Gegevensbescherming

JAARRAPPORTAGE 2019-2020



gemeente
GENNEP

Inhoudsopgave

1 juni 2021

Opgesteld door mr. F.M.H. Croonen, Functionaris Gegevensbescherming van de gemeente Gennep.

Samenvatting

Sinds 25 mei 2018 is de Algemene Verordening Gegevensbescherming (verder: AVG) van kracht. Vanaf dat moment houdt de Functionaris Gegevensbescherming (FG) intern toezicht op de toepassing van deze wet. Met de jaarrapportage legt de FG verantwoording af over het gevoerde toezicht.

Het college van burgemeester en wethouders (verder: het college) is verantwoordelijk voor het merendeel van de verwerkingen van persoonsgegevens in onze organisatie. Dit brengt verplichtingen met zich mee. In deze jaarrapportage staat beschreven welke maatregelen de gemeente Gennep in 2019 en 2020 heeft genomen om de doelstellingen en beginselen uit de AVG te behalen en te waarborgen. Ook bevat dit document aandachtspunten voor het jaar 2021 en 2022. Adequaat omgaan met persoonsgegevens is een blijvend en continue proces en zal dan ook aandacht blijven vergen van zowel bestuur, management als medewerkers.

Het algemene beeld is dat de gemeente Gennep de implementatie van de AVG heeft volbracht en grotendeels voldoet aan de wetgeving. Aan de hand van een 0-meting op de volgende 10 thema's uit de AVG is de mate waarin de gemeente voldoet onderzocht. Kort samengevat:

1. **Bewustwording** scoort goed. In samenwerking met de Privacy Officer (PO), Chief Information Security Officer (CISO), Technisch Informatie Adviseur (TIA) en de Functionaris Gegevensbescherming (FG) zijn grote stappen gezet met betrekking tot bewustwording en kennis om binnen de organisatie zorgvuldig en AVG-proof te werken, onder andere door middel van het opstellen van beleid en protocollen, het organiseren van workshops, het informeren via maandthema's en het organiseren van de jaarlijkse campagnes.
2. **Beleid** scoort voldoende. Er is een privacybeleid en een privacyverklaring vastgesteld, werkend en gepubliceerd. Domein-specifiek beleid is nog niet gereed.
3. Het **register van verwerkingen** is opgesteld. Van alle activiteiten/processen zijn de verwerkingen in beeld gebracht in een register van verwerkingen. Het register is van voldoende kwaliteit, maar behoeft nog aanvulling op een aantal onderdelen.
4. De **Functionaris Gegevensbescherming** (FG) en de Privacy Officer (PO) zijn aangesteld.
5. **Rechten van betrokken** zijn geborgd. Er is een procesbeschrijving omtrent de omgang met privacyrechten van inwoners opgesteld en werkend. Het actief informeren van betrokkenen behoeft verbetering.
6. Er is een methode beschikbaar van NOREA[1] om **Data Protection Impact Analyse (DPIA)** uit te kunnen voeren, maar gelet op het aantal uitgevoerde DPIA's moet de gemeente nog een substantiële inspanning verrichten om meerdere hoog-risico processen te auditen. De gegevensverwerkingen binnen de processen Wmo, Jeugdwet (JW) en Participatiewet (PW) in het sociaal domein en het zaaksysteem Djuma zijn onderworpen aan DPIA in 2019/2020.

[1] Beroepsvereniging IT-auditors.

7. **Privacy by design en default** zijn bedoeld om bij het procesontwerp privacyaspecten als dataminimalisatie en opslagbeperkingen standaard mee te nemen. Dit wordt toegepast binnen de organisatie. Dit moet nog wel vastgelegd worden in de procesbeschrijvingen.
8. Er is een protocol voor het **melden van datalekken**. Dit is document is intern bekend en werkend. Datalekken en beveiligingsincidenten zijn keurig gemeld door medewerkers en door de PO/CISO geregistreerd binnen de organisatie. Binnen de kaders van de wetgeving zijn ze gemeld bij de Autoriteit Persoonsgegevens.
9. Bij het sluiten van **verwerkersovereenkomsten** wordt gebruik gemaakt van het landelijke standaardmodel van de VNG. Dit wordt in de organisatie toegepast. Het overzicht van verwerkers en gesloten overeenkomsten wordt nog gerealiseerd.
10. **Toestemming** scoort nog onvoldoende. Voor de meest voorkomende, primaire diensten die de gemeente levert, bestaat de grondslag veelal uit de uitvoering van een wettelijke verplichting of het algemeen belang. Toch zijn er situaties waarbij toestemming expliciet gevraagd wordt aan de betrokkenen. Denk daarbij aan toestemming voor doeleinden zoals nieuwsbrieven, andere (niet wettelijke) voorzieningen of producten, het doen van tevredenheidsonderzoeken en enquêtes of het doorbreken van geheimhoudingsplicht. Of de toestemming ondubbelzinnig en actief is gegeven wordt nog onvoldoende aantoonbaar gemaakt. In het sociaal domein wordt de toestemming aantoonbaar gemaakt middels een algemeen formulier.

Nu de AVG is geïmplementeerd in de organisatie, dient de volgende uitdaging zich aan. Hoe blijft de gemeente voldoen en in controle? Aan de hand van de door de VNG ontwikkelde criteria en handvatten wordt de organisatie geadviseerd aan de slag te gaan met het borgen van de AVG. Hierbij rekening houdend met de schaal en ambities van de organisatie.

Randvoorwaarden voor het borgen en voldoen aan de wetgeving is de aanscherping van de positionering en rolverdeling in de organisatie. Het is een misvatting dat de FG of PO zorgdragen voor het geheel voldoen aan de wetgeving. Zij hebben een advies en faciliterende rol, maar de procesverantwoordelijken en de afdelingen zijn zelf verantwoordelijk voor de uitvoering en naleving. Het MT heeft zijn commitment gegeven aan de verdere optimalisatie van de AVG-doelstellingen in de organisatie.

Inleiding

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.

De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de privacyregels in Nederland. Daarnaast beschikt de gemeente Gennep over een interne toezichthouder: de **Functionaris voor de Gegevensbescherming** (FG). Met deze jaarrapportage beoogt de FG verantwoording af te leggen over de taak van de FG zoals die is vastgelegd in de AVG (art 39). In het kort omvat deze taak het informeren en adviseren van de medewerkers van de gemeente inzake hun verplichtingen, het uitoefenen van toezicht op naleving van de AVG, advisering over de uitvoering van DPIA en het onderhouden van contacten met de AP.

De verantwoording zoals in deze jaarrapportage is verwoord, gaat in op het algemene beeld over het jaar 2019 en 2020 en de adviespunten voor 2021 en 2022. De rapportage van de FG wordt aangeboden aan **het college van B&W,** omdat het eindverantwoordelijk is voor de verwerking van de persoonsgegevens. Het college neemt kennis van het rapport en neemt (indirect) besluiten over de realisatie en borging in de organisatie. Daarnaast kan het college de rapportage ter informatie aanbieden aan de **gemeenteraad**.

De criteria die in dit verslag zijn genoemd, zijn afkomstig uit het document ‘Het borgen van de Algemene Verordening Gegevensbescherming in de gemeentelijke organisatie’ van de Informatiebeveiligingsdienst/ VNG.

1 TERUGBLIK OP 2019 EN 2020

Op 25 mei 2018 is de AVG van kracht geworden. Er is een project opgesteld voor de implementatie van de maatregelen als gevolg van de AVG in de organisatie. De onderdelen worden fasegewijs uitgevoerd met als einddoel AVG-compliant te zijn. In dit deel van de rapportage een terugblik op wat in 2019 en 2020 is gerealiseerd.

1.1 BELEID

Op 28 november 2018 heeft de het college van burgemeester en wethouders van de gemeente Gennep het privacybeleid en –verklaring vastgesteld. Het **privacybeleid** geeft het kader waarin de gemeente Gennep persoonsgegevens verwerkt. Het laat zien hoe de gemeente omgaat met persoonsgegevens en welke maatregelen zij treft om te voldoen aan de relevante wet- en regelgeving. Het beleid en de verklaring zijn op de website van de gemeente te raadplegen.

1.2 PROCESSEN

De verwerkingen van persoonsgegevens van de gemeente Gennep moeten 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.

Gelet op de schaal van de gemeente Gennep zijn nog niet alle werkprocessen AVG-technisch in beeld gebracht. Door de medewerkers wordt bewust aandacht besteed aan de verwerking van persoonsgegevens (hoe zij daarmee omgaan), echter dit is niet aantoonbaar (op schrift) verwerkt in de beschrijving van de processen. De organisatie zal dit fasegewijs oppakken.

Er is een **register van verwerkingen** vastgesteld en gepubliceerd op de website. Dit register geeft een overzicht van alle verwerkingen van persoonsgegevens in de gemeentelijke processen. De PO zorgt voor het beheer van het register door jaarlijks aan de procesverantwoordelijke te vragen of er wijzigingen zijn. Van de procesverantwoordelijken wordt verwacht dat zij de PO actief informeren over wijzigingen.

De gemeente Gennep heeft een procesbeschrijving ‘**Rechten van betrokkenen op grond van de AVG’**. Hierin staat beschreven op welke wijze betrokkenen verzoeken tot inzage, wijziging, verwijdering en dergelijke in kunnen dienen en hoe de organisatie het verzoek behandelt.

Voor de meest voorkomende, primaire diensten die de gemeente levert, bestaat de grondslag voor het verwerken van persoonsgegevens veelal uit de uitvoering van een wettelijke verplichting of het algemeen belang. Toch zijn er situaties waarbij **toestemming** van de betrokkenen expliciet gevraagd moet worden. Denk daarbij aan toestemming voor doeleinden zoals nieuwsbrieven, het doen van tevredenheidsonderzoeken en enquêtes of het doorbreken van geheimhoudingsplicht. Om de toestemming aan te tonen wordt gebruik gemaakt van een (algemeen) formulier. Echter, blijkt uit dit

formulier onvoldoende de specifieke toestemming voor een bepaald doel. Het is te algemeen geformuleerd.

Een **DPIA** is verplicht voor processen en systemen met een hoog privacy-risico of waarin op grote schaal persoonsgegevens worden verwerkt. Hiervoor is een werkproces beschikbaar.

In 2019 is het zaaksysteem Djuma binnen de organisatie inwerking getreden. Het zaaksysteem is software waarmee regie wordt gehouden op lopende processen en geeft inzicht in de actuele status van een zaak. Binnen dit systeem worden op grote schaal persoonsgegevens verwerkt, waardoor een DPIA verplicht is en is uitgevoerd.

Ook is een DPIA uitgevoerd binnen het sociaal domein op de processen Wet maatschappelijke ondersteuning, Jeugdwet en Participatiewet. In deze processen worden op grote schaal (bijzondere) persoonsgegevens verwerkt van kwetsbare groepen in de gemeente. Hiermee zijn de risico's binnen deze kwetsbare processen in beeld. De resultaten van de DPIA's zijn in 2020 opgeleverd. De resultaten waren zeer positief met een aantal (kleine) verbetermaatregelen om de gegevens nog zorgvuldiger te verwerken. Daarnaast voert de VNG landelijk DPIA's uit op verwerkingen die bij gemeenten voorkomen, zoals voor de Wet geestelijke gezondheidszorg. De informatie gebruikt de organisatie om in het betreffende proces toe te passen.

Privacy by design en default zijn bedoeld om bij het procesontwerp privacyaspecten als dataminimalisatie en opslagbeperkingen standaard mee te nemen. Dit is in de praktijk toegepast bij bijvoorbeeld de inkoop van het zaaksysteem Djuma. Ook bij inkoop en aanbesteding diensten is aandacht voor privacy-aspecten.

1.3 ORGANISATORISCHE INBEDDING

Voor een goede en juiste uitvoering is het van belang dat een ieder 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 samenwerking met de CISO, PO en FG is het document **'Governance Privacy en Informatieveiligheid**' opgesteld. Dit document bevat een compacte beschrijving van rollen, taken en verantwoordelijkheden voor de bescherming van (persoons)gegevens en privacy. Dit document is verwerkt in het Informatiebeveiligingshandboek. Dit handboek is op 21 oktober 2020 vastgesteld door het Managementteam.

De CISO, FG, PO en TIA werken veelvuldig samen. Enerzijds omdat informatiebeveiliging en privacy nauw aan elkaar verbonden zijn. Anderzijds om op deze wijze technische en organisatorische maatregelen goed op elkaar afgestemd te krijgen en zo de gegevens nog beter te kunnen beschermen bij verwerkingen en in systemen. Daarnaast wordt samengewerkt bij beleidsplannen, protocollen, datalekken, beschermingsniveaus en de bewustwording binnen de organisatie.

Om medewerkers (nog) **bewuster** met privacygevoelige gegevens om te laten gaan, wordt er maandelijks een thema over privacy en informatieveiligheid op het intranet besproken. Hierbij kan bijvoorbeeld gedacht worden aan de vuistregels van de AVG, wachtwoordbeleid, veilig thuiswerken

en phishingmail. Daarnaast worden elk kwartaal workshops informatiebeveiliging en privacy georganiseerd voor de nieuwe medewerkers. Een keer per jaar wordt een “Dag van de Privacy en Informatieveiligheid” georganiseerd om de bewustwording aan te scherpen. In september 2019 is een tweedaagse escaperoom georganiseerd, waarin alle opdrachten gerelateerd waren aan vraagstukken rondom privacy en veilig werken. Aan deze interactieve sessie heeft 90% van de medewerkers deelgenomen. Het resultaat van deze sessie zeer positief. Uit interviews met een aantal deelnemers blijkt dat er veel bewuster met persoonsgegevens wordt gewerkt en ook veel kennis is blijven hangen over deze onderwerpen.

1.4 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 middels de bovenstaande rechten controle en invloed uit te oefenen over zijn of haar persoonsgegevens.

In 2019 is één verzoek tot inzage ingediend. Het overzicht is verstrekt. In 2020 zijn vier verzoeken tot inzage ingediend. De overzichten zijn verstrekt. Er is een verzoek tot wissen van persoonsgegevens ingediend. Dit verzoek is niet in behandeling genomen, wegens het uitblijven van legitimering van betrokkenen.

De gemeente dient betrokkenen **actief te informeren** over de persoonsgegevens die zij verwerkt. Hoewel dit in de uitvoering gebeurt, is dit niet aantoonbaar. Het moet in de processen worden beschreven. Deze aanbeveling vloeit voort uit de wettelijke verantwoordingsplicht uit de AVG. Hoe de gemeente omgaat met een verzoek over de privacy-rechten van betrokkenen, is vastgelegd in een procesbeschrijving. Hierin staat hoe een verzoek gedaan moet worden, wie verantwoordelijk is voor de behandeling, de termijnen en de criteria voor toe- of afwijzen van het verzoek.

1.5 SAMENWERKING

De gemeente Gennep werkt op meerdere beleidsterreinen, in verschillende rollen en hoedanigheden samen met (mede) overheden en private organisaties. In veel gevallen zal er 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 verwerken. Alle mogelijke vormen van verwerken moeten voldoen aan de AVG. De gemeente Gennep maakt dan ook afspraken met deze andere partijen.

De gemeente Gennep sluit **verwerkersovereenkomsten** -conform het VNG model- met de partijen die persoonsgegevens voor de gemeente verwerken.

1.6 BEVEILIGING

Vanuit het algemene behoorlijkheidsbeginsel, het integriteitsbeginsel en het vertrouwelijkheidsbeginsel is het essentieel dat de gemeente Gennep passende technische en organisatorische maatregelen neemt ter beveiliging van persoonsgegevens. Op dit onderdeel vindt nauwe samenwerking plaats met de CISO en TIA. Er is een Informatiebeveiligingsplan op basis van de ENSIA en BIO-normen.

Daarnaast geldt er onder de AVG een **meldplicht datalekken**. Dit houdt in dat ernstige inbreuken, zoals onbevoegde toegang, vernietiging of wijziging van persoonsgegevens gemeld dienen te worden aan de Autoriteit Persoonsgegevens (AP) en/of de betrokkene(n).

Kengetal:

Incidenten			
	2018	**2019**	**2020**
Datalekken gemeld bij AP	5	0	2
Incidenten intern geregistreerd	4	9	10

In 2020 zijn 2 datalekken gemeld bij de AP en 10 datalekken/data-incidenten intern behandeld. Het valt op dat het gross van de datalekken ontstaan, doordat een email naar het verkeerde emailadres wordt gestuurd. Dit kan eenvoudig gebeuren door dat er een . of _ ontbreekt(bijv piet.puk@ ipv pietpuk@). Daarnaast komt het voor dat de adressering op een brief onjuist is of personen voor een online vergadering niet via de bcc worden uitgenodigd. Niet alle beveiligingsincidenten zijn datalekken. Alleen de inbreuken die ernstige nadelige gevolgen hebben voor de bescherming van persoonsgegevens dienen bij de AP gemeld te worden. Alle incidenten worden intern geregistreerd, behandeld en lering uitgetrokken.

Het MT heeft in 2016 een Protocol ‘Meldplicht datalekken’ vastgesteld. De medewerkers zijn over de werkinstructie geïnformeerd in de workshops en in de jaarlijkse AVG campagne is hier extra aandacht voor. Medewerkers weten wat zij moeten doen in geval van een datalek of beveiligingsincident. Datalekken worden volgens het protocol behandeld.

1.7 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 het college aan moet kunnen tonen dat de verwerkingen van persoonsgegevens voldoen aan de beginselen van de AVG en aan de relevante wet- en regelgeving.

Het college beschikt over een privacybeleid, een informatiebeveiligingshandboek, een register van verwerkingen, een protocol datalekken en een incidentmanagementbeleid. De datalekken en

incidenten worden in een register bijgehouden. Rapportages en DPIA's zijn via zaaksysteem Djuma raadpleegbaar. De beveiliging van de persoonsgegevens is conform de ENSIA en de BIO. Door jaarlijks een GAP-analyse en een risicoanalyse uit te voeren is inzichtelijk waar maatregelen nodig zijn.

1.8 CONCLUSIE

De gemeente Gennep voldoet aan de basisvereisten van de AVG. Er zijn grote stappen gezet de afgelopen periode om de organisatie Privacyproof te maken. De organisatie beschikt over kennis, beleid, registers en processen. De organisatie mag daar trots op zijn.

Er is veel ondernomen om de kennis en het bewust zijn bij de medewerkers te vergroten en er wordt gewerkt volgens de algemene normen uit het Privacybeleid. Er is een register van verwerkingen, waarin alle activiteiten/processen in beeld zijn gebracht. De volgende stap is om de hoog-risico processen te onderwerpen aan een DPIA.

De Functionaris Gegevensbescherming (FG) en de Privacy Officer (PO) zijn aangesteld en werken nauw samen met de Chief Information Security Officer (CISO) en de Technisch Informatie Adviseur (TIA). Ook heeft de gemeente Gennep een proces omtrent het borgen van de rechten van betrokken. Privacy by design en default zijn bedoeld om bij het procesontwerp privacyaspecten als dataminimalisatie en opslagbeperkingen standaard mee te nemen. Dit wordt in de praktijk toegepast. Verder heeft de gemeente een protocol voor het melden van datalekken. Datalekken en beveiligingsincidenten zijn door de medewerkers keurig (intern) gemeld en door de PO/CISO geregistreerd binnen de organisatie. Binnen de kaders van de wetgeving zijn de datalekken gemeld bij de Autoriteit Persoonsgegevens.

De AVG eist niet alleen dat de organisatie zorgvuldig omgaat met de persoonsgegevens, maar ook dat dit aantoonbaar is. Dit betekent dat de wijze waarop de organisatie de AVG toepast in de werkprocessen moet zijn vastgelegd. Het borgen van de AVG vraagt de komende periode aandacht.

Het tweede deel van de rapportage worden aanbevelingen gedaan om de gegevensbescherming verder te optimaliseren en te borgen in de organisatie.

2 VOORUITKIJKEN NAAR 2021 EN 2022

Gegevensbescherming onderdeel laten worden van de organisatie, en daarmee aantoonbaar voldoen aan de relevante wet- en regelgeving, is geen afvinklijst, maar een continu proces. Waar de jaren 2019 en 2020 in het teken stonden van de implementatie van de AVG, zullen de komende jaren in het teken staan van het beheren en borgen van de AVG. Hierbij is het voldoen aan de verantwoordingsplicht een belangrijke opgave. Uit gesprekken en interviews blijkt dat de organisatie zorgvuldig omgaat met persoonsgegevens, maar in vastleggen (aantonen) dat er zodanig gehandeld wordt zijn we nog niet zo ver.

Op basis van een 0-meting[2] over de periode 2019-2020 uitgevoerd door de FG, is in beeld gebracht waar we staan op het gebied van gegevensbescherming en waar nog aandacht aan besteed moet worden. Op basis van deze meting worden de volgende aanbevelingen gedaan voor de komende periode.

2.1 BELEID

Niet alle processen hebben voldoende houvast aan een algemeen privacybeleid. Bijvoorbeeld in het sociaal domein en HRM zijn hoog risico activiteiten die een verdieping vragen. Daarnaast wordt er in de organisatie meer tijd- en plaats- onafhankelijk gewerkt. Dit brengt risico's op het gebied van privacy en informatieveiligheid met zich mee. Naast technische maatregen kan het opstellen van een werkinstructie de risico's verkleinen. Open en transparant bestuur staat soms op gespannen voet met de omgang met persoonsgegevens. Wanneer maken we gegevens wel en wanneer maken we ze niet openbaar? Een gedragscode voor de raad geeft hier houvast.

2.2 PROCESSEN

Het verantwoordingsprincipe uit de AVG houdt in dat iedere organisatie die persoonsgegevens verwerkt, moet kunnen laten zien op welke manier zij persoonsgegevens verwerkt. Uit interviews blijkt dat medewerkers zorgvuldig omgaan met de aan hen toevertrouwde gegevens. Het is belangrijk dat zowel de verwerkingen als de afwegingen geborgd worden in de processen, zodat de wijze van werken ook aantoonbaar is. Er geldt een documentatieplicht.

Het is verplicht dat DPIA's worden uitgevoerd op bestaande en nieuwe verwerkingen met hoog privacy-risico en bij de invoering van nieuwe processen en systemen. Een risicobeoordeling is draagt bij aan het in beeld brengen van de risico's zodat er maatregelen getroffen kunnen worden om de risico's te beheersen/verminderen. De gemeente beschikt over veel persoonsgegevens van inwoners. Het is de verantwoordelijkheid van de gemeente om zorg te dragen dat met deze gegevens zorgvuldig wordt omgegaan en dat zij niet in verkeerde handen vallen. De inwoners moeten op de gemeente kunnen vertrouwen. Dit vertrouwen kan door een incident eenvoudig afgebroken worden. Een datalek kan grote gevolgen hebben voor een inwoner, denk hierbij niet alleen aan fraude en

[2] VNG realisatie, Borgen van de AVG in de gemeentelijke organisatie.

financiële schade, maar ook het imago van deze persoon kan een flinke deuk oplopen. De gevolgen voor de gemeente zijn ook groot; verlies van vertrouwen, financiële- en imagoschade. Daarom zijn DPIA's zo belangrijk.

Er zijn slechts twee DPIA's uitgevoerd. Een (omvangrijke) DPIA in het sociaal domein op de processen Wmo, Jeugdwet en Participatiewet, omdat in deze werkprocessen veel persoonsgegevens van kwetsbare groepen worden verwerkt. Ook is het nieuwe zaaksysteem Djuma aan een DPIA onderworpen. De gemeente dient de komende jaren meer in te zetten op de het uitvoeren van DPIA's.

2.3 ORGANISATORISCHE INBEDDING

Binnen de organisatie is het belangrijk dat ieder zijn verantwoordelijkheid kent en neemt voor gegevensbescherming. De gezamenlijke verantwoordelijkheid is randvoorwaarde voor het succes van de AVG in de organisatie. De posities en rollen mogen worden verstrekt in de organisatie.

2.4 RECHTEN VAN BETROKKENEN

Met de inwerkingtreding van de AVG zijn de rechten van inwoners versterkt. Inwoners hebben verschillende rechten om controle te houden over hun persoonsgegevens. Gehoor geven aan inwoners die een beroep doen op hun privacy-rechten is een belangrijk onderdeel van een gezond privacybeleid en draagt bij aan het vertrouwen in onze organisatie.

Mede door de coronacrisis is er vraag ontstaan naar het doen van digitale verzoeken tot inzage. In het kader van fraudebestrijding is het belangrijk om de verzoeker te kunnen identificeren. Bijvoorbeeld door een webformulier met Digid-inlogsysteem.

Verder blijkt uit interviews met medewerkers blijkt dat zij betrokkenen actief informeren over de verwerking van persoonsgegevens, maar dat ondersteuning met informatiemateriaal nog een pré is.

2.5 SAMENWERKING

De gemeente werkt met veel partijen en ketenpartners samen. Het is belangrijk dat afspraken over gegevensdeling met deze ketenpartners worden vastgelegd. Wanneer deel ik wel of niet gegevens? Met welk doel doen we dit en op basis van welke grondslag mogen wij dit?

Met partijen, die gegevens voor de gemeente verwerken, worden verwerkersovereenkomsten gesloten. Het is belangrijk dat de gemeente inzichtelijk heeft welke partijen gegevens verwerken en met welke partijen gegevensdeling plaatsvindt, zodat goede afspraken gemaakt kunnen worden en dit gecontroleerd kan worden.

2.6 BEVEILIGING

De persoonsgegevens moeten goed beveiligd worden om datalekken en misbruik van informatie te voorkomen. De beveiliging is een continue punt van aandacht. Zowel binnen de organisatie als daarbuiten liggen beveiligingsinbreuken op de loer.

Van belang is dat de organisatie continue blijft investeren in de alertheid en bewustzijn van medewerkers bij het verwerken van persoonsgegevens en de veilige omgang met informatie.

Om datalekken en beveiligingsrisico's te verminderen is het opschonen van documenten en systemen (niet langer bewaren dan noodzakelijk) vereist. Ook het zorgvuldig autoriseren van medewerkers en het loggen van systemen en applicaties door de betreffende systeem- en applicatiebeheerders draagt aan de beveiliging bij. Tenslotte dient er aandacht te zijn voor privacy en beveiligingsaspecten in de ontwerpfase (privacy by design)van processen en applicaties. Door bij het ontwerp al rekening te houden met veilige en zorgvuldige verwerking (dataminimalisatie, bewaartermijnen) worden risico's verkleind. Ook door het gebruik van standaardinstellingen (privacy by default), zoals het verwijderen na afloop van de termijn, worden privacy-risico's verminderd.

2.7 VERANTWOORDING

De AVG-regels dwingen om goed na te denken over hoe de organisatie persoonsgegevens verwerkt en beschermt. De verantwoordingsplicht houdt in dat de organisatie kan aantonen dat de verwerkingen aan de regels voldoen. Het is een kwestie van in kaart brengen en documenteren. Dit betekent dat gegevensverwerkingen in processen en/of -beschrijvingen moeten worden geborgd. De FG en CISO leggen (gezamenlijk), (periodiek) verantwoording af over Informatieveiligheid en Privacy via de P&C-cyclus aan het college en de raad. Tevens wordt één keer in de tweejaar een uitgebreid verslag van de FG aan het college en raad aangeboden. Desgevraagd legt de organisatie verantwoording af aan de Autoriteit Persoonsgegevens.

2.8 CONCLUSIES

De gemeente Gennep mag trots zijn op de stappen die gezet zijn om de AVG in de organisatie te implementeren en op haar medewerkers die bewust en zorgvuldig omgaan met de persoonsgegevens van de haar inwoners. Informatiebeveiliging en privacy is echter wél een doorlopend proces dat continue aandacht vergt.

De organisatie moet zich bewust zijn van haar handelen en de privacygevoelige gegevens optimaal beschermen. Gelet op de schaal van de gemeente heeft het MT zich gecommitteerd aan het fasegewijs beheren en borgen van de AVG in de organisatie. Geadviseerd wordt om kennis, beleid en processen domein-specifiek op te pakken. Ondanks dat medewerkers zeer zorgvuldig en bewust omgaan met persoonsgegevens is deze (uniforme) werkwijze niet terug te vinden in processen en beschrijvingen (accountability). Ook het belang van DPIA's moet niet onderschat worden. Deze (verplichte) audits leveren een schat aan informatie op over hoe wij nog veiliger met de gegevens van onze inwoners om kunnen gaan. De gevolgen van datalekken en beveiligingsincidenten kunnen voor de inwoners en de gemeente enorm zijn.

De AVG is in het leven geroepen om de privacy van inwoners beter te beschermen. De gemeente dient zorgvuldig om te gaan met de toevertrouwde persoonsgegevens en moet dit kunnen aantonen. Het moet duidelijk zijn welke persoonsgegevens verwerkt worden en voor welk doel. De AVG versterkt de privacy-rechten van burgers. Onze inwoners moeten op de gemeente kunnen vertrouwen. Deze rapportage draagt hier aan bij. Het geeft inzicht in de naleving van deze wet en waar de organisatie nog aan kan werken. Met een zorgvuldige omgang van persoonsgegevens worden de risico's op data-incidenten en identiteitsfraude bij onze inwoners, medewerkers en partners voorkomen.