Jaarrapportage
functionaris gegevensbescherming 2024

Leidschendam-Voorburg

Aan	het college van burgemeester & wethouders
Van	Susana Denneman
Afdeling	concern control
Datum	18 maart 2025
Versie	4179
Onderwerp	Jaarrapportage FG 2024

1. Inleiding

1.1 Rol en taken functionaris gegevensbescherming

De functionaris gegevensbescherming (hierna: FG) is een onafhankelijke toezichthouder die binnen de gemeente Leidschendam-Voorburg (hierna: gemeente) toezicht houdt op de toepassing en naleving van de Algemene verordening gegevensbescherming (hierna: AVG) en de Wet politiegegevens (hierna: Wpg). De taken van de FG bestaan kort gezegd uit (i) toezien op de naleving van de AVG en Wpg; (ii) adviseren over uitgevoerde privacy-risicobeoordelingen (hierna: DPIA's); (iii) informeren en adviseren van de organisatie en de werknemers over de AVG en voor de buitengewoon opsporingsambtenaren de Wpg en (iv) optreden als aanspreekpunt voor de Autoriteit Persoonsgegevens.

1.2 Samenvatting

In deze jaarrapportage wordt teruggekeken naar het jaar 2024. Deze jaarrapportage bevat naast de aanbevelingen in hoofdstuk 3 ook de resultaten van het onderzoek naar de stand van privacy en de bescherming van persoonsgegevens in onze organisatie dat in het kader van artikel 213a Gemeentewet (hierna: het Onderzoek) is uitgevoerd.[1]

Het is positief dat het directie team zich in 2024 herkende in de vijf grootste privacy risico's die in de jaarrapportage 2023 zijn opgenomen (zie ook hoofdstuk 3 van deze jaarrapportage) en bereid is om actie te ondernemen. De grootste uitdaging zit het komende jaar om de rest van de organisatie onderdelen aan te laten sluiten teneinde de organisatie privacy proof te maken. De focus zal vooral moeten liggen op het aanpakken van het risico (i) dat het (lijn)management onvoldoende verantwoordelijkheid neemt voor het onderwerp en (ii) het gestructureerd aanpakken van het ontbreken van procesbeschrijvingen.

Deze jaarrapportage bevat 19 aanbevelingen. Deze aanbevelingen zijn gebaseerd op de observaties van de FG en de resultaten van het Onderzoek. Er is goed nagedacht over het verwoorden van de aanbevelingen zodat de organisatie concrete doelen kan stellen om de aanbevelingen effectief op te volgen. Ik begrijp dat de organisatie voor meer uitdagingen staat dan enkel het opvolgen van de aanbevelingen van de FG. Laat de organisatie daarom aansluiting vinden bij andere thema's en/of duidelijke keuzes maken in het prioriteren ervan.

Susana Denneman, functionaris gegevensbescherming

[1] Het college is verplicht om onderzoek te doen naar de doelmatigheid en de doeltreffendheid van het door haar gevoerde bestuur (art 213a Gemeentewet). Wethouder Veller heeft namens het college op 23 oktober 2023 een brief gestuurd aan de Raad Brief (iBabs 3539) dat het onderzoek naar de stand van privacy en de bescherming van persoonsgegevens in onze organisatie onderwerp zal zijn van het onderzoek in 2024.

2. Onderzoek

2.1 Achtergrond en methodiek

Het college heeft in 2024 een zelfonderzoek uitgevoerd verplicht naar de stand van privacy en de bescherming van persoonsgegevens in onze organisatie in het kader van artikel 213a Gemeentewet.

Voor het Onderzoek is gebruik gemaakt van het door de Informatiebeveiligingsdienst (onderdeel van de VNG) ontwikkeld borgingsproduct. Aan de hand van de beantwoording van 155 vragen is vastgesteld of de gemeente voldoet aan een basisniveau van privacybescherming. Hierbij is het uitgangspunt dat gemeente aan alle criteria (maatregelen) uit het borgingsproduct voldoet, tenzij gemotiveerd onderbouwd is waarom een bepaalde maatregel in een concreet geval niet van toepassing is.[2]

Het onderzoek is uitgevoerd door de FG, twee privacy officers, CISO, twee information security officers en technical information security officer van de gemeente. Zij kwalificeren als expert op het gebied van privacy, gegevensbescherming en informatiebeveiliging. Bij vragen over het bewaar- en vernietigingsbeleid is advies ingewonnen bij een adviseur informatiebeheer.

Het Onderzoek is opgebouwd uit zeven thema's. Ieder thema wordt hieronder verduidelijkt.

Beleid *De organisatie heeft processen en bijbehorende verantwoordelijkheden en risico's in kaart gebracht en vastgelegd in beleidsstukken. Deze stukken moeten voor alle werknemers goed vindbaar en begrijpelijk zijn.*

Processen *De organisatie heeft alle processen waarbinnen persoonsgegevens worden verwerkt in kaart gebracht. De beschrijving van deze processen wordt actueel gehouden, werkinstructies worden nageleefd en processen met een hoog risico worden getoetst op juistheid.*

Organisatorische inbedding *De organisatie heeft een FG aangesteld en kan zich voor inhoudelijke vraagstukken tot een intern privacyteam richten. Er wordt doorlopend aan bewustwording gedaan.*

[2] Meer informatie over het borgingsproduct kan worden gevonden op https://www.informatiebeveiligingsdienst.nl/product/avg-borgingsproduct-3-0-handreiking

Rechten van betrokkenen *De organisatie voldoet aan alle wettelijke eisen die er zijn op het gebied van rechten van betrokkenen. De organisatie is transparant over hoe en welke persoonsgegevens verwerkt worden.*

Samenwerking *De organisatie heeft in kaart gebracht met wie zij samenwerkt en heeft daarbij passende afspraken gemaakt. Deze afspraken worden door de betrokken partijen nageleefd.*

Gegevensbescherming *Hoewel pas echt een volledig beeld kan worden geschetst van de stand van zaken op het gebied van gegevensbescherming middels de Baseline Informatiebeveiliging Overheid, zijn privacy en gegevensbescherming niet geheel van elkaar los te trekken. Een aantal informatiebeveiligingsaspecten met een duidelijke privacycomponent zijn ook in het Onderzoek opgenomen.*

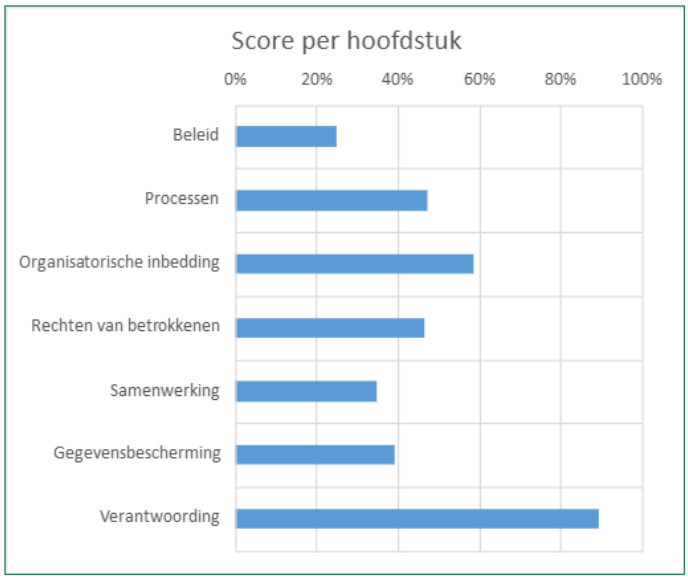
Verantwoording *De organisatie evalueert de naleving van de AVG en rapporteert over de voortgang.*

2.2 Uitkomsten

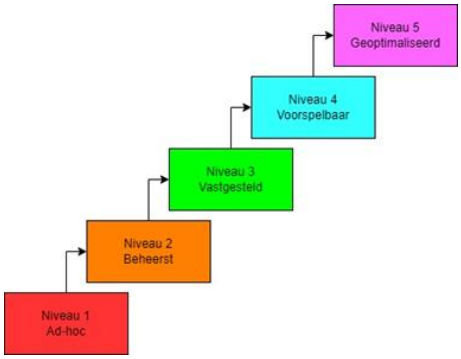
Hieronder is gedetailleerd een score per onderwerp weergegeven.

Par	Titel	Leeg	N.v.t	Beantwoord	Percentage
1.	Beleid	0	0	17	25%
1.1	Beleid vaststellen	0	0	2	0%
1.2	Privacybeleid	0	0	9	42%
1.3	Verantwoordelijkheden	0	0	6	8%
2.	Processen	0	0	38	47%
2.1	Werkprocessen	0	0	7	11%
2.2	Verwerkingsregister	0	0	10	75%
2.3	Pre-DPIA's	0	0	3	58%
2.4	DPIA's	0	0	10	45%
2.5	Bewaar- en vernietigingsbeleid	0	0	8	44%
3.	Organisatorische inbedding	0	0	20	59%
3.1	Privacyteam	0	0	2	63%
3.2	Aanstelling, positie en taken FG	0	0	11	84%
3.3	Informeren OR	0	0	2	50%
3.4	Bewustwording	0	0	5	5%
4.	Rechten van betrokkenen	0	0	30	47%
4.1	Recht op informatie	0	0	5	50%
4.2	Processen rechten van betrokkenen	0	0	9	78%
4.3	Toestemming	0	0	4	44%
4.4	Geautomatiseerde individuele besluitvorming	0	0	5	0%
4.5	Websites en applicaties	0	0	3	67%
4.6	Technische ondersteuning	0	0	4	19%
5.	Samenwerking	0	0	15	35%
5.1	AVG rollen	0	0	8	28%
5.2	Gegevensverstrekking	0	0	7	43%
6.	Gegevensbescherming	0	0	28	39%
6.1	Risico's	0	0	2	50%
6.2	Gegevensbescherming door ontwerp	0	0	2	25%
6.3	Gegevensbescherming door standaardinstellinger	0	0	1	25%
6.4	Informatiebeveiliging	0	0	10	35%
6.5	Privacyincidenten en datalekken	0	0	13	44%
7.	Verantwoording	0	0	7	89%
7.1	Evaluatie naleving AVG	0	0	4	81%
7.2	Evaluatie informatiebeveiliging	0	0	2	100%
7.3	Rapportage	0	0	1	100%

Onderstaand figuur geeft het scoringspercentage per onderwerp weer.



De gemeente scoort op zes van de zeven onderwerpen tussen 20-60%. Op basis van de score kan een vertaling worden gemaakt naar het niveau waarop de gemeente zich bevindt. De vijf niveaus zijn afkomstig van het 'Privacy maturity model' van de IAPP. Deze niveaus van de IAPP zijn weer afgeleid van de GAPP's (Generally Accepted Privacy Principles) en het CMM (Capability Maturity Model).[3] Een score tussen 20-40% komt ongeveer overeen met een volwassenheidsniveau 1 tot 2 (op een schaal van 5). Een score tussen 40-60% komt ongeveer overeen met een volwassenheidsniveau 2 tot 3. In onderstaand figuur en in de handleiding van borgingsproduct (zie noot 3) wordt uitgelegd wat ieder niveau betekent.



[3] Privacy volwassenheidsniveaus

2.3 Analyse

Het nemen van een rekenkundig gemiddelde om tot een volwassenheidsniveau te komen maakt het eenvoudig om de stand van zaken met stakeholders te communiceren. Ik wil niet onvermeld laten dat cijfers soms een verkeerd beeld kunnen geven. Hieronder licht ik dit toe.

Dit onderzoek is uitgevoerd naar de gehele organisatie. Onderlinge verschillen waarbij het ene goed presterende domein een duidelijk minder goed presterend domein compenseert, levert mogelijk een vertekend beeld op van de werkelijkheid. De praktijk is namelijk dat er grote verschillen per domein zijn. De afdeling VTH loopt bijvoorbeeld voorop in het voldoen aan het basisniveau van privacybescherming.

Ook zijn er per thema grote verschillen zichtbaar. In onderstaande tabel is per deelonderwerp de score inzichtelijk. Bij organisatorische inbedding (nummer 3) zijn grote verschillen zichtbaar. Het onderwerp bewustwording zit op 5%, terwijl aanstelling, taken en positie FG 84% scoort. Uiteindelijk levert het een totaalscore van 60% op.

Het Onderzoek kan om die reden niet los worden gezien van de aanbevelingen die zijn gebaseerd op de observaties van de FG die verderop in deze jaarrapportage zijn opgenomen.

Tot slot kunnen de resultaten van het Onderzoek worden vergeleken met een eerder onderzoek dat in 2021 is uitgevoerd. In 202 heeft de gemeente een nulmeting uitgevoerd waarvan de resultaten in februari 2022 met het college zijn gedeeld. Bij dat onderzoek werd gebruik gemaakt van het door adviesbureau BMC ontwikkeld Privacy Framework, dat uit 11 onderdelen bestaat. Bij het Onderzoek in 2024 is gekozen voor een andere onderzoeksmethode dan het Privacy Framework. Het door de Informatiebeveiligingsdienst ontwikkelde borgingsproduct is namelijk specifiek ontwikkeld voor gemeenten en is gebaseerd op zeven thema’s die die overeenkomen met de hoofdstukken die verderop zijn opgenomen in de jaarrapportage (Beleid, Processen, Organisatorische inbedding, Rechten van betrokken). Bovendien heeft de FG haar jaarrapportage 2023 ook opgebouwd volgens dezelfde zeven thema’s. Ondanks het feit dat er gebruik is gemaakt van een andere onderzoeksmethode kunnen de resultaten wel met elkaar worden vergeleken.

De meest belangrijke resultaten uit het onderzoek 2021 waren dat (i) wettelijk verplichte verantwoordingsdocumentatie voor een belangrijk deel ontbrak of niet op orde was; (ii) de inrichting van het privacy management door capaciteitsgebrek ernstig was achtergebleven; (iii) er geen structuur en overzicht was in de privacy activiteiten, omdat het register van verwerkingen niet op orde was én niet werd benut als beheersinstrument. Ook (iv) het (van te voren) toetsen van risico’s en rechtmatigheid bij

nieuwe verwerkingen; (v) de transparantie richting betrokkenen; (vi) datalekken beheer, en (vii) het contractbeheer van (verwerkers)overeenkomsten was niet voldoende ingericht.

Ten opzichte van 2021 zijn wel stappen gezet. Zo is er sinds 2023 een FG in dienst genomen en is de privacy organisatie versterkt met twee privacy officers. De komst van de twee privacy officers heeft ertoe geleid dat de FG zich meer kan toeleggen op het houden van toezicht en de privacy officers met het geven van privacy juridisch advies. Sinds maart 2022 is het verwerkingsregister gereed en zijn er grote stappen gezet in het kader van de verantwoording; de FG heeft over 2023 gerapporteerd. Er is ook meer structuur en overzicht in de privacy activiteiten. Er is een actueel overzicht van DPIA's. Er is eind 2024 een procedure geïmplementeerd voor privacy inzageverzoeken.

Onderstaande tabel geeft een overzicht van de resultaten van 2024 ten opzichte van 2021. De tabel bevat lege plekken omdat de Privacy Framework onderwerpen niet altijd vergeleken kunnen worden met de thema's uit het borgingsproduct.

Titel	Percentage 2024	Percentage 2021
Beleid	25%	25%
Processen	47%	
Verwerkingsregister	75%	26%
DPIA's	45%	25%
Bewaar- en vernietigingsbeleid	44%	55%
Organisatorische inbedding	59%	46%
Rechten van betrokkenen	47%	
Recht op informatie	50%	33%
Processen rechten van betrokkenen	78%	25%
Samenwerking	35%	
Gegevensverstrekking	43%	14%
Gegevensbescherming	39%	
Informatiebeveiliging	35%	60%
Privacyincidenten en datalekken	44%	20%
Verantwoording	89%	

3. Aanbevelingen

Vorig jaar is de eerste jaarrapportage van de FG opgesteld en gedeeld met de organisatie. De jaarrapportage is besproken met het management (het directie team) op maandag 25 maart 2024 en in het ontwikkel CMT op woensdag 10 april 2024. Ook heeft de gemeentesecretaris de jaarrapportage gedeeld met de Ondernemingsraad. In het document acties en advies aanbevelingen jaarrapportage FG 2023 heeft het directie team opgeschreven hoe de organisatie de aanbevelingen van de FG op zal volgen.

Opnieuw zijn de in de jaarrapportage FG 2023 geïdentificeerde vijf grootste privacy risico's belangrijk. Hieronder zijn ze nogmaals summier opgesomd:

1. Het lijnmanagement neemt onvoldoende verantwoordelijkheid voor gegevensbescherming;
2. het ontbreken van procesbeschrijvingen (en ernaar handelen);
3. er is een kennisachterstand op het gebied van informatiebeveiliging en privacy bij de medewerkers;
4. er is een gebrek aan borging van informatiebeveiliging en privacy;
5. de organisatie is onvoldoende voorbereid op (gewijzigde) verplichtingen voortkomend uit (toekomstige) wetgeving.

3.1 Beleid

De gemeente heeft in 2022 het strategisch informatiebeveiligingsbeleid vastgesteld. Dit loopt in 2025 af en moet worden geactualiseerd. Er is overlap tussen informatiebeveiliging en privacy. Er is door de directie voorgesteld om het bestaande informatiebeveiligingsbeleid uit te breiden tot strategisch informatiebeveiligings- en privacybeleid.

Aanbeveling 1 *Zorg ervoor dat het strategisch privacybeleid in 2025 is vastgesteld en geïmplementeerd*

Uit de resultaten van het Onderzoek komt naar voren dat de organisatie laag scoort op het onderwerp beleid. Er zijn nog onvoldoende privacy beleidsstukken opgesteld, vastgesteld en geïmplementeerd.

Aanbeveling 2 *Zorg ervoor dat in 2025 een overzicht is opgesteld van verschillende beleidsdocumenten en richtlijnen die samen een kader vormen voor de bescherming van informatie en persoonsgegevens binnen de gemeente. Maak hiervan een planning wanneer deze onderliggende documentatie moet zijn vastgesteld. Begin met het opstellen van beleidsstukken*

3.2 Processen

Gemeenten verwerken veel (gevoelige) persoonsgegevens in het kader van hun taken en activiteiten. Bestaande en nieuwe processen moeten volgens de privacywetging voldoen aan de volgende beginselen: behoorlijkheid, transparantie, doelbinding, dataminimalisatie, opslagbeperking, juistheid, integriteit en vertrouwelijkheid.

3.2.1 Procesbeschrijvingen

De FG merkt op dat medewerkers vaak niet bekend zijn hoe een bepaald proces verloopt of zou moeten verlopen. Er ontbreekt in die gevallen veelal een procesbeschrijving, of medewerkers zijn niet bekend met bestaan ervan. Het komt ook voor dat er wel procesbeschrijvingen zijn opgesteld, maar dat er niet naar wordt gehandeld. Vanuit het oogpunt van gegevensbescherming heeft het ontbreken van een procesbeschrijving tot gevolg dat dat er niet gestart kon worden met de uitvoer van de DPIA's en/of de uitvoer van een DPIA ontzettend veel tijd kost, omdat eerst uitgezocht moet worden hoe de uitvoering van een bepaald taak/proces verloopt. De FG kan op die manier niet haar controletaak uitvoeren en de privacy officers of anderen die daarvoor zijn aangewezen kunnen geen DPIA's uitvoeren.

Er is momenteel geen centrale regie op procesmanagement. Dit risico is uitgebreid onder de aandacht gebracht tijdens het CMT en tijdens de taskforce overleggen met de FG, CISO gemeentesecretaris en concern controller en afdelingshoofd IISO. De concern controller is in de taskforce benoemd tot regievoerder van dit onderwerp.

Aanbeveling 3 *Zorg voor een centrale regie op procesmanagement. Verken hoe je procesmanagement binnen de organisatie wil vormgeven*

3.2.2 DPIA's

De gemeente is verplicht om bij risicovolle werkprocessen waarbij persoonsgegevens worden verwerkt een DPIA uit te voeren.

In 2024 zijn 4 DPIA's uitgevoerd. Deze DPIA's zijn voorzien van advies van de FG.

In het kader van het privacyproof maken van de organisatie heeft er in 2024 een verkenning plaatsgevonden. Er is in de periode juni - augustus 2024 een uitvraag gedaan bij de afdelingshoofden naar de risicovolle processen waarbij persoonsgegevens worden verwerkt, met als doel om door het lijnmanagement een prioriteitenlijst voor het uitvoeren van DPIA's vast te stellen. Uit de door de privacy officers en FG uitgevoerde inventarisatie zijn 34 risicovolle processen geïdentificeerd. Door het directie team is – op voordracht van het CMT - besloten dat de risicovolle

processen van WIJZ en KCC in de eerste plaats zullen worden onderworpen aan een DPIA in 2025.

Aanbeveling 4 *Zorg ervoor dat de DPIA template gebruiksvriendelijker wordt opdat het voor afdelingen/teams wordt vergemakkelijkt om input te leveren*
Aanbeveling 5 *Faciliteer dat de afdelingen/teams zelf DPIA's uitvoeren en laat privacy coachend optreden*

3.2.3 Verwerkingsregister

De gemeente is verplicht om een actueel register van verwerkingen in stand te houden. De gemeente voldoet weliswaar aan deze verplichting, maar er is ruimte voor verbetering op dit vlak. Er is een online applicatie aangeschaft om privacy en informatiebeveiligingszaken te regelen. Deze applicatie omvat ook het online bijhouden van het verwerkingsregister. Het grote voordeel van deze applicatie is dat het voor de key users gemakkelijker wordt om de proceseigenaren/uitvoerders te betrekken bij het actualiseren van het verwerkingsregister.

Aanbeveling 6 *Implementeer het verwerkingsregister in de nieuwe applicatie*

3.3 Organisatorische inbedding

Elk proces binnen de gemeente dient belegd te zijn bij een proceseigenaar. Niet elke proceseigenaar weet wat van hem of haar precies verwacht wordt op het gebied van gegevensbescherming. Zo zijn zij er verantwoordelijk voor dat passende privacy- en informatiebeveiligingsmaatregelen binnen hun eigen processen worden geïmplementeerd. Ook zorgen ze ervoor dat een privacy officer in een vroeg stadium wordt betrokken bij plannen voor nieuwe en gewijzigde processen met persoonsgegevens. De Autoriteit Persoonsgegevens signaleert ook dat de kennis van de privacywet- en regelgeving binnen overheidsorganisaties soms te wensen overlaat, in het bijzonder bij bestuurders.[4]

Het is dan ook van groot belang dat proceseigenaren voldoende kennis van zaken hebben om goede besluiten te kunnen nemen over (nieuwe) verwerkingen van persoonsgegevens. Onvoldoende kennis belemmert ook de voortgang van de besluitvorming; bestuurders durven geen beslissingen te nemen, omdat zij de privacywet- en regelgeving – onterecht – als belemmering zien. Privacy hoort ook thuis in de managementgesprekken tussen directie en afdelingshoofden. Het directie team heeft laten weten dat dit onderwerp wordt meegenomen in de doorontwikkeling van het lijnmanagement.

[4] Zie Rapport Sectorbeeld overheid 2024.pdf

Aanbeveling 7 *Zorg voor een privacy bewustwordingsprogramma voor lijnmanagement en voor medewerkers. Meer specifiek, zorg dat elk proces een proceseigenaar heeft en dat deze bekend is met diens taken, verantwoordelijkheden en bevoegdheden op het gebied van gegevensbescherming. Zo kan deze binnen het proces gaan sturen op het zorgvuldig omgaan met persoonsgegevens*

3.4 Rechten van betrokkenen

De gemeente is verplicht om de personen van wie zij de persoonsgegevens verwerkt (dit wordt betrokkene genoemd) te informeren over het verwerken, de wijze van het verwerken, de grondslag en de maatregelen die zij neemt om onrechtmatige toegang en - verwerking te voorkomen. Daarnaast stelt de AVG en Wpg betrokkenen in staat om controle en invloed uit te oefenen over zijn of haar persoonsgegevens.

Steeds meer burgers weten de weg te vinden naar de gemeente met vragen over hun persoonsgegevens. De FG ervaart dit als positieve ontwikkeling. De organisatie moet in staat zijn om inkomende vragen of verzoeken over persoonsgegevens of datalekken te herkennen en aan de juiste personen toe te wijzen. Dit gaat nog te vaak verkeerd en hierdoor gaat kostbare tijd verloren. Het niet in acht nemen van wettelijke behandeltermijnen levert een overtreding van de privacywetten op. Dit moet worden voorkomen.

Aanbeveling 8 *Zorg voor voldoende kennis en/of naslagwerken bij medewerkers, met name bij de eerstelijnsmedewerkers van KCC (MIC, en medewerkers informatiebeheer), om verschillende privacyvragen of -verzoeken te identificeren*

De FG handelt privacyvragen van burgers af. Dit zijn veelal kwesties waarbij burgers zich zorgen maken over hun privacy in combinatie met een wantrouwen richting de overheid. De FG heeft in 2024 zes privacyvragen behandeld over uiteenlopende onderwerpen.

In 2024 heeft de FG drie inzageverzoeken en vijf verwijderverzoeken van bewoners behandeld. Eind 2024 is er een procedure geïmplementeerd die ervoor zorgt dat privacy (AVG of Wpg) inzageverzoeken conform de wetgeving kunnen worden afgehandeld. Een medewerker informatiebeheer is de behandelaar van privacy inzageverzoeken en er wordt gewerkt met key users van applicaties. Het project krijgt een vervolg in 2025 voor de afhandeling van verwijderverzoeken in de brede zin.

Aanbeveling 9 *Creëer een procedure voor privacy verwijderverzoeken waarbij ook verwijderverzoeken in het kader van bijzondere wetgeving is meegenomen*

De privacyverklaring op de website is verouderd en te generiek. Voor de leesbaarheid dient de privacyverklaring meer op specifieke onderwerpen gericht te zijn. De privacyverklaring ziet momenteel alleen op de AVG en niet op de Wpg en voldoet hiermee niet aan de Wpg.

Aanbeveling 10 *Zorg voor een up to date privacyverklaring*

Er ontbreekt informatie (althans de FG heeft hiervoor onvoldoende bewijs gezien), of is deze gebrekkig, over wat de gemeente doet met persoonsgegevens in het contact met de burger (denk hierbij aan het informeren tijdens een intake, brieven, folders, etcetera). Een voorbeeld in positieve zin is de Wmo folder. Hier wordt in begrijpelijke taal uitgelegd wat een burger kan verwachten van de gemeente, ook in het kader van de gegevensuitwisseling.

Aanbeveling 11 *Laat de proceseigenaren in kaart brengen of en in hoeverre zij betrokkenen informeren wanneer persoonsgegevens worden verzameld*

3.5 Samenwerkingen

De gemeente verzamelt en gebruikt veel persoonsgegevens om haar taken uit te voeren. Zij maakt hiervan gebruik van dienstverleners/verwerkers. Een overzicht met bestaande afspraken ontbreekt. Onduidelijk is of afspraken nog actueel zijn, of er afspraken ontbreken en of ze worden nageleefd. De systematische controle hierop is onvoldoende. Hierdoor kan ook niet worden onderzocht of er afspraken zijn gemaakt over hoe er met de persoonsgegevens wordt omgegaan.

Aanbeveling 12 *Controleer periodiek of de afspraken op papier in de praktijk worden nagekomen*

Ook werkt de gemeente op meerdere beleidsterreinen, in verschillende bedrijfsfuncties, in diverse rollen en hoedanigheden samen met (mede) overheden en private organisaties. Vooral bij gemeentelijke samenwerkingsverbanden is nog vaak is er onvoldoende aandacht voor de risico’s en is onvoldoende duidelijk waarvoor welke partij verantwoordelijk is.

Aanbevelingen 13 *Maak een overzicht van alle gemeentelijke samenwerkingsverbanden en maak inzichtelijk welke risico’s er zijn op het gebied van gegevensbescherming*

3.6 Inbreuken op de beveiliging

Het is een wettelijke plicht dat de gemeente passende technische en organisatorische maatregelen neemt om persoonsgegevens te beveiligen. Daarnaast geldt er onder de AVG en Wpg een meldplicht datalekken. Dit houdt in dat incidenten – waaronder inbreuken – op de beveiliging onder omstandigheden gemeld dienen te worden aan de Autoriteit Persoonsgegevens en/of de betrokkene(n).

Er zijn in 2024 14 datalekken gemeld bij de FG. Het datalek dat het meest is gemeld is de situatie dat een brief of bestand met persoonsgegevens is verstuurd aan de verkeerde ontvanger(s). Van twee datalekken is melding gemaakt bij de Autoriteit Persoonsgegevens. Er wordt nog onvoldoende gemonitord of de preventieve maatregelen naar aanleiding van een datalek daadwerkelijk zijn genomen.

Aanbeveling 14 *Zorg ervoor dat monitoring en evaluatie van datalekken is ondergebracht bij de afdelingen*

Aanbeveling 15 *Lever bewijs aan dat de FG structureel toezicht houdt op de naleving van de preventieve maatregelen als gevolg van een datalek*

Er is op intranet informatie beschikbaar over het melden van datalekken (beveiligingsincidenten), maar er is behoefte dat een allesomvattend proces wordt opgesteld en vastgesteld voor het melden van beveiligingsincidenten.

Aanbeveling 16 *Stel een incident response proces op, stel vast en implementeer*

3.7 Verantwoording

De controle die de FG uitvoert vindt veelal ad hoc plaats. Er is behoefte aan gestructureerde monitoring. Dit volgt onder andere uit de resultaten van de WPG rapportage waarbij de organisatie onvoldoende scoorde op de uitvoering van gepland toezicht. Daarnaast heeft het lijnmanagement ook behoefte aan een meer planmatige aanpak van toezicht. Door het geplande toezicht op te nemen in afdelingsjaarplannen, is de afdeling beter voorbereid op wat van hen kan worden verwacht.

3.7.1 Toezichtsplan

De FG heeft een voorlopig toezichtsplan voor 2025 opgesteld. Dit plan geeft de FG een leidraad. In dit toezichtplan worden de algemeen beschreven taken uitgewerkt in meer concrete werkzaamheden en wordt toegelicht waar de focus van het toezicht zal liggen in het kalenderjaar 2025.

Het is de bedoeling dat dit toezichtsplan deel gaat uitmaken van een gemeenschappelijk toezichtspan voor de onderwerpen Verbijzonderde Interne Controle (VIC), Gegevensbescherming (FG) en informatiebeveiliging (CISO) omdat veel uitgangspunten voor de controles gelijk zijn, maar ook om het besluitvormingsproces te vereenvoudigen. Door deze geïntegreerde aanpak wordt de efficiëntie verhoogd en de samenhang tussen de verschillende toezichtactiviteiten versterkt.

Aanbeveling 17 *Zorg voor een geïntegreerde toezichtskalender voor de onderwerpen Verbijzonderde Interne Controle (VIC), gegevensbescherming (FG) en informatiebeveiliging (CISO) dat een overzicht geeft van alle toezichtactiviteiten en inzichtelijk maakt waarop wordt toegezien, waarom en wanneer*

3.7.2 Wpg audit

Het is de derde keer dat de gemeente een toets heeft uitgevoerd op de Wpg. In het najaar 2022 is voor de eerste keer een audit uitgevoerd. Vorig jaar vond de hercontrole plaats over 2023 en dit jaar een ‘gewone’ interne audit. Deze audit kan worden gezien als een goede generale repetitie van de externe audit die in 2025 gepland staat. De voorbereidingen zijn hiervoor inmiddels getroffen.

In het auditrapport is per onderwerp opgenomen of deze qua opzet, bestaan en werking effectief zijn. Daarbij wordt gebruik gemaakt van de kleuren groen (effectief), oranje (gedeeltelijk effectief), rood (niet effectief) en grijs (niet van toepassing of non-occurence). Waar de auditresultaten van 2022 en 2023 veelal rood kleurde, voert oranje de boventoon. Dit is te danken aan de inspanningen van de medewerkers die betrokken waren bij de uitvoering van de audit. Het is een realistische verwachting dat veel gedeeltelijk effectieve maatregelen in 2025 kunnen worden omgezet naar effectief.

Een punt van aandacht blijft het audit proces. De betrokken medewerkers zijn van mening dat deze efficiënter aangepakt zou kunnen worden. Een centrale sturing is gewenst. Ik pleit er dan ook voor om een interne projectleider te benoemen voor het coördineren van de Wpg audit. Daarnaast zou het uitvoeren van het Wpg auditonderzoek kunnen worden belegd bij de gemeente. Het meest logische is dat dit wordt ondergebracht bij concern control. Ik pleit er dan ook voor om te onderzoeken of het uitvoeren van de Wpg audit door de gemeente kan worden gedaan. Tot slot zal de FG actiever toezicht moeten uitvoeren op de Wpg verplichtingen omdat de gemeente op dit punt veelal onvoldoende scoort.

Aanbeveling 18 *Benoem een interne projectleider Wpg audit*
Aanbeveling 19 *Onderzoek of het uitvoeren van de Wpg audit door de gemeente kan worden gedaan*