Raadsbrief

Jaarverslag Functionaris Gegevensbescherming 2022

aan:	de raad van de gemeente Hillegom
zaaknummer:	Z-23-293539
datum collegevergadering:	7 februari 2023
portefeuillehouder:	Dhr. A. van Erk
behandelend ambtenaar:	Leo Koelman
emailadres:	L. Koelman@HLTsamen.nl
telefoon:	14 0252
embargo:	☐

Inleiding
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.

De FG heeft in haar jaarrapportage gebruik gemaakt van het document 'AVG Borgingsproduct 2.0' 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.

Kern van de boodschap
Uw raad informeren over de stand van zaken met betrekking tot privacy en gegevensbescherming en achterliggende context.

Nadere toelichting
We stellen vast in de bijlage het jaarverslag van de FG over 2022.
We zijn verheugd vast te stellen dat inderdaad stevige stappen zijn gezet om gegevensbescherming (privacy en informatieveiligheid) verder te implementeren in de systemen en processen. Er is een gegevensbeschermingsplan gemaakt voor de periode 2023-2025 en een jaarplan gegevensbescherming. Deze worden in het eerste kwartaal van 2023 vastgesteld. In het gegevensbeschermingsplan is de ambitie uitgesproken om binnen 3 jaar te zitten op volwassenheidsniveau 3 op een schaal van 5 gemeten volgens het VNG Privacy borgingsmodel. Bij een dergelijk volwassenheidsniveau zijn de grootse risico's in beeld en kunnen die worden beheerst.
Daarmee wordt er een bredere basis gelegd voor het borgen van gegevensbescherming in de organisatie en is er meer samenhang gekomen tussen privacy en informatieveiligheid. Dit komt ook de kwaliteit van de beleidsdocumenten ten goede en de aansluiting op de behoefte van de organisatie. De verschillende actoren binnen het gegevensbeschermingsgebied treden ook steeds meer als één team naar de organisatie toe naar buiten. Dit doen zij onder de naam Team PIV.
De personele bezetting komt steeds meer op orde. In augustus 2022 is een Privacy Officer (PO) in dienst gekomen van HLTsamen. De werving voor een tweede PO in dienstverband loopt. In de tussentijd is de vacatureruimte met externen ingevuld. Per 1

december 2022 is ook een Information Security Officer (ISO) aangesteld ter ondersteuning van de Chief information Security Officer (CISO).
Tevens is er een start gemaakt met het inrichten van risicomanagement en de daarbij behorende rollen. Bovendien is besloten de FG en CISO onder te brengen bij Concern Control. Hierdoor is hun onafhankelijke rol beter geborgd en wordt de samenwerking met audit en control geïntensiveerd.

Adequaat omgaan met persoonsgegevens is een blijvend proces en zal dan ook aandacht blijven vergen van zowel bestuur, management als medewerkers. Voor de uitvoering van de plannen zullen de verschillende organisatieonderdelen hun rol moeten pakken. Hoewel de gezette stappen positief zijn, zijn er ook zorgen vanwege de krapte op de arbeidsmarkt die in alle sectoren voelbaar is en de daarmee gepaard gaande hoge werkdruk binnen HLTsamen.

De directie HLT heeft haar tevredenheid uitgesproken over haar Jaarrapportage en kan zich vinden in de samenvatting en de conclusies. Ze acht het daarom niet nodig een aparte directiereactie ten behoeve van het College en de Raad op te stellen.

De FG is eventueel bereid om een toelichting te geven op het jaarverslag en daarbij vragen te beantwoorden.

Bijlagen:
Jaarrapportage FG Hillegom 2022

JAARRAPPORTAGE GEGEVENSBESCHERMING

Gemeente Hillegom

Ten behoeve van

het College van de gemeente Hillegom

Functionaris Gegevensbescherming
10 Januari 2023

Samenvatting

In de jaarrapportage 2021 is aangegeven welke acties en maatregelen de gemeente Hillegom heeft genomen om de doelstellingen en beginselen uit de Algemene Verordening Gegevensbescherming (AVG) te behalen en te waarborgen. Ook bevatte de jaarrapportage aandachtspunten en actiepunten voor het jaar 2022. Op 22 november 2022 is de nieuwe Functionaris Gegevensbescherming (FG) gestart. In deze jaarrapportage wordt teruggekeken hoe de geplande actiepunten uit 2022 zijn opgepakt.

Het directieteam heeft op 3 maart 2022 een reactie gegeven op het jaarverslag 2022 en daarbij de ambitie uitgesproken om in 2022 stevige vervolgstappen te zetten om de AVG verder te implementeren in de systemen en processen. In het concernplan 2022 heeft de directie opgenomen dat zij hiervoor met de FG een actieplan gaat opstellen. Deze acties moeten ertoe leiden dat de gemeente Hillegom toegroeit naar het minimale niveau waarop de risico's kunnen worden beheerst. Ook heeft het directieteam aangegeven in 2022 met het HLT-bestuur het gesprek aan te gaan over het ambitieniveau (ook wel volwassenheidsniveau genoemd) rondom het werken met privacy. Zodat ook voor de periode daarna gewerkt kan worden aan de vervolgopdracht.

We zijn verheugd vast te stellen dat inderdaad stevige stappen zijn gezet om gegevensbescherming (privacy en informatieveiligheid) verder te implementeren in de systemen en processen. Er is een gegevensbeschermingsplan gemaakt voor de periode 2023-2025 en een jaarplan gegevensbescherming. Deze worden in het eerste kwartaal van 2023 vastgesteld. In het gegevensbeschermingsplan is ook de ambitie uitgesproken om binnen 3 jaar te zitten op volwassenheidsniveau 3 van 5 gemeten volgens het VNG Privacy borgingsmodel. Bij een dergelijk volwassenheidsniveau zijn de grootse risico's in beeld en kunnen die worden beheerst.

Hierdoor is er een bredere basis gelegd voor het borgen van gegevensbescherming in de organisatie en is er meer samenhang gekomen tussen privacy en informatieveiligheid. Dit komt ook de kwaliteit van de beleidsdocumenten ten goede en de aansluiting op de behoefte van de organisatie. De verschillende actoren binnen het gegevensbeschermingsgebied treden ook steeds meer als een team naar de organisatie toe naar buiten. Dit doen zijn onder de naam Team PIV.

De personele bezetting komt steeds meer op orde. In augustus 2022 is een Privacy Officer (PO) in dienst gekomen van HLTsamen. De werving voor een tweede PO in dienstverband loopt. In de tussentijd is de vacatureruimte met externen ingevuld. Per 1 december 2022 is ook een Information Security Officer (ISO) aangesteld ter ondersteuning van de Chief information Security Officer (CISO).

Ook is er een start gemaakt met het inrichten van risicomanagement en de daarbij behorende rollen. Bovendien is besloten de FG en CISO vooruitlopend op de inrichting van de nieuwe organisatie per 1 januari 2023 onder te brengen bij Concern Control. Hierdoor is hun onafhankelijke rol beter geborgd en wordt de samenwerking met audit en control geïntensiveerd.

Adequaat omgaan met persoonsgegevens is een blijvend proces en zal dan ook aandacht blijven vergen van zowel bestuur, management als medewerkers. Voor de uitvoering van de plannen zullen de verschillende organisatieonderdelen hun rol moeten pakken. Hoewel de gezette stappen positief zijn, zijn er ook zorgen vanwege de krapte op de arbeidsmarkt die in alle sectoren voelbaar is en de daarmee gepaard gaande hoge werkdruk binnen HLTsamen.

Hillegom, 10 Januari 2023
Annerine Blufpand en Leo Koelman, Functionaris Gegevensbescherming.

Inhoud

1 Inleiding

De gemeente Hillegom dient zorgvuldig om te gaan met persoonsgegevens. De ambtelijke werkorganisatie 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 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 moeten 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 Hillegom 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 de werkzaamheden en bevindingen en doet naar aanleiding daarvan aanbevelingen. Dit jaarverslag is bedoeld voor het college van de gemeente Hillegom.

Leeswijzer

De jaarrapportage is opgesteld op basis van het AVG-borgingsproduct 2.0 van de Informatie-beveiligingsdienst. In dit document worden criteria en maatregelen omschreven die de AVG vertalen naar een kwaliteitscyclus voor gegevensbescherming en privacy voor gemeentelijke processen. In het AVG borgingsproduct zijn de controls opgenomen om nog meer aan te sluiten bij de gemeentelijke praktijk, en kunnen worden uitgebreid met relevante maatregelen voortvloeiende uit o.a. het (gemeentelijke) privacy beleid, specifieke privacywetgeving en/of richtlijnen, informatie-beveiligingsnormen en overige interne of externe richtlijnen.

Het gebruikte volwassenheidsmodel is een groeimodel gebaseerd op het Privacy Maturity Model van de Informatiebeveiligingsdienst en bestaat uit de volgende 5 niveaus:

1	Ad hoc	• Geen of onduidelijke privacy rollen en -verantwoordelijkheden • Geen of nauwelijks beheersmaatregelen aanwezig • Reactief en sturing n.a.v. incidenten • Grote afhankelijkheid van één of enkele privacyfunctionarissen • Onbewust onbekwaam
2	Herhaalbaar	• Privacy rollen en -verantwoordelijkheden toegewezen • Beheersmaatregelen zijn aanwezig, maar worden op informele wijze uitgevoerd • Standaarden en formats aanwezig: juist en in duidelijke taal • Bewust onbekwaam
3	Bepaald	• (Privacy)medewerkers tonen eigenaarschap, d.w.z. dat de rollen en verantwoordelijkheden actief worden opgepakt • Beheersmaatregelen worden consistent en gestructureerd uitgevoerd en zijn gedocumenteerd • Er wordt aantoonbaar aan de verplichtingen voldaan • Verwerkingsverantwoordelijke bestuursorganen nemen beslissingen mede op grond van risicoanalyses zoals een DPIA. • Er is een duidelijke samenhang met informatiebeveiliging • Bewust bekwaam

4	Beheerst	• De effectiviteit van beheersmaatregelen wordt periodiek geëvalueerd in een PDCA-cyclus • Er wordt proactief geïnformeerd door de proceseigenaar over de realisering van de geconstateerde benodigde verbeteringen in een PDCA-cyclus • In een jaarlijkse evaluatie blijkt een correcte PDCA-cyclus • Bewust bekwaam
5	Geoptimaliseerd	• Toekomstgericht • Proactieve houding van het college en het bestuur • Het verantwoordelijk management verzoekt aan de FG om hun verantwoording van een oordeel te voorzien. • Privacy wordt gezien als een vanzelfsprekendheid • Er wordt continu gezocht naar verbetering, zoals in de vorm van (interne of externe) tooling • Privacy wordt gezien als een kans of unique selling point (USP) • Er wordt verbinding gezocht met andere concerndisciplines • Kennis en ervaringen worden actief gedeeld met n en andere relevante organisaties waardoor best practices in land ontstaan • Onbewust bekwaam

Vanaf niveau 3 wordt voldaan aan de minimale wettelijke vereisten. Dit is het niveau dat het bestuur nastreeft. Op dit moment voldoet de gemeente Hillegom hier nog niet aan.

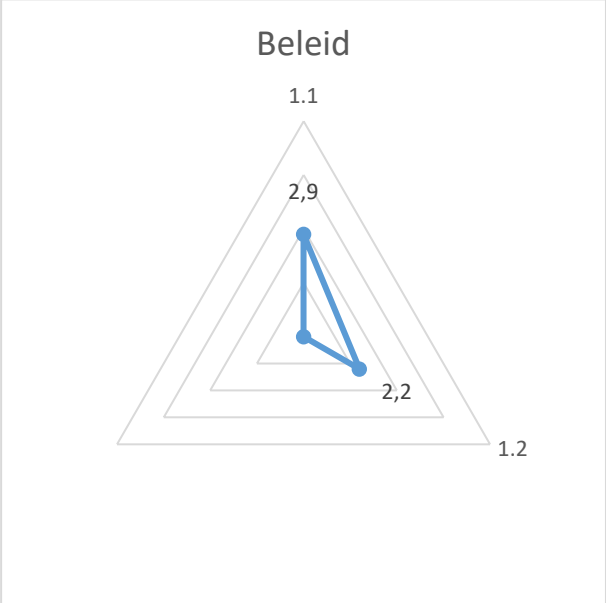
Het volwassenheidsniveau wordt bepaald door een zevental aandachtsgebieden, thema's. Per thema wordt bepaald in welke mate aan de vijf hiervoor genoemde niveaus wordt voldaan. Gezamenlijk levert dit het volwassenheidsniveau van de gemeente Hillegom op. Op dit moment bevindt de gemeente Hillegom zich nagenoeg op volwassenheidsniveau 2.

Hieronder wordt elk privacy thema toegelicht met een korte beschrijving van het thema, de resultaten uit het borgingsdocument AVG, de beschrijving van de activiteiten in 2022 en de aandachtspunten voor 2023 om een hoger niveau te bereiken. Elk thema bevat een spindiagram die de status van de implementatie van de privacy maatregelen weergeeft.

2 Privacy in de gemeente Hillegom

2.1 Het beleid

Het verplichte gestelde Privacybeleid is een kader waarin de gemeente Hillegom aangeeft aan welke principes zij zich houdt bij de verwerking van persoonsgegevens. Tevens beschrijft het hoe verantwoordelijkheden op het niveau van lijnmanagement zijn benoemd, belegd en vastgelegd.



1.1 Er is algemeen privacybeleid en uitwerkingen daarvan.
1.2 Verantwoordelijkheden op het niveau van het lijnmanagement zijn benoemd, belegd en vastgelegd.

2.1.1 Beschrijving activiteiten 2022

In 2022 is het Gegevensbeschermingsplan 2023-2025 opgesteld. Hierin is ook de ambitie voor gegevensbescherming opgenomen. Verder is het een jaarplan Gegevensbescherming 2023 opgesteld. Gedurende de periode april 2022 tot en met september 2022 is een nulmeting uitgevoerd bij de verschillende teams. De uitkomsten zijn meegenomen in het jaarplan Gegevensbescherming 2023.

2.1.2 Aandachtspunten voor 2023

- **Actualiseren beleid en opstellen nieuw beleid**

Het Privacybeleid is in 2019 opgesteld en dient in 2023 geactualiseerd te worden.
In het jaarplan privacy is opgenomen dat het Privacy by design en default beleid in 2023 wordt vastgesteld.

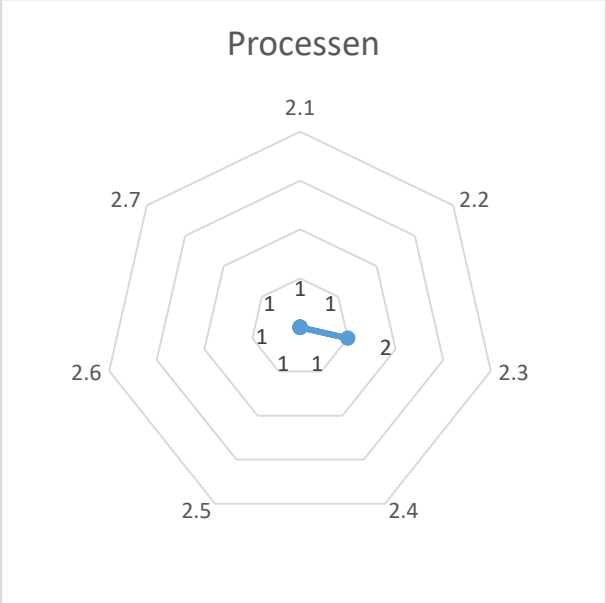
- Opstellen van domein specifiek beleid

In domein specifiek beleid wordt beschreven hoe het betreffende domein omgaat met de bescherming van persoonsgegevens bij de uitvoering van (sectorspecifieke) wet- en regelgeving. Waar nodig dient domein specifiek beleid opgesteld te worden. Denk bijv. aan beleid voor hoe om te gaan met privacy van sollicitanten/medewerkers.

2.2 Processen

De verwerkingen van persoonsgegevens door de gemeente Hillegom 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. Alle verwerkingen van

persoonsgegevens dienen actueel gehouden te worden middels registratie in het Register van Verwerkingen. Daarnaast is de gemeente Hillegom in bepaalde gevallen verplicht om een gegevensbeschermingseffectbeoordeling (ook wel DPIA genoemd) uit te voeren.



2.1	Werkprocessen (voor hoge risico verwerkingen) waarin persoonsgegevens worden verwerkt zijn vastgesteld.
2.2	Er zijn passende instructies en protocollen (voor hoge risico verwerkingen) voor medewerkers over de omgang met persoonsgegevens in werkprocessen.
2.3	De organisatie heeft de verwerkingen waar zijzelf (gezamenlijke) verwerkingsverantwoordelijk of verwerker voor is in een verwerkingsregister opgenomen.
2.4	Voor verwerkingen (met hoge privacyrisico's) worden (pre-) DPIA's uitgevoerd en de mitigerende maatregelen worden doorgevoerd.
2.5	Persoonsgegevens die niet meer nodig zijn worden tijdig verwijderd of geanonimiseerd.
2.6	Doorgiftes van persoonsgegevens naar buiten de EER zijn bekend.
2.87	Sancties in wetgeving en contracten en contractuele eisen over de bescherming van persoonsgegevens zijn bekend.

2.2.1 Beschrijving activiteiten 2022

Het format voor het uitvoeren van een gegevensbeschermingseffectbeoordeling (DPIA) is geactualiseerd, ook de procedure voor het uitvoeren van een DPIA is beschreven. De besluitvorming over de toepassing en uitvoering gaat in 2023 plaatsvinden.

	2022
Aantal uitgevoerde en geaccordeerde DPIA's	2

Het toetsen van (nieuwe) verwerkingen van persoonsgegevens aan de beginselen van de AVG krijgt steeds meer structuur en lijkt meer in de organisatie ingebed te zijn. Denk aan het (vooraf) verplicht invullen van de privacy checklist bij nieuwe én bestaande verwerkingen, het opstellen van beleid, een aanbesteding, een nieuwe business case of andere verwerkingen als hier persoonsgegevens bij betrokken zijn.
Ook is een start gemaakt met het invullen van het handboek PIV waarin protocollen en richtlijnen zijn vastgelegd. Dit is een doorlopende activiteit.

2.2.2 Aandachtspunten voor 2023

- **Uitvoeren van DPIA's**

In 2023 dient een plan van aanpak voor de uitvoering van DPIA's vastgesteld te worden en dient actief aan de slag gegaan te worden met de uitvoering hiervan. Op die manier krijgt de organisatie zicht op haar grootste risico's.
Bovendien is het uitvoeren van DPIA's geen eenmalige activiteit. Het is van belang om bij nieuwe processen en systemen alert te zijn op de eventuele verplichting tot het uitvoeren van DPIA's, maar er ook op toe te zien dat de aanbevelingen uit de uitgevoerde DPIA's worden uitgevoerd. Ook hebben DPIA's een beperkte houdbaarheid en dienen deze periodiek beoordeeld te worden of aanpassing nodig is en zullen in een PDCA-cyclus meegenomen moeten worden.

- **Actualisatie van het register van verwerkingen**

De verantwoordelijkheid voor het onderhoud en de actualisatie van (onderdelen van) het register ligt bij de Privacy Officer. Proceseigenaren zijn verantwoordelijk voor het signaleren van wijzigingen met betrekking tot de verwerkingen van persoonsgegevens maar zijn nog onvoldoende bewust om wijzigingen op bestaande verwerkingen of het toevoegen van nieuwe verwerkingen tijdig door te geven. Hier dient in 2023 meer aandacht gegeven te worden. Het register van verwerkingen is in 2021 op een aantal punten geactualiseerd, maar ook dit is geen eenmalige activiteit. Het register dient periodiek geactualiseerd te worden en waar nodig aangevuld om te blijven voldoen aan de AVG. Het register moet aantonen dat de organisatie in control is over alle verwerkingen van persoonsgegevens die in de organisatie plaatsvinden.

- Borgen handboek PIV

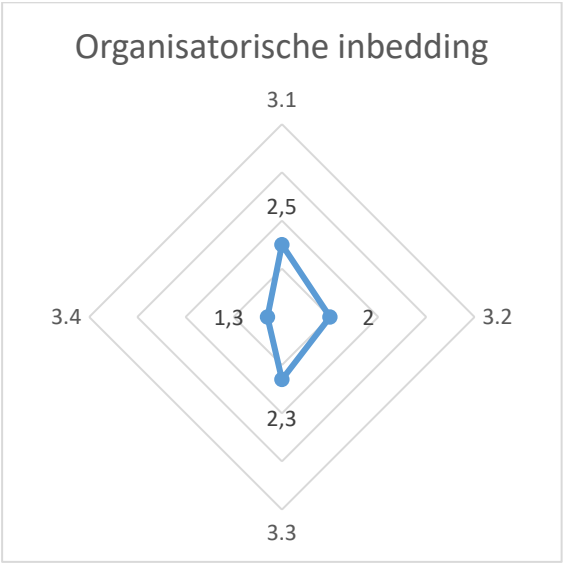
In het handboek PIV worden protocollen en/of een instructies opgesteld.
Denk aan een protocol hoe om te gaan met privacy en informatiebeveiliging bij het gebruik van telefoons van medewerkers die zowel zakelijk als privé worden gebruikt. Deze moet nog ingebed worden in de organisatie.

- Tijdig verwijderen of anonimiseren van persoonsgegevens

Het verwijderen of anonimiseren van persoonsgegevens is een belangrijk punt van aandacht. In 2022 is een applicatie hiervoor in gebruik genomen. Onduidelijk is of het vernietigen van papieren en digitale informatie tijdig gebeurt. Het niet tijdig vernietigen van persoonsgegevens is in strijd met de AVG en andere specifieke wetgeving. Geadviseerd wordt te onderzoeken hoe en op welke wijze digitale informatie conform de Archiefwet vernietigd moet worden.

2.3 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.



3.1 De gemeente heeft een FG aangesteld en goed gepositioneerd.
3.2 Er is – naast de FG - ruime (juridische) kennis en ervaring aanwezig over privacy en relevante wet- en regelgeving.
3.3 De Ondernemingsraad (OR) wordt geïnformeerd en betrokken wanneer het gaat om de bescherming van persoonsgegevens van medewerkers.
3.4 Er zijn voldoende middelen beschikbaar om privacybescherming te bevorderen in kennis, houding en gedrag van medewerkers in de organisatie.

2.3.1 Beschrijving activiteiten 2022

Naast de integrale aanpak vanuit privacy en informatieveiligheid komt de personele bezetting steeds meer op orde. In Augustus 2022 is een Privacy Officer (PO) in dienst gekomen van HLTsamen. De werving voor een tweede PO in dienstverband loopt. In de tussentijd is de vacature ruimte met extern opgevuld. Per 1 December 2022 is ook een Information Security Officer (ISO) aangesteld ter

ondersteuning van de Chief information Security Officer (CISO). Het team moet verder worden opgebouwd. Dat gebeurd aan de hand van een PIV team visie, missie en ambitie.
Ook is er een start gemaakt met het inrichten van risicomanagement en de daarbij behorende rollen. Bovendien is besloten de FG en CISO vooruitlopend op de inrichting van de nieuwe organisatie per 1 januari 2023 onder te brengen bij Concern Control. Hierdoor is hun onafhankelijke rol beter geborgd en wordt de samenwerking met audit en control geïntensiveerd.

Bij Maatschappelijke Ontwikkeling is in juni 2022 een bewustwording sessie voor de medewerkers gehouden, toegespitst op hun werkzaamheden. Op 5 oktober 2022 heeft er een raadsbijeenkomst plaatsgevonden voor de drie raden om hen bij te praten over gegevensbescherming en om bewustwording te creëren. Hierbij zijn privacy (FG) en informatieveiligheid (CISO) gezamenlijk opgetrokken. Ook zijn er filmpjes gemaakt waarin het PIV zich voorstelt en ingaat op wat de AVG inhoud en wat informatieveiligheid. In december 2022 is vanuit het PIV team ook meegedacht met de invulling van het introductieprogramma voor nieuwe medewerkers. Om het beleid actief uit te dragen zijn door de PO tenslotte regelmatig blogs op het intranet geschreven. Er is een nieuwe E-learning (nano-learning) gestart op het gebied van privacy en informatieveiligheid. Daarbij worden alle medewerkers wekelijks getriggerd en bewuster gemaakt op de invloed en noodzaak van privacy en informatiebeveiliging binnen het gemeentelijke werkveld met aandacht voor kennis, houding en gedrag.

2.3.2 Aandachtspunten 2023

- Aanstellen en inzetten ambassadeurs gegevensbescherming

Om verdere stappen te kunnen maken en gegevensbescherming goed te kunnen borgen in de organisatie is het gewenst dat de domeinen hun rol op privacy en informatiebeveiliging gebied pakken. Het aanwijzen van een privacy ambassadeurs kan hen daarbij behulpzaam zijn.

- Introductie en aanpak PIV in de organisatie

De PIV aanpak zoals opgenomen in het Gegevensbeschermingsplan 2023 moet nog goed landen in de organisatie door het actiever uit te dragen met de ondersteuning van een communicatieplan.

2.4 Rechten van betrokkenen

Degene van wie persoonsgegevens verwerkt worden (de betrokkene) dienen zowel actief als passief geïnformeerd te worden: 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 rechtmatig in staat controle en invloed uit te oefenen over zijn of haar persoonsgegevens die door de organisatie verwerkt worden.

4.1	De verwerkingsverantwoordelijke heeft processen ingericht om de rechten van betrokkenen te faciliteren.
4.2	De gemeente heeft inzichtelijk welke besluiten zij neemt op basis van automatisch verwerkte persoonsgegevens. Geautomatiseerde besluitvorming is omkleed met passende waarborgen om de privacy van betrokkenen te beschermen.
4.3	Voorafgaand aan de verwerking worden betrokkenen actief, tijdig en adequaat geïnformeerd.
4.4	Er is een communicatieplan over privacy om invulling te geven aan de AVG-transparantieverplichtingen.
4.5	Op de gemeentelijke website staat een privacy- en cookieverklaring met informatie over verwerkingen van persoonsgegevens door de gemeente.
4.6	Verdergaande mogelijkheden om invulling te geven aan de rechten van betrokkenen worden toegepast.

2.4.1 Beschrijving activiteiten 2022

Binnen de gemeente Hillegom zijn processen ingericht om de rechten van betrokkenen te faciliteren. In 2022 zijn deze op papier geactualiseerd. De procedure en het proces dienen verder uitgewerkt te worden en formeel te worden vastgesteld.
In de privacyverklaring geeft de gemeente Hillegom aan hoe en waar betrokkenen verzoeken kunnen indienen. Verzoeken kunnen zowel schriftelijk als elektronisch worden ingediend. Intern zijn proceseigenaren verantwoordelijk voor de afhandeling van de verzoeken op grond van de AVG. De coördinatie vindt plaats via de Privacy Officer. In de praktijk vindt de feitelijke afhandeling door de Privacy Officer plaats.

Soms komen ook verzoeken binnen via de FG. De FG ziet erop toe dat de proceseigenaren de verzoeken binnen de wettelijke termijn oppakken. Bij de afhandeling van verzoeken wordt gebruik gemaakt van de informele aanpak. Indien een inwoner zowel een AVG-verzoek als een klacht indient tegen de organisatie trekt de PO in overleg met de betrokkene, samen met de klachten coördinator op. Dit proces is nog niet formeel vastgesteld. In 2022 zijn er in totaal 8 AVG-verzoeken ingediend bij de HLTsamen gemeenten.

	2021	2022
Verzoek tot inzage	1	1
Wissen van persoonsgegevens	0	0
Verzoek tot rectificatie	0	0
Totaal	**1**	**1**

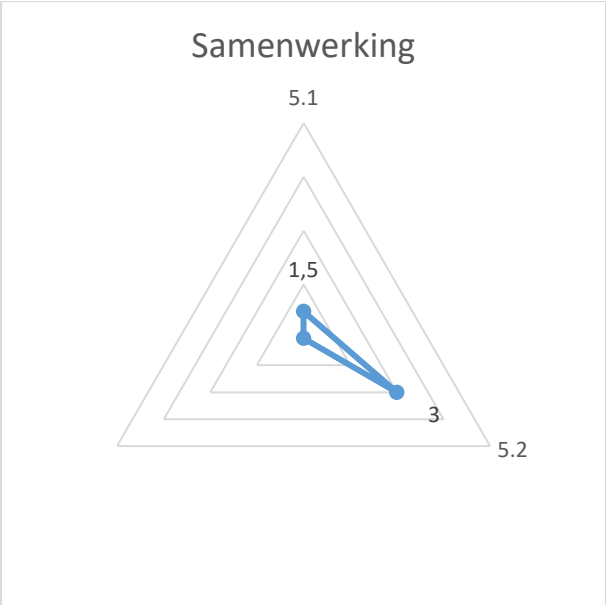
2.4.2 Aandachtspunten voor 2023

- Verbeteren intern proces van afhandeling van verzoeken

Binnen de gemeente Hillegom zijn processen ingericht om de rechten van betrokkenen te faciliteren. In 2022 zijn deze op papier geactualiseerd. De procedure en het proces dienen verder uitgewerkt te worden en formeel te worden vastgesteld. Het afwegingskader is nog niet beschreven. Niet alle medewerkers weten hierdoor hoe zij een verzoek op grond van de AVG moeten oppakken. Dit kan worden verbeterd door concrete instructies zoals het opstellen van een concreet stappenplan voor proceseigenaren, zodat zij beter in staat worden gesteld om verzoeken van betrokkenen op te pakken. De Privacy Officer en de nog aan te stellen ambassadeurs gegevensbescherming spelen hier een belangrijke rol bij. Extra aandacht is hierbij gewenst op misbruik van de uitoefening van de AVG-rechten door een betrokkene.

2.5 Samenwerking

De gemeente Hillegom werkt in diverse rollen en hoedanigheden samen met 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 ook te voldoen aan de AVG. De AVG verplicht om deze verwerkingen schriftelijk vast te leggen in een zogenaamde Verwerkersovereenkomst.



5.1 De organisatie heeft inzichtelijk welke AVG-rol externe partijen innemen en er worden afspraken gemaakt conform de AVG.

5.2 Eenmalige gegevensverstrekkingen worden getoetst aan de relevante privacywet- en regelgeving.

2.5.1 Beschrijving activiteiten 2022

De gemeente Hillegom dient dan ook afspraken te maken met deze andere partijen. De gemeente Hillegom heeft deels inzichtelijk welke AVG-rol externe partijen innemen (verwerkers, gezamenlijke en zelfstandige verwerkingsverantwoordelijken). De bewustwording onder medewerkers om bij gegevensverwerkingen afspraken te maken groeit. In het inkoopproces is het nu geborgd. Er wordt gebruik gemaakt van de standaard verwerkersovereenkomst van de VNG. In 2022 is vanuit Juridische Zaken gestart met het in kaart brengen van alle (keten)samenwerkingen en de daarbij behorende verantwoordelijkheden.

2.5.2 Aandachtspunten voor 2023

- Grip krijgen op gegevensverwerkingen door externe partijen

Er is niet voldoende grip op de gegevensverwerkingen door externe partijen. Het is niet bekend of bij alle verwerkingen afspraken worden gemaakt conform de AVG. Geadviseerd wordt om dit beter in te bedden in de organisatie.
Het is overigens niet altijd even inzichtelijk welke AVG-rol een externe partij inneemt. Dit wordt ook landelijk als een probleem ervaren. De Informatiebeveiligingsdienst heeft een factsheet en een beslisboom ontwikkeld om gemeenten op weg te helpen bij het vaststellen van de privacy positie van externe partijen. Ook zijn concrete voorbeelden uit de gemeentelijke praktijk uitgewerkt. Het is aan te bevelen medewerkers die in de praktijk veel contracten sluiten, via een workshop op de hoogte te brengen van deze factsheet. Hier zou de aan te stellen PO een rol kunnen spelen.

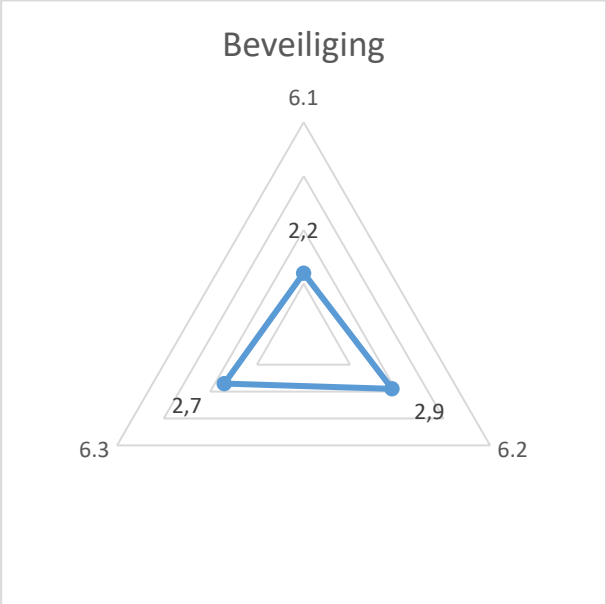
- Archiveren verwerkersovereenkomsten

Er is een systematiek ontwikkeld voor het opslaan van contracten in het zaaksysteem. Deze kan voor verwerkersovereenkomsten en gegevensleveringsovereenkomsten gevolgd worden. Een organisatie brede instructie kan daarbij behulpzaam zijn.

2.6 Beveiliging

Vanuit het algemene behoorlijkheidsbeginsel, het integriteitsbeginsel en het vertrouwelijkheidsbeginsel is het essentieel dat de organisatie passende technische en organisatorische maatregelen neemt ter beveiliging van persoonsgegevens. Daarnaast geldt er onder de AVG een meldplicht met betrekking tot 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.



6.1 Verwerkingen worden zodanig ingericht dat rekening wordt gehouden met de beginselen van Privacy by Design (PbD) en privacy by default.
6.2 De gemeente heeft inzicht in (potentiële) privacy-incidenten, zoals datalekken.
6.3 Het IB-beleid en de IB-procedures houden rekening met privacyspecifieke beveiligingseisen. Deze beveiligingseisen worden geïmplementeerd.

2.6.1 Beschrijving activiteiten 2022

In februari 2022 is het Informatiebeveiligingsplan vastgesteld. In dit plan zijn de acties met de hoogste prioriteit volgens de risicoanalyse methode Digitale Weerbaarheid benoemd. Een groot deel van de acties zijn in 2022 uitgevoerd.

De gemeente Hillegom streeft een open cultuur na waarin datalekken intern en zonder enige impact voor de melder gemeld kunnen worden.
Bij een ernstig datalek moet het datalek ook aan de Autoriteit Persoonsgegevens melden. Voor HLTsamen is dit in 1 geval gebeurd. Opvallend is dat de meeste datalekken net als vorig jaar een menselijke oorzaak hebben. De analyse van datalekken heeft geleid tot diverse verbeteringen.

Overzicht datalekken:

	2022 (2021)	2022 (2021)
Oorzaak	Meldenswaardig	Niet meldenswaardig
Menselijke oorzaak	1 (5)	6 (7)
Technische oorzaak	0 (0)	1 (0)
Organisatie	0 (0)	0 (0)
Totaal aantal datalekken	**8 (12)**	

2.6.2 Aandachtspunten voor 2023

- Privacy by design & Privacy by default

Er wordt nog niet structureel rekening gehouden met privacy by design en privacy by default bij (potentieel) nieuwe verwerkingen. Ook het implementeren van de privacy specifieke beveiligingseisen van het IB-beleid en de IB-procedures vereisen meer aandacht. Bij ICT-aanbestedingen is dit geborgd door de eis dat voldaan moet worden aan de GIBIT (betekent voldoen aan AVG en Baseline Informatie Overheid) en door de invoering van het STRategie en Projecten Portfolio (STRaPP). De processen en

middelen om privacy by design en privacy by default te borgen zijn reeds opgetogen, maar de borging hiervan behoeft organisatie-breed aandacht. Zie ook hetgeen hierover bij beleid is opgemerkt.

- Crisiscommunicatieplan

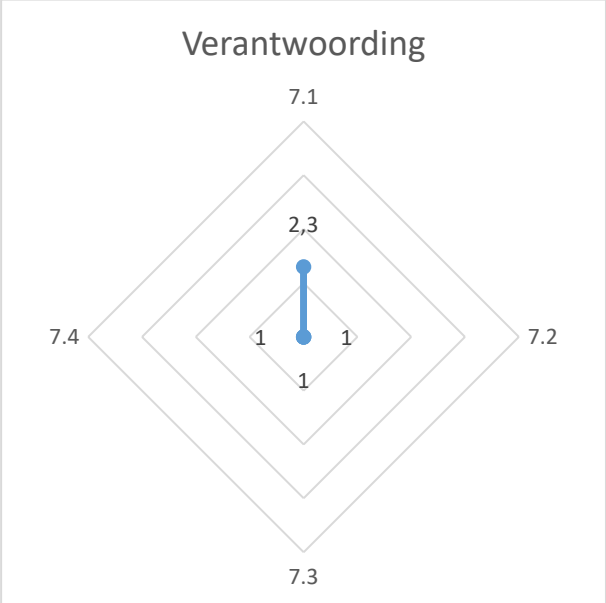
De hacks bij het Hof van Twente en Lochem laten zien dat communicatie naar buiten toe essentieel is voor het herstel van vertrouwen bij de burger. Een crisiscommunicatieplan dient te worden opgesteld voor datalekken met een hoge (maatschappelijke) impact dat aansluit en onderdeel uitmaakt van het crisisplan.

- **Proceseigenaren wijzen op verantwoordelijkheid**

Het wijzen op de verantwoordelijkheid van proceseigenaren m.b.t beveiligingsincidenten en het oplossen daarvan moet worden geïntensiveerd.

2.7 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 moet kunnen aantonen (bewijzen) dat de verwerkingen van persoonsgegevens voldoen aan de beginselen en verplichtingen vanuit de AVG en aan andere geldende wet- en regelgeving.



7.1	Periodiek worden gegevensverwerkingen geëvalueerd en is de naleving van de AVG aangetoond.
7.2	Er is een actueel overzicht van de verwerkingen met een hoog privacy risico en de uitgevoerde DPIA's.
7.3	Periodiek worden interne en externe partijen op de hoogte gehouden over de omgang met persoonsgegevens binnen de gemeente
7.4	Periodiek wordt een GAP-analyse uitgevoerd om inzichtelijk te maken waar de organisatie staat op het gebied van het beschermen van persoonsgegevens.

2.7.1 Beschrijving activiteiten in 2022

De FG geeft organisatie-breed advies aan de wijze waarop persoonsgegevens worden beschermd. Hiervoor is de afgelopen jaren het borgingsdocument AVG van de IBD gebruikt als het privacy normenkader waaraan de organisatie moet voldoen om een bepaald volwassenheidsniveau te bereiken. De FG rapporteert jaarlijks over de gegevensbescherming binnen de gemeente Hillegom. Het openbaar maken van de jaarrapportage draagt bij aan de verantwoordingsplicht van het college van B&W. Het college is transparant naar de inwoners over de stand van zaken rondom gegevensbescherming binnen de organisatie en wil zo laten zien dat zij stappen zet om een hoger volwassenheidsniveau te bereiken. Ook draagt de FG bij aan de verticale verantwoording in het kader van informatiebeveiliging (zoals bij de beantwoording van ENSIA vragen). Daar er binnen de gemeente Hillegom meer samenwerking is tussen privacy en informatiebeveiliging zal ook bekeken worden hoe de verantwoording vanaf 2023 het beste integraal kan plaatsvinden.

2.7.2 Aandachtspunten 2023

- Blijf zicht houden op risicovolle processen

Gegevensbescherming maakt nog geen structureel onderdeel uit van de risicomanagementaanpak. Voor het uitvoeren van DPIA is weinig tot geen budget of capaciteit beschikbaar, terwijl het juist bijdraagt aan de verbetering van de kwaliteit van de gemeentelijke dienstverlening. Het analyseren van de gemeentelijke processen en het vinden en mitigeren van de risico's in deze processen zorgen er uiteindelijk voor dat HLTsamen gegevensbescherming structureel in de organisatie inbedt en actief bouwt aan het fundament: een betrouwbare overheid. Hierbij het advies dat er voor privacy en informatiebeveiliging een actueel te houden overzicht komt van 1) de meest risicovolle processen, 2) de meest risicovolle applicaties 3) de meest risicovolle maatschappelijke processen en 4) de meest risicovolle verbonden partijen.

- Verantwoording op Domeinniveau

Nadat een volwassenheidsniveau voor de privacy is vastgesteld kan het college de status van het niveau van gegevensbescherming per domein volgen en, waar nodig, bijsturen wanneer de domeinen hierover rapporteren. Voorstel: Nu er een volwassenheidsniveau wordt vastgesteld kan er in de toekomst op domein niveau door de afzonderlijke domeinen gerapporteerd worden.

3 Conclusie

Er zijn in 2022 stevige stappen zijn gezet om gegevensbescherming (privacy en informatieveiligheid) verder te implementeren in de systemen en processen. Er is een gegevensbeschermingsplan gemaakt voor de periode 2023-2025 en een jaarplan gegevensbescherming. Daarbij is ook de ambitie uitgesproken om de komende jaren te groeien naar volwassenheidsniveau 3 van 5. Bij een dergelijk volwassenheidsniveau zijn de grootse risico's in beeld en kunnen die worden beheerst.

Hierdoor is er een bredere basis gelegd voor het borgen van gegevensbescherming in de organisatie en is er meer samenhang gekomen tussen privacy en informatieveiligheid. Dit komt ook de kwaliteit van de beleidsdocumenten ten goede en de aansluiting op de behoefte van de organisatie.

Vooruitlopend op de inrichting van de nieuwe organisatie is besloten de FG en CISO per 1 januari 2023 onder te brengen bij HLTsamen Concern Control. Hierdoor is hun onafhankelijke rol beter geborgd en wordt de samenwerking met audit en control geïntensiveerd.