JAARVERSLAG 2025

FUNCTIONARIS GEGEVENSBESCHERMING

GEMEENTE HEUSDEN

Ton Donders

Functionaris Gegevensbescherming

19 mei 2025

Inhoudsopgave

Kijkend naar de norm is op alle thema's blijvend actie nodig. De verbetering ten opzichte van 2024 is deels het gevolg van de nieuwe scoring in het borgingsdocument. In 2026 zal moeten blijken of de positieve lijn kan worden doorgezet.

Samenvatting

In het jaar 2025 is afgesproken om de achterstand op het uitvoeren van DPIA's met een concrete doelstelling aan het eind van 2026 deels in te lopen. Het is te vroeg om conclusies te trekken, maar het inlopen van de achterstand wordt wel vooruitgeschoven. Aandacht van het management hiervoor blijft een vereiste.

AVG Thema:		2025
Borging	*Score norm*	
Beleid	*91%*	
Processen	*79%*	
Organisatorische inbedding	*91%*	
Rechten van betrokkenen	*88%*	
Samenwerking	*77%*	
Gegevensbescherming	*91%*	
Verantwoording	*86%*	

De beschikbare formatie in relatie tot de dagelijkse werkzaamheden en de begeleiding van de in te lopen achterstand blijft een punt van aandacht.

In het jaar 2026 wordt een managementsysteem ingericht waarin risico's in gezamenlijkheid worden beoordeeld en waarmee toetsing plaatsvindt.

De score die is opgenomen komt uit het borgingsdocument. Hierin zijn de maatregelen opgenomen waarvan de Informatiebeveiligingsdienst (IBD) vindt dat deze geïmplementeerd moeten zijn om te kunnen voldoen aan de AVG. Er wordt gewerkt aan het verbeteren van deze scores waarbij zoveel mogelijk risico gestuurd prioriteiten worden gesteld.

Inleiding

De Functionaris voor de Gegevensbescherming (FG) is de intern toezichthouder op de verwerking van persoonsgegevens. Dit is het jaarverslag over 2025 en bevat een terugblik op dat kalenderjaar, inzicht in hoe we ons verhouden ten opzichte van de landelijk bepaalde minimumnormen en aanbevelingen voor verbetering.

Binnen de gemeente Heusden is de FG aangesteld door het college, niet door de andere zelfstandige bestuursorganen (raad, burgemeester en rekenkamer). Omdat alle bestuursorganen door dezelfde organisatie ondersteund worden, wordt er indirect toch toezicht gehouden voor al deze bestuursorganen. Dit is echter niet geformaliseerd. Eerder is al geconcludeerd dat een afzonderlijk jaarverslag voor de gemeenteraad weinig tot geen toegevoegde waarde heeft. In plaats daarvan wordt in één jaarverslag gerapporteerd.

Er is gekozen voor één FG voor het interne toezicht op de algemene privacy (op basis van de AVG) en de verwerking van politiegegevens (op basis van de Wpg). Dit jaarverslag richt zich op beide onderdelen. Aangezien de wetten naar hun aard verschillend zijn is het verslag in twee verschillende onderdelen verdeeld.

De FG-rol is belegd bij de Concerncontroller. Om invulling te kunnen geven aan de beide FG-rollen in combinatie met andere werkzaamheden zijn afspraken gemaakt over de omvang en invulling van de werkzaamheden. De focus ligt op (intern) toezicht, advies bij risicoanalyses gericht op gegevensverwerking en aanspreekpunt voor inwoners en de Autoriteit Persoonsgegevens. Adviseren en ondersteunen van de organisatie is primair belegd bij de Privacy Officer. Door interne doorstroom is de FG-rol gedurende de eerste maanden van 2025 gecombineerd met een andere functie. Per april 2025 is de nieuwe Concerncontroller benoemd als FG. De Privacy Officer is in september 2025 extern gegaan en na een korte interim-periode eind 2025 is begin 2026 een nieuwe Privacy Officer gestart.

Gedurende het kalenderjaar is er geen contact geweest met de Autoriteit Persoonsgegevens, anders dan een viertal meldingen van datalekken. Zowel vanuit de kant van de gemeente als van de Autoriteit Persoonsgegevens is verder geen aanleiding geweest voor contact.

AVG Borgingsproduct

In het jaarverslag wordt al enkele jaren gebruik gemaakt van het borgingsproduct van de Informatiebeveiligingsdienst (IBD). Op basis hiervan kon het volwassenheidsniveau worden afgeleid. Hiervoor is het nieuwe borgingsproduct (versie 3.1, 2025) gebruikt. Dit bevat uitsluitend zaken waarvan de IBD ze als noodzakelijk beschouwt om aan de AVG te voldoen. Het uitgangspunt is dan ook dat gemeenten aan alle criteria voldoen.

In de samenvatting is te zien hoe de gemeente Heusden zichzelf scoort per thema. Het is geen verrassing dat er geen 100% score is. Wat opvalt is dat er forse positieve afwijkingen zichtbaar zijn ten opzichte van 2024. Dit is deels verklaarbaar door genomen maatregelen en verbeteracties, maar ook doordat voor een groot deel van de antwoorden de mogelijkheden van een drietrapsscore (ja, deels, nee) naar een vijftrapsscore (geen enkel geval, enkele gevallen, ongeveer de helft van de gevallen, meeste gevallen, alle gevallen) zijn gegaan. In het jaarverslag wordt per onderdeel een duiding van de resultaten gegeven en zijn er aanbevelingen geformuleerd voor de organisatie. Het borgingsproduct zal gebruikt blijven worden voor de monitoring van de ontwikkelingen.

Leeswijzer

Dit jaarverslag bestaat uit 2 onderdelen, deel A over de AVG en deel B over de Wpg. In het onderdeel over de AVG wordt per thema uit het borgingsproduct teruggekeken op 2025, een duiding gegeven bij de score van het borgingsproduct en met aanbevelingen vooruitgekeken naar 2026 (en mogelijk verder). In het onderdeel van de Wpg ligt de focus op de opvolging van de auditverplichting en het interne toezichtsplan.

Deel A: AVG

Jaarverslag over het intern toezicht op privacy in het algemeen

1. Beleid

Het beleid geeft richting en laat zien dat de gemeente de privacy waarborgt, beschermt en handhaaft. Met de privacyverklaring laat de gemeente zien hoe dit gebeurt. Samen vormen ze het kader voor hoe de gemeente omgaat met persoonsgegevens.

1.1 Terugblik op 2025

2025 kenmerkt zich vooral door personele wisselingen van functionarissen belast met advisering en toezicht over en op privacy gerelateerde thema's. De overgang van de oude naar de nieuwe functionarissen heeft gelukkig niet geleid tot een stap terug in wat al bereikt was. Sterker nog, er is met nieuwe energie voortgeborduurd op de ingeslagen weg met de geplande en reeds ingezette verbeteracties en maatregelen. In een intensivering van de samenwerking tussen de Privacy Officer, de CISO (Chief Information Security Officer) en de FG wordt veel bespreekbaar gemaakt en lijkt het steeds beter te lukken om de thema's privacy en informatiebeveiliging standaard een gesprekspunt te laten zijn. Dit is terug te zien in de aansluiting bij de opschalingsprincipes volgens GRIP[1], wanneer sprake is van een beveiligingsincident - zo'n incident kan leiden tot een datalek waardoor het ook voor privacy relevant is - en de betrokkenheid bij het I-team[2].

1.2 Basisniveau privacy volgens de IBD

Het borgingsproduct dat is ingevuld door de Privacy Officer, de CISO en de Concerncontroller laat de volgende scores zien:

1.	Beleid	91%
1.1	Beleid vaststellen	100%
1.2	Privacybeleid	94%
1.3	Verantwoordelijkheden	83%

Deze scores zijn iets hoger dan in het voorgaande jaar. Dit lijkt voornamelijk het gevolg van de verruiming (explicitering) van de scoremogelijkheden op de vraagstelling in het borgingsproduct. Alleen op het beleid vaststellen wordt een 100% score gehaald. Het beschikbare beleid is vastgesteld en terug te vinden op een logische plek. Er is overkoepelend privacy beleid en daarnaast voor politiegegevens (Wpg) en burgerzaken domeinspecifiek privacybeleid.

1.3 Aanbevelingen

Blijf aandacht geven aan privacyrisico's en zorg ervoor dat iedereen hier steeds bewust afstemming over zoekt. Op die wijze wordt inzichtelijk of de caseload van de Privacy Officer past bij de beschikbare tijd. Alleen dan kan helder worden of de Privacy Officer voldoende ruimte heeft om alles te doen wat tot haar takenpakket behoort. De advisering, begeleiding van de DPIA's en het aanjagen van het inhalen van de achterstand op deze DPIA's behoren tot de taken van de Privacy Officer. De DPIA's zelf zijn de verantwoordelijkheid van het lijnmanagement. Zorg dat zij dit oppakken.

[1] GRIP = Gecoördineerde Regionale Incidentbestrijdingsprocedure, de werkwijze waarmee Nederlandse hulpverleningsdiensten bepalen hoe het werk gecoördineerd moet worden bij incidenten.
[2] Een samenwerking rondom informatiebeheer met betrokkenen vanuit de clusters documentaire informatievoorziening (DIV), informatie & automatisering (I&A), kwaliteitscontrol (KC), CISO en PO.

2. Processen

Verwerkingen van persoonsgegevens moeten 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. Voor inzicht in eventuele privacyrisico's en mogelijke maatregelen die getroffen kunnen of moeten worden kan gebruik gemaakt worden van een Data Protection Impact Assessment (DPIA), een instrument om gegevensverwerkingen binnen een proces in kaart te brengen. In een aantal gevallen zijn gemeenten verplicht een DPIA uit te voeren.

2.1 Terugblik op 2025

In 2025 zijn concrete afspraken gemaakt over een inhaalslag van (pre-)DPIA's. Juist omdat net als vorig jaar prioriteiten steeds weer lijken te verschuiven door de waan van alledag was het van belang hierover afspraken vast te leggen. Daar komt bij dat door de onverminderd hoge werkdruk in de organisatie en de nieuwe invulling van de rollen ook nodig maakt dat hier specifieke aandacht voor is. In die afspraken zijn de meest belangrijke (hoog prioriteit) DPIA's benoemd en is afgesproken dat die eind 2026 gereed zijn. Er wordt op gemonitord om de voortgang hiervan te bewaken.

Inmiddels is er wel in 2025 extra ervaring opgedaan, omdat een besluit tot cameratoezicht is aangegrepen om de DPIA's voor deze, en eerder ingezet cameratoezicht meteen goed te regelen.

In 2025 is zichtbaar geworden dat de Privacy Officer, ook door betere werking van het I-team, steeds vaker geconsulteerd wordt. In 2025 is ook een groot deel van de in 2024 onderhande zijnde DPIA's afgerond.

Het inzicht in de verplichte DPIA's met prioritering voor de uitvoering daarvan is dus intern vastgesteld. Daarnaast wordt de eerdere lijn voortgezet, namelijk met de bestaande capaciteit zo goed mogelijk de organisatie ondersteunen. De prioriteit ligt bij nieuwe en/of veranderende processen / gegevensverwerkingen en daarnaast moet de achterstand worden ingelopen. Dit blijft een uitdaging maar laat ook zien hoe belangrijk het is dat lijnmanagers en medewerkers hun verantwoordelijkheid nemen. Het inlopen van de achterstand vraagt echter bemoeienis en coördinatie van de Privacy Officer en binnen de bestaande capaciteit blijft deze dus lastig te realiseren.

2.2 Basisniveau privacy volgens de IBD

Het borgingsproduct dat is ingevuld door de Privacy Officer, de CISO en de Concerncontroller laat de volgende scores zien:

2.	Processen	79%
2.1	Werkprocessen	71%
2.2	Verwerkingsregister	70%
2.3	Pre-DPIA's	83%
2.4	DPIA's	81%
2.5	Bewaar- en vernietigingsbeleid	94%

Ten opzichte van vorig jaar is dit thema verbeterd. Toch is hier nog veel ruimte voor verbetering. Een analyse van de verschillen ten opzichte van de scores van vorig jaar laat zien dat hier interpretatie van de vraagstelling van het borgingsproduct en de meerdere (explicietere) antwoordmogelijkheden vooral hebben geleid tot dit verschil. Maar tegelijkertijd is ook een mooie (her)start gemaakt met DPIA's en een concrete afspraak met betrekking tot het inhalen van (een deel van de) achterstand.

2.3 Aanbevelingen

Maak de managers binnen Heusden verantwoordelijk voor de inhaalacties met betrekking tot in eerste instantie de hoog-risico DPIA's. Afspraken voor realisatie van deze inhaalslag aan het eind van 2026 zijn gemaakt, de voortgang dient tussentijds gemonitord te worden.

In 2025 is een nieuw proces gestart om in het kader van privacy samen te werken met het risicomanagement in gemeente Heusden. Er was al een goede samenwerking op het gebied van privacy en informatiebeveiliging en nu worden er stappen gemaakt om deze thema's nog sterker te verankeren in de organisatie in combinatie met risicomanagement. Om dit doel te bewerkstelligen zal er samengewerkt worden in een GRC-applicatie waar ook de maatregelen en uitvragen van de BIO en NIS2 een plek zullen krijgen. Aansluiting vanuit de vastgelegde processen in de gebruikte informatiemanagement applicatie is daarbij gewenst.

3. Organisatorische inbedding

Voor een goede en juiste uitvoering is het belangrijk dat iedereen binnen de organisatie op de hoogte is van het belang van privacy en de beginselen van de AVG. Organisatorische inbedding gaat over het toewijzen van taken, verantwoordelijkheden en bevoegdheden en bewustwording.

3.1 Terugblik op 2025

Sir Askalot wordt als bewustwordings-tool en onderdeel van het I&P team ingezet en daagt op een laagdrempelige manier medewerkers uit om zich te verdiepen in informatiebeveiliging en privacy. Deelname en resultaten worden gemonitord om het effect te vergroten. Er is doorgegaan met het organiseren van sessies voor nieuwe collega's en periodiek worden nog extra ludieke acties georganiseerd. Uiteraard verschijnen er ook berichten op het intranet over specifieke (actuele) onderwerpen als daar aanleiding voor is.

3.2 Basisniveau privacy volgens de IBD

Het borgingsproduct dat is ingevuld door de Privacy Officer, de CISO en de Concerncontroller laat de volgende scores zien:

3.	Organisatorische inbedding	91%
3.1	Privacyteam	63%
3.2	Aanstelling, positie en taken FG	95%
3.3	Informeren OR	88%
3.4	Bewustwording	95%

De score is verbeterd ten opzichte van vorig jaar, behalve waar het gaat om het privacyteam. Dit heeft te maken met de beperkt beschikbare tijd voor specifieke FG-taken, met name de achterstand op de (pre)DPIA's. De beschikbare capaciteit blijft dus een aandachtspunt. Door te blijven prioriteren en zeer gericht te werk te gaan lukt het om ervoor te zorgen dat de organisatie voldoende ondersteund wordt. De tijd om te kunnen voldoen aan de verzoeken uit de organisatie gaat echter vaak ten koste van de tijd die nodig is om privacy te waarborgen en preventief werkzaamheden uit te voeren.

Zoals beschreven is er veel gedaan om de bewustwording gestructureerd te organiseren in de organisatie. Dit kan nog verder doorgroeien door ook te evalueren op effectiviteit.

3.3 Aanbevelingen

Ga door met de campagnes voor meer bewustwording in de organisatie. Daarmee komen de vragen om afstemming door die zorgen voor inzicht in de daadwerkelijke tijdsbesteding van de Privacy Officer.

Veel tijd lijkt nu gevraagd te worden voor de (achterstand van de) DPIA's maar als het management daarin haar verantwoordelijkheid neemt, wordt pas echt zichtbaar hoe de Privacy Officer belast wordt. Zorg dus dat de verantwoordelijkheid duidelijk is en dat de uitdagingen op de juiste plekken worden opgepakt.

4. Rechten van betrokkenen

De gemeente moet betrokkenen (diegene van wie zij de persoonsgegevens verwerkt) zowel actief als passief infomeren over het verwerken, de wijze van het verwerken, de grondslag en de maatregelen die genomen zijn om onrechtmatige toegang en – verwerking te voorkomen. Daarnaast hebben betrokkenen een aantal rechten om controle en invloed uit te kunnen oefenen op zijn of haar persoonsgegevens.

4.1 Terugblik op 2025

In december 2023 is een gewijzigde procedure vastgesteld voor verzoeken om inzage, correctie en verwijdering van persoonsgegevens. Behalve toevoegen van de privacyrechten en evt. weigeringsgronden volgens de Wpg is de procedure ook vereenvoudigd zodat deze duidelijker is. De Privacy Officer is degene die dit soort verzoeken coördineert en afhandelt in samenwerking met betrokken clusters. In het geval van voorgenomen afwijzing van verzoeken wordt dit altijd afgestemd met de FG.

In 2025 zijn er 17 inzageverzoeken ingediend, waarvan er drie zijn afgebroken. De andere 14 verzoeken zijn in behandeling genomen en ingewilligd. De identiteit van verzoekers is correct vastgesteld.

4.2 Basisniveau privacy volgens de IBD

Het borgingsproduct dat is ingevuld door de Privacy Officer, de CISO en de Concerncontroller laat de volgende scores zien:

4.	Rechten van betrokkenen	88%
4.1	Recht op informatie	90%
4.2	Processen rechten van betrokkenen	92%
4.3	Toestemming	88%
4.4	Geautomatiseerde individuele besluitvorming	70%
4.5	Websites en applicaties	100%
4.6	Technische ondersteuning	88%

De scores op dit onderdeel zijn verder verbeterd ten opzichte van 2024. Inwoners worden beter geïnformeerd over hun rechten en de websites van de gemeente voldoen aan de gestelde eisen. Wel blijft aandacht nodig voor periodieke evaluatie.

4.3 Aanbevelingen

Geef aandacht aan periodieke toetsing of bij wijzigingen nog steeds voldaan wordt aan de vereisten. Ondanks de druk op de formatie moet hiervoor wel tijd vrijgemaakt worden.

5. Samenwerking

Net als iedere gemeente werkt de gemeente Heusden op meerdere beleidsterreinen, in diverse rollen en hoedanigheden samen met publieke en private organisaties. Vaak is hierbij sprake van het verwerken van persoonsgegevens tussen partijen: het ontvangen, opslaan en verzenden van en inzage hebben in persoonsgegevens. Deze verwerkingen moeten ook voldoen aan de AVG. Hierover moeten dus afspraken gemaakt worden.

5.1 Terugblik op 2025

In 2025 is er op het gebied van samenwerkingspartners vooral aandacht geweest voor gegevensdeling met de GGD en Sterk Huis. Hierbij is met name door de Privacy Officer kritisch gekeken naar AVG- risico's in de wederzijdse gegevensuitwisselingen.

Ook zijn zowel de Privacy Officer als de FG betrokken bij de totstandkoming van een DPIA die gemaakt is voor de werkprocessen van het ZVHMB (Zorg- en veiligheidshuis Midden-Brabant). Deze DPIA is gemaakt in het kader van de inwerkingtreding van de WGS (Wet Gegevensdeling door Samenwerkingsverbanden).

5.2 Basisniveau privacy volgens de IBD

Het borgingsproduct dat is ingevuld door de Privacy Officer, de CISO en de Concerncontroller laat de volgende score zien:

5.	Samenwerking	77%
5.1	AVG rollen	81%
5.2	Gegevensverstrekking	69%

Bij samenwerking met externe partijen krijgen we steeds meer helder hoe verantwoordelijkheden liggen, er is steeds meer aandacht voor dataminimalisatie en-bescherming. Veelal ontbreekt inzicht in verwerkersovereenkomsten op het niveau van samenwerkingsverbanden. Via convenanten en overeenkomsten moeten we toezien op naleving van de wettelijke eisen. Er is aandacht voor het verkrijgen van inzicht hoe een externe de persoonsgegevens dan daadwerkelijk beschermt. Het belangrijkste aandachtspunt is dat naleving van de afspraken niet of nauwelijks periodiek geëvalueerd wordt. Dit geldt ook voor gegevensverstrekkingen. Reactief zijn we vaak betrokken bij aanpassingen van samenwerkingsafspraken, maar proactief hebben we daar nog stappen te zetten. Periodieke evaluatie of deze voldoen aan wet- en regelgeving vindt niet expliciet plaats.

5.3 Aanbevelingen

Stel vast in welke gevallen binnen samenwerkingsverbanden bijzondere gegevens of persoonsgegevens van gevoelige aard worden verwerkt. Leg beter vast in het verwerkingsregister waar de afspraken zijn vastgelegd. Periodiek moet gecontroleerd worden of partijen zich hier ook aan houden.

6. Gegevensbescherming

Vanuit het algemene behoorlijkheidsbeginsel, het integriteitsbeginsel en het vertrouwelijkheidsbeginsel is het essentieel dat een 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 moeten worden aan de Autoriteit Persoonsgegevens en afhankelijk van de aard van het incident ook de betrokkene(n).

6.1 Terugblik op 2025

In 2025 zijn er 21 incidenten intern gemeld waarvan er 4 bij de Autoriteit Persoonsgegevens zijn gemeld. Er is naar aanleiding hiervan geen vervolgcontact met de Autoriteit Persoonsgegevens geweest. Hoewel er wettelijk gezien eerder een plicht is tot het melden bij de Autoriteit Persoonsgegevens dan melden bij betrokkenen, is er in de meeste gevallen voor gekozen om betrokkenen te informeren zonder dat daar een verplichting toe was of melding bij de Autoriteit Persoonsgegevens is gedaan.

6.2 Basisniveau privacy volgens de IBD

Het borgingsproduct dat is ingevuld door de Privacy Officer, de CISO en de Concerncontroller laat de volgende scores zien:

6.	Gegevensbescherming	91%
6.1	Risico's	50%
6.2	Gegevensbescherming door ontwerp	88%
6.3	Gegevensbescherming door standaardinstellingen	75%
6.4	Informatiebeveiliging	91%
6.5	Privacyincidenten en datalekken	98%

De scores op het terrein van gegevensbescherming laten een wisselende ontwikkeling zien die op totaalniveau positief uitpakt. Het meest opvallend is de score van 50% op het terrein van risico's. Deze komt doordat er geen uitgewerkt beoordelingsproces is met een managementsysteem voor het identificeren en aanpakken van risico's die samenhangen met persoonsgegevens. Overige zaken binnen deze categorie zijn allemaal verbeterd ten opzichte van 2024.

6.3 Aanbevelingen

Ga een applicatie gebruiken om de risico's vast te leggen, en daar de PDCA cyclus op toe te passen. Het GRC systeem kan daarvoor ingericht en gebruikt worden. Sluit daarbij bij voorkeur aan op de organisatie brede risicomanagement aanpak, waarbij samenwerking tussen Risicomanagement, Privacy Officer en CISO een logische stap is.

7. Verantwoording

De AVG legt de verantwoordelijkheid bij een 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.

7.1 Terugblik op 2025

Het borgingsdocument is een manier waarop de organisatie zichtbaar maakt in hoeverre voldaan wordt aan het basisniveau van de privacy volgens de IBD. De organisatie heeft deze ingevuld maar hier zelf verder niets mee gedaan. Het aantonen dat voldaan wordt aan de privacyregels zal door de organisatie altijd reactief, op verzoek, worden gedaan.

De score is iets hoger dan deze in 2024 was. Deze ziet voornamelijk toe op het intern toezicht. Hiervan kan gesteld worden dat deze grotendeels voldoet, maar dat blijft wel beperkt tot het minimale niveau. Aanvullende toetsingen blijven achterwege door de beperkte beschikbaarheid en de in te lopen achterstanden. De invulling van de functie is met name reactief (op verzoek van de organisatie) en signalerend (zorgen dat tijdig privacy deskundigheid wordt ingeschakeld).

7.2 Basisniveau privacy volgens de IBD

Het borgingsproduct dat is ingevuld door de Privacy Officer, de CISO en de Concerncontroller laat de volgende scores zien:

7.	Verantwoording	86%
7.1	Evaluatie naleving AVG	75%
7.2	Evaluatie informatiebeveiliging	100%
7.3	Rapportage	100%

De evaluatie van naleving van de AVG blijft een aandachtspunt. Wel is de evaluatie van informatiebeveiliging op orde, waardoor de totaalscore op verantwoording iets is verbeterd. Het blijft in zijn algemeenheid wel een uitdaging om periodiek te blijven evalueren.

7.3 Aanbevelingen

Verantwoording afleggen is ook het expliciteren van afwegingen over wat, wanneer wordt opgepakt. Dit gaat bijvoorbeeld over de risicogerichte aanpak om de volgorde van het uitvoeren van DPIA's te bepalen, maar ook de hoeveelheid capaciteit die hiervoor beschikbaar wordt gesteld. Capaciteit is op dit moment het knelpunt voor begeleiding bij het uitvoeren van DPIA's en dus het voldoen aan de betreffende wettelijke eisen. Het management is verantwoordelijk voor de uitvoering van de DPIA's, maar begeleiding daarbij door de Privacy Officer is essentieel. Blijf dit bespreekbaar maken en bewaak de voortgang.

Deel B: Wpg

Jaarverslag over het intern toezicht op omgaan met politiegegevens

3

1. Werkzaamheden van de FG voor de Wpg

1.1 Wettelijke voorschriften voor de FG

Artikel 36 van de Wpg bevat de bepalingen over de functionaris voor gegevensbescherming. Naast een aantal algemene bepalingen beschrijft lid 3 specifiek de taken van de FG:

De functionaris voor gegevensbescherming is tenminste belast met de volgende taken:

a. *het toezien op de naleving van het bepaalde bij of krachtens deze wet en op het beleid van de verwerkingsverantwoordelijke met betrekking tot de bescherming van persoonsgegevens, met inbegrip van de toewijzing van de autorisaties, bedoeld in artikel 6, de bewustmaking en opleiding van de ambtenaren van politie die zijn betrokken bij de verwerking van politiegegevens en de audits, bedoeld in artikel 33;*
b. *het informeren en adviseren van de verwerkingsverantwoordelijke en de ambtenaren van politie die politiegegevens verwerken over hun verplichtingen op grond van het bepaalde bij of krachtens deze wet en andere gegevensbeschermingsbepalingen op grond van het Unierecht of het Nederlandse recht;*
c. *het desgevraagd verstrekken van advies over de gegevensbeschermingseffectbeoordeling, bedoeld in artikel 4c, en het toezien op de uitvoering ervan;*
d. *het samenwerken met de Autoriteit persoonsgegevens;*
e. *het optreden als contactpunt voor de Autoriteit persoonsgegevens inzake aangelegenheden in verband met de verwerking van persoonsgegevens en, voor zover dienstig, het plegen van overleg over enige andere aangelegenheid.*

1.2 Invulling van deze werkzaamheden binnen de gemeente Heusden

De rol van FG voor de Wpg is door het college aangewezen en belegd bij de concerncontroller, die ook is aangewezen als FG voor de AVG. De Wpg is strikter van aard ten opzichte van de AVG, inhoudelijk maar ook als het gaat over de werkzaamheden van de FG en de jaarlijkse rapportage. In de Wpg is veel strikter voorgeschreven wat moet worden gedaan.

Om de rol als FG voor de Wpg te kunnen combineren met de andere werkzaamheden zijn afspraken gemaakt over de verdeling van taken. Deze zijn hetzelfde voor de AVG als voor de Wpg: het informeren en adviseren (zoals opgenomen in artikel 36 lid 3b) is voornamelijk belegd bij de Privacy Officer. Vanuit haar positie in de organisatie verzorgt ze de ondersteuning van de verantwoordelijken.

De Wpg kent ook een audit verplichting. Jaarlijks moet een interne audit worden uitgevoerd en iedere vier jaar een externe audit. In 2025 is de externe audit uitgevoerd. Deze gaat over de periode 2021 tot en met 2024. Net als in de vorige interne audits werd niet aan alle vereisten uit de Wpg voldaan. Het verbeterplan dat in maart 2023 is vastgesteld met een beschrijving en planning van de maatregelen die worden genomen, is eerder wel uitgevoerd maar is onvoldoende geborgd door personele mutaties . De focus van het interne toezicht moet daarmee blijven liggen op de naleving van de audit verplichtingen en opvolging van het verbeterplan. Hierin is een gedetailleerde inhoudelijke toets op naleving opgenomen.

2. Terugblik op 2025

2.1 Resultaten externe audit 2021-2024

Eind 2025 is door de externe auditor een Assurance rapport opgeleverd, waarin een aantal tekortkomingen zijn vermeld, die hebben geleid tot een afkeurend oordeel.

Een deel van deze tekortkomingen zijn bij eerdere (externe zowel als interne) audits ook al vastgesteld, echter is nog niet in alle gevallen gelukt om hier voldoende actief op bij te sturen, ondanks de maatregelen die zijn opgenomen in een intern verbeterplan.

De te nemen maatregelen in het verbeterplan blijken in een aantal gevallen meer tijd te kosten, soms afhankelijk te zijn van de interne tijdsbesteding van de Privacy Officer maar ook soms af te hangen van de technische mogelijkheden die leveranciers in hun programmatuur in kunnen passen. Ook is gebleken dat er kwetsbaarheid is bij personele mutaties en onvoldoende vastlegging en borging van procedures.

Eerder (in 2024) was vastgesteld dat nog in twee gevallen in het geheel niet voldaan werd aan de Wpg. Dit ging over de risico analyses (DPIA's) die nog niet waren uitgevoerd. Omdat andere maatregelen uit het verbeterplan vertraging hadden opgelopen had het nog geen zin deze tussentijds uit te voeren.

Uiteindelijk is in de rapportage over de periode 2021-2024 vastgesteld dat er nog steeds een aantal zaken zijn die verbetering nodig hebben. Dat zijn de volgende:

- Er zijn geen DPIA's in het WPG-domein uitgevoerd in de periode 2021-2024. Net als bij de rest van de DPIA's bestaat ook in het WPG-domein achterstand in de te realiseren DPIA's;
- Er is geen beleidsdocument waarin is vastgesteld dat met alle relevante WPG-verwerkingsorganisaties een verwerkersovereenkomst is overeengekomen;
- Er is niet geborgd dat verstrekking van politiegegevens aan personen of instanties buiten het politiedomein alleen gebeurt voor zover dat noodzakelijk is. Ook ontbreekt een werkwijze hoe te handelen bij onrechtmatige verstrekkingen of onjuiste gegevens;
- WPG-verwerkingen worden niet altijd opgenomen in het verwerkingsregister;
- Er is geen beleid of procedure waarin wordt bepaald dat de verwerkingsverantwoordelijke moet documenteren als er sprake is van doorgifte van politiegegevens;
- Niet van alle raadplegingen en mutaties in systemen is adequate logging voorhanden. De meest gebruikte applicaties voldoen wel, maar gebleken is dat medewerkers in voorkomende gevallen ook gebruik maken van andere applicaties, waarbij de logging niet voldoet;
- De noodzaak en rechtmatigheid van politiegegevens moet aantoonbaar gemaakt kunnen worden;
- Het gebruik van andere dan leerplichtsystemen zou bij de leerplicht BOA's afgebouwd moeten worden;

Deze audit geeft informatie over hoe goed eerder genomen verbetermaatregelen zijn uitgevoerd. Uit de rapportage blijkt dat we nog steeds, ondanks de ondernomen acties, niet volledig voldoen aan de vereisten. Dit wordt onder andere zowel bij domein 1 (veiligheid) als domein 3 (leerplicht) veroorzaakt doordat niet alleen in Wpg-gecertificeerde applicaties gewerkt wordt. Voor domein 1 was dit bekend en ook dat dit (nog) niet is opgelost. Waar het gaat om de procedures die wel in de gecertificeerde applicatie worden uitgevoerd blijkt dat we het inmiddels op orde hebben en wel voldoen. Voor domein 3 voldoen we nagenoeg, helaas bleek uit de audit dat er toch af en toe nog Outlook werd gebruikt voor contact met betrokkenen of ketenpartners. In dat geval zijn er onvoldoende waarborgen voor het verwijderen van de politiegegevens. Hier is aandacht voor in de uitvoering.

Overigens is het wel zo dat er aan het eind van 2025 de nodige DPIA's zijn uitgevoerd in het WPG-domein. Dit betreft cameratoezicht op nieuwe en bestaande locaties.

3. Intern toezicht 2026

Door de personele wisselingen op zowel de post van Privacy Officer als die van FG in 2025 heeft het toezicht op de WPG niet alle aandacht gekregen die nodig was om de externe audit positief af te sluiten. Toch bestaat de indruk dat er niet stilgestaan is en veel zaken onderhanden zijn. Het lijkt dus slechts een kwestie van tijd en hernieuwde afspraken met de collega's van domein 1 en 3 om binnen afzienbare tijd veel van de verbeterpunten te kunnen afstrepen. Hier gaat op gefocust worden in 2026.