JAARRAPPORTAGE GEGEVENSBESCHERMING GEMEENTE WOENSDRECHT 2019 en ONTWIKKELING 2020

Functionaris Gegevensbescherming
September 2020

Gebaseerd op IBD FG jaarrapportage v1.1 2020

Beknopte weergave ontwikkeling 2019 - 2020



Samenvatting

Het jaar 2019 was een interessant vervolg op het eerste jaar (2018) van de AVG. Inmiddels is de AVG in toenemende mate geïmplementeerd binnen de gemeente Woensdrecht. De verhoogde aandacht voor het beschermen van de privacy van burgers stond centraal. De (gemeentelijke)overheid heeft hierin een belangrijke voorbeeldfunctie.

De verantwoordelijkheden voor de gemeente Woensdrecht voor het verwerken van persoonsgegevens van burgers (en medewerkers) liggen in hoofdlijnen bij drie bestuursorganen, nl. de burgemeester, het college van B&W en de gemeenteraad.
Het college is verantwoordelijk voor het merendeel van de verwerkingen van persoonsgegevens binnen de gemeente. Dit brengt verplichtingen met zich mee. In deze jaarrapportage staat beschreven welke acties en maatregelen er in 2019 genomen zijn om de doelstellingen en beginselen uit de AVG te behalen en te waarborgen. Ook bevat dit document aandachtspunten en actiepunten voor de toekomst. Adequaat, verantwoord en rechtmatig omgaan met persoonsgegevens is een blijvend proces en zal dan ook structureel aandacht blijven vergen van zowel bestuur, management als medewerkers.

In 2019 is er binnen de gemeente Woensdrecht heel wat werk verzet om de AVG te implementeren in de organisatie, de systemen en de processen.
De introductie van de zgn. 'leercirkels' was zeer effectief, in die zin dat de privacy bewustwording van de medewerkers kon worden vastgesteld. Deze bleek sinds de voorgaande meeting aantoonbaar gestegen te zijn.
De rol van Privacy Officer (PO) is ingevuld. De PO is een belangrijke schakel tussen de uitvoerende organisatie en de Functionaris Gegevensbescherming (FG). Daarnaast geeft hij operationeel invulling aan het intern borgen van de privacy vereisten en ondersteunt daarbij het verantwoordelijke lijnmanagement. Een gevolg is dat de FG zich kan richten op de invulling van de zuivere FG rol. De PO wordt weer ondersteund door de privacy teamleden. Dit zijn medewerkers verdeeld over de diverse afdelingen, en zij fungeren als privacy ambassadeurs.
Het privacy beleid is herzien. Daarbij heeft de gemeente onder andere een standpunt ingenomen en vastgelegd omtrent haar ambitie t.a.v. volwassenheid op het gebied van privacy en bescherming van persoonsgegevens. Het college heeft als doelstelling vastgelegd, het volwassenheid niveau 3 op een schaal van 5, te willen bereiken in een termijn van 2 jaar. Dit is 2022. Medio 2019 is het volwassenheidsniveau vastgesteld op 1,2. Medio 2020 is dit 1,8. Voor alle duidelijkheid; volwassenheidsniveau 3 betekent dat er in de basis voldaan wordt aan de AVG.

Over het algemeen kan gesteld worden dat de gemeente op de goede weg is om aantoonbaar te voldoen aan de AVG. In het proces dat de gemeente en haar medewerkers hierbij doorlopen, en de voortgang, wijkt niet noemenswaardig af van dat van andere vergelijkbare gemeenten.

Op het gebied van privacy en gegevensbescherming is er in 2020 zeker nog winst te behalen. Met name het vroegtijdig betrekken van de privacy functionarissen bij nieuwe initiatieven door zowel college als management gaat dit opleveren. Dit zorgt nl. voor een tijdige toetsing van deze initiatieven aan de AVG vereisten. Niet als rem maar als belangrijke randvoorwaarde en toetsingskader. In dit verband wordt er aandacht gevraagd voor de samenwerkingsverbanden met andere gemeenten, netwerkorganisatie en overige. Niet in alle gevallen is de grondslag voor gegevensuitwisseling helder of de onderlinge verhoudingen van de deelnemende partijen en daarmee de afzonderlijke verantwoordlijkheden op het gebied van beheer, toegang, honoreren van rechten van betrokkenen en het correct omgaan met datalekken. Daarnaast is er zonder een duidelijke doelomschrijving kans op ongewild of ongeoorloofd gebruik van betrokkene persoonsgegevens. De Autoriteit

Persoonsgegevens heeft samenwerkingsverbanden als aandachtpunt opgenomen in haar focus document 2020-2023. Gemeente Woensdrecht is hieromtrent zeker nog niet in control.

.

Dataminimalisatie verdient meer aandacht. Daarmee wordt bedoeld dat medewerkers alleen die data verzamelen die nodig zijn voor de uitvoering van hun taak. Screening van de gegevens uitvraag is daarbij een eerste stap.

Ook verdient het actueel houden van het register van verwerkingen de nodige aandacht. Dit register kan gezien worden als een van de brondocumenten als het gaat om het aantoonbaar voldoen aan de AVG.

Het DPIA instrument (Data Protection Impact Assessment) wordt nog niet tot nauwelijks actief en tijdig gebruikt om risico's van de verschillende verwerkingen van persoonsgegevens in kaart te brengen, adequate beveiligingsmaatregelen te treffen, en dit ook controleerbaar vast te leggen. Ook al is dat in een bepaalde gevallen verplicht. Hier is de AVG aantoonbaarheidseis nadrukkelijk van toepassing. De gemeente geeft, door dit instrument wel te gebruiken, aan in control te zijn.

Tot slot zal er op korte termijn begonnen moeten worden met het inrichten van een PDCA cyclus om zo periodiek alle AVG vereisten, als onderdeel van de managementcyclus, te toetsen en evt. bij te stellen.

Het college en management zullen hun afzonderlijke verantwoordelijkheid moeten nemen en deze invulling geven, als proceseigenaren, om het geambieerde volwassenheidsniveau te bereiken.

INHOUDSOPGAVE

INLEIDING 6

LEESWIJZER 6

DEEL 1. TERUGBLIK OP 2019 8

BELEID 8

PROCESSEN 8

ORGANISATORISCHE INBEDDING 9

RECHTEN VAN BETROKKENEN 9

SAMENWERKING 10

BEVEILIGING 10

VERANTWOORDING 11
CONCLUSIE 11
DEEL 2. VOORUITKIJKEN NAAR 2020 13
BELEID 13
PROCESSEN 13
ORGANISATORISCHE INBEDDING 15
RECHTEN VAN BETROKKENEN 16
SAMENWERKING 16
BEVEILIGING 17
VERANTWOORDING 17
CONCLUSIE 17
BIJLAGE 1 - STAND VAN ZAKEN AVG PER ONDERWERP 19
BIJLAGE 2 - OVERZICHT UITGEVOERDE DPIA'S 20
BIJLAGE 3 - OVERZICHT BEROEP OP RECHTEN VAN BETROKKENEN 21
BIJLAGE 4 - OVERZICHT DATALEKKEN 22

Inleiding

De gemeente Woensdrecht is zich steeds meer bewust van het belang van het beschermen van persoonsgegevens van haar burgers. Er worden immers bij de uitoefening van onze taken veel (privacy gevoelige) gegevens verwerkt van veel (kwetsbare) burgers in veel verschillende domeinen. Daarbij is ook aandacht voor persoonsgegevens 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 worden verwerkt, voor welk doel en met welke grondslag. Tijdens de bewaarperiode van persoonsgegevens moeten ze goed worden beveiligd, mogen ze niet zomaar voor een ander doel worden verwerkt en moeten ze na afloop worden vernietigd of geanonimiseerd. Aanvullend hebben we 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 de verantwoordelijkheid van de burgemeester het college van B&W als ook de gemeenteraad vindt een groot aantal verwerkingen van persoonsgegevens plaats. Daar vindt externe en interne toezicht op plaats. De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de privacyregels in Nederland. Daarnaast dient de gemeente te beschikken over een interne toezichthouder: de Functionaris Gegevensbescherming (FG).
Op 1-4-2018 hebben de bestuursorganen van gemeente Woensdrecht[1] Paul Muller aangesteld als FG, die daarnaast ook actief was als FG voor de gemeente Steenbergen. Aanvullend is op 4-3-2020 Dries Wiersma aangesteld als FG. Beiden zijn nu actief als FG voor 5 gemeenten, nl, Woensdrecht, Steenbergen, Zundert, Rucphen en Halderberge.

[1] Hiermee worden de drie bestuursorganen van de gemeente bedoeld: de burgemeester, het college van burgemeester en wethouders en de gemeenteraad.

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. De FG behoort in voldoende mate ondersteund te worden door hem toegang te verschaffen tot persoonsgegevens en verwerkingen daarvan en hem de benodigde middelen ter beschikking te stellen voor het vervullen van de taak en het in standhouden van zijn deskundigheid. De uitvoerende taken liggen bij de Privacy Officer ondersteund door het privacy team.

De FG brengt jaarlijks een verslag uit aan de verwerkingsverantwoordelijke van zijn werkzaamheden, bevindingen en aanbevelingen. Dit jaarverslag is bedoeld voor de burgemeester en het college van B&W. De gemeenteraad zal als zelfstandig verwerkingsverantwoordelijke en als controlerend orgaan van het college van B&W separaat een verslag ontvangen.

Leeswijzer

Deze jaarrapportage bestaat uit twee onderdelen. In het eerste deel wordt teruggekeken naar het jaar 2019. Wat heeft de gemeente bereikt op het gebied van gegevensbescherming? Welke maatregelen zijn er genomen om te voldoen aan de AVG? In het tweede deel worden aanbevelingen gedaan om gegevensbescherming en privacy in het jaar 2021 naar het geambieerde niveau te tillen. Hierbij wordt waar nodig tevens aandacht geschonken aan de technische en organisatorische middelen die nodig zijn om dit hogere niveau te bereiken.

De thema's die in dit rapport worden genoemd zijn afkomstig uit het AVG borgingsproduct van de Informatiebeveiligingsdienst (IBD).[2] Er worden zeven thema's onderscheiden:

1. Beleid
2. Processen
3. Organisatorische inbedding
4. Rechten van betrokkenen
5. Samenwerking
6. Beveiliging
7. Verantwoording

In het borgingsproduct worden thema's, criteria en maatregelen omschreven die de AVG vertalen naar een kwaliteitscyclus voor gegevensbescherming en privacy voor gemeentelijke processen.

In bijlage 1 staat per thema aangegeven in hoeverre de gemeente de criteria reeds heeft geïmplementeerd.

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

Deel 1. Terugblik op 2019

Het jaar 2019 stond in het teken van de ‘lessons learned’ na het eerste AVG-jaar (2018) en verdere implementaties en verbeteringen. In dit deel van de rapportage zal worden teruggeblikt op hetgeen de gemeente in 2019 heeft bereikt en welke werkzaamheden zijn verricht.

Beleid

Het privacy beleid is een kader waarin de gemeente Woensdrecht 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 privacy beleid is in 2017 door kwartiermakers opgesteld. Dit bleek echter te algemeen en niet alles omvattend. Daarnaast was het binnen de organisatie niet of nauwelijks bekend, laat staan gedragen. Reden om het beleid te actualiseren en toegankelijker te maken. In 2019 is het privacy beleid aangepast. In Q2 van 2020 is het nieuwe beleid vastgelegd en vastgesteld door het college. De raad zal zich er in Q3 2020 over uitspreken.

Gerelateerd aan volwassenheidsniveau 3 is het volgende gerealiseerd:

Er is algemeen vastgelegd en vastgesteld privacy beleid waarin wordt uitgelegd hoe de gemeente omgaat met persoonsgegevens en hoe de rollen, taken en verantwoordelijken zijn belegd. Het privacy beleid is door het management bekrachtigd en wordt actief uitgedragen.

Op de gemeentelijke website staat in een privacyverklaring wanneer en hoe de gemeente via de website persoonsgegevens verzameld. Bezoekers van de gemeentelijke website worden voorafgaand geïnformeerd of de gemeente persoonsgegevens via de website verzameld, en zo ja voor welk doel. Aanvullend informeert de gemeente bezoekers van de gemeentelijke website actief of zij cookies plaatst, en zo ja welke cookies.

Processen

De verwerkingen van persoonsgegevens van de gemeente Woensdrecht 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 wettelijk verplicht zijn om gegevensbeschermingseffectbeoordeling (DPIA[3]) uit te voeren, om zo vast te stellen welke risico's er zijn verbonden aan een bepaalde verwerking of processen en welke maatregelen er genomen moeten worden om deze risico's te beperken.

Gerelateerd aan volwassenheidsniveau 3 is het volgende gerealiseerd:

De meeste verwerkingen waar de gemeente verwerkingsverantwoordelijk of medeverantwoordelijk voor is, zijn, in de basis, in een register van verwerkingsactiviteiten opgenomen , dat eventueel te overleggen is aan de Autoriteit persoonsgegevens.
De Privacy Officer is verantwoordelijke voor de inrichting, bewaking en actualisatie van (onderdelen van) het register. Dit doet hij op aangeven van de verschillende proceseigenaren, die wijzigingen van de bestaande verwerkingen of het toevoegen van nieuwe verwerkingen doorgeven. Er is een standaardformat beschikbaar voor de DPIA. Deze standaard is echter nog niet vastgesteld en wordt niet tot onvoldoende gebruikt. Zie hierover Deel 2 - Vooruitkijken naar 2020 – Processen.

In bijlage 2 is een overzicht opgenomen van de uitgevoerde DPIA's door de gemeente Woensdrecht voor het jaar 2019.

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 aandacht voor privacy. Organisatorische inbedding betekent het toewijzen van taken, verantwoordelijkheden en bevoegdheden en bewustzijn creëren.

Er is veel energie gestoken in de organisatorische inbedding. Zo is de bewustwording vergroot door het organiseren van de leercirkels. Dit is bv te concluderen uit het aantal deelnemers dat geslaagd is voor de afsluitende toets.

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

Gerelateerd aan volwassenheidsniveau 3 is het volgende gerealiseerd:

De gemeente heeft een Functionarisgegevensbescherming (FG) aangesteld en gepositioneerd. Naast deze FG is ruime (juridische) kennis over privacy, gegevensbescherming en relevante wet- en regelgeving aanwezig binnen de organisatie in de persoon van de Privacy Officer (PO) Deze PO adviseert de gemeente op casusniveau omtrent de bescherming en de verwerking van persoonsgegevens.
De verantwoordelijkheden op het niveau van lijnmanagement zijn benoemd, belegd en vastgelegd.
Het lijnmanagement betrekt de FG weliswaar bij aangelegenheden die verband houden met de bescherming van persoonsgegevens, alleen gebeurt dit nu alleen vaak nog op initiatief van de PO.
Het lijnmanagement wint weliswaar advies in alvorens persoonsgegevens worden verstrekt aan een externe partij, alleen gebeurt nu vaak reactief en op aangeven van de PO.
Op elke afdeling is een privacy ambassadeur aangewezen, welke privacy gerelateerde vragen en opmerkingen verzamelt en op de hoogte is van de wensen en ontwikkelingen binnen de afdeling.
Het privacy team komt periodiek bij elkaar om ontwikkelingen te bespreken.
De verantwoordingsplicht van de gemeente is bekend. Er moet aantoonbaar voldaan worden aan de AVG
Organisatie breed is iedereen op de hoogte van het bestaan van het register van verwerkingsactiviteiten.
Medewerkers zijn in grote lijnen op de hoogte van de definitie van een datalek en weten bij wie zij een datalek intern moeten melden.
De algemene privacy normen van de gemeente zijn organisatie breed bekend.
Het privacy beleid is bekend gemaakt binnen de organisatie wordt uitgedragen.
Medewerkers van de verschillende afdelingen zijn op de hoogte van de rechten die inwoners en betrokkenen hebben zoals verwoord in de AVG. De Privacy Officer is binnen de organisatie als verantwoordelijke aangesteld voor de afhandeling van verzoeken.
Er is een procedure autorisatie en controle toegangsrechten voor medewerkers die uit dienst treden. Toegangsrechten worden dan actief aangepast. Voor functie wijzigingen is dit minder tot niet het geval.
De Ondernemingsraad (OR) wordt geïnformeerd en betrokken wanneer het gaat om het verwerken en ook de bescherming van de persoonsgegevens van medewerkers.
Alle medewerkers en externen hebben een geheimhoudingsverklaring getekend. Alle ambtenaren zijn op de hoogte van de algemene geheimhoudingsplicht voor ambtenaren.

Rechten van betrokkenen

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

Er zijn tot nu toe zijn alleen verzoeken om inzage ontvangen. Dat is als reden aangegrepen om geen verdere aandacht aan te geven aan het maken van procedures voor de overige rechten.

In sommige gevallen wilden personen gebruikmakend van hun rechten op grond van de AVG proberen de gemeente aansprakelijk te stellen voor het overschrijden van de behandeltermijn om vervolgens een schadevergoeding te ontvangen. Dit is vergelijkbaar met pogingen tot misbruik van de WOB. Deze pogingen waren niet succesvol door doortastend optreden.

In bijlage 3 is een overzicht opgenomen van het aantal en soort verzoeken van betrokkenen in het jaar 2019.

Gerelateerd aan volwassenheidsniveau 3 is het volgende gerealiseerd:

Betrokkenen worden duidelijk geïnformeerd hoe zij een AVG-verzoek kunnen indienen. De contactgegevens van de FG zijn makkelijk vindbaar voor betrokkenen, zodat deze als aanspreekpunt kan fungeren.
Er is een werkproces ingericht om de rechten van betrokkenen te faciliteren. Dit geldt echter nu nog slechts voor het recht op inzage.
De systemen en voorzieningen van de gemeente faciliteren in principe de rechten van betrokkenen.

Samenwerking

De gemeente Woensdrecht 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 dient dan ook afspraken te maken met deze andere partijen.

Er is een register van verwerkingen en een register van verwerkingsovereenkomsten Dit horen dynamische documenten te zijn. Dat wil zeggen ze actief bijgehouden moeten worden wanneer er sprake is van wijzigingen. Dit is nog niet het geval. De initiatieven tot het vullen en aanpassen van deze 2 registers komen nu nog vrijwel alleen van de Privacy Officer. Terwijl de verantwoordelijkheid voor het actualiseren bij het lijnmanagement tof /proceseigenaren behoort te liggen. De PO loopt in de praktijk vaak achter de feiten aan. Met als gevolg 2 incomplete en niet actuele registers.
.
Gerelateerd aan volwassenheidsniveau 3 is het volgende gerealiseerd:

De organisatie heeft inzichtelijk welke partijen zij aanmerkt als verwerker, gezamenlijk verwerkingsverantwoordelijke of zelfstandig verwerkingsverantwoordelijk, voor zover dit is opgenomen in het verwerkingsregister.
Er is een toetsingskader op grond waarvan duidelijk is welke derde partij die namens/in samenwerking met de gemeente verwerker, gezamenlijk verwerkingsverantwoordelijke of zelfstandig verwerkingsverantwoordelijke is.
In het register van verwerkingsactiviteiten is duidelijk opgenomen in welke categorie de externe partij valt.
De standaard verwerkingsovereenkomst is op afdelingsniveau beschikbaar.
De organisatie heeft met grotendeels alle bestaande verwerkers afspraken gemaakt over de verwerking van persoonsgegevens.
Het beheer van het register van verwerkersovereenkomsten is in de organisatie belegd, nl bij de Privacy Officer.

Beveiliging

Vanuit het algemene beschikbaarheidsbeginsel, het integriteitsbeginsel en het vertrouwelijkheidsbeginsel (BIV) is het essentieel dat de gemeente Woensdrecht passende technische en organisatorische maatregelen neemt ter beveiliging van persoonsgegevens. Daarnaast geldt er onder de AVG een meldplicht datalekken. Dit houdt in dat incidenten – waaronder inbreuken – op de beveiliging onder omstandigheden gemeld dienen te worden aan de AP en/of de betrokkene(n).

Gerelateerd aan volwassenheidsniveau 3 is het volgende gerealiseerd:

Het protocol melding datalekken dateert van 2017 opgesteld. Daarmee was er formeel voldaan aan de geldende regelgeving. In 2019 is dit protocol herzien en aangepast aan de laatste inzichten en om beter bij de praktijk aan te sluiten. Het gaat hierbij om een duidelijker rolverdeling in het behandelen en afhandelen van een beveiligingsincident of datalek. Wie doet wat, wanneer en wie draagt verantwoordelijkheid. Ook is er vastgelegd dat wanneer de organisatie wenst af te wijken van het advies van de FG dat dit gemotiveerd moet gebeuren en worden vastgelegd.

In 2019 zijn er 11 datalekken gemeld. Geen van deze datalekken kwalificeerden als datalekken met meldplicht aan de Autoriteit Persoonsgegevens, omdat de impact op de rechten en vrijheden van betrokkene(n) beperkt bleek.

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

Voor geautomatiseerde systemen zijn autorisatieschema's vastgesteld. Deze autorisaties worden periodiek gecontroleerd.
Verwerkingen worden zodanig ingericht dat rekening wordt gehouden met de beginselen van Privacy by Design (PbD) en privacy by default.

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 van B&W aan moet kunnen tonen dat de verwerkingen van persoonsgegevens voldoen aan de beginselen van de AVG en aan de relevante wet- en regelgeving.

Gerelateerd aan volwassenheidsniveau 3 is het volgende gerealiseerd:

De verwerkingen van de organisatie zijn grotendeels vastgelegd in het register van verwerkingsactiviteiten en getoetst aan het privacy beleid en de relevante wet- en regelgeving. Er is een actueel register van alle incidenten, waaronder inbreuken in verband met persoonsgegevens. De zgn datalekken.
De organisatie voert periodiek controles uit op de juiste werking van de getroffen beveiligingsmaatregelen.
Periodiek worden de verantwoordelijk bestuursorganen geïnformeerd over de omgang met persoonsgegevens en de naleving van de AVG binnen de gemeente.
De FG doet periodiek verslag aan het verantwoordelijk bestuursorgaan over de omgang met persoonsgegevens binnen de gemeente.

Periodiek wordt een beveiligingsniveau GAP-analyse uitgevoerd om inzichtelijk te maken waar de organisatie staat.
De gemeente heeft daarmee inzichtelijk welke acties en maatregelen genomen moeten worden om het beveiligingsniveau van persoonsgegevens en de zorgvuldige omgang van persoonsgegevens naar een hoger niveau te brengen.

Conclusie

In 2019 is er binnen de gemeente Woensdrecht heel wat werk verzet om de AVG te implementeren in de organisatie, de systemen en de processen.

De introductie van de zgn. 'leercirkels' was zeer effectief, in die zin dat de privacy bewustwording van de medewerkers kon worden vastgesteld. Deze bleek sinds de voorgaande meeting aantoonbaar gestegen te zijn.
De rol van Privacy Officer is ingevuld. De Privacy Officer is een belangrijke schakel tussen de uitvoerende organisatie en de FG (Functionaris Gegevensbescherming). Daarnaast geeft hij operationeel invulling aan het intern borgen van de privacy vereisten en ondersteunt daarbij het verantwoordelijke lijnmanagement. Een gevolg is dat de FG zich kan richten op de invulling van de zuivere FG rol.
De Privacy Officer wordt weer ondersteund door de privacy teamleden. Dit zijn medewerkers verdeeld over de diverse afdelingen, die fungeren als privacy ambassadeurs.
Het privacy beleid is herzien. Daarbij heeft de gemeente onder andere een standpunt ingenomen en vastgelegd omtrent haar ambitie t.a.v. volwassenheid op het gebied van privacy en bescherming van

persoonsgegevens. Het college heeft als doelstelling vastgelegd het volwassenheid niveau 3 op een schaal van 5 te willen bereiken in een termijn van 2 jaar. Dit is 2022. Medio 2019 is het volwassenheidsniveau vastgesteld op 1,5. Medio 2020 is dit 1,8. Voor alle duidelijkheid; volwassenheidsniveau 3 betekent dat er in de basis voldaan wordt aan de AVG.

Over het algemeen kan gesteld worden dat de gemeente op de goede weg is om compliant te worden aan de AVG. In het proces daar naartoe loopt de gemeente niet uit de pas ten opzichte van de ontwikkeling die andere gemeenten doormaken.

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

Deel 2. Vooruitkijken naar 2020

Gegevensbescherming onderdeel laten zijn van de processen en systemen van het college, en daarmee aantoonbaar voldoen aan privacywetgeving, is een continu proces. Het vraagt om structurele borging van dit onderwerp. Waar het jaar 2019 in het teken stond van de 'lessons learned' van het eerste jaar van het van kracht zijn van de AVG (2018) en van de implementaties en verbeteringen, zal in 2020 de verdere inrichting van de interne privacy organisatie centraal staan. Hierbij kan gedacht worden aan:

- Vasstellen van een privacy governance verbijzonderd naar de verschillende AVG vereisten (taak, bevoegdheid, verantwoordelijkheid)
- Een duidelijke rolscheiding tussen Functionaris gegevensbescherming en Privacy Officer.
- Het privacy team in haar kracht zetten als ambassadeurs op het gebied van privacy en hier tijd en gelegenheid voor bieden.
- Structuur brengen in nieuwe verwerkingen door een betere gebruik van het register van verwerkingen en daar waar nodig gebruik maken van DPIA's.
- Opzetten en borgen van de PDCA cyclus.

Beleid

Aanbevelingen in relatie tot het bereiken van volwassenheidsniveau 3

1. Er is algemeen privacy beleid. De meest recente versie is in Q2 2020 vastgesteld door het de burgemeester en het college. In Q3 zal de raad zich hierover uitspreken.
   1.1. Maak het nieuwe privacy beleid bekend binnen en buiten de organisatie.
   1.2. Stel een communicatieplan op om dit beleid actief uit te dragen.
2. Maak het privacy beleid leidend bij ontwerp en ontwikkelingen van (nieuwe) verwerkingen.
   2.1. Toets nieuwe ontwikkelingen, verwerkingen of wijzigingen van verwerkingen voorafgaand aan het beleid en geldende wet- en regelgeving.
3. Laat het privacy beleid – waar nodig – domein specifiek uitwerken.
   3.1. Stel - waar nodig - domein specifiek privacy beleid op waarin wordt beschreven hoe het betreffende domein omgaat met (sectorspecifieke) wet- en regelgeving, persoonsgegevens en gegevensbescherming. Dit zal o.a. gelden voor het sociaal domein als HRM.
   3.2. Zorg dat medewerkers van een domein op de hoogte zijn van de inhoud van de domein specifieke uitwerking. Zet hier communicatiemiddelen voor in, zoals bv intranet, lunchbijeenkomsten en cursussen.
4. Leg afspraken en maatregelen vast over de omgang met persoonsgegevens en gegevensbescherming van personen binnen de organisatie.
   4.1. Maak afspraken over hoe de organisatie omgaat met persoonsgegevens van binnen de gemeentelijke organisatie, zoals de persoonsgegevens van medewerkers, gemeenteraadsleden, externen, etc.
   4.2. Zorg dat binnen de gemeente iedereen op de hoogte is van de inhoud van deze afspraken. Zet hiervoor communicatiemiddelen in, zoals bv intranet, lunchbijeenkomsten en cursussen.
5. Toets het privacy beleid periodiek en pas waar nodig aan.
   5.1. Controleer periodiek of verwerkingen in lijn zijn met het privacy beleid van de organisatie en geldende wet- en regelgeving.

Processen

Aanbevelingen in relatie tot het bereiken van volwassenheidsniveau 3

1 Alle werkprocessen waarin persoonsgegevens worden verwerkt behoren te zijn vastgesteld.
   1.1 Maak inzichtelijk in welke werkprocessen, die de organisatie in huis heeft, persoonsgegevens worden verwerkt.

1.2 Besteedt in deze werkprocessen aandacht aan wat gegevensbescherming en de privacywetgeving concreet betekenen voor de betreffende afdeling en hoe medewerkers om dienen te gaan met persoonsgegevens binnen de taken en werkzaamheden.

2 Zorg dat de verwerkingsactiviteiten voldoen aan de beginselen van de AVG.
- 2.1 Leg van alle verwerkingen binnen de gemeente vast dat zij een doel en een grondslag hebben en voldoen aan de beginselen van proportionaliteit, subsidiariteit, integriteit en dataminimalisatie.
- 2.2 Leg het resultaat van deze toetsing aan de AVG beginselen vast in het register van verwerkingsactiviteiten.

3 Zorg voor actief beheer van het register van verwerkingsactiviteiten. Dit is een dynamisch document.
- 3.1 De verantwoordelijke voor (onderdelen van) het register behoort te zorgen voor de daadwerkelijke actualisatie. Dit is een lijnverantwoordelijkheid.
- 3.2 Toets nieuwe verwerkingen of wijzigingen van bestaande verwerkingen structureel aan de beginselen uit de AVG en andere relevante wet- en regelgeving. Ook dit is een lijnverantwoordelijkheid.

1 Beschrijf processen voor alle rechten van betrokkenen. (inzage, wijziging, beperking, verwijdering)
- 1.1 Beschrijf in de processen ten minste het volgende:
  - Op welke wijze verzoeken kunnen worden ingediend;
  - Wie verantwoordelijk is voor de afhandeling;
  - De termijnen;
  - De criteria voor het toewijzen en afwijzen van een verzoek.

2 Zorg voor een compleet en actueel beeld van bestaande verwerkingen die een hoog privacy risico opleveren en waar een DPIA voor is uitgevoerd, dan wel uitgevoerd zal gaan worden.
- 2.1 Maak inzichtelijk welke bestaande verwerkingen een hoog privacy risico opleveren, bijvoorbeeld met behulp van het register van verwerkingsactiviteiten.
- 2.2 Zorg dat het voor de organisatie inzichtelijk is wanneer er voor welke verwerking een DPIA is uitgevoerd.
- 2.3 Registreer rapportages van de DPIA's en maak ze makkelijk vindbaar voor de betrokken medewerkers.
- 2.4 Breng bij nieuwe verwerkingen of bij de aanschaf van nieuwe systemen voorafgaand in kaart of deze een hoog risico voor de inbreuk op rechten en vrijheden van personen vormen en zo ja, voer een DPIA uit.

3 Leg een proces vast voor het uitvoeren en actualiseren van DPIA's.
- 3.1 De organisatie behoort daarbij inzichtelijk te hebben wanneer een DPIA uitgevoerd zal worden en op welke wijze dit gebeurd.
- 3.2 Binnen de organisatie behoort bekend te zijn door welke verantwoordelijken de DPIA uitgevoerd moeten worden.
- 3.3 Actualiseer DPIA's periodiek en ten minste om de 3 jaar of vaker indien nodig. Aanleiding kan een wijzigingen in bestaande verwerkingen zijn.

4 Er is een standaardformat beschikbaar voor de DPIA
- 4.1 Stel een format vast en maak het beschikbaar en bekend voor de gehele organisatie.

5 Intern verantwoordelijken (= proceseigenaren) dragen er zorg voor dat nieuwe verwerkingen of potentieel nieuwe verwerkingen, welke mogelijk een hoog privacy risico opleveren voorafgaand worden getoetst middels een DPIA.
- 5.1 Zorg dat zowel het lijnmanagement als de privacy ambassadeurs bekend zijn met het bestaan van de DPIA en het verplichte DPIA format van de organisatie.
- 5.2 Realiseer dat nieuwe verwerkingen of wijzigingen van bestaande verwerkingen actief worden aangemeld bij de verantwoordelijke en de privacy officer, zodat deze kan toetsen of een DPIA noodzakelijk is.
- 5.3 Leg de belangenafweging om al dan niet over te gaan tot een DPIA vast voor latere verantwoording.

6 Zorg dat de proceseigenaar, en daarmee de verantwoordelijke, kennis neemt van de inhoud van de DPIA.
- 6.1 Leg het verslag en de rapportage van de uitgevoerde DPIA met het advies van de FG ter besluitvorming voor aan de verantwoordelijke.

6.2 De verantwoordelijke motiveert de besluitvorming wanneer die afwijkt van het advies van de FG.

7 Gebruik en deel de resultaten van de DPIA om de betrokken afdeling(en) bewust te maken van de privacy risico's en het belang van privacy management.
7.1 Deel uitkomsten van de DPIA en het advies van de FG met de betrokken medewerkers.
7.2 Stel de uitkomst van de DPIA en het advies van de FG wordt indien nodig organisatie breed beschikbaar.

8 De organisatie behoort opvolging te geven aan de uitkomsten van de DPIA.
8.1 Leg in het (werk)proces vast welke technische en organisatorische maatregelen worden genomen om privacy risico's af te dekken, dan wel in te perken.
8.2 Benoem deze maatregelen in het register van verwerkingsactiviteiten.

Organisatorische inbedding

Aanbevelingen in relatie tot het bereiken van volwassenheidsniveau 3

1 Benoem, en beleg de verantwoordelijkheden op het niveau van lijnmanagement.
1.1 Uitgangspunt is dat iedere lijnmanager verantwoordelijk is voor privacy binnen zijn/haar domein.

2 Wijs in elke team een privacy ambassadeur aan, die privacy gerelateerde vragen en opmerkingen verzamelt en op de hoogte is van de wensen en ontwikkelingen binnen de team.
2.1 De privacy ambassadeur is bekend bij alle medewerkers en dient als aanspreekpunt voor het gehele team.

3 Organisatie breed hoort bekend te zijn welke verantwoordelijkheid de gemeente heeft ten aanzien van gegevensbescherming.
3.1 Medewerkers behoren te weten bij wie zij wijzigingen kunnen doorgeven, zodat het register aangepast kan worden en actueel blijft.
3.2 Voorafgaand aan een nieuwe verwerking of het wijzigen van een bestaande verwerking, hoort een toets plaats te vinden of dit binnen de geldende wet- en regelgeving mogelijk is.
3.3 Voor verwerkingen met een hoog risico wordt voorafgaand aan de wijziging dan wel invoering een DPIA uitgevoerd.

4 Maak de algemene privacy normen van de gemeente organisatie breed bekend.
4.1 Medewerkers zijn dan op de hoogte van de omgang met persoonsgegevens door de organisatie
4.2 Actualiteiten en ontwikkelingen die betrekking hebben op de werkwijze van de gemeente worden daarbij breed gedeeld en toegelicht.

5 Medewerkers zijn op de hoogte van de rechten die inwoners en betrokkenen hebben.
5.1 Er is een procedure voor de afhandeling van verzoeken van alle rechten van betrokkenen.

6 Medewerkers behoren alleen toegang te hebben tot de systemen die zij nodig hebben ter uitvoering van hun werkzaamheden.
6.1 Stel voor alle geautomatiseerde systemen autorisatieschema's op.
6.2 Geef binnen deze systemen alleen toegang tot die gegevens die zij nodig hebben ter uitvoering van hun werkzaamheden.

7 Stel een procedure op voor de autorisatie en de controle van toegangsrechten
7.1 Toegangsrechten behoren actief aangepast te worden een medewerker van functie verandert.
8 Maak het logging beleid van de gemeente bekend aan de medewerkers.
8.1 Maak kenbaar bij het verkrijgen van de autorisatie tot een bepaald systeem, op welke manier de gemeente het gebruik van de gegevens in het systeem logt.

9 Stel voldoende middelen beschikbaar om privacybescherming te bevorderen in kennis, houding en gedrag van alle medewerkers in de organisatie.
9.1 Maak op teamniveau – wanneer noodzakelijk - actuele protocollen en procedures beschikbaar over de wijze van omgang met persoonsgegevens.
9.2 Train medewerkers actief om de kennis van het privacy recht en het privacy bewustzijn op het specifieke domein te verhogen.

9.3 Maak medewerkers doorlopend bewust van de risico's en randvoorwaarden bij de omgang met persoonsgegevens, bijvoorbeeld door interne opleidingen of trainingen, het delen van DPIA's en het verstrekken van adviesmateriaal.

10 Laat medewerkers die te maken hebben met bijzondere persoonsgegevens tevens een specifieke geheimhoudingsverklaring ondertekenen die ziet op het verwerken van die bijzondere persoonsgegevens.
10.1 Laat alle externen een integriteits- en geheimhoudingsverklaring ondertekenen.

Rechten van betrokkenen

Aanbevelingen in relatie tot het bereiken van volwassenheidsniveau 3

1. De verwerkingsverantwoordelijke behoort processen in te richten om alle rechten van betrokkenen te faciliteren. Naast recht op inzage betreft het hier:
   1.1. het recht op rectificatie en aanvulling.
   1.2. het recht op vergetelheid.
   1.3. Het recht op beperking van de verwerking.
   1.4. het recht van data portabiliteit.
   1.5. het recht om bezwaar te maken tegen de gegevensverwerking.
   Voorwaarde is dat toe-, dan wel afwijzingscriteria bekend zijn en de processen vastgesteld en intern bekend zijn.
   Het proces recht van inzage moet nog vastgelegd en vastgesteld te worden. Overige rechten kunnen grotendeels van dit proces worden afgeleid.
2. Zorg dat alle systemen en voorzieningen van de gemeente de rechten van betrokkenen faciliteren.
   2.1. Neem bij de aanschaf van nieuwe systemen de mogelijkheid voor betrokkenen om hun rechten op grond van de AVG uit te oefenen als criterium mee.
3. Informeer betrokkenen voorafgaand aan de verwerking actief, tijdig en adequaat.
   3.1. Voorafgaand aan de verwerking worden betrokkenen dan geïnformeerd over de soort gegevens die worden verwerkt, de bron van gegevens, het doel van de verwerking, de grondslag van de verwerking, aan wie de gegevens worden verstrekt.
   3.2. Vermeld bij aanvraagformulieren voor producten of diensten duidelijk welke gegevens worden verwerkt.
   3.3. Stel evt. (digitale) informatiefolders beschikbaar.
4. Richt producten, diensten, instellingen en functies in systemen privacy vriendelijk in.
   4.1. Vraagt bij de aanvraag van producten en diensten niet meer persoonsgegevens dan noodzakelijk uit. (gegevensminimalisatie)
   4.2. In het uitzonderlijke geval waar voor verwerkingen toestemming als grondslag dient, vereist dit een actieve handeling. welke ook weer kan worden ingetrokken. Opgemerkt wordt dat het verwerkingsregister geen compleet overzicht geeft.
   4.3. De oganisatie heeft inzichtelijk aan welke randvoorwaarden deze toestemming moet voldoen.

Samenwerking

Aanbevelingen in relatie tot het bereiken van volwassenheidsniveau 3

1. Maak als organisatie inzichtelijk met welke externe partijen er sprake is van het verwerken van persoonsgegevens.
   1.1. Inventariseer aan welke partijen persoonsgegevens worden verstrekt en geef daarbij aan welke (categorieën van) persoonsgegevens deze partijen van de gemeente verkrijgen.
   1.2. Inventariseer van welke partijen de gemeente persoonsgegevens ontvangt en geef daarbij aan welke (categorieën van) persoonsgegevens de gemeente ontvangt.

2. Toets bij het inschakelen van externe partijen voorafgaand of er sprake is van het verwerken van persoonsgegevens en wanneer dit het geval is, maak voorafgaand aan de inschakeling afspraken over de verwerking.
   2.1. Actualiseer het verwerkingsregister bij de inschakeling van een externe partij volgens afgesproken lijnen.
3. Maak als organisatie met alle bestaande verwerkers en (gezamenlijke) verwerkingsverantwoordelijken afspraken over de verstrekkingswijze en verwerking van persoonsgegevens. Leg dit bij voorkeur vast in het verwerkingsregister
4. Stel een duidelijk overzicht beschikbaar van alle ingeschakelde verwerkers, bij voorkeur in het register van verwerkingsactiviteiten.
   4.1. Toets (ook) eenmalige gegevensverstrekkingen aan de beginselen van de AVG en andere relevante wetgeving. Zorg daarbij voor duidelijkheid over de rol van de derde partij. Dienovereenkomstig kunnen er afspraken gemaakt worden met deze derde partij.

Beveiliging

Aanbevelingen in relatie tot het bereiken van volwassenheidsniveau 3

1. Er is een datalek protocol.
   1.1. Stel een crisiscommunicatieplan op voor datelekken met een hoge impact.
2. Middels technische en organisatorische maatregelen wordt het risico op incidenten die verband houden met persoonsgegevens geminimaliseerd.
   2.1. Test en evalueer de beveiligingsmaatregelen periodiek.
   2.2. Betrek de FG bij het opstellen van het informatieveiligheidsbeleid
   2020 is het jaar waarin het informatieveiligheidsbeleid geënt hoort te worden op de Baseline Informatiebeveiliging Overheid (BIO) als opvolger van de baseline Informatiebeveiliging gemeenten (BIG)
3. Voor alle geautomatiseerde systemen waarmee persoonsgegevens worden verwerkt zijn autorisatieschema's vastgesteld.
   3.1. Stel een autorisatieprocedure op voor het wijzigen van functie.
   3.2. Stel een loggingsbeleid op, als onderdeel van het informatieveiligheidsbeleid, waarbij alle verwerkingen binnen geautomatiseerde systemen worden gelogd en loggingsbestanden periodiek worden gecontroleerd. De OR hoort hier om instemming gevraagd te worden.
   3.3. Richt verwerkingen zodanig in dat rekening wordt gehouden met zowel de beginselen van Privacy by Design (PbD) als privacy by default. Dit ter borging van de privacy van betrokkenen en de AVG-beginselen.

Verantwoording

Aanbevelingen in relatie tot het bereiken van volwassenheidsniveau 3

1. Maak een actueel overzicht van verwerkingen waar een DPIA voor is uitgevoerd.
   1.1. Maak de rapportages van de DPIA beschikbaar.
   1.2. Wanneer de organisatie afwijkt van het advies van de FG, behoort dit gemotiveerd vastgelegd te worden.
2. Voer periodiek controles uit om de juiste werking van de getroffen beveiligingsmaatregelen te controleren, als onderdeel van de PDCA cyclus.
3. Mocht in een enkel geval voor een verwerkingsactiviteit gegevens verwerkt worden op basis van toestemming, leg dan in een proces vast op welke manier de organisatie toestemming ontvangt, vastlegt en bewaart.
   3.1. Houdt als organisatie een register bij van ontvangen verklaringen van toestemming.
   3.2. Informeer betrokkenen specifiek waarvoor zij toestemming geven.
   3.3. Maak het intrekken van toestemming even eenvoudig als het geven van toestemming.
4. De organisatie is transparant over de verwerking van persoonsgegevens.

4.1. Vergroot de transparantie over de over de omgang met persoonsgegevens door de gemeente door o.a. het publiceren van (een publieke versie van) het privacy beleid en evnetueel het verstrekken van informatiefolders bij aanvragen van producten en diensten.
5. Stel, n.a.v. het verslag van de FG vast welke acties en maatregelen er genomen moeten worden in een plan van aanpak.
6. Houd burgers periodiek op de hoogte – bijvoorbeeld op de gemeentelijke website – van de omgang met persoonsgegevens en de naleving van de AVG binnen de gemeente.

Conclusie

Op het gebied van privacy en gegevensbescherming is er in 2020 zeker nog winst te behalen. Met name het vroegtijdig betrekken van de privacy functionarissen bij nieuwe (beleids)initiatieven door zowel college als management gaat dit opleveren. Dit zorgt nl. voor een tijdige toetsing van deze initiatieven aan de AVG vereisten. Niet als rem maar als belangrijke randvoorwaarde en toetsingskader.
In dit verband wordt er aandacht gevraagd voor de samenwerkingsverbanden met andere gemeenten, netwerkorganisatie en overige. Niet in alle gevallen is de grondslag voor gegevensuitwisseling helder of de onderlinge verhoudingen van de deelnemende partijen en daarmee de afzonderlijke verantwoordlijkheden op het gebied van beheer, toegang, honoreren van rechten van betrokkenen en het correct omgaan met datalekken. Daarnaast is er zonder een duidelijke doelomschrijving kans op ongewild of ongeoorloofd gebruik van betrokkene persoonsgegevens. De Autoriteit Persoonsgegevens heeft samenwerkingsverbanden als aandachtpunt opgenomen in haar focus document 2020-2023 Gemeente Woensdrecht is hieromtrent zeker nog niet in control.

Dataminimalisatie verdient meer aandacht. Daarmee wordt bedoeld dat medewerkers alleen die data verzamelen die nodig zijn voor de uitvoering van hun taak. Screening van de gegevens uitvraag is daarbij een eerste stap.

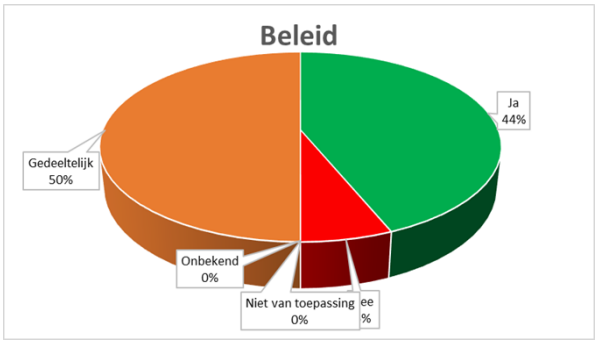
Ook verdient het actueel houden van het register van verwerkingen de nodige aandacht. Dit register kan gezien worden als een van de brondocumenten als het gaat om het aantoonbaar voldoen aan de AVG.

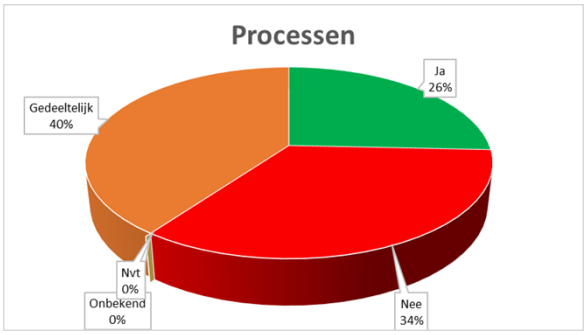
Het DPIA instrument (Data Protection Impact Assessment) wordt nog niet of nauwelijks actief en tijdig gebruikt om risico's van de verschillende verwerkingen van persoonsgegevens in kaart te brengen, adequate beveiligingsmaatregelen te treffen, en dit ook controleerbaar vast te leggen. Hier is de AVG aantoonbaarheidseis nadrukkelijk van toepassing. De gemeente geeft, door dit instrument wel te gebruiken, aan in control te zijn.

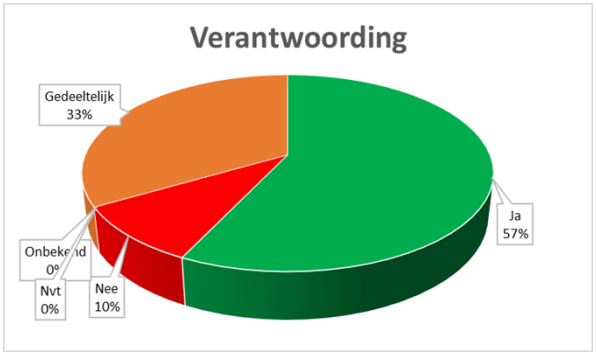
Tot slot zal er op korte termijn begonnen moeten worden met het inrichten van een PDCA cyclus om zo periodiek alle AVG vereisten, als onderdeel van de managementcyclus periodiek te toetsen en evt. bij te stellen.

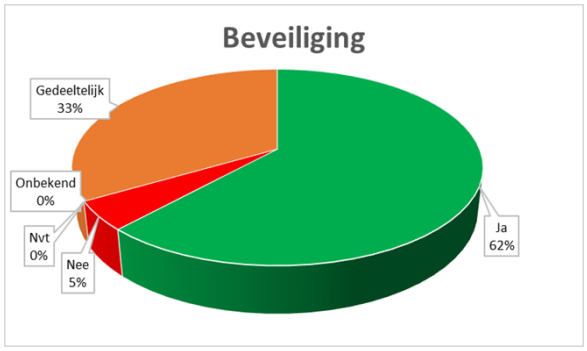
Het college en management zullen hun verantwoordelijkheid moeten nemen, en deze invulling geven als proceseigenaren, om een hoger privacy volwassenheidsniveau te bereiken.

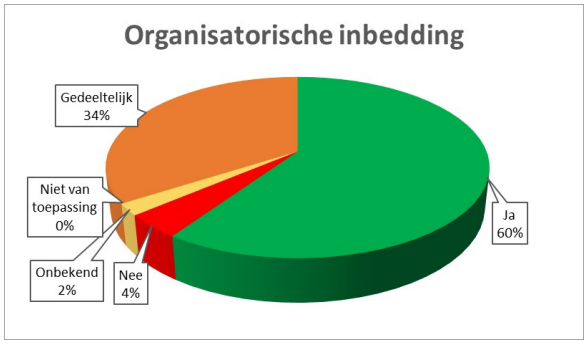
Bijlage 1 Stand van zaken AVG per onderwerp

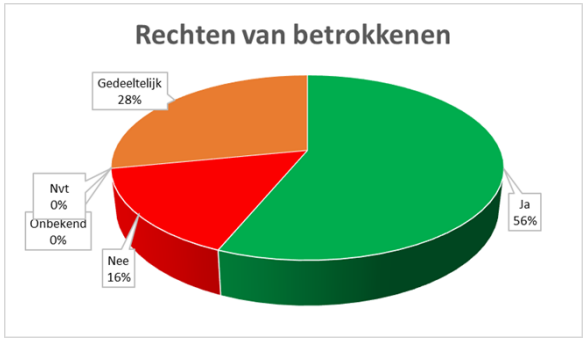


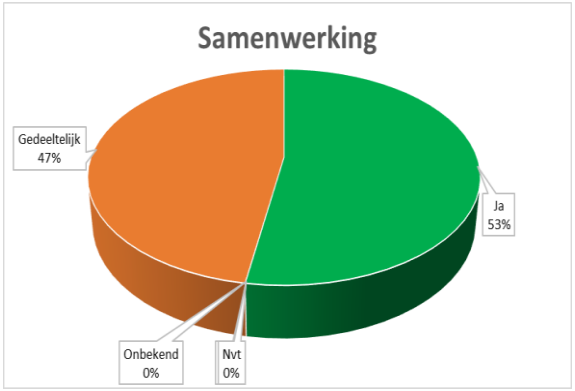


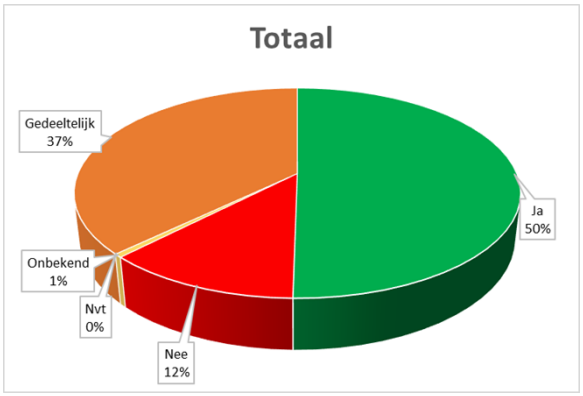












-

Bijlage 2 Overzicht uitgevoerde DPIA's

Onderwerp DPIA	Datum	Status	
Sociaal Domein	Medio 2018	Afgerond	Dit was een richting gevend onderzoek.
Corsa	Begin 2019	Afgerond	Dit is gebruikt om het zaaksysteem op privacy te onderzoeken.

Bijlage 3 Overzicht beroep op rechten van betrokkenen

In 2019 is er geen beroep gedaan op de rechten van betrokkenen zoals bedoeld in de AVG

Zaak	Datum	AVG-recht	Opmerking
	00-00-2019	Inzage / Correctie / Verwijdering	
	00-00-2019	Inzage / Correctie / Verwijdering	

Bijlage 4 Overzicht datalekken

In 2019 is geen overzicht gemaakt. Wel zijn de verschillend datalekken vastgelegd in het zaaksysteem. Er waren in 2019 11 datalekken. Geen van deze datlekken is gemeld aan de Autoriteit persoonsgegevens omdat de impact als gering werd ingeschat.