JAARRAPPORTAGE GEGEVENSBESCHERMING
GEMEENTE STEENWIJKERLAND 2018/2019

Datum: mei 2019
Versie: 1.0. CMT
2.0. B&W

Samenvatting

Het jaar 2018 was op het gebied van gegevensbescherming een bijzonder jaar voor organisaties en burgers, zo ook voor de gemeente Steenwijkerland. Op 25 mei 2018 werd namelijk de Algemene Verordening Gegevensbescherming (AVG) van kracht. De AVG verving de Wet bescherming persoonsgegevens (Wbp) en zorgt voor een verhoogde aandacht voor een rechtmatige verwerking van persoonsgegevens in alle sectoren. De overheid heeft hierin een belangrijke voorbeeldfunctie.

Het college van burgemeester en wethouders is verantwoordelijk voor het merendeel van de verwerkingen van persoonsgegevens in onze gemeente. De gemeentesecretaris draagt namens het college de verantwoordelijkheid dat de ambtelijke organisatie het gewenste niveau van privacybescherming vaststelt en uitvoert. Dit brengt verplichtingen met zich mee. In deze jaarrapportage staat beschreven welke acties en maatregelen de gemeente Steenwijkerland 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.

Samenvattend heeft de gemeente in 2018 veel werk verzet op het gebied van gegevensbescherming. Begin 2018 is door de kwartiermakende Functionaris voor Gegevensbescherming een Beleidsplan Privacy opgesteld. Ook zijn er bewustwordingssessies gehouden, waarin alle medewerkers op hoofdlijnen zijn geïnformeerd over de betekenis en de gevolgen van de AVG. Daarnaast zijn de volgende ‘verplichtingen’ uit de AVG gerealiseerd:

- Een geactualiseerde algemene privacyverklaring (art. 12 AVG)
- Verwerkersovereenkomsten met verwerkers en het ontwikkelen van een model Verwerkersovereenkomst (art. 28 AVG)
- Een register van verwerkingsactiviteiten (art. 30 AVG)
- Een proces met betrekking tot beveiligingsincidenten/(vermoedens van) datalekken (art. 33 en 34 AVG)
- Een register van beveiligingsincidenten/(vermoedens van) datalekken (art. 33, lid 5, AVG)
- Aanwijzen van een Functionaris voor Gegevensbescherming (art. 37 t/m 39 AVG)

De gemeenten Staphorst, Steenwijkerland, Westerveld en Zwartewaterland hebben gezamenlijk twee Functionarissen voor Gegevensbescherming (FG) aangesteld. De FG’s zijn tot eind 2018 gezamenlijk opgetrokken en vanaf 1 januari 2019 hebben de FG’s hun werkzaamheden ieder hoofdzakelijk gericht op twee gemeenten, zodat in elk van de vier gemeenten twee dagen in de week één FG aanwezig is. Maar ook buiten die twee dagen zijn de FG’s beschikbaar. De FG’s overleggen regelmatig en zijn elkaars achtervang.

Door het privacyteam is een meetinstrument gebruikt om een beeld te krijgen van de privacy-volwassenheid van de organisatie. Hieruit komt naar voren dat de gemeente nog niet voldoet aan de minimale eisen vanuit de AVG. In deel 2 van deze rapportage/jaarplan wordt beschreven wat er moet gebeuren om door te kunnen groeien naar een hoger privacy volwassenheidsniveau. Om dat te bereiken zal (het creëren van) bewustwording ook het komende jaar veel prioriteit krijgen. Daarnaast ligt de focus op de verdere organisatorische inbedding, het ontwerpen van processen ten aanzien van de rechten van betrokkenen (o.a. recht op inzage) en het vaststellen van autorisaties.

Tot slot kan het voorbereiden op de overkomst van taken vanuit de IGSD[1] naar de gemeente Steenwijkerland hier niet onbenoemd blijven. Zeker gelet op de aard en de hoeveelheid van de (persoons)gegevens die in het sociaal domein worden verwerkt, is een zorgvuldige voorbereiding hierop van groot belang.

[1] IGSD is de Intergemeentelijke Sociale Dienst Steenwijkerland en Westerveld waar uitvoering plaatsheeft vanuit o.a. Participatiewet, Wet Structuur Uitvoeringsorganisatie Werk en Inkomen en Wet Gemeentelijke schuldhulp-verlening. De IGSD houdt op te bestaan per 1-1-2020, waarna deze taken (weer) naar de gemeente Steenwijkerland komen.

Inhoudsopgave

Inleiding

De gemeente dient zorgvuldig om te gaan met persoonsgegevens. Gemeenten verwerken immers bij de uitoefening van hun taken veel informatie. Niet alleen persoonlijke informatie van eigen inwoners, maar ook van andere burgers, medewerkers, externen en zakenrelaties. 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 het college van burgemeester en wethouders 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 de gemeente Steenwijkerland te beschikken over een interne toezichthouder: de Functionaris voor de Gegevensbescherming (FG). Per 1 juli 2018 en 1 september 2018 zijn twee FG's benoemd voor de bestuursorganen van de gemeenten Staphorst, Steenwijkerland, Westerveld en Zwartewaterland.

Rol en taak 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 aangelegenheden die verband houden met de bescherming van persoonsgegevens. De gemeentesecretaris draagt namens het college de verantwoordelijkheid dat de ambtelijke organisatie het gewenste niveau van privacybescherming vaststelt en uitvoert. 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. Gelet op het privacyvolwassenheidsniveau van de organisatie is de FG de komende jaren ook kwartiermaker voor de implementatie van de AVG.

De FG brengt jaarlijks een verslag uit van haar werkzaamheden en bevindingen en doet naar aanleiding daarvan aanbevelingen. Dit jaarverslag is bedoeld voor het college van burgemeester en wethouders.

Leeswijzer

Deze jaarrapportage bestaat uit twee onderdelen. In het eerste deel wordt teruggekeken op het jaar 2018. Wat heeft de gemeente bereikt op het gebied van gegevensbescherming? Welke maatregelen zijn er genomen om te voldoen aan de AVG? In het tweede deel worden de aandachtspunten en actiepunten genoemd om gegevensbescherming en privacy in het jaar 2019 naar een 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.

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.

Privacybeleid

Het privacybeleid is het kader waarin de gemeente Steenwijkerland 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.

Begin 2018 heeft de kwartiermakende FG voor de gemeenten Steenwijkerland, Westerveld en Zwartewaterland een Beleidsplan Privacy opgesteld. Dit om in die gemeenten (die samen met de gemeente Staphorst in de loop van 2018 gezamenlijk twee FG's hebben aangesteld) zoveel mogelijk hetzelfde startpunt te hebben bij het van kracht worden van de AVG. In april 2018 is het Beleidsplan Privacy Steenwijkerland door het college vastgesteld. Dit beleidsplan bevat het algemene kader voor gegevensverwerkingen.

Om invulling te geven aan de informatieverplichting uit de AVG zijn in 2018 voorts de algemene privacy- en cookieverklaringen op de gemeentelijke website aangepast aan de eisen van de AVG. Ook is de privacyverklaring voor werknemers en sollicitanten geüpdatet.

Processen

De verwerkingen van persoonsgegevens van de gemeente Steenwijkerland 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 (art. 5 AVG). Daarnaast kan de gemeente in bepaalde gevallen verplicht zijn om een gegevensbeschermingseffectbeoordeling (DPIA[2]) uit te voeren. In het tweede deel van deze jaarrapportage wordt hier nader op ingegaan.

Om in beeld te krijgen of werkprocessen voldoen aan de beginselen van de AVG is in de eerste maanden van 2018 een register van verwerkingsactiviteiten opgesteld (art. 30 AVG). Dit register biedt een overzicht van alle processen waarbij persoonsgegevens worden verwerkt. Per proces is in het register beschreven wat het doel en de grondslag is van de verwerking, om welke categorieën van persoonsgegevens het gaat, of gegevens worden gedeeld met andere organisaties en wat de bewaartermijn is.

Het register van verwerkingsactiviteiten dient voor de FG tevens als instrument om op basis van een prioritering van de risico's toezicht te kunnen houden.

Organisatorische inbedding

Voor een goede en juiste uitvoering is het van belang dat eenieder 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 hebben de gemeenten Staphorst, Steenwijkerland, Westerveld en Zwartewaterland gezamenlijk twee FG's aangesteld. In 2018 zijn zij veelal gezamenlijk opgetrokken. Dit betekende in de praktijk dat de FG's gemiddeld één dag in de week gezamenlijk aanwezig waren bij elk van de vier gemeenten.

Om organisatiebreed bekendheid te geven aan de verantwoordelijkheden van de gemeente ten aanzien van gegevensbescherming en privacy zijn in 2018 informatieve bijeenkomsten georganiseerd en is regelmatig via intranet gecommuniceerd, bijvoorbeeld over het onderwerp datalekken.

In het Beleidsplan Privacy Steenwijkerland is beschreven dat op twee niveaus uitvoering wordt gegeven aan het privacybeleid: op concern- en op procesniveau. Op concernniveau vertaalt zich dat in de driehoek, bestaande uit de Functionaris voor Gegevensbescherming, de Chief Information Security Officer (CISO) en de Privacy Officer (PO). Op procesniveau was in het Beleidsplan Privacy een inhoudelijk coördinerende rol[3] toegekend aan de procesregisseurs.

---

[2] De gegevensbeschermingseffectbeoordeling wordt ook wel afgekort tot DPIA naar de Engelse term Data Protection Impact Assessment.

[3] Antenne- en signaalfunctie, nemen van beveiligingsmaatregelen, AVG toepassing in werkprocessen; tekeningsbevoegd verwerkersovereenkomsten.

Deze rol is tot op heden binnen de organisatie nog niet verder ingevuld. Dat komt ook omdat niet in elk team procesregisseurs zijn en per team de taken kunnen verschillen. Begin 2019 is een organisatieverandering ingezet, waarbij de inhoudelijk coördinerende rol van de procesregisseur wordt neergelegd bij de teamleiders. De teamleiders worden in de lijn integraal verantwoordelijk. Daarbij past dat de teamleiders ook verantwoordelijk zijn voor de verwerkingen met persoonsgegevens binnen hun team. De teams worden heringedeeld en de functies van de teamleiders worden opnieuw beschreven. Naar verwachting gaan de (nieuwe) teamleiders in het derde kwartaal van 2019 van start.

Er is een Privacy Governance vastgesteld door het CMT waarin is vastgelegd hoe en bij wie in de organisatie de verantwoordelijkheid ligt om te voldoen aan de AVG.

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 een aantal rechten controle en invloed uit te oefenen over zijn of haar persoonsgegevens.

De AVG kent betrokkenen een aantal rechten toe. In de privacyverklaring (www.steenwijkerland.nl/privacy) is opgenomen welke rechten betrokkenen hebben (o.a. het recht op inzage) en op welke manier een verzoek kan worden ingediend. In 2018 zijn geen verzoeken ingediend.

Samenwerking

De gemeente Steenwijkerland werkt op meerdere beleidsterreinen, in verschillende bedrijfsfuncties, in diverse rollen en hoedanigheden samen met (mede) overheden en private organisaties. In veelvoorkomende 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. Deze verwerkingen dienen dan ook te voldoen aan de AVG. De gemeente Steenwijkerland dient dan ook afspraken te maken met deze andere partijen.

Medio 2018 is in kaart gebracht welke organisaties persoonsgegevens verwerken in opdracht van de gemeente Steenwijkerland. Die organisaties zijn ‘Verwerker’ in de zin van de AVG, ten aanzien van de gemeente als ‘Verwerkingsverantwoordelijke’ in de zin van de AVG. Bij een verwerker kan bijvoorbeeld gedacht worden aan softwareleveranciers (van SaaS-oplossingen). De AVG bepaalt in artikel 28 dat er tussen een verwerkingsverantwoordelijke en een verwerker bepaalde zaken ten aanzien van de verwerking van persoonsgegevens moeten worden vastgelegd. In de regel geschiedt dat door het sluiten van een verwerkersovereenkomst.

Inmiddels is met ruim twintig verwerkers een verwerkersovereenkomst afgesloten. We maken daarbij in beginsel gebruik van de Standaard Verwerkersovereenkomst van de IBD/VNG-Realisatie. Overigens is de gemeente Steenwijkerland ook vertegenwoordigd in de Beheergroep Verwerkersovereenkomst van de IBD/VNG-Realisatie. Deze beheergroep houdt zich bezig met de doorontwikkeling van de Standaard Verwerkersovereenkomst, die met ingang van 2020 door alle gemeenten verplicht moet worden gebruikt.

Beveiliging

Vanuit het algemene behoorlijkheidsbeginsel, het integriteitsbeginsel en het vertrouwelijkheidsbeginsel is het essentieel dat de gemeente Steenwijkerland passende technische en organisatorische maatregelen neemt ter beveiliging van persoonsgegevens. Een voorbeeld van een technische maatregel die in 2018 is gerealiseerd ter bescherming van persoonsgegevens, is dat e-mails die gevoelige informatie bevatten nu beveiligd kunnen worden verstuurd. Het risico dat via de e-mail verzonden informatie door onderschepping in verkeerde handen terechtkomt, is daarmee veel kleiner gemaakt.

Onder de AVG geldt een zogeheten ‘meldplicht datalekken’. Dit houdt in dat beveiligingsincidenten onder omstandigheden gemeld dienen te worden aan de AP en/of de betrokkene(n). In 2018 is een procesbeschrijving opgesteld voor het melden van datalekken. Een (vermoeden van een) beveiligingsincident/datalek kan via een formulier op intranet eenvoudig intern worden gemeld. Het komt dan terecht bij de FG, CISO en PO. De eerste beoordeling vindt plaats door de PO en de CISO. Zij adviseren over te nemen maatregelen en stellen gezamenlijk een advies op aan de FG. De FG beslist uiteindelijk of het incident als datalek wordt gemeld aan de AP en of betrokkenen moeten worden geïnformeerd.

De AVG verplicht organisaties alle beveiligingsincidenten te documenteren. Ook de incidenten die niet worden gemeld aan de Autoriteit Persoonsgegevens, moeten worden gedocumenteerd. Er is daarom een register opgesteld waarin alle beveiligingsincidenten/datalekken worden geregistreerd. In 2018 hebben acht beveiligingsincidenten plaatsgevonden. Drie daarvan zijn als datalek gemeld aan de Autoriteit Persoonsgegevens.

In 2018 zijn er op het gebied van informatieveiligheid diverse bewustwordingsacties geweest, onder meer door workshops, een postercampagne en een clean-desk actie. Ook is er een werkvergadering met raadsleden geweest.

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 (sectorspecifieke) wet- en regelgeving.

Om aan de verantwoordings- (en informatie)plicht te voldoen, is – zoals hierboven reeds vermeld – een algemene privacyverklaring opgesteld, evenals een register van verwerkingsactiviteiten en een datalekkenregister. Ook vinden periodiek controles plaats om de technische beveiliging te testen en aan te kunnen tonen dat deze voldoet aan de daaraan gestelde eisen.

Conclusie

In 2018 heeft de gemeente Steenwijkerland heel wat werk verzet om de AVG te implementeren in de organisatie, de systemen en de processen. Een aantal acties en maatregelen waren zeer effectief, waaronder het houden van enkele sessies om medewerkers bekend te maken met de AVG (op hoofdlijnen) en bewustwording te creëren voor het zorgvuldig omgaan met persoonsgegevens. De hoeveelheid vragen die terechtkomt bij de Privacy Officer en de FG toont aan dat de bewustwording in de organisatie aan het toenemen is.

Daarnaast zijn er het afgelopen jaar de nodige stappen gezet om te kunnen voldoen aan de in de AVG neergelegde verantwoordingsplicht. Zo is er een register van verwerkingsactiviteiten en een (algemene) privacyverklaring opgesteld. Ook de processen ten aanzien van datalekken staan al goed in de verf.

De organisatie heeft de implementatie van de AVG nog niet gecompleteerd. Er zijn aandachtspunten voor de organisatie om verder en aantoonbaar te kunnen voldoen aan de AVG. In het tweede deel van de rapportage worden de actiepunten genoemd om in 2019 door te groeien naar een hoger privacy volwassenheidsniveau en gegevensbescherming ook 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 (het creëren van) bewustwording, de verdere organisatorische inbedding en het ontwerpen van processen ten aanzien van de rechten van betrokkenen.

Ook het voorbereiden op de overkomst van taken vanuit de IGSD naar de gemeente Steenwijkerland krijgt een hoge prioriteit. Zeker gelet op de aard en de hoeveelheid van de (persoons)gegevens die in het sociaal domein worden verwerkt, is een zorgvuldige voorbereiding hierop van groot belang.

Verder is van belang dat de technische en organisatorische beveiligingsmaatregelen voor het beschermen van persoonsgegevens worden vastgesteld, vastgelegd (in het register van verwerkingen) en uitgevoerd. Daarbij staat voorop dat een autorisatiematrix wordt gemaakt en beheerd. Dit is reeds in het Informatiebeveiligingsplan 2019 als actie benoemd en wordt opgepakt. Hierbij horen ook afspraken over loggen en het monitoren ervan.
De laatste prioriteit die in 2019 wordt opgepakt is het beantwoorden van vragen van medewerkers die betrekking hebben op invulling van de privacywetgeving voor hun eigen praktijk en voor de bescherming van hun eigen persoonsgegevens.

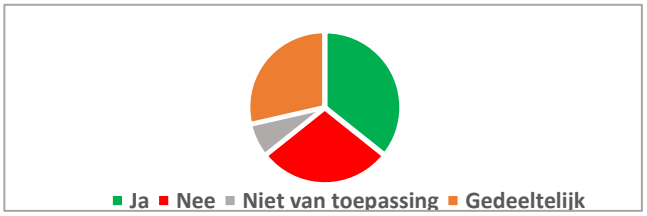
De top 6 prioriteiten voor 2019 op een rij:

- Bewustwording
- Organisatorische inbedding
- Processen voor de uitoefening van rechten van betrokkenen
- Integratie IGSD
- Technische en organisatorische beveiligingsmaatregelen voor het beschermen van persoonsgegevens vaststellen, vastleggen, uitvoeren en beheren.
- Interne communicatie over invulling van de privacywetgeving persoonsgegevens medewerkers

Om inzichtelijk te maken wat de huidige situatie is ten aanzien van het borgen van de AVG in de organisatie, is gebruik gemaakt van een meetinstrument. De cirkeldiagrammen geven aan wat de situatie eind 2018 was. Per onderdeel uit het meetinstrument wordt hieronder de doelstelling voor 2019 geformuleerd, evenals de daaraan gekoppelde acties die ervoor moeten zorgen dat de organisatie eind 2019 is doorgegroeid naar een hoger privacyvolwassenheidsniveau.

Privacybeleid

Figuur 1. Resultaat 2018 - onderwerp 'Privacybeleid'



Om de bekendheid met het privacybeleid en de geldende wet- en regelgeving te vergroten, worden ook in de eerste helft van 2019 workshops gehouden om bewustwording te creëren ten aanzien van een zorgvuldige omgang met persoonsgegevens. Ook wordt er op intranet een plek ingericht waar meer informatie komt te staan over privacy en gegevensbescherming, bijvoorbeeld over vragen als: wat is een datalek, en wat moet ik doen bij een datalek? Of: in welke gevallen moet er een Verwerkersovereenkomst worden gesloten? En wanneer moet een DPIA worden uitgevoerd? Ook is er behoefte aan een concrete vertaalslag: wat mag wel/niet volgens de privacywetgeving voor de bescherming van de persoonsgegevens van medewerkers. Voorbeelden hierbij zijn: een kaartje sturen naar zieke collega's en het hebben van een verjaardagenlijst. Op de interne website kan met een Q&A medewerkers worden aangegeven hoe het voldoen aan de AVG in de praktijk wordt ingericht, zodanig dat het ook werkbaar blijft.

In het privacybeleid maakt de gemeente duidelijk op welke manier zij met persoonsgegevens omgaat en welke uitgangspunten daarbij gelden. De komst van de AVG en andere ontwikkelingen op het gebied van privacy en gegevensbescherming maakt het noodzakelijk dat het privacybeleid periodiek wordt geactualiseerd. Het privacybeleid biedt een algemeen kader voor de gehele gemeentelijke organisatie. In de komende jaren zal vervolgens aandacht besteed moeten worden aan de domeinspecifieke uitwerking van het privacybeleid. Een zorgvuldige omgang met persoonsgegevens wordt namelijk niet alleen gereguleerd door de AVG. Ook sectorspecifieke wetgeving is hierop van invloed. Waar het bijvoorbeeld gaat om de privacy van werknemers, is dit deels ook in het arbeidsrecht geregeld. En voor het sociaal domein geldt dat de bepalingen uit de Wmo, Jeugd- en Participatiewet belangrijke kaders bieden.

	Actiepunten	Kwartaal				Wie
1	Workshops (i.s.m. informatiebeveiliging) voor alle medewerkers om bewustwording te creëren t.a.v. zorgvuldige omgang met persoonsgegevens		x			CISO/FG/PO
2	Actualiseren privacybeleid			x	x	PO/FG
3	Medewerkers zijn op de hoogte van de inhoud van het privacybeleid, o.m. door informatievoorziening op intranet			x	x	PO
4	Praktische invulling persoonsgegevens medewerkers Q&A		x	x		FG, PO
5	Het privacybeleid wordt actief uitgedragen door het concernmanagement en de teamleiders	x	x	x	x	CMT/TL

Processen

Figuur 2. Resultaat 2018 - onderwerp 'Processen'

In de eerste helft van 2019 worden processen uitgewerkt voor de rechten van betrokkenen (o.a. inzage- en correctieverzoeken en het elektronisch aanvragen ervan). Daarnaast krijgt het meer bekendheid geven aan de DPIA (Data Protection Impact Assessment) prioriteit. De AVG schrijft voor dat, wanneer een verwerking waarschijnlijk een hoog risico inhoudt, er een DPIA moet worden uitgevoerd. Een DPIA brengt de risico's in kaart van een bestaande en voorgenomen nieuwe verwerking van persoonsgegevens, evenals de maatregelen die kunnen worden getroffen om die risico's weg te nemen of te beperken. De werkprocessen die vanuit de IGSD overkomen naar de gemeente, en de inzet van Whatsapp voor klantcontact zijn voorbeelden van (nieuwe) verwerkingen waarop een DPIA uitgevoerd dient te worden. Medio 2019 volgt een voorstel op welke wijze het instrument DPIA in de organisatie wordt ingezet.

Met ingang van 2020 zullen processen vanuit de IGSD overkomen naar de gemeente Steenwijkerland. Deze processen worden in het tweede kwartaal van 2019 in kaart gebracht en uitgewerkt, waarbij het 'AVG-proof' maken van de processen de aandacht heeft.

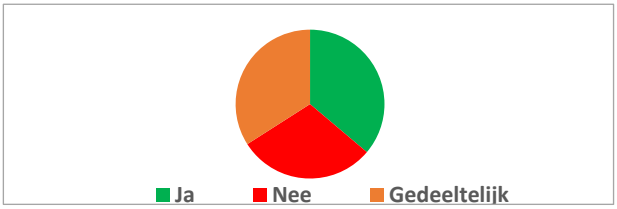
Als de nieuwe teamindeling in de loop van 2019 in de organisatie is doorgevoerd, wordt dat moment aangegrepen om een volgende kwaliteitsslag op het register van verwerkingsactiviteiten te maken. Aandachtspunten hierbij zijn het beschrijven van de technische en organisatie beveiligingsmaatregelen, het toekennen van eigenaarschap aan de teamleiders (TL's) en het uitwerken van de categorieën persoonsgegevens.

Voorwaardelijk voor het actualiseren van het verwerkingsregister is dat helder beschreven is welke processen bij welk team liggen en wie de proceseigenaar van welk proces is.

	Actiepunten	Kwartaal				Wie
1	Processen uitwerken voor uitoefening van rechten van betrokkenen (o.a. recht op inzage)		x	x		PO/Burgerzaken
2	Voorstel over hoe invulling te geven aan het instrument DPIA (wanneer en hoe in te zetten)		x			FG
3	AVG-proof inrichten werkprocessen die overkomen vanuit IGSD		x	x		Werkgroep werkprocessen/PO/ FG
4	Actualiseren en aanvullen register van verwerkingsactiviteiten			x	x	TL's /PO
5	In kaart brengen welke verwerkingen een hoog privacy risico opleveren				x	FG
6	Toetsen rechtmatigheid van verwerkingen (aan de hand van het verwerkingsregister)				x	FG

Organisatorische inbedding

Figuur 3. Resultaat 2018 - onderwerp 'Organisatorische inbedding'



Om hun zichtbaarheid binnen de vier gemeentelijke organisaties te vergroten, hebben de twee FG's er met ingang van 2019 voor gekozen zich op te splitsen en zich ieder hoofdzakelijk op twee gemeenten te richten. Zij overleggen wel regelmatig en fungeren als elkaars achtervang bij afwezigheid.

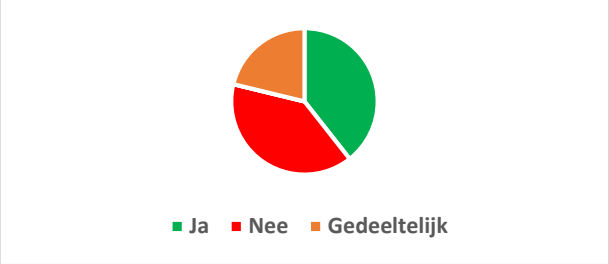
In 2018 is privacy veelal projectmatig aangevlogen. Voorkomen moet echter worden dat privacy wordt gezien als iets van de driehoek FG, CISO en PO. In 2019 ligt daarom prioriteit bij het benadrukken van de lijnverantwoordelijkheid. Door de aanpassingen in de organisatie verdient de verdeling van rollen, taken en verantwoordelijken, zoals neergelegd in het Beleidsplan Privacy Steenwijkerland, een nadere uitwerking. Hiertoe is door de FG een Privacy Governance model opgesteld, waarin de recente ontwikkelingen in het kader van de organisatiestructuur zijn meegenomen. Op dit moment komen privacygerelateerde vraagstukken vanuit de hele organisatie veelal terecht bij de Privacy Officer. Vaak is echter niet alleen kennis van de AVG, maar juist ook kennis van sectorspecifieke wetgeving vereist. Het is daarom wenselijk om in de organisatie enkele privacy (en informatieveiligheid) ambassadeurs/-aanspreekpunten aan te wijzen (per domein). De Privacy Officer kan dan een meer coördinerende rol vervullen.

	Actiepunten	Kwartaal				Wie
1	Benadrukken en verder invulling geven aan lijnverantwoordelijkheid			x	x	TL, FG
2	Opstellen Privacy Governance model waarin rollen, taken en verantwoordelijkheden zijn beschreven en belegd		x			FG
3	Aanwijzen van privacy (en informatieveiligheid) ambassadeurs/-aanspreekpunten			x	x	TL

Rechten van betrokkenen

Figuur 4. Resultaat 2018 - onderwerp 'Rechten van betrokkenen'

Mensen zijn zich steeds bewuster van hun privacy en ook van de rechten die zij op dat gebied hebben. Het is dan ook niet de vraag óf er verzoeken worden ingediend op grond van de AVG, maar wanneer en hoeveel. In de eerste helft van 2019 zullen daarom (zoals hierboven onder het kopje 'processen' al is opgemerkt) processen worden uitgewerkt om de uitoefening van de rechten van betrokkenen binnen de daarvoor gestelde termijnen te faciliteren.



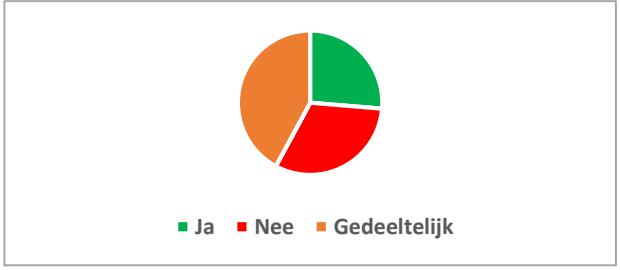
Een belangrijk speerpunt voor 2019 is ook het verder invulling geven aan de informatieverplichting uit de AVG. Die informatieverplichting brengt met zich mee dat voor betrokkenen duidelijk is welke gegevens worden verwerkt, hoe die gegevens worden verzameld, met welk doel, wat de grondslag is, aan wie de gegevens worden doorgegeven, hoe lang de gegevens worden bewaard, etc. Ook met het oog hierop is het noodzakelijk dat het register van verwerkingsactiviteiten actueel en volledig is.

	Actiepunten	Kwartaal				Wie
1	Verder inrichten en beleggen in de organisatie van de rechten van betrokkenen		x	x		PO, TL's

Samenwerking

Figuur 5. Resultaat 2018 - onderwerp 'Samenwerking'

Als samengewerkt wordt met externe partijen (of dat nu andere overheden of private organisaties zijn), zal er in veel gevallen ook sprake zijn van het 'verwerken van persoonsgegevens'. Het is in die situaties van belang dat allereerst duidelijk wordt hoe partijen zich tot elkaar verhouden om vervolgens te kunnen bepalen of en zo ja, welke afspraken tussen partijen moeten worden gemaakt ten aanzien van een zorgvuldige omgang met persoonsgegevens.



Om een voorbeeld te geven: als sprake is van een verwerkingsverantwoordelijke en een verwerker, dient een verwerkersovereenkomst te worden afgesloten. Daarvoor is een standaard model beschikbaar. Overigens is het beheer van verwerkersovereenkomsten een aandachtspunt in een breder kader (contractbeheer- en contractmanagement).

In andere situaties kan een basis voor gegevensuitwisseling in de wet worden gevonden. Soms bestaan er andere verhoudingen, zoals twee verwerkingsverantwoordelijken of een gedeelde verantwoordelijkheid. In dat geval moeten afspraken over het veilig omgaan met persoonsgegevens in de hoofdovereenkomst worden

gemaakt of dienen afspraken te worden vastgelegd in een protocol of convenant om gegevensuitwisseling mogelijk te maken.

De praktijk leert dat dit zeer nauw luistert. Het is daarom van belang dat, wanneer wordt samengewerkt met externe partijen, de PO en de FG vroegtijdig om advies worden gevraagd. Ook door informatievoorziening op intranet en in workshops, kan op dit punt nog een belangrijke stap worden gezet.

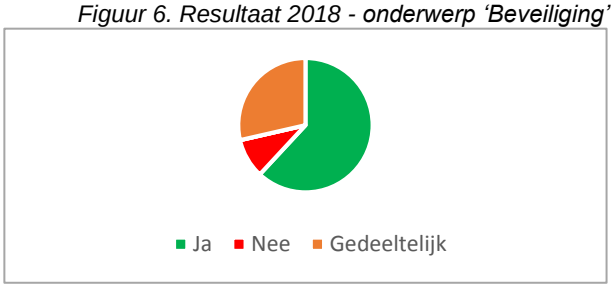
Door in een zo vroeg mogelijk stadium alert te zijn op hoe partijen zich tot elkaar verhouden en op welke wijze persoonsgegevens worden uitgewisseld en verwerkt, wordt voorkomen dat zaken achteraf gerepareerd moeten worden. Samen met de inkoop- en aanbestedingsadviseur wordt daarom bezien op welke manier standaard inkoopdocumenten hieraan kunnen bijdragen.

Tot slot verdient het aanbeveling de Verordening gegevensverstrekking BRP te actualiseren.

	Actiepunten	Kwartaal				Wie
1	Organisatiebreed onder de aandacht brengen van de Standaard Verwerkersovereenkomst		x	x	x	FG/PO/CISO/ Inkoop- en aanbestedings-adviseur
2	Adviseren over (on)mogelijkheden incidentele en structurele gegevensverstrekkingen aan/door externe partijen	x	x	x	x	FG/PO
3	Aanpassing standaard inkoopdocumenten zodat privacygerelateerde vraagstukken vroegtijdig in beeld komen			x		PO/Inkoop- en aanbestedings-adviseur
4	Actualiseren Verordening gegevensverstrekking BRP			x	x	TL Ontvangst/PO

Beveiliging

Figuur 6. Resultaat 2018 - onderwerp 'Beveiliging'



Op het gebied van beveiliging is reeds het nodige gerealiseerd. Op basis van in 2018 uitgevoerde risicoanalyses is het jaarplan informatiebeveiliging 2019 opgesteld, waarin specifieke acties en maatregelen op het gebied van informatiebeveiliging staan opgenomen.

Bij (nieuwe) verwerkingen en de aanschaf van nieuwe systemen zal in het bijzonder aandacht moeten zijn voor de in de AVG verankerde uitgangspunten 'privacy by design' en 'privacy by default'. Hiermee wordt bedoeld dat al bij het ontwerp van nieuwe systemen rekening wordt gehouden met de privacy van betrokkenen en dat de standaardinstellingen zo privacyvriendelijk mogelijk zijn. Het beginsel van dataminimalisatie hangt hier nauw mee samen. Dit betekent dat niet meer gegevens worden uitgevraagd dan voor het doel noodzakelijk is.

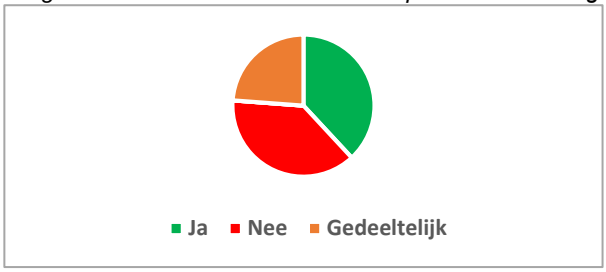
In 2018 is een procesbeschrijving voor datalekken opgesteld. Daarin is ook vastgelegd onder welke omstandigheden dient te worden opgeschaald naar de securityboard. In het vierde kwartaal van 2019 zal een crisiscommunicatieplan worden opgesteld voor datalekken die (mogelijk) een hoog risico voor de privacy van betrokkenen betekenen.

Eén van de uitgangspunten van de AVG is dat goed geborgd is dat alleen degenen die de persoonsgegevens voor de uitvoering van hun werk nodig hebben, hier toegang tot hebben. Daarom is het belangrijk om autorisaties vast te leggen en actief te monitoren, te loggen en te beheren. Dit speelt bijvoorbeeld bij in- en uitdiensttreding en verandering van functie.
Omdat in het zaaksysteem veel persoonsgegevens worden geregistreerd, moet geborgd worden dat alleen de medewerker die vanuit zijn functie toegang tot een dossier moet hebben, de zaak kan inkijken en de daarbij behorende rechten heeft. Dit wordt ook opgepakt vanuit het Informatiebeveiligingsplan 2019.

	Actiepunten	Kwartaal				Wie
1	Beginsel van 'dataminimalisatie' en de uitgangspunten 'privacy by design & privacy by default' organisatiebreed onder de aandacht brengen			x	x	FG/PO/CISO
2	Uitvoering geven aan jaarplan informatiebeveiliging 2019	x	x	x	x	CISO
3	Vastleggen en actualiseren autorisaties in geautomatiseerde systemen, w.o. zaaksysteem			x	x	TL's / CISO

Verantwoording

Figuur 7. Resultaat 2018 - onderwerp 'Verantwoording'



De AVG verplicht organisaties, veel meer dan zijn voorganger de WBP, de naleving van de belangrijkste beginselen uit de wet- en regelgeving aan te kunnen tonen. Deze verantwoordingsplicht vertaalt zich onder meer in een informatieplicht richting betrokkenen, het documenteren van alle beveiligingsincidenten en het bijhouden van een register van verwerkingsactiviteiten. In de onderdelen hierboven is duidelijk geworden dat er op dit punt een goed begin gemaakt is en het de komende jaren vooral zaak is om dit verder door te ontwikkelen.

De FG zal periodiek verslag uitbrengen aan de verantwoordelijke bestuursorganen over de omgang met persoonsgegevens binnen de gemeente. Naar aanleiding daarvan zullen acties en maatregelen worden vastgesteld voor de organisatie, zodat de komende jaren stappen gezet worden op de privacy volwassenheidsladder.

	Actiepunten	Kwartaal				Wie
1	Periodiek rapporteren aan college over omgang met persoonsgegevens	x	x	x	x	FG
2	Aan CMT acties en maatregelen voorleggen uit het jaarplan gegevensbescherming 2019, om door te groeien naar een hoger privacyvolwassenheidsniveau		x			FG

Conclusie

Op het gebied van privacy en gegevensbescherming is er in 2019 winst te behalen. Doorgroeien naar een hoger privacyvolwassenheidsniveau, door uitvoering te geven aan de acties uit dit jaarplan, is de doelstelling. Om die doelstelling te behalen, za (het creëren van) bewustwording ook het komende jaar veel prioriteit krijgen. Daarnaast ligt de focus op de verdere organisatorische inbedding en het ontwerpen van processen ten aanzien van de rechten van betrokkenen en het nemen van technische en organisatorische beveiligingsmaatregelen. Ook wordt in 2019 prioriteit gegeven aan het (binnen de organisatie) communiceren over de bescherming van de persoonsgegevens van medewerkers en een werkbare invulling ervan naar de praktijk. En uiteraard krijgt een zorgvuldige voorbereiding op de overkomst van taken vanuit de IGSD naar de gemeente Steenwijkerland prioriteit. Zeker gelet op de aard en de hoeveelheid van de (persoons)gegevens die in het sociaal domein worden verwerkt, is dit van groot belang.

De top 6 prioriteiten voor 2019 op een rij:

- Bewustwording
- Organisatorische inbedding
- Processen voor de uitoefening van rechten van betrokkenen
- Integratie IGSD
- Technische en organisatorische beveiligingsmaatregelen voor het beschermen van persoonsgegevens vaststellen, vastleggen en actief beheren.
- Interne communicatie over bescherming van de persoonsgegevens van medewerkers en werkbare invulling ervan.