FG Jaarverslag (AVG en WPG)

Gemeente Deurne

1 Jaarverslag Gegevensbescherming 2025

2 Leeswijzer

2.1 Doel

Dit document bevat het jaarverslag gegevensbescherming van de Functionaris voor Gegevensbescherming (FG) en geeft inzicht in de naleving van de wetgeving inzake de bescherming van persoonsgegevens binnen de organisatie.

De FG rapporteert hiermee aan het College van burgemeester en wethouders en de gemeenteraad over de bevindingen uit het toezicht en de mate waarin de organisatie voldoet aan de wettelijke verplichtingen en deze naleving kan aantonen.

Voor de Wet politiegegevens (WPG) geldt een expliciete verplichting tot verslaglegging. Voor de Algemene Verordening Gegevensbescherming (AVG) is een jaarverslag niet expliciet voorgeschreven, maar wordt dit gezien als best practice in het kader van de verantwoordingsplicht en de onafhankelijke positie van de FG.

2.2 Opbouw van het verslag

Het verslag is opgebouwd uit drie delen:

- Deel A: AVG
  Dit deel beschrijft de stand van zaken rondom de naleving van de AVG. Per thema worden de bevindingen en aanbevelingen van de FG weergegeven.
- Deel B: WPG
  Dit deel bevat het verslag van bevindingen over de naleving van de WPG.
- Deel C: Ontwikkelingen en toezichtactiviteiten
  In dit deel worden relevante ontwikkelingen en toezichtactiviteiten van de FG beschreven. Dit betreft onder andere onderzoeken, signalen en nieuwe toepassingen waarbij persoonsgegevens worden verwerkt, zoals het gebruik van nieuwe technologieën, gegevensuitwisselingen en andere privacy relevante ontwikkelingen binnen de organisatie.

In de bijlagen is aanvullende onderbouwing opgenomen, waaronder registraties, kengetallen en verdiepende analyses die ten grondslag liggen aan de bevindingen in dit verslag.

2.3 Doelgroep

Dit verslag is opgesteld voor het College van burgemeester en wethouders en de gemeenteraad.

3 Managementsamenvatting

Dit jaarverslag geeft een integraal beeld van de stand van zaken rondom gegevensbescherming binnen de gemeente Deurne in 2025, voor zowel de Algemene Verordening Gegevensbescherming (AVG) als de Wet politiegegevens (Wpg). Daarnaast wordt ingegaan op relevante ontwikkelingen en toezichtactiviteiten.

3.1 Algemeen beeld

De organisatie heeft de afgelopen jaren belangrijke stappen gezet in het inrichten van privacy en gegevensbescherming. De basis is aanwezig: beleid, registers, rollen en processen zijn ingericht, waarbij de verdere doorontwikkeling zich met name richt op volledigheid, actualiteit en samenhang.

De Functionaris Gegevensbescherming (FG) constateert dat de organisatie zich in een volgende fase bevindt, waarin de nadruk verschuift van inrichting naar aantoonbare beheersing. Met name de samenhang tussen instrumenten en de structurele controle op de werking daarvan vragen verdere versterking.

Belangrijke aandachtspunten zijn:

- de volledigheid en actualiteit van het verwerkingsregister;
- het integrale inzicht in het landschap van gegevensverwerkingen en de samenhang tussen systemen, processen en externe partijen;
- de aantoonbaarheid van uitgevoerde DPIA's en de opvolging van maatregelen;
- en de verdere inrichting van structurele monitoring en controle.

3.2 AVG - belangrijkste bevindingen

Binnen de AVG zijn de belangrijkste instrumenten aanwezig, zoals het privacybeleid, het verwerkingsregister en processen voor datalekken en verzoeken van betrokkenen.
De FG constateert dat verdere versterking nodig is op de volgende punten:

- het verder volledig en actueel maken van het verwerkingsregister;
- het borgen dat voor alle risicovolle verwerkingen aantoonbaar een DPIA wordt uitgevoerd;
- het vergroten van de samenhang tussen verwerkingen, systemen en externe partijen, zodat afspraken met alle relevante partijen inzichtelijk en aantoonbaar zijn;
- en het verder versterken van de aantoonbaarheid dat maatregelen effectief werken.

Positief is dat de processen rondom de rechten van betrokkenen functioneren en voldoen aan de wettelijke eisen. Deze beoordeling is gebaseerd op beschikbare registraties; niet is vastgesteld of alle verzoeken volledig worden geregistreerd.

Beeld AVG: de basis is ingericht en functioneert op onderdelen goed, met ruimte voor verdere versterking van grip en aantoonbaarheid. Verdere professionalisering is wenselijk.

3.3 Wpg - belangrijkste bevindingen

Binnen de Wpg is in 2025 een belangrijke stap gezet door de uitbreiding naar domein I (Openbare Ruimte). Hiermee is de reikwijdte van politiegegevens binnen de organisatie toegenomen en zijn aanvullende processen ingericht.
De organisatie heeft:

- beleid en werkprocessen verder ingericht, waaronder voor toezicht en handhaving;
- een DPIA uitgevoerd voor het nieuwe domein;
- stappen gezet in het formaliseren van autorisaties en het verbeteren van registraties.

De FG constateert dat de organisatie zich verder ontwikkelt richting structurele en aantoonbare beheersing. Daarbij zijn de volgende aandachtspunten zichtbaar:

- autorisaties zijn ingericht en deels hersteld, met aandacht voor structurele borging en -periodieke controle;
- logging is technisch aanwezig, waarbij verdere inrichting van structurele controleprocessen gewenst is;
- registratie van verstrekkingen kan nog verder worden geharmoniseerd en gecentraliseerd;
- de opvolging van auditbevindingen is in uitvoering, waarbij nog enkele punten openstaan;
- de aantoonbaarheid van maatregelen is in sommige gevallen afhankelijk van externe partijen, wat aanvullende aandacht vraagt.

Beeld Wpg: de organisatie heeft zichtbare stappen gezet in inrichting en ontwikkeling. Verdere uitwerking is nodig om te komen tot structurele controle en aantoonbare naleving.

3.4 Ontwikkelingen en risico’s

De externe ontwikkelingen laten zien dat de druk op gegevensbescherming toeneemt. Toezichthouders signaleren onder andere aandachtspunten rondom:

- algoritmegebruik en AI;
- grootschalige dataverzameling en koppeling van gegevens;
- en afhankelijkheid van externe (met name buitenlandse) technologieleveranciers.

Voor de gemeente betekent dit dat:

- transparantie over algoritmen en datagebruik steeds belangrijker wordt;
- DPIA's en juridische onderbouwing verder aangescherpt moeten worden;
- en aandacht nodig is voor proportionaliteit en grondrechten, naast privacy.

3.5 Toezichtactiviteiten FG

De FG heeft in 2025 toezicht gehouden op diverse concrete situaties, waaronder:

- het gebruik van BRP-gegevens via een constructie met de peelgemeente, waarbij juridische aandachtspunten zijn vastgesteld;
- de inzet van nieuwe technologie zoals Copilot;
- controles op personeelsvolgsystemen;
- en de beoordeling van incidenten en signalen.

Deze toezichtactiviteiten bevestigen het algemene beeld dat processen aanwezig zijn en dat verdere borging en structurele naleving in ontwikkeling zijn.

3.6 Conclusie en prioriteiten

De gemeente Deurne heeft de basis voor gegevensbescherming ingericht en zet stappen richting verdere professionalisering. Tegelijkertijd vraagt de verantwoordingsplicht uit de AVG en de naleving van de Wpg om verdere versterking van aantoonbaarheid en beheersing.

De FG adviseert om in de komende periode te focussen op:

1. Het volledig en aantoonbaar actueel maken van het verwerkingsregister;
2. Het structureel uitvoeren, vastleggen en opvolgen van DPIA's, inclusief periodieke herbeoordeling van risico's;
3. Het versterken van de samenhang tussen verwerkingen, applicaties, gegevensstromen en betrokken (externe) partijen;
4. Het inrichten en aantoonbaar uitvoeren van structurele controles, waaronder logging, autorisatiebeheer en analyse van incidenten en datalekken;
5. En het vergroten van bewustwording en sturing binnen de organisatie.

De kernopgave voor 2026 is de verdere ontwikkeling van "ingericht" naar "aantoonbaar in control".

4 Inleiding

4.1 Leeswijzer jaarverslag

Dit jaarverslag bestaat uit 3 onderdelen:

- Deel A: betreft het verslag over de AVG;
- Deel B: gaat over de bevindingen over de WPG;
- Deel C: relevante ontwikkelingen op het gebied van gegevensbescherming.

Aangezien zowel de AVG als de WPG betrekking hebben op de bescherming van persoonsgegevens, is gekozen voor één gecombineerd jaarverslag.

De opbouw van het verslag is als volgt:

- Dashboard: een stoplichtenrapportage die een samenvattend beeld geeft van de stand van zaken per thema binnen de AVG en WPG.
- Verdieping per thema: per onderwerp worden de bevindingen van de FG en de bijbehorende aanbevelingen beschreven.
- Bijlagen: in de bijlagen is een nadere onderbouwing opgenomen, onder andere op basis van registraties, kengetallen en beschikbare documentatie.

Bij de beoordeling is gebruikgemaakt van bestaande instrumenten binnen de organisatie, zoals registraties en interne overzichten. Deze zijn gebruikt als ondersteunende bron, waarbij de FG een zelfstandige beoordeling heeft uitgevoerd op basis van de feitelijke situatie en de mate van aantoonbaarheid.

5 Deel A: AVG

5.1 AVG-dashboard

Het onderstaande dashboard geeft een samenvattend beeld van de stand van zaken rondom de naleving van de AVG binnen de organisatie in 2025. De beoordeling is uitgevoerd door de FG op basis van beschikbare documentatie, registraties en toezichtactiviteiten.

De beoordeling is gebaseerd op de mate waarin de organisatie voldoet aan de wettelijke verplichtingen uit de AVG en in hoeverre dit aantoonbaar kan worden gemaakt.

Thema: 2025

Borging AVG	Jaarverslag (beeld)	Resultaat 2025	Verwacht (norm AVG)
Beleid	Beleid aanwezig, maar toepassing niet aantoonbaar	🟠	🟢
Processen (register & DPIA)	Register en DPIA's aanwezig, maar niet volledig en niet geborgd	🔴	🟢
Organisatorische inbedding	Rollen aanwezig, maar niet structureel geborgd	🟠	🟢
Rechten van betrokkenen	Proces ingericht en functioneert binnen termijnen	🟢	🟢
Samenwerking (verwerkers)	Verwerkingen met externe partijen aanwezig, maar geen volledig en samenhangend inzicht in verwerkingen, betrokken partijen en controle op naleving	🟠	🟢
Gegevensbescherming (incidenten)	Incidentproces aanwezig, maar weinig analyse en sturing	🟠	🟢
Verantwoording (accountability)	Instrumenten aanwezig, maar werking niet aantoonbaar	🔴	🟢

Legenda:

🔴	AANDACHT VEREIST VAN MANAGEMENT
🟠	IN TE HALEN ACHTERSTAND
🟢	OP SCHEMA

5.2 Deel 1. Terugblik op 2025

In dit deel van de rapportage kijkt de FG terug op hetgeen de gemeente in 2025 heeft bereikt en welke werkzaamheden en bevindingen zijn gedaan in het kader van het toezicht op de naleving van de AVG.

De beoordeling is gebaseerd op een analyse van beschikbare documentatie, registraties en toezichtactiviteiten van de FG. Hierbij is onder andere gekeken naar:

- het verwerkingsregister en het DPIA-register;
- registraties van verzoeken van betrokkenen;
- meldingen van privacy- en beveiligingsincidenten;
- de samenhang tussen verwerkingen, applicaties, gegevensstromen en (externe) partijen (gegevenslandschap);
- en de inrichting en toepassing van beleid en processen binnen de organisatie.

Deze informatie is gebruikt om te beoordelen in hoeverre de organisatie voldoet aan de verplichtingen uit de AVG en in hoeverre deze naleving aantoonbaar is.

In de bijlagen is aanvullende onderbouwing opgenomen, waaronder overzichten, kengetallen en registraties die ten grondslag liggen aan de bevindingen in dit verslag.

5.2.1 Beleid

De AVG verplicht organisaties om passende organisatorische maatregelen te treffen (artikel 24 AVG). Het vaststellen van beleid is hiervan een onderdeel.

Binnen de organisatie is een privacybeleid vastgesteld en gepubliceerd op het interne platform (Trefpunt). Daarnaast is zichtbaar dat onderdelen van dit beleid, zoals de privacyverklaring, recent zijn geactualiseerd naar aanleiding van ontwikkelingen binnen de organisatie. Dit duidt erop dat het beleid wordt onderhouden en beschikbaar is voor medewerkers.

Binnen de organisatie wordt daarnaast aandacht besteed aan privacy in het kader van onboarding van nieuwe medewerkers. Op basis van de beschikbare informatie kan echter niet worden vastgesteld dat deze onboarding structureel, verplicht en aantoonbaar wordt uitgevoerd en gemonitord.

Tegelijkertijd constateert de FG dat op basis van de beschikbare informatie niet kan worden vastgesteld in hoeverre het beleid structureel en actief wordt toegepast in de dagelijkse praktijk. Hoewel het beleid via het intranet toegankelijk is, is er geen aantoonbaar inzicht in:

- de wijze waarop het beleid actief onder de aandacht wordt gebracht binnen de organisatie;
- de mate waarin medewerkers bekend zijn met het beleid en weten hoe dit toe te passen;
- de vertaling van het beleid naar concrete werkinstructies en procesbeschrijvingen;
- en de wijze waarop wordt gecontroleerd of het beleid wordt nageleefd.

Dit betekent niet dat deze activiteiten niet plaatsvinden, maar wel dat dit niet aantoonbaar is gemaakt.

De AVG vereist dat de organisatie niet alleen beleid vaststelt en beschikbaar stelt, maar ook kan aantonen dat dit beleid daadwerkelijk wordt toegepast (artikel 24 en artikel 5 lid 2 AVG).

Dit vereist dat de organisatie:

- vastlegt hoe en wanneer beleid actief wordt gecommuniceerd aan medewerkers;
- inzicht heeft in de mate waarin medewerkers bekend zijn met het beleid, bijvoorbeeld via training en monitoring;
- beleid aantoonbaar vertaalt en geborgd heeft in concrete werkinstructies en procesbeschrijvingen;
- en periodiek controleert en vastlegt of het beleid wordt nageleefd.

Op basis van de beschikbare informatie kan niet worden vastgesteld dat deze elementen structureel zijn ingericht en gedocumenteerd. Hierdoor is de toepassing van het beleid onvoldoende aantoonbaar.

Daarom is de beoordeling**:** oranje**.**
Het beleid is aanwezig, wordt onderhouden en is intern beschikbaar gesteld, maar de toepassing is onvoldoende aantoonbaar.

5.2.2 Processen

De AVG stelt eisen aan de inrichting van processen rondom gegevensverwerking. Organisaties moeten onder andere:

- een volledig en actueel verwerkingsregister bijhouden (artikel 30 AVG);
- privacyrisico’s beoordelen en waar nodig een DPIA uitvoeren (artikel 35 AVG);
- kunnen aantonen dat verwerkingen voldoen aan de privacybeginselen.

Binnen de organisatie is een verwerkingsregister aanwezig. Op basis van de beschikbare informatie kan echter niet worden vastgesteld dat dit register volledig en actueel is. De

inhoud van het register is afhankelijk van input vanuit de organisatie, en het is niet aantoonbaar dat alle verwerkingen structureel worden gemeld en opgenomen.

Daarnaast is een DPIA-register aanwezig en zijn DPIA's uitgevoerd. Tegelijkertijd kan niet worden vastgesteld dat:

- voor alle verwerkingen is beoordeeld of sprake is van een hoog risico;
- voor alle risicovolle verwerkingen daadwerkelijk een DPIA is uitgevoerd;
- maatregelen uit DPIA's structureel worden opgevolgd en gecontroleerd.

Dit betekent dat de processen in opzet aanwezig zijn, maar dat de volledigheid en werking niet aantoonbaar zijn.

Volgens de AVG moet de organisatie aantoonbaar inzicht hebben in alle verwerkingen en de bijbehorende risico's. Dit betekent dat:

- het verwerkingsregister volledig en actueel moet zijn;
- er een proces moet zijn om wijzigingen structureel te registreren;
- DPIA's systematisch moeten worden uitgevoerd waar nodig;
- en dat maatregelen uit DPIA's aantoonbaar worden gemonitord.

Daarnaast ontbreekt aantoonbare samenhang tussen verwerkingen, applicaties, gegevensstromen en betrokken (externe) partijen. Hierdoor is geen volledig en consistent beeld van het gegevenslandschap beschikbaar, wat het risico vergroot dat verwerkingen onvolledig worden geregistreerd en privacyrisico's niet structureel in beeld zijn.

Dit gebrek aan samenhang ondermijnt de betrouwbaarheid van het verwerkingsregister en de uitvoering van DPIA-processen, waardoor de organisatie onvoldoende aantoonbare grip heeft op haar verwerkingen en risico's.

Omdat dit niet aantoonbaar is, kan niet worden vastgesteld dat de organisatie voldoet aan deze verplichtingen.

Daarom is de beoordeling: rood.
De organisatie heeft onvoldoende aantoonbare grip op haar verwerkingen en risico's.

5.2.3 Organisatorische inbedding

De AVG vereist dat privacy structureel is ingebed in de organisatie (artikel 24 en 25 AVG).

Binnen de organisatie zijn rollen ingericht, zoals de FG, Privacy Officer en CISO. Daarmee is de basis voor governance aanwezig.

Tegelijkertijd blijkt uit de beoordeling dat niet in alle gevallen kan worden vastgesteld dat privacy structureel en in een vroeg stadium wordt betrokken bij projecten en ontwikkelingen. Ook hebben wisselingen in de invulling van de rol van Privacy Officer invloed gehad op de continuïteit.

Daarnaast worden trainingen aangeboden, maar is niet aantoonbaar dat deelname en effectiviteit structureel worden gemonitord.

Dit betekent dat de organisatorische inrichting aanwezig is, maar dat de werking en borging niet volledig aantoonbaar zijn.

Volgens de AVG moet privacy structureel onderdeel zijn van de organisatie. Dit betekent dat:

- privacy aantoonbaar wordt meegenomen in projecten en besluitvorming;
- rollen en verantwoordelijkheden niet alleen zijn belegd, maar ook functioneren;
- en dat bewustwording en training aantoonbaar worden georganiseerd en gemonitord.

Daarom is de beoordeling: oranje.

5.2.4 Rechten van betrokkenen

De AVG verplicht organisaties om betrokkenen in staat te stellen hun rechten uit te oefenen (artikelen 12-23 AVG).

Binnen de organisatie is een proces ingericht voor het behandelen van verzoeken van betrokkenen. Op basis van de beschikbare registraties blijkt dat verzoeken worden geregistreerd en binnen de wettelijke termijnen worden afgehandeld.

De FG constateert op basis van beschikbare registraties dat het proces functioneert en dat hiermee wordt voldaan aan de wettelijke verplichtingen.

Wel geldt dat deze beoordeling is gebaseerd op beschikbare registraties en dat niet aanvullend is vastgesteld of alle verzoeken volledig worden geregistreerd.

Daarom is de beoordeling: groen.
Het proces is ingericht en functioneert aantoonbaar.

5.2.5 Samenwerking

De AVG stelt eisen aan de verwerking van persoonsgegevens door externe partijen (artikel 28 AVG).

Binnen de organisatie zijn verwerkersovereenkomsten afgesloten en wordt een contractenregister bijgehouden. Tegelijkertijd kan niet worden vastgesteld dat er sprake is van voldoende samenhang tussen verwerkingen, applicaties, gegevensstromen en betrokken (externe) partijen.

Hierdoor is niet aantoonbaar dat:

- alle externe verwerkingen volledig en integraal in beeld zijn;
- de rollen en verantwoordelijkheden van betrokken partijen eenduidig en correct zijn vastgelegd;
- met alle relevante partijen passende (verwerkers)afspraken zijn gemaakt;
- en dat naleving van deze afspraken structureel wordt gemonitord.

Dit betekent dat de organisatie onvoldoende aantoonbare en integrale grip heeft op verwerkingen door externe partijen.

Volgens de AVG moet de organisatie aantoonbaar controle hebben op verwerkingen door derden. Dit vereist dat externe verwerkingen integraal inzichtelijk zijn, rollen en verantwoordelijkheden duidelijk zijn vastgelegd en dat naleving van afspraken structureel wordt bewaakt.

Omdat deze samenhang en beheersing niet aantoonbaar zijn, kan niet worden vastgesteld dat aan deze verplichtingen wordt voldaan.

Daarom is de beoordeling: oranje.

5.2.6 Gegevensbescherming

De AVG verplicht organisaties om passende beveiligingsmaatregelen te treffen en datalekken te melden (artikel 32 en 33 AVG).

Binnen de organisatie zijn processen ingericht voor het melden en behandelen van incidenten. Uit de beschikbare informatie blijkt dat incidenten worden geregistreerd en beoordeeld en dat waar nodig meldingen worden gedaan.

Tegelijkertijd kan niet worden vastgesteld dat incidenten structureel worden geanalyseerd en gebruikt voor verbetering. Hierdoor is niet aantoonbaar dat de organisatie leert van incidenten en risico’s structureel reduceert.

Volgens de AVG moet de organisatie niet alleen reageren op incidenten, maar ook aantonen dat maatregelen effectief zijn en risico’s worden beheerst.

Dit betekent dat:

- incidenten structureel moeten worden geanalyseerd;
- oorzaken moeten worden vastgesteld;
- en verbetermaatregelen moeten worden gemonitord.

Daarom is de beoordeling: oranje.
De basis is aanwezig, maar structurele verbetering is niet aantoonbaar.

5.2.7 Verantwoording

De AVG vereist dat organisaties kunnen aantonen dat zij voldoen aan de privacyregels (artikel 5 lid 2 AVG).

Binnen de organisatie zijn verschillende instrumenten aanwezig, zoals het verwerkingsregister, DPIA's en incidentregistraties.

De FG constateert echter dat niet kan worden vastgesteld dat deze instrumenten in samenhang functioneren en dat de werking van maatregelen structureel wordt gecontroleerd.

Met name:

- de volledigheid van het verwerkingsregister is niet aantoonbaar;
- de opvolging van DPIA-maatregelen is niet aantoonbaar;
- structurele controle op maatregelen ontbreekt.

Hierdoor kan de organisatie niet aantonen dat zij voldoet aan de AVG.

Volgens de AVG moet de organisatie kunnen laten zien dat maatregelen werken. Dit vereist samenhang, controle en monitoring.

Daarom is de beoordeling: rood.

5.2.8 Conclusie

De FG constateert dat de organisatie de basis voor privacybeheer heeft ingericht. Beleid, rollen en instrumenten zijn aanwezig.

Tegelijkertijd blijkt dat in meerdere gevallen niet kan worden vastgesteld dat deze instrumenten volledig, actueel en effectief functioneren. De kern van de bevindingen ligt daarmee niet in het ontbreken van maatregelen, maar in het ontbreken van aantoonbaarheid en samenhang.

De organisatie voldoet op onderdelen aan de AVG, maar kan dit nog niet in alle gevallen aantoonbaar maken. Daarmee is nog niet volledig voldaan aan het accountability-principe.

Om te voldoen aan de AVG is het noodzakelijk dat de organisatie:

- het verwerkingsregister volledig en actueel maakt en als leidend instrument gebruikt;
- de toepassing en opvolging van DPIA's structureel borgt;
- inzicht en controle realiseert op externe verwerkingen;
- incidenten gebruikt voor structurele verbetering;
- en privacy integraal opneemt in de planning- en controlcyclus.

De FG concludeert dat de organisatie nog niet volledig voldoet aan de verantwoordingsplicht uit de AVG, doordat de werking en samenhang van maatregelen onvoldoende aantoonbaar zijn.

5.3 Deel 2. Vooruitkijken naar 2026

In dit deel geeft de FG per thema aanbevelingen voor stappen die de organisatie in 2026 kan zetten om de naleving van de AVG te verbeteren en de aantoonbaarheid daarvan te versterken.

5.3.1 Beleid

De organisatie beschikt over privacybeleid, maar de toepassing en doorwerking in de praktijk zijn nog onvoldoende aantoonbaar.

In 2026 moet de organisatie zich richten op het versterken van de implementatie van beleid. Dit betekent dat niet alleen beleid beschikbaar moet zijn, maar dat ook aantoonbaar moet zijn dat medewerkers dit kennen en toepassen. Binnen de organisatie zijn via Trefpunt werkinstructies en privacygerelateerde informatie beschikbaar gesteld en zijn initiatieven zichtbaar, zoals aandacht voor privacy tijdens de Dag van de Privacy. Op basis van de beschikbare informatie kan echter niet worden vastgesteld in hoeverre deze structureel bijdragen aan de aantoonbare toepassing van het beleid.

De FG adviseert om vast te leggen hoe beleid binnen de organisatie wordt gecommuniceerd en om inzichtelijk te maken dat medewerkers toegang hebben tot en kennis hebben van het beleid. Daarnaast moet aantoonbaar worden gemaakt dat beleid is vertaald naar en geborgd in concrete werkinstructies en procesbeschrijvingen, en dat deze in de praktijk worden toegepast.

Tot slot is het noodzakelijk om periodiek te controleren en te documenteren of het beleid nog actueel is en daadwerkelijk wordt nageleefd. Hiermee wordt invulling gegeven aan de verantwoordingsplicht uit artikel 24 AVG.

5.3.2 Processen

De grootste opgave voor 2026 ligt bij het versterken van de processen rondom gegevensverwerking, met name het verwerkingsregister en de toepassing van DPIA's.

De organisatie moet ervoor zorgen dat het verwerkingsregister volledig en actueel is en daadwerkelijk als leidend instrument wordt gebruikt. Dit betekent dat alle verwerkingen, voortkomend uit systemen, processen en applicaties, in het register moeten zijn opgenomen.

Daarnaast moet structureel worden geborgd dat nieuwe en gewijzigde verwerkingen worden gemeld en beoordeeld voordat zij in gebruik worden genomen.

Voor DPIA's geldt dat niet alleen de uitvoering moet worden verbeterd, maar vooral de opvolging van maatregelen. De organisatie moet aantoonbaar maken dat risico's uit DPIA's worden opgevolgd en periodiek worden geëvalueerd.

De FG adviseert om het verwerkingsregister, DPIA's en processen integraal met elkaar te verbinden, zodat een samenhangend beeld ontstaat van verwerkingen en risico's.

5.3.3 Organisatorische inbedding

De organisatie heeft de basis voor privacy governance ingericht, maar verdere professionalisering is noodzakelijk.

In 2026 wordt aanbevolen om de rol van proceseigenaren te versterken en privacy structureel te betrekken bij nieuwe projecten en ontwikkelingen. Privacy kan daarbij als vast onderdeel van besluitvorming en projectinrichting worden ingericht.

Daarnaast is het belangrijk om de continuïteit in rollen, zoals de Privacy Officer, te borgen en verantwoordelijkheden duidelijk vast te leggen.

Op het gebied van bewustwording moet een structureel programma worden ingericht, waarbij niet alleen trainingen worden aangeboden, maar ook wordt gemonitord of medewerkers daadwerkelijk beschikken over voldoende kennis en vaardigheden.

5.3.4 Rechten van betrokkenen

De organisatie beschikt over een werkend proces voor het afhandelen van verzoeken van betrokkenen. In 2026 ligt de nadruk op het verder bestendigen en waar mogelijk versterken van dit proces in de uitvoering.

Het wordt aanbevolen om de herkenning van verzoeken binnen de organisatie te verbeteren en te zorgen voor een uniforme werkwijze bij de afhandeling. Daarnaast is het van belang om periodiek te evalueren of verzoeken tijdig en volledig worden afgehandeld, zodat eventuele verbeterpunten tijdig worden gesignaleerd.

De informatievoorziening richting betrokkenen is via de privacyverklaring ingericht. Aanvullend kan worden bezien of de toegankelijkheid en begrijpelijkheid hiervan verder kan worden versterkt.

5.3.5 Samenwerking

De samenwerking met externe partijen vormt een belangrijk risicogebied en vraagt in 2026 nadrukkelijke aandacht.

De organisatie moet zorgen voor een volledige en consistente koppeling tussen het contractenregister en het verwerkingsregister. Dit betekent dat voor elke verwerking met een externe partij duidelijk moet zijn:

- welke partij betrokken is;
- welke rol deze partij heeft (verwerker of verwerkingsverantwoordelijke);
- en welke afspraken zijn gemaakt.

Daarnaast moet structureel worden gecontroleerd of leveranciers voldoen aan de gemaakte afspraken, bijvoorbeeld door middel van periodieke evaluaties of audits.

De FG adviseert om samenwerking met externe partijen risicogestuurd te benaderen en prioriteit te geven aan verwerkingen met een hoog risico. Binnen de organisatie is een CAB (Change Advisory Board) ingericht waarin wijzigingsverzoeken, waaronder inkoop van IT-diensten, worden besproken. Dit draagt bij aan het bewustzijn rondom wijzigingen en externe samenwerking. Op basis van de beschikbare informatie kan echter niet worden vastgesteld dat hiermee alle verwerkingen met externe partijen volledig en structureel in beeld zijn en worden getoetst aan de AVG. De CAB vormt daarmee een belangrijke maatregel, maar biedt op zichzelf geen volledige waarborg voor beheersing van de privacyrisico’s.

5.3.6 Beveiliging

De organisatie heeft de basis voor informatiebeveiliging en incidentmanagement ingericht, maar moet in 2026 sterker inzetten op structurele verbetering.

Dit betekent dat incidenten en datalekken niet alleen moeten worden geregistreerd en afgehandeld, maar ook systematisch moeten worden geanalyseerd. De organisatie moet inzicht krijgen in oorzaken en trends en op basis daarvan maatregelen nemen om herhaling te voorkomen.

Daarnaast moet worden geborgd dat beveiligingsmaatregelen aansluiten bij de risico's van de verwerkingen en dat deze maatregelen periodiek worden geëvalueerd.

De FG adviseert om informatiebeveiliging en privacy sterker met elkaar te verbinden en te sturen op een continue verbetercyclus. Op basis van de beschikbare informatie ontstaat het beeld dat incidenten, zoals het verlies of verkeerd gebruik van mobiele gegevensdragers (bijvoorbeeld USB-sticks), wel worden opgepakt, maar dat een structurele analyse van oorzaken, trends en herhalingsrisico's ontbreekt en niet aantoonbaar is ingericht.

5.3.7 Verantwoording

De grootste uitdaging voor 2026 ligt bij het versterken van de verantwoordingsplicht (accountability).

De organisatie dient niet alleen te voldoen aan de AVG, maar ook aantoonbaar te maken dat hieraan wordt voldaan. Dit vraagt om samenhang tussen de verschillende instrumenten, zoals het verwerkingsregister, DPIA's, contracten en incidentregistraties.

In 2026 moet worden ingezet op het structureel controleren van de werking van maatregelen en het vastleggen van deze controles. Dit betekent dat niet alleen wordt vastgelegd wat is ingericht, maar ook dat wordt aangetoond dat dit in de praktijk werkt.

De FG adviseert om een structurele PDCA-cyclus in te richten, waarin beleid, uitvoering, controle en bijsturing met elkaar verbonden zijn.

5.3.8 Conclusie

De organisatie heeft de basis voor gegevensbescherming ingericht, maar bevindt zich nog in een fase waarin de nadruk moet verschuiven van inrichting naar borging en aantoonbaarheid.

Voor 2026 ligt de belangrijkste opgave in het versterken van de samenhang tussen processen, systemen en registraties, en in het aantoonbaar maken van de werking van maatregelen.

De FG concludeert dat het voor de organisatie in 2026 van belang is om prioriteit te geven aan:

- het volledig en actueel maken van het verwerkingsregister;
- het versterken van de toepassing en opvolging van DPIA's;
- het verbeteren van de beheersing van samenwerking met externe partijen;
- en het structureel inrichten van controle- en evaluatieprocessen.

Door deze stappen te zetten kan de organisatie doorgroeien naar een situatie waarin niet alleen wordt voldaan aan de AVG, maar dit ook aantoonbaar en duurzaam wordt geborgd.

6 Deel B: WPG

6.1 Inleiding

De Functionaris Gegevensbescherming (FG) houdt onafhankelijk toezicht op de naleving van de Wet politiegegevens (Wpg) binnen de gemeente Deurne. Het college draagt er zorg voor dat de FG tijdig en naar behoren wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van politiegegevens.

De FG rapporteert jaarlijks de bevindingen in een jaarverslag. In dit hoofdstuk wordt beschreven welke acties en maatregelen in 2025 zijn genomen om de doelstellingen en beginselen uit de Wpg te behalen en te waarborgen.

Om de huidige stand van zaken goed te kunnen duiden, is ook gekeken naar de ontwikkeling over de afgelopen jaren.

In 2023 bevond de organisatie zich nog in een beginfase van Wpg-naleving. Beleid was beperkt uitgewerkt en processen waren nog niet structureel ingericht. Belangrijke onderdelen zoals autorisatiebeheer, logging en registratie van verstrekkingen waren nog onvoldoende aanwezig of aantoonbaar. Ook ontbrak een volledig register van Wpg-verwerkingen.

In 2024 zijn belangrijke stappen gezet in de verdere inrichting. Beleid en processen zijn opgesteld, registers zijn ingericht en eerste controles zijn uitgevoerd. Tegelijkertijd bleek dat de werking van deze maatregelen nog onvoldoende geborgd was. Met name de aantoonbaarheid van maatregelen en de structurele controle hierop bleven achter.

In 2025 is deze ontwikkeling verder doorgezet en uitgebreid. De reikwijdte van de Wpg is vergroot door de inrichting van domein I (Openbare Ruimte), naast het reeds bestaande leerplichtdomein (domein III). Voor dit nieuwe domein is een DPIA uitgevoerd en zijn verwerkingen opgenomen in het Wpg-register.

Daarnaast zijn stappen gezet in het formaliseren van autorisaties, het verkrijgen van inzicht in logging en het verbeteren van de registratie van verstrekkingen.

De FG constateert echter dat deze maatregelen nog niet in alle gevallen structureel zijn geborgd of aantoonbaar worden uitgevoerd.

Tegelijkertijd constateert de FG dat de organisatie zich in 2025 nog bevindt in een overgangsfase van inrichting naar structurele en aantoonbare beheersing. De basis is aanwezig, maar de borging en controle van maatregelen zijn nog niet in alle gevallen volledig uitgewerkt of aantoonbaar.

De inrichting en toetsing van de Wpg-processen vindt plaats op basis van het normenkader uit de Handreiking Wpg-privacy audit van NOREA.

6.2 WPG-dashboard (2025)

Onderdeel	Resultaat 2025	Toelichting
Beleid	🟠	Beleid en procesbeschrijvingen zijn uitgebreid (incl. domein I) en grotendeels actueel, maar toepassing en naleving zijn nog onvoldoende structureel geborgd en aantoonbaar
Bewustwording	🟠	Kennis van Wpg en MAS aanwezig in de uitvoering, maar geen structureel en aantoonbaar trainingsprogramma
Autorisatieproces	🟠	Autorisaties zijn formeel ingericht (incl. besluiten, formulieren, BOA-status en controles via o.a. JVS-checks). Vanuit het JVS-systeem worden maandelijks controlelijsten ontvangen en beoordeeld. Op basis van de beschikbare informatie kan echter niet worden vastgesteld dat de beoordeling en opvolging van deze controles structureel is vastgelegd en gedocumenteerd, en onderdeel vormt van een integraal autorisatiebeheerproces (inclusief periodieke review en lifecyclebeheer). Hierdoor is de structurele borging nog onvoldoende aantoonbaar.
Bewaartermijnen	🟠	Bewaartermijnen zijn vastgelegd in processen en DPIA, maar uitvoering en naleving nog niet overal uniform aantoonbaar
Verstrekken politiegegevens	🟠	Registratie van verstrekkingen is gestart, maar nog niet volledig en deels buiten systemen georganiseerd (bijv. e-mail)
DPIA	🟢	DPIA uitgevoerd en formeel vastgesteld; aandachtspunten t.a.v. volledigheid en scope zijn bekend
Register van verwerkingen	🟢	Wpg-register uitgebreid met domein I
Logging & monitoring	🟠	Logging is aanwezig in afzonderlijke systemen, maar een volledig en operationeel logging- en controleproces is nog niet ingericht; structurele en aantoonbare uitvoering ontbreekt
Auditverplichting	🟠	Interimcontrole en deelcontroles uitgevoerd; volledige interne auditcyclus nog niet afgerond

Legenda:

	AANDACHT VEREIST VAN MANAGEMENT
	IN TE HALEN ACHTERSTAND
	OP SCHEMA

6.3 Taak van de FG

De FG houdt onafhankelijk toezicht op de naleving van de Wpg en voert periodiek controles uit op de wettelijke verplichtingen die hieruit voortvloeien.

Dit betreft onder meer toezicht op:

- het bestaan en de toepassing van beleid;
- de mate van bewustwording binnen de organisatie;
- het autorisatieproces;
- de rechtmatigheid en proportionaliteit van verwerkingen;
- de naleving van bewaartermijnen;
- de verstrekking en terbeschikkingstelling van politiegegevens;
- informatiebeveiliging en risicoanalyse;
- het register van verwerkingen;
- en de naleving van auditverplichtingen.

In 2025 lag de nadruk van het toezicht op:

- de uitbreiding naar domein I;
- de opvolging van auditbevindingen;
- en het versterken van de aantoonbaarheid van beheersmaatregelen.

6.3.1 Reikwijdte

Dit verslag beschrijft de stand van zaken ten aanzien van de naleving van de Wet politiegegevens (Wpg) binnen de gemeente Deurne. De beoordeling richt zich op de verwerkingen binnen domein III (onderwijs/leerplicht) en domein I (toezicht en handhaving door BOA’s).

In 2025 is sprake van een gewijzigde situatie ten opzichte van voorgaande jaren. De gemeente heeft ervoor gekozen het toezicht en de handhaving zelfstandig te organiseren door inzet van eigen BOA’s. Daarnaast is het systeem CityControl in gebruik genomen als primair systeem voor de verwerking van politiegegevens. Naast CityControl wordt gebruik gemaakt van andere systemen, waaronder JVS binnen het leerplichtdomein en Brickyard voor dossieropbouw en registraties.

In 2024 heeft een audit plaatsgevonden waarbij bevindingen zijn geconstateerd. In 2025 vindt een heraudit plaats, gericht op de opvolging van deze bevindingen. Dit verslag geeft een actuele beoordeling van de inrichting en werking van de Wpg-processen, met het oog op deze heraudit.

6.3.2. Algemeen beeld

Binnen de gemeente Deurne is zichtbaar dat de belangrijkste onderdelen voor de verwerking van politiegegevens zijn ingericht. Voor zowel leerplicht als toezicht en handhaving zijn processen beschreven, rollen belegd en systemen ingericht die de verwerking van gegevens ondersteunen. Er zijn DPIA's opgesteld voor de relevante domeinen en de verwerking van gegevens vindt in de praktijk grotendeels plaats binnen de daarvoor bedoelde systemen.

Tegelijkertijd blijkt dat de inrichting nog niet volledig structureel is geborgd. De nadruk ligt momenteel op het aanwezig zijn van processen en maatregelen, terwijl de periodieke controle, vastlegging en aantoonbaarheid daarvan nog onvoldoende zijn uitgewerkt. Dit betekent dat de gemeente in veel gevallen kan uitleggen hoe wordt gewerkt, maar nog niet overal kan aantonen dat dit structureel en controleerbaar gebeurt.

De belangrijkste opgave ligt daarmee in het versterken van de governance: het cyclisch controleren, bijsturen en vastleggen van de uitvoering van de Wpg-processen.

6.3.3. Domein III - Leerplicht

Binnen het leerplichtdomein worden persoonsgegevens verwerkt in het kader van de uitvoering van de Leerplichtwet. Deze verwerkingen hebben betrekking op onder andere leerlingen, ouders en verzorgers, en omvatten gegevens over schoolinschrijving, verzuim en eventuele handhavingsmaatregelen. De verwerking vindt plaats conform de landelijke Methodische Aanpak Schoolverzuim (MAS) en wordt ondersteund door systemen zoals JVS en DUO.

De verwerking valt onder de AVG zolang sprake is van toezicht en begeleiding. Op het moment dat wordt overgegaan tot strafrechtelijke handhaving, bijvoorbeeld bij het opmaken van een proces-verbaal of een Halt-verwijzing, is de Wpg van toepassing. Dit onderscheid is in de processen beschreven en vormt een belangrijk moment in de gegevensverwerking.

De procesbeschrijvingen voor absoluut en relatief verzuim zijn aanwezig en sluiten aan op de landelijke werkwijze. De DPIA voor leerplicht geeft inzicht in de aard van de gegevensverwerkingen, de betrokken partijen en de bijbehorende risico's. Hiermee is een belangrijke basis gelegd voor de rechtmatige verwerking van gegevens.

Uit de beoordeling blijkt echter dat de beschrijving van de verwerkingen nog niet volledig is. Niet alle gegevensstromen zijn afzonderlijk en volledig uitgewerkt en sommige verwerkingen, zoals gegevensuitwisseling met andere partijen, vallen deels buiten de huidige scope. Daarnaast is de scheiding tussen verschillende processen niet overal scherp aangebracht, waardoor het risico bestaat dat niet in alle gevallen duidelijk is onder welk regime (AVG of Wpg) wordt gewerkt.

Verder blijkt dat de structurele borging van maatregelen nog onvoldoende is uitgewerkt. Autorisaties zijn ingericht, maar worden niet periodiek en aantoonbaar herzien. Logging is aanwezig, maar wordt nog niet volgens een vastgestelde frequentie gecontroleerd. Ook de registratie van verstrekkingen van politiegegevens aan derden is nog niet volledig en vindt deels buiten de systemen plaats.

De uitvoering van het leerplichtproces is daarmee inhoudelijk op orde, maar de controle en aantoonbaarheid van de naleving van de Wpg vereisen verdere uitwerking. Voor een volledig compliant situatie is het noodzakelijk dat alle verwerkingen volledig in beeld worden gebracht, dat onderscheid tussen regimes expliciet wordt vastgelegd en dat periodieke controles structureel worden ingericht en gedocumenteerd.

6.3.4 Domein I - Toezicht en handhaving

Binnen domein I is in 2025 een nieuwe situatie ontstaan doordat de gemeente Deurne is overgestapt naar een eigen organisatie van toezicht en handhaving met BOA’s. De verwerking van gegevens vindt plaats in het kader van toezicht op de openbare ruimte en de handhaving van wet- en regelgeving.

De processen binnen dit domein beginnen doorgaans onder de AVG, bijvoorbeeld bij meldingen van overlast en eerste observaties. Zodra sprake is van een concrete verdenking of een strafrechtelijke afhandeling, zoals het opmaken van een proces-verbaal, valt de verwerking onder de Wpg. Deze overgang is in de processen beschreven en vormt een essentieel onderdeel van de rechtmatige gegevensverwerking.

De DPIA voor domein I geeft een volledig en gedetailleerd beeld van de gegevensverwerkingen, de betrokken partijen en de risico’s. De processen van melding, analyse, waarneming, handhaving en afhandeling zijn duidelijk uitgewerkt en sluiten aan bij de werkzaamheden van de BOA’s.

De gemeente Deurne maakt sinds 1 januari 2025 gebruik van CityControl voor de verwerking van politiegegevens binnen domein I. Uit het assurance-rapport van de leverancier blijkt dat het systeem in opzet en bestaan voldoet aan de eisen die vanuit de Wpg worden gesteld voor de serviceorganisatie.

Dit oordeel heeft echter uitsluitend betrekking op de beheersmaatregelen van de serviceorganisatie en niet op het gebruik van het systeem binnen de gemeente Deurne als

gebruikersorganisatie. Op grond van het normenkader (NOREA 3000D) blijft de gemeente zelf verantwoordelijk voor de inrichting, toepassing en controle van de verwerking van politiegegevens binnen de eigen organisatie.

Inmiddels is het systeem gedurende een jaar in gebruik binnen de gemeentelijke organisatie. De FG constateert dat de technische inrichting van het systeem passend is, maar dat de werking van de beheersmaatregelen binnen de eigen organisatie nog niet volledig aantoonbaar is. Structurele controles, zoals periodieke autorisatiereviews, loggingcontroles en interne audits, zijn nog niet volledig ingericht en uitgevoerd. Hierdoor kan nog niet worden vastgesteld dat de verwerking van politiegegevens binnen de gemeente in de praktijk volledig voldoet aan de eisen van de Wpg.

Binnen de huidige werkwijze wordt gebruik gemaakt van Brickyard voor de vastlegging van dossiers. Uit het assurance-rapport van Brickyard blijkt dat op onderdelen sprake is van tekortkomingen, onder andere op het gebied van toegangsbeveiliging en het vastleggen van controlemaatregelen. Dit brengt het risico met zich mee dat gegevens buiten het primaire systeem worden verwerkt zonder volledige borging van de Wpg-eisen.

Daarnaast blijkt dat binnen domein I verdere uitwerking nodig is op het gebied van governance. De registratie van verstrekkingen van politiegegevens is nog niet volledig ingericht, de scheiding tussen AVG- en Wpg-verwerkingen is niet in alle gevallen expliciet vastgelegd en de structurele controle op logging en autorisaties is nog niet geborgd. Ook het gebruik van specifieke instrumenten, zoals signaleringslijsten, vereist nadere juridische en procedurele uitwerking.

De inrichting van het proces en de systemen is in belangrijke mate gerealiseerd. De structurele borging, controle en documentatie van de uitvoering zijn echter nog niet volledig uitgewerkt, waardoor de naleving van de Wpg nog niet volledig aantoonbaar is.

6.3.5 Overkoepelende beoordeling

Voor beide domeinen geldt dat de basis van de Wpg-naleving aanwezig is. Processen zijn beschreven, systemen zijn ingericht en medewerkers handelen in lijn met de beoogde werkwijze. De overgang naar CityControl en de inrichting van de BOA-organisatie vormen belangrijke stappen in de verdere professionalisering van de gegevensverwerking.

De belangrijkste tekortkoming ligt in het ontbreken van een structurele en aantoonbare borging van de maatregelen. Er is nog onvoldoende sprake van een cyclische aanpak waarbij periodiek wordt gecontroleerd of processen, autorisaties, logging en registraties daadwerkelijk conform de Wpg worden uitgevoerd. Daarnaast is de vastlegging van deze controles en de opvolging van bevindingen nog niet overal ingericht.

Ook is sprake van versnippering door het gebruik van meerdere systemen, waardoor het risico bestaat dat gegevens buiten de centrale systemen worden verwerkt zonder volledige controle en registratie.

6.3.6 Conclusie

De gemeente Deurne heeft de inrichting van de verwerking van politiegegevens binnen domein I en III in belangrijke mate op orde gebracht. De belangrijkste processen, systemen en maatregelen zijn aanwezig en sluiten aan bij de wettelijke vereisten.

Voor de heraudit voor Leerplicht in 2026 is het noodzakelijk dat de gemeente de volgende stap zet van inrichting naar structurele borging. Dit houdt in dat controles op autorisaties, logging, gegevensverwerking en verstrekkingen periodiek worden uitgevoerd, vastgelegd en geëvalueerd. Daarnaast moeten alle verwerkingen volledig in beeld zijn, moet het onderscheid tussen AVG en Wpg expliciet worden gemaakt en dient het gebruik van systemen centraal en beheerst plaats te vinden.

Binnen de huidige situatie wordt gewerkt met meerdere systemen voor de verwerking en vastlegging van politiegegevens, waaronder CityControl (in gebruik sinds 1 januari 2025) als primair systeem en Brickyard voor aanvullende dossiervorming. Dit vraagt om extra aandacht voor samenhang, volledigheid en centrale sturing, om te voorkomen dat gegevens buiten het primaire proces worden verwerkt zonder volledige borging van de Wpg-eisen.

Wanneer deze stappen worden gerealiseerd, kan de gemeente aantonen dat de verwerking van politiegegevens niet alleen is ingericht, maar ook duurzaam en controleerbaar wordt uitgevoerd.

6.4 Bevindingen en aanbevelingen 2025

6.4.1 Beleid

De Wpg verplicht de organisatie om beleid vast te stellen waarin is uitgewerkt hoe politiegegevens rechtmatig worden verwerkt en beschermd. Dit beleid dient actueel te zijn en aantoonbaar te worden toegepast in de praktijk.

In 2025 is zichtbaar dat de organisatie hierin verdere stappen heeft gezet. Met de uitbreiding naar domein I (toezicht en handhaving in de openbare ruimte) zijn aanvullende werkprocessen en beleidskaders opgesteld. Daarnaast is voorzien in een jaarlijkse actualisatie van beleid, waarmee invulling wordt gegeven aan het onderhoud van de documentatie.

De FG constateert echter dat de toepassing en toetsing van dit beleid nog onvoldoende structureel is geborgd. De nadruk ligt op de aanwezigheid van beleid en processen, terwijl periodieke controle op naleving en evaluatie van de werking nog beperkt aantoonbaar is. Hierdoor kan niet in alle gevallen worden vastgesteld dat het beleid consistent wordt toegepast binnen zowel domein I als domein III.

Daarmee voldoet de organisatie in opzet aan de wettelijke verplichting, maar is de structurele naleving nog niet volledig geborgd.

Aanbeveling:
Zorg voor een vaste governancecyclus waarin beleid jaarlijks wordt geëvalueerd, geactualiseerd en aantoonbaar wordt getoetst op toepassing in de praktijk binnen alle Wpg-domeinen.

6.4.2 Bewustwording

De Wpg vereist dat medewerkers die met politiegegevens werken beschikken over voldoende kennis van de wetgeving en de risico's van gegevensverwerking. Dit vraagt om structurele training en aantoonbare bewustwording.

In 2025 is zichtbaar dat de kennis binnen de organisatie is toegenomen. Met name door de implementatie van nieuwe processen binnen domein I en de overgang naar CityControl, evenals de uitvoering van audits en DPIA's, hebben betrokken medewerkers meer inzicht gekregen in hun rol en verantwoordelijkheden.

De FG constateert echter dat deze bewustwording nog niet structureel is ingericht. Er is geen organisatiebreed, doorlopend trainingsprogramma en deelname wordt niet centraal geregistreerd. Hierdoor is niet aantoonbaar dat alle relevante medewerkers, inclusief nieuwe BOA's en ondersteunende functies, structureel voldoen aan de vereiste kennisniveaus.

Dit betekent dat de organisatie nog niet volledig voldoet aan de bewustwordingsverplichting uit de Wpg.

Aanbeveling:
Richt een structureel trainingsprogramma in voor alle medewerkers die met politiegegevens werken en leg deelname en kennisniveau centraal en aantoonbaar vast.

6.4.3 Autorisatieproces

De Wpg stelt dat alleen geautoriseerde medewerkers toegang mogen hebben tot politiegegevens en dat deze autorisaties moeten aansluiten bij de functie en taak van de medewerker.

In 2025 zijn duidelijke verbeteringen gerealiseerd. Autorisaties zijn opgeschoond en opnieuw ingericht, waarbij beter wordt aangesloten op functies en verantwoordelijkheden binnen zowel leerplicht (domein III) als toezicht en handhaving (domein I). Autorisaties zijn binnen het huidige systeem ingericht conform rollen, passend bij de mogelijkheden van het systeem.

Daarnaast vinden periodieke controles plaats, onder andere via maandelijkse controlelijsten vanuit het JVS-systeem. Dit draagt bij aan het inzicht in de juistheid en actualiteit van autorisaties.

De FG constateert echter dat de borging van het autorisatieproces nog grotendeels handmatig en reactief plaatsvindt en niet aantoonbaar is verankerd in een structureel proces. Op basis van de beschikbare informatie kan niet worden vastgesteld dat de beoordeling en opvolging van de uitgevoerde controles structureel wordt vastgelegd en gedocumenteerd.

Ook is de koppeling met HR-processen (zoals in-, door- en uitstroom) nog niet volledig geborgd en ontbreekt een integraal lifecyclebeheer van autorisaties. Hierdoor bestaat het risico dat autorisaties na verloop van tijd niet meer aansluiten bij de feitelijke situatie.

De inrichting van autorisaties is daarmee op orde, maar de structurele beheersing en aantoonbare borging van het proces zijn nog onvoldoende ontwikkeld.

Aanbeveling:

Borg het autorisatieproces structureel door het uitvoeren en vastleggen van periodieke autorisatiereviews, het formaliseren van de beoordeling en opvolging van controles (zoals de JVS-controlelijsten) en het koppelen van autorisatiebeheer aan HR-processen. Zorg daarnaast voor aantoonbare documentatie van controles en wijzigingen, zodat de organisatie inzichtelijk kan maken dat autorisaties actueel en passend zijn.

6.4.4 Bewaartermijnen

De Wpg verplicht organisaties om politiegegevens niet langer te bewaren dan noodzakelijk en om bewaartermijnen correct toe te passen en te handhaven.

In 2025 zijn bewaartermijnen vastgelegd in processen, DPIA’s en het register van verwerkingen. Hiermee is een belangrijke stap gezet in de inrichting van deze verplichting.

De FG constateert echter dat de uitvoering nog niet volledig uniform en technisch geborgd is. In sommige systemen, waaronder ondersteunende systemen naast CityControl, zijn bewaartermijnen niet correct geconfigureerd of ontbreekt automatische vernietiging. In enkele gevallen worden gegevens aanzienlijk langer bewaard dan toegestaan, wat niet in lijn is met de uitgangspunten van de Wpg.

Hierdoor bestaat een concreet risico op te lange bewaartermijnen en daarmee onrechtmatige verwerking van politiegegevens.

Aanbeveling:
Voer periodieke controles uit op bewaartermijnen in alle gebruikte systemen en implementeer waar mogelijk automatische vernietiging of signalering van verwijdermomenten.

6.4.5 Verstrekken van politiegegevens

De Wpg stelt strikte eisen aan het verstrekken van politiegegevens aan derden. Deze verstrekkingen moeten rechtmatig zijn, noodzakelijk en aantoonbaar worden vastgelegd.

In 2025 is gestart met het gebruik van standaardformulieren en het registreren van verstrekkingen, met name binnen domein I. Dit vormt een duidelijke verbetering ten opzichte van de eerdere situatie.

De FG constateert echter dat de registratie nog niet volledig en uniform plaatsvindt. In de praktijk worden verstrekkingen nog deels buiten de formele processen afgehandeld, bijvoorbeeld via e-mail, en niet altijd centraal geregistreerd. Hierdoor ontbreekt een volledig en betrouwbaar overzicht van alle verstrekkingen.

Dit betekent dat de organisatie nog niet volledig kan aantonen dat verstrekkingen rechtmatig en conform de Wpg plaatsvinden.

Aanbeveling:
Richt een centraal en uniform verstrekkingenregister in, borg dat alle verstrekkingen via dit proces verlopen en voorkom verwerking buiten de vastgestelde systemen en procedures.

6.4.6 DPIA

De Wpg vereist dat voor verwerkingen met een verhoogd risico een DPIA wordt uitgevoerd en dat de daarin opgenomen maatregelen worden opgevolgd.

In 2025 zijn DPIA’s opgesteld voor zowel domein III (leerplicht) als domein I (toezicht en handhaving). Hiermee is invulling gegeven aan deze verplichting en is inzicht verkregen in risico’s en benodigde maatregelen.

De FG constateert echter dat de borging van het DPIA-proces nog aandacht behoeft. Met name de periodieke herbeoordeling van DPIA’s en de structurele opvolging van de daarin opgenomen maatregelen zijn nog niet vastgelegd in een vaste cyclus. Ook is niet in alle gevallen aantoonbaar dat alle relevante verwerkingen volledig binnen de DPIA’s zijn opgenomen.

Hierdoor bestaat het risico dat risico's onvoldoende worden gemonitord en maatregelen niet tijdig worden geactualiseerd.

Aanbeveling:
Richt een structurele cyclus in voor herbeoordeling van DPIA's en borg de opvolging en monitoring van maatregelen aantoonbaar.

6.4.7 Register van verwerkingen

De Wpg verplicht tot het bijhouden van een actueel en volledig register van alle verwerkingen van politiegegevens.

In 2025 is het register uitgebreid met de verwerkingen binnen domein I, waardoor het inzicht in de gegevensverwerkingen is toegenomen.

De FG constateert echter dat het register nog niet volledig actueel en volledig is. De actualisatie vindt grotendeels handmatig plaats en is niet structureel gekoppeld aan wijzigingen in processen, systemen of DPIA's. Hierdoor bestaat het risico dat nieuwe of gewijzigde verwerkingen niet tijdig worden opgenomen.

Dit betekent dat de organisatie nog niet volledig kan aantonen dat alle verwerkingen correct en volledig zijn geregistreerd.

Aanbeveling:
Koppel de actualisatie van het register aan proceswijzigingen, DPIA's en systeemwijzigingen en voer periodieke controles uit op volledigheid en actualiteit.

6.4.8 Logging en monitoring

De Wpg verplicht dat alle raadplegingen en verwerkingen van politiegegevens worden gelogd en dat deze logging periodiek wordt gecontroleerd.

In 2025 kan op basis van de beschikbare informatie niet worden vastgesteld dat logging en monitoring structureel zijn ingericht en uitgevoerd binnen de organisatie. Voor zover bekend is nog geen sprake van een volledig en operationeel logging- en controleproces voor alle relevante systemen en verwerkingen van politiegegevens.

De FG constateert dat hierdoor niet aantoonbaar is dat raadplegingen van politiegegevens systematisch worden vastgelegd, gecontroleerd en beoordeeld. Ook ontbreekt een structureel proces voor het analyseren van logginggegevens en het opvolgen van eventuele afwijkingen.

Hierdoor bestaat het risico dat onrechtmatige toegang tot of misbruik van politiegegevens niet tijdig wordt gesignaleerd en opgevolgd.

Aanbeveling:

Richt een structureel logging- en controleproces in voor alle systemen waarin politiegegevens worden verwerkt. Zorg daarbij voor een vaste frequentie van controles, duidelijke vastlegging van bevindingen en opvolging van afwijkingen, en borg dit binnen de reguliere management- en controlcyclus.

6.4.9 Auditverplichting

De Wpg verplicht organisaties tot het uitvoeren van periodieke audits op de naleving van de wet.

In 2025 is een interimcontrole uitgevoerd en is gestart met de opvolging van eerder geconstateerde bevindingen. Daarnaast wordt gebruik gemaakt van externe assurance-rapportages voor systemen zoals CityControl en Brickyard.

De FG constateert dat de interne audit voor domein I nog niet volledig is uitgevoerd en dat de opvolging van bevindingen nog niet structureel wordt gemonitord en vastgelegd. Hierdoor is de naleving van de Wpg nog niet volledig en integraal getoetst voor alle relevante domeinen.

Met het oog op de heraudit in 2025 is het van belang dat de organisatie de opvolging van bevindingen aantoonbaar afrondt en borgt.

Aanbeveling:
Voer de interne audit voor domein I volledig uit, borg de opvolging van bevindingen in een structureel proces en zorg voor aantoonbare voortgang richting de heraudit.

7 Deel C: Ontwikkelingen en toezicht

7.1 Inleiding

In dit hoofdstuk worden de belangrijkste ontwikkelingen beschreven die van invloed zijn op de naleving van de AVG binnen de gemeente. Het gaat hierbij om technologische, juridische en organisatorische ontwikkelingen, evenals de bevindingen uit de toezichtactiviteiten van de FG.

De ontwikkelingen geven richting aan de eisen die aan de organisatie worden gesteld en plaatsen de bevindingen uit dit verslag in een breder kader.

7.2 Ontwikkelingen rondom AI en algoritmen

Een belangrijke ontwikkeling in het verslagjaar is de toenemende inzet van algoritmen en kunstmatige intelligentie (AI) binnen overheden. Deze toepassingen worden gebruikt om processen te ondersteunen, risico's te signaleren en dienstverlening te verbeteren.

Tegelijkertijd blijkt uit landelijke onderzoeken dat gemeenten moeite hebben om deze toepassingen volledig in lijn met de AVG toe te passen. In veel gevallen ontbreekt inzicht in welke algoritmen worden gebruikt, is de juridische grondslag onvoldoende concreet onderbouwd en worden risicoanalyses, zoals DPIA's, niet altijd tijdig uitgevoerd.

Dit betekent dat het risico bestaat dat algoritmen worden ingezet zonder dat voldoende is vastgesteld of deze noodzakelijk en proportioneel zijn. Daarnaast bestaat het risico op (indirecte) discriminatie, met name bij toepassingen waarbij gebruik wordt gemaakt van risicoprofielen op basis van historische gegevens.

Voor de gemeente betekent dit dat de inzet van AI en algoritmen niet alleen een technische ontwikkeling is, maar nadrukkelijk een privacy- en governancevraagstuk. Van de organisatie wordt verwacht dat zij inzicht heeft in deze toepassingen, risico's vooraf beoordeelt en transparant is richting burgers.

7.3 Toegenomen aandacht vanuit de Autoriteit Persoonsgegevens

De Autoriteit Persoonsgegevens (AP) heeft in recente publicaties aangegeven dat het toezicht zich in toenemende mate richt op grootschalige gegevensverwerkingen, AI-toepassingen en het koppelen van gegevensbestanden.

De AP waarschuwt dat het massaal verzamelen en combineren van persoonsgegevens kan leiden tot risico's voor grondrechten, zoals privacy, gelijke behandeling en vrijheid van

meningsuiting. Daarbij wordt expliciet gewezen op het risico dat burgers zich anders gaan gedragen wanneer zij het gevoel hebben dat zij worden gemonitord.

De AP benadrukt dat organisaties niet alleen moeten voldoen aan de AVG, maar dit ook moeten kunnen aantonen. Dit betekent dat organisaties vooraf moeten kunnen onderbouwen:

- waarom een verwerking noodzakelijk is;
- welke risico's er zijn;
- en welke maatregelen zijn getroffen om deze risico's te beperken.

Voor de gemeente betekent dit dat het belang van aantoonbaarheid en onderbouwing verder toeneemt en dat met name risicovolle verwerkingen onder een vergrootglas liggen.

7.4 Ontwikkelingen in samenwerking en gegevensuitwisseling

Een andere belangrijke ontwikkeling betreft de complexiteit van samenwerking tussen organisaties. Gemeenten werken steeds vaker samen met andere overheden en externe partijen, waarbij persoonsgegevens worden gedeeld.

Dit brengt risico's met zich mee op het gebied van rolverdeling, verantwoordelijkheden en rechtmatigheid. In de praktijk blijkt dat tijdelijke oplossingen of constructies soms langer blijven bestaan dan oorspronkelijk bedoeld, zonder dat opnieuw wordt beoordeeld of deze nog voldoen aan de AVG.

Voor de gemeente betekent dit dat er structureel aandacht moet zijn voor:

- het vaststellen van rollen (verwerkingsverantwoordelijke/verwerker);
- het borgen van afspraken;
- en het periodiek herbeoordelen van bestaande constructies.

7.5 Digitale afhankelijkheid en leveranciers

De gemeente is in toenemende mate afhankelijk van digitale systemen en externe leveranciers voor de uitvoering van haar taken. Hierbij worden persoonsgegevens vaak verwerkt in systemen die niet volledig onder directe controle van de gemeente vallen.

Deze afhankelijkheid brengt risico's met zich mee, onder andere op het gebied van transparantie, beveiliging en controle over gegevens.

De AP wijst erop dat organisaties zich bewust moeten zijn van deze afhankelijkheid en hier actief op moeten sturen. Voor de gemeente betekent dit dat keuzes voor systemen en

leveranciers niet alleen technisch of financieel moeten worden beoordeeld, maar ook vanuit privacy- en gegevensbeschermingsperspectief.

7.6 Toezichtactiviteiten van de FG

In het verslagjaar heeft de FG verschillende toezichtactiviteiten uitgevoerd gericht op de naleving van de AVG en de bescherming van persoonsgegevens. Deze activiteiten hadden betrekking op zowel bestaande verwerkingen als nieuwe ontwikkelingen binnen de organisatie.

7.6.1 Gebruik van BRP-gegevens via de makelaar van Deurne

De Functionaris Gegevensbescherming (FG) concludeert dat de beschreven constructie niet in overeenstemming is met de geldende wet- en regelgeving, in het bijzonder de Algemene verordening gegevensbescherming (AVG) en de Wet basisregistratie personen (Wet BRP).

In het kader van de Wet BRP geldt dat verstrekking en verwerking van persoonsgegevens uitsluitend is toegestaan voor bestuursorganen die daartoe wettelijk zijn aangewezen, en enkel voor zover dit noodzakelijk is voor de uitvoering van hun publiekrechtelijke taak. Tegen deze achtergrond stelt de FG vast dat:

- onvoldoende is onderbouwd op welke specifieke wettelijke grondslag binnen de Wet BRP de gegevensverwerking berust;
- niet helder is welke partijen optreden als verwerkingsverantwoordelijke, afnemer of eventuele verwerker, en hoe de verantwoordelijkheden juridisch zijn belegd;
- niet is aangetoond dat de verwerking voldoet aan de eisen van doelbinding, noodzakelijkheid en proportionaliteit, zoals vereist onder zowel de AVG als de Wet BRP.

Daarnaast merkt de FG op dat het stelsel van de Wet BRP uitgaat van autorisatie per afzonderlijk bestuursorgaan. Dit impliceert dat gegevensverstrekking in beginsel plaatsvindt aan individueel gerechtigde afnemers, en niet via een generieke of centrale doorleverconstructie zonder expliciete wettelijke basis.

7.6.2 Pilot met het gebruik van Copilot

In het verslagjaar is binnen de organisatie een pilot uitgevoerd met het gebruik van Copilot, waarbij medewerkers gebruik maken van AI-functionaliteiten die mogelijk persoonsgegevens verwerken.

De FG heeft toezicht gehouden op deze pilot, met name gericht op de vraag in hoeverre de verwerking van persoonsgegevens binnen deze toepassing voldoet aan de AVG.

Daarbij is onder andere gekeken naar:

- welke gegevens in de tool worden ingevoerd;
- of deze gegevens mogelijk worden verwerkt door externe partijen;
- hoe logging en opslag van gegevens plaatsvinden;
- en in hoeverre sprake is van gebruik van gevoelige of vertrouwelijke informatie.

Uit de beoordeling blijkt dat de inzet van deze technologie risico's met zich meebrengt, met name op het gebied van:

- onbedoelde gegevensdeling met externe leveranciers;
- onvoldoende inzicht in de verdere verwerking van gegevens;
- en het gebruik van persoonsgegevens in een omgeving die niet volledig onder controle staat van de organisatie.

Hoewel voor de pilot een DPIA is uitgevoerd, constateert de FG dat de toepassing van maatregelen en het bewustzijn bij gebruikers aandachtspunten blijven.

De FG benadrukt dat bij dit soort toepassingen privacy vanaf de start moet worden meegenomen en dat het gebruik van AI-tools niet zonder duidelijke kaders en toezicht mag plaatsvinden.

7.6.3 Controle op personeelsvolgsystemen

Uit de controle blijkt dat de betreffende systemen in gebruik zijn en dat persoonsgegevens worden verwerkt binnen de HR-processen conform de beschreven doeleinden.

Tegelijkertijd constateert de FG dat:

- de periodieke controle op autorisaties niet in alle gevallen organisatiebreed aantoonbaar en uniform is ingericht;
- de onderbouwing van dataminimalisatie en proportionaliteit in sommige gevallen nadere uitwerking behoeft, waardoor niet altijd expliciet inzichtelijk is dat de verwerking beperkt blijft tot wat strikt noodzakelijk is.

De FG kwalificeert dit als een aandachtspunt op het gebied van toegangsbeheer en dataminimalisatie, waarbij met name behoefte bestaat aan verdere concretisering, documentatie en borging van deze principes.

7.6.4 Beoordeling van meldingen en signalen

In het verslagjaar heeft de FG verschillende meldingen en signalen ontvangen met betrekking tot de verwerking van persoonsgegevens.

Deze meldingen hadden onder andere betrekking op:

- mogelijke datalekken;
- vragen over rechtmatigheid van gegevensverwerking;
- en signalen vanuit de organisatie over het gebruik van systemen en gegevens.

De FG heeft deze meldingen beoordeeld en waar nodig nader onderzoek gedaan. In voorkomende gevallen zijn adviezen gegeven om risico's te beperken of werkwijzen aan te passen.

Uit deze meldingen komt een terugkerend beeld naar voren waarbij incidenten vaak ontstaan door:

- menselijke fouten (bijvoorbeeld verkeerd adresseren);
- onduidelijkheid over processen;
- of onvoldoende bewustzijn bij medewerkers.

Hoewel meldingen worden opgepakt en afgehandeld, constateert de FG dat structurele analyse en terugkoppeling nog beperkt plaatsvinden. Hierdoor worden lessen uit incidenten nog onvoldoende organisatiebreed benut.

7.6.5 Samenhang en bevindingen

De uitgevoerde toezichtactiviteiten laten een consistent beeld zien.

Binnen de organisatie zijn belangrijke privacy-instrumenten en processen aanwezig. Tegelijkertijd blijkt uit de praktijk dat:

- nieuwe toepassingen (zoals AI) sneller worden ingevoerd dan dat governance is ingericht;
- bestaande constructies (zoals BRP-koppelingen) blijven bestaan zonder herbeoordeling;
- en dat beheersmaatregelen (zoals autorisaties en DPIA-opvolging) niet altijd structureel worden geborgd.

De FG concludeert dat de organisatie zich in een fase bevindt waarin de basis aanwezig is, maar waarin verdere professionalisering nodig is om te komen tot structurele beheersing en aantoonbaarheid.

7.7 Betekenis voor de organisatie

De beschreven ontwikkelingen en toezichtbevindingen laten zien dat de eisen aan gegevensbescherming toenemen en concreter worden.

Waar voorheen de nadruk lag op het opstellen van beleid en het inrichten van processen, ligt de nadruk nu op:

- het daadwerkelijk beheersen van risico's;
- het hebben van inzicht in gegevensverwerkingen;
- en het aantoonbaar voldoen aan de AVG.

Voor de gemeente betekent dit dat de komende periode de focus moet liggen op het versterken van de samenhang tussen beleid, processen en systemen, en op het vergroten van de aantoonbaarheid van genomen maatregelen.

Alleen op die manier kan de gemeente blijven voldoen aan de wettelijke verplichtingen en inspelen op de toenemende verwachtingen vanuit toezicht en samenleving.

7.7.1 Wat betekent dit concreet voor de organisatie

De beschreven ontwikkelingen en toezichtbevindingen vragen om een gerichte doorvertaling naar de praktijk. Voor de organisatie betekent dit concreet dat:

- Bij de inzet van AI en algoritmen privacy en grondrechten vanaf de start moeten worden meegenomen, waarbij DPIA's tijdig worden uitgevoerd en duidelijke kaders worden gesteld aan het gebruik van deze toepassingen.
- Bestaande gegevensverwerkingen en samenwerkingsconstructies, zoals gegevensuitwisseling met andere organisaties, periodiek moeten worden herbeoordeeld op rechtmatigheid, noodzaak en proportionaliteit.
- De organisatie actief moet sturen op transparantie en inzicht in gegevensverwerkingen, zodat duidelijk is welke gegevens worden verwerkt, met welk doel en op basis van welke grondslag.
- Bij de inzet van externe leveranciers en systemen nadrukkelijk aandacht moet zijn voor gegevensbescherming, controle en afhankelijkheden, en dat dit onderdeel wordt van besluitvorming.
- De focus verschuift van het inrichten van beleid en processen naar het aantoonbaar beheersen van risico's en het structureel kunnen verantwoorden van gemaakte keuzes.

Deze ontwikkeling vraagt om versterking van governance, sturing en samenhang binnen de organisatie.

Bijlagen (2)

Bijlage 1 - Stand van zaken AVG per thema
Bijlage 2 - Kengetallen

Bijlage 1 - Stand van zaken AVG per thema

Deze bijlage bevat een nadere onderbouwing van de beoordeling per AVG-thema zoals opgenomen in hoofdstuk 5. De beoordeling is gebaseerd op beschikbare registraties, documentatie en uitgevoerde controles.

De focus ligt op de mate waarin:

- wettelijke verplichtingen zijn ingevuld;
- maatregelen zijn ingericht;
- en aantoonbaar is dat deze maatregelen functioneren.

1. Beleid

Wat moet (AVG):
De organisatie moet passende organisatorische maatregelen treffen (artikel 24 AVG), waaronder vastgesteld, geïmplementeerd en toegepast beleid.

Wat is aanwezig:

- Privacybeleid is vastgesteld
- Rollen en uitgangspunten zijn beschreven

Wat ontbreekt/ risico:

- Niet aantoonbaar dat beleid structureel wordt gecommuniceerd binnen de organisatie
- Niet aantoonbaar dat beleid wordt toegepast in werkprocessen
- Geen aantoonbare periodieke toetsing op naleving en actualiteit

Onderbouwing oordeel:
Het beleid is aanwezig en wordt onderhouden, maar de toepassing en borging zijn niet aantoonbaar. Hierdoor kan niet worden vastgesteld dat wordt voldaan aan artikel 24 AVG.

Beoordeling: 🟠

2. Processen (verwerkingsregister & DPIA)

Wat moet (AVG):

- Een volledig en actueel verwerkingsregister (artikel 30 AVG)
- Het uitvoeren van DPIA’s bij verwerkingen met een hoog risico (artikel 35 AVG)

Wat is aanwezig:

- Verwerkingsregister aanwezig
- DPIA's uitgevoerd
- DPIA-register aanwezig

Wat ontbreekt/ risico:

- Niet vastgesteld dat het verwerkingsregister volledig en actueel is
- Actualisatie is afhankelijk van input vanuit de organisatie en niet structureel geborgd
- Niet aantoonbaar dat alle hoog-risico verwerkingen zijn geïdentificeerd en beoordeeld
- Niet aantoonbaar dat maatregelen uit DPIA's structureel worden opgevolgd en gemonitord

Onderbouwing oordeel:
De processen zijn in opzet aanwezig, maar de volledigheid en werking zijn niet aantoonbaar. Hierdoor kan niet worden vastgesteld dat de organisatie voldoet aan artikel 30 en 35 AVG en ontbreekt aantoonbare grip op verwerkingen en risico's.

Beoordeling: 🔴

3. Organisatorische inbedding

Wat moet (AVG):
Privacy moet structureel organisatorisch zijn ingebed, inclusief rollen, verantwoordelijkheden, bewustwording en betrokkenheid van de FG.

Wat is aanwezig:

- FG, Privacy Officer en CISO aanwezig
- Basis governance ingericht

Wat ontbreekt/ risico:

- Niet aantoonbaar dat privacy structureel en tijdig wordt betrokken bij projecten en besluitvorming
- Wisselingen in rollen beïnvloeden de continuïteit van de inrichting
- Niet aantoonbaar dat bewustwording en training structureel worden gemonitord

Onderbouwing oordeel:
De organisatorische structuur is aanwezig, maar de werking en borging zijn niet aantoonbaar. Hierdoor kan niet worden vastgesteld dat privacy structureel onderdeel is van de organisatie.

Beoordeling: 🟠

4. Rechten van betrokkenen

Wat moet (AVG):
De rechten van betrokkenen moeten uitvoerbaar zijn ingericht (artikelen 12-23 AVG).

Wat is aanwezig:

- Proces ingericht
- Verzoeken worden geregistreerd
- Termijnen worden gehaald

Wat ontbreekt/ risico:

- Beperkte zichtbaarheid en herkenning van verzoeken binnen de organisatie
- Technische ondersteuning is niet in alle gevallen volledig geborgd

Onderbouwing oordeel:
Op basis van beschikbare registraties functioneert het proces en worden verzoeken binnen de wettelijke termijnen afgehandeld. Hiermee wordt voldaan aan de wettelijke verplichtingen.

Beoordeling: 🟢

5. Samenwerking (verwerkers)

Wat moet (AVG):

- Duidelijke rolverdeling (artikel 4 AVG)
- Verwerkersovereenkomsten (artikel 28 AVG)
- Toezicht op verwerkers

Wat is aanwezig:

- Contractenregister
- Verwerkersovereenkomsten

Wat ontbreekt/ risico:

- Geen aantoonbare volledige koppeling tussen verwerkingsregister en contractenregister
- Onvoldoende aantoonbaar inzicht in rollen en verantwoordelijkheden van partijen
- Niet aantoonbaar dat naleving door leveranciers structureel wordt gecontroleerd

- Contracten zonder expliciete koppeling aan verwerkingen

Onderbouwing oordeel:
Er is onvoldoende samenhang en controle op externe verwerkingen. Hierdoor kan niet worden vastgesteld dat wordt voldaan aan artikel 28 AVG en ontbreekt aantoonbare grip op verwerkingen door derden.

Beoordeling: 🟠

6. Gegevensbescherming

Wat moet (AVG):
De organisatie moet passende technische en organisatorische maatregelen treffen en een datalekproces inrichten (artikel 32 AVG).

Wat is aanwezig:

- Incidentproces ingericht
- Datalekken worden geregistreerd

Wat ontbreekt/ risico:

- Geen aantoonbare structurele analyse van incidenten en datalekken
- Geen aantoonbare structurele verbetercyclus (PDCA)

Onderbouwing oordeel:
De inrichting is primair reactief. Het is niet aantoonbaar dat incidenten structureel worden geanalyseerd en leiden tot verbetering. Hierdoor kan niet worden vastgesteld dat maatregelen effectief bijdragen aan risicobeheersing.

Beoordeling: 🟠

7. Verantwoording (accountability)

Wat moet (AVG):
De organisatie moet kunnen aantonen dat zij voldoet aan de AVG (artikel 5 lid 2 AVG).

Wat is aanwezig:

- Verwerkingsregister
- DPIA’s
- Incidentregistraties

Wat ontbreekt/ risico:

- Geen aantoonbare samenhang tussen instrumenten
- Niet vastgesteld dat het verwerkingsregister volledig is
- Niet aantoonbaar dat DPIA-maatregelen worden opgevolgd
- Geen aantoonbare structurele controle op de werking van maatregelen

Onderbouwing oordeel:
De benodigde instrumenten zijn aanwezig, maar functioneren niet aantoonbaar in samenhang. Hierdoor ontbreekt een integraal en aantoonbaar beeld van de naleving en kan niet worden vastgesteld dat wordt voldaan aan de verantwoordingsplicht.

Beoordeling: 🔴

Bijlage 2 Kengetallen

Overzicht privacyincidenten

Dit betreft zowel datalekken als beveiligingsincidenten met mogelijke impact op persoonsgegevens.

Privacyincidenten	2025
Totaal	22
Meldingen AP	5
Betrokkenen geïnformeerd	8

Overzicht DPIA's

Onderwerp DPIA	Datum	Status	Advies FG
Wgs Fase 3+4 Saneringskrediet en financieel beheer (DPIA AVG)	03-02-2025	Afgerond	Ja
Gehandicapten Parkeerkaart (GPK) (DPIA AVG)	18-02-2025	Afgerond	Ja
Wpg Domein 1 Handhaving (DPIA Wpg)	20-02-2025	Afgerond	Ja
Agressieprotocol (DPIA AVG)	13-05-2025	Afgerond	Nee
Cameratoezicht tijdelijk centrum (DPIA AVG)	28-11-2025	Afgerond	Ja
Tribe CRM (DPIA AVG)	15-12-2025	Afgerond	Ja

Overzicht rechten van betrokkenen

Type verzoek	Aantal
Inzage	1
Correctie	1
Verwijdering	1

Overzicht meldingen en klachten

Onderwerp	Omschrijving	Afhandeling
Publicatie koopakte	Publicatie van een koopakte met persoonsgegevens in het raadsinformatiesysteem.	Onderzocht en maatregelen genomen.

Samenwerkingspartner Groene Zone	Klacht over verstrekking van contractinformatie zonder verificatie van identiteit.	Onderzocht en afgehandeld.
Zorg Deurne	Klacht bij de Autoriteit Persoonsgegevens over delen van persoonsgegevens.	Onderzoek afgerond.