VIJFHEERENLANDEN

JAARRAPPORTAGE 2019 GEGEVENSBESCHERMING

Opgesteld door de Functionaris Gegevensbescherming

Samenvatting

De gemeenten Leerdam, Vianen en Zederik zijn per 1 januari 2019 gefuseerd in de gemeente Vijfheerenlanden (voor de leesbaarheid zal in deze rapportage worden gesproken over 'de gemeente'). De bestuursorganen van de gemeente zijn verantwoordelijk voor de verwerkingen van persoonsgegevens in onze gemeente. Voor het merendeel gaat het om het college van Burgemeester en Wethouders. De gemeenteraad is zelf verantwoordelijk voor de verwerkingen binnen de gemeenteraad en de griffie. Dit brengt verplichtingen met zich mee. In deze jaarrapportage staat beschreven welke acties en maatregelen de gemeente in 2019 heeft genomen om de doelstellingen en beginselen uit de AVG te behalen en te waarborgen. Ook bevat dit document aandachtspunten en actiepunten voor het jaar 2020. Adequaat omgaan met persoonsgegevens is een blijvend proces en zal dan ook aandacht blijven vergen van zowel bestuur, management als medewerkers.

In 2019 heeft de gemeente veel werk verzet op het gebied van gegevensbescherming. Na het halverwege het jaar aanstellen van een privacybeheerder is onder andere een procedure voor het melden en afhandelen van beveiligingsincidenten opgesteld, gestart met het updaten van het register van verwerkingen en de hierbij behorende controle van verwerkingen en benodigde afspraken met bijvoorbeeld verwerkers en gewerkt aan bewustwording door middel van presentaties en berichten op intranet.

Inhoudsopgave

Inleiding

De gemeente is zich steeds meer bewust van het belang van het beschermen van persoonsgegevens van haar inwoners. We verwerken immers bij de uitoefening van onze taken veel (gevoelige) gegevens van veel (kwetsbare) inwoners in veel verschillende domeinen. Daarnaast staan persoonsgegevens van andere burgers, medewerkers, externen en zakenrelaties op de radar.

In de AVG wordt het wettelijk kader beschreven voor verwerken van persoonsgegevens. Zo dient de gemeente transparant te zijn welke persoonsgegevens zij verwerkt en voor welk doel en welke grondslag. Tijdens de levensduur van persoonsgegevens moet de gemeente ze goed beveiligen, mogen we ze niet zomaar voor een ander doel verwerken en moeten we ze na afloop vernietigen of anonimiseren. Daarnaast heeft de gemeente ook te maken met tal van privacyregels in sectorspecifieke wetgeving. Dit alles heeft gevolgen voor de inrichting van processen en systemen in en van de gemeente.

Onder verantwoordelijkheid van zowel het college van Burgemeester en Wethouders als de gemeenteraad vindt een groot aantal verwerkingen van persoonsgegevens plaats. Daar vindt extern en intern toezicht op plaats. De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de privacyregels in Nederland. Daarnaast dient een gemeente te beschikken over een interne toezichthouder: de Functionaris Gegevensbescherming (FG). De gemeente heeft mevrouw mr. L. de Keijzer-Krens CIPP/E CIPM aangesteld als FG.

De FG ziet erop toe dat de AVG intern wordt nageleefd. Het college dient erop toe te zien dat de FG naar behoren en tijdig wordt betrokken bij alle gelegenheden die verband houden met de bescherming van persoonsgegevens. Daarnaast dient de FG ondersteund te worden door haar toegang te verschaffen tot persoonsgegevens en verwerkingen daarvan en haar de benodigde middelen ter beschikking te stellen voor het vervullen van de taak en het in standhouden van haar deskundigheid. De uitvoerende taken liggen bij de privacybeheerder.

De FG brengt jaarlijks een verslag uit aan de verwerkingsverantwoordelijke van haar werkzaamheden en bevindingen en hierin doet zij naar aanleiding daarvan aanbevelingen. Dit jaarverslag is bedoeld voor zowel de directie als de drie bestuursorganen van de gemeente.

Leeswijzer

Deze jaarrapportage bestaat uit twee onderdelen. In het eerste deel wordt teruggekeken naar het jaar 2019. Wat heeft de gemeente bereikt op het gebied van gegevens-bescherming? Welke maatregelen zijn genomen om te voldoen aan de AVG? In het tweede deel worden aanbevelingen gedaan om gegevensbescherming en privacy in het jaar 2020 naar een nog hoger niveau te tillen. Hierbij wordt waar nodig tevens aandacht geschonken aan de technische en organisatorische middelen die nodig zijn om dit hogere niveau te bereiken.

De thema's die in dit rapport worden genoemd zijn afkomstig uit het AVG borgingsproduct van de Informatiebeveiligingsdienst (IBD).[1] In het borgingsproduct worden thema's, criteria en maatregelen omschreven die de AVG vertalen naar een kwaliteitscyclus voor gegevensbescherming en privacy voor gemeentelijke processen. In bijlage 1 staat per thema aangegeven in hoeverre de gemeente de criteria reeds heeft geïmplementeerd.

[1] Zie het document 'Criteria borging AVG / Borgingsproduct gegevensbescherming in de gemeentelijke organisatie', link.

Deel 1. Terugblik op 2019

Het jaar 2019 stond in het teken van verdere implementaties en verbeteringen na het eerste AVG-jaar. In dit deel van de rapportage wordt teruggeblikt op wat de gemeente in 2019 heeft bereikt en welke werkzaamheden zijn verricht.

1. Het privacybeleid

Het privacybeleid is een kader waarin de gemeente aangeeft aan welke principes zij zich houdt bij de verwerking van persoonsgegevens. Het laat zien hoe de gemeente omgaat met persoonsgegevens en welke maatregelen zij treft om te voldoen aan de relevante wet- en regelgeving.

In 2018 is een extern privacybeleid gepubliceerd en is een privacyverklaring op de website opgenomen. In 2019 is een start gemaakt met een meer intern privacybeleid.

2. Processen

De verwerkingen van persoonsgegevens van de gemeente dienen te voldoen aan de AVG. Dit houdt in dat de werkprocessen die persoonsgegevens bevatten getoetst en ingericht moeten worden volgens de volgende beginselen: behoorlijkheid, transparantie, doelbinding, dataminimalisatie, opslagbeperking, juistheid, integriteit en vertrouwelijkheid. Daarnaast kan de gemeente in gevallen verplicht zijn om een gegevensbeschermingseffectbeoordeling (DPIA[2]) uit te voeren.

Alle verwerkingen van persoonsgegevens zijn opgenomen in het register van verwerkingen dat in 2018 voor de drie afzonderlijke gemeenten is opgesteld. In 2019 is gestart met het opstellen van één register voor de nieuwe gemeente. Hiervoor worden opnieuw alle verwerkingen geïnventariseerd en tevens getoetst aan de eisen uit de AVG.

Indien nieuwe werkprocessen worden opgenomen in het Zaaksysteem wordt hiervoor een eenvoudige variant van een DPIA uitgevoerd. Dit wordt via het desbetreffende zaaktype in Zaaksysteem opgevoerd door de proceseigenaar. Vervolgens controleert de FG of de verwerking voldoet aan de bovengenoemde beginselen en/of het proces een uitgebreidere DPIA nodig heeft.

In bijlage 2 is een overzicht opgenomen van de uitgevoerde DPIA's in 2019.

3. Organisatorische inbedding

Voor een goede en juiste uitvoering is het van belang dat iedereen binnen de organisatie op de hoogte is van de beginselen van de AVG en het belang van privacy. Organisatorische inbedding betekent het toewijzen van taken, verantwoordelijkheden en bevoegdheden en bewustzijn creëren.

Per 1 juli 2019 is een privacybeheerder aangesteld. Deze vormt samen met de FG en de CISO[3] het subteam 'Privacy en Informatieveiligheid' (PIN). PIN heeft in 2019 verder gewerkt aan rolduidelijkheid, zichtbaarheid in de organisatie en aan bewustwording door middel van berichten op intranet en voorlichting aan specifieke teams.

In het najaar is een presentatie over privacy en informatiebeveiliging gegeven aan de directie en netwerkmanagers. Tevens zijn deze onderwerpen onderdeel van de introductie-bijeenkomsten die georganiseerd worden door HRM. Hier wordt een verkorte variant gepresenteerd van de presentatie voor directie en netwerkmanagers. Een onderdeel van de bijeenkomsten is het afleggen van een integriteitsverklaring door nieuwe medewerkers waarin aandacht wordt besteed aan de omgang met (gevoelige) gegevens.

[2] De gegevensbeschermingseffectbeoordeling wordt afgekort tot DPIA naar de Engelse term Data Protection Impact Assessment.
[3] De Chief Information Security Officer.

4. Rechten van betrokkenen

De gemeente dient degene van wie zij de persoonsgegevens verwerkt (de betrokkene) zowel actief als passief te informeren over het verwerken, de wijze van het verwerken, de grondslag en de maatregelen die zij neemt om onrechtmatige toegang en verwerking te voorkomen. Daarnaast stelt de AVG betrokkenen in staat om door een aantal rechten controle en invloed uit te oefenen over zijn of haar persoonsgegevens.

Zoals aangegeven is op de website een privacyverklaring opgenomen. In deze verklaring staat hoe de gemeente omgaat met persoonsgegevens en hoe betrokkenen hun rechten kunnen uitvoeren. Daarnaast is bij nieuwe verwerkingen via de website en bij nieuwe formulieren een tekst opgenomen waarin betrokkenen worden geïnformeerd.

In bijlage 3 is een overzicht opgenomen van de verzoeken van betrokkenen in 2019.

5. Samenwerking

De gemeente werkt op meerdere beleidsterreinen, in verschillende bedrijfsfuncties, in diverse rollen en hoedanigheden samen met (mede) overheden en private organisaties. In veelvoorkomende gevallen zal sprake zijn van een verwerking van persoonsgegevens tussen partijen: ontvangen van persoonsgegevens, verzenden van persoonsgegevens, maar ook het opslaan van en inzage hebben in persoonsgegevens valt onder dit begrip. Deze verwerkingen dienen dan ook te voldoen aan de AVG. De gemeente dient daarom afspraken te maken met deze andere partijen.

Door het updaten van het register van verwerkingen is (meer) inzicht gekomen in lopende samenwerkingen met diverse partijen. Ook zijn in 2019 nieuwe samenwerkingen gestart. Hierbij is gekeken naar de hoedanigheid van deze partijen en waar nodig is een verwerkersovereenkomst gesloten dan wel zijn andere afspraken gemaakt.

6. Beveiliging

Vanuit het algemene behoorlijkheidsbeginsel, integriteitsbeginsel en vertrouwelijkheids-beginsel is het essentieel dat de gemeente passende technische en organisatorische maatregelen neemt ter beveiliging van persoonsgegevens. Daarnaast geldt onder de AVG een meldplicht datalekken. Dit houdt in dat beveiligingsincidenten onder omstandigheden gemeld dienen te worden aan de AP en/of de betrokkene(n).

In Zaaksysteem was al een zaaktype aangemaakt voor het melden van incidenten. In 2019 is de ‘Procedure voor het melden van beveiligingsincidenten en datalekken’ opgesteld en intern gepubliceerd, waardoor voor iedereen duidelijk is wie welke verantwoordelijkheid heeft bij (het melden van) incidenten.

Bij het verstrekken van toegang tot systemen wordt gekeken welke autorisatie nodig is voor de betreffende medewerker. Ook wordt gelogd wie welke informatie raadpleegt. Medewerkers kunnen via Zaaksysteem een gemotiveerd verzoek indienen tot wijziging van de verleende autorisatie. Dit verzoek wordt beoordeeld door de FG.

In bijlage 4 is een overzicht opgenomen van het aantal datalekken in 2019.

7. Verantwoording

De AVG legt de verantwoordelijkheid bij de organisatie zelf om aantoonbaar te maken dat deze voldoet aan de privacyregels. Door te voldoen aan de verantwoordingsplicht, levert de organisatie een belangrijke bijdrage aan de bescherming van het grondrecht van mensen op privacy. Dit betekent dat de gemeente aan moet kunnen tonen dat de verwerkingen van persoonsgegevens voldoen aan de beginselen van de AVG en aan de relevante wet- en regelgeving.

De verantwoordingsplicht komt voornamelijk tot uiting in het gepubliceerde register van verwerkingen en de openheid die met dit jaarverslag wordt gegeven in uitgevoerde DPIA's en (gemelde) datalekken.

8. Conclusie

In 2019 heeft de gemeente heel wat werk verzet om de AVG te implementeren in de organisatie, de systemen en de processen. Een aantal maatregelen waren - net zoals vorig jaar - zeer effectief, zoals het voorlichten van medewerkers, zowel in het algemeen als in specifieke vraagstukken, en het verstrekken van handreikingen en modellen.

Daarnaast is een belangrijke basis geslagen voor de komende jaren door onder meer de 'Procedure voor het melden van beveiligingsincidenten en datalekken' en de start van het actualiseren van het register van verwerkingen. Dit stelt ons in staat om de komende jaren structureler te gaan controleren op het gebruik van privacygevoelige gegevens in de gemeente.

Er zijn ook aandachtspunten voor de organisatie om aantoonbaar te kunnen voldoen aan de AVG. In het tweede deel van de rapportage zullen we ingaan op de aanbevelingen om gegevensbescherming (verder) in te bedden in de organisatie.

Deel 2. Vooruitkijken naar 2020

Gegevensbescherming onderdeel laten worden van de organisatie, en daarmee aantoonbaar voldoen aan de relevante wet- en regelgeving, is geen afvinklijst, maar een continu proces. Het vraagt om structurele borging van dit onderwerp. In 2018 hebben we ons bezig gehouden met het voorbereiden op de AVG en het nemen van de eerste hobbels om uiteindelijk aantoonbaar te kunnen voldoen aan deze wet. Het jaar 2019 stond in het teken van de vervolgstappen op dit gebied evenals het borgen van een aantal structurele zaken in de organisatie. In het vorige jaarverslag zijn hiervoor diverse aanbevelingen gegeven die zijn onderschreven door het college. Helaas is het door diverse omstandigheden, waaronder het pas in de tweede helft van het jaar beschikbaar hebben van een privacybeheerder, niet gelukt om alle gedane aanbevelingen te realiseren. Het jaar 2020 zal dan ook in het teken staan van het verder uitvoeren van de aanbevelingen. Hieronder bespreken we de aanbevelingen en voortgang per thema.

1. Het privacybeleid

Voor 2019 stond de aanbeveling om het huidige privacybeleid verder uit te werken en tevens intern privacybeleid op te stellen voor alle medewerkers van de gemeente. Deze aanbeveling blijft gelden voor 2020. Tevens dient het privacybeleid goed te worden geborgd binnen de organisatie en daarom is aanbevolen dit mee te nemen in het bewustwordingstraject. Hier is mee gestart, maar dit zal in 2020 worden vervolgd.

2. Processen

Het register van verwerkingen moest worden geharmoniseerd, met daarbij tevens een controle van processen en verwerkingen. Hier zijn grote stappen in gezet en dit zal naar verwachting voor de zomer van 2020 worden afgerond. Daarnaast is aanbevolen om een schema te maken wanneer welke DPIA's worden uitgevoerd. Een aantal DPIA's zijn reeds uitgevoerd en dit aantal zal in 2020 worden verhoogd.

3. Organisatorische inbedding

Voor een goede inbedding van privacy en informatieveiligheid binnen de teams is niet alleen aanbevolen om een bewustwordingstraject op te starten, maar ook om per team een privacy-ambassadeur te benoemen. Deze personen zijn aanspreekpunt voor de FG en de privacybeheerder. Zoals gezegd is een start gemaakt met het bewustwordings-traject door middel van onder andere informatie op intranet en een presentatie aan de directie en netwerkmanagers. Verder is gewerkt aan een postercampagne en een privacy escaperoom. Deze zullen in 2020 worden uitgerold onder de naam '5 voor veilig' met aansluitend een zoektocht naar de gewenste privacy-ambassadeurs.

4. Rechten van betrokkenen

De aanbevolen procedure voor de afhandeling van alle rechten van betrokkenen is opgesteld en alle betrokken collega's zijn hiervoor in kaart gebracht en geraadpleegd. In het tweede kwartaal van 2020 wordt de procedure opgenomen in Zaaksysteem en verder bekendgemaakt binnen en buiten de organisatie.

5. Samenwerking

Door het updaten van het register van verwerkingen is inzicht verkregen in wie onze verwerkers zijn en met welke partijen wij samenwerken. In 2020 wordt de laatste hand gelegd aan het inventariseren van afspraken die hierbij zijn of moeten worden gemaakt.

6. Beveiliging

Zoals gezegd is de 'Procedure voor het melden van beveiligingsincidenten en datalekken' opgesteld en intern gepubliceerd. Daarnaast wordt bij het verstrekken van toegang tot systemen gekeken welke autorisatie nodig is voor de betreffende medewerker en worden wijzigingsverzoeken geregistreerd en beoordeeld door de FG. In 2020 wordt verder gekeken naar gemaakte en te maken afspraken omtrent (het controleren van) autorisaties, een voorbeeld hiervan is het opstellen van een autorisatiematrix, en logging.

7. Verantwoording

Via intranet zijn standaardteksten verspreid die men kan gebruiken bij het informeren van betrokkenen via brieven, op de website en in aanvraagformulieren. In het tweede kwartaal van 2020 worden deze bij alle processen in Zaaksysteem opgenomen.

8. Conclusies

In 2019 zijn grote stappen gezet op het gebied van privacy en gegevensbescherming, maar dit moet in 2020 worden vervolgd. Vooral de bewustwording van medewerkers en het op orde krijgen van zaken als DPIA's, autorisaties en logging verdient komend jaar extra aandacht. Ook dient in 2020 de analyse in verband met de gewijzigde Wet politiegegevens te worden afgerond.

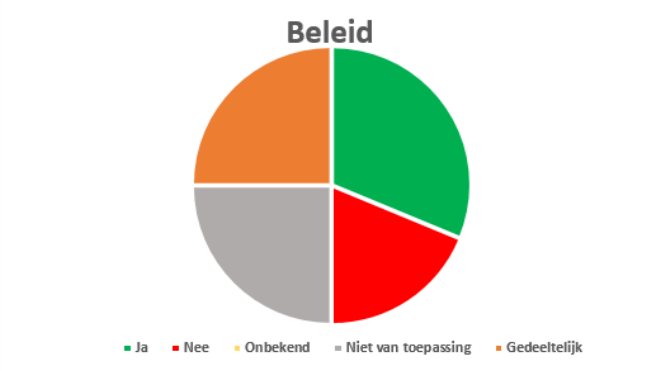
Bijlage 1. Stand van zaken AVG per onderwerp

Leeswijzer

In het document 'Het borgen van de Algemene Verordening Gegevensbescherming in de gemeentelijke organisatie' van de Informatiebeveiligingsdienst worden per onderdeel vragen gesteld of bepaalde taken (deels) zijn gerealiseerd. In onderstaande diagrammen is te zien waar we per onderdeel staan. Onder elk diagram wordt toegelicht wat de opvallendste punten zijn.

Beleid

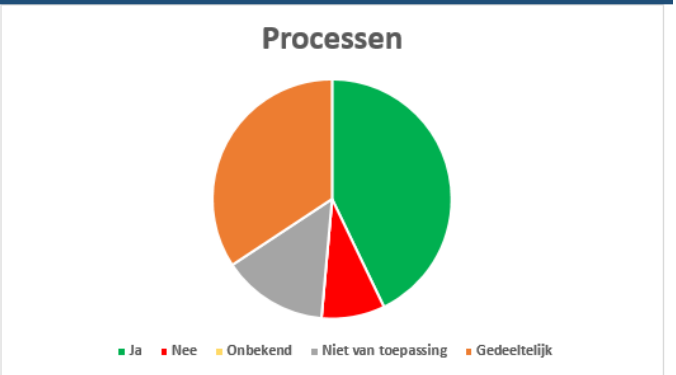
Resultaat	Aantal
Ja	5
Nee	3
Onbekend	0
Niet van toepassing	4
Gedeeltelijk	4



Toelichting
Geen noemenswaardige wijzigingen ten opzichte van 2018. De gemeente beschikt over een privacyverklaring en extern privacybeleid. Dit laatste dient echter nog te worden gespecificeerd en ook dient een intern privacybeleid te worden opgesteld.

Processen

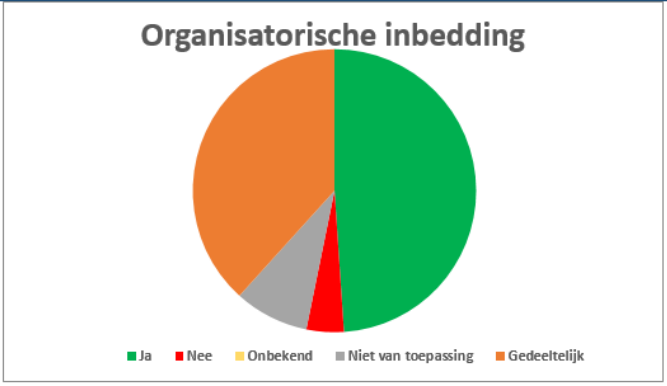
Resultaat	Aantal
Ja	15
Nee	3
Onbekend	0
Niet van toepassing	5
Gedeeltelijk	12



Toelichting
Ten opzichte van 2018 zijn een tweetal vragen van Nee naar Ja gegaan. Dit zit hem in het actualiseren van het register van verwerkingen, waardoor inzicht is gekomen in benodigde verwerkersovereenkomsten en eventuele andere afspraken. Verder dienen (meer) DPIA's te worden uitgevoerd en dient de AVG (meer) onderdeel te worden van werkprocessen. Aan dit laatste wordt gewerkt door middel van het bewustwordingstraject.

Organisatorische inbedding

Resultaat	Aantal
Ja	23
Nee	2
Onbekend	0
Niet van toepassing	4
Gedeeltelijk	18



Toelichting
Op dit onderdeel zijn grote wijzigingen doorgevoerd. Halverwege 2019 is een privacy-beheerder aangesteld, waardoor meer taken konden worden opgepakt. Ook zijn stappen gezet in het bewustwordingstraject.

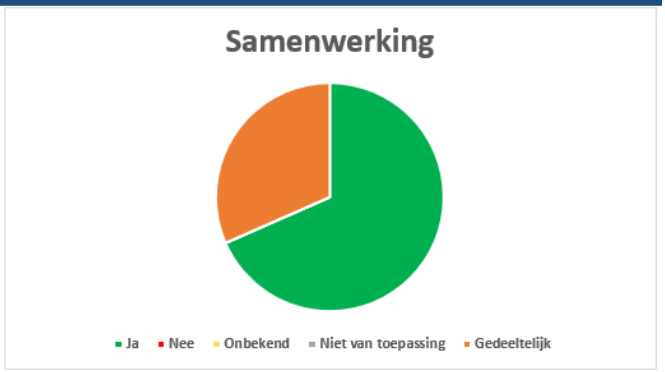
Rechten van betrokkenen

Resultaat	Aantal
Ja	14
Nee	1
Onbekend	0
Niet van toepassing	2
Gedeeltelijk	15

Toelichting
Het grote verschil met 2018 komt door het opstellen van een formele procedure voor de rechten van betrokkenen. Deze procedure wordt begin 2020 verwerkt in Zaaksysteem en vervolgens bekendgemaakt in de organisatie.

Samenwerking

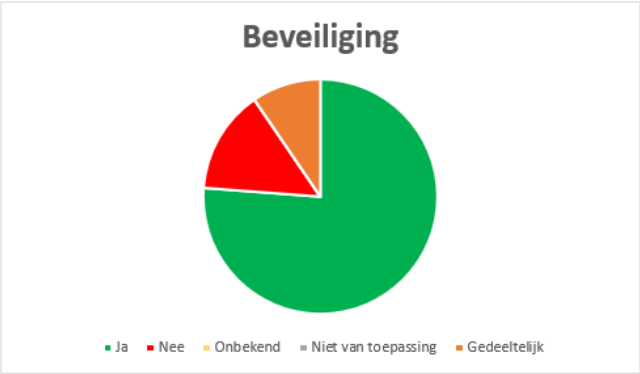
Resultaat	Aantal
Ja	13
Nee	0
Onbekend	0
Niet van toepassing	0
Gedeeltelijk	6



Toelichting
De getallen zijn dit jaar precies omgedraaid. Bij de actualisatie van het register van verwerkingen is onderzocht of we inzichtelijk hebben wie onze verwerkers dan wel samenwerkingspartners zijn en of hiermee de juiste afspraken zijn gemaakt.

Beveiliging

Resultaat	Aantal
Ja	16
Nee	3
Onbekend	0
Niet van toepassing	0
Gedeeltelijk	2



Toelichting
Op dit gebied is een kleine vooruitgang geboekt, vooral door het bekendmaken van een formele procedure voor de afhandeling van datalekken. Wel dienen nog afspraken te worden gemaakt op het gebied van autorisatiebeleid en logging en de controle hiervan.

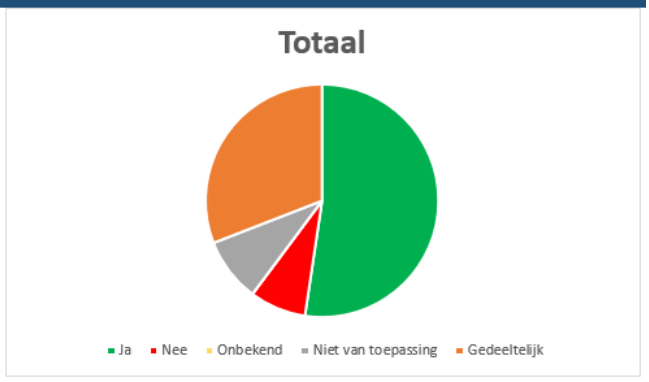
Verantwoording

Resultaat	Aantal
Ja	14
Nee	3
Onbekend	0
Niet van toepassing	2
Gedeeltelijk	2

Toelichting
Door publicatie van het register van verwerkingen en het jaarverslag met daarin gegevens over bijvoorbeeld datalekken is een stap gezet in transparantie. Daarom is ook op dit gebied een kleine vooruitgang geboekt.

Totaal

Resultaat	Aantal
Ja	100
Nee	15
Onbekend	0
Niet van toepassing	17
Gedeeltelijk	59



NB: Aangezien het gebruikte document van de Informatiebeveiligingsdienst voor 2019 is aangepast, kan de vergelijking met 2018 niet helemaal één op één worden gemaakt. Bij diverse onderdelen zijn vragen toegevoegd. Daarom is hierboven per onderwerp beschreven wat de verschillen zijn ten opzichte van het voorgaande jaar, maar is niet gekozen voor een visuele weergave.

Bijlage 2. Overzicht DPIA'S

In 2019 zijn 4 DPIA's uitgevoerd bij het starten van nieuwe processen in Zaaksysteem. Het gaat hier om:

- Toezicht APV & Bijzondere wetten
  Betreft NAW en gegevens op uittreksel KvK en verleende vergunningen
  Op basis van wettelijke grondslag

- Beroep
  Betreft NAW en geboortedatum en overige gegevens die door de betrokkene worden ingebracht
  Op basis van wettelijke grondslag

- Activiteitensubsidie
  Betreft NAW, telefoonnummer, e-mailadres en IBAN
  Indien wordt ingelogd met eHerkenning/Digi-D ook BSN
  Eventueel kan bv. een geloofsovertuiging duidelijk worden van een voorzitter van een kerkelijke stichting
  Op basis van aanvraag en taak van algemeen belang of in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen

- Dagvaarding / Dagvaarding HRM
  Betreft NAW en overige gegevens die door de betrokkene worden ingebracht
  Op basis van wettelijke grondslag

Daarnaast is een DPIA uitgevoerd door de VNG in verband met de nieuwe Wet verplichte geestelijke gezondheidszorg (Wvggz). Deze hebben we overgenomen, waar nodig aangepast aan onze (regionale) situatie.

Bijlage 3. Overzicht rechten van betrokkenen

Recht op inzage

In 2019 is één verzoek ingekomen omtrent inzage in verstrekking van persoonsgegevens, maar dit betrof een specifiek dossier, dus eigenlijk meer een verzoek op grond van de Wet openbaarheid van bestuur (Wob).

Tevens zijn een aantal verzoeken ingediend voor het inzien van dossiers, maar deze zijn feitelijk gebaseerd op specifieke wetgeving (Jeugdwet en Wmo).

Recht om bezwaar te maken tegen de gegevensverwerking

In 2019 is één verzoek binnengekomen dat feitelijk betrekking had op bezwaar tegen de verwerking. Het ging enerzijds om het opnemen van diverse (onjuiste) gegevens in een dossier en anderzijds om het (onterecht) verstrekken van gegevens uit een dossier aan andere partijen. De kwestie was onderdeel van een lopende rechtszaak, dus is ook in die zaak afgehandeld. Wel is het dossier doorgenomen met betrokkene en waar mogelijk opgeschoond.

Geen verzoeken zijn ingekomen op basis van het recht op beperking van verwerking, dataportabiliteit, vergetelheid, rectificatie/aanvulling en het recht met betrekking tot geautomatiseerde besluitvorming en profilering.

Bijlage 4. Overzicht datalekken

In 2019 zijn 6 gemelde beveiligingsincidenten gekwalificeerd als een datalek:

- Plan van aanpak van een betrokkene meegestuurd met plan van aanpak andere betrokkene. Betreft een omissie van een individuele medewerker die hier voortaan beter op zal letten. Datalek is gemeld bij AP en betrokkenen.
- Actieplan vermist, onduidelijk is of het door PostNL is kwijtgeraakt of door betrokkene zelf. Gemeld bij AP en betrokkene.
- Actieplan gemaild naar verkeerde gezin. Direct gebeld en mail verwijderd. Datalek gemeld bij AP. Besloten is om niet te melden bij betrokkene, omdat de casemanager, gezien de situatie bij het betrokken gezin, overtuigd is dat het document ongelezen is verwijderd en niet verder zal worden verspreid. De afdeling heeft maatregelen genomen om dergelijke fouten in de toekomst te voorkomen. Ook zal in 2020 beveiligd mailen worden ingevoerd.
- Omissie in software waardoor formulieren met gegevens over nieuwe woningen naar de oude adressen zijn verstuurd. Door 5 betrokkenen bij ons gemeld. Leverancier heeft probleem opgelost. Gemeld bij AP en betrokkenen (voor zover bekend).
- Beveiligingslek in software waardoor toegang mogelijk was tot het netwerk. Alle mogelijke controles gedaan en geen onjuiste toegang aangetroffen. Voor het verleden (lek schijnt sinds 2014 te bestaan, maar pas eind 2019 ontdekt en opgelost) is dit echter niet meer te controleren, daarom voor de volledigheid gemeld bij AP.
- Via een zoekfunctie konden in ons registratiesysteem meer gegevens worden ingezien dan waarvoor autorisatie is afgegeven. Dit is opgepakt door de leverancier en gemeld aan AP.