Gemeente Scherpenzeel

Jaarverslag

Functionaris Gegevensbescherming 2020

Jaarverslag

Functionaris Gegevensbescherming 2020

Opdrachtgever:	gemeente Scherpenzeel Afdeling Bedrijfsvoering
Auteur:	Sascha Beekman, FG
Datum:	15 januari 2021

Inhoud

MANAGEMENTSAMENVATTING

Dit verslag betreft de periode van 1 januari 2020 tot en met 31 december 2020. In deze verslagperiode is het volgende gerealiseerd:

- Het Jaarverslag FG over 2019 is in februari 2020 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 2017/2018 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.
- Om het bewustzijn over het veilig en zorgvuldig werken met persoonsgegevens vast te houden en te verbeteren, is er in de periode van februari tot en met september 2020 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. Deze e-learning zal in2021 een vervolg krijgen.
- 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 voorgaande verslagperiodes, van 1 oktober 2017 tot en met 31 december 2018 en van 1 januari 2019 tot en met 31 december 2019, is hard gewerkt om aan alle vereisten van de AVG te voldoen. Daarbij 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 2020, zijn de in 2019 geanalyseerde noodzakelijke stappen gezet om de privacy en de bescherming van persoonsgegevens nog beter te borgen. Daar komt bij dat de baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) is omgezet naar de Baseline Informatiebeveiliging Overheid (BIO), waarbij de gewijzigde en/of aangescherpte maatregelen en normen geïmplementeerd en nageleefd moeten worden, waarbij 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 2020 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 2020 zijn 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. De standaard en door VNG/IBD verplicht gestelde verwerkersovereenkomst wordt door bijna alle verwerkers geaccepteerd. Zie verder bij 3.6.

Verder zijn in 2020 de eerder in 2017/2018 uitgevoerde DPIA's herzien en opnieuw uitgevoerd en beoordeeld. De resterende DPIA's worden in 2021 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, 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 2020 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 2020 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 2021 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 2020 zijn een tiental 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 2021 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 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 2020 zo'n 18 DPIA's uitgevoerd. In 2021 volgen er nog 9.

○ 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). In dit gremium is de basis gelegd voor het nieuwe informatieveiligheidsbeleid conform BIO maatregelen.

Het jaar 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 2020 is het beleid beoordeeld op actualiteit en het beleid voldoet nog en hoeft nog niet herzien te worden. In 2021 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 zal het register wederom beoordeeld worden op actualiteit en zal dan opnieuw ter vaststelling aangeboden worden aan het college. Het register zal na actualisatie in 2021 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 2020 hebben 8 beveiligingsincidenten plaatsgevonden, waarvan er 2 zijn aangemerkt als meldenswaardig datalek. Deze zijn gemeld bij de AP. Van deze gemelde datalekken is er 1 melding gedaan aan betrokkenen.

Verder is er een incident geweest dat is aan te merken als datalek, maar dat veroorzaakt is door een fout in het sorteer- en bezorgproces van PostNL. De Gemeente Scherpenzeel heeft

de veroorzakende partij erop gewezen hiervan melding te maken aan AP, maar die ontkent de fout en het feit dat sprake is van een datalek. In dit geval is er bij PostNL op aangedrongen een aantekening te maken op deze zaak dat de Gemeente Scherpenzeel het datalek bij hen gemeld heeft en dat de Gemeente Scherpenzeel niet verantwoordelijk is voor dit datalek.

○ 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 wordt in 2021, samen met een aantal andere werkprocesbeschrijvingen door het MT vastgesteld, waarna de werkprocesbeschrijving op intranet geplaatst worden en daarmee voor alle medewerker te raadplegen is.

Er is door betrokkenen in de verslagperiode geen gebruik gemaakt van de mogelijkheden om hun rechten in te roepen.

○ 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 januari 2021 wordt deze aanvullende module gebruikt 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 zal niet eerder dan in het tweede halfjaar van 2021 plaatsvinden.

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 is hierop toegezien, waarbij vooral de eigen mappen van de medewerkers de aandacht verdienen. In 2021 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 twee gevallen is daarvan afgeweken. Dat zijn de volgende:

24-1-2020 Securitech:
ID-document scanner Burgerzaken. De verwerkersovereenkomst van Securitech is uitgebreider en goed gedetailleerd. Aangezien het gaat om ID-documenten is de uitgebreidere en gedetailleerdere overeenkomst geaccepteerd.

30-7-2020 Embrace:
Aan de standaard verwerkersovereenkomst is door Embrace in artikel 4 toegevoegd dat een vrijwaringsverklaring wordt ondertekend door de auditor voorafgaande aan de security check. Betreffende verklaring is opgenomen als bijlage 3 bij de verwerkersovereenkomst.

Het overzicht wordt consequent bijgehouden. In totaal zijn er 92 partijen beoordeeld, waarbij met 79 partijen een verwerkersovereenkomst afgesloten is en in 4 gevallen alleen nog gewacht wordt op het retour ontvangen van de ondertekende overeenkomst. 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 6 gevallen was sprake van een kortdurende hoofdovereenkomst, waarvan de dienstverlening is beëindigd, zodat daarmee de verwerkersovereenkomst ook is komen te vervallen.

○ 3.7 Privacy in het Sociaal Domein

Er is een checklist opgesteld voor 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.

Er is in regionaal verband (Foodvalley) een vernieuwd privacyprotocol en een convenant voor gegevensdeling opgesteld, die naar verwachting in 2021 afgerond en vastgesteld zullen 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 12 januari 2021 haar jaarcijfers gepubliceerd.

Het jaar 2020 was voor gemeenten ook op het terrein van informatiebeveiliging en gegevensbescherming een veelbewogen jaar. Risico's rond de informatievoorziening werden op verschillende manieren zichtbaar. Waar men in het begin van het jaar niet meer kon thuiswerken door problemen met Citrix, was men krap een maand later nagenoeg volledig aangewezen op thuiswerkfaciliteiten door maatregelen rond het nieuwe coronavirus. De IBD ondersteunde gemeenten ook in 2020 bij de structurele verhoging van digitale weerbaarheid en bescherming van persoonsgegevens. Hiermee hebben gemeenten een collectieve voorziening die steunt op drie pijlers: incidentcoördinatie, advies en kennisdeling. In dit jaaroverzicht treft u de belangrijkste resultaten en ontwikkelingen.

Het jaar in cijfers
De IBD ontving het afgelopen jaar 3.845 vragen en meldingen rondom informatiebeveiliging en 715 privacyvragen. De IBD registreerde 175 incidenten met een hulp-, coördinatie- of ondersteuningsvraag van gemeenten en ontving hierover 750 inkomende telefoongesprekken. Eén maal werd het gemeentelijk responsnetwerk ingeroepen. Bij het incident in Hof van Twente in december, verleenden de IBD en experts van andere gemeenten ter plaatse assistentie. Behulpzame onderzoekers meldden 19 kwetsbaarheden onder de voorwaarden van responsible disclosure en kregen een plekje in onze hall of fame of een T-shirt als dank. De IBD verleende bij deze incidenten hulp variërend van bijvoorbeeld vertegenwoordiging in landelijk crisisoverleg bij de problemen rond Citrix tot advies over herstelwerkzaamheden en aanvullende maatregelen na een geslaagde phishingaanval. De IBD-CERT verstuurde 1.878 kwetsbaarheidsmeldingen. De IBD organiseerde in 2020 meer dan 40 online bijeenkomsten zoals werkgroepen, intervisiebijeenkomsten, webinars en bespreekuren waarbij de nadruk lag op onderlinge gesprekken tussen de deelnemers. De website informatiebeveiligingsdienst. nl werd 134.103 maal bezocht en daar verschenen 72 nieuwe en bijgewerkte kennisproducten die samen met het totale aanbod maar liefst 94.115 keer werden gedownload. De meest gedownloade producten waren de BIO, de baselinetoets, de handreiking dataclassificatie en de standaard verwerkersovereenkomst. De IBD voert het beheer over het VNG privacyforum met meer dan 4.700 gemeentelijke deelnemers. Via de online DPIA-tool werden 70 nieuwe privacy-impactanalyses gemaakt op verschillende gemeentelijke processen en applicaties.

Uit het jaarbericht van IBD blijkt dat er het afgelopen jaar veel beveiligingsincidenten zijn geweest, maar minder dan het jaar daarvoor. 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, de telewerkovereenkomsten en cartoons 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.

○ 3.10 Data Protection Impact Assessments

3.10.1 Overzicht DPIA's

In 2020 zijn er DPIA's uitgevoerd/geactualiseerd op de volgende vakgebieden:

- BRP/burgerzaken
- Belastingen (WOZ), omdat de belastingsamenwerking toch niet is doorgegaan en sinds zomer 2020 de Gemeente Scherpenzeel dit weer volledig zelf doet
- Crediteurenadministratie
- Debiteurenadministratie
- Gehandicaptenparkeerkaart/plaats

- Huisvesting statushouders
- ICT - informatiebeveiliging gemeentebreed
- ICT - applicaties
- Jeugdwet
- Koninklijke Onderscheidingen
- Openbare Orde & handhaving
- Onderwijs en leerplicht
- Participatiewet en Suwinet
- Personeelszaken
- Uitkeringenadministratie
- Vergunningenadministratie (omgevingsvergunningen, parkeerzones, etc.)
- Wet maatschappelijke ondersteuning
- Woningurgentie

In 2021 zullen de volgende DPIA's uitgevoerd gaan worden:

- BAG/BGT
- Diftar/afvalpassen
- Veiligheid (o.a. RIEC, Bibob, terugkeer begeleiding ex-gedetineerden, tijdelijk huisverbod, inclusief bestuurlijke informatie justitiabelen)
- vergunningen (evenementen, DHW, APV), in combinatie met Veiligheid
- Wet gemeentelijke schuldhulpverlening, nu de nieuwe wet per 1 januari 2021 in werking treedt en bekend is wat er gewijzigd is ten opzichte van de voorgaande wetgeving en werkwijze

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 wordt ondernomen.

Bij vakgebieden waarvoor een formulier beschikbaar is voor het doen van een aanvraag zijn de formulieren beoordeeld en waar nodig zijn aanpassingen doorgevoerd of geadviseerd. Bij landelijk gebruikte formulieren wordt dit meegenomen naar vakoverleggen die regionaal of landelijk plaatsvinden of bij een meldpunt voor vragen en opmerkingen.

Het informeren van betrokken kan vaak ook beter. Niet altijd wordt gemeld met welke ketenpartners gegevens worden gedeeld, zodat hiervoor meer aandacht wordt gevraagd. In sommige vakgebieden kan een folder of brochure hieraan bijdragen. Voor Sociaal Domein zijn in 2019 de bestaande folders en brochures beoordeeld en aangevuld met informatie over het verwerken en delen van gegevens. Omdat niet voor alle onderdelen van het Sociaal Domein folders en brochures beschikbaar zijn, zal dit waar nodig in 2021 aangevuld worden. Ook voor vakgebieden buiten het Sociaal Domein kan dit een zinvolle aanvulling zijn, zodat ook daarnaar gekeken gaat worden in 2021.

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. Zoals bijvoorbeeld bij het COA. De gemeente registreert en bewaart zelf geen gegevens van statushouders, omdat dit in een landelijk systeem van het COA wordt bijgehouden. Daarin kan echter te ver terug gekeken worden, zodat een verzoek om opschoning van het systeem en het verwijderen van te oude gegevens en dossiers bij het COA gedaan zal worden. Ook bij leerlingenvervoer wordt gebruik gemaakt van een applicatie waar de gemeente zelf niet de bewaartermijnen kan inregelen, zodat ook in dat geval de vraag uitgezet zal moeten worden bij de leverancier of ketenpartner.

Daarnaast blijven er ook regelmatig gegevens en documenten in outlook staan die bewaard moeten worden in Djuma of SuiteSD. Hiervoor zal in 2021 aandacht gevraagd worden met het verzoek om e-mailboxen op te schonen en belangrijke mails met gegevens en documenten te archiveren in het geldende zaaksysteem.

Verder zijn de raadpleegprofielen in de verschillende applicaties niet altijd correct en bij een functie passend. De autorisaties voor de verschillende functies, rollen en taken zullen doorgelicht en waar nodig aangepast worden.

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. Zo is in het Sociaal Domein bijvoorbeeld de werkafspraak gemaakt om alleen initialen van klanten te noemen in plaats van volledige namen. In het kader van handhaving werden nog weleens informatie en documenten gedeeld via what's app, zodat daarvoor in het DPIA-gesprek al aandacht is gevraagd om gebruik te maken van beveiligde e-mail in plaats van what's app.

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.

Tot slot wordt nog aanbevolen om een convenant Sociaal Domein op te gaan stellen in 2021, waarbij eerst geïnventariseerd moet worden welke partijen hierbij betrokken moeten zijn en wat de gemeente in een convenant geregeld wil hebben.

○ 3.11 Bewustwording

Van februari tot en met september 2020 is wekelijks een e-mail 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.

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.

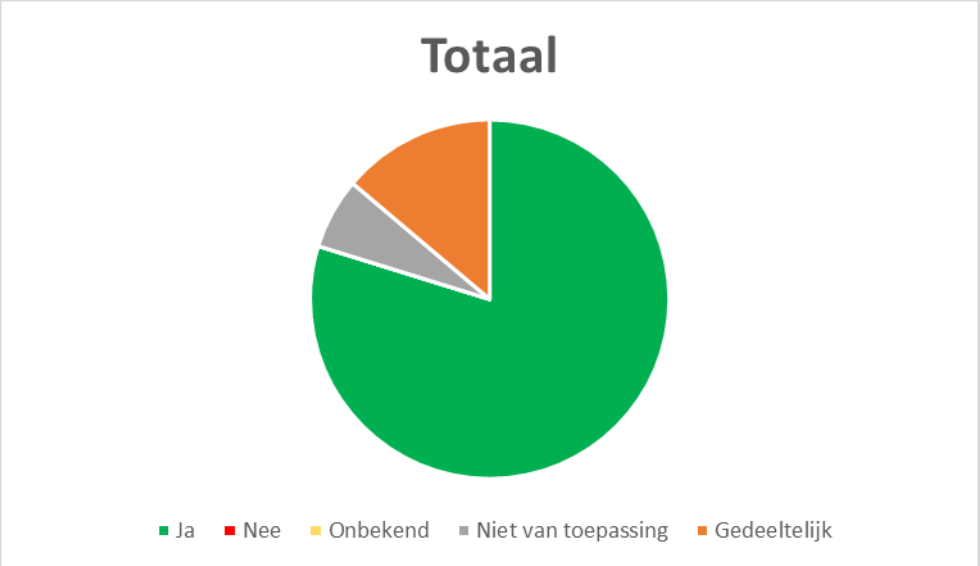
○ 3.12 Borging

De VNG en IBD hebben samen 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.

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

Score per onderdeel	Ja	Nee	Onbekend	N.v.t.	Gedeeltelijk
Beleid	11	0	0	1	2
Processen	28	0	0	1	5
Organisatorische Inbedding	38	0	0	5	4
Rechten van betrokkenen	27	0	0	3	3
Samenwerking	15	0	0	2	2
Beveiliging	15	0	0	1	5
Verantwoording	16	0	0	0	5
Totaal	150	0	0	12	26

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 aanbesteed 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 2021 en volgende jaren. In 2021 worden de werkprocesbeschrijvingen die gemeentebreed van toepassing zijn, van afdeling Gemeentewinkel en van afdeling Bedrijfsvoering vastgesteld, zodat dan beter en volledieger aan deze norm wordt voldaan. In 2022 volgen dan de werkprocesbeschrijvingen van de afdeling Ruimte & Groen, zodat daarna 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.

○ 3.13 Overige zaken

Op 30 april 2020 kwam het verzoek van de Burgemeester, via de beleidsmedewerker Onderwijs, of het vanuit privacy mogelijk was om alle Scherpenzeelse schoolkinderen een brief (per e-mail) te sturen om ze veel plezier te wensen als ze vanaf 11 mei 2020 weer naar school mogen. Voor de leerlingen van de basisscholen wordt dat door de scholen zelf geregeld. Voor de leerlingen van de speciaal (basis)onderwijs scholen geldt dat deze scholen niet in Scherpenzeel staan, maar dat er wel leerlingen uit Scherpenzeel op school zitten. In het kader van leerlingenvervoer heeft de beleidsmedewerker Onderwijs een bestand met e-mailadressen van de ouders van deze leerlingen. Na overleg is ervoor gekozen om gebruik te maken van dit bestand. De gemeente heeft als taak de ouders/verzorgers van de leerlingen uit Scherpenzeel te informeren (of in dit geval veel plezier te wensen) over de versoepelde maatregelen in verband met de covid-19-pandemie en het weer opengaan van de scholen. Het gegevensbestand is weliswaar voor een ander doel verzameld (leerlingenvervoer), maar dit is aan te merken als een afgeleid belang daarvan. De FG heeft daarom geen bezwaar tegen deze verwerking gezien, aangezien dit afgeleid belang op grond van de uitoefening van de publiekrechtelijke taak van de Gemeente Scherpenzeel danwel als een gerechtvaardigd belang in de zin van artikel 6 AVG aangemerkt kan worden.

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.

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 worden. Uit statistische gegevens blijkt dat 44% van de medewerkers de e-learning gevolgd heeft voor het gedeelte privacy en 46% voor het gedeelte security, waarvan voor beide onderdelen 96% de lessen ook heeft afgerond. In 2021 komt hier een vervolg op om het bewustzijn hoog te houden, waarbij gestreefd wordt naar >60 % deelname en 100% afronding van de lessen.

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, 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: 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 2021

In de hoofdstukken 2 en 3 is aangegeven welke werkzaamheden in 2020 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 2021 worden de onderstaande acties opgepakt, waarover in het Jaarverslag FG 2021 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 om het bewustzijn over privacy en security hoog te houden, waarbij nieuwe medewerker in een eenmalige e-learning van 45 minuten alle lessen uit 2020 ineens kunnen doen, zodat zij gelijktijdig met de andere medewerkers aan de e-learning van 2021 kunnen deelnemen.
- Aanvullende actiepunten / aandachtspunten voortkomend uit borgingsdocument oppakken en uitvoeren, zoals:
    - het opstellen van (werk)procesbeschrijvingen, protocollen etc.
    - het opstellen van beleid specifiek gericht op cameratoezicht en de communicatie van dit beleid in de organisatie;
    - 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.

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, jurisprudentie en nieuwsberichten van Autoriteit Persoonsgegevens**

1. AP nieuwsbericht 24 april 2020

De European Data Protection Board (EDPB) heeft twee nieuwe guidelines vastgesteld gerelateerd aan de bestrijding van het coronavirus. Het gaat om guidelines voor het verwerken van gezondheidsgegevens voor wetenschappelijk onderzoek en om guidelines rondom het gebruik van locatiegegevens en rondom het gebruik van apps die inzage geven in contacten tussen mensen, de zogenoemde (contact) tracing apps. De guidelines zijn onder meer bedoeld voor Europese overheden, bedrijven en organisaties zoals ziekenhuizen.

2. AP nieuwsbericht 17 juni 2020

EDPB: Grenzen EU weer open tijdens corona? Let op privacy!
Steeds meer grenzen tussen EU-lidstaten gaan weer open, nu de coronamaatregelen versoepeld zijn. De lidstaten kunnen hierbij extra maatregelen willen nemen. Bijvoorbeeld coronatests aan de grens, een verplichte medische verklaring of verplicht gebruik van een corona-app. De Europese privacytoezichthouders waarschuwen dat de EU-lidstaten hierbij het recht op privacy moeten blijven beschermen. En dat samenwerking tussen corona-apps in verschillende landen niet mag leiden tot schending van de privacywetgeving. Dat stellen de EU-privacytoezichthouders in 2 verklaringen die ze aannamen tijdens een vergadering van de European Data Protection Board (EDPB) op 16 juni 2020.

Maatregelen grenzen: In de verklaring over maatregelen bij grenzen benadrukt de EDPB dat de privacywetgeving van kracht blijft, ook in deze tijd. Natuurlijk moet corona bestreden worden. Maar daarbij moeten fundamentele rechten en vrijheden beschermd blijven, aldus de EDPB.
Samenwerking tussen apps: Verschillende landen in de EU gebruiken 'corona contact tracing apps'. Met het openen van de grenzen willen overheden dat de verschillende nationale apps kunnen samenwerken. De EDPB stelt in de verklaring over de samenwerking tussen corona-apps dat het delen van data tussen verschillende apps alleen kan met de vrijwillige deelname van de gebruiker. Daarbij stelt de EDPB dat die samenwerking tussen apps ('interoperabiliteit') niet mag leiden tot het verzamelen van meer data dan nodig. De EDPB benadrukt tot slot dat samenwerking tussen de apps kan leiden tot verhoogde risico's voor gegevensbescherming. Overheden moeten daar dus heel voorzichtig mee omgaan en alle mogelijke opties overwegen.

3. AP nieuwsbericht 23 juli 2020

AVG-guidelines over de PSD2-richtlijn open voor consultatie: De European Data Protection Board (EDPB) heeft guidelines opgesteld over de verhouding tussen de PSD2-richtlijn en de Algemene verordening gegevensbescherming (AVG). De openbare consultatie van deze guidelines loopt tot en met 16 september 2020.
PSD2: In 2019 is de nieuwe Europese richtlijn voor betaaldiensten in Nederland in werking getreden, Payment Service Directive 2 (PSD2). Deze richtlijn regelt onder meer dat niet alleen banken maar ook andere partijen toegang mogen hebben tot een betaalrekening. Dat mag onder bepaalde voorwaarden, zoals toestemming van de rekeninghouder. De bescherming van de privacy van consumenten is een belangrijk onderdeel van PSD2, omdat betaalgegevens gevoelige financiële persoonsgegevens zijn.
Guidelines PSD2 & AVG: Deze guidelines geven aanbieders van betaaldiensten meer duidelijkheid over de wijze waarop zij persoonsgegevens kunnen verwerken. De guidelines besteden onder meer aandacht aan toestemming, dataminimalisatie, beveiliging en transparantie.

4. AP nieuwsbericht 8 september 2020

Consultatie nieuwe guidelines EDPB: De European Data Protection Board (EDPB) heeft 2 nieuwe guidelines opgesteld: over de begrippen 'verantwoordelijke' en 'verwerker' en over targeting van gebruikers van sociale media. Beide (Engelstalige) guidelines staan nu open voor feedback.
Guidelines 'verantwoordelijke' en 'verwerker': Sinds de Algemene verordening gegevensbescherming (AVG) van toepassing is, zijn er veel vragen over de begrippen 'verantwoordelijke' en 'verwerker' en in hoeverre die zijn gewijzigd door de AVG. Vooral als het gaat om gezamenlijke verantwoordelijkheid en de verplichtingen voor verwerkers. Deze guidelines geven uitleg over de verschillende begrippen. Ook gaan de guidelines in op de belangrijkste gevolgen van deze begrippen voor verantwoordelijken, verwerkers en gezamenlijke verantwoordelijken.
Guidelines targeting sociale media: Targeting van gebruikers van sociale media is een manier om gericht te kunnen adverteren. Het is onderdeel van het verdienmodel van veel aanbieders van sociale media. Deze guidelines richten zich op de rollen en

verantwoordelijkheden van adverteerders en aanbieders. De guidelines gaan daarbij onder meer in op de privacyrisico's voor gebruikers van sociale media en op de belangrijkste vereisten uit de privacywetgeving, zoals de juridische basis voor de verwerking.

5. AP nieuwsbericht 11 november 2020

Aanbevelingen EDPB voor doorgifte persoonsgegevens na Schrems II-uitspraak (vervolg op: Statement on the Court of Justice of the European Union Judgment in Case C-311/18 - Data Protection Commissioner v Facebook Ireland and Maximillian Schrems d.d. 17 juli 2020)
De European Data Protection Board (EDPB) heeft aanbevelingen opgesteld voor de doorgifte van persoonsgegevens naar derde landen. Dat zijn landen waar persoonsgegevens minder goed beschermd zijn dan in de EU. De EDPB wil het bedrijfsleven hiermee meer duidelijkheid geven, nadat het Europese Hof van Justitie het EU-VS Privacy Shield ongeldig verklaarde. In juli concludeerde de hoogste Europese rechter in de Schrems II-uitspraak dat de bescherming van persoonsgegevens in de VS ernstig tekortschiet, ondanks het Privacy Shield. Dat waren de afspraken tussen de EU en de VS op basis waarvan bedrijven persoonsgegevens vanuit de EU mochten doorgeven aan de VS. Met de uitspraak zette het Hof een streep door het Privacy Shield. Alleen als organisaties kunnen waarborgen dat gegevens net zo goed beschermd worden als in de EU, mogen zij nog persoonsgegevens doorgeven aan de VS. En aan andere landen waarmee de EU geen (geldige) afspraken heeft over bescherming van persoonsgegevens.
Modelcontracten: De meest praktische oplossing voor bedrijven die persoonsgegevens willen doorgeven naar derde landen, is het gebruik van modelcontracten (ook wel standaardbepalingen, standard contractual clauses of SCC's genoemd). Maar dat mag in de meeste gevallen alléén als een bedrijf voldoende aanvullende maatregelen neemt om de veiligheid van de doorgifte te waarborgen.
Aanbevelingen EDPB: Om bedrijven te helpen die bescherming te waarborgen, heeft de EDPB aanbevelingen opgesteld voor aanvullende maatregelen bij het gebruik van 'doorgifte-instrumenten', waaronder modelcontracten. De EDPB noemt verschillende aanvullende maatregelen die bedrijven kunnen overwegen, zoals goede encryptie en pseudonimisering. Bedrijven zullen per geval moeten bekijken welke maatregel of combinatie van maatregelen nodig is om persoonsgegevens goed te beschermen.
Zie verder:

- Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data
- Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.

Bij twijfel: houd data in EU
Het zal niet altijd mogelijk zijn om aanvullende maatregelen te treffen die persoonsgegevens voldoende beschermen. Sommige landen beschermen privacy en andere grondrechten onvoldoende. Daar hebben Europese bedrijven en Europese privacytoezichthouders weinig directe invloed op. Als bedrijven persoonsgegevens willen opslaan in landen waar persoonsgegevens minder goed worden beschermd, is het hun eigen verantwoordelijkheid om te waarborgen dat dit alsnog net zo veilig gebeurt. Is er na nader onderzoek nog steeds enige twijfel over de veiligheid van doorgifte van persoonsgegevens? Stop dan met de doorgifte of begin niet aan een nieuwe doorgifte. Houd data dan in de EU.

Inzage door veiligheidsdiensten VS: Veel bedrijven slaan data op in de VS. Nu heeft de Europese rechter dit land specifiek benoemd als land waar persoonsgegevens niet goed beschermd zijn. De veiligheidsdiensten in de VS mogen alle persoonsgegevens op servers in de VS inzien en gebruiken. Ook kunnen deze diensten persoonsgegevens al onderscheppen vóórdat ze in de VS aankomen. Het is daarom niet altijd mogelijk om te voorkomen dat de Amerikaanse veiligheidsdiensten inzage krijgen in persoonsgegevens die naar de VS worden doorgegeven. Bovendien is de rechtsbescherming door een onafhankelijke rechter onvoldoende geregeld in de VS, concludeerde het Europese Hof van Justitie. Het is dus van groot belang dat de VS zorgen voor een betere bescherming van persoonsgegevens. En het is nu aan de Amerikaanse regering en de Europese Commissie om te onderzoeken of er vervanging kan komen voor het Privacy Shield.

6. AP nieuwsbericht 26 november 2020

De European Data Protection Board (EDPB) heeft een verklaring gepubliceerd over de toekomstige e-Privacyverordening. In deze verklaring uit de EDPB zorgen over het toezicht op de e-Privacyverordening.
De EDPB, het samenwerkingsverband van privacytoezichthouders uit de Europese Unie (EU), heeft zich uitgesproken over het toezicht op de e-Privacyverordening. Deze verordening moet de e-Privacyrichtlijn uit 2002 gaan vervangen. De EDPB vindt dat het toezicht op verwerkingen van persoonsgegevens onder de e-Privacyverordening zou moeten worden toevertrouwd aan dezelfde nationale autoriteiten die toezicht houden op de Algemene verordening gegevensbescherming (AVG). Dat zorgt voor een hoog niveau van bescherming, een gelijk speelveld en een geharmoniseerde interpretatie en handhaving door de EU, aldus de EDPB. Verder benadrukte de EDPB haar eerdere standpunt dat de e-Privacyverordening het beschermingsniveau van de huidige de e-privacyrichtlijn niet zou mogen verlagen. Ook zou de e-Privacyverordening de AVG moeten aanvullen, door sterke waarborgen te bieden voor vertrouwelijkheid en bescherming van alle types van elektronische communicatie.

- **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.