VIJFHEERENLANDEN

JAARRAPPORTAGE 2018 GEGEVENSBESCHERMING

Opgesteld door de Functionaris Gegevensbescherming

Samenvatting

Het jaar 2018 was op het gebied van gegevensbescherming een bijzonder jaar voor organisaties en inwoners. Zo ook voor de gemeenten Leerdam, Vianen en Zederik, samenwerkend in de Bedrijfsvoeringsorganisatie Vijfheerenlanden en per 1 januari 2019 gefuseerd in de gemeente Vijfheerenlanden (voor de leesbaarheid zal in deze rapportage worden gesproken over 'de gemeente'). Op 25 mei 2018 werd namelijk de Algemene Verordening Gegevensbescherming (AVG) van kracht. De AVG verving de Wet bescherming persoonsgegevens (Wbp) en zorgt voor verhoogde aandacht voor een rechtmatige verwerking van persoonsgegevens in alle sectoren. De overheid heeft hierin een belangrijke voorbeeldfunctie.

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 2018 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 2019. Adequaat omgaan met persoonsgegevens is een blijvend proces en zal dan ook aandacht blijven vergen van zowel bestuur, management als medewerkers.

In 2018 heeft de gemeente veel werk verzet op het gebied van gegevensbescherming. Na het aanstellen van een Functionaris Gegevensbescherming (FG) en een Chief Information Security Officer (CISO) is onder andere een privacyverklaring op de website opgenomen, extern privacybeleid gepubliceerd en een register van verwerkingen opgesteld. Daarnaast worden inwoners via deze kanalen geïnformeerd over hun rechten, is gewerkt aan interne bewustwording door modellen, handreikingen en voorlichting en zijn diverse verwerkersovereenkomsten met derden tot stand gekomen. Tevens is gewerkt aan een goede beveiliging van gegevens door onder andere juiste autorisaties en het loggen van toegang.

Inhoudsopgave

Inleiding

De gemeente dient zorgvuldig om te gaan met persoonsgegevens. Gemeenten verwerken immers bij de uitoefening van hun taken veel persoonlijke informatie. In de AVG wordt het wettelijk kader beschreven voor het verwerken van persoonsgegevens. Zo dient de gemeente transparant te zijn welke persoonsgegevens zij verwerkt en voor welk doel. Persoonsgegevens mogen alleen worden verwerkt wanneer dit in overeenstemming is met het doel waarvoor zij zijn verzameld en gegevens mogen niet langer bewaard worden dan strikt noodzakelijk. Bovendien moet de gemeente passende technische en organisatorische beveiligingsmaatregelen treffen om onrechtmatige toegang tot deze persoonsgegevens tegen te gaan en daardoor een onrechtmatig gebruik van deze persoonsgegevens te voorkomen. 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. Het gaat hierbij om persoonsgegevens van eigen inwoners, inwoners van andere gemeenten, zakenrelaties, medewerkers en externen. 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). Op 1 maart 2018 heeft de Bedrijfsvoeringsorganisatie Vijfheerenlanden (en daarmee de bestuursorganen van de gemeenten Leerdam, Vianen en Zederik) mevrouw mr. L. de Keijzer-Krens 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 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 2018. Wat heeft de gemeente bereikt op het gebied van gegevens-bescherming? Welke maatregelen zijn er genomen om te voldoen aan de AVG? In het tweede deel worden aanbevelingen gedaan om gegevensbescherming en privacy in het jaar 2019 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 criteria die in beide delen worden genoemd zijn afkomstig uit het document 'Het borgen van de Algemene Verordening Gegevensbescherming in de gemeentelijke organisatie' van de Informatiebeveiligingsdienst. In dit document worden criteria en maatregelen omschreven die de AVG vertalen naar een kwaliteitscyclus voor gegevensbescherming en privacy voor gemeentelijke processen. In bijlage 1 is een overzicht opgenomen waar in cirkeldiagramvorm wordt aangegeven in hoeverre de gemeente de criteria reeds heeft geïmplementeerd.

De FG heeft tevens samen met BMC begin 2019 een Zelfevaluatie AVG uitgevoerd. De resultaten uit de rapportage zijn opgenomen in dit jaarverslag.

Deel 1. Terugblik op 2018

Het eerste deel van het jaar 2018 stond voor wat betreft privacy volledig in het teken van het van kracht worden van de AVG. In dit deel van de rapportage zal worden teruggeblikt op hetgeen de gemeente in 2018 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 opgesteld, vastgesteld door het college en vervolgens gepubliceerd op onder andere de website van de gemeente en het intranet. Daarnaast is een privacyverklaring op de website opgenomen waarin mensen worden geïnformeerd over wat we doen met persoonsgegevens, wie de FG is en hoe betrokkenen hun rechten kunnen uitvoeren.

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, oftewel Data Protection Impact Assessment en kortweg DPIA, uit te voeren.

Alle verwerkingen van persoonsgegevens zijn opgenomen in het vorig jaar opgestelde register van verwerkingen. Dit register is één van de verplichtingen 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 voor het jaar 2018.

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.

In 2018 is een FG aangesteld en is besloten om in 2019 een privacybeheerder aan te stellen. De FG heeft, samen met de CISO, gewerkt aan rolduidelijkheid en zichtbaarheid in de organisatie en daarnaast aan bewustwording door middel van berichten op intranet en voorlichting aan specifieke teams. Tevens is gewerkt aan technische inbedding, zoals afspraken over autorisaties en logging.

Alle medewerkers hebben (opnieuw) een integriteitsverklaring afgelegd waar tevens aandacht is besteed aan de omgang met (gevoelige) gegevens.

4. Rechten van betrokkenen

De gemeente dient degene van wie zij de persoonsgegevens verwerkt (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 hierboven 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 het aantal verzoeken van betrokkenen voor het jaar 2018.

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 opstellen van het register van verwerkingen is (meer) inzicht gekomen in lopende samenwerkingen met diverse partijen. Ook zijn in 2018 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 incidenten - waaronder inbreuken op de beveiliging - onder omstandigheden gemeld dienen te worden aan de AP en/of de betrokkene(n).

Bij toegang tot systemen wordt gekeken naar welke autorisatie nodig is voor de betreffende medewerker. Nieuw aangeschafte software beschikt over mogelijkheden van logging.

In Zaaksysteem is een zaaktype aangemaakt voor het melden van incidenten. De CISO of FG beoordeelt vervolgens of sprake is van een datalek en of het incident moet worden gemeld aan de AP en/of betrokkene(n). Indien nodig wordt de melding aan de AP gedaan en wordt het betreffende team ondersteund bij de melding aan betrokkene(n).

In bijlage 4 is een overzicht opgenomen van het aantal datalekken voor het jaar 2018.

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.

Door middel van het opstellen van het register van verwerkingen en de mogelijkheid om uit het Zaaksysteem te rapporteren over uitgevoerde DPIA's en gemelde incidenten en datalekken is een grote slag gemaakt in de verantwoording.

8. Conclusie

In 2018 heeft de gemeente heel wat werk verzet om de AVG te implementeren in de organisatie, de systemen en de processen. Een aantal maatregelen waren zeer effectief, zoals het voorlichten van medewerkers, zowel in het algemeen als in specifieke vraagstukken, en het verstrekken van handreikingen en modellen.

Er zijn ook aandachtspunten voor de organisatie om aantoonbaar te kunnen voldoen aan de AVG. In het tweede deel van de rapportage zullen aanbevelingen worden gedaan om gegevensbescherming daadwerkelijk in te bedden in de organisatie.

Deel 2. Vooruitkijken naar 2019

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. Waar het jaar 2018 in het teken stond van voorbereiden op de AVG en het nemen van de eerste hobbels om uiteindelijk aantoonbaar te kunnen voldoen aan deze wet, zal 2019 in het teken staan van de laatste stappen op dit gebied evenals het borgen van een aantal structurele zaken in de organisatie. Zoals aangegeven is begin dit jaar een analyse uitgevoerd van waar we staan en wat nog moet gebeuren. De belangrijkste punten zijn meegenomen in onderstaande aanbevelingen.

Per 1 januari 2019 is een wetswijziging in werking getreden van de Wet politiegegevens in verband met Europese regelgeving over de verwerking van persoonsgegevens met het oog op de voorkoming, het onderzoek, de opsporing en vervolging van strafbare feiten of de tenuitvoerlegging van straffen. De buitengewone opsporingsambtenaren (boa's) van de gemeente hebben te maken met deze wetgeving, waardoor op korte termijn moet worden bekeken wat de impact is van de wet en welke zaken geregeld moeten worden.

1. Het privacybeleid

Het huidige privacybeleid is gebaseerd op een model van de VNG. Dit is in de basis een prima beleid, maar diverse keuzemogelijkheden zijn niet uitgewerkt. Het is aan te raden dit uit te werken voor de nieuwe gemeente en tevens intern privacybeleid op te stellen voor alle medewerkers van de gemeente. De focus dient daarnaast te liggen op het goed borgen van het privacybeleid binnen de organisatie. Aanbeveling is dan ook dit mee te nemen in het bewustwordingstraject.

2. Processen

Het register van verwerkingen moet worden geharmoniseerd. Aanbevolen wordt om hierbij de bestaande processen en verwerkingen te controleren aan de hand van de beginselen uit de AVG. Uiteraard geldt dit ook voor nieuwe processen en verwerkingen. Daarnaast is het raadzaam om een schema te maken wanneer welke DPIA's worden uitgevoerd, zowel nieuwe DPIA's als een evaluatie van reeds uitgevoerde DPIA's.

3. Organisatorische inbedding

Eén belangrijke aanbeveling was het aanstellen van een privacybeheerder. Deze vacature is intern uitgezet en wordt per 1 juli a.s. ingevuld. Naast deze nieuwe functie verdient het aanbeveling om in alle teams een privacy-ambassadeur te benoemen. Deze personen zijn aanspreekpunt voor de FG en de privacybeheerder. Hierdoor zal het delen van kennis en borging van privacy in de organisatie makkelijker verlopen. Een goede samenwerking zorgt ervoor dat wederzijds signaleringen worden gedaan en op het juiste moment kan worden ingespeeld op een bepaalde behoefte. Een laatste, maar zeer belangrijke, aanbeveling is het opstarten van een bewustwordingstraject, want het is gebleken dat niet overal voldoende kennis aanwezig is. Hier wordt echter ook al aan gewerkt.

4. Rechten van betrokkenen

Aanbeveling is een procedure op te stellen voor de afhandeling van alle rechten van betrokkenen. Hierin moet ook worden meegenomen waar welke taken zijn belegd. Het is van belang dit goed te borgen in de organisatie, zodat voor iedereen duidelijk is wat een verzoek inhoudt en wat er mee moet gebeuren. De afhandeling van dergelijke verzoeken moet tevens worden opgenomen in processen en systemen.

5. Samenwerking

In het register van verwerkingen staat voor welke verwerkingen wij verantwoordelijke zijn en wie daarbij onze verwerkers zijn. Hierbij moet worden geïnventariseerd welke verwerkersovereenkomsten zijn of moeten worden gesloten. Daarnaast dient inzichtelijk te worden gemaakt voor welke verwerkingen wij medeverantwoordelijke dan wel verwerker zijn en welke afspraken hierbij zijn of moeten worden gemaakt.

6. Beveiliging

Aanbevolen wordt de procedure voor het melden van incidenten vast te stellen en te delen in de organisatie. Daarnaast is het goed om te kijken naar gemaakte en te maken afspraken omtrent (het controleren van) autorisaties en logging.

7. Verantwoording

Voor 2019 is het van belang een stap te maken in het informeren van betrokkenen door bijvoorbeeld standaardteksten te ontwikkelen die te gebruiken zijn in brieven, op de website en in aanvraagformulieren.

8. Conclusies

Op het gebied van privacy en gegevensbescherming is in 2019 winst te behalen. Vooral de bewustwording van medewerkers en het op orde krijgen van zaken als verwerkers-overeenkomsten en DPIA's verdient komend jaar extra aandacht. Door het aanstellen van een privacybeheerder kan hier naar verwachting een grote stap in worden gemaakt. In 2019 dient tevens een analyse in verband met de gewijzigde Wet politiegegevens plaats te vinden en zal ook worden bekeken welke middelen nodig zijn om bepaalde ambities te verwezenlijken.

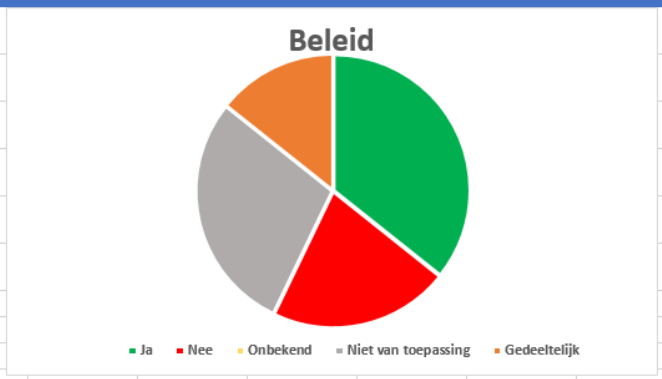
Bijlage 1. Stand van zaken AVG per onderwerp

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

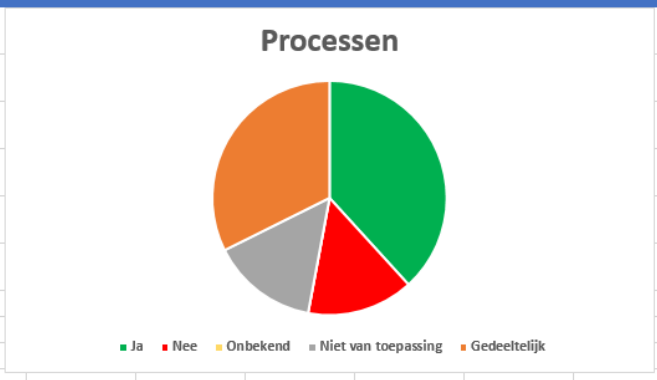
Resultaat	Aantal
Ja	5
Nee	3
Onbekend	0
Niet van toepassing	4
Gedeeltelijk	2



Toelichting
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

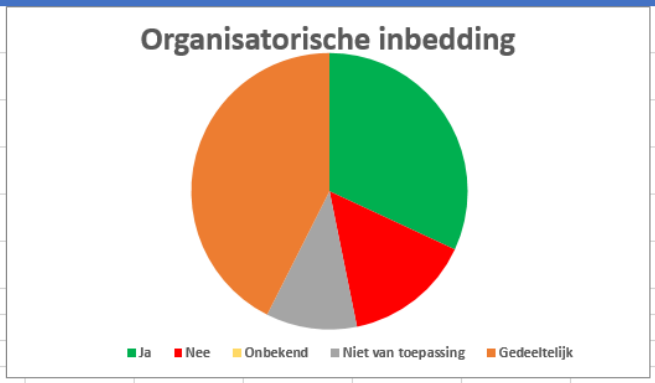
Resultaat	Aantal
Ja	13
Nee	5
Onbekend	0
Niet van toepassing	5
Gedeeltelijk	11



Toelichting
De gemeente beschikt over een register van verwerkingen. Wel moet deze nog worden geactualiseerd, inclusief onderzoek naar benodigde verwerkersovereenkomsten en eventuele andere afspraken. Ook moet een planning voor DPIA's worden opgesteld en dient de AVG nog (meer) onderdeel te worden van werkprocessen.

Organisatorische inbedding

Resultaat	Aantal
Ja	15
Nee	7
Onbekend	0
Niet van toepassing	5
Gedeeltelijk	20



Toelichting
De gemeente beschikt over een FG, daarnaast is besloten over aanstelling van de privacybeheerder. De teams beschikken echter nog niet over privacy-ambassadeurs. Ook wordt gewerkt aan een bewustwordingstraject en een verduidelijking van wie welke taken heeft binnen het vakgebied privacy (en informatiebeveiliging).

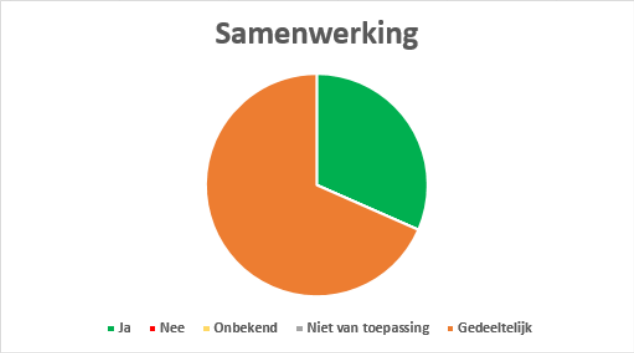
Rechten van betrokkenen

Resultaat	Aantal
Ja	11
Nee	11
Onbekend	0
Niet van toepassing	1
Gedeeltelijk	10

Toelichting
De gemeente heeft nog geen formele procedure voor de rechten van betrokkenen. De hoeveelheid Nee in bovenstaand overzicht wordt verklaard door het feit dat in het document per recht van betrokkene wordt gevraagd of hiervoor een procedure aanwezig is. Betrokkenen worden wel via de privacyverklaring op de website gewezen op hun rechten en hoe zij deze kunnen uitoefenen. Vooral intern moet echter nog worden verduidelijkt hoe deze verzoeken moeten worden afgehandeld.

Samenwerking

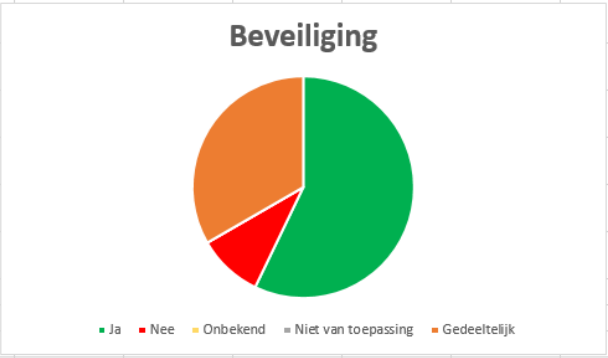
Resultaat	Aantal
Ja	6
Nee	0
Onbekend	0
Niet van toepassing	0
Gedeeltelijk	13



Toelichting
Bij de actualisatie van het register van verwerkingen zal worden onderzocht of we (compleet) inzichtelijk hebben wie onze verwerkers dan wel samenwerkingspartners zijn en of hiermee de juiste afspraken zijn gemaakt.

Beveiliging

Resultaat	Aantal
Ja	12
Nee	2
Onbekend	0
Niet van toepassing	0
Gedeeltelijk	7



Toelichting
De gemeente heeft nog geen formele procedure voor de afhandeling van datalekken. Ook op het gebied van autorisatiebeleid en logging en de controle hiervan dienen afspraken te worden gemaakt.

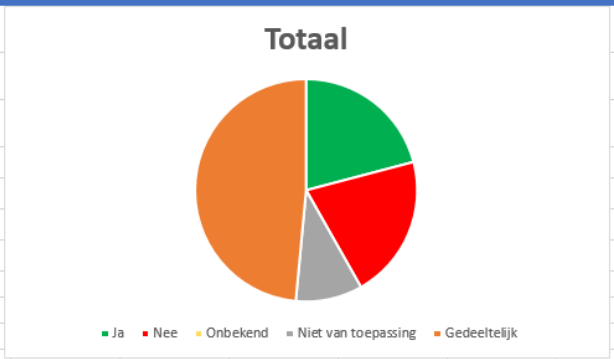
Verantwoording

Resultaat	Aantal
Ja	12
Nee	3
Onbekend	0
Niet van toepassing	2
Gedeeltelijk	4

Toelichting
De gemeente beschikt niet over een eenduidige werkwijze voor het verkrijgen en bewaren van toestemming van betrokkenen. Ook kan nog een stap worden gezet in transparantie, bijvoorbeeld door middel van het publiceren van dit jaarverslag.

Totaal

Resultaat	Aantal
Ja	28
Nee	28
Onbekend	0
Niet van toepassing	13
Gedeeltelijk	65



Bijlage 2. Overzicht DPIA'S

In 2018 zijn 5 DPIA's uitgevoerd bij het starten van nieuwe processen in Zaaksysteem. Het gaat hier om:

- Toezicht evenementen
  Betreft NAW en e-mailadres
  Op basis van aanvraag en wettelijke grondslag

- Bewonersinitiatief
  Betreft naam en e-mailadres
  Via website wordt om specifieke toestemming gevraagd

- Afscheidscadeau Vianen
  Betreft NAW, telefoonnummer en e-mailadres
  Bij deelname wordt om specifieke toestemming gevraagd

- Exploitatievergunning
  Betreft NAW
  Op basis van aanvraag en wettelijke grondslag

- Gehandicaptenparkeerplaats
  NAW, kenteken voertuig en nummer gehandicaptenparkeerkaart
  Op basis van aanvraag en wettelijke grondslag

Bijlage 3. Overzicht rechten van betrokkenen

Recht op inzage
In 2018 is één verzoek ingekomen omtrent inzage in verstrekking van persoonsgegevens uit de BRP.

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 2018 zijn vier verzoeken binnengekomen die feitelijk betrekking hadden op bezwaar tegen de verwerking. Het ging om:

- Inzage in het dossier van betrokkene terwijl een aanvraag is gedaan door een partner. Dossier van betrokkene bleek hierbij uit een stuk service onterecht betrokken, afdeling past proces hierop aan.
- Vermelding van BSN op verzonden brief. Het gebruik van het BSN was in dit geval onnodig, afdeling past proces hierop aan.
- Bij bepaalde aanvraag wordt BSN gevraagd en tevens toestemming om BSN te delen. Zal voortaan specifieker worden gevraagd, toelichting wordt aangepast op formulieren.
- Betrokkene gecontacteerd door instantie zonder toestemming te hebben gegeven voor delen gegevens met betreffende instantie. Bleek te berusten op een misverstand.

Recht op beperking van verwerking
In 2018 is eenmaal verzocht om toepassing van geheimhouding bij verstrekken gegevens uit BRP.

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

Bijlage 4. Overzicht datalekken

In 2018 zijn 9 gemelde beveiligingsincidenten gekwalificeerd als een datalek:

- Vanwege te breed opengesteld archief op netwerkschijf waren mappen toegankelijk voor ongeautoriseerde gebruikers. Dit betrof slechts een intern lek. Na constatering is het archief gesloten en slechts op verzoek specifiek toegankelijk gemaakt op basis van gecontroleerde autorisaties. Geen sprake van melding bij AP dan wel betrokkenen.
- Eenzelfde situatie deed zich voor bij het openstellen van de Outlook-agenda's. Hierbij waren tevens agenda's van collega's van het sociaal domein, met daarin afspraken en daarmee namen van cliënten, zichtbaar voor andere collega's. Dit betrof slechts een intern lek. Na vrijwel directe constatering zijn de betreffende agenda's direct gesloten en alleen opengesteld voor collega's binnen het sociaal domein. Geen sprake van melding bij AP dan wel betrokkenen.
- Bovenstaande gold tevens voor agenda's van collega's van HRM die namen van sollicitanten bij afspraken vermeldden. Dit wordt nu niet meer gedaan óf de afspraak wordt gemarkeerd als privé, zodat hij niet zichtbaar is voor collega's. Daarnaast zal voor de organisatie een e-mail- en agendaprotocol worden opgesteld. Geen sprake van melding bij AP dan wel betrokkenen.
- Diverse plannen van aanpak met betrekking tot sociaal domein zijn kwijtgeraakt bij de post. Onduidelijk is of dit een interne of externe oorzaak had. Gehele postproces is tegen het licht gehouden en waar nodig aangepast. Datalek is gemeld bij AP en betrokkenen.
- Document met NAW-gegevens via beveiligde e-mail naar foutieve aanbieder verstuurd. Zij hebben ons geïnformeerd en het stuk verwijderd. Wij hebben een verwerkersovereenkomst met deze aanbieder en het gaat om minimale persoonsgegevens. Geen sprake van melding bij AP dan wel betrokkene.
- Brief met NAW-gegevens per abuis meegestuurd met brief aan andere betrokkene. Deze laatste bij ons gemeld en brief retour gezonden. Betreft een omissie van een individuele medewerker die hier voortaan beter op zal letten. Geen sprake van melding bij AP en betrokkene.
- Container met archiefstukken heeft ongeveer 10 minuten onbewaakt open buiten gestaan. Na constatering is medewerker ernaast blijven staan en vervolgens is er een slot opgedaan. Datalek is gemeld bij AP.
- Plan van aanpak van ene 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.
- Betrokkene heeft documenten aan de gemeenteraad verstuurd en deze zijn integraal zichtbaar op de gemeentelijke website. Betrokkene heeft dit zelf gemeld waarop de stukken zijn verwijderd van de website. Tevens is een verzoek bij Google ingediend om links naar de betreffende documenten via zoekresultaten te verwijderen. In samenspraak met de griffie is besloten ingezonden stukken niet langer zonder toestemming integraal te publiceren. Datalek is gemeld bij AP.