Inleiding

De gemeente Heerenveen is zich steeds meer bewust van het belang van het beschermen van persoonsgegevens van haar burgers. We verwerken immers bij de uitoefening van onze taken veel (gevoelige) gegevens van veel (kwetsbare) burgers in veel verschillende domeinen. Daarnaast staan persoonsgegevens van andere burgers, medewerkers, externen en zakenrelaties op de radar.

In de AVG wordt het wettelijk kader beschreven voor het verwerken van persoonsgegevens. Zo dienen we transparant te zijn welke persoonsgegevens we verwerken, voor welk doel en welke grondslag. Tijdens de levensduur 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. Daarnaast 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 onze gemeente.

Onder de verantwoordelijkheid van zowel het college van B&W als de gemeenteraad vindt een groot aantal verwerkingen van persoonsgegevens plaats. Daar vindt extern en intern toezicht op plaats. De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de privacyregels in Nederland. Daarnaast dienen we te beschikken over een interne toezichthouder: de Functionaris Gegevensbescherming (FG). Per mei 2018 is mevrouw. mr. Lucy Huizinga aangesteld als FG.

De FG ziet erop toe dat de AVG intern wordt nageleefd. Het college dient erop toe te zien dat de FG naar behoren en tijdig wordt betrokken bij alle gelegenheden die verband houden met de bescherming van persoonsgegevens. Daarnaast dient de FG ondersteund te worden door haar toegang te verschaffen tot persoonsgegevens en verwerkingen daarvan en haar de benodigde middelen ter beschikking te stellen voor het vervullen van de rol en het in standhouden van haar deskundigheid. In Heerenveen worden taken die verband houden met de rol van de FG uitgevoerd samen met de privacy officers. Het toezicht ligt te allen tijde bij de FG.

De FG brengt jaarlijks een verslag uit aan de verwerkingsverantwoordelijke van zijn werkzaamheden, bevindingen en aanbevelingen. Dit jaarverslag is een afwijking hierop, want deze gaat over de periode 25 mei 2018 tot en met het jaar 2019.

Leeswijzer

Deze jaarrapportage bestaat uit twee onderdelen. In het eerste deel wordt teruggekeken naar de periode van invoering van de AVG (25 mei 2018 tot en met 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 2020 naar een hoger niveau te brengen. Hierbij wordt tevens waar nodig 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). 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.

Deel 1. Terugblik

Het jaar 2018 stond in het teken van het voldoen aan de verplichte onderdelen van de AVG en het jaar 2019 in het teken van de 'lessons learned' na het eerste AVG-jaar en verdere implementaties en verbeteringen. In dit deel van de rapportage zal worden teruggeblikt op hetgeen de gemeente in deze periode heeft bereikt en welke werkzaamheden zijn verricht.

1. Beleid

Het privacybeleid is een kader waarin de gemeente Heerenveen 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.

Er is privacybeleid voor de gehele gemeente opgesteld, dat het Privacyreglement Gemeente Heerenveen heet, waarin wordt uitgelegd hoe de gemeente omgaat met persoonsgegevens en hoe de rollen, taken en verantwoordelijkheden zijn belegd. Het reglement is een uitwerking van de AVG. Hoewel dit beleid nog niet formeel is vastgesteld worden nieuwe ontwikkelingen, verwerkingen of wijzigingen van verwerkingen hier wel aan getoetst. Er is ook een stroomschema opgesteld aan de hand waarvan een medewerker een casus kan doorlopen om te toetsen aan de AVG normen. In het beleid is opgenomen dat het beleid eens per 2 jaar wordt geëvalueerd. Het beleid wordt indien nodig geactualiseerd en verbeterd. Naast algemeen beleid is er ook domein specifiek privacybeleid voor het Sociaal Domein opgesteld. In het Sociaal Domein is dit beleid door middel van trainingen en intervisie uitgedragen.

Bezoekers van de gemeentelijke websites worden voorafgaand geïnformeerd of de gemeente persoonsgegevens via de website verzameld, en zo ja voor welk doel. Op de websites kan in een privacyverklaring worden gelezen hoe de gemeente omgaat met privacy.

2. Processen

De verwerkingen van persoonsgegevens van de gemeente Heerenveen dienen te voldoen aan de AVG. Dit houdt in dat de werkprocessen die verwerking van persoonsgegevens meebrengen, 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[1]) uit te voeren.

Er is een Verwerkingsregister opgesteld waarin staat bij welke werkprocessen er persoonsgegevens worden verwerkt. In het Verwerkingsregister staat wie de verwerkingsverantwoordelijke is, de verwerkingsdoeleinden, de categorieën van betrokkenen, de categorieën van persoonsgegevens, de categorieën van ontvangers, of de gegevens worden doorgegeven aan een derde land of een internationale organisatie, de beoogde termijnen waarbinnen de verschillende categorieën van gegevens moeten worden gewist en de bewaartermijnen. De verwerkingen die zijn opgenomen zijn getoetst aan rechtmatigheid en doelbinding. De verwerkingen moeten nog getoetst worden aan de andere beginselen waarbij met name aandacht moet worden besteed aan transparantie en dataminimalisatie. In het Verwerkingsregister is verder vastgelegd welke technische en organisatorische maatregelen worden genomen om privacyrisico's af te dekken, dan wel in te perken. Het register is gepubliceerd en vindbaar op de website

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

van de gemeente Heerenveen. De afdeling JzenI zorgt op aanwijzing van de afdelingen ervoor dat wijzigingen van de bestaande verwerkingen of het toevoegen van nieuwe verwerkingen worden verwerkt. Er wordt nog gewerkt aan een procedure om het Verwerkingsregister up to date te houden.

Om de werkprocessen te toetsen en ingericht te hebben volgens de beginselen van de AVG is het van belang dat de medewerkers op de afdelingen weten hoe deze beginselen toegepast moeten worden. Hiervoor is ingezet op bewustwording, door onder meer voorlichtingen op de verschillende afdelingen. Daarnaast zijn er privacy adviseurs op de afdelingen aangewezen als vraagbaak voor de directe collega's, zodat er doorlopend op de afdeling aandacht besteed wordt aan wat gegevensbescherming en de privacywetgeving concreet betekenen voor de betreffende afdeling en hoe medewerkers om dienen te gaan met persoonsgegevens binnen hun taken en werkzaamheden.

Bij nieuwe verwerkingen of bij de aanschaf van nieuwe systemen moet voorafgaand in kaart worden gebracht of deze een hoog privacyrisico met zich meebrengen. Er is een checklist gemaakt om te kunnen beoordelen of dit het geval is en zo ja, dan wordt er een DPIA uitgevoerd. Er is nog geen proces voor het uitvoeren van de DPIA vastgesteld maar er is al wel ervaring opgedaan met het doen van een DPIA.

Voor de DPIA wordt het format van de IBD gebruikt. De verantwoordelijke voor de verwerking of systeem zorgt ervoor dat er een DPIA wordt gedaan. De ondersteuning bij de DPIA wordt gedaan door JzenI waar ook de juridische toets plaatsvindt. De FG adviseert in het proces. De rapportage van de uitgevoerde DPIA met het advies van de FG wordt ter besluitvorming voorgelegd aan de verantwoordelijke. In het format van de DPIA is opgenomen dat de verantwoordelijke motiveert als de besluitvorming afwijkt van het advies van de FG. Het is van belang om de uitkomsten van de DPIA en het advies van de FG te delen met de betrokken medewerkers zodat duidelijk is waar de risico's liggen en welke maatregelen er genomen moeten worden.

De uitgevoerde DPIA's moeten periodiek geactualiseerd worden. Om overzicht te hebben over wanneer de actualisering moet plaatsvinden, zal in het vervolg in het Verwerkingsregister opgenomen worden dat de DPIA is uitgevoerd met vermelding van het jaar waarin deze is uitgevoerd. Actualisatie moet ten minste om de drie jaar plaatsvinden of vaker indien nodig, zoals bij wijzigingen in bestaande verwerkingen. De maatregelen die uit de DPIA voortvloeien moeten worden opgenomen in een bestand zodat deze inzichtelijk zijn en gemonitord kunnen worden. Er is nog geen bestand waar dit overzichtelijk in opgenomen is. Van belang is in ieder geval dat tijdig aangegeven wordt dat er een DPIA moeten worden uitgevoerd omdat het uitvoeren van een DPIA tijd kost. Nu er steeds meer DPIA's uitgevoerd gaan worden, is het ook steeds belangrijker om een overzicht te hebben van te houden en gehouden DPIA's.

In bijlage 2 is een overzicht opgenomen van de uitgevoerde DPIA's.

3. 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 het creëren van bewustzijn. Alle onderdelen die in dit jaarverslag genoemd worden, zorgen tezamen voor een organisatorische inbedding van de AVG.

In 2018 is er een FG aangesteld. De FG heeft de wettelijke taken die in de AVG worden benoemd. Naast de FG hebben een aantal juridische adviseurs binnen JzenI de taak van Privacy Officer. De Privacy Officers adviseren op casusniveau over de bescherming en verwerking van persoonsgegevens. Er is een emailadres privacy@heerenveen.nl waarmee contact kan worden opgenomen met de FG of de Privacy Officers. De FG en de

Privacy Officers hebben wekelijks overleg om te kijken welke vragen er spelen. Daarnaast wordt gekeken naar ontwikkelingen in de organisatie om te kijken waar advies nodig is en wordt er dan contact gezocht met de betreffende medewerkers.
De FG heeft ook een keer in de maand een overleg met alle Friese FG's. Hier wordt gekeken naar kennisdeling en mogelijkheden om gezamenlijk op te trekken.

Bij de voorlichtingen op de afdelingen is benoemd wie de FG is en wat de taken zijn. Hier kan echter nog wel meer aandacht aan besteed worden. De FG wordt nog niet altijd (tijdig) betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. Doordat er aandacht is besteed aan de DPIA checklist wordt dit wel steeds meer gedaan.

Op basis van het Organisatiebesluit is elk afdelingshoofd verantwoordelijk voor privacy binnen zijn/haar afdeling. De afdelingshoofden nemen deze verantwoordelijkheid ook steeds meer. In 2019 is er met elk afdelingshoofd gesproken over het Plan van aanpak om te komen tot borging van de AVG. Om de afdelingshoofden te ondersteunen hebben zij privacy adviseurs op de afdeling aangewezen. De rol van privacy adviseur moet in 2020 meer vorm krijgen. Hiermee is een extra impuls gegeven om de AVG op de afdeling te borgen.

Er is in 2018 en 2019 ingezet op bewustwording. Elke afdeling is geïnformeerd over de beginselen van de AVG en het belang van privacy. Daarnaast konden de medewerkers een e-learning doen en is er een pagina op fean@work waar alle informatie over de AVG staat.

De Ondernemingsraad heeft een rol wanneer het gaat om het verwerken en beschermen van de persoonsgegevens van de medewerkers. De OR wordt hierbij betrokken.

4. Rechten van betrokkenen

De gemeente dient degene van wie zij de persoonsgegevens verwerkt (betrokkene) zowel actief als passief te informeren over het feit dat gegevens worden verwerkt, 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 moet de betrokkene, op het moment dat verwerking van persoonsgegevens plaatsvindt, hierover informeren. Dit informatierecht vangt aan bij het vragen van persoonsgegevens (aan betrokkene) of bij de eerste verwerking van de persoonsgegevens (bij gegevens verkregen van anderen). Zo is er voor het Sociaal Domein een folder gemaakt die aan melders en aanvragers wordt overhandigd. Daarnaast is het Verwerkingsregister openbaar en beschikbaar voor betrokkenen. Op zijn/haar verzoek verstrekt de gemeente informatie aan de betrokkene. Nog niet bij elke verwerking is nagegaan of de betrokken voldoende wordt geïnformeerd.

Betrokkenen hebben de mogelijkheid om te controleren of, en op welke manier, zijn/haar gegevens worden verwerkt. En wanneer gegevens verwerkt worden, hebben zij het recht om inzage te verkrijgen in de persoonsgegevens die verwerkt worden. Hiervoor is een proces vastgesteld. Op de website staat een formulier waar betrokkenen hun verzoek mee kunnen indienen. Bij dit formulier wordt aangegeven dat zij zich na indiening dienen te legitimeren aan de balie van burgerzaken. Als dit niet mogelijk is, dan wordt er naar andere mogelijkheden gekeken. Het verzoek komt bij IenI binnen die dan na bevestiging dat legitimatie heeft plaatsgevonden, gaat kijken welke informatie er over betrokkenen wordt verwerkt. JzenI ondersteunt bij deze procedure. Een verzoek wordt in beginsel binnen vier weken afgehandeld tenzij het een omvangrijk verzoek is.

Als duidelijk wordt dat de gegevens niet kloppen, kan de betrokkene een verzoek indienen bij de gemeente om dit te corrigeren. Deze wijziging moet meteen plaatsvinden. Met inachtneming van de doeleinden van de verwerking heeft de betrokkene ook het recht onvolledige persoonsgegevens aan te vullen.

In gevallen waar de betrokkene toestemming heeft gegeven om gegevens te verwerken, heeft de betrokkene het recht om de persoonsgegevens te laten verwijderen (recht op gegevenswissing (vergetelheid).
Voor de gemeente geldt in het algemeen dat er sprake is een afhankelijke relatie zodat toestemming niet vrijelijk kan worden gegeven. De gemeente heeft inzichtelijk wanneer toestemming wel als grondslag voor de verwerking moet worden gebruikt en aan welke randvoorwaarden de toestemming moet voldoen. In dergelijke situaties die met name in het Sociaal Domein zich voordoen, moet er ook nog een andere grondslag aanwezig zijn om persoonsgegevens te verwerken. Voor het Posthuis geldt wel dat er sprake is van toestemming. Hier is dan ook geregeld dat de toestemming op een eenvoudige wijze weer kan worden ingetrokken.

Het recht op dataportabiliteit komt bij de gemeente niet voor. Er is ook geen proces voor het gebruik maken van het recht op bezwaar (verzet). Deze processen ontbreken omdat het rechten betreffen die de inwoners bij de gemeente in feite niet kunnen uitoefenen, omdat de gemeente de grondslag gerechtvaardigd belang niet mag gebruiken bij haar gemeentelijke taken. Ook vind er geen geautomatiseerde besluitvorming plaats.

In het privacyreglement is opgenomen dat de gemeente Heerenveen de rechten van betrokkenen honoreert tenzij regelgeving zich hier tegen verzet. Een beslissing op een dergelijk verzoek is een besluit waar bezwaar en beroep tegen mogelijk is.

In bijlage 3 is een overzicht opgenomen van de verzoeken van betrokkenen voor het jaar 2018 en 2019 en het aantal bezwaren.

5. Samenwerking

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

In het Verwerkingsregister is ook opgenomen aan welke derde partij persoonsgegevens worden verstrekt. Hier staat ook wie verwerkingsverantwoordelijk is. Bij het inschakelen van externe partijen wordt gekeken of er sprake is van verwerken van gegevens en worden afspraken gemaakt over de verwerking. Hiervoor wordt zoveel mogelijk de standaardovereenkomst van de VNG gebruikt. Ook is de AVG verwerkt in Algemene Voorwaarden die van toepassing worden verklaard op elke overeenkomst. Alle overeenkomsten zijn geïnventariseerd en waar nodig is er een verwerkersovereenkomst afgesloten. Uit de inventarisatie bleek dat niet altijd inzichtelijk was bij welke overeenkomst er sprake was van het verwerken van persoonsgegevens.

Ook in samenwerkingsverbanden worden er afspraken gemaakt over hoe er wordt omgegaan met persoonsgegevens.

6. Beveiliging

Vanuit het algemene behoorlijkheidsbeginsel, het integriteitsbeginsel en het vertrouwelijkheidsbeginsel is het essentieel dat de gemeente Heerenveen 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).

Er is een protocol datalekken dat gevolgd wordt als er een melding wordt gedaan. De CISO heeft meerdere informatierondes gedaan om uit te leggen wanneer er sprake is van een datalek. Ook in de informatieronde over de AVG is hier aandacht aan besteed. Medewerkers zijn in grote lijnen op de hoogte van de definitie van een datalek en weten bij wie zij een datalek intern moeten melden. Op fean@work komt een meldknop zodat het nog makkelijker voor medewerkers wordt om het datalek te melden. Er is een datalekregister waarin de meldingen worden geregistreerd. Hierin staat ook de afweging of er sprake is van een datalek dat gemeld moet worden bij de AP. Als dit het geval is, dan wordt dit gedaan onder verantwoordelijkheid van de feitelijke verantwoordelijke met ondersteuning van de PO, CISO en FG. Uit de meldingen die zijn gedaan blijkt dat medewerkers niet altijd inzichtelijk hebben wat ze moeten doen om de risico’s te beperken. Hier kan nog extra op ingezet worden.

De beveiligingsmaatregelen binnen de gemeente Heerenveen hebben een passend niveau van beveiliging. Deze maatregelen worden periodiek getest en geëvalueerd.

Voor de geautomatiseerde systemen zijn autorisatieschema’s vastgesteld. Medewerkers hebben binnen de systemen alleen toegang tot die gegevens die zij nodig hebben ter uitvoering van hun werkzaamheden. De toegangsrechten worden actief aangepast wanneer een medewerker uit dienst treedt of van functie verandert. Een van de onderdelen die genoemd wordt om te kunnen verantwoorden dat de toegangsrechten ook op een juiste manier worden toegepast is logging. De gemeente Heerenveen kent een aantal systemen die loggen. Elk afdelingshoofd is hier zelf verantwoordelijk voor. Geadviseerd wordt om loggingsbeleid te hebben zodat het voor medewerkers duidelijk is dat er gelogd wordt en wat er gelogd wordt. Logging wordt steeds belangrijker om ook aan de inwoners te kunnen laten zien dat hun gegevens alleen verwerkt worden door de aangewezen personen.

Bij een nieuwe verwerking of nieuw systeem wordt er rekening gehouden met de privacy van betrokkenen en de AVG beginselen. Door de checklist voor de DPIA te gebruiken kan hier een goede afweging in gemaakt worden.

Met de afdeling IenI is besproken dat bij het inrichten van systemen de meest privacy vriendelijke instellingen worden aangehouden. Hierbij wordt er voor gezorgd dat er niet meer gegevens worden uitgevraagd dan noodzakelijk is.

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

7. Verantwoording

De AVG legt de verantwoordelijkheid bij de organisatie zelf om aan te tonen dat deze voldoet aan de privacyregels. Door te voldoen aan de verantwoordingsplicht, levert de organisatie een belangrijke bijdrage aan de bescherming van het privacy-grondrecht van mensen. 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.

De verantwoording wordt gedaan aan de hand van het Verwerkingsregister, het vastleggen van de uitkomsten van privacy by design, de DPIA's en het documenteren van de incidenten in verband met persoonsgegevens.
Door de processen die opgenomen zijn in het Verwerkingsregister te toetsen kan de organisatie laten zien dat ze aan de AVG voldoet. Zo worden ook periodiek controles uitgevoerd om de juiste werking van de getroffen beveiligingsmaatregelen te controleren.

In 2019 is nog ingezet op de implementatie van de AVG. In 2020 zal de toetsing worden meegenomen in de interne controle en ook zal de FG controles uitvoeren.

8. Conclusie

In 2018 en 2019 heeft de gemeente Heerenveen heel wat werk verzet om de AVG te implementeren in de organisatie, de systemen en de processen. Er is op korte termijn voor gezorgd dat de gemeente de juiste maatregelen kan nemen om aan de AVG te voldoen. Vooral het maken van het verwerkingsregister was een grote klus die samen met de afdelingen is geklaard.

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 meer 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 de AVG en de verdere implementatie en verbeteringen, zal in 2020 de borging in de processen centraal staan.

1. Beleid

Aanbevelingen:
Zorg ervoor dat het privacybeleid door middel van het Privacyreglement wordt vastgesteld door het verantwoordelijke bestuursorgaan en dat dit beleid door het MT actief wordt uitgedragen.

2. Processen

Aanbevelingen:
Zorg ervoor dat er een proces is waarbij het Verwerkingsregister actueel wordt gehouden. Bespreek dit proces met de afdelingshoofden en medewerkers zodat het voor iedereen duidelijk is hoe ze het register up to date kunnen houden.

Zorg ervoor dat in de werkprocessen aandacht wordt besteed 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.

Zorg ervoor dat in de werkprocessen aandacht wordt besteed aan dataminimalisatie en zorg ervoor dat betrokkenen meer vooraf geïnformeerd worden over wat er met hun persoonsgegevens gebeurt.

Zorg ervoor dat er aandacht blijft voor de rechtspraak over privacy, standpunten van de AP en toekomstige wetgeving over de gegevensdeling in het sociaal domein en integraal werken.

Zorg ervoor dat er een proces is voor het uitvoeren en actualiseren van een DPIA.

3. Organisatorische inbedding

Aanbevelingen:
Zorg dat er aandacht blijft voor bewustwording.

Omschrijf de taken van de FG duidelijk en zorg ervoor dat iedereen zich bewust is wanneer de FG betrokken dient te worden en dat dit tijdig gebeurt.

Zorg dat de AVG (verder) geborgd wordt op de afdelingen en privacy adviseurs hierin een rol krijgen.

4. Rechten van betrokkenen

Aanbevelingen:
Zorg ervoor dat onderzocht wordt of het aanbeveling verdient om de uitoefening van de rechten van betrokkenen te centraliseren in een systeem.

5. Samenwerking

Aanbevelingen:

Er is veel moeite gedaan om alle overeenkomsten waar een verwerkersovereenkomst bij moest worden afgesloten in kaart te brengen. Zorg ervoor dat dit op orde blijft.

Zorg ervoor dat het Verwerkingsregister actueel blijft bij het inschakelen van een derde.

Zorg ervoor dat er een overzicht is van alle afspraken met (keten-)partners die gemaakt zijn.

Zorg ervoor dat het inzichtelijk is of er verwerkingen zijn waar de gemeente verwerker is en zo ja, neem dit op in het Verwerkingsregister.

6. Beveiliging

Aanbevelingen:
Zorg ervoor dat het voor de medewerkers duidelijk is welke stappen zij moeten zetten bij de ontdekking van een datalek (direct melden en welke actie ondernomen moet worden om de risico's te verkleinen).

Zorg ervoor dat duidelijk wordt hoe de gemeente om wil gaan met logging en bespreek dit met de OR.

7. Verantwoording

Aanbevelingen:
Zorg ervoor dat het Verwerkingsregister actueel is en getoetst wordt.

Zorg ervoor dat er aandacht blijft voor de maatregelen die voortvloeien uit de DPIA en dat deze worden gemonitord.

Zorg ervoor dat te allen tijde in werkprocessen waar toch de grondslag van toestemming wordt gebruikt, er een proces is voor het geven, vastleggen en (het eenvoudig) intrekken van de toestemming.

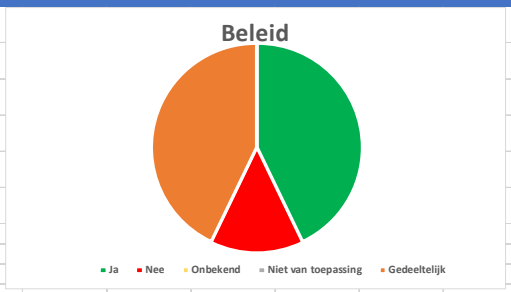
8. Conclusies

Op het gebied van privacy en gegevensbescherming is er in 2020 winst te behalen. Met name het uitvoeren van DPIA's, de toetsing van de processen en het vergroten van de zichtbaarheid van de FG verdienen komend jaar extra aandacht. Vooral het uitvoeren van DPIA's is nieuw. Dit kost dan zowel de afdelingen als JzenI tijd. Hier is nog geen rekening mee gehouden en dit betekent dat er een organisatie brede prioritering moet komen bij nieuwe verwerkingen en aankoop van nieuwe systemen.

Bijlage 1 - Stand van zaken AVG per onderwerp

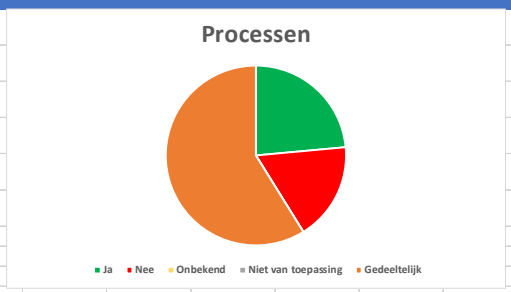
Beleid

Resultaat	Aantal
Ja	6
Nee	2
Onbekend	0
Niet van toepassing	0
Gedeeltelijk	6



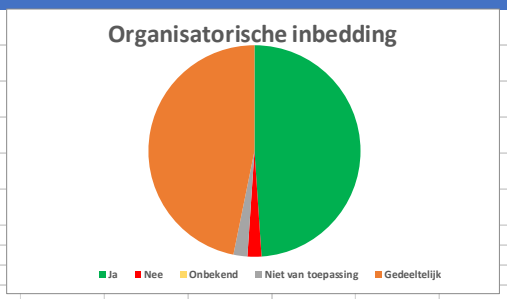
Processen

Resultaat	Aantal
Ja	8
Nee	6
Onbekend	0
Niet van toepassing	0
Gedeeltelijk	20



Organisatorische inbedding

Resultaat	Aantal
Ja	23
Nee	1
Onbekend	0
Niet van toepassing	1
Gedeeltelijk	22



Rechten van betrokkenen

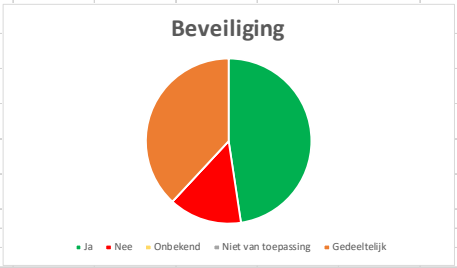
Resultaat	Aantal
Ja	22
Nee	0
Onbekend	0
Niet van toepassing	4
Gedeeltelijk	7

Samenwerking

Resultaat	Aantal
Ja	9
Nee	0
Onbekend	0
Niet van toepassing	0
Gedeeltelijk	10

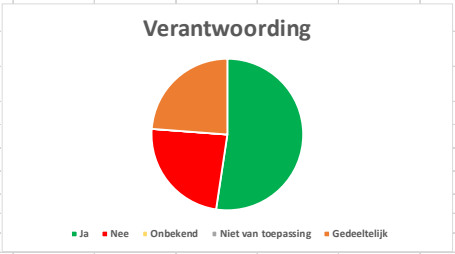
Beveiliging

Resultaat	Aantal
Ja	10
Nee	3
Onbekend	0
Niet van toepassing	0
Gedeeltelijk	8



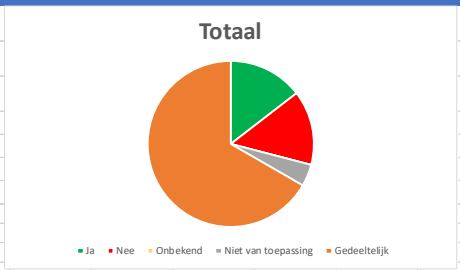
Verantwoording

Resultaat	Aantal
Ja	11
Nee	5
Onbekend	0
Niet van toepassing	0
Gedeeltelijk	5



Totaal

Resultaat	Aantal
Ja	17
Nee	17
Onbekend	0
Niet van toepassing	5
Gedeeltelijk	78



Bijlage 2 - Overzicht DPIA’s

Onderwerp DPIA	**Datum**	**Status**
DPIA door SDF naar aanleiding van de HUB. Advisering door FG.	2019	Afgerond
Ketenvoorziening Voetbal Advisering door FG	2019	Afgerond
WvGGZ	2019	In behandeling
Jeugd	2019	In behandeling

Bijlage 3 - Overzicht rechten van betrokkenen

Zaak	Datum	AVG-recht	Opmerking
Verzoek om inzage in ingediend formulier.	25-05-2018	Inzage	Op 5 juli 2018 is het besluit aan verzoeker verzonden, met afwijzing van het verzoek om inzage omdat recht niet tevens een recht op inzage in stukken betekent.
Verzoek om inzage in verwerkte persoonsgegevens.	13-06-2018	Inzage	Op 12 juli 2018 is het verzoek afgehandeld in inzage gegeven.
Verzoek om inzage in verwerkingsregister.	14-06-2018	Inzage	Op 18 juli 2018 verzoeker verwezen naar het openbare register.
Verzoek om inzage in verwerkingsregister (tweede verzoek).	14-06-2018	Inzage	Op 18 juli 2018 verzoeker verwezen naar het openbare register.
Verzoek om inzage in alle persoonsgegevens.	19-06-2018	Inzage	Op 19 juli 2018 is het verzoek afgehandeld en informatie verstrekt over verwerkingen.
Verzoek om uitschrijving van adres middels inzageformulier.	21-09-2018	Inzage	Op 27 september 2018 is besluit verzonden dat dit geen inzageverzoek betreft.
Verzoek om informatie gegevensdeling.	28-11-2018	Inzage	Op 19 december 2018 is het verzoek afgehandeld en aan verzoeker informatie verstrekt.
Verzoek om wissen van alle persoonsgegevens van verzoeker.	25-05-2019	Verwijdering	Het verzoek is op 23 juli 2019 buiten behandeling gesteld, wegens het achterwege blijven van identificatie.
Verzoek om inzage in persoonsgegevens.	13-08-2019	Inzage	Op 27 september 2019 buiten behandeling gesteld, wegens het achterwege blijven van identificatie.
Verzoek om inzage in persoonsgegevens.	26-09-2019	Inzage	Het verzoek is op 10 december 2019 buiten behandeling gesteld, wegens het achterwege blijven van identificatie.
Verzoek om verwijdering naam gepubliceerd document.	21-10-2019	Verwijdering	Op 30 oktober 2019 is het verzoek afgehandeld.

Bijlage 4 - Overzicht datalekken

In deze bijlage wordt een overzicht gegeven van de belangrijkste datalekken in 2018 en 2019 en daarbij is aangegeven of deze wel/niet zijn gemeld aan de AP en de burger, plus welke maatregelen de organisatie heeft genomen om de risico's weg te nemen.

Datalek	**Gemeld aan AP**	**Gemeld aan betrokkenen**	**Mitigerende maatregelen**
19-10-2018 Niet geanonimiseerde besluitenlijst gedeeld met derden.	Nee	Nee	Aandacht besteed aan bewustwording en anonimisering.
19-11-2018 Verzending van persoonsgegevens aan verwerker per e-mail zonder Cryptshare	Nee	Nee	Aandacht besteed aan juiste wijze van verzending; vernietiging van e-mail hoefde niet plaats te vinden, want was aan juiste partij verstrekt.
18-12-2018 Verzending van te veel gegevens aan een verwerker.	Nee	Nee	Leverancier software gevraagd om data uitwisseling aan te passen.
24-06-2019 Mail naar verkeerde ontvanger gestuurd.	Nee	Nee	Ontvanger direct gevraagd om mail ongelezen te verwijderen en dat is gebeurd.
04-12-2019 Een bijlage bij een brief met persoonsgegevens is per e-mail naar verkeerde ontvanger gestuurd.	Nee	Nee	Ontvanger direct gevraagd om mail ongelezen te verwijderen en dat is gebeurd.