit Persoonsgegevens (AP) wordt regelmatig onderzoek gedaan naar de verwerking van persoonsgegevens en de naleving van privacywetgeving in specifieke situaties. Deze onderzoeken worden veelal gepubliceerd en geven meer inzicht in de wijze waarop de AP regelmatig richtsnoeren of uitspraken die relevant kunnen zijn voor een juiste toepassing van privacyregels. In 2019 heeft de AP verschillende onderzoeken gedaan, belangrijke onderzoeken zijn bijvoorbeeld:

- Onderzoek Toegang tot digitale patiëntdossiers door medewerkers van het HagaZiekenhuis, maart 2019;
- Verkennend onderzoek Gegevensbeschermingsbeleid, april 2019;
- Onderzoek naar de positie en taakuitoefening van functionarissen voor de gegevensbescherming in elf ziekenhuizen, juni 2019;
- Meldplicht datalekken: Overzicht feiten en cijfers eerste helft 2019, september 2019;
- Onderzoek Verwerking van persoonsgegevens over de gezondheid door Alliantie kwaliteit in de Geestelijke Gezondheidszorg, december 2019.

Daarnaast moet de Autoriteit Persoonsgegevens geconsulteerd worden bij voorstellen voor nieuwe wetgeving die betrekking heeft op de verwerking van persoonsgegevens. Ook kan de Autoriteit Persoonsgegevens op eigen initiatief overgaan tot het geven van een wetgevingsadvies. Een aantal wetgevingsadviezen die de AP in 2019 heeft gedaan zijn:

- Goedkeuring AVG-certificaten. Samenwerking Autoriteit Persoonsgegevens en Raad voor Accreditatie. De AP en RvA gaan samen zorgen voor de goedkeuring van AVG-certificaten en hebben daartoe een Informatieprotocol ondertekend. Met een AVG-certificaat kan de verwerker van persoonsgegevens aantonen dat zijn product, proces of dienst aan de eisen uit de AVG voldoet, december 2019;
- Advies kredietstrategie ten behoeve van het opstellen van nieuwe wetgeving die ervoor zorgt dat bij kredietregistratie vastgelegde persoonsgegevens beter worden beschermd, november 2019;
- Advies conceptwetsvoorstel tot wijziging van de Wet gemeentelijke schuldhulpverlening ten behoeve van de uitwisseling van persoonsgegevens, mei 2019;
- Aanvullend advies wetsvoorstel gegevensverwerking samenwerkingsverbanden, april 2019;
- Advies Ontwerp-Invoeringsbesluit Omgevingswet, januari 2019.

Daarnaast worden door de European Data Protection Board, voorheen Working Party 29, de samenwerking van alle nationale privacytoezichthouders van de Europese Unie (EDPB), regelmatig guidelines gepubliceerd die meer richting kunnen geven aan de juiste toepassing van de AVG. Guidelines die de EDPB over de AVG heft gepubliceerd zijn bijvoorbeeld:

- EDPB Guidelines 5/2019 on the criteria of the Right to be forgotten in search engines cases under the GDPR (part 1), aangenomen 2 december 2019;
- EDPB Guidelines 4/2019 on article 25 data protection by design and by default, aangenomen 20 november 2019;
- EDPS (Supervisor) Guidelines on the concepts of controller, processor and joint controllership under Regulation 2018/1725 (EU), aangenomen 7 november 2019;
- EDPB Guidelines 3/2019 on processing of personal data through video devices, aangenomen op 10 juli 2019;
- EDPB Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects.
- Recommendation 01/2019 on the draft list of the European Data Protection Supervisor regarding the processing operations subject to the requirement of a data protection impact assessment, aangenomen op 10 juli 2019.

○ Toezichtskader AP: ontwikkelingen en gevolgen

De Autoriteit Persoonsgegevens (AP) heeft in november 2019 haar toezichtkader voor 2020 tot en met 2023 gepubliceerd. In dit kader geeft de AP haar prioriteiten aan voor de komende jaren.

De Autoriteit Persoonsgegevens (AP) legt de komende jaren in het toezichtwerk extra nadruk op drie focusgebieden: datahandel, digitale overheid en artificiële intelligentie en algoritmes. Dat maakt de AP op 11 november 2019 bekend met het visiedocument ‘Dataprotectie in een digitale samenleving’. Extra nadruk op deze thema’s is nodig om de bescherming van persoonsgegevens in Nederland te borgen. Misbruik of onverantwoordelijk gebruik van persoonsgegevens kan bijvoorbeeld leiden tot foutieve beslissingen, uitsluiting

van mensen en discriminatie. Tot en met 2023 geven de focusgebieden onder meer richting aan de uitvoering van de wettelijke taken van de AP.

Voorzitter Aleid Wolfsen: *"Bescherming van persoonsgegevens is een belangrijk grondrecht dat er is om ons tegen misbruik te beschermen. Het gaat in de kern over zeggenschap, over autonomie, over dat wij als burgers zelf gaan over wat we met wie delen. Ik hoor nog veel te vaak onterecht dat de privacywet ontwikkelingen in de weg staat. Het is geen kwestie van of-of, maar van en-en. Zorgvuldig omgaan met persoonsgegevens is onderdeel van ontwikkeling en innovatie."*

Trends en ontwikkelingen
Steeds meer apparaten en diensten verzamelen persoonsgegevens waardoor ze steeds meer van ons weten. Dit gebeurt zonder dat we altijd precies weten wat er met die gegevens gebeurt en wie er toegang toe heeft. Dit maakt ons en onze democratische rechtstaat kwetsbaar.

De AP ziet drie grote trends die van invloed zijn op de bescherming van persoonsgegevens:
- Doorgroei van de datasamenleving
- Toename van digitaal onrecht
- Toename van privacybewustzijn

Focusgebieden
In vervolg op de gesignaleerde trends kiest de AP voor drie focusgebieden:

Datahandel
Data maken producten en diensten slimmer en deze producten en diensten creëren vervolgens weer meer data. Dit heeft voordelen, maar ook nadelen: er vindt steeds meer ongeoorloofde doorverkoop plaats van persoonsgegevens aan derden. Mensen verliezen hierdoor steeds meer grip op hun gegevens en daarmee op hun leven.

Digitale overheid
Centrale en lokale overheden, uitvoeringsorganisaties en politie en justitie beschikken over een grote hoeveelheid – vaak gevoelige en bijzondere – persoonsgegevens. De overheid werkt gericht aan het inzetten van persoonsgegevens. Het is van belang dat de overheid verantwoordelijk omgaat met persoonsgegevens, zodat mensen niet onnodig in de knel kunnen komen.

Artificiële Intelligentie en algoritmes
Steeds meer bedrijven en organisaties maken gebruik van algoritmes en AI. Dit biedt voordelen en leidt tot nieuwe nuttige toepassingen. Maar de inzet van AI en algoritmes kent ook risico´s en schadelijke effecten. Onverantwoordelijk gebruik van algoritmes kan leiden tot foutieve beslissingen, tot uitsluiting van mensen en tot discriminatie. De AP is als toezichthouder verantwoordelijk voor het toezicht op de verwerking van persoonsgegevens, en daarmee ook op de toepassing van AI en algoritmes waarbij persoonsgegevens worden gebruikt.

Deze thema's passen bij de missie van de AP en spelen in meerdere sectoren. De AP kan hier het verschil maken door grenzen te markeren ten aanzien van wat er wel en niet kan onder de AVG. De focusgebieden geven onder meer richting aan de uitvoering van de wettelijke taken van de AP. Daarnaast houdt de AP oog voor actuele ontwikkelingen.

Risicogestuurd toezicht

De AP is de onafhankelijke toezichthouder in Nederland die de bescherming van persoonsgegevens bevordert en bewaakt. Het toezichtveld is omvangrijk: internationale en nationale bedrijven en organisaties, de gehele overheid, inclusief politie en justitie en ook verenigingen, scholen, stichtingen en individuele burgers.

De AP houdt daarom risicogestuurd toezicht. Dat betekent dat de AP is gespitst op onderwerpen met een groot risico voor burgers. Daarbij weegt de AP af om hoeveel data het gaat en hoe gevoelig die data zijn. Op basis daarvan gebruikt de AP een of meerdere toezichtsinstrumenten, zoals normuitleg, wetgevingsadvies, voorlichting of handhaving.