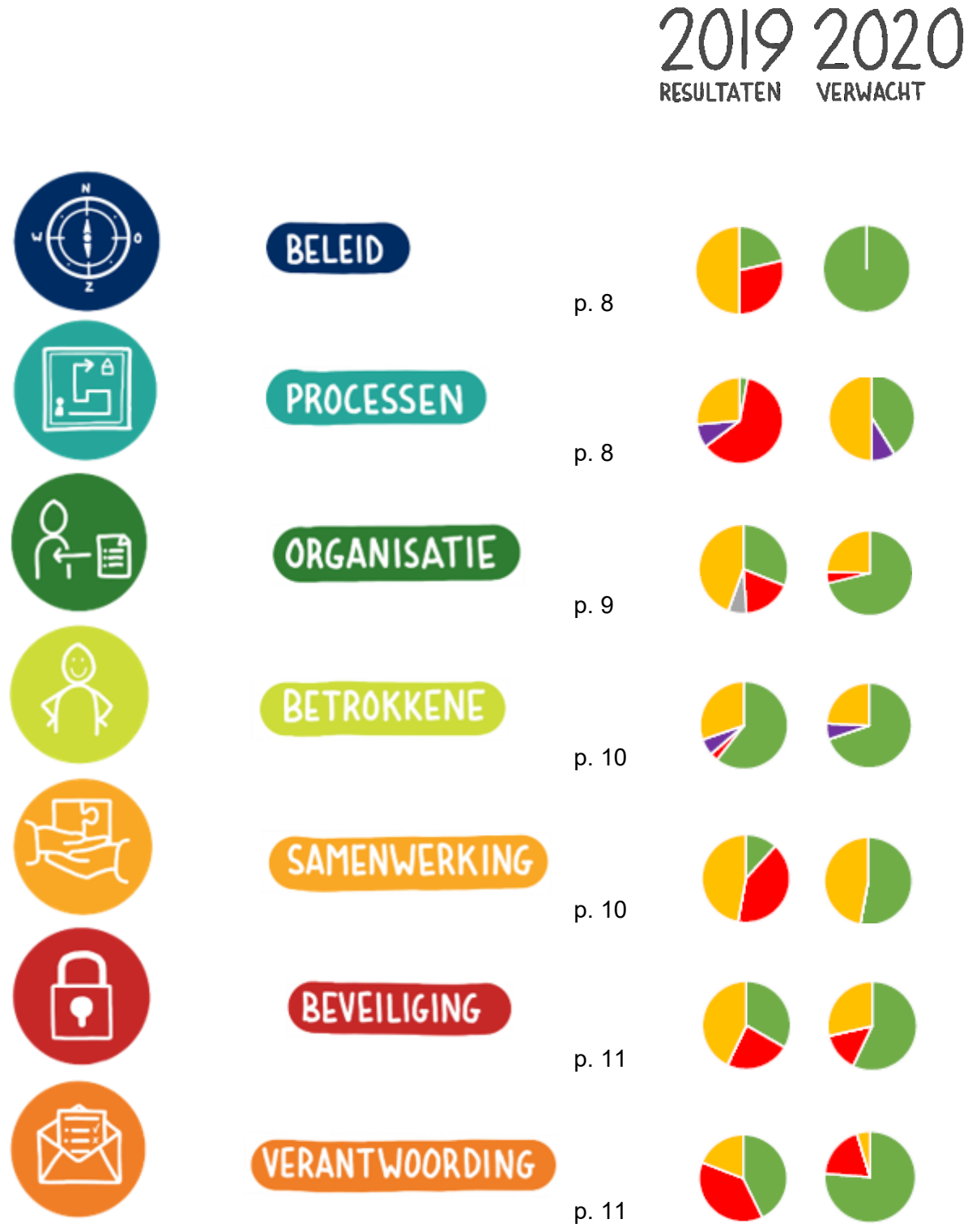
de BUCH

Jaarrapportage gegevensbescherming 2019

Jaarrapportage voor het college van Burgemeester en Wethouders

Gemeenten Bergen (NH), Uitgeest, Castricum en Heiloo

FG Jaarrapportage 2019
College van B&W



Voorwoord

Het is de hoofdtaak van een Functionaris Gegevensbescherming (FG) om er onafhankelijk op toe te zien dat de organisatie persoonsgegevens verwerkt conform de vigerende wetgeving op het gebied van de bescherming van persoonsgegevens. De Algemene Verordening Gegevensbescherming (AVG) vormt hiervoor de basis.

De FG moet zijn taken met voldoende onafhankelijkheid kunnen uitvoeren. De FG mag van de hoogste geplaatste functionaris of andere functionarissen in de organisatie geen instructies ontvangen met betrekking tot de uitvoering van zijn taken: hij moet in staat zijn om zijn taken en verplichtingen onafhankelijk in te vullen. Aan de genoemde randvoorwaarden heeft de Werkorganisatie voldaan.

Dit jaaroverzicht is opgesteld binnen de kaders van de gedragsnormen van het Nederlands genootschap voor FG's (het NGFG). Het heeft betrekking op de verwerkingen van persoonsgegevens die onder verantwoordelijkheid van het college van B&W bij de Werkorganisatie BUCH zijn gedaan. Het management van de Werkorganisatie de BUCH hebben kennisgenomen van de resultaten in een MT-versie van het jaaroverzicht. Voorliggend document is de bestuurlijke rapportage voor het college van B&W, en is gebaseerd op de MT-versie. Met deze jaarrapportage rapporteert de FG rechtstreeks aan het hoogst verantwoordelijke orgaan dat verantwoordelijk is voor de verwerking van persoonsgegevens waar de FG toezicht op houdt.
Met voorliggende jaarrapportage kan het college van B&W horizontaal verantwoording afleggen aan de gemeenteraad.

Youri Lammerts van Bueren
Functionaris voorde Gegevensbescherming (FG)
18.9.2020

Samenvatting

De Algemene Verordening Gegevensbescherming
Het jaar 2019 was een interessant vervolg op het eerste jaar van de Algemene Verordening Gegevensbescherming (AVG). De AVG bevat veel open normen. Afgelopen periode hebben gemeenten veel kennis uitgewisseld en producten met elkaar gedeeld om van elkaar te leren. De Informatiebeveiligingsdienst voor Gemeenten (IBD/VNG) heeft hierin een aanjagende rol. Ontwikkelingen in rechtspraak en wetgeving hebben daarbij ook meer duidelijkheid geboden bij de interpretatie van de open normen uit de AVG. De verhoogde aandacht voor het beschermen van de privacy van burgers stond centraal in 2019. De overheid heeft hierin een belangrijke voorbeeldfunctie.

Opzet jaarrapportage
In deze jaarrapportage is beschreven welke acties en maatregelen in 2019 zijn genomen om de doelstellingen en beginselen uit de AVG te behalen en te waarborgen. Ook geeft dit document een doorkijk naar de verwachte uitgevoerde acties en maatregelen in 2020. Adequaat omgaan met persoonsgegevens is een blijvend proces en zal dan ook aandacht blijven vergen van zowel bestuur, management als medewerkers.

Spanning tussen privacy-ambitie en beschikbare resources waren zichtbaar
Afgelopen periode (2019-2020) was spanning tussen de privacy-ambities en de beschikbare resources om dit aan te sturen. Werkorganisatie de BUCH heeft privacy (net als informatiebeveiliging) als een van haar speerpunten benoemd. In 2017 was eerder alleen nog een Chief Information Security Officer (CISO); in 2018 werd een privacy-officer (1 FTE) aangesteld en een onafhankelijke functionaris voor de Gegevensbescherming aangewezen (+/- 8 uur per maand). In 2019 en 2020 vond een wisseling plaats op de functie van CISO. In 2020 is de privacy-officer naar een parttime functie gegaan (0,6), en wordt per 1.6.2020 de FG-functie door een andere onafhankelijk persoon ingevuld. Door het spanningsveld tussen ambities en beschikbare resources lag de focus in 2019 op het beheren van de dagelijkse privacy-activiteiten. Dit bestond uit het afhandelen van datalekken en verzoeken van betrokkenen, als ook het adviseren van de organisatie (gevraagd en ongevraagd). Hierdoor was minder tijd beschikbaar om in te zetten op het verder inbedden van de AVG.

De Werkorganisatie heeft laten weten dat het bezig is met formatie-uitbreiding voor privacy, zodat aansluiting wordt gevonden op de privacy ambities. Er komt 1 FTE voor de functie van privacy-officer erbij en de formatie van de FG groeit door van 2 uur in de week naar 12 uur in de week. Deze functies zullen begin 2021 worden geworven. Dit is randvoorwaardelijk om de naleving van de open normen van de AVG verder in te bedden, en is daarmee ook een positieve ontwikkeling dat vertrouwen geeft in de inbedding en naleving van de AVG.

Samenvatting resultaten
De mate waarin de Werkorganisatie compliant is aan de AVG is onderzocht door de vorige FG aan de hand van een vragenlijst met 185 vragen.[1] Deze zijn op thema gerubriceerd. De organisatie is beoordeeld op de thema's beleid, processen, organisatorische inbedding, rechten van betrokkenen, samenwerking, beveiliging en verantwoording. Overzicht 1, op de volgende pagina, geeft de gemiddelde totaalscore weer.

Er is in 2018 een goede start gemaakt met het voldoen aan de nieuwe privacywetgeving, echter in 2019 heeft de organisatie, door verklaarbare omstandigheden, weinig voortuitgang geboekt. Er is op iets minder dan 1/3 van het totaal te behalen punten volmondig 'Ja' geantwoord (zie overzicht 1). Ongeveer net zoveel met 'Nee', en iets meer dan 1/3 is een criterium 'Gedeeltelijk' aantoonbaar ingevoerd. De antwoorden zijn eerst in concept beantwoord door de FG en later bekrachtigd door de Privacy-officer en de CISO.

Als een criterium een 'Nee' of 'Gedeeltelijk' scoort is onderzocht wat daarvan de oorzaak is. Hiervoor zijn aanbevelingen gedaan aan het management van de Werkorganisatie de BUCH.

Op het thema Rechten van betrokkenen scoort de organisatie het hoogst. De thema's Processen, Verantwoording en Samenwerking scoren verhoudingsgewijs laag. Voornamelijke reden was dat de processen nog niet privacy-proof zijn opgeschreven en ingericht, waarmee de verplichte aantoonbaarheid nog niet kan worden bevestigd.
In het bedrijfsonderdeel Samenleving is, zoals te verwachten, het privacy-bewustzijn het hoogst. Echter daar is de opbouw van de huidige dossiers niet conform de richtlijnen uitgevoerd. Met name in het WMO-domein zijn gezondheidsgegevens verwerkt waarvan de rechtmatigheid ontbreekt. Deze vormen een risico en veroorzaken extra werk indien er een inzageverzoek wordt ingediend.

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

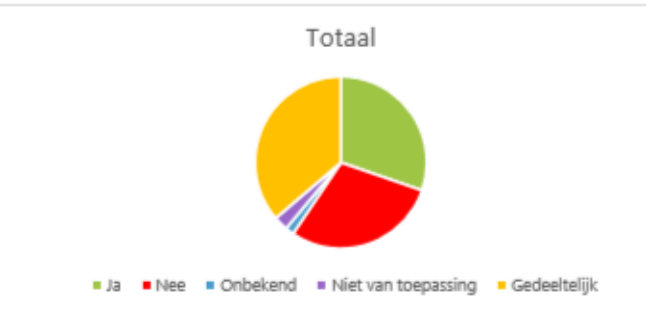
In de andere bedrijfsonderdelen is vaak niet bekend dat voor de uitvoering van werkzaamheden er altijd gewerkt moet worden met juiste gegevens wat wil zeggen dat deze gekoppeld zouden moeten zijn aan brondata (BRP, GBV-V, BAG etc). Dit heeft tot diverse datalekken geleid die vermijdbaar waren.

De beschikbare uren voor onderzoek en toezicht op de inbedding van de AVG is in de afgelopen periode erg beperkt gebleken. De observaties die in deze rapportages zijn opgenomen kunnen daarom geen compleet en gedetailleerd beeld geven. Deze audit is daarom op hoofdlijnen beschreven.

Conclusie van de FG is dat er in niet voldoende mate is voldaan aan de AVG en dat er op verschillende onderdelen niet conform de eisen van de privacywetgeving wordt gewerkt. De wil bij de meeste betrokken medewerkers is er zeker en mijn verwachting is dat met voldoende ondersteuning de score in het komende tijdvak ruim omhoog zal kunnen gaan.

Overzicht 1 Resultaat op de 185 vragen over periode mei 2019 – mei 2020 (in tabel en diagram-vorm)

Totaal	
Resultaat	**Aantal**
Ja	56
Nee	54
Onbekend	3
Niet van toepassing	5
Gedeeltelijk	67
Totaal vragen	185



De privacy-officer heeft op basis van een zelfevaluatie op dezelfde vragenlijst in beeld gebracht hoe de totaalscore over 2020 zal zijn. Overzicht twee geeft de totaalscore van 2019 en 2020 weer

Overzicht 2 Vergelijk totaalscore: links eindstand mei 2020, rechts verwachte eindstand december 2020

Als de Werkorganisatie de BUCH eind 2020 haar verwachtingen waar maakt en deze lijn doortrekt in 2021 met ondersteuning van aanvullende structurele mankracht, dan zal de in te halen achterstand aanzienlijk gereduceerd moeten zijn en de AVG in beginsel goed geborgd zijn.

Inhoudsopgave

Inleiding

Werkorganisatie de BUCH verwerkt veel (gevoelige) persoonsgegevens van veel (kwetsbare) inwoners bij de uitoefening van haar taken. Daarnaast worden ook persoonsgegevens verwerkt van andere burgers, medewerkers, externen en ondernemers.

In de AVG wordt het wettelijk kader beschreven voor het verwerken van persoonsgegevens. Werkorganisatie de BUCH verwerkt namens de gemeente veel persoonsgegevens, waar het college van B&W voor verantwoordelijk is en blijft. Zo dient het college ervoor te zorgen dat verwerkingen van persoonsgegevens transparant zijn, voor welk doel en welke grondslag. Tijdens de levensduur van persoonsgegevens moeten deze goed worden beveiligd, mogen ze niet zomaar voor een ander doel worden verwerkt en moeten ze na afloop worden vernietigd of geanonimiseerd. Daarnaast zijn er ook tal van privacyregels in sectorspecifieke wetgeving. Dit alles heeft gevolgen voor de inrichting van processen en systemen in en van de Werkorganisatie de BUCH.

Onder de verantwoordelijkheid van zowel het college van B&W als 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 is de Functionaris Gegevensbescherming (FG) de interne toezichthouder. Tot juni 2020 was Wendeline Sjouwerman de FG voor de gemeente en Werkorganisatie de BUCH. Zij heeft de meting verricht en de jaarrapportage voor het MT opgesteld. Sinds juni 2020 is Youri Lammerts van Bueren tijdelijk de FG, totdat deze functie in 2021 structureel wordt ingevuld (voor 12 uur per week). Youri Lammerts van Bueren heeft de bestuurlijke jaarrapportage opgesteld, op basis van de bevindingen van vorige FG (mevrouw Sjouwerman).

De FG ziet erop toe dat de AVG intern wordt nageleefd. Het college (als ook Werkorganisatie de BUCH) 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 uitvoerende taken liggen bij de privacy-officer, die samenwerkt voor de informatiebeveiliging met de Chief Information Security Officer (CISO).

De FG brengt jaarlijks een verslag uit aan de verwerkingsverantwoordelijke (het college van B&W) van zijn werkzaamheden, bevindingen en aanbevelingen. Voorliggend jaarrapport is bedoeld voor het college van B&W. Hiermee kan het college ook horizontaal verantwoording afleggen aan de gemeenteraad, als controlerend orgaan.

Leeswijzer

Deze jaarrapportage bestaat uit twee onderdelen. In het eerste deel wordt teruggekeken naar het jaar 2019 (mei 2019 – mei 2020). 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 naar een hoger niveau te tillen.

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 zijn thema's, criteria en maatregelen omschreven die de AVG vertalen naar een kwaliteitscyclus voor gegevensbescherming en privacy voor gemeentelijke processen. Op pagina 2 is per thema aangegeven in hoeverre de gemeente de criteria reeds heeft geïmplementeerd en is tevens aangegeven in hoeverre de gemeente zelf verwacht eind 2020 te hebben geïmplementeerd.

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

Deel 1. Terugblik op 2019

Het jaar 2019 stond 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 Werkorganisatie de BUCH in 2019 (tot mei 2020) heeft bereikt en welke werkzaamheden zijn verricht.

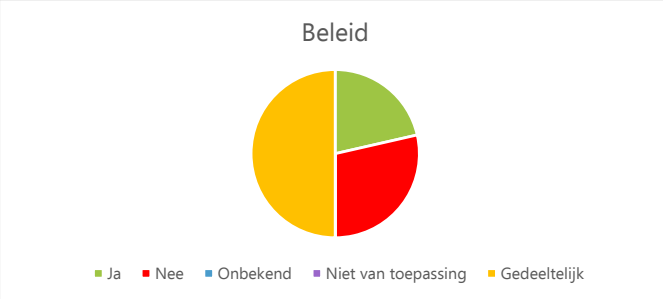
1. Beleid

Het privacybeleid is een kader waarin het college aangeeft aan welke principes zij zich houdt bij de verwerking van persoonsgegevens. Het laat zien hoe het college wil omgaan met persoonsgegevens en welke maatregelen zij treft om te voldoen aan de relevante wet- en regelgeving.

Bevindingen
Het in 2018 opgestelde privacybeleid was met de mogelijkheden van toen opgesteld en was nog onvoldoende. Inmiddels is deze herzien en is nu basaal conform wet- en regelgeving. De capaciteit voor het verder uitwerken, implementeren en communiceren van dit beleid staat onder druk wegens onvoldoende bezetting. Hiervoor is in de begroting een aanvraag voor 2021 gedaan. Om te kunnen (blijven) voldoen aan wet- en regelgeving is deze capaciteit noodzakelijk. De aanbevelingen hoe de organisatie vollediger kan voldoen aan de AVG worden in het tweede deel beschreven.

Overzicht 3 Score op de vragen ‘Thema Beleid’

Beleid	
Resultaat	**Aantal**
Ja	3
Nee	4
Onbekend	0
Niet van toepassing	0
Gedeeltelijk	7



2. Processen

De verwerking van persoonsgegevens dient te voldoen aan de wet, de AVG en UAVG . Dit houdt in dat de werkprocessen die persoonsgegevens bevatten getoetst en ingericht moeten worden volgens de volgende beginselen: behoorlijkheid, transparantie, doelbinding, noodzakelijkheid, dataminimalisatie, opslagbeperking, juistheid, integriteit en vertrouwelijkheid. Daarnaast kan de Werkorganisatie in bepaalde gevallen verplicht zijn om een Data Protection Impact Assessment (DPIA[3]) uit te voeren.

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

Bevindingen
Het maken van procesbeschrijvingen waarbij persoonsgegevens worden verwerkt is geen standaard uitvoering. Er zijn gedeeltelijk procesbeschrijvingen aanwezig. Deze zijn nog niet in overeenkomst met de beginselen van de wet. De focus van de processen ligt nu primair op efficiëntie en doelmatigheid. Nog niet op de rechtmatigheid van de uitvoeringsprocessen ten aanzien van de AVG, wat wel zou moeten.
Van het merendeel van de processen kan niet worden aangetoond dat deze voldoen aan de AVG. Wat niet direct wil zeggen dat er niet rechtmatig wordt gewerkt. Er heeft vooraf geen toets aan de beginselen plaatsgevonden.

Overzicht 4 Score op de vragen 'Thema Processen'

Processen	
Resultaat	**Aantal**
Ja	1
Nee	21
Onbekend	0
Niet van toepassing	3
Gedeeltelijk	9

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 bewustzijn creëren.

Bevindingen
De beschrijving van deze organisatorische inbedding is nog niet opgesteld. De organisatorische en financiële gevolgen voor deze inbedding heeft een relatie met de organisatiewijzigingen en moet in het geheel bij Bedrijfsvoering passen. Doordat de taken en verantwoordelijkheden van medewerkers betrokken bij de AVG-uitvoeringsprocessen onvoldoende bekend zijn wordt daar meer tijd aan besteed dan nodig zou zijn .

De wetgeving gaat niet meer weg en zal een volwaardige aanspraak op het budget moeten kunnen krijgen. Kennis en kunde van de uitvoeringsaspecten van deze wet is van essentieel belang. Het voorkomt datalekken die erg veel tijd en overbodige kosten met zich meebrengen. Van belang is dat iedereen op een basis- en soms op specialistisch kennisniveau wordt gebracht, zich bewust is van de risico's en zich vervolgens houdt aan de afspraken .

Er is veel tijd besteed aan 1-op1 trainingen door de privacy-officer waarmee bewustwording en kennis is gestart op generiek niveau. Op basaal niveau zouden medewerkers op de hoogte moeten zijn. Bewijs hiervoor is er niet . Herhaling en diepgang is noodzakelijk om de uitvoering niet in de waan van de dag te laten handelen zoals ze altijd al deden. AVG wordt vaak als 'moetje' ervaren en kost in de ogen van de uitvoering 'extra' tijd.

Overzicht 5 Score op de vragen 'Thema Organisatorische inbedding'

Organisatorische inbedding	
Resultaat	**Aantal**
Ja	14
Nee	8
Onbekend	3
Niet van toepassing	0
Gedeeltelijk	20

4. Rechten van betrokkenen

De organisatie 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.

Bevindingen
De informatieplicht aan betrokkenen is nieuw terrein, en zit nog niet standaard in de communicatie en werkprocessen ingebed. De medewerkers doen het echter al wel. Er zijn in het genoemde tijdvak relatief veel en complexe inzageverzoeken van betrokkenen binnen gekomen. Als er bij het contact met betrokkenen effectief gecommuniceerd wordt is er meestal weinig aanleiding tot het opvragen van gegevens.

Het doen van een inzageverzoek[4] of opvragen van het dossier door betrokkene is vaak ingebed in een gevoel van onmacht of ontevredenheid met de dienstverlening aan de betrokkene. Als in het primaire proces de verwachtingen en mogelijkheden goed worden toegelicht kan dat leiden tot een vermindering van inzageverzoeken.

De dossiers die opgevraagd zij,n waren niet efficiënt opgebouwd. Nu zitten in de dossiers vaak notities voor oordeelsvorming en overleg, of staat er bijvoorbeeld in WMO-dossiers medische informatie. De eerste moeten er handmatig uit worden gehaald. Op de tweede, medische gegevens, rust een verwerkingsverbod. Alleen een medisch deskundige mag deze voor de gemeente verwerken en hiervan een samenvattend advies schrijven. Werkorganisatie de BUCH mag zelf geen medische informatie verwerken, maar alleen het samenvattende advies. In de huidige gearchiveerde WMO-dossiers is veelvuldig medische informatie aanwezig. Dit vormt een risico indien dossiers opgevraagd worden door andere personen/organisaties dan betrokkene zelf.

Overzicht 6 Score op de vragen ‘Thema Rechten van betrokkenen’

Rechten van betrokkenen	
Resultaat	**Aantal**
Ja	20
Nee	1
Onbekend	0
Niet van toepassing	2
Gedeeltelijk	10

In bijlage 1 is een overzicht opgenomen van het aantal verzoeken van betrokkenen voor het jaar 2019 en eerste helft 2020.

5. Samenwerking

De Werkorganisatie 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 Werkorganisatie dient dan ook afspraken te maken met deze andere partijen en deze te documenteren en beheren.

Bevindingen
Voor de samenwerking met verschillende organisaties (RIEC (Regionaal Informatie- en Expertisecentrum), Woonfraude, HVC, Hennepconvenant en bijv. Veiligheidshuis) is de privacy-officer betrokken bij het opstellen van een nieuw convenant, het beoordelen van bestaande of nieuwe overeenkomsten, waarbij de rechtmatigheid van de gegevensverstrekkingen tussen de betrokken partijen wordt geformuleerd. De betrokkenheid van de privacy-officer is op het juiste niveau en heeft een grote toegevoegde waarde.

Er is een intensieve samenwerking gestart tussen de FG’s, privacy-officers van de gemeenten en ketenpartners en hun security officers. Bij toerbeurt komen ze bijeen en delen kennis, meningen en geven voorbeelden en

[4] Een inzageverzoek in het kader van de AVG en een dossier opvragen zijn twee aparte verzoeken en hebben een ander afhandelingsproces.

stukken. Hierdoor hoeft niet overal het wiel opnieuw te worden uitgevonden en wordt een vergelijkbaar implementatieniveau met elkaar afgestemd. Deze ontwikkeling is zeer positief.

Overzicht 7 Score op de vragen 'Thema Samenwerking'

Samenwerking	
Resultaat	**Aantal**
Ja	2
Nee	7
Onbekend	0
Niet van toepassing	0
Gedeeltelijk	8

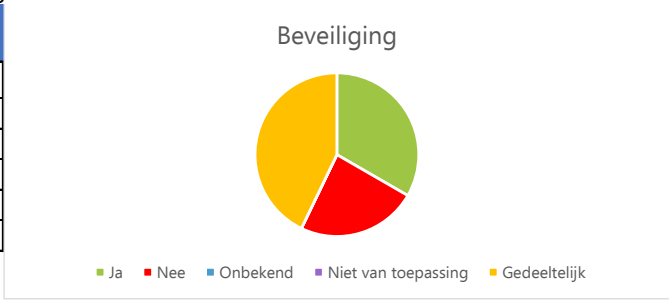
6. Beveiliging

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

Bevindingen
Het zorgdragen voor passende technische en organisatorische maatregelen is het afgelopen jaar goed gebleken. Er is een groot impactvol incident geweest (Thuiswerkomgevingen met Citrix) waardoor de organisatie een aantal dagen geen toegang had tot een bedrijfskritisch systeem. De benodigde patches waren ruim op tijd al door de organisatie uitgevoerd, waardoor de organisatie geen risico heeft gelopen. Door landelijke beeldvorming is ervoor gekozen de omgeving toch tijdelijk dicht te zetten.
De communicatie en inhoudelijke afstemming met de FG tijdens dit incident is bijzonder goed te noemen.
Het college is via het jaarverslag van de CISO al uitgebreid geïnformeerd over het informatiebeveiligingsniveau.

Overzicht 8 Score op de vragen 'Thema Beveiliging'

Beveiliging	
Resultaat	**Aantal**
Ja	7
Nee	5
Onbekend	0
Niet van toepassing	0
Gedeeltelijk	9



In bijlage 2 is een overzicht opgenomen van het aantal veiligheidsincidenten in 2019 en eerste helft 2020.

7. Verantwoording

De AVG legt de verantwoordelijkheid bij de organisatie zelf om aantoonbaar te maken dat deze voldoet aan de privacyregels. Door te voldoen aan de verantwoordingsplicht, levert de organisatie een belangrijke bijdrage aan de bescherming van het grondrecht van mensen op privacy. Dit betekent dat het college 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. Dit jaaroverzicht maakt onderdeel uit van de verantwoordingsplicht.

Bevindingen
Het opgestelde register van verwerkingen, het datalekregister en het risicolog voldoen nog niet aan de kwaliteitseisen. Ze zijn wel opgesteld echter niet meer bijgehouden. Er is geen zichtbare verbetercirkel n.a.v. incidenten. De Werkorganisatie is op dit onderdeel matig voldoende compliant aan de AVG.

Overzicht 8 Score op de vragen 'Verantwoording'

Verantwoording	
Resultaat	**Aantal**
Ja	9
Nee	8
Onbekend	0
Niet van toepassing	0
Gedeeltelijk	4

8. Conclusie

Er is een goede start gemaakt met het compliant zijn aan de AVG-wetgeving. Er is veel en goed werk verzet. Na de opzet is er door personele bezettingsproblemen geen voortgang meer gemaakt. Op bepaalde onderdelen is ook nog veel werk te doen aan kennis en bewustwording, houding en gedrag, organisatorische inbedding van de benodigde functionarissen t.a.v. uitvoering van privacywetgeving, procesbeschrijvingen die voldoen aan wetgeving, betere systemen en systeeminrichting, leveranciersmanagement en daaraan gerelateerde verplichting Privacy-by-design inrichting.

Op hoofdlijnen kan de gemeente voldoen aan haar verantwoordingsplicht. De uitvoering van AVG-gerelateerde taken staat onder druk in verband de beperkte bezetting. Voor 2021 staat formatie-uitbreiding gepland voor de priavcy-officer en de FG.

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 kwalitatiever in te bedden in de organisatie.

Deel 2. Aanbevelingen

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 tijdvak 2019-2020 in het teken stond van voorbereiden op en implementatie van de AVG en het nemen van de eerste hobbels om uiteindelijk aantoonbaar te kunnen voldoen aan deze wet, zal 2020-2021 in het teken staan van onderstaande onderwerpen en uitvoering van nog te kiezen aanbevelingen.

1. Beleid

Het privacy-beleid moet bestuurlijk worden vastgesteld door het college van B&W. Voor het managementteam ligt hier de taak dit beleid actief en aantoonbaar uit te dragen en ervoor te zorgen dat medewerkers in staat worden gesteld dit beleid te kunnen uitvoeren. Het beleid dient nog te worden aangevuld met beleid omtrent de interne verwerking van gegevens van medewerkers.

Zorg voor voldoende formatieve bezetting, incidenteel en structureel budget. Creëer een veilig klimaat waarin medewerkers beveiligingsincidenten durven doen en zorg voor continue bewustwording en kennis. Leer vooral van incidenten en ook van incidenten gemaakt door anderen. Jaarlijks zal het privacy-beleid opnieuw geëvalueerd en eventueel geactualiseerd moeten worden.

2. Processen

Het advies is alle werkprocessen inzichtelijk te maken, te starten met het in kaart brengen van de hoog risicoprocessen. Controleer of alle risico's m.b.t. verwerking van persoonsgegevens gemitigeerd zijn door middel van een Data Protection Impact assessment (DPIA=risicoanalyse). Deze hebben prioriteit. Deze DPIA's vervolgens voor iedereen toegankelijk maken. Het nog te kiezen processchema toont in een helder stappenplan de route van een proces met de daarbij behorende gegevens, type uitwisselingen en uitwisselingspartijen (zowel intern als extern).

Indien sprake is van mogelijk risicovolle nieuwe processen is het verplicht dat de organisatie voorafgaand aan de gegevensverwerking een DPIA uitvoert. Het is de taak van de organisatie dat inzichtelijk is gemaakt wanneer een DPIA uitgevoerd moet worden en op welke wijze. De FG ondersteunt hen hierbij.

Van belang is dat in de processen aandacht wordt besteed aan wat gegevensbescherming en de privacywetgeving concreet betekenen voor de betreffende afdeling, hoe de noodzakelijkheid van de verwerking van specifieke gegevens kan worden aangetoond en hoe medewerkers om dienen te gaan met persoonsgegevens binnen de taken en werkzaamheden.

Het advies is te controleren of medewerkers zich houden aan deze procesbeschrijvingen en of daarbij ondersteuning geboden kan worden als dit niet het geval is.
Ten aanzien van privacy-by-design: Zorg ervoor dat voordat een verwerking van persoonsgegevens begint bij de inkoop of bij de start van een proces, er een toets heeft plaats gevonden op grond van de AVG .

3. Organisatorische inbedding

De uitvoering van privacy wordt gedaan door een team van experts. De privacy-officer, de CISO en FG. Binnen elke afdeling is een privacy- en informatiebeveiligingsambassadeur aangewezen. Deze dient als aanspreekpunt voor de gehele afdeling en heeft nauw contact met het privacy team. Het vaststellen van hun taken, verantwoordelijkheden en bevoegdheden, in de vorm van een privacy management organisatieplan, is nog niet beschreven. Hiervan ligt weinig vast of is raadpleegbaar.
Advies is hiervoor een sessie met het management te organiseren. De ophanging van de eenheid is bij voorkeur op een neutrale plaats in de organisatie welke een bedrijfsbrede reikwijdte heeft.

De AVG verplicht organisaties ook tijd en middelen ter beschikking te stellen voor kennis- en bewustwordingssessies. Advies is persoonlijke en e-learning trainingen in een permanente cyclus te organiseren voor algemene kennis, leereffecten uit jurisprudentie en voor specifieke doelgroepen (Samenleving, HR, leidinggevenden en BOA's). In ieder geval is van belang te regelen dat alle medewerkers (in- en extern) die te maken hebben met bijzondere informatie naast het afleggen van de eed of belofte tevens een geheimhoudingsverklaring hebben ondertekend.

4. Rechten van betrokkenen

Er zijn geen volledige procesbeschrijvingen van de rechten van betrokkenen. De uitvoering van rechten van betrokkenen kan verbeteren als bij de start van het proces van gegevensdeling duidelijker wordt gecommuniceerd welke rechten de betrokkene heeft. Dit kan in de procesbeschrijving worden meegenomen en aan het begin van een gesprek, formulier of website worden gepubliceerd.

Daar waar gegevens worden verwerkt op basis van toestemming van de betrokkene is dat onvoldoende bekend in de organisatie. Ook de daarbij behorende rechten zijn nog niet voldoende bekend. Deze kunnen in de opleiding en kennissessies verder worden opgepakt.

Rechten medewerkers: ook medewerkers hebben het recht te weten hoe en welke persoonsgegevens verwerkt worden. Voor deze doelgroepen kan een aparte privacyverklaring en -beleid worden opgesteld.

5. Samenwerking

Bij de inschakeling van derden (ketenpartner, leverancier, collega organisatie etc.) is van belang te weten hoe deze zich verhouden tot de Werkorganisatie. Dit in verband met de verschillende verantwoordelijkheden en aansprakelijkheden. De AVG kent rollen als ‘Verantwoordelijke’ en ‘Verwerker’ met eigen verplichtingen. Indien een nieuwe leverancier wordt ingeschakeld, of een nieuwe taak bij een bestaande leverancier, is van belang dat bekend is of, hoe en welke er gegevens uitgewisseld worden. Deze moeten, voorafgaand aan de dienstverlening, in overeenkomsten waaruit de rechtmatigheid blijkt, worden vastgelegd. Hierbij heeft de (juridische) inkoopfunctie een belangrijke rol, maar tevens iedereen die contact heeft met ketenpartners. De lijst met verwerkersovereenkomsten moet nog verder worden aangevuld.

Bij samenwerking met ketenpartners (bijv. RIEC of hennep, of Sociale dienst) is van belang dat daar, ook weer voorafgaand aan de samenwerking, een convenant voor is opgesteld waarin o.a. de rechtmatigheid van de verwerking juridisch getoetst is.
Ook bij ad hoc bevragingen zorgt de Werkorganisatie dan voor duidelijkheid over de rol van de derde partij. De organisatie maakt dienovereenkomstig afspraken met deze derde partij.

De samenwerkingsovereenkomsten tussen de Werkorganisatie en haar opdrachtgevers is nog niet formeel op het onderdeel gegevensuitwisseling specifiek gemaakt. Dit betreft vooral de afspraken indien een partij zich terugtrekt uit het de samenwerking. Advies is deze overeenkomsten op te stellen dan wel aan te vullen.

6. Beveiliging

Beveiliging maakt onderdeel uit van de verplichtingen in de wet (art AVG 32). De organisatie is verplicht zodanige organisatorische en technische maatregelen te treffen dat de beschikbaarheid, vertrouwelijkheid en integriteit van gegevens en systemen adequaat beschermd zijn.

De belangrijkste zaken die voor de Werkorganisatie relevant zijn, zijn opgenomen in het Informatie beveiligingsplan (IB) wat weer is afgeleid van de BIO (baseline informatiebeveiliging overheid). 2019 was het overgangsjaar en in 2020 wordt verwacht dat de BIO geïmplementeerd is.

De zaken die een relatie hebben met privacywetgeving en zeer urgent zijn, zijn het invoeren van het in- en uitdienst proces, rol-gebaseerde toegang (niet meer kunnen zien dan voor je functie relevant is), en het incident- en changemanagementproces. De Werkorganisatie is op dit moment niet aantoonbaar in control .

Het loggen van handelingen van medewerkers en de controle hiervan is een belangrijke eis die de toezichthouder stelt. Deze worden nu nog niet adequaat uitgevoerd. De verwachting is dat het IB-plan de belangrijkste hiaten zal gaan oplossen.

7. Verantwoording

Voor elke verwerkingsactiviteit waarbij gegevens verwerkt worden op basis van toestemming, kan beter worden vastgelegd op welke manier de organisatie toestemming ontvangt, vastlegt en bewaart.

De organisatie kan transparanter zijn over de omgang met persoonsgegevens door het publiceren van het privacybeleid en bijvoorbeeld het verstrekken van informatiefolders bij aanvragen van producten en diensten. De Werkorganisatie kan, bijvoorbeeld op de website, de inwoners informeren over de ontwikkelingen van de bescherming van privacy en de omgang met persoonsgegevens binnen de organisatie. Door het uitvoeren van periodieke controles om de juiste werking van de getroffen beveiligingsmaatregelen te controleren kan beter worden voldaan aan de verantwoordingsverplichtingen. Ook kan er iets over worden opgenomen in het jaarverslag.

Bijlage 1 – Overzicht rechten van betrokkenen

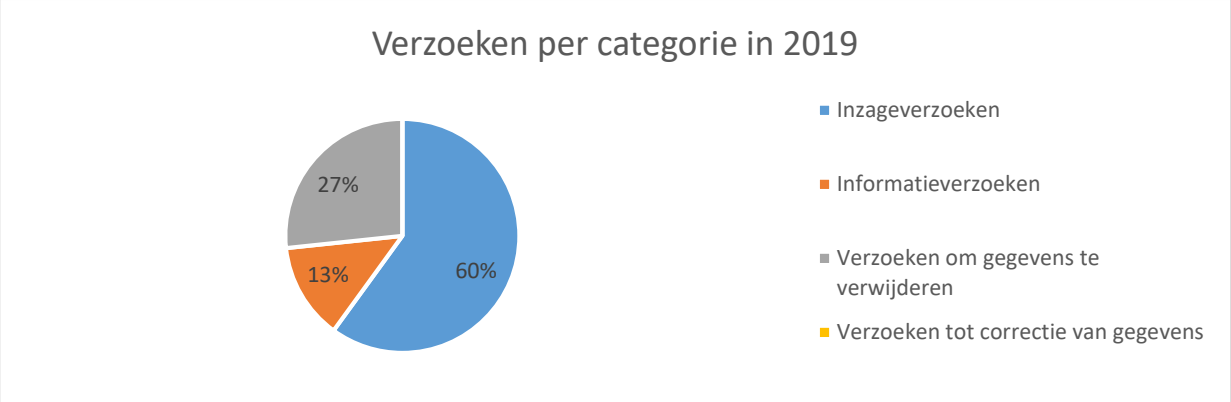
Frequentie van de rechten van betrokkenen

Rapportage van de verzoeken in 2019

Aantal verzoeken en verzoeken per categorie

In de Werkorganisatie BUCH zijn in 2019 in totaal 15 verzoeken ingediend.

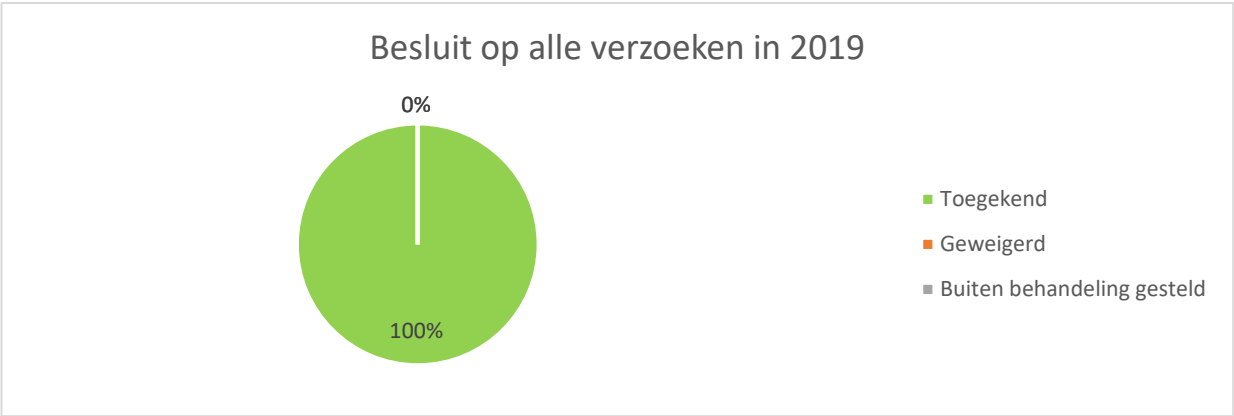
Verzoek categorie	Aantallen
Inzageverzoeken	9
Informatieverzoeken	2
Verzoeken om gegevens te verwijderen	4
Verzoeken tot correctie van gegevens	0
Totaal	**15**



Besluit op de verzoeken

In 2019 zijn alle verzoeken toegekend.

Besluit op alle verzoeken	Aantallen
Toegekend	15
Geweigerd	0
Buiten behandeling gesteld	0
Totaal	**15**

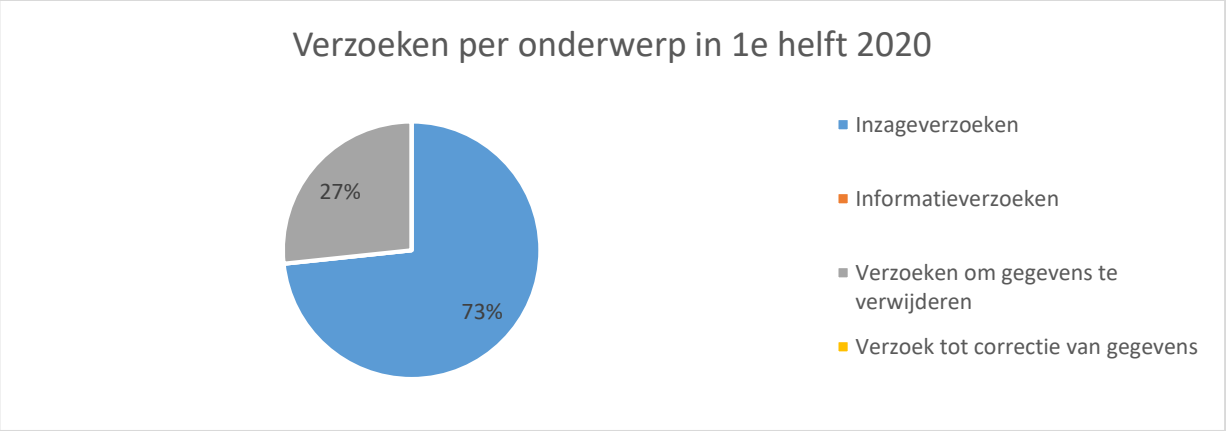


Rapportage van de verzoeken in de 1e helft van 2020

Aantal verzoeken en verzoeken per categorie

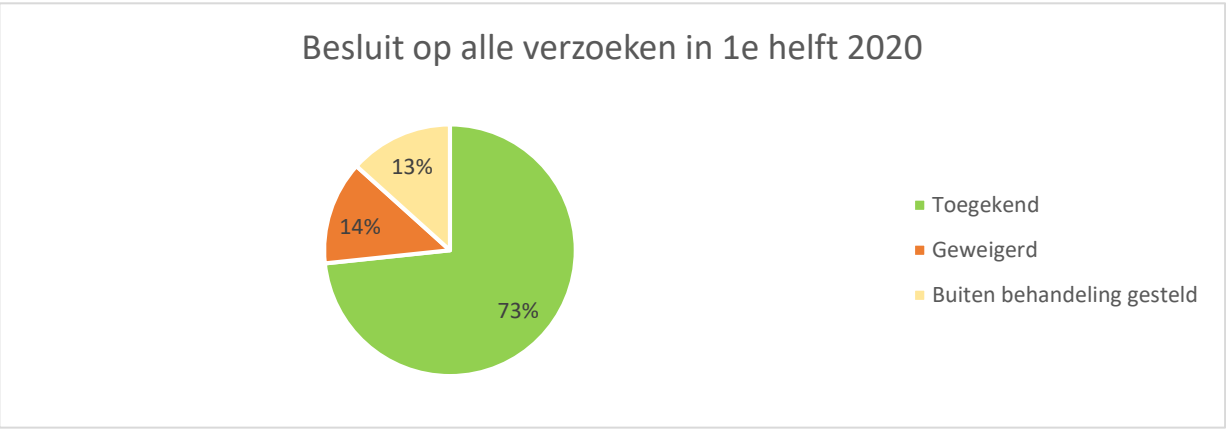
In de Werkorganisatie BUCH zijn van 1 januari 2020 tot en met 30 juni 2020 in totaal 15 verzoeken ingediend.

Verzoek categorie	Aantallen
Inzageverzoeken	11
Informatieverzoeken	0
Verzoeken om gegevens te verwijderen	4
Verzoeken tot correctie van gegevens	0
Totaal	**15**



Besluit op de verzoeken

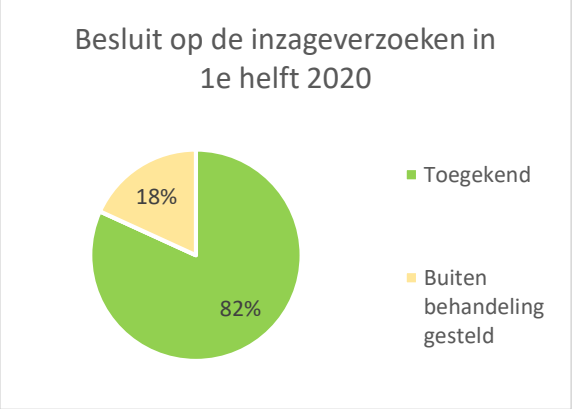
Besluit op alle verzoeken	Aantallen
Toegekend	11
Geweigerd	2
Buiten behandeling gesteld	2
Totaal	**15**



Besluit op de verzoeken per categorie

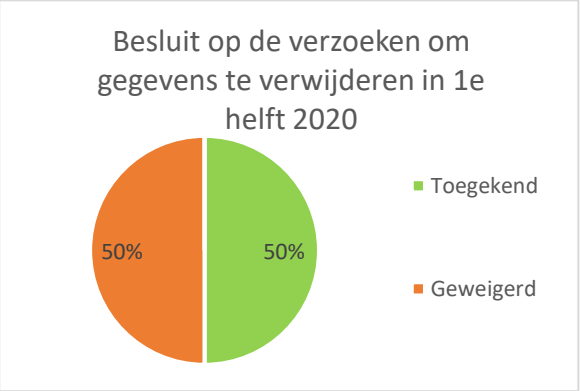
Van alle **inzage**verzoeken in de eerste helft van 2020 zijn 9 verzoeken toegekend en 2 verzoeken buiten behandeling gesteld.

Besluit op de inzageverzoeken	**Aantallen**
Toegekend Geweigerd Buiten behandeling gesteld	9 0 2
Totaal	**11**



Van alle verzoeken om **gegevens te verwijderen** in de eerste helft van 2020 zijn 2 verzoeken toegekend en 2 verzoeken geweigerd.

Besluit op de verzoeken om gegevens te verwijderen	**Aantallen**
Toegekend Geweigerd Buiten behandeling gesteld	2 2 0
Totaal	**4**



Bijlage 2 – Overzicht veiligheidsincidenten

Dit is een overzicht van de (belangrijkste) datalekken in 2019 en eerste helft 2020. Hierin is ook opgenomen of deze wel/niet zijn gemeld aan de AP en de burger.

Een veiligheidsincident (datalek) is een inbreuk in verband met persoonsgegevens. Datalekken worden ingedeeld volgens 3 informatiebeveiligingsprincipes:

1. Inbreuk op vertrouwelijkheid: als er sprake is van ongeoorloofde of onbedoelde verstrekking van of toegang tot persoonsgegevens;
2. Inbreuk op integriteit: als er sprake is van ongeoorloofde of onopzettelijke wijziging van persoonsgegevens
3. Inbreuk op beschikbaarheid; als er sprake is van ongeoorloofd of opzettelijk verlies van toegang tot persoonsgegevens of ongeoorloofde of onopzettelijke vernietiging van persoonsgegevens.

Een datalek wordt gemeld aan de Autoriteit Persoonsgegevens als de inbreuk een risico op de rechten en vrijheden van de betrokkenen oplevert.
Een datalek wordt gemeld aan de betrokkenen als de inbreuk op de rechten en vrijheden een hoog risico oplevert.

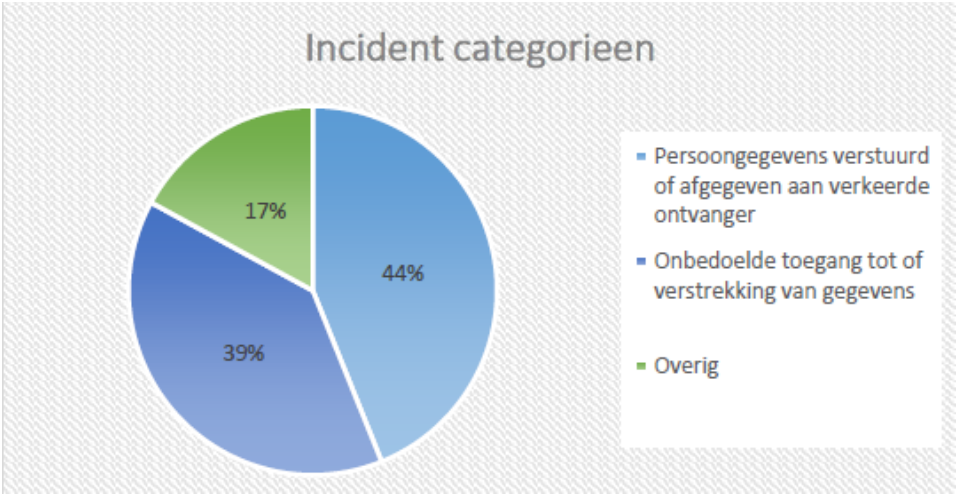
Het veiligheidsincidentenoverzicht geeft inzicht in hetvolgende:

- Welke categorie incidenten er zijn geweest;
- Het aantal gemelde incidenten aan de Autoriteit Persoonsgegevens;
- Bij welk aantal incidenten de betrokkenen zijn geïnformeerd;
- Bij welk aantal incidenten er mitigerende maatregelen zijn getroffen;
- Bij welk aantal incidenten er preventieve maatregelen zijn getroffen.

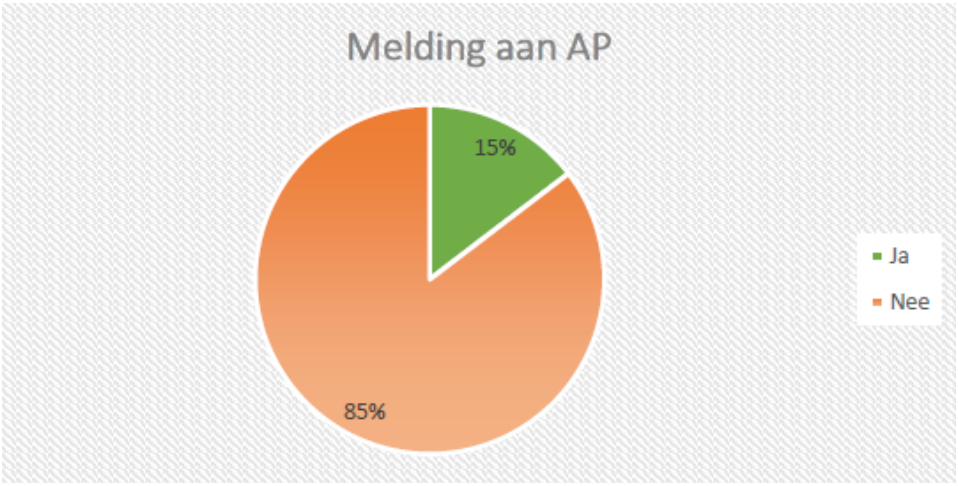
VEILIGHEIDSINCIDENTENRAPPORTAGE 2019

In de Werkorganisatie BUCH zijn in 2019 41 incidenten geregistreerd die allen een inbreuk op de vertrouwelijkheid waren.

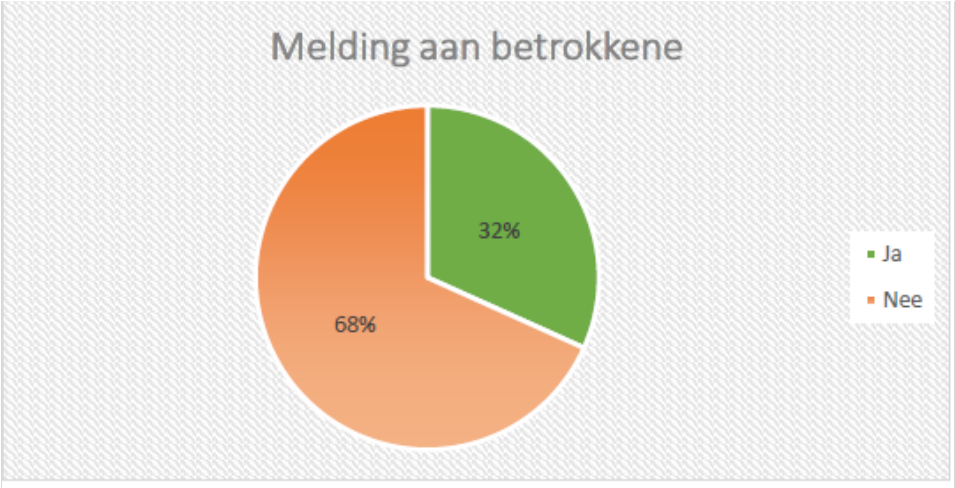
Incident categorie	Aantallen
Persoonsgegevens verstuurd of afgegeven aan verkeerde ontvanger	18
Onbedoelde toegang tot of verstrekking van gegevens	16
Overig	7
TOTAAL	41



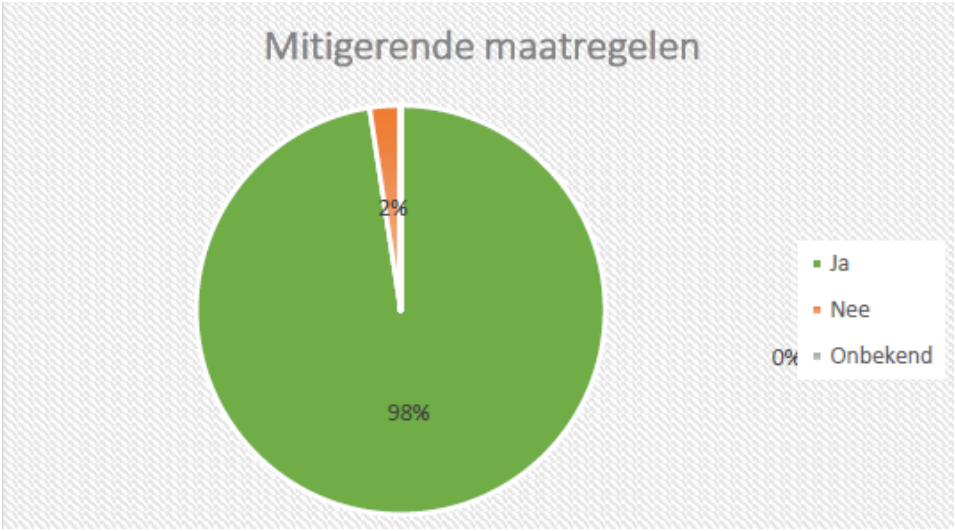
Melding aan de Autoriteit Persoonsgegevens	Aantal
Ja	6
Nee	35
TOTAAL	41



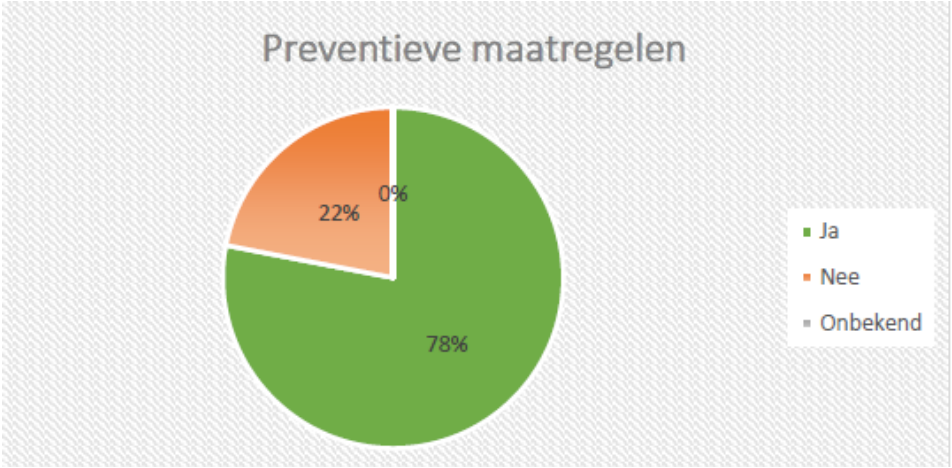
Melding aan betrokkenen	Aantallen
Ja	13
Nee	28
TOTAAL	41



Mitigerende maatregelen	Aantallen
Ja	40
Nee	1
TOTAAL	41



Preventieve maatregelen	Aantallen
Ja	32
Nee	9
TOTAAL	41

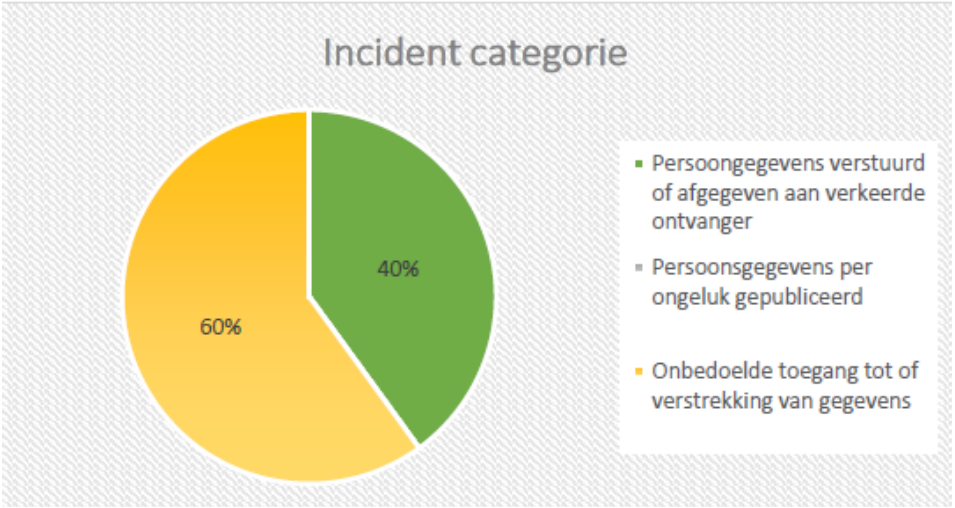


VEILIGHEIDSINCIDENTENRAPPORTAGE 1E HELFT 2020

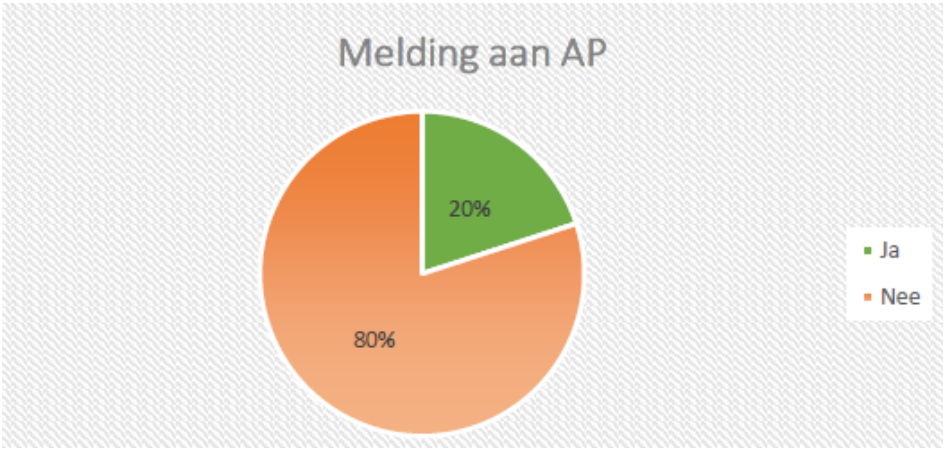
In de Werkorganisatie BUCH zijn tot en met 30 juni 2020:

- 15 incidenten gemeld die een inbreuk op de vertrouwelijkheid waren
- 1 kwetsbaarheidsmelding die een inbreuk op de vertrouwelijkheid, integriteit en beschikbaarheid kon zijn. Naar deze kwetsbaarheidsmelding is onderzoek gedaan met de constatering dat er geen inbreuk had plaatsgevonden.

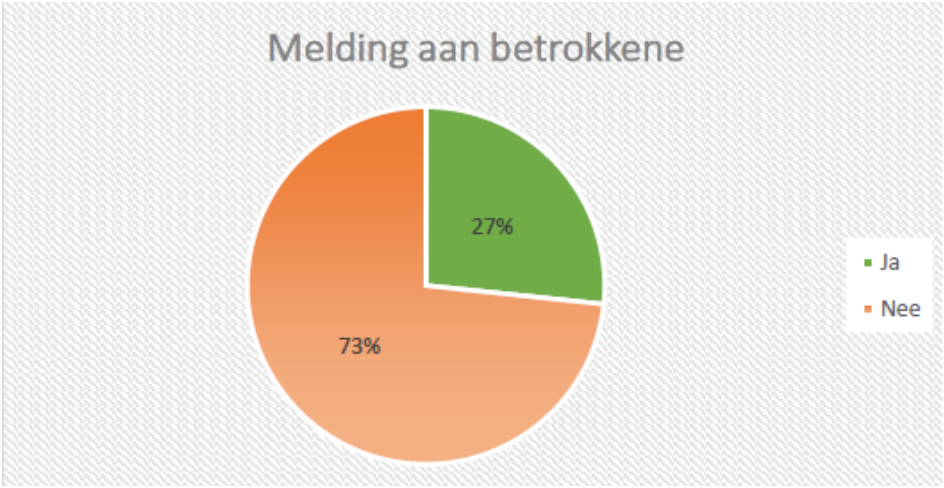
Incident categorie	Aantallen
Persoonsgegevens verstuurd of afgegeven aan verkeerde ontvanger	6
Persoonsgegevens per ongeluk gepubliceerd	0
Onbedoelde toegang tot of verstrekking van gegevens	9
TOTAAL	15



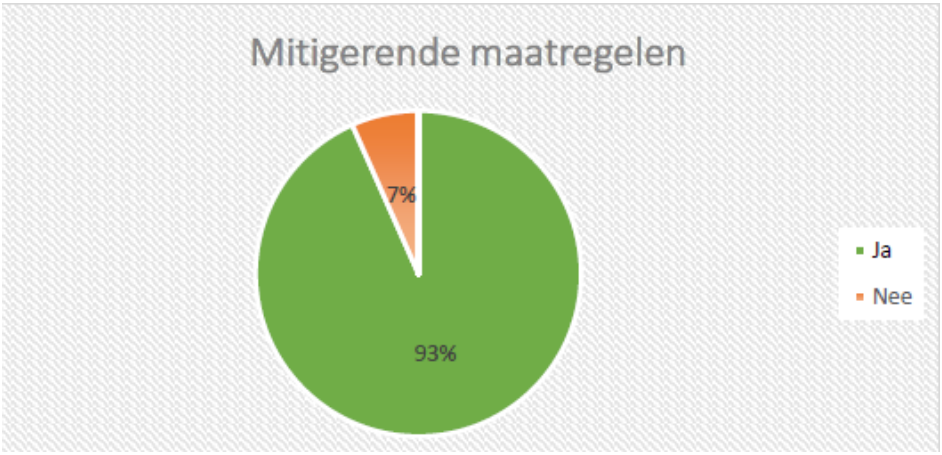
Melding aan AP	Aantallen
Ja	3
Nee	12
TOTAAL	15



Melding aan Betrokkene	Aantallen
Ja	4
Nee	11
TOTAAL	15



Mitigerende maatregelen	Aantallen
Ja	14
Nee	1
TOTAAL	15



Preventieve maatregelen	Aantallen
Ja	11
Nee	4
TOTAAL	15