VIJFHEERENLANDEN

JAARRAPPORTAGE 2020 GEGEVENSBESCHERMING

Opgesteld door de Functionaris Gegevensbescherming

Samenvatting

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 2020 heeft genomen om de doelstellingen en beginselen uit de Algemene Verordening Gegevensbescherming (AVG) te behalen en te waarborgen. Ook bevat dit document aandachtspunten en actiepunten voor het jaar 2021. Adequaat omgaan met persoons-gegevens is een blijvend proces en zal dan ook aandacht blijven vergen van zowel bestuur, management als medewerkers.

In 2020 heeft de gemeente veel werk verzet op het gebied van gegevensbescherming. Hoofdonderwerp was dit jaar bewustwording onder medewerkers. Hiervoor is de campagne '5 voor veilig' gestart met een poster in het personeelsmagazine en op intranet. Vanwege corona is de campagne vooralsnog digitaal uitgerold. Regelmatig werden op intranet themaposters met een toelichting geplaatst. Dit zal de komende jaren doorlopen en worden uitgebreid met bijvoorbeeld teamspecifieke bijeenkomsten, e-learning en phishing testen. Na het halverwege het jaar aanstellen van een nieuwe privacybeheerder is onder andere gewerkt aan het updaten van het register van verwerkingen met daarbij een controle van alle facetten rondom een verwerking, zoals de juiste grondslag, gegevensdeling met derden en gemaakte afspraken met leveranciers.

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 2020. 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 2021 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 borgings-product van de Informatiebeveiligingsdienst (IBD).[1] In het borgingsproduct worden thema's, criteria en maatregelen omschreven die de AVG vertalen naar een kwaliteits-cyclus 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 2020

Het jaar 2020 stond in het teken van verdere implementaties en verbeteringen en vooral het verhogen van de bewustwording onder medewerkers. In dit deel van de rapportage wordt teruggeblikt op wat de gemeente in 2020 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.

Het externe privacybeleid en een online privacyverklaring zijn reeds gepubliceerd. Verder 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 staan in het register van verwerkingen dat in 2018 is opgesteld. In 2020 is verder gewerkt aan een update waarbij opnieuw alle verwerkingen worden 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 2020.

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 2020 is een (nieuwe) privacybeheerder aangesteld. Deze vormt samen met de FG en de CISO[3] het subteam 'Privacy en Informatieveiligheid' (PIN). PIN heeft in 2020 verder gewerkt aan rolduidelijkheid, zichtbaarheid in de organisatie en vooral aan bewustwording door middel van opvallende posters met uitleg via berichten op intranet en voorlichting aan teams.

Voor vrijwel alle teams is een privacy-ambassadeur aangewezen. Hierdoor kan meer inzicht worden verkregen in de mogelijke problemen per team en zijn er kortere lijnen voor het stellen van vragen en geven van informatie.

[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.

Op de website van de gemeente is 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 2020.

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 en deze verwerkingen dienen 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. Bij het starten van nieuwe samenwerkingen wordt gekeken naar de hoedanigheid van partijen en waar nodig wordt 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).

Medewerkers kunnen via het Zaaksysteem een beveiligingsincident melden. De procedure is eenvoudig te vinden via intranet. Samen met de privacybeheerder wordt gekeken of al dan niet sprake is van een datalek en zo ja, of het moet worden gemeld aan de Autoriteit Persoonsgegevens en betrokkene(n). Tevens wordt uiteraard gekeken welke maatregelen eventueel nodig zijn om het incident op te lossen en/of ervoor te zorgen dat een dergelijk incident niet nogmaals kan plaatsvinden. In bijlage 4 is een overzicht opgenomen van het aantal beveiligingsincidenten, met specifieke aandacht voor datalekken, in 2020.

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.

Afgelopen jaar zijn daarnaast twee belangrijke ontwikkelingen geweest op het gebied van veilig werken en persoonsgegevens. Ten eerste is in maart 2020 gestart met een nieuwe veilig e-mailen oplossing (ZIVVER). Deze is gebruiksvriendelijker dan de vorige oplossing en ondersteunt ook het delen van grotere bestanden. Daarnaast is men vanwege de coronamaatregelen op zeer korte termijn overgegaan op thuiswerken. Dit was door het werken via Citrix direct en zonder grote risico's mogelijk, maar het was wel noodzakelijk om de mogelijkheden voor videobellen te verbeteren. Sinds juni 2020 beheert de gemeente een beveiligde videoverbinding die alle medewerkers kunnen gebruiken.

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 2020 heeft de gemeente heel wat werk verzet om de AVG verder te implementeren in de organisatie, de systemen en de processen. Specifieke aandacht is besteed aan het voorlichten van medewerkers over het werken met persoonsgegevens.

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 2021

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. De afgelopen jaren is gewerkt aan het aantoonbaar voldoen aan de AVG en het vergroten van de bewustwording bij medewerkers en zichtbaarheid van het privacyteam. De eerder gedane aanbevelingen zijn nog niet volledig gerealiseerd, dus in 2021 zal hier verder aan worden gewerkt. Hieronder bespreken we de aanbevelingen en voortgang per thema.

1. Het privacybeleid

Voor 2020 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 2021. 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 2021 worden vervolgd.

2. Processen

Het register van verwerkingen moet verder worden geharmoniseerd, met daarbij een controle van processen en verwerkingen. Daarnaast worden DPIA's nu relatief ad hoc uitgevoerd, maar voor komend jaar wordt aanbevolen om een schema te maken wanneer welke DPIA's worden uitgevoerd.

3. Organisatorische inbedding

In 2020 is een vervolg gegeven aan het bewustwordingstraject met een postercampagne via intranet. In 2021 zal de campagne worden voortgezet en uitgebreid met bijvoorbeeld een phishing test of een privacy escaperoom.

4. Rechten van betrokkenen

De procedure voor de afhandeling van alle rechten van betrokkenen is opgenomen in Zaaksysteem en bekendgemaakt binnen en buiten de organisatie. In 2021 zal het proces verder worden aangescherpt en worden gecontroleerd of alle applicaties en beheerders op een juiste wijze bij het proces worden betrokken.

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 2021 wordt de laatste hand gelegd aan het inventariseren van afspraken die hierbij zijn of moeten worden gemaakt.

6. Beveiliging

In 2021 wordt gewerkt aan het verbeteren van het beheer op applicaties. Hiermee krijgen we beter zicht op welke data aanwezig is in welke applicatie en of deze bijvoorbeeld niet te lang bewaard blijven. Ook geeft dit de mogelijkheid om effectief te gaan controleren op rechten- en toegangsbeheer binnen applicaties. Het toegangsbeheer tot de gemeentelijke omgeving wordt verbeterd door het altijd toepassen van multi-factor authenticatie. Tot slot worden de periodieke scans om de kwetsbaarheid van het systeem te testen, de zogenaamde vulnerability scans, opnieuw aanbesteed.

7. Verantwoording

In overleg met de privacy-ambassadeurs zal worden bekeken op welke wijze betrokkenen worden geïnformeerd over het verwerken van hun gegevens. Vervolgens kunnen meer en vooral specifiekere standaardteksten worden opgesteld, zodat we daadwerkelijk alle betrokkenen volledig informeren.

8. Conclusies

In 2020 zijn grote stappen gezet op het gebied van privacy en gegevensbescherming en dit moet in 2021 worden voortgezet. Vooral het op orde krijgen van zaken als DPIA's, autorisaties en logging verdient komend jaar extra aandacht. Ook dient in 2021 de analyse in verband met de gewijzigde Wet politiegegevens te worden afgerond, aangezien aan het eind van het jaar een audit moet zijn verricht en worden toegestuurd aan de Autoriteit Persoonsgegevens.

Bijlage 1. Stand van zaken AVG per onderwerp

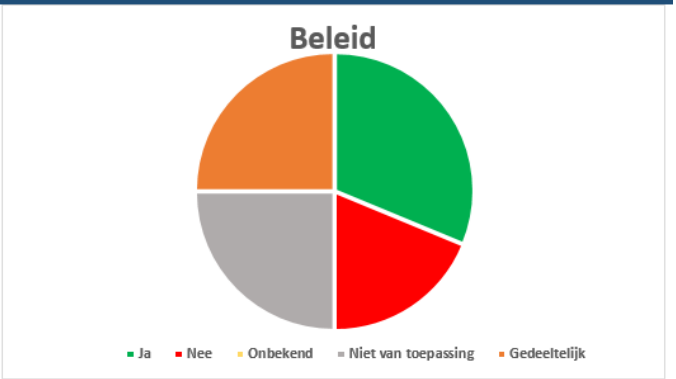
Leeswijzer

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. Aangezien dezelfde vragenlijst wordt gehanteerd als in het vorige verslag is een duidelijke vergelijking te zien tussen de stand van zaken in 2019 en 2020. Onder elk diagram wordt toegelicht wat de opvallendste punten zijn.

Onderdeel Beleid

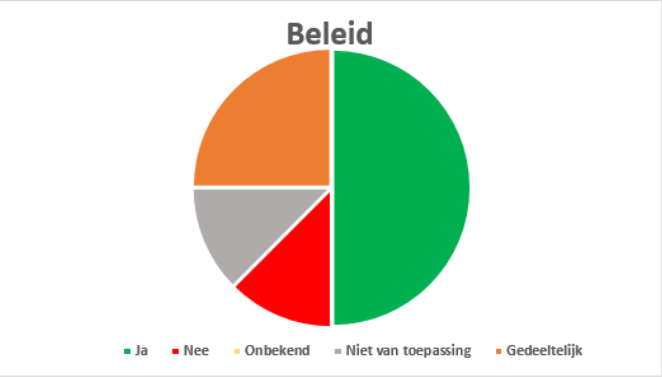
2019

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



2020

Beleid	
Resultaat	**Aantal**
Ja	8
Nee	2
Onbekend	0
Niet van toepassing	2
Gedeeltelijk	4



Toelichting
Mede dankzij het bewustwordingstraject worden meer verwerkingen vooraf getoetst aan het geldende privacybeleid. Wel dient op termijn het externe privacybeleid te worden gespecificeerd en dient eveneens een intern privacybeleid te worden opgesteld.

Onderdeel Processen

2019

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

2020

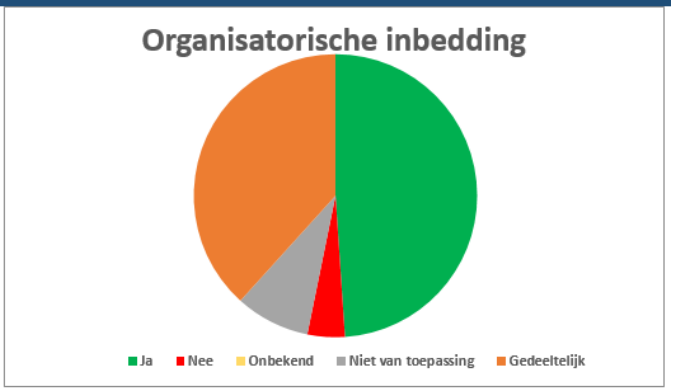
Processen	
Resultaat	**Aantal**
Ja	17
Nee	2
Onbekend	0
Niet van toepassing	4
Gedeeltelijk	12

Toelichting
Op dit onderdeel is weinig gewijzigd. Dit komt omdat nog wordt gewerkt aan het actualiseren van het register van verwerkingen, het uitvoeren van DPIA's en het lopende bewustwordingstraject.

Onderdeel Organisatorische inbedding

2019

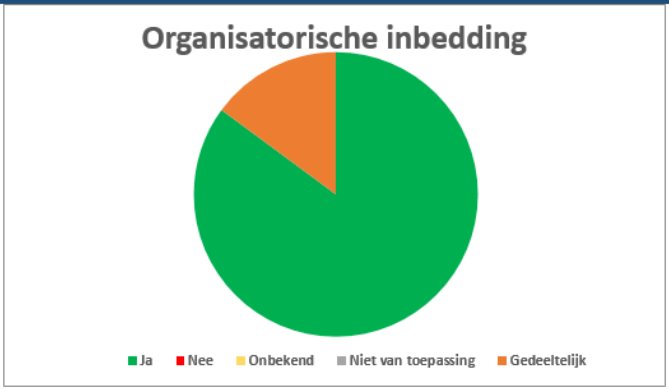
Organisatorische inbedding	
Resultaat	**Aantal**
Ja	23
Nee	2
Onbekend	0
Niet van toepassing	4
Gedeeltelijk	18



2020

Organisatorische inbedding

Resultaat	Aantal
Ja	40
Nee	0
Onbekend	0
Niet van toepassing	0
Gedeeltelijk	7



Toelichting
Door het bewustwordingstraject en het aanstellen van privacy-ambassadeurs zijn op dit onderdeel grote vorderingen te zien. De organisatie raakt steeds meer bewust van de regels rondom privacy en hoe de organisatie hiermee omgaat.

Onderdeel Rechten van betrokkenen

2019

Rechten van betrokkenen

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

2020

Rechten van betrokkenen

Resultaat	Aantal
Ja	25
Nee	1
Onbekend	0
Niet van toepassing	2
Gedeeltelijk	4

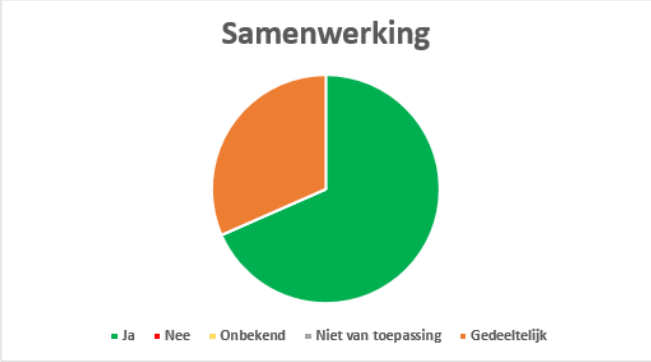
Toelichting
Betrokkenen kunnen hun rechten uitvoeren door middel van een heldere procedure die is ingebed in Zaaksysteem. Alle applicatiebeheerders worden automatisch bij de afhandeling van een verzoek betrokken en de FG verzorgt het uiteindelijke besluit.

Onderdeel Samenwerking

2019 en 2020

Samenwerking

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



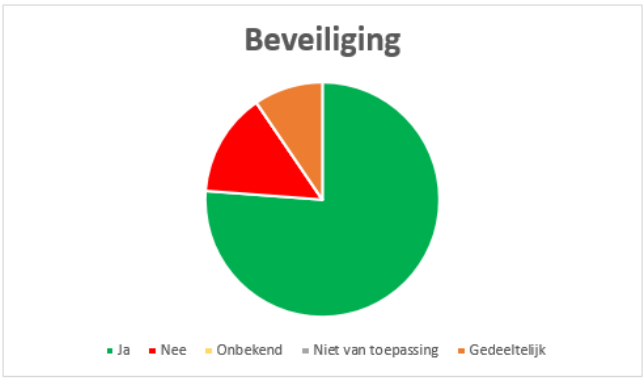
Toelichting
Op dit onderdeel is niets gewijzigd. Bij de actualisatie van het register van verwerkingen blijven we onderzoeken of inzichtelijk is wie onze verwerkers dan wel samenwerkings-partners zijn en of hiermee de juiste afspraken zijn gemaakt.

Onderdeel Beveiliging

2019

Beveiliging

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



2020

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

Toelichting
Op dit gebied is een kleine vooruitgang geboekt. Dit wil niet zeggen dat er weinig is ondernomen, maar zoals te zien in de grafiek is de beveiliging binnen de gemeente al goed op orde. Er worden verdere stappen gemaakt in de richting van een gemeentebreed autorisatiebeleid, logging en de controle hiervan.

Onderdeel Verantwoording

2019

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

2020

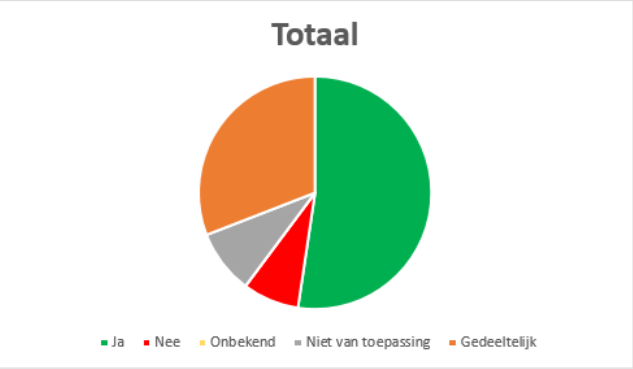
Verantwoording	
Resultaat	**Aantal**
Ja	17
Nee	1
Onbekend	0
Niet van toepassing	0
Gedeeltelijk	3

Toelichting
Op diverse gebieden worden periodieke controles uitgevoerd en de organisatie wordt geïnformeerd over de bevindingen en eventuele aanpassingen.

Totaaloverzicht

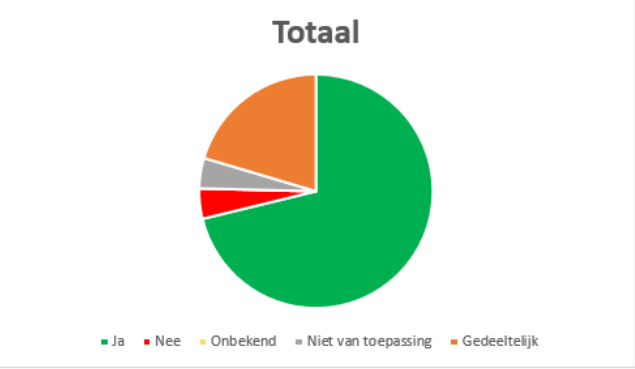
2019

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



2020

Totaal	
Resultaat	**Aantal**
Ja	136
Nee	8
Onbekend	0
Niet van toepassing	8
Gedeeltelijk	39



Toelichting
Hier is goed te zien dat afgelopen jaar stappen zijn gezet. Het aantal vragen waarop in 2019 nog Nee moest worden geantwoord is in 2020 bijna gehalveerd. In 2019 konden we al ruim 52% van de vragen met Ja beantwoorden, in 2020 is dat gegroeid naar ruim 71%.

Bijlage 2. Overzicht DPIA'S

In 2020 zijn 2 verkorte DPIA's uitgevoerd bij het starten van nieuwe processen in Zaaksysteem. Het gaat hier om:

- Handhaving samenscholing
  Betreft NAW, geboortedatum en Burgerservicenummer
  Op basis van de noodverordening COVID-19

- Leermanagementsysteem (LMS)
  Betreft een dashboard per medewerker met daarin de persoonlijke leeromgeving waaronder afspraken over te volgen opleidingen. Deze DPIA loopt door in 2021
  Op basis van gerechtvaardigd belang

Daarnaast hebben we een volledige DPIA uitgevoerd op het softwarepakket ZIVVER. Dit pakket zorgt ervoor dat we beveiligde e-mails, inclusief grote bestanden, kunnen versturen. Na de DPIA is het pakket aangeschaft en in gebruik genomen.

Tevens is gestart met een DPIA voor cameratoezicht binnen de gemeente en het proces PGAx. Deze DPIA's lopen door in 2021.

Bijlage 3. Overzicht rechten van betrokkenen

Recht op inzage

In 2020 is één verzoek ingekomen omtrent inzage in verstrekking van persoonsgegevens. Verzoeker heeft een overzicht gekregen van de persoonsgegevens die wij verwerken met alle bijbehorende informatie.

Er is ook een verzoek ingekomen omtrent inzage in verstrekking van persoonsgegevens, maar dit ging feitelijk om het opvragen van een Burgerservicenummer. Hier was dus geen sprake van een formeel AVG-verzoek.

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

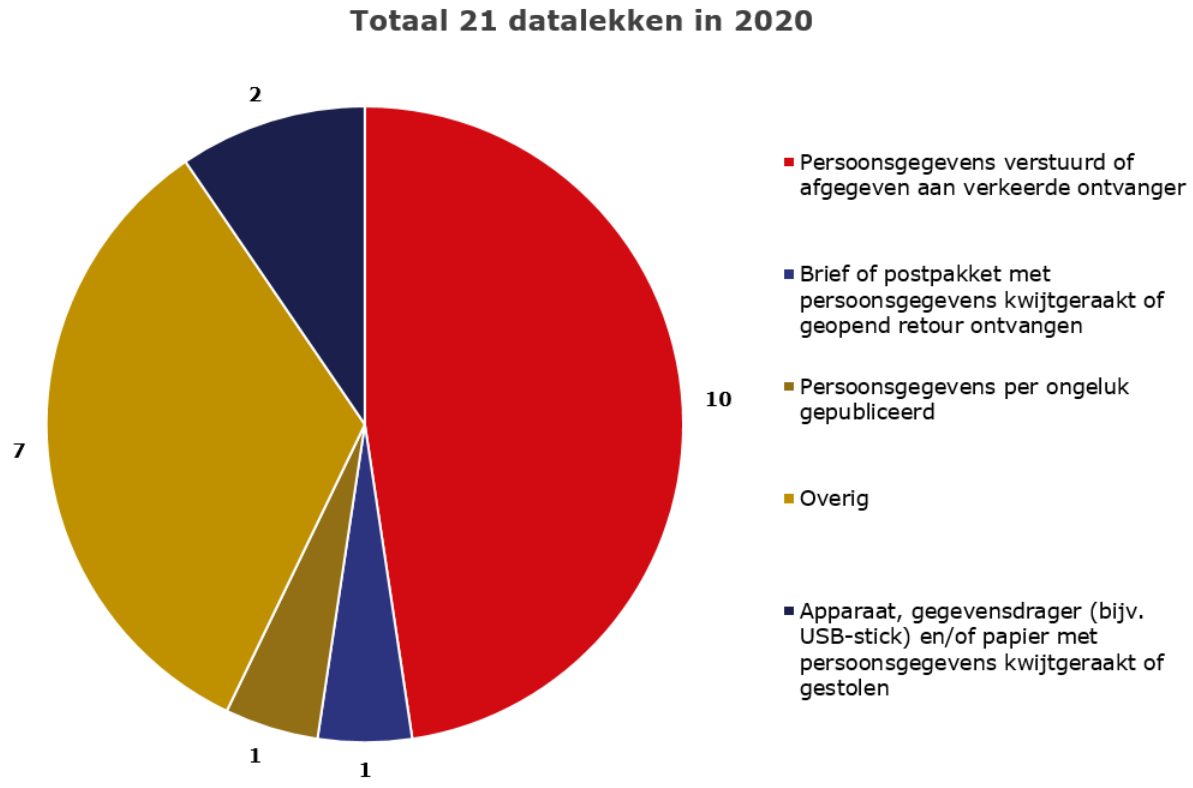
In 2020 is één verzoek ingekomen omtrent bezwaar tegen de gegevensverwerking. Het bezwaar was niet toegelicht, maar de verwerking waarop het betrekking kon hebben kent een wettelijke grondslag en hierdoor is het bezwaar afgewezen.

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 2020 zijn er 37 beveiligingsincidenten gemeld. Het is goed te zien dat er een piek ontstaat in het aantal meldingen op de momenten dat in het bewustwordingstraject specifieke aandacht is besteed aan dit onderwerp.

Van deze 37 meldingen zijn er 21 gekwalificeerd als een datalek, hieronder gespecificeerd naar de meest voorkomende categorieën.



Het gaat om de volgende zaken:

- Poststuk kwijtgeraakt bij interne post. Postproces is aangepast. Datalek is gemeld bij AP en betrokkenen.
- Naam gepubliceerd bij verleende ontheffing. Procedure wordt hierop aangepast. Datalek is gemeld bij AP en betrokkene.
- Informatie via WhatsApp gedeeld met foutief telefoonnummer. Betrof omissie derde partij. Afdeling zal letten op delen van zo min mogelijk informatie voordat nummer is geverifieerd. Datalek gemeld bij AP.
- Algemene mappen op de netwerkschijven zijn gecontroleerd op persoonlijke informatie. Waar nodig zijn mappen verplaatst dan wel verwijderd. Tevens aandacht besteed aan opties voor delen informatie. Datalek gemeld bij AP.
- Vertrouwelijk stuk van HRM blijven liggen bij printer. Door medewerker gevonden en direct teruggegeven. Gegevens zijn dus niet buiten de organisatie terecht gekomen en slechts door één 'onbevoegde' medewerker ingezien. Betreft een omissie van een individuele medewerker die hier voortaan beter op zal letten. Datalek gezien lage impact niet gemeld bij AP en betrokkene.
- Oude dossiers met daarin persoonsgegevens lagen vrij toegankelijk voor medewerkers in een kast in het gemeentehuis. De dossiers zijn direct op juiste wijze gearchiveerd. Kans dat onbevoegden de gegevens hebben ingezien is nihil, datalek daarom niet gemeld bij AP en betrokkenen.
- Factuur met bedrijfsgegevens naar foutieve crediteur verzonden. Het betreft zakelijke contactgegevens en ontvanger heeft e-mail op verzoek verwijderd. Datalek daarom niet gemeld bij AP en betrokkene.
- Tweemaal is een document geplaatst in het verkeerde personeelsdossier. Procedure is hierop aangepast. Toegang slechts door netwerkmanager, niet door medewerker. Risico voor betrokkene nihil, datalek daarom niet gemeld bij AP en betrokkene.
- Informatie intern te breed gedeeld, echter wel alleen met direct betrokken professionals. Betreft een omissie van een individuele medewerker die hier voortaan beter op zal letten. Risico voor betrokkene nihil, daarom niet gemeld bij AP en betrokkene.
- Brief met gezondheidsgegevens aan foutieve persoon gestuurd. Betreft een omissie van een individuele medewerker die hier voortaan beter op zal letten. Datalek is gemeld bij AP en betrokkene.
- Bij het versturen van een e-mail vanuit het Zaaksysteem werden irrelevante namen en e-mailadressen getoond. Deze gegevens zijn in principe wel voor medewerkers te raadplegen, alleen zou niet via deze weg moeten zijn. Betreft fout in systeem en is opgelost door de leverancier. Melden was niet aan de orde.
- Namen gedeeld met convenantpartners, terwijl cases anoniem worden besproken. Betreft een omissie van een individuele medewerker die hier voortaan beter op zal letten. Het proces is hier eveneens op aangepast. Risico voor betrokkene in dit geval nihil, daarom niet gemeld bij AP en betrokkenen.
- Persoonsgegevens gedeeld met partner, maar dit bleek achteraf onjuist te zijn. Partner direct verzocht gegevens te verwijderen. Datalek is gemeld bij AP en betrokkene.
- Document verzonden naar verkeerde medewerker. Betreft een omissie van een individuele medewerker die hier voortaan beter op zal letten. Document niet geopend door ontvanger, risico voor betrokkene nihil. Datalek daarom niet gemeld bij AP en betrokkene.
- Tweemaal een e-mail aan diverse inwoners verstuurd met e-mailadressen in het aan/cc-veld in plaats van in het bcc-veld. Betreft een omissie van twee individuele medewerkers die hier voortaan beter op zullen letten. Risico voor betrokkenen minimaal te noemen, datalek niet gemeld aan AP.
- Informatie in MS Teams was intern te breed zichtbaar, betrof bijvoorbeeld namen van cliënten in verband met gemaakte afspraken. Verder geen inhoudelijke informatie. Direct na constatering kanaal dichtgezet en risico afgedicht. Datalek niet gemeld aan AP en betrokkenen.

- Een medewerker is een zakelijke telefoon verloren. Op de telefoon zat encryptie. Tevens is direct melding gemaakt van het kwijtraken en is de telefoon op afstand leeggemaakt. Datalek niet gemeld bij AP.
- Een medewerker is een privé telefoon verloren met daarop Outlook en Authenticator. Het wachtwoord voor Office365 is succesvol gereset en de medewerker is afgemeld voor alle sessies. Datalek niet gemeld bij de AP.
- Medewerkers die geautoriseerd zijn voor het financiële pakket kunnen meer facturen zien dan die voor hun team zijn bedoeld. Gegevens blijven intern, maar de leverancier gaat dit verder afschermen. Datalek niet gemeld bij de AP.