Gemeente Scherpenzeel

Jaarverslag

Functionaris Gegevensbescherming 2021

Jaarverslag

Functionaris Gegevensbescherming 2021

Opdrachtgever:	gemeente Scherpenzeel Afdeling Bedrijfsvoering
Auteur:	Sascha Beekman, Functionaris Gegevensbescherming
Datum:	14 februari 2022

Inhoud

MANAGEMENTSAMENVATTING

Dit verslag betreft de periode van 1 januari 2021 tot en met 31 december 2021. In deze verslagperiode is het volgende gerealiseerd:

- Het Jaarverslag FG over 2020 is in maart 2021 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.
- De in 2018 uitgevoerde Data Protection Impact Assessments (DPIA's) zijn herzien en opnieuw uitgevoerd en beoordeeld, omdat dit iedere 3 jaar gedaan moet worden. De daaruit voorkomende zaken zijn verwerkt in het register. Voor nieuw aan te schaffen of in gebruik te nemen (gewijzigde) software wordt standaard een DPIA uitgevoerd.
- Naar aanleiding van de in 2019 opgestelde (interne) procedure / werkinstructie hoe een verzoek ten aanzien van de rechten van betrokkenen behandeld moet worden, is hiervan een werkprocesbeschrijving gemaakt. Deze werkprocesbeschrijving is door het MT goedgekeurd en daarna op Flash gezet.
- Om het bewustzijn over het veilig en zorgvuldig werken met persoonsgegevens vast te houden en te verbeteren, is er – net als in 2020 – in de periode van februari tot en met september 2021 een bewustwordingsactie gehouden, waarbij wekelijks korte e-learning modules worden ingezet. Door met regelmaat de onderwerpen "Informatieveiligheid" en "Privacy" onder de aandacht te brengen, beklijft dit beter. Ook in 2022 zal een vergelijkbare bewustwordingstool gebruikt worden, maar dan van een andere aanbieder.
- Thuiswerken/telewerken is vanwege de covid-19-pandemie vanaf medio maart 2020 de standaard werkwijze geworden, waarbij de mogelijkheden van digitaal vergaderen zijn verkend. Er is al snel gekozen voor MS Teams als online vergadertool. In het voorjaar van 2019 is tijdens de gesprekscyclus met alle medewerkers een telewerkovereenkomst voor incidenteel of structureel telewerken afgesloten, zodat iedereen op de hoogte is van de rechten en verplichtingen van het digitaal werken op afstand. In 2021 is dit onveranderd. De Telewerkregeling zal in 2022 herzien worden, omdat hybridewerken andere mogelijkheden en risico's met zich meebrengt.

In voorgaande verslagperiodes, van 1 oktober 2017 tot en met 31 december 2020, is hard gewerkt om aan alle vereisten van de AVG te voldoen. Daarbij 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 2021, zijn de in 2020 geanalyseerde noodzakelijke stappen gezet om de privacy en de bescherming van persoonsgegevens nog beter te borgen. Daarbij zijn niet alleen naar de vereisten van de AVG betrokken, maar ook de in de Baseline Informatiebeveiliging Overheid (BIO) opgenomen normen, zodat steeds aandacht is voor Privacy & Security.

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

In de periode februari tot en met september 2021 is er wekelijks een korte e-learning aan alle medewerkers gestuurd, waarbij de onderwerpen "privacy" en "informatiebeveiliging" onder de aandacht zijn gebracht om het bewustzijn bij de medewerkers te verhogen en vast te houden.

In 2021 zijn een achttiental 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. De standaard en door VNG/IBD verplicht gestelde verwerkersovereenkomst wordt door bijna alle verwerkers geaccepteerd. Zie verder bij 3.6.

De privacyverklaring die in 2018 was opgesteld en op de website geplaatst, is herzien en geactualiseerd. Verder zijn in 2020 de eerder in 2018 uitgevoerde DPIA's herzien en opnieuw uitgevoerd en beoordeeld. De resterende DPIA's worden in 2022 gedaan. In het implementatietraject van de regiemodule die toegevoegd wordt aan Suite4Sd is in samenspraak met de gemeente Barneveld een DPIA uitgevoerd en is gezamenlijk het implementatietraject doorlopen, waarbij aspecten van Privacy & Security bij iedere stap zijn doorlopen.

De VNG heeft medio 2019 een borgingsdocument opgeleverd, dat herzien is in 2021, 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 in 2021 wederom 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 voorgaande jaren, ook in 2021 ondersteund door een externe privacy officer. Door deze privacy officer zijn op verschillende terreinen werkzaamheden verricht.

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 2022 wordt de overeenkomst aan partijen voorgelegd.

Toetsingskader verwerkers

In 2018 en 2019 zijn door de Functionaris gegevensbescherming de meeste verwerkersovereenkomsten afgesloten. In deze overeenkomsten staan een groot aantal verplichtingen voor verwerkers. In 2021 zijn een achttiental verwerkersovereenkomsten geactualiseerd en/of afgesloten met nieuwe verwerkers. Om te toetsen of de verwerkers voldoen aan de afspraken, is door de privacy officer een toetsingskader opgesteld. In 2022 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 is in 2020 en in 2021 gebruikt bij de actualisatie van de DPIA's. De privacy officer heeft de FG ondersteund bij de DPIA's en de gesprekken uitgevoerd voor de actualisering van de DPIA's. Er zijn in 2021 zo'n 6 DPIA's uitgevoerd. In 2022 volgen er nog 3.

Register van verwerkingen

Na iedere DPIA is tevens het register van verwerkingen geactualiseerd. De versie van het register dat op de website is geplaatst, is van mei 2018. Het geactualiseerde register zal na de uit te voeren DPIA's in voorjaar 2022 op website geplaatst worden.

○ 2.4 Verantwoording CISO

In regionaal verband is er regulier CISO overleg waarbij zaken zoals informatiebeveiliging, samenwerking met betrekking tot ENSIA en de invoering van de BIO (Baseline Informatiebeveiliging Overheden). In dit gremium is de basis gelegd voor het nieuwe informatieveiligheidsbeleid conform BIO maatregelen en is de aansluiting op het landelijke digitale netwerk van VNG gerealiseerd (GGI Veilig).

Het jaar 2020 is 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. In 2021 is de implementatie verder uitgerold.

Op 12 januari 2021 heeft het college het gemeente brede Informatieveiligheidsbeleid vastgesteld en in juli 2018 heeft het college het Informatieveiligheidsplan vastgesteld. In

2021 is een begin gemaakt met de actualisering van het Informatieveiligheidsplan, zodat deze in de loop van 2022 vastgesteld kan worden. 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 2021 is het beleid beoordeeld op actualiteit en het beleid voldoet nog en hoeft nog niet herzien te worden. In 2022 wordt het beleid opnieuw beoordeeld en indien nodig geactualiseerd en herzien.

○ 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 is het register geactualiseerd naar aanleiding van uit de DPIA's voortgekomen zaken. Daarbij is ook (opnieuw) een toets worden gedaan aan de beginselen van de AVG, zoals proportionaliteit en subsidiariteit. In 2021 is het register wederom beoordeeld op actualiteit. In 2022 zal het register eveneens op actualiteit beoordeeld worden en zal dan opnieuw ter vaststelling aangeboden worden aan het college, omdat dan de bevindingen uit alle herziene DPIA's daarin meegenomen kunnen zijn. Het register zal na actualisatie in 2022 op de website geplaatst worden, zodat een ieder daarvan kennis kan nemen. Op intranet zal daar dan ook aandacht aan besteed worden, zodat alle medewerkers goed op de hoogte zijn en weten dat zij gewijzigde of nieuwe verwerkingen bij de FG moeten melden.

○ 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 2021 hebben 9 beveiligingsincidenten plaatsgevonden, waarvan er 3 zijn aangemerkt als meldenswaardig datalek. Daarvan is er één door de gemeente Ede gemeld bij de AP, omdat dit een regionale aangelegenheid betrof (Regio Foodvalley). De andere 2 meldingswaardige datalekken zijn niet gemeld bij de AP wegens gewijzigd beleid van de AP. Wel zijn deze

datalekken intern geregistreerd. Van de 9 beveiligingsincidenten is in 4 gevallen melding gedaan aan betrokkenen.

○ 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. 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 procedures.

In 2020 is een werkprocesbeschrijving gemaakt voor het behandelen van verzoeken van betrokkenen. Deze is in 2021 door het MT goedgekeurd, waarna de werkprocesbeschrijving op intranet geplaatst is en daarmee voor alle medewerker te raadplegen is.

Er is in de verslagperiode door één betrokkene gebruik gemaakt van de mogelijkheden om zijn rechten in te roepen. Het Inzageverzoek is behandeld en betrokkene is geïnformeerd dat er geen persoonsgegevens van betrokkene worden verwerkt. Vervolgens is het Verwijderingsverzoek van dezelfde betrokkene geweigerd vanwege de bewaartermijn.

○ 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 2019 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.

In 2020 in de Regiemodule toegevoegd aan de Suite4SD voor de gemeente Barneveld, waarbij ook de Gemeente Scherpenzeel betrokken is geweest bij het implementatietraject. Per 1 maart 2021 is deze aanvullende module in gebruik genomen door de gemeente Barneveld. Als de gebruikerservaringen daarvan positief zijn, gaat de Gemeente Scherpenzeel ook over tot implementatie die een korter traject zal doorlopen, omdat in samenspraak alles al uitgedacht en doorlopen is. Gelijktijdig met de regiemodule worden de bewaartermijnen ingeregeld. De implementatie en het in gebruik nemen is het tweede halfjaar van 2021 aangevangen. In 2022 zal hierop een evaluatie plaatsvinden.

Daarnaast is het van belang dat de medewerkers ook in eigen mappen en in de mailbox de betreffende gegevens verwijderen en vernietigen na afloop van de bewaartermijnen. In

voorgaande jaren is hierop toegezien, waarbij vooral de eigen mappen en de mailbox van de medewerkers de aandacht verdienen. In 2022 zal dit wederom de aandacht vragen.

○ 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. De standaard en door VNG/IBD verplicht gestelde verwerkersovereenkomst wordt in vrijwel alle gevallen geaccepteerd. In één geval is daarvan afgeweken. Dat is:

25-1-2021:
Helpdeskovereenkomst OSV verkiezingssoftware voor tellingen en verwerkersovereenkomst zijn niet conform model. Dit betreft een eigen model op Rijksniveau dat landelijk gebruikt wordt, zodat een verzoek om aanpassing geen nut heeft.

Het overzicht wordt consequent bijgehouden. In totaal zijn er 101 partijen beoordeeld, waarbij met 91 partijen een verwerkersovereenkomst afgesloten is en met 2 partijen een aangepaste afspraak is gemaakt. Met 8 partijen is het afsluiten van een verwerkersovereenkomst niet noodzakelijk, omdat geen persoonsgegevens worden verwerkt (wel zijn deze in het overzicht opgenomen om een compleet beeld te hebben van de verwerkers). Verder 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, zodat er geen reminders meer gestuurd zijn. Wel is dit genoteerd als aandachtspunt. En in 13 gevallen was sprake van een kortdurende hoofdovereenkomst, waarvan de dienstverlening is beëindigd, zodat daarmee de verwerkersovereenkomst ook is komen te vervallen. Er zijn dus met 78 partijen actuele, nog lopende, overeenkomsten.

○ 3.7 Privacy in het Sociaal Domein

De FG van Regio Foodvalley heeft in juni 2021 een signaal uitgestuurd dat de verwerkingen van data-analyse jeugdhulp en data-analyse leerplicht door het Knooppunt niet goed verwerkt worden. Hierop hebben de deelnemende gemeenten gezamenlijk de verwerking stopgezet. Er is een DPIA uitgevoerd, waarin een aantal risico's naar voren zijn gekomen. Er zijn maatregelen vastgesteld om deze risico's te beperken, waaronder het opstellen van nieuwe/verbeterde werkprocesbeschrijvingen en het opnemen van de verwerking in het register van verwerkingen. Daarnaast zal begin 2022, een verwerkersovereenkomst worden opgesteld en worden de samenwerkingsovereenkomst en het convenant aangepast. Na het nemen van deze maatregelen zijn de verwerkingen die het Knooppunt doet in overeenstemming met de AVG en de informatieveiligheid-vereisten. Begin 2022 kan de verwerking naar verwachting weer opgestart worden.

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 2020 een lichte daling te zien ten opzichte van het jaar 2019.

De Informatiebeveiligingsdienst voor gemeenten (IBD) heeft op 20 januari 2022 haar jaarcijfers gepubliceerd.

Het jaar 2021 laat zien dat zien dat een goede informatiebeveiliging en gegevens-bescherming voor gemeenten van groot belang blijft. Risico's rond de informatievoorziening werden op verschillende manieren zichtbaar en tastbaar, ook voor gemeenten en hun ketenpartners. Zo werden twee gemeentelijke samenwerkingsverbanden getroffen door ernstige ransomwareaanvallen. Eind 2021 moesten alle gemeenten actie ondernemen toen een ernstige kwetsbaarheid in Apache Log4J aan het licht kwam. Op het terrein van gegevensbescherming legde de Autoriteit Persoonsgegevens een gemeente een flinke boete op voor het gebruik van wifitracking. Ook waren er enkele incidenten met het onterecht verwerken van persoonsgegevens door gemeenten.

De IBD ondersteunde gemeenten ook in 2021 bij de structurele verhoging van digitale weerbaarheid en bescherming van persoonsgegevens. Het vergroten van het risicobesef en prioritering van risico's zijn daarbij belangrijke facetten.

Met de IBD hebben gemeenten een collectieve voorziening die steunt op drie pijlers: incidentcoördinatie, advies en kennisdeling. In dit jaaroverzicht van IBD zijn de belangrijkste resultaten en ontwikkelingen opgenomen.

Het jaar in cijfers

De IBD ontving het afgelopen jaar 2.487 aanvragen- en meldingen over informatiebeveiliging en 542 privacyaanvragen. De IBD registreerde 276 incidenten met een hulp-, coördinatie- of ondersteuningsvraag van gemeenten en ontving hierover ruim 1600 inkomende telefoongesprekken.

De IBD-CERT verstuurde 1.846 kwetsbaarheidsmeldingen waarvan 90 met een hoge kans op misbruik en een grote potentiële schade. De SMS-waarschuwing werd in 2021 vijf keer ingezet, waarvan twee keer voor de Log4J-problematiek.

De IBD organiseerde 82 onlinebijeenkomsten, zoals werkgroepen, intervisiebijeenkomsten,

webinars en (be)spreekuren. De IBD streeft ernaar vooral onderlinge interactie tussen de deelnemers te stimuleren.

De website van de IBD werd ruim 135.000 keer bezocht. Op de website verschenen 27 nieuwe en bijgewerkte kennisproducten. De top 3 meest gedownloade producten waren dit jaar de BIO, de baselinetoets en de standaard verwerkersovereenkomst. De IBD voert het beheer over het VNG-privacyforum, dat inmiddels meer dan 4.700 gemeentelijke deelnemers heeft.

Uit het jaarbericht van IBD blijkt dat er het afgelopen jaar ongeveer even veel beveiligingsincidenten zijn geweest als in 2020. 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 is e-learning uitgevoerd 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 Telewerken

Met ingang van 16 maart 2020 zijn er door het RIVM en vervolgens aanvullend door de Veiligheidsregio's maatregelen afgekondigd ter bestrijding van de covid-19-pandemie. Hierdoor is thuiswerken/telewerken de standaard geworden en is werken op het gemeentehuis een uitzondering, behalve voor de medewerkers die werken in de vitale processen zoals bijvoorbeeld burgerzaken, buitendienst, afvalinzameling, postverwerking en dergelijke. Deze werkwijze bracht nieuwe uitdagingen en risico's, voor- en nadelen met zich mee.

In de Telewerkregeling, die in december 2018 is vastgesteld, is afgesproken dat bij telewerken geen gebruik gemaakt mag worden van BRP, Suwi en Open Wave.
Vanwege het verplichte thuiswerken is hierop – na akkoord van de gemeentesecretaris - voor de duur van de landelijk tevens lokaal opgelegde maatregelen een uitzondering gemaakt voor de medewerkers van burgerzaken en de administratief juridisch medewerker RO. Tevens hebben externen ook toegang tot VPN verkregen om thuis te kunnen werken, ter voorkoming dat te veel personen op een kamer bij elkaar zitten. Deze externe medewerkers hebben allemaal een geheimhoudings- en integriteitsverklaring ondertekend, waarin zij verklaren zorgvuldig om te gaan met persoonsgegevens en bij het gebruik maken van het telewerken de beveiligingsregels van de gemeente in acht te nemen.

Voorts is meerdere keren aan alle medewerkers nadrukkelijk gevraagd vertrouwelijk en zorgvuldig om te gaan met telewerken, waarbij de telewerkregeling en de telewerkovereenkomsten ingezet zijn ter verduidelijking en voor het bewustzijn.
Voor het veilig thuiswerken wordt met regelmaat de VPN updates afgedwongen door het systeem, zodat de meest recente beveiligingspatches zijn geïnstalleerd.

In 2021 is de Telewerkregeling op een aantal kleine punten herzien. Hiervan zijn de medewerkers op de hoogte gesteld door Personeelszaken. Heel 2021 is er veel vanuit huis gewerkt. In 2022 wordt de Telewerkregeling grondig herzien, omdat het hybride werken zowel mogelijkheden als risico's met zich meebrengt voor privacy en security. Dit wordt eveneens meegenomen in de e-learning in het kader van bewustwording.

○ 3.10 Data Protection Impact Assessments

3.10.1 Overzicht DPIA's

In 2021 zijn er DPIA's uitgevoerd/geactualiseerd op de volgende vakgebieden:

- DIV/Djuma
- Veiligheid: RIEC
- Veiligheid: DHW(Alcoholwet)/Bibob
- Veiligheid: Tijdelijk Huisverbod
- Veiligheid: Terugkeerbegeleiding ex-gedetineerden, inclusief bestuurlijke informatie justitiabelen
- Vergunningen (evenementen, DHW, APV): deze is niet uitgevoerd, omdat de gegevensverwerking al in andere DPIA's aan bod komen.

In 2022 zullen de volgende DPIA's uitgevoerd gaan worden:

- WvGGZ. Hiervoor is landelijk een DPIA door VNG uitgevoerd eind 2019, zodat het te verwachten is dat er weer een landelijke DPIA uitgevoerd zal worden. Mocht dat niet het geval zijn, zal eind 2022 zelf een DPIA uitgevoerd worden.
- Wet gemeentelijke schuldhulpverlening. Nu de nieuwe wet per 1 januari 2021 in werking is getreden en bekend is wat er gewijzigd is ten opzichte van de voorgaande wetgeving en werkwijze. Werkwijze en proces waren in 2021 nog onvoldoende duidelijk. Gemeente Barneveld voert voor Gemeente Scherpenzeel hiervoor in mandaat taken uit. Begin 2022 wordt deze DPIA opgepakt.
- Vroegsignalering schulden, eventueel in combinatie met Wgs.

3.10.2 resultaten, bevindingen en conclusie uitgevoerde DPIA's

Bij nagenoeg alle DPIA's kwam naar voren dat er geen of verouderde procesbeschrijvingen zijn, zodat daar in 2021 actie op is ondernomen. Omdat het om veel werkprocesbeschrijvingen gaat, wordt hiermee verder gegaan in 2022.

Het informeren van betrokken kan vaak ook beter. Niet altijd wordt gemeld met welke ketenpartners gegevens worden gedeeld, zodat hiervoor meer aandacht wordt gevraagd.

Bewaartermijnen zijn ook niet altijd (goed) ingeregeld en wat betreft de naleving is er nog veel winst te behalen, zowel binnen de gemeente als bij ketenpartners

Daarnaast blijven er ook regelmatig gegevens en documenten in outlook staan die bewaard moeten worden in Djuma of SuiteSD. Hiervoor is in 2021 aandacht gevraagd, maar daarvoor zal in 2022 wederom aandacht gevraagd worden met het verzoek om e-mailboxen op te

schonen en belangrijke e-mails met gegevens en documenten te archiveren in het geldende zaaksysteem.

Tevens wordt blijvende aandacht gevraagd voor het gebruik maken van beveiligde e-mail. Door het vele thuiswerken wordt daar overigens al goed mee gewerkt, maar op enkele punten kan dat nog beter.

Ook is blijvende aandacht nodig voor het uitvragen van gegevens. Soms worden er teveel gegevens uitgevraagd aan klanten, omdat het handig kan zijn om een breder beeld van iemand te krijgen bij de beoordeling van een aanvraag. Dit is niet toegestaan, zodat hier tijdens de DPIA-gesprekken nog eens aandacht voor gevraagd is. Ook in werkoverleggen zal dit regelmatig meegenomen moeten worden om alert te blijven.

○ 3.11 Bewustwording

Van februari tot en met september 2021 zijn wekelijks twee e-mails met een korte e-learning over privacy en informatiebeveiliging gestuurd aan alle medewerkers. Door de grote regelmaat van deze korte lessen over beide onderwerpen en het steeds terug kunnen kijken van eerder gestuurde lessen is het bewustzijn verhoogd en blijft dit beter tussen de oren zitten. Ook in 2022 komt hier een vervolg op om het bewustzijn hoog te houden, maar dan wordt bij een andere aanbieder voor een iets andere vorm gekozen.

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.

○ 3.12 Borging

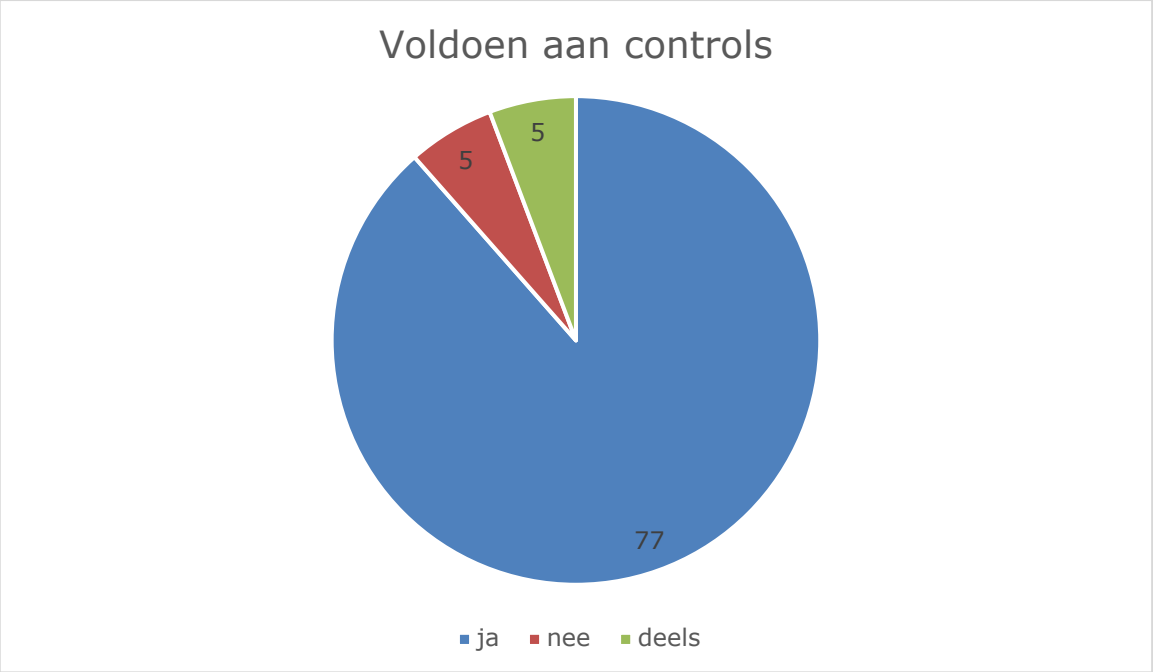
De VNG en IBD hebben samen begin 2021 een vernieuwd borgingsdocument opgesteld, met quickscans en controlevragen. De quickscans kunnen worden gebruikt om snel te meten waar de organisatie staat op de diverse thema's. Vervolgens kan een verdiepingsslag worden gemaakt met de control-vragenlijsten, opgesplitst in O- controls en P-controls (P-controls per afdeling). O ziet op organisatiemaatregelen (circa 221 controlevragen/normen) en P ziet op procesmaatregelen (circa 224 controlevragen/normen per afdeling/vakgebied). In de control-vragen wordt gevraagd om het volgende aan te geven:
(1) de mate waarin de maatregelen zijn geïmplementeerd;
(2) het volwassenheidsniveau per control (5 niveaus per set controlevragen/normen);
(3) de motivatie waarom voldaan is aan de omschrijving van het volwassenheidsniveau (en maatregel).

De vragen zijn opgesplitst in 7 onderdelen: beleid, processen, organisatorische inbedding, rechten van betrokkenen, samenwerking, beveiliging en verantwoording.

Tabel. In onderstaande tabel is de score per onderdeel uit de algemene quickscan weergegeven:

Score per onderdeel	Ja	Nee	Gedeeltelijk
Beleid	8	0	1
Processen	21	1	2
Organisatorische Inbedding	12	0	1
Rechten van betrokkenen	9	4	0
Samenwerking	3	0	0
Beveiliging	13	0	1
Verantwoording	11	0	0
Totaal	77	5	5

Grafiek. 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 2022 en volgende jaren. In 2021 zijn de werkprocesbeschrijvingen die gemeentebreed van toepassing zijn, een deel van de werkprocesbeschrijvingen van afdeling Gemeentewinkel, een deel van de werkprocesbeschrijvingen van afdeling Bedrijfsvoering en een deel van de werkprocesbeschrijvingen van de afdeling Ruimte en Groen vastgesteld, zodat dan beter en volledi ger aan deze norm wordt voldaan.

In 2022 volgt het tweede deel van de werkprocesbeschrijvingen van de afdelingen, waarbij het streven is dat medio 2022 de werkprocesbeschrijvingen compleet zijn.

Verder worden een aantal zaken die op gedeeltelijk staan in de actualisering van beleid en de opstelling van nieuw beleid meegenomen. Overigens kan opgemerkt worden dat een 100% score nooit te garanderen is, omdat privacy & security vakgebieden zijn die continue in beweging zijn. Gelet op de grootte van de gemeente Scherpenzeel is het ook niet haalbaar om op alle onderdelen toe te werken naar het hoogste volwassenheidsniveau, omdat de middelen en capaciteit daarvoor niet toereikend zijn. Er moeten dan keuzes gemaakt worden welk volwassenheidsniveau acceptabel is, waarbij privacy en security goed geborgd zijn. In 2021 is een gemeentebrede toetsing gedaan en in 2022 zal een toetsing per afdeling/per vakgebied gedaan worden.

○ 3.13 Overige zaken

Ook in 2022 zijn er wetswijzigingen te verwachten, waarin gegevensverwerking voorkomt.

Zo treedt op 1 mei 2022 de Wet open Overheid (Woo) als opvolger van de Wet openbaarheid van bestuur (Wob) in werking. Het uitgangspunt van de Woo is een actievere openbaarmakingsverplichting en een ruimere openbaarmaking in geval van passieve openbaarmaking (als een verzoek is ingediend). Ook wordt gestreefd naar het zoveel mogelijk digitaal communiceren met de indieners van verzoeken. Naast nieuwe mogelijkheden, levert dit vanuit privacy & security ook risico's op, zodat bij implementatie betrokkenheid PO, CISO en FG van belang is.

En vermoedelijk treedt Wet Aanpak Meervoudige problematiek Sociaal Domein (WAMS) eind 2022 of in 2023 in werking. In de WAMS wordt wettelijke borging van de regionale meldpunten voorbereid. Dit wetsvoorstel, voortvloeiend uit het traject Uitwisseling Persoonsgegevens (UPP) is in 2021 in consultatie geweest. De wet WAMS betreft een aanpassing van de Wmo en regelt een basis voor gegevensdeling in het sociaal domein en een gemeentelijk meldpunt niet-acuut. Ook deze wet levert, naast nieuwe mogelijkheden, vanuit privacy & security risico's op, zodat bij implementatie betrokkenheid PO, CISO en FG van belang is.

4. AANBEVELINGEN

Belang (1): 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.

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 is gestart met een "Nano" e-learning die bestaat uit korte lessen van een paar minuten die iedere week gedurende 8 maanden per e-mail gestuurd zijn. In 2021 is daar een vervolg op gekomen, waarin gedurende 6 maanden iedere week twee korte lessen per e-mail gestuurd zijn. Ook in 2022 komt hier een vervolg op om het bewustzijn hoog te houden, maar dan wordt bij een andere aanbieder voor een iets andere vorm gekozen.

Belang (2): 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, door in bestaande of reeds beschreven werkprocessen op te nemen wanneer een verwerkersovereenkomst nodig is, zodat dit tijdens het werkproces al onder de aandacht gebracht wordt.

Belang (3): 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 2022

In de hoofdstukken 2 en 3 is aangegeven welke werkzaamheden in 2021 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 2022 worden de onderstaande acties opgepakt, waarover in het Jaarverslag FG 2022 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.
- Continue aandacht voor en 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.
- Continuering van bewustwording, onder andere door het voortzetten van de e-learnings. Vervolg op e-learning van 2020 en 2021 om het bewustzijn over privacy en security hoog te houden.
- De afdelingsspecifieke controls/controls per vakgebied beoordelen in het borgingsdocument
- Aanvullende actiepunten / aandachtspunten voortkomend uit borgingsdocument oppakken en uitvoeren, zoals:
    - het opstellen van (werk)procesbeschrijvingen, protocollen etc.
    - toetsing en waar nodig herzien van de privacyverklaring van de gemeente Scherpenzeel;
    - uitwerken en vaststellen van werkprocessen en daarin ook aandacht schenken aan de bescherming van persoonsgegevens en de communicatie van de processen in de organisatie;
    - controle of opvolging wordt gegeven aan de maatregelen die zijn geadviseerd in de DPIA’s;
    - controle of systemen en voorzieningen voldoen aan de uitoefening van de rechten van betrokkenen;
    - opnieuw onder de aandacht brengen van de procedure rechten van betrokkenen;
    - maken van afspraken met externe partijen die persoonsgegevens ontvangen van de gemeente en zelf verwerkingsverantwoordelijk zijn;
    - per applicatie vaststellen of logging noodzakelijk is. Aandacht voor loggingbeleid en de controle van logging;
    - opstellen van een procedure voor toestemming en medewerkers hierover informeren;

- Plaatsen van een Nieuwsbericht in Scherpenzeelse Krant of in de Gemeentegids over een AVG-onderwerp voor burgers over bijvoorbeeld, recht van inzage, het beleid of het register, etc.
- Telewerkregeling actualiseren en daarin het hybride werken opnemen, omdat dit zowel mogelijkheden als risico's meebrengt voor privacy en security.

BIJLAGE WETTELIJK KADER

I. 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.

II. Specifieke wetgevende ontwikkelingen, jurisprudentie en nieuwsberichten van Autoriteit Persoonsgegevens

1. AP nieuwsbericht 6 mei 2021

AP verzwaart toezicht op gemeente

De AP heeft besloten het toezicht op een gemeente te verzwaren. De AP heeft zorgen of deze gemeente de (gevoelige) gegevens van de inwoners wel voldoende beschermt. De betreffende gemeente wordt daarom verplicht elke 3 maanden een uitgebreide rapportage aan de AP te verstrekken. Aanleiding zijn signalen over overtredingen van de privacywet. Verder constateert de lokale Rekenkamer dat er na dik 2 jaar AVG nog geen privacybeleid was vastgesteld. Ook stelt het rapport van de Rekenkamer dat de zowel de onafhankelijkheid als de informatiepositie van de interne toezichthouder, de functionaris gegevensbescherming (FG), onvoldoende waren geborgd. De wet verbindt duidelijke eisen aan de positionering van een FG. Zo is het essentieel dat de FG onafhankelijk kan toezien op de naleving van de AVG in de betreffende organisatie.

Verzwaren van toezicht

Het is de bevoegdheid van een inspectie of een toezichthouder te bepalen welke vorm en welke intensiteit van toezicht noodzakelijk is. Om de (gevoelige) informatie van inwoners te beschermen, is snelheid essentieel. Daarom is besloten voor een interventie die direct ingezet kan worden; het verzwaren van het toezicht. De AP heeft de gemeente gesommeerd om een jaar lang elk kwartaal een voortgangsrapportage te sturen over de maatregelen die

de gemeente neemt om aan de AVG te voldoen. Het doel is dat de gemeente zorgdraagt voor een veilige en betrouwbare verwerking van persoonsgegevens van de inwoners van deze gemeente. De AP sluit een nader onderzoek niet uit. Dat kost echter veel tijd. Inmiddels heeft de gemeente de eerste rapportage aangeleverd.
Intern toezicht verplicht
Een gemeente is verantwoordelijk voor het opstellen en het uitvoeren van het privacybeleid. Net als alle overheden is een gemeente verplicht om een FG aan te stellen; een onafhankelijke, interne privacy-functionaris. De FG ziet toe op de naleving van het privacybeleid en adviseert over privacyrisico's. Voorkomen is beter dan genezen. Daarom moet de FG in een vroeg stadium betrokken worden en toegang hebben tot alle relevante informatie. Op die manier wordt de organisatie in staat gesteld maatregelen te nemen en de persoonsgegevens van burgers en klanten te beschermen.

2. AP nieuwsbericht van 30 juli 2021

AP publiceert aanbevelingen voor smart cities
De Autoriteit Persoonsgegevens (AP) publiceert aanbevelingen voor de ontwikkeling van zogenoemde smart city-toepassingen. De aanbevelingen zijn bedoeld voor gemeenten die met slimme sensoren en meetapparatuur data in de openbare ruimte verzamelen of dat van plan zijn. De adviezen van de AP zijn nodig omdat gemeenten niet altijd voldoende stilstaan bij de privacywetgeving terwijl dit juist bij smart city-toepassingen waarbij persoons-gegevens van de burgers verwerkt worden essentieel is. Slecht ontwikkelde toepassingen kunnen namelijk ten koste gaan van de vrijheid van inwoners en bezoekers van die gemeente. Bijvoorbeeld wanneer burgers in de openbare ruimte worden gevolgd op een manier die niet nodig is of niet is toegestaan.
Een gemeente die technologie inzet, kan daarbij persoonsgegevens verwerken. Met sensoren of meetapparatuur worden bijvoorbeeld verkeersstromen en bezoekersaantallen gemeten of uitgaansgebieden gemonitord om de mobiliteit en veiligheid te verbeteren. De privacywet - de Algemene verordening gegevensbescherming (AVG) - beschermt mensen tegen het onnodig of ongeoorloofd verzamelen of gebruiken van hun persoonsgegevens in de openbare ruimte.
Ongedwongen over straat
Monique Verdier, vicevoorzitter AP: "*Het gevaar bestaat dat we naar een surveillancemaatschappij gaan waar je niet meer ongedwongen over straat kunt lopen. De inzet van technologie kan gemeenten weliswaar meer inzicht geven in het gebruik van de openbare ruimte, maar dat mag niet zonder stil te staan bij de prijs die de inwoners en bezoekers van die gemeente hiervoor betalen. Hoe verhoudt het verzamelen van hun gegevens in de openbare ruimte zich tot hun vrijheid? Wie kan er allemaal bij die gegevens en waar mogen die voor worden gebruikt? Welke informatie mag aan elkaar worden gekoppeld? De technische mogelijkheden zijn oneindig, maar aan wat ethisch en juridisch toelaatbaar is zit een grens.*
Technologie kan ons helpen om onze problemen op te lossen en de stad leefbaarder en veiliger te maken. Maar we moeten het wel zo inregelen dat ze niet zelf allerlei nieuwe problemen en onveiligheidsgevoelens veroorzaken. Bestuurders en ambtenaren moeten de rechten en vrijheden van burgers uiterst serieus nemen. Dat betekent dat zij hun privacy

ook daadwerkelijk meenemen bij elke stap in de ontwikkeling naar een smart city. Laat privacy het startpunt zijn van innovatie, niet het sluitstuk."

3. AP nieuwsbericht van 16 september 2021

Handreiking Wet gemeentelijke schuldhulpverlening

De gewijzigde Wet gemeentelijke schuldhulpverlening (Wgs) geeft meer duidelijkheid over wat wel en niet mag bij de verwerking van persoonsgegevens voor (de toeleiding naar) schuldhulpverlening. Toch blijken er in de praktijk nog veel vragen te zijn. Daarom heeft de Autoriteit Persoonsgegevens (AP) een handreiking opgesteld met aandachtspunten. Hiermee moeten gemeenten en hulpverleners rekening houden om aan de privacywetgeving te voldoen. De Wgs regelt dat mensen met (dreigende) problematische schulden bij gemeenten terecht kunnen voor onder meer advies, schuldbemiddeling of een saneringskrediet.

Wat is het probleem?

De AP heeft de afgelopen jaren meerdere signalen, klachten en vragen ontvangen over schuldhulpverlening. Probleem is vaak dat niet duidelijk is welke gegevens de verschillende partijen met elkaar mogen delen en onder welke voorwaarden. En dat in de praktijk gegevens worden gedeeld zonder dat daarvoor een wettelijke grondslag bestaat.
Een aantal van deze onduidelijkheden komt aan bod in de wijziging van de Wgs, die op 1 januari 2021 van kracht is geworden.

III. Toezichtskader AP: ontwikkelingen en gevolgen

De Autoriteit Persoonsgegevens (AP) heeft in november 2019 haar toezichtkader voor de jaren 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.