Gemeente Huizen

JAARVERSLAG 2020

FUNCTIONARIS GEGEVENSBESCHERMING

Mei 2021

Inhoudsopgave:

1 Inleiding en terugblik

Het afgelopen jaar is mede door de uitbraak van de COVID-19 pandemie en de hieruit voortkomende beperkende maatregelen een heel ander jaar geworden dan van te voren ingeschat.
Vanaf half maart 2020 was het dringende verzoek van de directie om zoveel mogelijk thuis te werken. Uitzonderingen vormden onder andere de functies waarvoor het werken op kantoor noodzakelijk was. Ook was het gemeentehuis langere tijd slechts beperkt geopend en werd het bedrijfsrestaurant gesloten. Gelukkig bleek onze organisatie snel om te kunnen schakelen naar het vanaf locatie (veelal de thuiswerkplek) werken en het via de applicatie Microsoft Teams online voeren van overleg.

De geschetste bijzondere omstandigheden zorgden er voor dat de plannen tot het verder investeren in de ontwikkeling en vergroting van de bewustwording van medewerkers op het vlak van privacybeheer en informatieveiligheid op een laag pitje werden gezet. Wel bleef het werken aan vergroting van de eigen (vak)kennis en deskundigheid, weliswaar in wat beperktere vorm, mogelijk. Met 3 collega's uit het sociaal domein werd, toen dit nog mogelijk was, in de regio deelgenomen aan een cursus AVG/privacy in het sociaal domein. Verder werden enkele webinars gevolgd over onder meer de digitale toekomst van het Centrum informatiebeveiliging en privacybescherming (CIP), Keten-DPIA als privacy-by-design instrument voor samenwerkingsverbanden en het optimaal thuiswerken met teams. Daarnaast werd een online training AVG Privacy Awareness gevolgd.
In de landelijke week van de privacy werd in verschillende webinars aandacht besteed aan onderwerpen als privacy-awareness voor en door bestuurders, pré-DPIA's, algoritmes en AI, Smart Cities: efficiency, veiligheid en privacy en er werd gesproken met een inspecteur van de Autoriteit Persoonsgegevens over diens werk en ervaringen.

In bijgevoegd jaarverslag vindt u op hoofdlijnen de weerslag van de verrichtte werkzaamheden, de bevindingen over het afgelopen jaar en aanbevelingen voor het komende jaar.

2 Aandachtspunten uitvoering AVG

Ondanks de hierboven geschetste situatie bleek in de afgelopen maanden dat het informatieveiligheids- en privacybewustzijn hieronder niet heeft geleden. Bij de aanschaf van nieuwe applicaties en de ontwikkeling van werkprocessen was er voldoende oog voor de privacy van inwoners en overige relaties en het moeten voldoen aan de wettelijke bepalingen.

In 2019 was al zichtbaar dat inwoners meer kennis hebben van de privacywetgeving en de impact hiervan op hun persoonlijk leven. Langzaam maar zeker wordt door inwoners vaker een beroep gedaan op hun rechten in de privacywetgeving. Ook het afgelopen jaar werd opnieuw aandacht besteed aan drie (belangrijke) rechten voor betrokkenen: toestemming aan betrokkenen vragen om hun persoonsgegevens te verwerken en de mogelijkheid deze ook weer in te trekken, vergetelheid en dataportabiliteit (overdraagbaarheid van gegevens).

Onverkort blijft het binnen de organisatie wel nodig aandacht te besteden aan het alleen verzamelen en verwerken van persoonsgegevens voor van te voren bestemde doelen. En dit dan alleen voor zolang als dat voor dat doel nodig is.

2a. Sturing en monitoring
De afdelingshoofden zijn verantwoordelijk voor de zorgvuldige verwerking van persoonsgegevens die binnen hun afdeling plaatsvinden. Ondergetekende houdt als functionaris gegevensbescherming (FG) toezicht op de toepassing en naleving van de Algemene verordening gegevensbescherming (AVG) binnen de organisatie en rapporteert daarover als dat nodig is rechtstreeks aan directie en bestuur. Bij de uitvoering van deze werkzaamheden bekleedt de FG een onafhankelijke positie en ontvangt deze geen instructies over de uitvoering van het bijbehorende takenpakket.

3 Rol en taken functionaris voor de gegevensbescherming (FG)

Naast functionaris voor de gegevensbescherming (FG) voor de gemeente Huizen is ondergetekende ook de FG voor de Rekenkamercommissie. Voor beide functies staat ondergetekende ingeschreven bij de toezichthoudende autoriteit, de Autoriteit Persoonsgegevens.
De rol en taken van de FG zijn in het afgelopen jaar niet veranderd.

3a. Rol en taken FG
Het takenpakket van de FG omvat onverminderd de volgende onderdelen:

- Het houden van toezicht op de toepassing en naleving van de AVG en het gemeentelijk beleid betreffende de bescherming van persoonsgegevens.
- De verantwoordelijkheid voor de opstelling en actualisering van het register van gegevens-verwerkingen.
- Het verstrekken van advies, informatie en voorlichting over de verwerking van persoons-gegevens aan de ambtelijke organisatie en het bestuur.
- Het fungeren als in- en extern aanspreekpunt over de AVG en de bescherming van de persoonlijke levenssfeer bij vragen, klachten en ingediende verzoeken met daarbij de coördinatie van de tijdige afhandeling hiervan.
- Het optreden als de gemeentelijk contactpersoon voor de Autoriteit Persoonsgegevens.
- Het houden van toezicht op en adviseren over de uitvoering van de gegevensbescherming effectbeoordelingen (=Privacy impact analyses).
- Rapporteren aan directie en college over het gevoerde beleid, de toepassing en naleving van de AVG en opgetreden incidenten met betrekking tot gegevensverwerkingen.

4 Uitvoering taken FG

4a. Toezicht op toepassing en naleving AVG en het gemeentelijk beleid betreffende de bescherming van persoonsgegevens
Het toezicht op de toepassing en naleving van de AVG wordt gecombineerd met de uitvoering van adviesverzoeken bij onder andere de ontwikkeling van nieuw beleid, werkprocessen en hierbij behorende formulieren binnen de ambtelijke organisatie.
18 maal werd een toetsing op het 'AVG proof' zijn van nieuw beleid, werkprocessen en formulieren uitgevoerd. (In 2019 gebeurde dit 14 maal.)
Hierdoor konden de vakafdelingen de door ondergetekende geplaatste kanttekeningen en suggesties tot aanpassing van de documenten in een vroegtijdig stadium verwerken zodat voldaan wordt aan de wettelijke bepalingen. Dit leidde niet tot oponthoud in de vaststelling en invoering van genoemde documenten en werkprocessen.

4b. Register gegevensverwerkingen
In 2018 werd in nauw overleg met en met behulp van de vakafdelingen een register van gegevens-verwerkingen ingericht en opgesteld. Het register werd op 23 mei 2018 vastgesteld en gepubliceerd op de gemeentelijke website. Daarnaast werd een papieren zichtexemplaar op een centrale plaats in de centrale hal van het gemeentehuis ter inzage gelegd.
In dit register is vastgelegd welke soorten persoonsgegevens er in de verschillende werkprocessen binnen de ambtelijke organisatie worden vastgelegd en verwerkt, wat de rechtmatige grondslag hiervoor is, aan wie deze gegevens worden verstrekt en hoe lang deze gegevens mogen worden bewaard.
Dit register is verplicht en wordt gezien als verantwoordingsinstrument voor de wijze van omgang met de AVG. Het was de bedoeling dat het register van verwerkingen het afgelopen jaar zou worden gekoppeld aan het zaaksysteem waarna dit tevens zou worden geactualiseerd.
Mede door een hoge werkdruk bij de betreffende medewerkers en andere prioriteiten binnen de vakafdeling, is de actualisatie van het in gebruik zijnde zaaksysteem later op de agenda geplaatst en kon nog niet tot koppeling en actualisatie van het register van verwerkingen worden overgegaan.

Na de zo gewenste koppeling zullen meldingen over wijzigingen in wet- en regelgeving per omgaande – en geautomatiseerd- worden verwerkt in dit register.

4c. Verwerkersovereenkomsten
Gemeenten zijn op basis van de AVG wettelijk verplicht een verwerkersovereenkomst (VWO) af te sluiten met alle opdrachtnemers die namens hen persoonsgegevens verwerken. Tijdens de algemene ledenvergadering van de Vereniging van Nederlandse Gemeenten werd op 5 juni 2019 besloten om de door de Informatiebeveiligingsdienst (IBD) opgestelde standaard verwerkersovereenkomst per 1 januari 2020 verbindend te verklaren voor alle Nederlandse gemeenten.
Met de vaststelling van deze standaard VWO hebben alle gemeenten gekozen voor uniforme afspraken over het verwerken van persoonsgegevens. Deze standaard is in overleg met landelijke leveranciers ontwikkeld door én voor gemeenten. Met deze overeenkomst wordt uitgesloten dat de andere partij de persoonsgegevens voor eigen doelen mag verwerken. In de verwerkings-overeenkomst worden onderwerp, duur, aard en doel van de verwerking vastgelegd met daarbij de soort persoonsgegevens en de getroffen technische en organisatorische maatregelen om de verwerkingen veilig te stellen en de persoonsgegevens en privacy van betrokkenen te beschermen.

Ook in het afgelopen kalenderjaar werden op verzoek van de intern verantwoordelijken binnen de vakafdelingen de ontvangen concept-verwerkersovereenkomsten getoetst op compleetheid en correctheid. Aan de hand van de geplaatste opmerkingen en verstrekte adviezen droegen de vakafdelingen zorg voor de aanpassing en ondertekening van deze verwerkersovereenkomsten door de betreffende organisaties.

Het afgelopen jaar werden 9 verwerkersovereenkomsten ondertekend en geregistreerd. Dit tegenover 15 in 2019 en 20 in 2018. Begin dit jaar waren er nog 4 verwerkersovereenkomst in bewerking.

Ondergetekende blijft de verantwoordelijken aanspreken op het zorgdragen voor de opstelling en ondertekening van nog ontbrekende en/of nieuwe verwerkersovereenkomsten. De verwachting is dat er ook het komend jaar nog enkele nieuwe verwerkersovereenkomsten moeten worden opgesteld. Na controle door ondergetekende zullen deze overeenkomsten worden ondertekend en geregistreerd.

4d. Advisering, informatieverstrekking en voorlichting over AVG
Het afgelopen jaar werd door medewerkers vaak gevraagd om advies over allerlei aangelegenheden waarbij verwerking van persoonsgegevens aan de orde was.
In totaal werden 92 adviezen over een breed scala aan onderwerpen verstrekt. Dit onder andere over anonimisering van besluiten en andere documenten, dataportabiliteit, informatie-uitwisseling met (keten)partners, binnengemeentelijke gegevensuitwisseling en de interpretatie van bepaalde protocollen op de uitleg van de privacy in relatie tot de AVG. Verder werd advies verstrekt bij vragen over het 'AVG proof' inrichten van werkprocessen, het ontwikkelen van beleid en werkinstructies.

5 Bewustwordingsactiviteiten

Na het eerder in gang gezette bewustwordingstraject werd 2020 een jaar waarin de geplande bewustwordingscampagne op een laag pitje moest worden gezet. Dit enerzijds door de geschetste uitbraak van het Covid -19 virus, de geschetste beperkende maatregelen en de hoge werkdruk binnen vrijwel de gehele organisatie. Het vele op locatie/online werken maakten een verdere uitrol van het bewustwordingstraject lastig en minder gepast gezien de omstandigheden.

Tijdens de "week van de privacy' werd het personeel via een artikeltje en flyer op het intranet nog eens voorgelicht over een aantal belangrijke onderwerpen met betrekking tot de privacy in relatie tot de AVG. Bij persoonlijke consultatie werden medewerkers tevens gericht voorgelicht over privacy in relatie tot de AVG.

5a. Rondgang 'clean desk'
Nadat er in de jaren 2018 en 2019 samen met de toenmalige projectleider BBP een rondgang "clean desk' door het gemeentehuis werd uitgevoerd werd deze actie door de COVID -19 pandemie en de hieruit voortkomende beperkende maatregelen het afgelopen jaar niet uitgevoerd.
Lange tijd was er sprake van een minimale bezetting in het gemeentehuis. Werkte het grootste deel van het personeel thuis of elders op locatie en werd het online werken gemeengoed.
In het laatste deel van het jaar nam de bezetting iets toe. Desondanks dat is het de vraag of een dergelijke rondgang het komende jaar wel nodig en nuttig zal zijn. De verwachting is immers dat het thuis en elders op locatie online werken veel meer ingeburgerd is geraakt en deze werkwijze waarschijnlijk deels structureel zal worden.
Het afgelopen jaar is niet gebleken dat er bij het thuis of elders op locatie werken minder zorgvuldig is omgegaan met persoonsgegevens. Ook is er geen toename gezien van beveiligingsincidenten.
Dit wil niet zeggen dat er geen documenten met gevoelige en vertrouwelijke informatie op gemakkelijk toegankelijke plaatsen hebben gelegen danwel dat er af en toe minder zorgvuldig is omgegaan met datadragers, zoals USB sticks, mobiele telefoons en laptops en/of deze altijd veilig werden opgeborgen bij het beëindigen van de werkdag.

6 Datalekken

Sinds 1 januari 2016 is de Wet meldplicht datalekken in werking. Een datalek is een inbreuk op de beveiliging waarbij een kans bestaat dat deze inbreuk ernstige gevolgen heeft voor de bescherming van de persoonsgegevens. Als er sprake is van een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, de wijziging of de ongeoorloofde verstrekking van persoonsgegevens dan wel ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens en de persoonlijke levenssfeer van betrokkenen hierdoor is geschaad, moet een dergelijk datalek binnen 72 uur na ontdekking hiervan worden gemeld aan de toezichthoudend autoriteit, de Autoriteit Persoonsgegevens. Ondergetekende is verantwoordelijk voor de melding aan de Autoriteit Persoonsgegevens. Bij alle andere datalekken volstaat de melding aan ondergetekende.

Het merendeel van de meldingen over inbreuken op de beveiliging worden via het gemeentelijk self service portal (ServicePunt) gemeld. Een enkele keer wordt een dergelijke melding via e-mail of een telefonisch onderhoud rechtstreeks aan ondergetekende gemeld.
Afhankelijk van de soort inbreuk wordt de melding hiervan per omgaande doorgezet naar het verantwoordelijke afdelingshoofd en/of vindt hierover eerst overleg plaats met de chief information security officer (de CISO); in onze organisatie is dat de teamleider van het team Informatiemanagement.
In alle gevallen worden door de organisatie zo snel als mogelijk maatregelen getroffen om het datalek te beëindigen en te voorkomen dat soortgelijke incidenten in de toekomst opnieuw plaatsvinden.

Daar waar is geconstateerd dat sprake is van een datalek, documenteert ondergetekende de gemelde incidenten en worden deze met het oog op de op grond van de AVG bestaande verantwoordingsplicht opgenomen in het interne 'register datalekken'.

In die situaties waarbij een datalek ontstaat bij een door de gemeente voor de uitvoering van bepaalde werkzaamheden ingeschakelde externe organisatie die als verwerker van persoonsgegevens optreedt, dient deze organisatie een beveiligingsincident zo snel mogelijk te melden aan de betreffende verantwoordelijke binnen de gemeente. Voor de afhandeling hiervan geldt eenzelfde procedure als bij de intern ontstane beveiligingsincidenten/datalekken. De betreffende organisatie dient het datalek zelf te melden aan de Autoriteit Persoonsgegevens.

6a. Register datalekken
Sinds 2018 wordt een register datalekken bijgehouden. In het register staat een beschrijving van de inbreuk, de mogelijke gevolgen hiervan, de getroffen corrigerende maatregelen en of hiervan een melding is gedaan aan de Autoriteit Persoonsgegevens en betrokkenen.

Dit register is enerzijds van belang voor het inzicht in het aantal en de soorten datalekken die er zijn geweest binnen de organisatie, maar dient ook als controlemiddel voor de Autoriteit Persoonsgegevens voor de toetsing of de organisatie aan haar meldplicht heeft voldaan.

In 2020 werden 9 datalekken gemeld (tegenover 12 in 2019 en 8 in 2018).
Van genoemde datalekken in 2020 werden 2 datalekken gemeld aan de Autoriteit Persoonsgegevens (tegenover 1 in 2019 en 2 in 2018).

- Bij het 1e aan de Autoriteit Persoonsgegevens gemelde datalek werd door een menselijke fout van een bestand met een grote hoeveelheid brieven een printopdracht gegeven waarbij niet werd gezien dat de optie tweezijdig printen aanstond. Hierdoor ontvingen de geadresseerden een brief met op de achterzijde een brief bestemd voor een andere geadresseerde. Door het betreffende hoofd van de afdeling waarin dit datalek plaatsvond werd een excuusbrief verstuurd waarbij tegelijkertijd werd verzocht de eerder ontvangen brief met daarin ten onrechte vermelde persoonsgegevens te vernietigen. Om dergelijke fouten in de toekomst te voorkomen werden werkafspraken gemaakt over een extra controle voor verzending van dergelijke grote hoeveelheden brieven.
- Het 2e gemelde datalek ontstond eveneens door een menselijke fout waarvoor geen speciale technische of organisatorische maatregelen zijn getroffen. Het betrof hier een situatie waarbij bij de opstelling van een e-mailbericht aan een aantal inwoners en externe organisaties de e-mailadressen niet in een BCC-regel, maar in een CC-regel werden geplaatst en daardoor bekend werden bij de overige ontvangers van dit bericht. Na ontdekking hiervan werd per omgaande een excuus e-mail gestuurd aan de geadresseerde inwoners en externe organisaties. Dit met het verzoek de betreffende e-mailadressen van de overige geadresseerden niet te gebruiken en deze te verwijderen.
- 1 datalek betrof de ontvangst van een melding bij onze ICT leverancier dat een zogenaamde 'inbox rule' was ingesteld op een e-mailbox van een medewerker waardoor alle aan deze medewerker verstuurde e-mailberichten automatisch zouden worden doorgestuurd naar een ander extern e-mailadres. Op het moment dat de ICT leverancier dit zogenaamde 'vals spel' ontdekte werd de betreffende regel per omgaande verwijderd. De betreffende medewerker werd verzocht per direct diens wachtwoord aan te passen en een 'defender antivirus scan' op de in gebruik zijnde laptop werd gestart. Nader onderzoek leerde dat er slechts twee e-mails werden doorgestuurd naar het vreemde externe e-mailadres. Nader onderzoek leerde dat er verder geen activiteit was geweest op het account van de medewerker. Na dit datalek is er bij de ICT dienstverlener een wijziging doorgevoerd waardoor het door laten sturen (forwarden) naar externe e-mailadressen onmogelijk is geworden. Alle betrokken personen waarbij het e-mailbericht op het onbekende e-mailaccount terecht waren gekomen werden geïnformeerd.
- Bij 1 datalek was sprake van onjuiste adressering van brieven aan enkele medewerkers door het niet tijdig doorgeven van adreswijzigingen. Medewerkers werden geattendeerd op het tijdig doorgeven van mutaties waaronder adreswijzigingen ter voorkoming van nieuwe datalekken.
- 1 datalek ontstond door het vermelden van een foutief/niet bestaand huisnummer in een brief aan een inwoner. De brief kwam niet aan/werd niet geretourneerd. Na een telefonische melding van de inwoner over het uitblijven van een besluit op en verzoek werd dit incident ontdekt en werd per omgaande excuses aangeboden. Vervolgens werd de betreffende brief naar het juiste huisnummer verstuurd.
- 1 datalek betrof het achterlaten van een lijst met namen van personen en telefoonnummers bij een printer, welke lijst door ondergetekende werd aangetroffen. De betreffende medewerkers is aangesproken op diens handelwijze.
- 1 datalek betrof het in een aan een inwoner gerichte e-mail abusievelijk meesturen van een e-mailadres en telefoonnummer van een andere inwoner. Na ontdekking werd een excuus e-mail verstuurd aan de betreffende inwoner waarbij werd verzocht de eerder gestuurde e-mail te vernietigen en deze als niet gezonden te beschouwen. Ook hier betrof het een menselijke fout waarvoor geen speciale technische of organisatorische maatregelen zijn getroffen.

- 1 datalek ontstond door verlies van een aantekeningen blok met de naam van de medewerker en gegevens over inwoners + enkele BDS nummers en inloggegevens van een studieaccount bij een opleidingsinstituut. Het in of bij de werkplek zoek geraakte aantekeningenblok werd niet terug gevonden. Onderzoek door de ICT dienstverlener leerde dat er geen ongeregeldheden in het betreffende e-mailaccount plaatsvonden (dus er werden ook geen externe forwards aangetroffen). Ditzelfde gold voor het studie-account. Met de betreffende medewerker werd gesproken over de ontstane situatie.
- Tot slot 1 datalek ontstond door een ransomware aanval bij een extern opleidingsinstituut waardoor oude gegevens (zoals mogelijk een niet meer in gebruik zijnd e-mailaccount van een vertrokken medewerker) bij hackers terecht waren gekomen. Op het in gebruik zijnde digitale platform binnen de gemeente staan geen persoonsgegevens zodat dit datalek geen consequenties heeft gehad.

7 Coördinatie indienen verzoeken door betrokkenen

Ondergetekende is het eerste aanspreekpunt bij vragen of klachten van en de indiening van verzoeken door betrokkenen over de verwerking van hun persoonsgegevens en de bescherming van de persoonlijke levenssfeer/privacy (conform de artikelen 15 tot en met 18 en 20 + 21 van de AVG). Bij ontvangst van dergelijke verzoeken beoordeelt ondergetekende welk soort verzoek het betreft, of betrokkene zich gelegitimeerd heeft en diens identiteit kon worden vastgesteld en waar behandeling van dit verzoek dient plaats te vinden. Vervolgens vindt doorzending naar de betreffende vakafdelingen plaats.

7a. Register ingediende verzoeken betrokkenen in kader AVG
Voor het zicht op het aantal ingediende verzoeken houdt ondergetekende een 'register ingediende verzoeken betrokkenen in kader AVG' bij. In dit register staan de datum van het verzoek, het onderwerp, het soort verzoek, de handelwijze en de ondernomen acties ter afhandeling van het verzoek.

Er werden in 2020 in totaal 17 verzoeken ontvangen tegenover 8 in 2019 en 4 in 2018.

- Er werden 10 verzoeken om inzage in persoonsgegevens ontvangen. 8 verzoeken werden toegekend en de gevraagde documenten werden toegestuurd.
- Er werd 1 verzoek dataportabiliteit ontvangen, welk verzoek werd ingewilligd waarna de betreffende dossiers werden overgedragen aan een andere gemeente.
- Er werden 2 verzoeken tot verwijdering/wissing van persoonsgegevens ontvangen. 1 verzoek werd gedeeltelijk toegekend; het andere verzoek werd afgewezen maar betrokkene werd geïnformeerd over het feit dat de betreffende documenten/dossiers nadat de bewaartermijnen zijn verstreken zullen worden verwijderd.
- Er werd 1 verzoek bezwaar tegen verwerking van persoonsgegevens ingediend; het verzoek werden ingewilligd en de betreffende persoonsgegevens werden verwijderd.
- Er 1 verzoek bezwaar gebruikmaking persoonsgegevens voor een ander doel dan waarvoor deze waren verstrekt. Excuses hiervoor werden aangeboden en geaccepteerd.
- Er werd 1 verzoek intrekking toestemming gebruikmaking persoonsgegevens ingediend. In overleg met betrokkene werd aan de partijen die de betreffende persoonsgegevens ontvingen verzocht de ontvangen persoonsgegevens niet langer te gebruiken.
- Er werd 1 verzoek ingediend de persoonsgegevens niet te verstrekken aan andere organisaties dan de overheid. Dit verzoek valt niet onder de AVG. Na overleg met het vakteam werd aan betrokkene de te volgen procedure om diens verzoek gehonoreerd te krijgen uitgelegd.

8 Samenwerking CISO/team Informatiemanagement (iTeam)

8a. Overleg informatieveiligheid en privacybeheer
Ondergetekende heeft voor het onderdeel informatieveiligheid/-beveiliging en privacy periodiek overleg met de chief information security officer (CISO)/teamleider team Informatiemanagement (iTeam) en de informatie-architect/Ensia coördinator van dit team. In dit overleg worden de stand van zaken, risico's en incidenten op genoemde gebieden besproken.

De CISO is de intern verantwoordelijke voor de ontwikkeling, invoering en naleving van het informatie-veiligheidsbeleid en de opstelling en uitvoering van informatiebeveiligingsplannen. Hij draagt zorg voor een samenhangend pakket van maatregelen ter waarborging van de vertrouwelijkheid, integriteit en beschikbaarheid van de informatie binnen de organisatie. Dit op basis van de algemeen aanvaarde standaard de BIG (Baseline Informatiebeveiliging Nederlandse Gemeenten).

Met betrekking tot het verantwoordingsstelsel voor informatieveiligheid is op basis van de Baseline Informatiebeveiliging Overheid (BIO), die per 1 januari 2020 de baseline informatieveiligheid voor Gemeente verving (BIG), een verantwoordingsproces opgesteld, zijnde Ensia (Eenduidige Normatiek Single Information Audit).
Ensia heeft tot doel het verantwoordingsproces over informatieveiligheid bij gemeenten verder te professionaliseren door het toezicht te bundelen en aan te sluiten op de gemeentelijke planning & controlcyclus. De Ensia coördinator zorgt dat het verantwoordingsproces over informatieveiligheid bij de organisatie conform de eisen en tijdig wordt doorlopen.

8b. Overleg beveiligingsadviescommissie
De CISO leidt projecten die als doel hebben beveiligingsmaatregelen te implementeren of de kwaliteit van de beveiliging op langere termijn te handhaven en/of verbeteren. Binnen de organisatie wordt onder andere gewerkt met een beveiligingsadviescommissie (BAC), waarvan ondergetekende ook deel uitmaakt. In dit periodieke overleg worden alle aangelegenheden met betrekking tot de informatieveiligheid en –beveiliging en privacy besproken.

9 Oordeel over 2020 en aanbevelingen

Het privacy- en informatieveiligheidsbewustzijn binnen de organisatie is het afgelopen jaar op een acceptabel niveau gebleven. Zowel leidinggevenden als medewerkers zijn zich vrij goed bewust van de noodzaak van bescherming van persoonsgegevens en weten ondergetekende te vinden bij vragen over verwerking van persoonsgegevens en de invloed hiervan op de persoonlijke levenssfeer van betrokkenen.
De organisatie voldoet aan de eisen die in de AVG zijn neergelegd. Aandacht binnen alle afdelingen blijft ook het komende jaar van belang voor de toetsing van de eigen werkprocessen en in gebruik zijnde formulieren op het 'privacyproof' zijn.

Verder is het zaak dat de afdelingen zorgen voor het verkrijgen van nog ontbrekende verwerkers-overeenkomsten voor die applicaties waarin persoonsgegevens worden verwerkt.

Een verdere doorontwikkeling van het privacy- en informatieveiligheidsbewustzijn geeft geen 100% zekerheid dat inbreuken op de beveiliging waardoor een datalek kan ontstaan worden voorkomen, danwel alle incidenten (tijdig) worden gemeld aan de CISO of ondergetekende.
Ditzelfde geldt voor het indienen van verzoeken door betrokkenen om hun rechten zoals opgenomen in de AVG te kunnen uitoefenen.
In de overleggen met leidinggevenden en medewerkers wordt men hierop geattendeerd.

10 Vooruitblik speerpunten werkzaamheden FG 2021

Naast de toezichthoudende, adviserende, informerende en voorlichtende rol zijn de speerpunten voor 2021:

- De koppeling van het huidige register van gegevensverwerkingen met het in gebruik zijnde zaaksysteem Decos Join, de applicatie iNavigator. Door andere prioriteiten bij de betreffende projectleider heeft dit onderdeel vertraging opgelopen.
- Leveren van een bijdrage aan het project 'invoering van het privacy en informatieveiligheid framework', het Information Security Management Systeem (ISMS) van ReCourse, waarin alle eisen vanuit de BIO, Ensia en AVG eenvoudig zijn vertaald en gemakkelijk toegankelijk zijn voor alle organisatorische rollen en verantwoordelijken. Dit systeem maakt gebruik van een PDCA-cyclus (Plannen, Doen, Controleren en Actualiseren) gebaseerd op wet- en regelgeving. Ook dit onderdeel is in 2020 niet gerealiseerd; de verwachting is dat dit in 2021 zal worden opgepakt.
- Het initiëren van de uitvoering van gegevensbescherming effectbeoordelingen, de zogenaamde data protection impact analyse (DPIA), in (nieuwe) werkprocessen waarin sprake is van risicovolle verwerkingen van persoonsgegevens. Door de hoge werkdruk en andere prioriteiten binnen de vakafdelingen zijn er tot en met 2020 nog geen DPIA's uitgevoerd. Binnen het sociaal domein wordt inmiddels gewerkt aan de opstelling van een plan van aanpak om een 8-tal DPIA's uit te voeren. Het voornemen is een kerngroep samen te stellen die de betreffende werkprocessen zal beoordelen. Ondergetekende zal hierbij als toezichthouder AVG worden betrokken.

Huizen, 25 mei 2021
De functionaris gegevensbescherming