



### FG jaarverslag Gegevensbescherming 2023 gemeente Hillegom

---

aan: de raad van de gemeente Hillegom  
datum: 14 maart 2023

ons kenmerk: Z-24-363917  
datum collegevergadering: 2 april 2024  
portefeuillehouder: Dhr. A. van Erk  
behandelend ambtenaar: Jos Baan  
emailadres: j.baan@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**

In 2023 zijn er goede stappen zijn gezet om gegevensbescherming (privacy en informatieveiligheid) verder te implementeren in de organisatie, in de systemen en in de processen.

Gebruikmakend van dezelfde meetlat als vorig jaar, middels het VNG Borgingproduct 2.0, kan geconcludeerd worden dat de organisatie van het vastgestelde volwassenheidsniveau 1,8 van eind 2022 een sprong heeft gemaakt naar een volwassenheidsniveau 2,2. De meeste winst is behaald door het opstellen van beleid en het beter beschrijven van de privacy- en informatieveiligheidsprocessen (PIV-processen) en het consequenter uitvoeren van privacy-risicoanalyses.

Er is nieuw langetermijnbeleid opgesteld in het Strategisch beleid Privacy en Informatieveiligheid plan. In het Tactisch beleid is dit verder uitgewerkt en zal uiteindelijk vertaald worden naar gedetailleerde werkafspraken in proces- en procedure beschrijvingen. Daarmee zal een solide basis worden gelegd om reproduceerbaar en controleerbaar de taken en verplichtingen te borgen die de AVG, de 'basisnormenkader Informatiebeveiliging Overheid' (BIO) en de nieuwe Europese richtlijn 'Network and Security' (NIS2) vereisen. Daarnaast geeft het duidelijkheid aan de organisatie hoe de taken worden uitgevoerd en draagt het bij aan een efficiëntere uitvoering van de gemeentelijke taken.

2023 is een jaar geweest dat de gehele organisatie veel bewuster is geworden. De grote deelname aan onze bewustwordingscampagnes, de hoeveelheid en de type meldingen van incidenten en de toename in adviesvragen getuigen hiervan. Van onbewust onbekwaam naar bewust onbekwaam is een grote sprong! De volgende stap naar bewust bekwaam, (de ambitie om volwassenheidsniveau 3 te bereiken) zal een uitdagend traject

zijn waarbij de betrokkenheid en inzet van de gehele organisatie nodig is. Daarbij is het van belang dat de huidige PIV-organisatie solide blijft acteren, hun taken, hun inzet en noodzaak door directie en bestuur ondersteund blijft en de betrokkenheid van alle medewerkers helpt stimuleren.

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

---

Bijlagen:

FG jaarverslag Gegevensbescherming 2023 gemeente Hillegom

# **JAARRAPPORTAGE GEGEVENSBESCHERMING 2023**



**Ten behoeve van  
het college van de gemeente Hillegom**

# Samenvatting

In de voorgaande jaarrapportage over 2022 is aangegeven welke acties en maatregelen de werkorganisatie HLTsamen in opdracht van de drie gemeenten Hillegom, Lisse en Teylingen op zich 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 2023. In deze jaarrapportage wordt teruggekeken hoe de geplande actiepunten uit 2022 zijn opgepakt.

We zijn verheugd vast te stellen dat er 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. In alle beleidsplannen en het meer op acties gedreven gegevensbeschermingsplan is de ambitie uitgesproken om in 2025 het volwassenheidsniveau 3 te behalen gemeten volgens het VNG Privacy borgingsmodel. Dit is ook volgens de VNG/IBD het minimale vereiste niveau voor een gemeentelijk organisatie. Bij een dergelijk volwassenheidsniveau zijn namelijk de grootse risico's goed in beeld en kunnen die door de organisatie worden beheerst.

Er is wederom verdere vooruitgang geboekt en een bredere basis gelegd voor het borgen van gegevensbescherming in de organisatie. Zo is er meer samenhang gekomen tussen privacy en informatieveiligheid. Dit als gevolg van de nauwe samenwerking tussen beide disciplines, door het opstellen van doordachte beleidsdocumenten 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 zij onder de naam Team PIV, nu inmiddels en mede door gerichte en ludieke acties bekend binnen de gehele organisatie.

De personele bezetting was in de basis op orde. In maart 2023 is een tweede Privacy Officer (PO) het team komen versterken, zodat het PIV-team nu bestaat uit twee Privacy Officers, een Technical Information Security Officer (TISO), een Information Security Officer (ISO), een Chief information Security Officer (CISO) en een Functionaris Gegevensbescherming (FG). Helaas heeft de per 1 december 2022 aangestelde Information Security Officer (ISO) ons noodgedwongen per augustus 2023 alweer moeten verlaten en is door speciaal verlof de CISO-functie de tweede helft van het jaar slechts beperkt ingevuld geweest.

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, 22 Januari 2024  
Leo Koelman, Functionaris Gegevensbescherming.

# Inhoudsopgave

<b>1</b>	<b>INLEIDING .....</b>	<b>4</b>
	LEESWIJZER .....	4
	HET VOLWASSENHEIDSMODEL.....	4
<b>2</b>	<b>PRIVACY IN DE GEMEENTE HILLEGOM.....</b>	<b>6</b>
2.1	HET BELEID .....	6
2.2	PROCESSEN .....	7
2.3	ORGANISATORISCHE INBEDDING.....	9
2.4	RECHTEN VAN BETROKKENEN.....	11
2.5	SAMENWERKING .....	13
2.6	BEVEILIGING.....	14
2.7	VERANTWOORDING .....	16
<b>3</b>	<b>CONCLUSIE .....</b>	<b>18</b>

# 1 Inleiding

De gemeente Hillegom dient zorgvuldig om te gaan met persoonsgegevens. De ambtelijke werkorganisatie HLTsamen 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 organisatie 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 er passende technische en organisatorische beveiligingsmaatregelen worden getroffen om onrechtmatige toegang tot deze persoonsgegevens tegen te gaan en daardoor een onrechtmatig gebruik van deze persoonsgegevens te voorkomen. Daarnaast heeft HLTsamen ook te maken met tal van privacyregels in sectorspecifieke wetgeving. Dit alles heeft gevolgen voor de inrichting van processen en systemen in en van HLTsamen.

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

Zoals bepaald in het onlangs hernieuwde Strategisch beleid wordt de mate van het voldoen aan de AVG-verplichtingen gemeten aan de hand van het AVG-borgingsproduct van de Informatie-beveiligingsdienst. In 2023 heeft de VNG een vernieuwde versie van het borgingsproduct versie 3.0 uitgegeven waarin wordt bepaald dat het minimale volwassenheidsniveau op niveau 3 wordt gesteld. In dit jaarrapport van 2023 wordt naast dit meest recente borgingsproduct ook de vorige versie gebruikt om aan de hand van de zogenaamde spindiagrammen de voortgang ten opzichte van vorig jaar te laten zien. In de AVG-borgingsproducten zijn controls opgenomen gericht op de gemeentelijke praktijk, en kunnen worden uitgebreid met relevante (aanvullende) maatregelen voortvloeiende uit o.a. het (gemeentelijke) privacy beleid, specifieke privacywetgeving en/of richtlijnen, informatie-beveiligingsnormen en overige interne of externe richtlijnen. Daar waar van toepassing zijn deze extra controls toegevoegd aan het rapport.

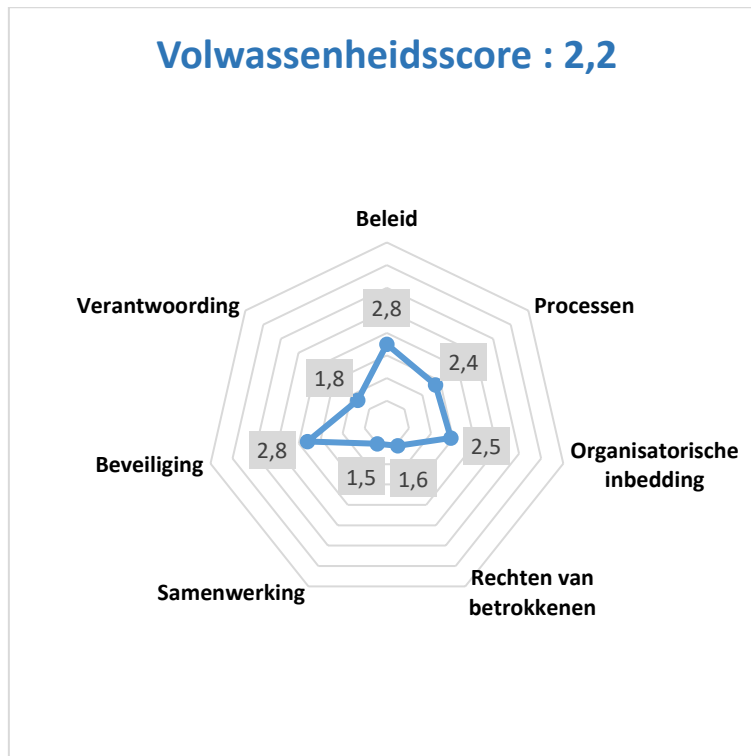
## Het volwassenheidsmodel

HLTsamen heeft de ambitie uitgesproken om voor 2025 blijvend aan de gestelde eisen te voldoen die behoren bij het volwassenheidsniveau 3. 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	<ul style="list-style-type: none"><li>• Geen of onduidelijke privacy rollen en -verantwoordelijkheden</li><li>• Geen of nauwelijks beheersmaatregelen aanwezig</li><li>• Reactief en sturing n.a.v. incidenten</li><li>• Grote afhankelijkheid van één of enkele privacyfunctionarissen</li><li>• Onbewust onbekwaam</li></ul>
2	Herhaalbaar	<ul style="list-style-type: none"><li>• Privacy rollen en -verantwoordelijkheden toegewezen</li><li>• Beheersmaatregelen zijn aanwezig, maar worden op informele wijze uitgevoerd</li><li>• Standaarden en formats aanwezig: juist en in duidelijke taal</li><li>• Bewust onbekwaam</li></ul>
3	Bepaald	<ul style="list-style-type: none"><li>• (Privacy)medewerkers tonen eigenaarschap, d.w.z. dat de rollen en verantwoordelijkheden actief worden opgepakt</li><li>• Beheersmaatregelen worden consistent en gestructureerd uitgevoerd en zijn gedocumenteerd</li><li>• Er wordt aantoonbaar aan de verplichtingen voldaan</li><li>• Verwerkingsverantwoordelijke bestuursorganen nemen beslissingen mede op grond van risicoanalyses zoals een DPIA.</li><li>• Er is een duidelijke samenhang met informatiebeveiliging</li><li>• Bewust bekwaam</li></ul>

4	Beheerst	<ul style="list-style-type: none"> <li>• De effectiviteit van beheersmaatregelen wordt periodiek geëvalueerd in een PDCA-cyclus</li> <li>• Er wordt proactief geïnformeerd door de proceseigenaar over de realisering van de geconstateerde benodigde verbeteringen in een PDCA-cyclus</li> <li>• In een jaarlijkse evaluatie blijkt een correcte PDCA-cyclus</li> <li>• Bewust bekwaam</li> </ul>
5	Geoptimaliseerd	<ul style="list-style-type: none"> <li>• Toekomstgericht</li> <li>• Proactieve houding van het college en het bestuur</li> <li>• Het verantwoordelijk management verzoekt aan de FG om hun verantwoording van een oordeel te voorzien.</li> <li>• Privacy wordt gezien als een vanzelfsprekendheid</li> <li>• Er wordt continu gezocht naar verbetering, zoals in de vorm van (interne of externe) tooling</li> <li>• Privacy wordt gezien als een kans of unique selling point (USP)</li> <li>• Er wordt verbinding gezocht met andere concerndisciplines</li> <li>• Kennis en ervaringen worden actief gedeeld met n en andere relevante organisaties waardoor best practices in land ontstaan</li> <li>• Onbewust bekwaam</li> </ul>

Het volwassenheidsniveau wordt bepaald door een zevental aandachtsgebieden, thema's. Per thema is bepaald in welke mate aan de vijf hiervoor genoemde niveaus wordt voldaan. Gezamenlijk levert dit het volwassenheidsniveau van HLTsamen op. Zoals het rapport zal aantonen bevindt HLTsamen zich op dit moment op volwassenheidsniveau 2,2.

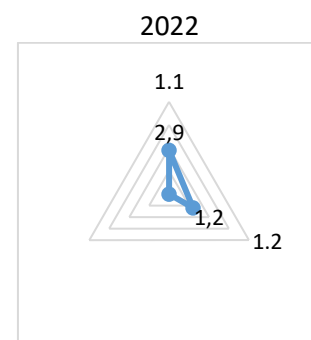
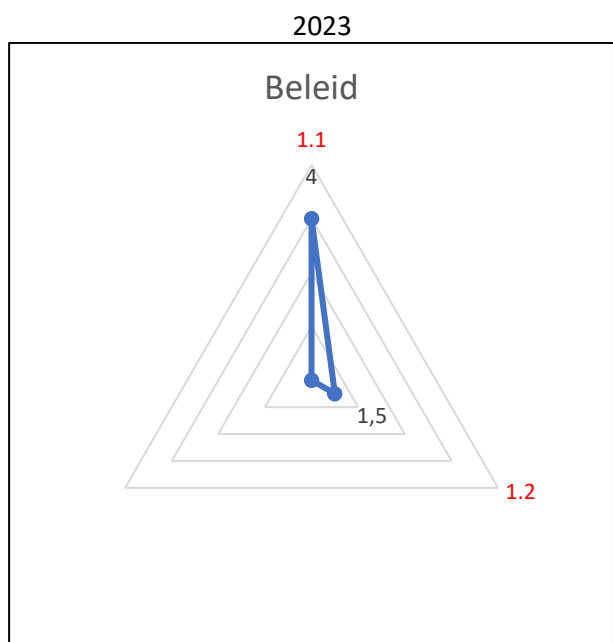


Hieronder wordt elk privacy thema toegelicht met een korte beschrijving van het thema, de resultaten uit het borgingsdocument AVG, de beschrijving van de activiteiten in 2023 en de aandachtspunten voor 2024 om een hoger niveau te bereiken. Elk thema bevat een spindiagram die de status van de implementatie van de privacy maatregelen weergeeft per eind 2023. Ter vergelijking zijn de spindiagrammen uit het vorige jaarrapport toegevoegd waarbij de dit jaar behaalde resultaten beter zichtbaar worden.

## 2 Privacy binnen de gemeente Hillegom

### 2.1 Het beleid

Het door de AVG verplicht 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 de verantwoordelijkheden binnen de organisatie zijn benoemd, belegd en vastgelegd.



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

#### Beschrijving activiteiten 2023

In 2022 is het Gegevensbeschermingsplan 2023-2025 opgesteld. Hierin is ook de ambitie voor privacy opgenomen. In het hiervan afgeleide jaarplan Gegevensbescherming 2023 zijn doelstellingen met betrekking tot het opstellen van Strategisch beleid voor Privacy en Informatieveiligheid opgesteld. Dit beleid is in 2023 opgesteld én vastgesteld door de HLT directie en het HLT Bestuur en wacht op de goedkeuring van de Colleges. Daarnaast is het Tactische Beleid Privacy en Informatieveiligheid in concept gereed en is er een start gemaakt met het opstellen van het PIV Handboek.

Begin 2023 zijn de rollen en verantwoordelijkheden van de privacy en informatieveiligheid functionarissen op organisatorisch niveau beter belegd. De Chief Information Officer (CISO) en de Functionaris Gegevensbescherming (FG) zijn toegevoegd aan het Audit en Control team en de Privacy Officers (PO) en de Information Security Officers (ISO en TISO) zijn ondergebracht in de I&A organisatie. Zo is er een eerste start gemaakt met de implementatie van het Three Lines of Management model.



## Aandachtspunten voor 2024

### - Actualiseren beleid en opstellen nieuw beleid

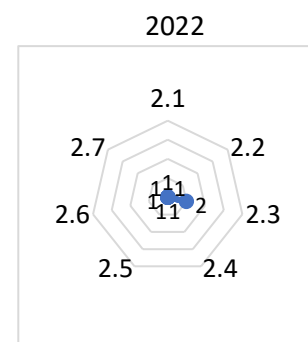
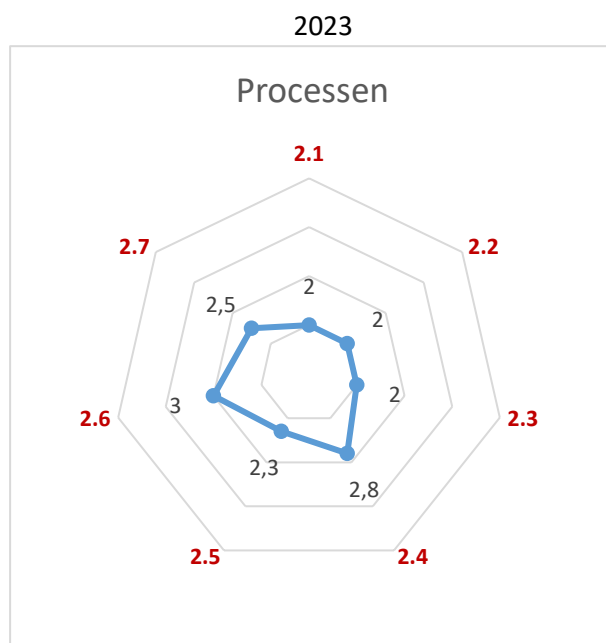
Het Tactische Privacy en Informatieveiligheidsbeleid voor alle vier organisaties laten vaststellen, prioriteiten voor implementatie bepalen, doelstellingen acties opnemen in het jaarplan en dit bewaken.

### - 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 of bij de verwerking van politiegegevens die vallen onder de Wet politiegegevens. Dit zal samen met de PIV-vertegenwoordigers van de domeinen worden geïnventariseerd.

## 2.2 Processen

De verwerkingen van persoonsgegevens door HLTsamen 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 door middel van registratie in het Register van Verwerkingen. Daarnaast is HLTsamen conform de AVG en de DPIA-lijst van de Autoriteit Persoonsgegevens 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.
- 2.7 Sancties in wetgeving en contracten en contractuele eisen over de bescherming van persoonsgegevens zijn bekend.

## Beschrijving activiteiten 2023

In 2023 is in het jaarplan een plan van aanpak voor de uitvoering van DPIA's vastgesteld en is actief aan de slag gegaan met de uitvoering hiervan. De doelstelling om gedurende 2023 acht DPIA's uitgevoerd te hebben is ruimschoots gehaald. Naast dit kwantitatieve resultaat heeft het ook bijgedragen om de "koudwatervrees" in de organisatie meer weg te nemen. Hierdoor is het bewustzijn op het inschatten van (privacy) risico's in positieve zin toegenomen en krijgt de organisatie beter zicht op haar grootste privacy risico's.

	2023	2022
Aantal uitgevoerde en geaccordeerde DPIA's	10	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. Zoals het (vooraf) verplicht invullen van de privacy checklist bij nieuwe én bestaande verwerkingen, een aanbesteding, een nieuwe business case of andere verwerkingen als hier persoonsgegevens bij betrokken zijn.

Tevens is een start gemaakt met het invullen van het handboek PIV waarin protocollen en richtlijnen zijn vastgelegd. Dit is een doorlopende activiteit.

## Aandachtspunten voor 2024

### - Uitvoeren en managen van DPIA's

Het uitvoeren van DPIA's is 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 en de te nemen maatregelen worden uitgevoerd. Ook hebben DPIA's een beperkte houdbaarheid en dienen periodiek beoordeeld te worden of aanpassing nodig is en zullen in een PDCA-cyclus meegenomen moeten worden. Er zal een methodiek of systematiek moeten worden ingevoerd om de proceseigenaren periodiek checks te laten uitvoeren op het actueel maken/houden van de risico's, en zodoende de PCDA cyclus op de DPIA's te borgen.

### - Actualisatie van het register van verwerkingen

De verantwoordelijkheid voor het onderhoud en de actualisatie van (onderdelen van) het register ligt nu nog 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 2024 meer aandacht aan gegeven te worden. Het register van verwerkingen is in 2023 weliswaar op een aantal punten geactualiseerd, maar ook dit is geen cyclische 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. Geadviseerd wordt om een centrale applicatie te implementeren waarin de PDCA cyclus kan worden beheerd. Acties kunnen dan het liefst automatisch aan de verantwoordelijken worden toebedeeld en het register van verwerkingen kan daarmee openbaar worden gemaakt.

### - Borgen handboek PIV

In het handboek PIV worden protocollen en/of een instructies opgesteld.

Dit zijn de beschrijvingen van de protocollen en (interne) richtlijnen hoe de privacy en informatiebeveiliging gerelateerde onderwerpen dienen te worden uitgevoerd door de organisatie. In 2024 zal hier verder aan gewerkt worden.

### - Tijdig verwijderen of anonimiseren van persoonsgegevens

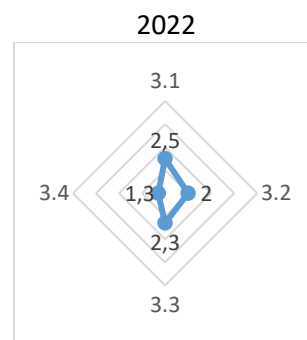
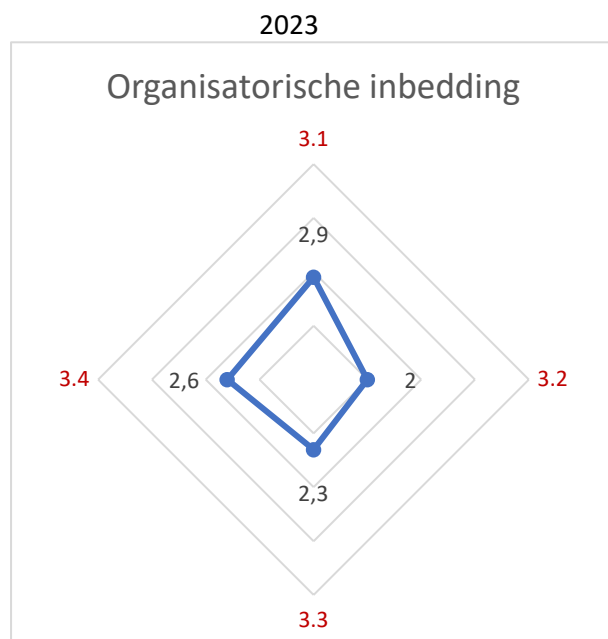
Het verwijderen of anonimiseren van persoonsgegevens is een belangrijk punt van aandacht. In 2022 is een applicatie hiervoor in gebruik genomen. De ervaringen opgedaan in 2023 zijn positief. Onduidelijk is of het vernietigen van papieren en digitale informatie overal tijdig gebeurt. Het niet tijdig vernietigen van persoonsgegevens is in strijd met de AVG en andere specifieke wetgeving. Met name de individuele opslag van persoonsgegevens bij medewerkers (e-mailinformatie en documenten) is niet duidelijk. Geadviseerd wordt te onderzoeken hoe met de overgang naar de Cloudomgeving (Samen digitaal transparant-project) digitale informatieopslag conform de AVG en Archiefwet vernietigd kan worden.

#### - **Procesbeschrijvingen opstellen**

Het ontbreekt in de meeste gevallen aan duidelijke en complete procesbeschrijvingen. Dit leidt er toe dat niet kan worden aangetoond hoe de Verwerkingen zijn ingericht. Hierdoor zijn de risico's moeilijker in kaart te brengen, is er geen inzicht welke partijen erbij betrokken zijn, welke persoonsgegevens hiervoor noodzakelijk zijn, welke applicaties worden gebruikt en wie benaderd moet worden in geval van (acute) calamiteiten. Het opstellen en vastleggen van procesbeschrijvingen is de verantwoordelijkheid van de proceseigenaar en dient meegenomen te worden de PDCA-cyclus.

## 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 creëren van bewustzijn.



- 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.

## Beschrijving activiteiten 2023

#### - **Samenstelling PIV Team**

Naast de integrale aanpak vanuit privacy en informatieveiligheid is de personele bezetting steeds meer op orde gekomen. Naast de al aangestelde FG, CISO en PO was vanaf december 2022 een vaste Information Security Officer (ISO) aangesteld. Hij had als taak om de uitvoerende taken, die tot dan

toe door de CISO werden gedaan, over te nemen. Echter, er zijn in het aanstellingsproces van deze ISO fouten gemaakt. Gedurende het jaar bleek dat de functie geen kostenplaats had en er dus geen financiële middelen voor waren gereserveerd. De ISO heeft HLTsamen per augustus 2023 helaas weer moeten verlaten.

In april 2023 is het Privacy team uitgebreid met een tweede Privacy Officer. Deze PO heeft de interne overstap gemaakt van I&A Functioneel beheer naar het PIV team. Door het wegvallen van de ISO taak heeft deze PO ook een aantal ISO taken vervuld, zoals het leveren van ondersteuning ten behoeve van de ENSIA audit.

In Augustus 2023 is de CISO met zwangerschapsverlof gegaan. Dit duurde tot eind December 2023. Als vervangende CISO is een externe kracht ingeschakeld die slechts een dag per week beschikbaar was. De inzet van de TISO heeft zich in 2023 beter kunnen ontplooiën. De oude en voorgaande werkzaamheden zijn voor het grootste gedeelte overgedragen en de TISO heeft zich meer kunnen richten op de technische kant van de informatiebeveiliging.

Er zijn grote stappen gezet om de bewustwording op PIV binnen de organisatie te verbeteren, wat geresulteerd heeft in het aanmelden van 6 collega's voor de rol van PIV vertegenwoordiger binnen hun afdeling. De PIV vertegenwoordiger zal de 1<sup>e</sup> lijns rol invullen, maar dient nog wel verder uitgewerkt te worden in taakstelling en opleidingstraject.

Acties die door het PIV team zijn georganiseerd waren de escaperoom/Cybertruck in Januari met een actieve deelname van meer dan 100 collega's, de Paasactie waar aan elke medewerker een paar paaseitjes van het PIV team werden aangeboden, het nano-leerprogramma Sir Askalot, met een deelname van meer dan 70%, een actieve positie op het HLTplein met adviezen (over o.a. Aliexpress, Tiktok, ChatGPT), het promoten van de noodzaak van DPIA's middels een filmpje en talloze kleinere initiatieven en interventies.

In november 2023 heeft de FG aangekondigd om per 1 Februari 2024 met zijn functie te zullen stoppen. De sollicitatie procedure voor een nieuwe FG is vrijwel direct daarna gestart. Er is ondertussen een externe FG ingehuurd die deze functie waarneemt totdat er een nieuwe FG is aangesteld.

Er kan duidelijk gesteld worden dat 2023 qua teambezetting een roerig jaar is geweest. Van de ambitieuze verwachtingen die aan het begin van het jaar waren opgesteld zijn ondanks de onderbezetting de meeste zaken uitgevoerd. Mede het inzetten van een externe projectmanager die de acties nauwgezet heeft gemanaged heeft hier aan bijgedragen.

#### - **Plek in de organisatie**

Per 1 maart 2023 zijn de 2<sup>e</sup> lijns en 3<sup>e</sup> lijns rollen gescheiden ondergebracht in de organisatie. Daar waar tot 2023 alle functies bij Juridische Zaken waren ondergebracht zijn de 3<sup>e</sup> lijns rollen van CISO en FG nu formeel ondergebracht bij Audit & Control. De 2<sup>e</sup> lijns rollen van de twee PO's, de ISO en TISO zijn ondergebracht bij de I&A organisatie.

### **Aandachtspunten 2024**

#### - **Ontwikkelen en inzetten vertegenwoordigers gegevensbescherming**

Om verdere stappen te kunnen maken en gegevensbescherming beter te kunnen borgen in de organisatie is het gewenst dat de organisatie eenheden hun rol op privacy en informatiebeveiliging gebied pakken. Het wervingsprogramma voor PIV vertegenwoordigers heeft al geresulteerd dat een zestal geïnteresseerden zich hebben aangemeld voor deze rol. De rollen en taken zullen verder uitgewerkt moeten worden om duidelijk de afbakening tussen 1<sup>e</sup> lijns taken en 2<sup>e</sup> lijns taken te kunnen onderscheiden. Dit zal in een glijdende schaal gedurende het jaar kunnen worden geïmplementeerd. Dit houdt in dat er een introductie/opleiding traject zal worden opgesteld en uitgevoerd. Dit zou ook

moeten leiden tot een uitbreiding van het aantal vertegenwoordigers zodat elk team een PIV vertegenwoordiger heeft.

- **(her)Aanstellen van de ISO-functie**

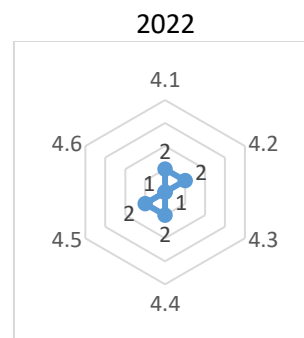
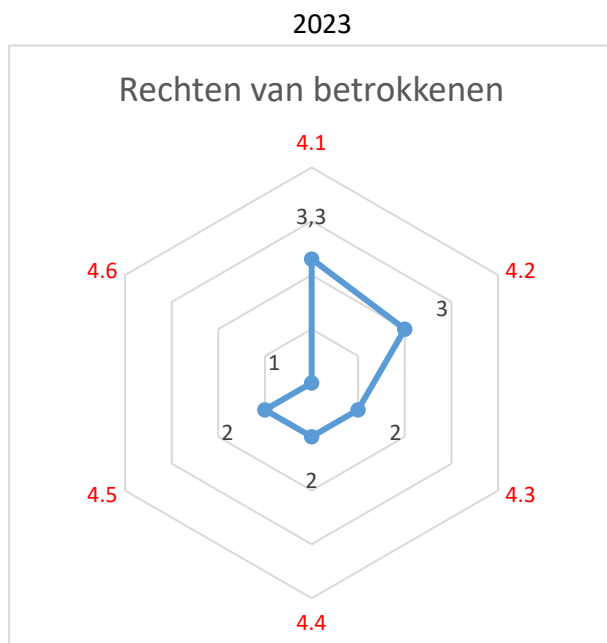
Door het vertrek van de ISO zal zo spoedig mogelijk deze functie weer moeten worden ingevuld. Daarmee vervallen een aantal ISO gerelateerde taken die tijdelijk aan de Privacy Officer zijn toebedeeld en kan hij zich weer volledig richten op zijn Privacy taken. Om het gestelde ambitieniveau te kunnen behalen is de rol van ISO onontbeerlijk.

- **Toewijzen van Proceseigenaren**

Binnen het kader van de invoering van het 3 lines of management zouden proceseigenaren aangesteld moeten worden die verantwoordelijk worden gehouden om de aan zijn/haar toebedeelde processen rechtmatig te laten verlopen en dit aan te tonen. Een belangrijk onderdeel van deze verantwoordelijkheid is het op de juiste manier van verwerken van persoonsgegevens en het bewaken van de processen binnen de wettelijke verplichtingen en de gestelde richtlijnen. De proceseigenaren zijn en stellen zich verantwoordelijk op bij het beantwoorden van vragen omtrent het proces, het identificeren en mitigeren van risico's, de tijdige uitvoering van de te nemen maatregelen, het anticiperen en identificeren van acties op veranderingen in het proces of aangepaste regelgeving, het meewerken dan wel leidinggeven aan onderzoeken als gevolg van incidenten, volledige medewerking openheid en transparantie bij de uitvoering van audits.

## 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-transparantieplichtingen.
- 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.

### Beschrijving activiteiten 2023

Binnen HLTsamen is het proces verder uitgewerkt om de rechten van betrokkenen te faciliteren. De procedures en het proces dienen nog wel verder uitgewerkt te worden en formeel te worden vastgesteld en opgenomen in het PIV Handboek

In de privacyverklaring geeft HLTsamen aan hoe en waar betrokkenen verzoeken kunnen indienen. Verzoeken kunnen zowel schriftelijk als elektronisch via een e-formulier worden ingediend.

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, een WOO-verzoek of een klacht indient tegen de organisatie trekt de PO in overleg met de betrokkene, samen met de WOO- en klachtencoördinator op. Dit proces is nog niet formeel vastgesteld. In 2023 zijn er in totaal 12 AVG-verzoeken ingediend bij de HLTsamen gemeenten.

	2023	2022
Verzoek tot inzage	8	8
Wissen van persoonsgegevens	1	0
Verzoek tot rectificatie	3	0
<b>Totaal</b>	<b>12</b>	<b>8</b>

### Aandachtspunten voor 2024

#### - Verbeteren intern proces van afhandeling van verzoeken

Binnen HLTsamen zijn processen ingericht om de rechten van betrokkenen te faciliteren. 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 nog aan te stellen PIV-vertegenwoordigers spelen hier een belangrijke rol in. Extra aandacht is hierbij gewenst op misbruik van de uitoefening van de AVG-rechten door een betrokkene.

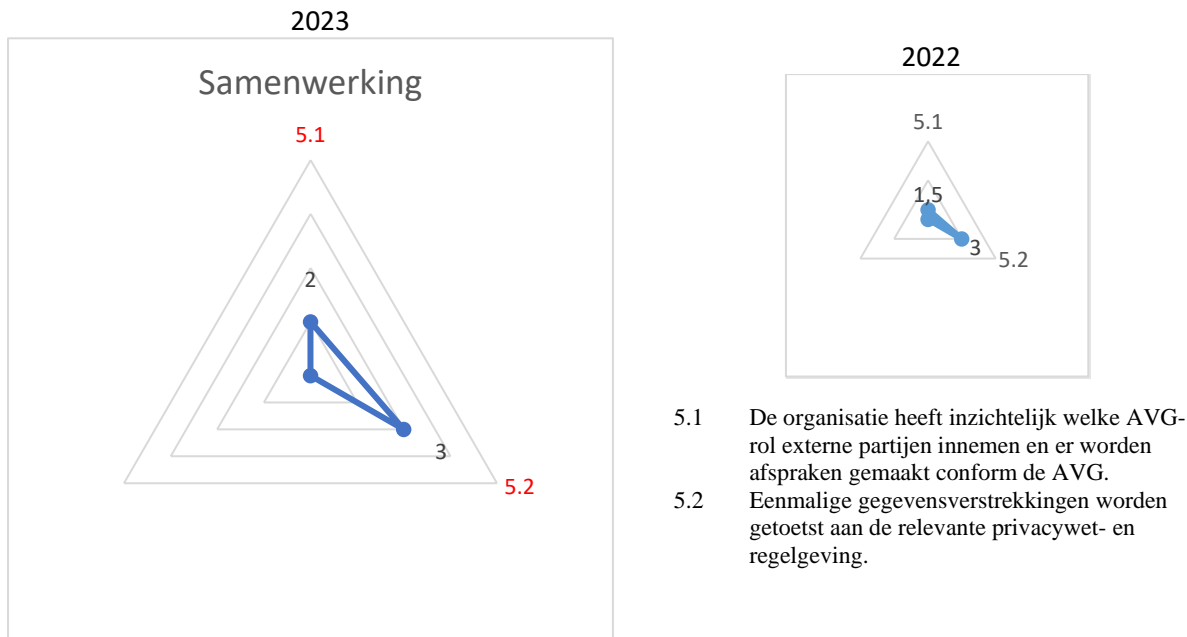
#### - Specifiekere privacyverklaringen

HLTsamen en de drie gemeenten hanteren nu één algemene privacyverklaring om aan betrokkenen uit te leggen waarvoor hun persoonsgegevens (kunnen) worden gebruikt. Dit is voor veel situaties te algemeen en te ruim beschreven. Betrokkenen moeten op een correcte manier geïnformeerd worden voor welk doel welke persoonsgegevens aan wie en voor hoelang, feitelijk worden verwerkt. Privacy verklaringen zullen in combinatie met een openbaar verwerkingsregister meer op maat moeten worden beschreven naar de werkelijke op feiten gebaseerde verwerkingen. Aangeboden op de desbetreffende websites op een eenvoudige en voor eenieder begrijpelijke taal.

Gezien de verdere internationalisering van de bewoners in de gemeenten zou de keuze moeten worden geboden om de privacyverklaring in een aantal gangbare vertalingen aan te bieden.

## 2.5 Samenwerking

HLTsamen 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.



### Beschrijving activiteiten 2023

HLTsamen dient dan ook afspraken te maken met deze andere partijen. HLTsamen heeft deels inzichtelijk welke AVG-rol externe partijen innemen (verwerkers, gezamenlijke en zelfstandige verwerkingsverantwoordelijken). Er wordt gebruik gemaakt van de standaard verwerkersovereenkomst van de VNG. De bewustwording onder medewerkers om bij gegevensverwerkingen afspraken te maken groeit. In het inkoopproces middels het STRAPP wordt het PIV team op tijd ingeschakeld om leveranciers en producten op PIV aspecten te beoordelen. In 2023 zijn er diverse nieuwe verwerkersovereenkomsten met derde partijen afgesloten en opgenomen in het JOIN zaaksysteem.

### Aandachtspunten voor 2024

#### - 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 afdoende afspraken worden gemaakt conform de AVG. Geadviseerd wordt om dit beter in te bedden in de organisatie.

Door de soms complexe samenwerking van partijen en is het overigens niet altijd even inzichtelijk welke AVG-rol een externe partij inneemt. De Informatiebeveiligingsdienst heeft hierover 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 en te begeleiden in de te maken afspraken en

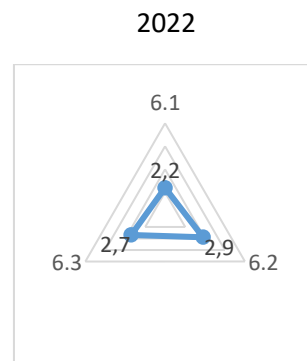
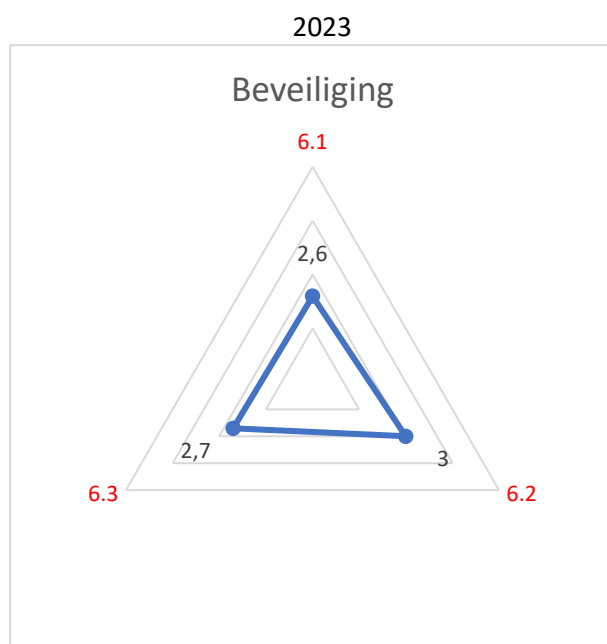
op te stellen contracten en verwerkersovereenkomsten. Hier zouden de PIV vertegenwoordigers in samenspraak met de PO een rol in kunnen spelen.

#### - Archiveren verwerkersovereenkomsten

Meerdere malen is gebleken dat bestaande verwerkersovereenkomsten niet in het zaakstelsel te vinden zijn. Deels omdat ze überhaupt niet waren opgenomen deels omdat het document niet herkenbaar als verwerkersovereenkomst opgeslagen was. Er is weliswaar een systematiek ontwikkeld voor het opslaan van contracten in het zaakstelsel maar die wordt onvoldoende nageleefd. Bestaande en nieuw op te stellen verwerkersovereenkomsten dienen op een centrale manier inzichtelijk te zijn voor proceseigenaren, contractmanagement en PIV team. Een uitgebreide inventarisatie naar alle derde partijen en GR's en de welke noodzakelijke afspraken er gemaakt zijn of zouden moeten zijn dienen op een centrale en gestructureerde manier te worden gearhiveerd.

## 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.

### Beschrijving activiteiten 2023

In de laatste helft van 2023 heeft het onderzoek plaatsgevonden naar de mogelijkheid van classificeren van data. Het project Samen Digitaal Transparant zal in de toekomst het beleid schrijven rondom dataclassificatie. Onderzocht is om de Microsoft DLP software hiervoor in te zetten. Het hoofddoel is om dataverlies te voorkomen en de naleving van privacy- en beveiligingsregels te handhaven.



Aanbevelingen hoe deze software kan worden ingezet worden opgesteld. In mei is een gecontroleerde actie uitgevoerd waarbij iedere HLT medewerker een phishing-email kreeg. De resultaten waren bemoedigend en heeft aangezet tot hogere bewustwording bij het afhandelen van vreemde e-mails. Bovendien zorgt nieuw ingezette software ervoor dat ontvangers worden gewaarschuwd als er een afwijkende email wordt afgeleverd.

De processen en procedures om het op een eenvoudige manier mogelijk te maken om beveiligingsincidenten en datalekken te melden is sterk verbeterd. Het melden is nu mogelijk door middel van een “tegel” met een duidelijke instructie in TopDesk. De gehele afhandeling en administratie van meldingen wordt tevens in TopDesk bijgehouden. In 2023 was er een sterke toename van het aantal gemelde incidenten en datalekmeldingen. Dit is met redelijke zekerheid niet te wijten aan dat er werkelijk meer incidenten hebben plaatsgevonden, maar dat de bewustwording bij de medewerkers om te moeten melden is toegenomen en het voor iedereen eenvoudiger is gemaakt om een melding te kunnen doen. HLTsamen streeft een open cultuur na waarin datalekken intern en zonder enige impact voor de melder gemeld kunnen worden.

In totaal zijn er 48 informatiebeveiligingsincident meldingen via TopDesk geplaatst. Daarvan zijn 21 als datalek zijn geclassificeerd. Bij een ernstig datalek moet HLTsamen het datalek ook aan de Autoriteit Persoonsgegevens melden. In twee gevallen is een voorlopige melding bij de AP ingediend. Dit was uit voorzorg gedaan om aan de wettelijke termijn van 72 uur te voldoen, terwijl er nog geen uitsluitel was dat er werkelijk sprake was van een datalek. Na afronding van de onderzoeken bleek gelukkig dat de vertrouwelijkheid van persoonsgegevens niet waren geschonden en zijn beide meldingen weer ingetrokken.

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:

	2023 (2022)	2023 (2022)
Oorzaak	Meldingen aan AP	Interne meldingen
Menselijke oorzaak	0 (1)	19 (6)
Technische oorzaak	0 (0)	2 (1)
Organisatie	0 (0)	0 (0)
<b>Totaal aantal datalekken</b>	<b>21 (8)</b>	

## Aandachtspunten voor 2024

### - 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. 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.

### - Proceseigenaren en PIV vertegenwoordigers

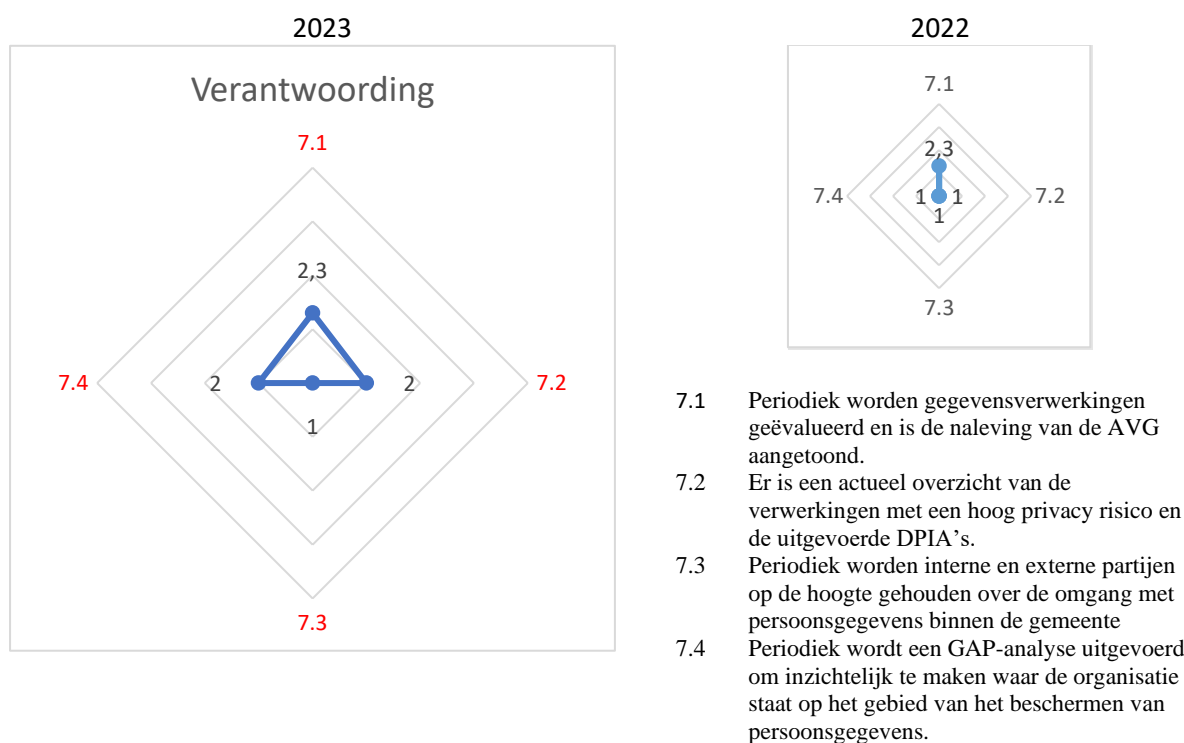
Het wijzen op de verantwoordelijkheid van proceseigenaren met betrekking tot privacy en informatieveiligheid binnen hun eigen processen moet door middel van verdere bewustwording worden geïntensiveerd. Het daarbij identificeren van risico's en het melden van incidenten behoort tevens tot hun verantwoordelijkheid. Door de werving en on-boarding van de PIV vertegenwoordigers zal hier een stimulans aan worden gegeven.

## - Voorbereiding op de NIS2

Gedurende 2024 zal de nieuwe Europese norm voor informatiebeveiliging van kracht worden De NIS2. Een van de uitbreidingen ten opzichte van de huidige BIO is de verplichting om verantwoording kunnen afleggen. Daarvoor is een ISMS (Information Security Management System) een vereiste. In het onderzoek en keuze naar het juiste platform dient de verantwoordingverplichtingen die de AVG heeft ook te worden meegenomen zodat er een systeem gebruikt kan worden voor alle PIV verantwoording verplichtingen.

## 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 bestuur van HLTsamen aan het College als eindverantwoordelijke 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.



### Beschrijving activiteiten in 2023

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 HLTsamen aan de bestuursorganen. Het openbaar maken van de jaarrapportage draagt bij aan de verantwoordingsplicht van het college van B&W als eindverantwoordelijke. Door de openbare publicatie van het jaarrapport is het college 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). De samenwerking tussen privacy en informatiebeveiliging is in 2023 verder geïntensiveerd. De rollen en verantwoordelijkheden van de

diverse PIV functies zijn beter ingebed in de organisatie (A&C en I&A) en wordt verantwoording binnen die organisatie onderdelen afgelegd. Hierdoor wordt beter zicht op planning en inzet mogelijk.

## **Aandachtspunten 2024**

### **- Blijf zicht houden op risicovolle processen**

Mede door het ontbreken van een gestructureerde risicomanagement aanpak maakt gegevensbescherming nog geen structureel onderdeel uit van de bedrijfsvoering. Alhoewel een begin is gemaakt met de organisatie bewuster maken van risicomanagement zullen in 2024 keuzes moeten worden gemaakt om tot een organisatie brede opzet van risicomanagement te komen. Door alle teams aan het risicospel te laten deelnemen wordt de bewustwording en de onbekendheid met risico's zeker vergroot. Het is aan te bevelen om die aandacht voor het onderwerp vast te houden en de team(manager)s te betrekken bij het bepalen en implementeren van de nog te kiezen risicomanagement methodiek

### **- PDCA**

Het blijven analyseren van de gemeentelijke processen en het vinden en mitigeren van de risico's in processen zorgen er voor dat HLTsamen gegevensbescherming structureel in de organisatie inbedt en actief bouwt aan het fundament: een betrouwbare overheid. Tot op heden is er geen PDCA-cyclus (Plan-Do-Check-Act) opgesteld voor de processen. In 2024 zou met de komst van de PIV-vertegenwoordigers hiermee een start gemaakt kunnen worden. Het bijhouden van de PDCA-cyclus zal per proces verschillen afhankelijk van de risico's van het proces. Vanwege het grote aantal processen in de organisatie zal het bijhouden van de PDCA-cyclus (het tijdstip, de soort actie en de actiehouders) omvangrijk zijn en zal moeten worden geautomatiseerd en geïnitieerd in bijvoorbeeld het in te voeren ISMS.

### **- Verantwoording op Teamniveau**

Op dit moment is de ambitie gesteld om als gehele organisatie een volwassenheidsniveau voor de privacy te behalen. Dit is een gemiddelde score over alle afdelingen en teams, zodat de minder scorende afdelingen niet direct zichtbaar worden en het voor hen voelbaar is. Gedacht kan worden om een (vereenvoudigd) borgingsproduct op te stellen dat per team of per PIV-vertegenwoordiger wordt bijgehouden. Zo wordt een beter overzicht verkregen van de uitdagingen en successen die zijn behaald. Bestuurders kunnen de status van het niveau van gegevensbescherming per team volgen en, waar nodig, bijsturen wanneer de teams hierover rapporteren.

### 3 Conclusie

In 2023 zijn er goede stappen zijn gezet om gegevensbescherming (privacy en informatieveiligheid) verder te implementeren in de organisatie, in de systemen en in de processen.

Gebruikmakend van dezelfde meetlat als vorig jaar, middels het VNG Borgingproduct 2.0, kan geconcludeerd worden dat de organisatie van het vastgestelde volwassenheidsniveau 1,8 van eind 2022 een sprong heeft gemaakt naar een volwassenheidsniveau 2,2. De meeste winst is behaald door het opstellen van beleid en het beter beschrijven van de PIV-processen en het consequenter uitvoeren van risicoanalyses door middel van DPIA's.

Er is nieuw langetermijnbeleid opgesteld in het Strategisch beleid Privacy en Informatieveiligheid plan. In het Tactisch beleid is dit verder uitgewerkt en uiteindelijk vertaald zal worden naar gedetailleerde werkafspraken in proces- en procedure beschrijvingen. Daarmee zal een solide basis worden gelegd om reproduceerbaar en controleerbaar de taken en verplichtingen te borgen die de AVG en BIO/NIS 2 vereisen. Daarnaast geeft het duidelijkheid aan de organisatie hoe de taken worden uitgevoerd en draagt het bij aan een efficiëntere uitvoering van de gemeentelijke taken.

2023 is een jaar geweest dat de gehele organisatie veel bewuster is geworden. De grote deelname aan Sir Askalot, de hoeveelheid en de type meldingen van incidenten en de toename in adviesvragen getuigen hiervan. Van onbewust onbekwaam naar bewust onbekwaam is een grote sprong! De volgende stap naar bewust bekwaam, (de ambitie om volwassenheidsniveau 3 te bereiken) zal een uitdagend traject zijn waarbij de betrokkenheid en inzet van de gehele organisatie nodig is. Daarbij is het van belang dat de huidige PIV-organisatie solide blijft acteren, hun taken, hun inzet en noodzaak door directie en bestuur ondersteund blijft en de betrokkenheid van alle medewerkers helpt stimuleren.