Gemeente Scherpenzeel

Jaarverslag

Functionaris Gegevensbescherming 2017-2018

Jaarverslag

Functionaris Gegevensbescherming 2017-2018

Opdrachtgever:	gemeente Scherpenzeel Afdeling Bedrijfsvoering
Auteur:	Sascha Beekman, FG
Datum:	12 februari 2019

Inhoud

MANAGEMENTSAMENVATTING

Dit verslag betreft de periode van 1 oktober 2017 tot en met 31 december 2018. Als begindatum is 1 oktober 2017 gekozen, omdat de Functionaris Gegevensbescherming (FG) en de Chief Information Security Officer (CISO) per 1 oktober 2017 zijn aangewezen.

In de periode daaraan voorafgaand hebben de FG en de CISO opleidingen gevolgd (van februari tot en met juni 2017), is een plan van aanpak over de implementatie van de Europese Algemene Verordening Gegevensbescherming (AVG) in de gemeente Scherpenzeel vastgesteld door het college op 29 augustus 2017 en zijn FG en CISO bij besluit van 5 september 2017 door het college aangewezen in deze functies.

In de verslagperiode is hard toegewerkt naar de datum van 25 mei 2018, de dag waarop de AVG werkelijk van toepassing is in de hele EU en de Wet bescherming persoonsgegevens (Wpb) is komen te vervallen. Er is gewerkt aan:

- een register van verwerkingen,
- een privacyverklaring (voor op de gemeentelijke website),
- een overzicht van de verwerkersovereenkomsten, het afsluiten van vele nieuwe of geactualiseerde verwerkersovereenkomsten,
- een overzicht van de rechten van betrokkenen (voor op de gemeentelijke website),
- een overzicht van de voorgekomen beveiligingsincidenten en datalekken en een procedure voor het melden en beoordelen hiervan,
- het uitvoeren van Privacy Impact Assessments (PIA's),
- een privacybeleid,
- en niet in het minste: bewustwording van medewerkers.

Hierbij kan opgemerkt worden dat de gemeente Scherpenzeel bij de kleine groep gemeenten hoort die 'klaar' was met de implementatie van de AVG op de gestelde datum van 25 mei 2018. Natuurlijk is 25 mei 2018 niet een einddatum, waarop alles op gebied van privacy echt klaar is. Dit is immers een vakgebied wat continue in beweging is en steeds onder de aandacht zal blijven. Verwerkersovereenkomsten, het register en de verschillende overzichten zijn altijd aan veranderingen onderhevig. Als bijvoorbeeld een overeenkomst afgesloten wordt met een nieuwe leverancier van een softwarepakket of voor het beheren van salarisadministratie zal daar altijd een verwerkersovereenkomst bij afgesloten moeten worden. Veelal zal ook een nieuwe PIA uitgevoerd moeten worden.

Kortom, er dient continue aandacht besteed 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.

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

Het college heeft op 13 februari 2018 het Privacybeleid vastgesteld.
Op 5 september 2017 hebben de CISO en FG een medewerkersbijeenkomst georganiseerd over de AVG en Informatieveiligheid in het kader van bewustwording. Op 22 mei 2018 is een vervolg bijeenkomst georganiseerd voor de medewerkers vanwege de in werking treding van de AVG en wat er tot op dat moment gerealiseerd is bij de implementatie van de AVG. Op 23 mei 2018 is er een bijeenkomst georganiseerd over de AVG voor de vrijwilligersorganisaties om ook deze verenigingen en clubs bewust te maken van het belang van de AVG.
In de periode van september tot en met november 2017 zijn de Privacy Impact Assessments (PIA's) uitgevoerd, waarbij een aantal aanvullende PIA's in april 2018 zijn uitgevoerd. Eind mei 2018 was de PIA rapportage afgerond, waarna deze op 17 juli 2018 door het college is vastgesteld. De rapportage is openbaar gemaakt op de gemeentelijke website.

2.3 Verantwoording Privacy Officer

Door een externe privacy officer is in de periode van november 2017 tot en met februari 2018 het register van verwerkingen opgesteld. In mei 2018 is, na een check met de wetgeving en het overzicht volledig maken, een kolom met bewaartermijnen toegevoegd aan het register en op 17 juli 2018 heeft het college het register vastgesteld. Het register is openbaar gemaakt op de gemeentelijke website.
Tevens is een overzicht gemaakt van de verwerkers en de daarmee afgesloten verwerkersovereenkomsten. Er zijn nieuwe en geactualiseerde overeenkomsten afgesloten en enkele moeten nog (opnieuw) afgesloten worden. Het overzicht wordt consequent bijgehouden.
In de periode september tot en met december 2018 is input geleverd over de AVG voor de ENSIA en is samen met de CISO de audit gedaan.

2.4 Verantwoording CISO

In regionaal verband is er CISO overleg waarbij zaken zoals de ICT-migratie (medio 2017-medio 2018), de BIG en ENSIA besproken worden, aangevuld met het

implementeren van gestelde BIG-normen. Om de implementatie van deze normen te verwezenlijken is 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.

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.

3.2 Register van verwerkingen

Eind februari 2018 was het Register van verwerkingen gereed, waaraan in mei 2018 de bewaartermijnen zijn toegvoegd. Op 17 juli 2018 heeft het college het Register vastgesteld. Het register is openbaar gemaakt door plaatsing op de gemeentelijke website. Begin 2019 zal het register geëvalueerd en geactualiseerd worden.

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 2017 hebben 4 beveiligingsincidenten plaatsgevonden, waarvan er 2 zijn aangemerkt als meldenswaardig datalek. Deze zijn gemeld bij de AP. Van deze gemelde datalekken zijn er 3 meldingen gedaan aan betrokkenen, waarbij in een van de gevallen de gemeente was aan te merken als betrokkene. De veroorzakende partij heeft melding van een datalek aan de gemeente gedaan, waarna de gemeente het datalek gemeld heeft aan de AP. In dit geval betrof het een technisch probleem dat de veroorzakende partij door een aanpassing in de software heeft opgelost.
In 2018 hebben 3 beveiligingsincidenten plaatsgevonden, die ook zijn aangemerkt als meldenswaardig datalek. Deze zijn gemeld bij de AP. Al deze datalekken zijn ook gemeld 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. Er is door betrokkenen in de verslagperiode geen

gebruik gemaakt van de mogelijkheden om hun rechten in te roepen. In 2019 worden de procedures die betrekking hebben op de rechten van burgers in 2019 geactualiseerd.

3.5 Bewaartermijnen

Aan het register is een kolom met bewaartermijnen opgenomen. 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. De besprekingen daarover zijn nog niet afgerond bij afronding van dit jaarverslag.
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 zal hierop toegezien worden, waarbij vooral de eigen mappen van de medewerkers de aandacht verdienen. In veel systemen zit namelijk een signaal dat aangeeft dat de bewaartermijn bijna is verstreken. Wel zal nagegaan worden of dat in ieder systeem zo is of dat daar ook actie op ondernomen moet worden. Momenteel lopen er onderhandelingen met enkele softwareleveranciers.

3.6 Verwerkers en verwerkersovereenkomsten

Bij het aangaan van een samenwerkings- of uitvoeringsovereenkomst komt bij de meeste partijen direct de vraag op of er ook een verwerkersovereenkomst afgesloten moet worden. Het bewustzijn is groot, zodat er nauwelijks discussies zijn waar geen oplossing voor gevonden wordt. Ook worden oude overeenkomsten met regelmaat vernieuwd en geactualiseerd om beter te voldoen aan de AVG.
Het overzicht wordt consequent bijgehouden. In totaal zijn er 52 partijen waarmee een verwerkersovereenkomst afgesloten moet worden. Daarvan zijn er nog 15 in behandeling, waarvan een deel het actualiseren van een verouderde overeenkomst betreft.

3.7 Privacy in het Sociaal Domein

Binnen het Sociaal Domein zijn de aanmeld-/aanvraag- en toestemmingsformulieren tegen het licht gehouden en waar nodig aangepast aan de AVG. Dit is in een werkoverleg met de collega's van het Sociaal Domein nader toegelicht om het belang van het gebruik van de vernieuwde formulieren en de vraag om toestemming voor het delen van gegevens, in gevallen dat dit niet rechtstreeks voortvloeit uit de publiekrechtelijke taak of wettelijke grondslag, te benadrukken.
Daarnaast is er in regionaal verband (Foodvalley) een vernieuwd privacyprotocol en een convenant voor gegevensdeling opgesteld.
De Adviesraad Sociaal Domein heeft de gemeente vanaf het begin van de implementatie van de AVG op de voet gevolgd. Door als FG meerdere keren per jaar aan te sluiten bij een vergadering van de adviesraad 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. In 2018 zijn 429 meldingen gedaan bij IBD.
Ook Scherpenzeel heeft te maken gehad met datalekken. De impact van deze meldingen was laag. De meeste meldingen worden onbewust veroorzaakt door medewerkers. Daarom zijn voorbereidingen gestart om de bewustwording te vergroten. Door complexiteit van systemen neemt het risico gehacked te worden toe. Informatiebeveiliging is niet alleen een ICT aangelegenheid, het is van ons allemaal.

3.9 Data Privacy Impact Assessments

In de periode van september 2017 tot en met april 2018 zijn er een twintigtal PIA's uitgevoerd op de volgende vakgebieden:

- Afvalpassen/Diftar,
- BAG/BGT,
- Basisregistraties personen/Burgerzaken (BRP),
- Belastingen,
- Buitendienst,
- Communicatie,
- Crediteuren,
- Debiteuren,
- Digitale Informatievoorziening (DIV),
- Financiën,
- Jeugdwet (Jw),
- Onderwijs,
- Openbare Orde & Handhaving,
- Participatiewet (PW),
- Personeelszaken (P&O),
- Suwinet,
- Uitkeringenadministratie,
- Veiligheid,
- Vergunningen en
- Wet maatschappelijke ondersteuning (WMO).

Per 1 januari 2019 wordt diftar ingevoerd, zodat de invoering daarvan – conform beleid AP – in de twee kwartalen voorafgaand aan de invoering is gestart. In die periode is er ook getest met de koppeling tussen de afvalpassen, de gegevens van de (ondergrondse) containers en de gegevens van de bewoners van het betreffende adres. In de eerdere periode is de koppeling ongedaan gemaakt vanwege het ontbreken van doelbinding. Zie voor een nadere toelichting hierop de PIA rapportage.

Een nieuwe PIA zal uitgevoerd worden nu de koppeling ter voorbereiding op de invoering van diftar wel toegestaan is.

Voorts zal er een nieuw zaaksysteem aangeschaft en geïmplementeerd worden in 2019, ter vervanging van en uitbreiding op Verseon. Voordat overgegaan wordt tot aanschaf is in december 2018 een PIA uitgevoerd.

De gemeenten Scherpenzeel en Woudenberg werken al een aantal jaren samen op het gebied van belastingen. Per 1 januari 2020 zal de belastingsamenwerking met Veenendaal een feit zijn. Een dienstverleningsovereenkomst en een verwerkersovereenkomst worden in 2019 afgesloten. Ook zal in 2019 een PIA worden uitgevoerd.

3.10 Bewustwording

In mei 2018 is een medewerkersbijeenkomst georganiseerd rondom de in werking treding van de AVG.

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.

4. AANBEVELINGEN

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

Aanbeveling: door met enige regelmaat de medewerkers hierop te attenderen en daarover te informeren door een berichtje op intranet of door het houden van een medewerkersbijeenkomst wordt het bewustzijn hoog gehouden. Een combinatie van de onderwerpen privacy en informatieveiligheid kan dit beeld versterken en het belang verduidelijken.

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 onder de aandacht brengen bij de medewerkers dat deze twee soorten overeenkomsten onlosmakelijk met elkaar verbonden zijn en dat deze voorafgaand aan de levering of uitvoering van de dienst afgesloten moeten zijn. Om dit beter inzichtelijk te maken, kan hiervoor een werkproces ontwikkeld worden door de projectgroep dienstverlening (processen en innovatie).

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. Uit de in 2017-2018 uitgevoerde PIA's is gebleken dat voor een aantal vakgebieden een opschoonactie nodig was, omdat de gegevens en documenten te lang werden bewaard of dat er teveel gegevens en documenten werden bewaard. In de PIA-rapportage d.d. 31 mei 2018 is dit nader toegelicht.

Aanbeveling: jaarlijkse opschoonactie om te controleren of niet te veel gegevens en documenten bewaard worden en dat deze niet te lang bewaard worden. Daarbij moet niet alleen naar de systemen en applicaties gekeken worden, maar dan moet ook aandacht gevraagd worden voor het opschonen van de schaduwbestanden en e-mailboxen.

5. ACTIES 2019

In de hoofdstukken 2 en 3 is aangegeven welke werkzaamheden in de jaren 2017 en 2018 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 2019 worden de onderstaande acties opgepakt, waarover in het Jaarverslag FG 2019 gerapporteerd zal worden.

- Actualiseren register van verwerkingen;
- Procedures rechten van betrokkenen opstellen c.q. actualiseren;
- Evaluatie eerder uitgevoerde PIA's en uitvoeren van nieuwe PIA's voor o.a. Diftar en de belastingsamenwerking;
- 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.
- De Belastingsamenwerking, waarbij verschillende acties uitgevoerd moeten worden zoals het aangaan van een verwerkersovereenkomst en het uitvoeren van een PIA.
- Begin 2019 zal een medewerkersbijeenkomst georganiseerd worden, waarbij de koppeling gelegd wordt tussen gegevensverwerking en informatieveiligheid. Daarbij zal ook ingezoomd worden op de nieuw in december 2018 vastgestelde telewerkregeling, waarin bepaalde werkzaamheden uitgesloten worden voor het werken op een andere locatie dan de vaste werkplek op het gemeentehuis zoals bijvoorbeeld BRP, Suwi en Open Wave. Met alle medewerkers wordt begin 2019 een telewerkovereenkomst afgesloten, waarin deze afspraken vastgelegd zijn in het belang van informatieveiligheid en in het belang van het kunnen waarborgen dat de persoonsgegevens beschermd worden door zorgvuldig en vertrouwelijk om te gaan met deze gegevens.

BIJLAGE WETTELIJK KADER

AVG Algemeen

Op 25 mei 2018 is de Europese Algemene Verordening Gegevensbescherming (AVG) in werking getreden. Deze verordening voor de verwerking van persoonsgegevens ken teen rechtstreekse werking voor de lidstaten en is in de plaats gekomen van de Wet bescherming persoonsgegevens. In de AVG worden de rechten van burgers versterkt en de AVG legt de nadruk op de eigen verantwoordingsplicht van organisaties die persoonsgegevens verwerken. Dit betekent dat organisaties bijvoorbeeld goed moeten vastleggen welke gegevens zij verwerken, met welk doel, hoe lang zij die gegevens bewaren, dat zij de gegevens goed beveiligen en met wie ze gegevens delen. De rechtstreekse werking van de AVG zorgt ervoor dat de regels voor bescherming van persoonsgegevens uniform zijn binnen de Europese Unie.

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

Specifieke wetgevende ontwikkelingen en jurisprudentie

Door de Autoriteit Persoonsgegevens (AP) wordt regelmatig onderzoek gedaan naar de verwerking van persoonsgegevens en de naleving van privacywetgeving in specifieke situaties. Deze onderzoeken worden veelal gepubliceerd en geven meer inzicht in de wijze waarop de AP regelmatig richtsnoeren of uitspraken die relevant kunnen zijn voor een juiste toepassing van privacyregels. In 2018 heeft de AP verschillende onderzoeken gedaan, belangrijke onderzoeken zijn bijvoorbeeld:

- Onderzoek naar de verwerking van BSN in BTW-nummers door de Belastingdienst, juni 2018;
- Onderzoeken gegevensverwerking gemeente Nijmegen en gemeente Zaanstad (over het gebruik van de zelfredzaamheidsmatrix in het sociaal domein), februari 2018.

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

- Guidelines on Data Protection Impact Assessments (wp248rev.01): van belang bij of wanneer een Data Protection Impact Assessment moet worden uitgevoerd;
- Guidelines on Data Protection Officers (DPO'S)(wp243rev.01): over de rol van de Functionaris Gegevensbescherming;
- Guidelines on consent under Regulation 2016/679 (wp259rev.01): over het gebruik van toestemming als rechtmatige grondslag.

Toezichtskader AP: ontwikkelingen en gevolgen

De Autoriteit Persoonsgegevens (AP) heeft in mei 2018 haar toezichtkader voor 2018 en 2019 gepubliceerd. In dit kader geeft de AP haar prioriteiten aan voor de komende periode.

Bevordering naleving van de privacywetgeving

Het belangrijkste doel van het toezicht van de AP is de bevordering van de naleving van de privacywetgeving. Dit doel wil de AP onder meer bereiken door het bieden van 'guidance'. De AP geeft als voorbeelden het geven van voorlichting en advies aan mensen en organisaties, het aanbieden van praktische hulpmiddelen, het aanbieden van een duidelijke normuitleg en het bevorderen van de totstandkoming van Europees gedragen normen.

De AP legt daarnaast de nadruk op de behandeling van klachten, omdat het klachtrecht onder de AVG is versterkt en het behandelen van klachten de naleving van de privacywetgeving kan bevorderen. Hiervoor heeft de AP een Informatie- en Meldpunt Privacy ingesteld. De AP neemt klachten in behandeling die wijzen op een mogelijke inbreuk op de verwerking van persoonsgegevens van mensen en wil betrokkenen hiermee versterken in hun rechten.

Controle op de naleving van de AVG

De verantwoordingsplichten in de AVG dwingen organisaties aan te tonen dat zij voldoen aan de AVG. Om vast te stellen dat aan de verantwoordingsplichten van de AVG is voldaan, wordt in de verschillende sectoren de naleving van één van deze verplichtingen gecontroleerd. Daarbij kan bijvoorbeeld gedacht worden aan de controle of een verplichte Functionaris gegevensbescherming is aangesteld, of ere en register van verwerkingen is en een register wordt bijgehouden van beveiligingsincidenten en de genomen maatregelen. Het op orde hebben van de verantwoordingsplichten is volgens de AP een geode indicatie van de mate waarin serieus werk is gemaakt van de implementatie van de AVG en dat is nagedacht over belangrijke onderdelen uit de AVG (zoals grondslagen, doelbinding en beveiliging).

Risicogericht toezicht

De AP geeft in haar toezichtkader aan dat zij een risicogerichte aanpak gaat hanteren en daarbij extra oog heeft voor mogelijke inbreuken op de bescherming van persoonsgegevens waarbij grote groepen mensen kunnen worden geraakt. Daarbij

richt zij zich de komende periode in het bijzonder op de overhead, de zorg en bedrijven die handelen in persoonsgegevens. Voor de overhead geldt dat de AP extra focus gaat leggen op zowel de beveiliging van persoonsgegevens als de vraag of de verwerking van de persoonsgegevens is gebaseerd op de juiste grondslag. De AP gaat daarvoor bijvoorbeeld controles uitvoeren op de naleving van de verplichtingen om ene register van verwerkingen op te stellen, de verplichting een Functionaris gegevensbescherming (FG) aan te stellen (deze controle is voor gemeenten reeds uitgevoerd in 2018), alsmede de wijze waarop de organisatie de FG positioneert en hem in staat stelt de taken en verplichtingen uit te voeren die hij op grond van de AVG heeft.

Datalekken
De AVG stelt een aantal nieuwe eisen aan de meldplicht datalekken. Organisaties moeten bijvoorbeeld alle datalekken documenteren en niet alleen de gemelde datalekken. Zij moeten een register van datalekken bijhouden. De AP geeft het komende jaar extra aandacht aan niet-gemelde datalekken en datalekken die (mede) zijn veroorzaakt door ernstige tekortkomingen in de beveiliging.