

Raadsbrief jaarverslag FG 2020

aan:	de raad van de gemeente Hillegom
datum:	8 juni 2021
zaaknummer:	Z-21-169099
datum collegevergadering:	15 juni 2021
portefeuillehouder:	Dhr. A. van Erk
behandelend ambtenaar:	G.Preenen/A.M. Blufpand
embargo:	<input type="checkbox"/>

Inhoud mededeling

Waarom deze mededeling

De Functionaris gegevensbescherming (FG) houdt toezicht op de toepassing en naleving van de Algemene verordening gegevensbescherming (AVG) binnen de gemeente en rapporteert jaarlijks over de voortgang op het gebied van privacy en gerelateerde informatiebeveiligingsacties. Middels deze raadsbrief informeren wij u over de Jaarrapportage 2020 van de FG en de managementreactie op deze jaarrapportage

De FG heeft in haar jaarrapportage gebruik gemaakt van het document 'Het borgen van de Algemene Verordening Gegevensbescherming in de gemeentelijke organisatie' van de Informatiebeveiligingsdienst. Hierin zijn criteria ontwikkeld om de AVG te vertalen naar een kwaliteitscyclus voor gegevensbescherming en privacy voor gemeentelijke processen. Het biedt concrete handvatten om een goede omgang met persoonsgegevens binnen de gemeente te waarborgen.

Jaarrapportage Functionaris Gegevensbescherming 2020

In haar jaarverslag meldt de FG dat de gemeente in 2020 een kleine vooruitgang heeft geboekt om de AVG te implementeren in de organisatie, de systemen en de processen. Dit beeld is overigens zichtbaar bij veel gemeenten in Nederland. Er is een procesbeschrijving en een format voor het uitvoeren van een gegevensbeschermingseffectbeoordeling (DPIA) gemaakt, maar nog niet formeel vastgesteld. De opgestelde privacy checklist om de gegevensbeschermingsrisico's vooraf in beeld te brengen werkt goed, maar wordt echter niet in alle gevallen toegepast. Verder is het voor burgers mogelijk om ook digitaal hun privacy rechten uit te oefenen en is het proces om dit te faciliteren op hoofdlijnen beschreven. Per 1 maart 2020 is er een Privacy Officer (PO) aangesteld. Medewerkers weten de PO en FG steeds beter te vinden. Om de onafhankelijke positie van de FG te borgen is door de directie van HLTsamen tenslotte op 18 juni 2020 een gedragslijn opgesteld die na een half jaar geëvalueerd gaat worden.

Managementreactie

Het management heeft naar aanleiding van de jaarrapportage van de FG teruggeblikt op 2020 en vooruitgekeken naar 2021. Het jaar 2020 was een bijzonder jaar. Een groot deel van de medewerkers moest vanwege de Coronacrisis thuis gaan werken. Het management is er trots op dat deze overgang snel maar ook veilig vorm heeft gekregen. Daarnaast is het zaakstelsel aangepast aan de eisen van de AVG is een richtlijn opgesteld om de onafhankelijkheid van de FG te waarborgen en zijn er bewustwordingssessies gehouden met het bestuur HLTsamen en de colleges. In 2021 wordt verder gegaan op de in 2020 ingeslagen weg. Voor 2022 zijn in de begroting van HLTsamen structureel extra middelen gevraagd om de onvermijdelijke ontwikkelingen op het gebied van informatieveiligheid en privacy mogelijk te maken

Bijlagen:

1. Jaarrapportage Functionaris Gegevensbescherming 2020
2. Managementreactie

**JAARRAPPORTAGE GEGEVENSBECHERMING
Gemeente Hillegom**

Het college van de gemeente Hillegom

Functionaris Gegevensbescherming
18 februari 2020

Samenvatting

In de jaarrapportage over 2019 heeft mijn voorganger aangegeven welke acties en maatregelen de gemeente Hillegom heeft genomen om de doelstellingen en beginselen uit de AVG te behalen en te waarborgen. Ook bevatte de jaarrapportage aandachtspunten en actiepunten voor het jaar 2020. In deze jaarrapportage kijk ik terug wat er met de aanbevelingen uit het vorige jaarverslag is gedaan en doe ik aanbevelingen voor 2021.

De uitdaging voor 2020 was om een begin te maken met het structureel inbedden van de AVG in de organisatie zodat hierop ook gestuurd kan worden. Hiervoor is het belangrijk dat het management haar rol op het gebied van gegevensbescherming pakt, maar ook dat er voldoende capaciteit en tijd beschikbaar gesteld wordt voor gegevensbescherming. Tenslotte is blijvende aandacht voor gegevensbescherming van zowel het bestuur, management als de medewerkers van belang.

In 2020 is een planning gemaakt waarin de aanbevelingen uit eerdere jaarrapportages gekoppeld zijn aan concrete acties. Het schema heb ik als bijlage toegevoegd ([bijlage 1](#)). Bij het opstellen van het overzicht was nog geen rekening gehouden met de gevolgen van de COVID-19 pandemie.

Ik heb gebruik gemaakt van het document 'Het borgen van de Algemene Verordening Gegevensbescherming in de gemeentelijke organisatie' van de Informatiebeveiligingsdienst. Het biedt concrete handvatten om een goede omgang met persoonsgegevens binnen de gemeente Hillegom te waarborgen. Hiermee kan het college de voortgang van de implementatie van de AVG monitoren en waar nodig bijsturen.

In 2020 heeft de gemeente Hillegom slechts een kleine vooruitgang geboekt om de AVG verder te implementeren in de organisatie, de systemen en de processen. Een procesbeschrijving en een format voor het uitvoeren van een gegevensbeschermingseffectbeoordeling (DPIA¹) is gemaakt, maar nog niet formeel vastgesteld. De opgestelde privacy checklist om de gegevensbeschermingsrisico's vooraf in beeld te brengen werkt goed, maar wordt echter niet in alle gevallen toegepast. Verder is het voor burgers mogelijk om ook digitaal hun privacy rechten uit te oefenen en is het proces om dit te faciliteren op hoofdlijnen beschreven. Per 1 maart 2020 is er een Privacy Officer (PO) aangesteld. Medewerkers weten de PO en Functionaris Gegevensbescherming (FG) steeds beter te vinden. Om de onafhankelijke positie van de FG te borgen is door de directie van HLTsamen tenslotte op 18 juni 2020 een gedragslijn opgesteld die na een half jaar geëvalueerd gaat worden.

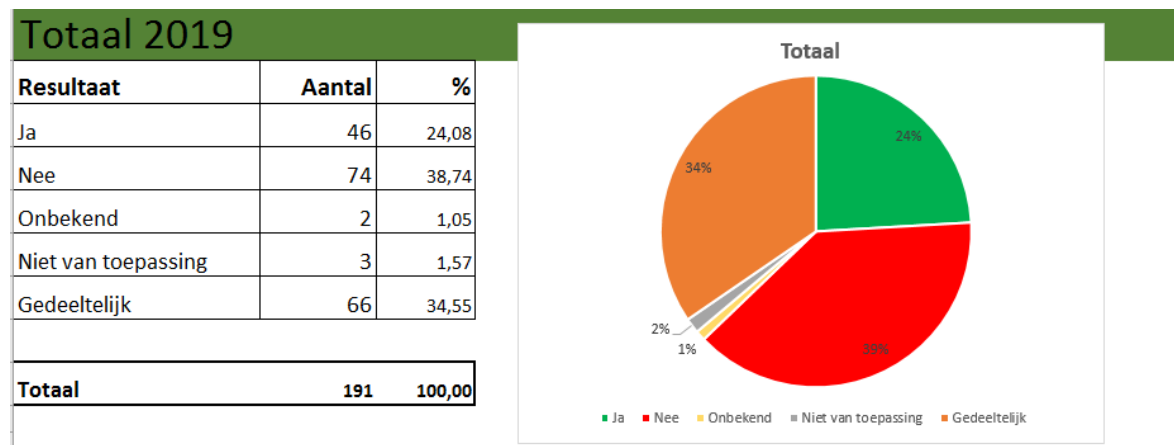
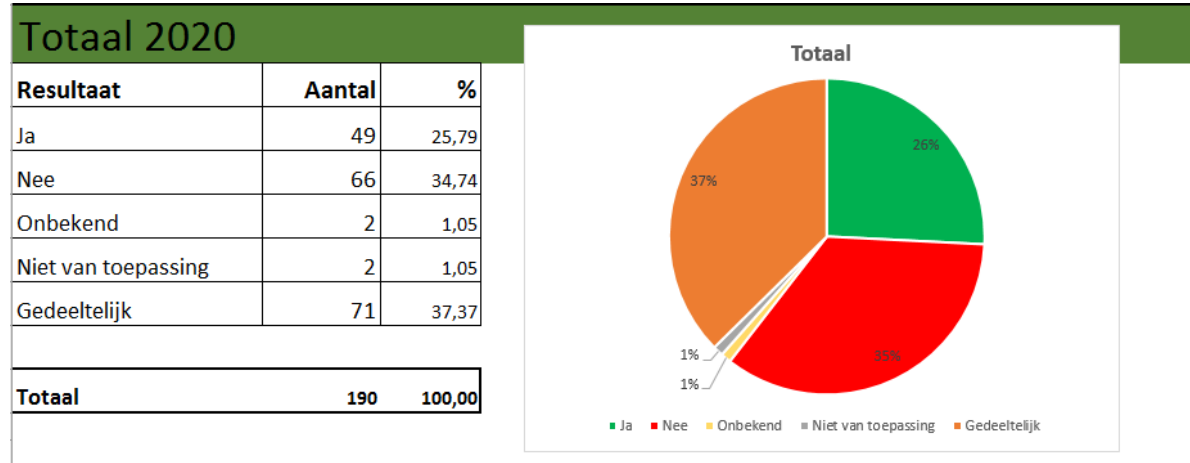
In onderstaande tabellen is in algemene termen aangegeven het aantal onderdelen waar de gemeente Hillegom wel of niet aan voldoet. [In bijlage 2](#) is er een en ander nader uitgewerkt.

Via deze weg wil ik van de gelegenheid gebruik maken om mijn zorgen te uiten over de ambitie van de organisatie in relatie tot het volwassenheidsniveau van de organisatie op het gebied van de gegevensbescherming. Zo is er een project gestart met betrekking tot datagedreven sturen. Maar ook ondermijning wordt serieus opgepakt. Bij deze ontwikkelingen is het van belang dat de medewerkers die hiermee aan de slag gaan over voldoende kennis van gegevensbescherming beschikken en dat voldoende capaciteit beschikbaar is. In de praktijk wordt er met name bij de uitvoering van de onderdelen van het project over datagedreven sturen veel geleund de PO en de FG, terwijl ook hun capaciteit beperkt is. Daarnaast kan de toezichhoudende rol van mij als FG in het geding komen wanneer ik teveel met de uitvoering meedenk. Ik adviseer dan ook om of de kennis op

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

peil te brengen of kennis in te huren, net zoals bij het project over het anders inrichten van de integrale toegang is gedaan.

Schematisch overzicht vorderingen AVG



Inhoudsopgave

INLEIDING	5
LEESWIJZER	5
DEEL 1. TERUGBLIK.....	6
1. HET BELEID	6
2. ORGANISATORISCHE INBEDDING	7
3. SAMENWERKING.....	7
4. BEVEILIGING	7
5. VERANTWOORDING.....	8
6. CONCLUSIE	8
DEEL 2. VOORUITBLIK.....	9
1. HET BELEID	9
2. PROCESSEN.....	9
3. ORGANISATORISCHE INBEDDING	10
4. VERANTWOORDING.....	10
5. CONCLUSIE	10

Inleiding

De gemeente Hillegom dient zorgvuldig om te gaan met persoonsgegevens. De gemeente verwerkt immers bij de uitoefening van haar taken veel informatie. Niet alleen persoonlijke informatie van klanten, maar ook van medewerkers, externen en zakenrelaties. In de AVG wordt het wettelijk kader beschreven voor het verwerken van persoonsgegevens. Zo dient de gemeente transparant te zijn welke persoonsgegevens zij verwerkt en voor welk doel. Persoonsgegevens mogen alleen worden verwerkt wanneer dit in overeenstemming is met het doel waarvoor zij zijn verzameld en gegevens mogen niet langer bewaard worden dan strikt noodzakelijk. Bovendien moet de gemeente passende technische en organisatorische beveiligingsmaatregelen treffen om onrechtmatige toegang tot deze persoonsgegevens tegen te gaan en daardoor een onrechtmatig gebruik van deze persoonsgegevens te voorkomen. Daarnaast heeft de gemeente ook te maken met tal van privacyregels in sectorspecifieke wetgeving. Dit alles heeft gevolgen voor de inrichting van processen en systemen in en van de gemeente.

De FG ziet erop toe dat de AVG intern wordt nageleefd. De FG brengt jaarlijks een verslag uit aan de verwerkingsverantwoordelijke van haar werkzaamheden en bevindingen en doet zij naar aanleiding daarvan aanbevelingen. Dit jaarverslag is bedoeld voor het college van de gemeente Hillegom.

Leeswijzer

Deze jaarrapportage bestaat uit twee onderdelen.

In het eerste deel wordt teruggekeken naar het jaar 2020. Wat heeft de gemeente Hillegom bereikt op het gebied van gegevensbescherming? Welke maatregelen zijn er genomen om te voldoen aan de AVG? In het tweede deel worden aanbevelingen gedaan om gegevensbescherming en privacy in het jaar 2021 naar een hoger niveau te tillen.

De criteria die in beide delen worden genoemd zijn afkomstig uit het document 'Het borgen van de Algemene Verordening Gegevensbescherming in de gemeentelijke organisatie' van de Informatiebeveiligingsdienst. In dit document worden criteria en maatregelen omschreven die de AVG vertalen naar een kwaliteitscyclus voor gegevensbescherming en privacy voor gemeentelijke processen. De jaarrapportage 2018 was een nulmeting. Hierin had mijn voorganger alle subonderdelen uit het borgingsdocument opgenomen en uitgebreid beschreven. Vanaf 2019 geeft de FG per hoofdonderdeel aan wat wel/niet is opgepakt. In [bijlage 2](#) is een overzicht opgenomen waar in cirkeldiagramvorm wordt aangegeven in hoeverre de gemeente Hillegom de criteria t/m december 2020 heeft geïmplementeerd.

Deel 1. Terugblik

In dit deel van de rapportage blik ik terug op hetgeen de gemeente Hillegom in 2020 heeft bereikt en welke werkzaamheden tot op heden zijn verricht.

1. Het beleid

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

1.1 Er is een algemeen privacybeleid

Het privacybeleid is in 2019 vastgesteld, maar het management draagt dit beleid nog niet actief uit. Het privacybeleid is bekend binnen en buiten de organisatie. Maar wat de taken en verantwoordelijkheden betekenen voor de werkprocessen is nog niet geheel bekend.

In 2020 zijn bewustwordingssessies gehouden met het bestuur van HLTsamen en de colleges van B&W over het belang van het vaststellen van een volwassenheidsniveau. Bij het bespreken van het voorstel in het MT zijn ook de Domeinmanagers meegenomen. Daarnaast hebben de PO en FG veel ad hoc juridische privacyvragen binnen de organisatie kunnen beantwoorden en samen met de Chief Information Security Officer (CISIO) tweemaal een introductiesessie voor nieuwe medewerkers gehouden. Ook is een tweewekelijks privacyspreekuur ingevoerd en wordt vanaf oktober iedere week op het intranet een item over privacy geplaatst om bewustwording onder de medewerkers te creëren.

1.2 Het privacybeleid is leidend bij ontwerp en ontwikkelingen van (nieuwe) verwerkingen.

Nieuwe ontwikkelingen, verwerkingen of wijzigingen van verwerkingen worden voorafgaand getoetst aan het beleid en geldende wet- en regelgeving.

Het toetsen vindt nog niet structureel plaats, maar op ad hoc basis. Vaak wordt ook achteraf pas advies gevraagd. Hoogstwaarschijnlijk vindt in veel gevallen ook geen toetsing plaats. Bij het project over datagedreven sturen, het project ondermijning en het anders inrichten van de integrale toegang is er vooraf wel aandacht voor privacy. Zo is in het project datagedreven sturen ingebed dat er voordat daadwerkelijk persoonsgegevens worden verwerkt, er eerst een DPIA uitgevoerd wordt om de privacy en informatiebeveiligingsrisico's in kaart te brengen. Voor het project ondermijning is voor de vier fasen een DPIA uitgevoerd en voor het anders inrichten van de toegang wordt er op korte termijn op hoofdlijnen een DPIA uitgevoerd.

1.3 Het privacybeleid wordt – waar nodig – domein specifiek uitgewerkt.

Er is - waar nodig - domeinspecifiek privacybeleid waarin wordt beschreven hoe het betreffende domein omgaat met (sectorspecifieke) wet- en regelgeving, persoonsgegevens en gegevensbescherming. Voor ondermijning is een privacyprotocol opgesteld gebaseerd op het landelijke voorbeeld.

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.

2.1 De organisatie heeft een FG aangesteld en gepositioneerd

Om de onafhankelijke positie van de FG te borgen is op 18 juni 2020 door de directie van HLTsamen een gedragslijn opgesteld die na een half jaar geëvalueerd gaat worden.

2.2 Er is – naast de FG - ruime (juridische) kennis over privacy, gegevensbescherming en relevante wet- en regelgeving.

Er is - ten minste - één privacyadviseur die beschikt over ruime kennis voor wat betreft het toepassen van relevante privacywet- en regelgeving in de praktijk. Per 1 maart 2020 is een PO aangesteld voor 2 dagen per week.

2.3 Er is een procedure voor de afhandeling van verzoeken van rechten van betrokkenen.

Voor burgers is het mogelijk om ook digitaal (via DigD) hun privacy rechten uit te oefenen. Het proces om dit te faciliteren is op hoofdlijnen beschreven.

In 2020 is er 1x een verzoek om inzage in persoonsgegevens ingediend bij de gemeente Hillegom

3. Samenwerking

De gemeente werkt in diverse rollen en hoedanigheden samen met gemeenten en private organisaties. In veelvoorkomende gevallen zal er sprake zijn van een verwerking van persoonsgegevens tussen partijen: ontvangen van persoonsgegevens, verzenden van persoonsgegevens, maar ook het opslaan van en inzage hebben in persoonsgegevens valt onder dit begrip. Deze verwerkingen dienen dan ook te voldoen aan de AVG. De gemeente dient dan ook afspraken te maken met deze andere partijen. Dit is voor een beperkt deel gebeurd.

Hierbij heeft er geen verandering ten opzichte van de jaarrapportage over 2019 plaatsgevonden.

4. Beveiliging

4.1 Vanuit het algemene behoorlijkheidsbeginsel, het integriteitsbeginsel en het vertrouwelijkheidsbeginsel is het essentieel dat de gemeente 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 Autoriteit Persoonsgegevens (AP) en/of de betrokkene(n). Of een datalek gemeld moet worden aan de AP en/of betrokkene, is afhankelijk van de (potentiële) impact van het datalek op de bescherming van persoonsgegevens en de persoonlijke levenssfeer van betrokkenen.

4.2 De organisatie heeft inzicht in alle incidenten en inbreuken.

De organisatie registreert alle inbreuken en incidenten die verband houden met persoonsgegevens in een datalekregister. De PO beheert het intern datalekregister.

In bijlage 3 is een overzicht opgenomen van het aantal datalekken over 2020.

5. Verantwoording

De AVG legt de verantwoordelijkheid bij de organisatie zelf om aantoonbaar te maken dat deze voldoet aan de privacyregels. Door te voldoen aan de verantwoordingsplicht, levert de organisatie een belangrijke bijdrage aan de bescherming van het grondrecht van mensen op privacy. Dit betekent dat het college aan moet kunnen tonen dat de verwerkingen van persoonsgegevens voldoen aan de beginselen van de AVG en aan de relevante wet- en regelgeving.

5.1 De organisatie is transparant over de verwerking van persoonsgegevens.

De privacyverklaring op de website is aangepast.

5.2 Periodiek wordt een GAP-analyse uitgevoerd om inzichtelijk te maken waar de organisatie staat.

De eerste jaarrapportage van de FG over 2018 kan worden gezien als een nulmeting. Het borgingsdocument geeft precies weer welke onderdelen wel/niet zijn opgepakt. In 2020 is een planning gemaakt waarin de aanbevelingen uit eerdere jaarrapportages gekoppeld zijn aan concrete acties. Het schema heb ik als bijlage toegevoegd (bijlage 1).

6. Conclusie

In 2020 heeft de gemeente Hillegom een beperkt aantal stappen gezet om de AVG te implementeren in de organisatie, de systemen en de processen. Er is een PO benoemd. Een procesbeschrijving en een format voor het uitvoeren van een DPIA is gemaakt. De opgestelde privacy checklist om de gegevensbeschermingsrisico's vooraf in beeld te brengen werkt goed, maar wordt echter niet in alle gevallen toegepast. Verder is het voor burgers mogelijk om ook digitaal hun privacy rechten uit te oefenen en is het proces om dit te faciliteren op hoofdlijnen beschreven. Medewerkers weten de PO en de FG steeds beter te vinden. Om de onafhankelijke positie van de FG te borgen is tenslotte een gedragslijn opgesteld die na een half jaar geëvalueerd gaat worden.

Deel 2. Vooruitblik

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. 2020 stond in het teken van het verhogen van de bewustwording en de structurele borging van de AVG binnen de gemeente. Hieronder geef ik aan welke onderdelen meer aandacht behoeven in 2021.

1. Het beleid

1.1 Er is een algemeen privacybeleid

Het privacybeleid is vastgesteld, maar het management draagt dit beleid nog niet actief uit. Het privacybeleid is bekend binnen en buiten de organisatie. Maar wat de taken en verantwoordelijkheden betekenen voor de werkprocessen is nog niet geheel bekend. Er is geen communicatieplan om het beleid actief uit te dragen.

In 2020 zijn bewustwordingssessies gehouden met het bestuur van HLTsamen en de colleges van B&W over het belang van het vaststellen van een volwassenheidsniveau. Bij de behandeling van het voorstel hiertoe in het MT in december 2020 zijn ook de domeinmanagers hiervan bewust gemaakt. Voor 2021 raad ik aan om actiever te sturen op het volgen van de e-learning privacy en informatiebeveiliging². Ook raad ik aan om voor de domeinen waar veel (gevoelige) persoonsgegevens worden verwerkt, een bewustwordingssessie privacy te houden.

2. Processen

De verwerkingen van persoonsgegevens van de gemeente 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 is de gemeente in bepaalde gevallen verplicht om een gegevensbeschermingseffectbeoordeling (ook wel DPIA genoemd³) uit te voeren.

2.1 Het register van verwerkingsactiviteiten wordt nog niet beheerd.

De PO is verantwoordelijk voor het onderhoud en de actualisatie van (onderdelen van) het register. Er is inmiddels een PO aangesteld. Proceseigenaren weten nog niet aan wie zij wijzigingen van de bestaande verwerkingen of het toevoegen van nieuwe verwerkingen kunnen doorgeven.

2.2 Er is nog geen proces voor het uitvoeren en actualiseren van DPIA's.

De organisatie is nog niet bekend welke verantwoordelijken de DPIA moeten uitvoeren.

Er is steeds meer aandacht voor het uitvoeren van DPIA's. De FG en PO worden hier steeds meer bij betrokken. Er is in 2019 een lijst opgesteld van risicovolle verwerkingen en met de betreffende verantwoordelijken gedeeld. Intern zijn ook nog geen privacy contactpersonen aangesteld die DPIA's kunnen uitvoeren. Geadviseerd wordt om in 2021 per afdeling/team een overzicht van risicovolle processen te maken waarvoor een DPIA uitgevoerd dient te worden en een planning voor uitvoering. Het register van verwerkingen kan als uitgangspunt dienen.

² Medewerkers die in dienst komen van HLTsamen dienen op grond van de Baseline Informatiebeveiliging Gemeenten binnen drie maanden na indiensttreding de e-learning informatiebeveiliging en privacy te volgen.

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

2.3 Intern verantwoordelijken dragen er zorg voor dat nieuwe verwerkingen of potentieel nieuwe verwerkingen, welke mogelijk een hoog privacyrisico opleveren, voorafgaand worden getoetst middels een DPIA.

Zowel het lijnmanagement als de privacy ambassadeurs zijn bekend met het bestaan van de DPIA. Er is een DPIA format beschikbaar, maar nog niet formeel vastgesteld. Privacy ambassadeurs of contactpersonen privacy zijn nog niet aangesteld. Geadviseerd wordt om dit in 2021 op te pakken.

3. Organisatorische inbedding

3.1 Medewerkers hebben nog niet enkel toegang tot de systemen die zij nodig hebben ter uitvoering van hun werkzaamheden.

De autorisaties in het zaakstelsel worden verbeterd. Het is gewenst dit breder op te pakken en een autorisatiematrix voor alle systemen op te stellen en in te regelen.

4. Verantwoording

4.1 Periodiek worden de verantwoordelijk bestuursorganen geïnformeerd over de omgang met persoonsgegevens en de naleving van de AVG binnen de organisatie.

Naar aanleiding van het verslag van de FG stellen de verantwoordelijken vast welke acties en maatregelen de organisatie dient te nemen om aan de AVG te voldoen. Het is niet duidelijk wat de ambitie van de verantwoordelijken is. Geadviseerd wordt om in 2021 een ambitie voor de privacy vast te stellen zodat ook naar de organisatie duidelijk is welke stappen er gezet dienen te worden.

5. Conclusie

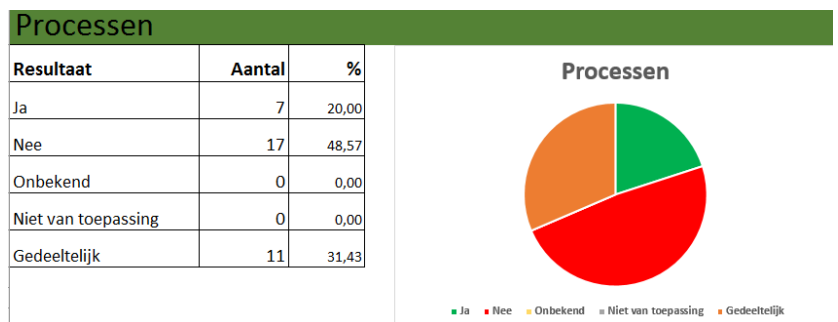
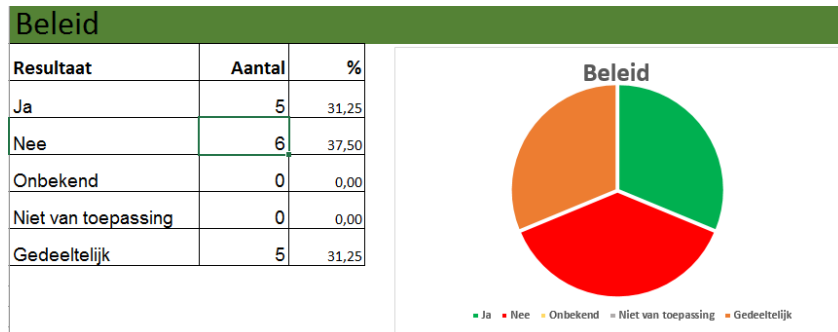
Op het gebied van privacy en gegevensbescherming is er in 2021 flinke winst te behalen. Het structureel inbedden van de AVG in de organisatie dient nu echt opgepakt te worden zodat hierop ook gestuurd kan worden. Hiervoor is het belangrijk dat het management haar rol op het gebied van gegevensbescherming pakt, maar ook dat er voldoende capaciteit en tijd beschikbaar gesteld wordt voor gegevensbescherming. Tenslotte is blijvende aandacht voor gegevensbescherming van zowel het bestuur, management als de medewerkers van belang.

Bijlage 1. Planningsoverzicht

Afkomstig uit Ambtelijk Advies (2020)

Nummer	Taak	Planning	Status
1	Beleid uitdragen	Heel 2020	Bezig
2	Aanstellen privacy contactpersoon	Oppakken 2 ^e kwartaal 2020	Nog te doen
3	Bewustwording sessies	2 ^e en 3 ^e kwartaal	Nog te doen
4	Verantwoorden via rechtmatigheidsverklaring	2 ^e kwartaal	Nog te doen
5	Werkprocessen via AVG beginselen inrichten	Oppakken 4 ^e kwartaal	Nog te doen
6	Prioriteringslijst DPIA	Oppakken 2020	Een voorstel hiervoor is in procedure gebracht
7	Uitvoeren DPIA	2020 en 2021	Deels gestart
8	Verwerkingsregister	Levend proces (2020 en 2021)	Loopt
9	Rechten betrokkenen inregelen	2 ^e kwartaal	Gereed
10	Verantwoordelijkheden lijnmanagement	3 ^e kwartaal	Loopt
11	Autorisaties in zaaksysteem		Gereed
12	Geheimhoudingsverklaringen	4 ^e kwartaal	Gereed
13	Verwerkersovereenkomst / gegevensuitwisselingsovereenkomst	Levend proces	bezig
14	Proces datalekken in JOIN	2 ^e kwartaal	Gereed
15	Datalekregister	Levend proces	Loopt
16	Toestemmingsprocedure	4 ^e kwartaal	Nog te doen
17	Register toestemming	2021	Nog te doen
18	Procesbeschrijving toestemming	2021	Nog te doen

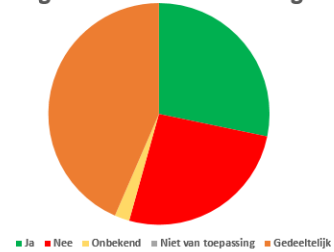
Bijlage 2. Stand van zaken AVG per onderwerp



Organisatorische inbedding

Resultaat	Aantal	%
Ja	13	28,26
Nee	12	26,09
Onbekend	1	2,17
Niet van toepassing	0	0,00
Gedeeltelijk	20	43,48

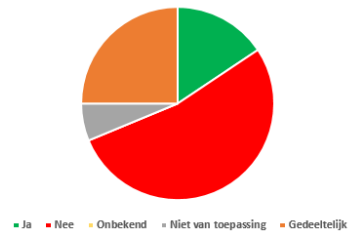
Organisatorische inbedding



Rechten van betrokkenen

Resultaat	Aantal	%
Ja	5	15,63
Nee	17	53,13
Onbekend	0	0,00
Niet van toepassing	2	6,25
Gedeeltelijk	8	25,00

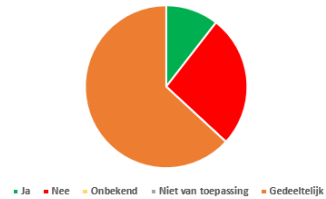
Rechten van betrokkenen



Samenwerking

Resultaat	Aantal	%
Ja	2	10,53
Nee	5	26,32
Onbekend	0	0,00
Niet van toepassing	0	0,00
Gedeeltelijk	12	63,16

Samenwerking



Beveiliging

Resultaat	Aantal	%
Ja	9	42,86
Nee	4	19,05
Onbekend	0	0,00
Niet van toepassing	0	0,00
Gedeeltelijk	8	38,10

Beveiliging



■ Ja ■ Nee ■ Onbekend ■ Niet van toepassing ■ Gedeeltelijk

Verantwoording

Resultaat	Aantal	%
Ja	8	38,10
Nee	5	23,81
Onbekend	1	4,76
Niet van toepassing	0	0,00
Gedeeltelijk	7	33,33

Verantwoording



■ Ja ■ Nee ■ Onbekend ■ Niet van toepassing ■ Gedeeltelijk

Bijlage 3: Overzicht datalekken

Oorzaak	2020 Meldingswaardig	2020 Niet meldingswaardig
Menselijke oorzaak	0	1
Technische oorzaak	0	0
Totaal	0	1
Totaal	1	

We hebben met veel belangstelling kennisgenomen van de Jaarrapportages HLTsamen, Lisse, Hillegom en Teylingen 2020 van de Functionaris Gegevensbescherming.

Terugblik 2020

Het jaar 2020 was een bijzonder jaar. Door de Coronacrisis kregen we niet alleen te maken met andere werkzaamheden maar ook met een andere manier van werken. Een groot deel van onze medewerkers heeft in 2020 thuis gewerkt. We zijn er trots op dat we deze overgang snel maar ook veilig vorm hebben kunnen geven.

Ondanks de onverwachte gebeurtenissen in 2020 hebben we een aantal belangrijke stappen kunnen zetten op het gebied van bescherming van de persoonsgegevens. We lichten er een aantal uit:

- In een omvangrijk project is ons zaakstelsel aangepast aan de eisen van de AVG. Het zaakstelsel was bij de start van HLTsamen ingericht op maximale transparantie en het zo goed mogelijk ondersteunen van integraal werken. In 2020 is extra capaciteit ingehuurd om met alle teams en domeinen de afweging te maken welke medewerkers toegang moeten hebben tot bepaalde zaaktypen en voor welke medewerkers dat niet noodzakelijk is. Op basis van de uitkomsten van de inventarisatie is de inrichting van het zaakstelsel aangepast;
- Een richtlijn is opgesteld voor borging van de onafhankelijkheid van de FG en de CISO. Op die manier dragen we er zorg voor dat deze functionarissen toegang hebben tot alle informatie die zij nodig hebben binnen de organisatie en direct toegang hebben tot directie en Burgemeesters. Deze richtlijn wordt samen met de FG en CISO in 2021 geëvalueerd;
- Er zijn bewustwordingssessies gehouden met het bestuur van HLTsamen en de colleges. Ook in het MT en in de domein MT's is aandacht besteed aan dit onderwerp;
- Er is een Privacy Officer aangesteld voor 2 dagen per week;
- Er is inzicht in alle incidenten en inbreuken;
- Er is een format voor DPIA's opgesteld.

Vooruitblik 2021

In 2021 gaan we verder op de in 2020 ingeslagen weg. Extra nadruk moet in de organisatie worden gelegd op de taakvolwassenheid op het gebied van privacy en informatiebeveiliging. Privacy en informatiebeveiliging gaat standaard onderdeel worden van de dagelijkse werkzaamheden.

Om dit te bereiken zetten we uiteraard voort wat we in 2020 gestart hebben. De aanpassing van het zaakstelsel is in het eerste kwartaal afgerond, de richtlijn voor borging van de FG en de CISO wordt geëvalueerd, het Protocol rond de melding van Datalekken wordt aangescherpt en binnen Bestuurlijke Besluitvorming blijft een juiste toepassing van de AVG een aandachtspunt. Daarnaast dient er voldoende capaciteit te zijn om te ondersteunen in projecten als Datagedreven sturen en Ondernijning.

Om deze onvermijdelijke ontwikkelingen op het gebied van informatieveiligheid en privacy mogelijk te maken vragen we in de begroting HLTsamen 2022 structureel extra middelen hiervoor.

Indien deze formatie aangetrokken kan worden, zal in het derde kwartaal een actieplan opgesteld worden om verder invulling te geven aan de aanbeveling van de Functionaris Gegevensbescherming. De Privacy Officer vervult een spilfunctie in het opstellen van het actieplan. Onderdeel van dit actieplan zullen zijn:

- Het opstellen van een communicatieplan om het privacybeleid actief uit te dragen. E-learning en bewustwordingssessies zijn mogelijke onderdelen van dit communicatieplan. Ook zal in dit communicatieplan aandacht zijn voor het verder bekendmaken in de organisatie van de functie Privacy Officer (PO). Ook wordt gekeken naar de mogelijkheden om gebruik te maken van Privacy ambassadeurs binnen de domeinen;
- Een uitvoeringsplan voor het uitvoeren en actualiseren van de DPIA's wordt opgesteld;
- Het opstellen van een autorisatiematrix voor alle systemen waar persoonsgegevens in verwerkt worden;
- Het voorbereiden van een besluit over een ambitie op privacy door alle verantwoordelijken.

Namens de directie HLTsamen

Constance Baauw
Voorzitter directie HLTsamen