Gemeente Woensdrecht

Jaarrapportage Gegevensbescherming 2019

JAARRAPPORTAGE GEGEVENSBESCHERMING GEMEENTE WOENSDRECHT

September 2019

Samenvatting

Deze rapportage is opgesteld door de Functionaris Gegevensbescherming (FG) van de gemeente Woensdrecht. Hij doet verslag over de periode 2018 en 2019.
Het jaar 2018 was op het gebied van gegevensbescherming een bijzonder jaar voor organisaties en burgers, zo ook voor de gemeente Woensdrecht. Op 25 mei 2018 werd 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 mede in aanloop naar de digitale overheid.

Onder de verantwoordelijkheid van het college van Burgemeester en Wethouders (college van B&W) 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 gemeente dient zorgvuldig om te gaan met persoonsgegevens. Gemeenten verwerken immers bij de uitoefening van hun taken veel informatie. In de AVG wordt het wettelijk kader beschreven voor het verwerken van persoonsgegevens. Zo dient de gemeente transparant te zijn welke persoonsgegevens zij verwerkt en voor welk doel. Persoonsgegevens mogen alleen worden verwerkt wanneer dit in overeenstemming is met het doel waarvoor zij zijn verzameld en gegevens mogen niet langer bewaard worden dan strikt noodzakelijk.
Bovendien moet de gemeente passende technische en organisatorische beveiligingsmaatregelen treffen om onrechtmatige toegang tot deze persoonsgegevens tegen te gaan en daardoor een onrechtmatig gebruik van deze persoonsgegevens te voorkomen.
Daarnaast heeft de gemeente ook te maken met tal van privacyregels in sectorspecifieke wetgeving. Dit alles heeft gevolgen voor de inrichting van processen en systemen in en van de gemeente.

De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de privacyregels in Nederland. Daarnaast dient de gemeente Woensdrecht te beschikken over een interne toezichthouder: de Functionaris voor de Gegevensbescherming (FG). Op 1 april 2018 hebben de bestuursorganen van de gemeente Woensdrecht …… aangesteld als FG[1].
De FG ziet erop toe dat de AVG intern wordt nageleefd. Het college dient erop toe te zien dat de FG naar behoren en tijdig wordt betrokken bij alle gelegenheden die verband houden met de bescherming van persoonsgegevens. Daarnaast dient de FG ondersteund te worden door 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 FG brengt jaarlijks een verslag uit aan de verwerkingsverantwoordelijke van zijn werkzaamheden en bevindingen en doet hij naar aanleiding daarvan aanbevelingen. Dit jaarverslag is hiervoor bedoeld.

In algemeen gesteld voldoet de gemeentelijke organisatie niet aan de AVG omdat de diverse systemen en werkprocessen niet (volledig) daarop zijn ingericht. Eerder gold nog “alles open tenzij”. Door middel van Privacy by Default wordt zoveel mogelijk de bestaande situatie gerepareerd en door Privacy by Design worden de vereisten aan nieuwe systemen opgesteld. Het zal nog de nodige tijd vergen om volledig AVG-proof te werken.

Verder dient de organisatie een selectie te maken van de meest kwetsbare processen. Van die processen dient een risicoanalyse (DPIA Data Protection Impact Assessment) opgesteld te worden. De aanbevelingen uit de analyse kunnen gebruikt worden om het proces te optimaliseren.

---

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

Tot slot biedt een register van gegevensverwerking de gemeente inzichten over alle verwerkingen van persoonsgegevens. Dit is dus een belangrijk dynamisch document dat inzage geeft aan alle betrokken partijen en daarmee tevens een middel is om te sturen.

Samenvattend heeft de gemeente in 2018 en 2019 veel werk verzet op het gebied van gegevensbescherming. Zo is onder andere het privacy team vormgegeven. Heeft een stagiaire tijdelijk de rol van privacy officer opgepakt. En per april 2019 is een medewerker benoemd als privacy officer.

Per januari 2019 is de privacy leercirkel van start gegaan. Medewerkers hebben een vragenlijst ingevuld, welke heeft geresulteerd in een nulmeting. De Infografic toonde aan dat medewerkers graag meer willen weten over privacy. Dat bleek ook uit de goedbezochte workshops. Inmiddels heeft 2/3 van het personeel de e-learnings met positief gevolg afgelegd. Deze initiatieven zijn vooral genomen om de bewustwording te verhogen. Want een datalek veroorzaakt door de gemeente vertaalt zich direct in wantrouwen in de gemeentelijke organisatie. En de toezichthouder kijkt mee.

Gemeente Woensdrecht

Inhoudsopgave

Inleiding

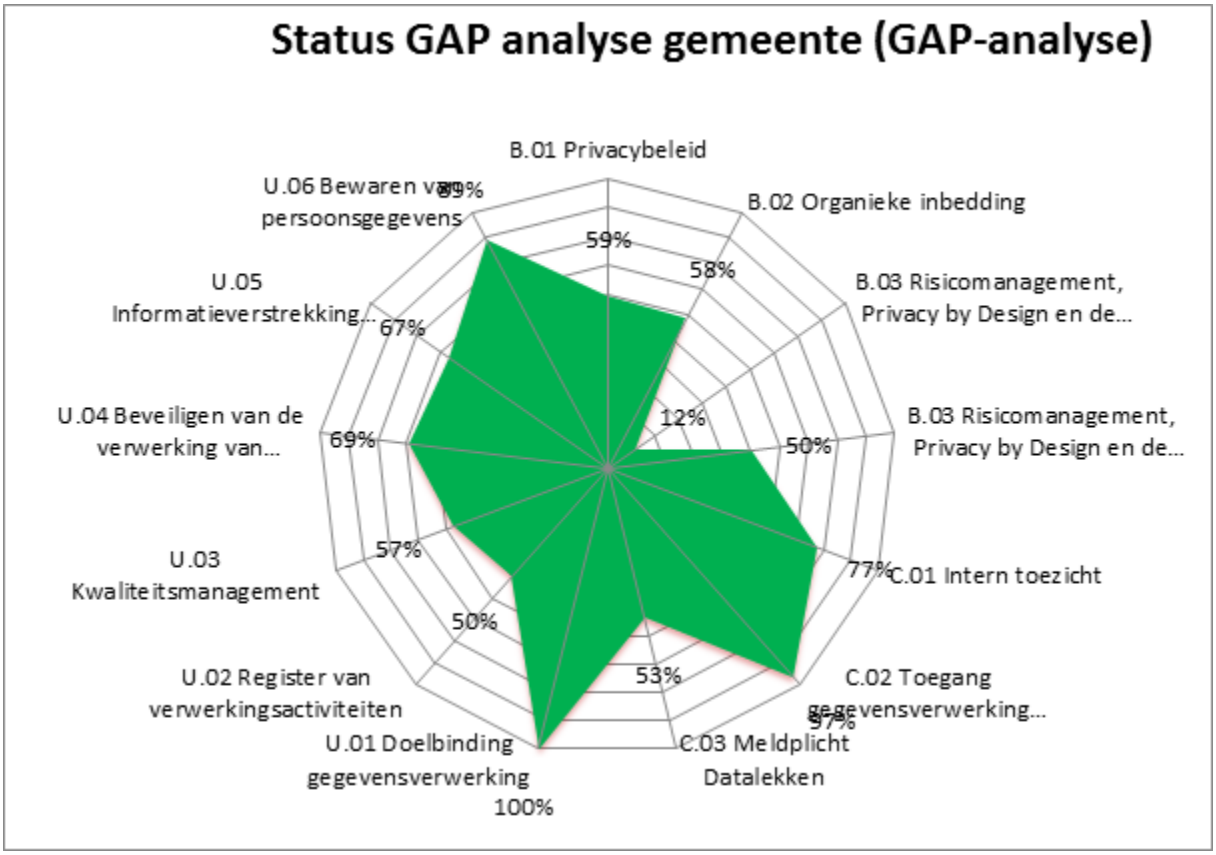
Het eerste deel van het jaar 2018 stond voor wat betreft privacy volledig in het teken van het van kracht worden van de AVG. In dit deel van de rapportage zal worden teruggeblikt op hetgeen de gemeente in 2018 en 2019 heeft bereikt en welke werkzaamheden zijn verricht.

Er zijn kwartiermakers aangesteld. Zij hebben het 10 stappenplan van de Autoriteit Persoonsgegevens geïmplementeerd. Daarmee was de buitenkant op orde. De samenhang met processen en systemen was daarbij ondergeschikt. Om te voldoen aan de AVG dient er een volwassen organisatie te zijn die steeds bewust is van de do's en don'ts.

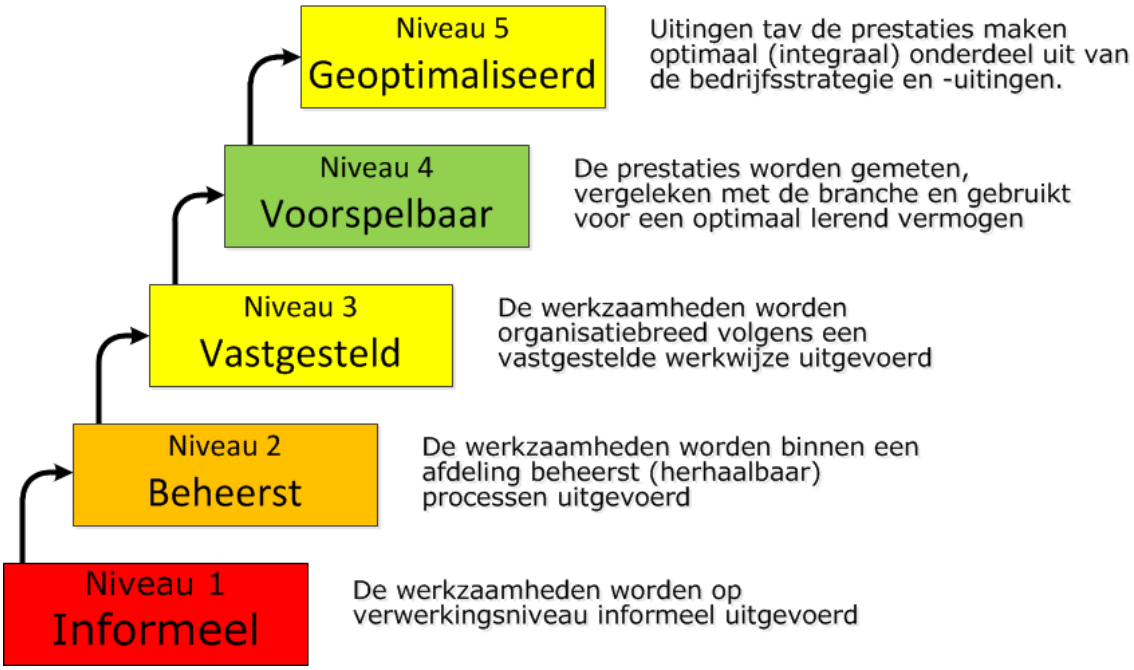
Daartoe is er een privacy Team benoemd. Zij zijn de ambassadeurs op de afdeling. Kennisdragers die geraadpleegd kunnen worden en die actief privacy op de werkvloer uitdragen. Zij doen dit onder initiatief en begeleiding van een privacy officer. Halverwege 2018 heeft een stagiaire de rol van privacy officer op zich genomen. Per april 2019 is er een vaste privacy officer benoemd.

In Q1 2019 is de gemeente gestart met een leercirkel. Er is de medewerkers gevraagd een nulmeting in te vullen. Daaruit bleek dat er veel behoefte is aan sturing hoe om te gaan met de AVG. Er zijn workshops gehouden en tot slot ontvingen de medewerkers een e-learning met maar liefst 8 modules.. De afronding loopt nog door. Maar bij schrijven had 2/3 van het personeel alle e-learning met goed gevolg afgelegd.

Door middel van vooraf vastgestelde vragen (normkader) is op een aantal criteria door de FG getoetst waar de gemeente Woensdrecht staat. Deze meting is gebaseerd op het volwassenheidsmodel. Onderstaand is een weergave van de analyse. Hieruit blijkt dat er forse stappen gezet zijn. Maar het toont ook aan dat er nog veel moet gebeuren.



De gemeente Woensdrecht heeft haar ambitie gesteld op niveau 3. Daarvoor is een tijdpad van 2 jaar uitgezet.
Om dit doel te bereiken is er een ontwikkelplan per afdeling opgezet. De uitrol hiervan vindt eind 2019 plaats.



Deel 1. Terugblik.

1. Het privacybeleid

Het privacybeleid 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 opgesteld en vastgesteld eind 2017. Het staat gepubliceerd op internet en intranet. In 2019 is het beleid herzien. Het privacy beleid is noodzakelijk wegens de ontwikkelingen. Gedacht moet worden aan de intensivering van het dataverkeer, diepere automatisering in de organisatie, de digitale overheid. Naar voren organiseren van de verzamelde informatie, waardoor eigen beheer door de betrokkene aan de orde komt.

2. 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.

De FG en Privacy officer zijn benoemd. Het privacy Team is geïnstalleerd. De bewustwording is invulling gegeven door de leercirkels. Het privacy bewustzijn is toegenomen.

3. Risicomanagement, en DPIA.

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 verplicht zijn om een gegevensbeschermingseffectbeoordeling (DPIA[2]) uit te voeren.

De enig uitgevoerde DPIA's voor de verwerkingen betreft Corsa. DPIA's dienen nog in het formele proces geïmplementeerd te worden. Het zicht op de gebruikelijke processen is op dit moment onvoldoende ontwikkeld. DPIA"s kunnen daarbij helpen.

4. Risicomanagement en Privacy by design.

Bij een nieuwe verwerking van persoonsgegevens al dan niet in combinatie met een applicatie dient er, steeds voor het starten van de verwerking, een afweging gemaakt te worden omtrent de risico;s van de verwerking met betrekking tot de borging van de privacy. Door toepassing van privacy by design kan in de

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

ontwerpfase van de inrichting van het proces al rekening worden gehouden met de risico's die bij de verwerking ontstaat. Door maatregelen en aanpassingen te doen wordt het risico zo veel als mogelijk gemitigeerd.

Privacy by design wordt nog te beperkt toegepast omdat privacy nog onvoldoende is geborgd in het formele proces.

5. Intern Toezicht

De organisatie dient te beschikken over een zelf herstellend en toetsend vermogen. Hoe organiseren we dat? Aan de basis van een proces ligt een cyclus waarin bewaakt wordt of het beoogde resultaat ook bereikt wordt. De meest gebruikte structurele processturing is een PDCA cirkel. Dit staat voor Plan Do Check Act. Inmiddels is er een PMS (privacy management systeem) aangeschaft. Met behulp van deze tool wordt de acties gedefinieerd, gepland; maak een plan met de resultaten die je wilt bereiken, voer het plan uit, vergelijk de resultaten met wat je had willen bereiken en bij afwijkingen neem maatregelen om het resultaat alsnog te bereiken.

6. 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.

De gemeente Woensdrecht heeft op internet het privacy beleid gepubliceerd. Daarnaast is kenbaar gemaakt welke rechten betrokkenen hebben en hoe zij deze kunnen uitoefenen. Tot slot is weergegeven wie de FG van de gemeente Woensdrecht is en hoe deze is te bereiken.

7. Meldplicht datalekken

Vanuit het algemene behoorlijkheidsbeginsel, het integriteitsbeginsel en het vertrouwelijkheidsbeginsel 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 direct gemeld moeten worden bij de Autoriteit persoonsgegevens (AP) zodra zij een ernstig datalek hebben geconstateerd. En soms moet daarop volgend het datalek ook gemeld worden aan de betrokkenen. (de mensen van wie de persoonsgegevens gelekt zijn)

Bij een datalek gaat het om de toegang tot of de vernietiging, wijziging of vrijkomen van persoonsgegevens zonder dat dit bedoeling is.

De gemeente Woensdrecht is verplicht een register van datalekken aan te houden en in voorkomend geval kan de Autoriteit persoonsgegevens vragen om inzage tot dat register.

Het datalekken register wordt periodiek besproken met de POHO.

De gemeente Woensdrecht heeft een protocol datalekken. Dit protocol is eind september 2019 door het college vastgesteld.

8. Doelbinding gegevensverwerking

Het doel van doelbinding gegevensverwerking is om te waarborgen dat de persoonsgegevens alleen worden verzameld en verwerkt voor gerechtvaardigde doelen.

Uitgangspunten van doelbinding is, dat gegevens worden verwerkt en verzameld voor een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel.
"Welbepaald en uitdrukkelijk omschreven" houdt in dat men géén gegevens mag verzamelen zonder een precieze doelomschrijving. Het doel moet zijn bepaald alvorens men tot verzamelen overgaat.
"Welbepaald" houdt in dat deze doelomschrijving duidelijk moet zijn, niet zo vaag of ruim dat zij tijdens het verzamelproces geen kader kan bieden waaraan getoetst kan worden of de gegevens nodig zijn voor dat doel of niet. Het doel mag ook niet in de loop van het verzamelproces geformuleerd worden. "Uitdrukkelijk

omschreven" houdt in dat de verwerkingsverantwoordelijke het doel waarvoor hij verwerkt moet hebben omschreven.

De gemeente Woensdrecht is veelal de uitvoerder van een wettelijke taak. Daarin is dan helder omschreven wat het doel is.

9. Register van gegevens verwerkingen

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.

Door de kwartiermakers is in samenspraak met de afdelingen een register van gegevensverwerkingen opgesteld. Inmiddels is er door de VNG een referentie register opgeleverd. Momenteel wordt het register door afdelingshoofden getoetst en herzien. Afdelingshoofden zijn uitvoeringsverantwoordelijken. Zij zullen de processen moeten identificeren en de informatie completeren.

10. Kwaliteitsmanagement

In 2018 en 2019 heeft de gemeente Woensdrecht heel wat werk verzet om de AVG te implementeren in de organisatie, de systemen en de processen. Een aantal maatregelen waren zeer effectief, zoals Het implementeren van het 10 stappenplan van de Autoriteit Persoonsgegevens. Daarnaast is de FG benoemd. Deze heeft de implementatie van kwartiermakers overgenomen. Hij is gestart met een eerste analyse. Vervolgens is het privacy team opgezet om de implementatie verder gevolg te geven. Daarna is er een privacy officer benoemd in tijdelijk dienst om de onafhankelijk rol van de FG niet te schaden.
Om de bewustwording in de organisatie te vergroten is er een leerprogramma opgestart. Dit is tevens ook beschikbaar voor het college en het management. Nieuwe medewerkers worden ook aangemeld voor de e-learning.
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.

11. Beveiliging van de verwerking van persoonsgegevens

Vanuit het algemene behoorlijkheidsbeginsel, het integriteitsbeginsel en het vertrouwelijkheidsbeginsel is het essentieel dat de gemeente Woensdrecht passende technische en organisatorische maatregelen neemt ter beveiliging van persoonsgegevens.
De CISO van de gemeente Woensdrecht heeft hierin de trekkende rol. Maar ook de FG toets en bewaakt de uitvoering.

12. Informatieverstrekking bij de verzameling van persoonsgegevens

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.

13. Bewaren van persoonsgegevens

De AVG geeft geen concrete bewaartermijn voor persoonsgegevens, maar noemt in artikel 5.1 wel opslagbeperking. Hierin wordt aangegeven dat een persoonsgegevens alleen bewaard mag worden als identificeerbaar gegeven, voor zolang het nodig is voor de doeleinden waarvoor het verzameld is. Als de gegevens geanonimiseerd kunnen worden mogende gegevens langer bewaard worden. Het is immers niet meer mogelijk een persoon hiermee direct of indirect te identificeren.

Bij het bewaren van persoonsgegevens kent de AVG een aantal fases. Elke fase heeft eigen regels voor het bewaren van persoonsgegevens. De gebruikersfase, de archiveringsfase en de fase waarin de persoonsgegevens op geen enkele manier (meer) nodig zijn. De gemeente is verplicht de gegevens in

deze fase te wissen, vernietigen of anonimiseren, tenzij in de wet- en regelgeving een andere bewaartermijn is vastgelegd.

Het archiveren en vernietigen van persoonsgegevens vormt een vast onderdeel van het verwerken van persoonsgegevens.
Het aantoonbaar inregelen om te voldoen aan deze vereisten is voor gemeenten een arbeidsintensieve activiteit.
Om inzicht te krijgen in de status wordt er gebruik gemaakt van het register van gegevensverwerkingen.

Deel 2. Vooruitkijken.

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 en 2019 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 2020 en 20121 in het teken staan van planmatige aanpak en toetsing.

Onderstaande zaken zijn op te pakken door het opstellen van een prioriteitenplan. Komende tijd zal dit met het management worden opgesteld. Daarna worden onderstaande zaken gefaseerd opgepakt. Dit is gebaseerd op volwassenheidniveau 3.

1. Het privacybeleid

Aanbevelingen:

- Op organisatieniveau dient de AVG geconcretiseerd te zijn.
- Stem procedures af op het privacy beleid
- Bewaak aantoonbaar organisatie breed de juistheid van beleidsbeslissingen.
- Pas het beleid aan door toepassing van Privacy by Design te beschrijven. Beschrijf de uitvoering van DPIA (data protection impact assessment) ofwel risicoanalyse op de gegevensbescherming.
- Integreer de monitoring van DPIA's in het risicomanagement
- Neem minimale gegevensverwerking op in het privacy beleid.
- Neem de nodige maatregelen om de juistheid en nauwkeurigheid van persoonsgegevens te borgen door periodieke controles uit te voeren op de juiste verwerking en breng hierover rapportage uit aan het management.
- Benoem de bijzondere rechten van kinderen.
- Benoem in het beleid onder informatieveiligheid anonimiseren en pseudonimiseren.
- Beschrijf alle rechten van betrokkenen.
- Benoem daarbij het transparantie beginsel.
- Beschrijf hoe geborgd wordt dat persoonsgegevens niet langer bewaard worden dan voor het doel noodzakelijk.
- Beschrijf hoe geborgd wordt dat persoonsgegevens uitsluitend op rechtmatige manier worden doorgegeven.
- Alle processen in beeld.
- Alle applicaties in beeld.
-

2. Organisatorische inbedding

Aanbevelingen:

- Stel een organisatiebrede matrix op met daarin de verdeling van taken, bevoegdheden en verantwoordelijkheden
- Stel organisatiebreed de onderlinge relatie vast.
- Stel een beleid op van logging.
- Pas actieve logging toe.

3. Risicomanagement en DPIA

Aanbevelingen:

- Stel een organisatiebrede standaard vast van risicomanagement.
- Maak DPIA onderdeel uit van dat risicomanagement.
- Stel risico's formeel vast in een cyclisch proces, organisatiebreed toegepast.

- Stel de te nemen maatregelen formeel vast.
- Maak een organisatiebreed beleid omtrent DPIA als onderdeel van risicomanagement.
- Integreer de monitoring van DPIA's in het risicomanagement.
- Stel een organisatiebreed DPIA proces vast.

4. Risicomanagement en Privacy by Design

Aanbevelingen:
- Maak Privacy by Design onderdeel uit van dat risicomanagement.
- Stel risico's formeel vast in een cyclisch proces, organisatiebreed toegepast.
- Stel de te nemen maatregelen formeel vast.
- Maak een organisatiebreed beleid omtrent Privacy by Design als onderdeel van risicomanagement.

5. Intern toezicht

Aanbevelingen:
- Geef organisatiebreed sturing aan de wijze waarop toezicht plaatsvindt.
- Maak dit toezicht structureel onderdeel van de processen op afdelings- en organisatieniveau.
- Zorg voor periodieke toetsing
- Rapporteer of de gegevensverwerking rechtmatig plaatsvindt.
- Regel cyclisch toezicht.

6. Toegang gegevensverwerking voor betrokkenen

Aanbevelingen:
- Stel vast en leg formeel vast hoe gereageerd moet worden op verzoeken van betrokkenen.
- Biedt in de processen de mogelijkheid tot toegang op afdelings- als op organisatieniveau.
- Regel de wijze van verstrekken van gevraagde informatie organisatiebreed.
- Hanteer vastgestelde richtlijnen om efficiëntie van de toegang te waarborgen.

7. Meldplicht datalekken

Aanbevelingen:
- Communiceer intern de leereffecten voortvloeiend ui de analyse datalekken.

8. Doelbinding gegevensverwerking

Aanbevelingen:
- Bepaal en omschrijf voor alle verzamelingen, verwerkingen, profileringen en doorgiften de doeleinden van rechtvaardiginggronden van een verwerking organisatiebreed op eenduidige wijze.
- Bepaal organisatiebreed en eenduidig hoe dit gebeurt. Richt bewaking hiervoor in.
- Regel dit voorafgaand aan de verwerking van persoonsgegevens

Op het gebied van privacy en gegevensbescherming is er in 2019 winst te behalen. Met name de implementatie van het werkplan privacy verdient komend jaar extra aandacht.

9. Register van gegevensverwerkingen

Aanbevelingen:
- Het register is incompleet. Breng het onder de aandacht van lijnmanagement en laat het aanvullen.
- Dit betreft een dynamisch brondocument, waardoor het steeds up to date gehouden moet worden.
- Borg dit in een proces met afspraken organisatiebreed.
- Gebruik het referentiel register van gegevensverwerkingen dat ter beschikking staat opgesteld door VNG.

10. Kwaliteitsmanagement

Aanbevelingen:

- Bewaak en stel formeel de kwaliteit organisatie breed vast door middel van kwaliteitsmanagement als integraal onderdeel van de processen.
- Informeer betrokkenen organisatiebreed op eenduidige manier.

11. Beveiligen van de verwerking van persoonsgegevens

Aanbevelingen:

- Stel organisatiebreed een informatie beveiligingsplan op, eenduidig vastgelegd en formeel vastgesteld.
- Regel de bewaking van de effectiviteit van de maatregelen op een formeel vastgestelde manier, zowel op uitvoerings-, afdelings- als organisatieniveau. Waardoor elk persoonsgegeven constant aantoonbaar adequaat beveiligd.
- Leg de beveiligingsprocessen organisatiebreed vast en stel deze formeel vast. Het gaat daarmee om taken, bevoegdheden en verantwoordelijkheden op het gebied van informatieveiligheid.

12. Informatieverstrekking bij de verwerking van persoonsgegevens

Aanbevelingen:

- Zorg dat organisatiebreed de keuze of en wanneer informatie wordt verstrekt op een eenduidige wijze geschiedt, is vastgelegd en vastgesteld. Ook de beslissing of een uitzondering op informatieplicht geldt valt hieronder.
- Regel het proces van informeren van betrokkenen organisatiebreed op eenduidige wijze vastgelegd en formeel vastgesteld.

13. Bewaren van persoonsgegevens

Aanbevelingen:

- Bepaal organisatiebreed de bewaartermijnen vastgelegd en formeel vastgesteld. Voor alle verzamelde persoonsgegevens.
- Bepaal organisatiebreed hoe en wanneer persoonsgegevens worden vernietigd. Leg vast en stel formeel vast.
- Bewaak organisatiebreed de te hanteren bewaartermijnen en wijze van vernietiging