

Organisatieonderdeel: Dienstverlening
Behandelaar: S. Beekman
Telefoonnummer:

Voorstelnr. 4513
Barneveld, 13 januari 2026
Portefeuillehouder: W. Oosterwijk

☐ Ter kennisname naar de raad
Nummer beleidsproduct:

☐ Op overzicht Bestaand beleid (website)

Onderwerp: **Jaarverslag Functionaris Gegevensbescherming 2025**

Gevraagde beslissing:

1. Het bijgevoegde Jaarverslag FG 2025 vast te stellen;
2. De memo en het Jaarverslag FG 2025 via rubriek B ter kennisname te doen toekomen aan de gemeenteraad;
3. Ter voldoening aan de verplichte registratie en publicatie het Jaarverslag FG 2025 op de website van de gemeente te plaatsen.

1. Inleiding

Het jaarverslag Functionaris Gegevensbescherming 2025 – dat mede in samenwerking met de Privacy Officer (PO) en de Chief Information Security Officer (CISO) – door de Functionaris Gegevensbescherming (FG) is opgesteld, geeft weer wat de Gemeente Barneveld in 2025 heeft ondernomen om aan de vereisten van de Algemene Verordening Gegevensbescherming (AVG) en de Wet Politiegegevens (Wpg) te voldoen.

2. Beoogd effect

De bestuursorganen van de gemeente en de inwoners worden geïnformeerd over wat de Gemeente Barneveld in 2025 heeft ondernomen om aan de vereisten van de AVG en de Wpg te voldoen.

3. Argumenten

1.1. De rapportage geeft een goed inzicht in wat de Gemeente Barneveld in 2025 heeft ondernomen om aan de vereisten van de AVG en de Wpg te voldoen

In 2025 zijn de volgende zaken gerealiseerd:

- Het register van verwerkingen voor AVG en voor Wpg is volledig geactualiseerd.
- Er zijn nieuwe of geactualiseerde verwerkersovereenkomsten afgesloten met verwerkers.
- Ook zijn er intern veel adviezen gegeven en workshops gehouden over privacy en informatieveiligheid.
- De komst van Artificiële Intelligentie (AI) wordt sinds Q4 2024 ook meegenomen in de workshops, omdat dit impact heeft op de werkwijze in verschillende processen van de gemeente. Ook zijn er in 2025 meerdere AI-trainingen gegeven om aan de AI geletterdheid te kunnen voldoen. Daarbij is uitgelegd wat AI is en hoe de gemeente daarmee om moet gaan. Er is gekeken wat de (on)mogelijkheden, kansen en bedreigingen van het gebruik van AI voor de gemeente (kunnen) zijn.
- In Q1 2025 is het Toezichtplan FG 2025-2026 opgesteld. Dit toezichtplan geeft een helder overzicht van alle verschillende onderdelen waarop toezicht gehouden wordt en welke taken uitgevoerd moeten worden.
- Sinds 2022 wordt jaarlijks een interne en vierjaarlijks een externe audit uitgevoerd voor de Wpg. In 2025 is zowel een interne als een externe audit uitgevoerd.

2.1. Conform het Privacybeleid wordt de gemeenteraad geïnformeerd

De AVG, de Wpg en het Privacybeleid van de Gemeente Barneveld schrijven voor dat de FG jaarlijks voor 1 maart verslag uitbrengt aan de bestuursorganen. Het onderhavige verslag wordt dan ook uitgebracht aan het college van burgemeester en wethouders, de burgemeester en de gemeenteraad van Barneveld.

3.1 Publicatie van het jaarverslag op de website geeft openheid

Met het publiceren van het Jaarverslag FG 2025 voldoet het college aan de in de AVG, Wpg en het Privacybeleid opgenomen verplichting. Hiermee geeft uw college aan de inwoners en andere belangstellenden opening van zaken over wat de Gemeente Barneveld in 2025 heeft ondernomen om aan de vereisten van de AVG en de Wpg te voldoen. In het verslagjaar wordt toegelicht welke werkzaamheden in 2025 zijn uitgevoerd en wat de acties voor 2026 zijn.

4. Kanttekeningen

n.v.t.

5. Financiën

n.v.t.

6. Participatie en communicatie

n.v.t.

7. Uitvoering

n.v.t.

8. Bijlagen

1. Jaarverslag FG 2025
2. Memo aan raad

Raadsmemo Jaarverslag FG 2025

Datum: 3 februari 2026

Onderwerp: Jaarverslag Functionaris Gegevensbescherming 2025

Ter attentie van: De Raad

Afzender: College van Burgemeester en Wethouders

Portefeuillehouder W. Oosterwijk

Mail behandelaar fg@barneveld.nl Telefoonnummer (0342) 495 381 / 06 2165 7166

Samenvatting

Het jaarverslag Functionaris Gegevensbescherming 2025 – dat mede in samenwerking met de Privacy Officer (PO) en de Chief Information Security Officer (CISO) – door de Functionaris Gegevensbescherming (FG) is opgesteld, geeft weer wat de Gemeente Barneveld in 2025 heeft ondernomen om aan de vereisten van de Algemene Verordening Gegevensbescherming (AVG) en de Wet Politiegegevens (Wpg) te voldoen.

Doel

Het doel van de memo is om de raad te informeren over het jaarverslag. De AVG, de Wpg en het Privacybeleid van de Gemeente Barneveld schrijven voor dat de FG jaarlijks voor 1 maart verslag uitbrengt aan de bestuursorganen. Het onderhavige verslag wordt dan ook uitgebracht aan het college van burgemeester en wethouders, de burgemeester en de gemeenteraad van Barneveld.

Inhoud memo

In 2025 zijn de volgende zaken gerealiseerd:

- Het register van verwerkingen voor AVG en voor Wpg is volledig geactualiseerd.
- Er zijn nieuwe of geactualiseerde verwerkersovereenkomsten afgesloten met verwerkers.
- Ook zijn er intern veel adviezen gegeven en workshops gehouden over privacy en informatieveiligheid.
- De komst van Artificiële Intelligentie (AI) wordt sinds Q4 2024 ook meegenomen in de workshops, omdat dit impact heeft op de werkwijze in verschillende processen van de gemeente. Ook zijn er in 2025 meerdere AI-trainingen gegeven om aan de AI geletterdheid te kunnen voldoen. Daarbij is uitgelegd wat AI is en hoe de gemeente daarmee om moet gaan. Er is gekeken wat de (on)mogelijkheden, kansen en bedreigingen van het gebruik van AI voor de gemeente (kunnen) zijn.

- In Q1 2025 is het Toezichtplan FG 2025-2026 opgesteld. Dit toezichtplan geeft een helder overzicht van alle verschillende onderdelen waarop toezicht gehouden wordt en welke taken uitgevoerd moeten worden.
- Sinds 2022 wordt jaarlijks een interne en vierjaarlijks een externe audit uitgevoerd voor de Wpg. In 2025 is zowel een interne als een externe audit uitgevoerd.

Vervolg

Met het publiceren van het Jaarverslag FG 2025 op de website van de gemeente voldoet het college aan de in de AVG, Wpg en het Privacybeleid opgenomen informatieverplichting. Hiermee geeft het college aan uw raad en aan de inwoners en andere belangstellenden opening van zaken over wat de Gemeente Barneveld in 2025 heeft ondernomen om aan de vereisten van de AVG en de Wpg te voldoen. In het jaarverslag wordt toegelicht welke werkzaamheden in 2025 zijn uitgevoerd en wat de acties voor 2026 zijn.



Jaarverslag

Functionaris Gegevensbescherming 2025

Opdrachtgever:	gemeente Barneveld Bestuursondersteuning
Auteur:	Sascha Beekman, Functionaris Gegevensbescherming
Datum:	21 januari 2026

Inhoud

1.	Managementsamenvatting	4
2.	Wettelijk kader	4
2.1	AVG Algemeen.....	4
2.2	Wet politiegegevens	5
2.3	Toezichtskader AP: ontwikkelingen en gevolgen	5
2.3.1.	Samenvatting Jaarplan 2025 AP.....	5
2.3.2	inspectie AP	6
3.	Governance	6
3.1	Governance algemeen.....	6
3.2	Verantwoording Functionaris gegevensbescherming	6
3.3	Verantwoording Privacy Officer.....	7
3.4	Verantwoording CISO	8
3.5	Borging	8
4.	Werkzaamheden en bevindingen	10
4.1	Privacybeleid.....	10
4.2	Thuiswerken	10
4.3	Wpg- audit.....	10
4.3.1	Audits over 2021 tot en met 2024	10
4.3.2	Interne audit over 2025	11
4.3.3.	Externe audit over 2024.....	19
4.4	Register van verwerkingen	20
4.5	Meldingen datalekken	20
4.5.1	Cijfers AVG.....	20
4.5.2	Cijfers Wpg	20
4.6	Rechten van betrokkenen	20
4.6.1	AVG verzoeken	20
4.6.2	Wpg verzoeken	20
4.7	Bewaartermijnen	20
4.8	Verwerkers en verwerkersovereenkomsten	20
4.9	Privacy in het Sociaal Domein	21
4.10	Informatieveiligheid	21
4.11	Data Protection Impact Assessments.....	21

4.12	Bewustwording	24
4.13	Overige zaken	24
4.14	Te verwachten ontwikkelingen wet- en regelgeving	24
4.15	Evaluatie Toezichtplan 2025-2026	26
5.	Aanbevelingen en acties.....	28
5.1	Aanbevelingen.....	28
5.2	Acties voor 2026.....	29
BIJLAGE	Autoriteit Persoonsgegevens Jaarplan 2025	30

1. MANAGEMENTSAMENVATTING

Dit jaarverslag – dat mede in samenwerking met de Privacy Officer (PO) en de Chief Information Security Officer (CISO) – door de Functionaris Gegevensbescherming (FG) is opgesteld, geeft weer wat de Gemeente Barneveld in 2025 heeft ondernomen om aan de vereisten van de Algemene Verordening Gegevensbescherming (AVG) en de Wet Politiegegevens (Wpg) te voldoen.

Het register van verwerkingen bevat zowel de AVG verwerkingen als de Wpg verwerkingen en is in 2025 volledig geactualiseerd. Daarnaast zijn er nieuwe of geactualiseerde verwerkers-overeenkomsten afgesloten met verwerkers. Ook zijn er intern veel adviezen gegeven en workshops gehouden over privacy en informatieveiligheid, omdat deze onlosmakelijk met elkaar verbonden zijn en het belangrijk is dat het bewustzijn bij de medewerkers aanwezig is en dat ook blijft. Daarbij is niet alleen aandacht besteed aan de grondslag en doelbinding die aanwezig moet zijn voordat gegevens verwerkt mogen worden, welke gegevens verwerkt mogen worden en hoe lang deze bewaard mogen worden, maar ook is het belang onderstreept van een zorgvuldige verwerking en deling van gegevens door bijvoorbeeld gebruik te maken van beveiligd e-mailen. Voor de risico's die thuiswerken met zich meebrengt is regelmatig aandacht gevraagd.

De komst van Artificiële Intelligentie (AI) wordt sinds Q4 2024 ook meegenomen in de workshops, omdat dit impact heeft op de werkwijze in verschillende processen van de gemeente. Ook zijn er specifieke basis trainingen gegeven aan alle medewerkers om te voldoen aan de per 1 februari 2025 verplicht gestelde AI geletterdheid. Daarbij is uitgelegd wat AI is en hoe de gemeente daarmee om moet gaan. Er is gekeken wat de (on)mogelijkheden, kansen en bedreigingen van het gebruik van AI voor de gemeente (kunnen) zijn. Er wordt daarbij benadrukt dat er geen persoonsgegevens in AI gebruikt mogen worden. In 2025 is er een projectgroep ingericht die zich bezig houdt met het in kaart brengen van AI kansen, mogelijkheden, risico's en bedreigingen. Er lopen een aantal pilots om te beoordelen hoe AI in het werk gebruikt kan worden en wat wel en niet kan of mag met AI, zodat de dienstverlening geoptimaliseerd kan worden, waarbij de menselijke factor altijd aanwezig moet blijven.

In het Jaarverslag over 2024 is opgenomen dat er een Toezichtplan FG komt. Dat is in het eerste kwartaal van 2025 opgesteld voor de jaren 2025 en 2026. Dit toezichtplan geeft een helder overzicht van alle verschillende onderdelen waarop toezicht gehouden wordt en welke taken uitgevoerd moeten worden. Zoals aandacht hebben voor bewustwording, opleiding, en training, maar ook de jaarlijks uit te voeren periodieke controles, audits enzovoorts. Verderop wordt daar dieper op ingegaan.

Gedetailleerde bevindingen, conclusies en aanbevelingen zijn beschreven in hoofdstuk 4.

2. WETTELIJK KADER

2.1 AVG Algemeen

In de AVG zijn regels vastgelegd voor het verwerken van persoonsgegevens. Deze verordening voor de verwerking van persoonsgegevens kent een rechtstreekse werking voor de lidstaten van de Europese Unie. In de AVG worden de rechten van burgers versterkt en de AVG legt de nadruk op de eigen verantwoordingsplicht van organisaties die persoonsgegevens verwerken. Dit betekent dat organisaties bijvoorbeeld goed moeten vastleggen welke gegevens zij verwerken, met welk doel, hoe lang zij die gegevens bewaren, dat zij de gegevens goed beveiligen en met wie ze gegevens delen. De rechtstreekse werking van de AVG zorgt ervoor dat de regels voor bescherming van persoonsgegevens uniform zijn binnen de Europese Unie.

De AVG geeft een overkoepelend kader voor het verwerken van persoonsgegevens en is nader uitgewerkt in de Nederlandse Uitvoeringswet AVG. Daarnaast zijn er in materiewetgeving, zoals de Jeugdwet, de Wet maatschappelijke ondersteuning en de Wet Basisregistratie personen specifieke regels te vinden voor het verwerken van persoonsgegevens. De AVG hangt daar altijd als een paraplu boven. Dat betekent dat als persoonsgegevens verwerkt mogen worden op grond van de materiewetgeving, de bepalingen van de AVG daarboven blijven hangen. Er moet bijvoorbeeld altijd een rechtmatige grondslag zijn voor het verwerken van persoonsgegevens en persoonsgegevens mogen alleen worden verwerkt voor het doel waarvoor ze zijn verzameld.

2.2 Wet politiegegevens

Buitengewone opsporingsambtenaren (boa's) die voor hun opsporingstaak persoonsgegevens verwerken, vallen onder de Wpg. Boa's verwerken de politiegegevens onder beheer van hun werkgever en daarmee is de werkgever van de boa's de verwerkingsverantwoordelijke. Voor de gemeente Barneveld geldt dat zij als werkgever boa's openbare ruimte en leerplichtambtenaren in dienst heeft die bij het uitvoeren van hun taken politiegegevens verwerken. De Gemeente Barneveld is daarom verantwoordelijk voor het toezicht op de naleving van de Wpg. In de Wpg is ook een auditverplichting opgenomen voor werkgevers van boa's.

- Interne Wpg-audit: elk jaar. Dat betekent dat de werkgever van die boa's verplicht is om elk jaar een interne Wpg-audit uit te voeren. De Gemeente Barneveld heeft in 2023 de privacy officer laten opleiden als interne auditor.
- Externe Wpg-audit: elke vier jaar. De werkgever moet elke vier jaar een externe Wpg-audit laten uitvoeren en de resultaten daarvan aan de Autoriteit Persoonsgegevens (AP) doen toekomen.

2.3 Toezichtskader AP: ontwikkelingen en gevolgen

De AP heeft eind december 2023 haar toezichtkader voor het jaar 2024 gepubliceerd. In het 'Jaarplan 2024'¹ geeft de AP haar prioriteiten aan voor de komende jaren, zodat dit ook van toepassing is voor het jaar 2025. Begin 2025 heeft de AP, nadat het Jaarverslag FG over 2024 al was vastgesteld, waardoor dit niet meer meegenomen kon worden, het Jaarplan 2025 gepubliceerd. Van dat jaarplan is in de volgende paragraaf een samenvatting opgenomen. het volledige jaarplan is opgenomen in de bijlage.

2.3.1. Samenvatting Jaarplan 2025 AP

In 2025 besteedde de AP, net als in 2024, extra aandacht aan onderstaande vijf thema's:

Algoritmes & AI

Onze wereld wordt steeds digitaler en de mogelijkheden van algoritmes en artificiële intelligentie (AI) nemen snel toe. Dit biedt een hoop kansen, maar kan ook leiden tot onrechtmatige verwerking van gegevens, discriminatie, willekeur, gebrek aan transparantie of misleiding en manipulatie. De AP wil deze risico's voorkomen door onze grondrechten goed en proactief te beschermen. In 2025 verwacht de AP een intensivering van haar werkzaamheden op het gebied van algoritmes en AI. Hieraan werkt onder meer de Directie Coördinatie Algoritmes.

Big Tech

Grote techbedrijven gebruiken de gegevens van hun gebruikers als brandstof. En dat is vaak niet in lijn met de Algemene verordening gegevensbescherming (AVG). Persoonsgegevens worden gebruikt om gericht reclames te kunnen aanbieden, AI-modellen te trainen en om gepersonaliseerde inhoud aan te bieden zodat gebruikers langer online blijven. Daarom is het van groot belang om hier scherp toezicht op te blijven houden. Burgers moeten de regie kunnen

¹ <https://www.autoriteitpersoonsgegevens.nl/documenten/ap-jaarplan-2024>

houden over hun persoonsgegevens. De AP blijft hier in 2025 aan werken, samen met andere (internationale) toezichthouders.

Vrijheid & veiligheid

De AP wil bijdragen aan een verdedigbare balans tussen vrijheid en veiligheid. Het zijn twee kanten van dezelfde medaille, waarbij veiligheid de vrijheid bevordert. Om de veiligheid te bewaken worden soms maatregelen genomen die de vrijheid inperken, zoals het delen van gegevens voor opsporing van strafbare feiten.

Datahandel

Slimme producten en diensten genereren bergen waardevolle data, wat kan leiden tot de ongeoorloofde doorverkoop van persoonsgegevens. Dat gebeurt niet alleen in Nederland, maar ook internationaal. Dat mag niet en de AP wil dat een halt toe roepen.

Digitale overheid

Centrale en lokale overheden, uitvoeringsorganisaties en politie en justitie beschikken over grote hoeveelheden - vaak gevoelige en bijzondere - persoonsgegevens van Nederlanders en maken hier veel gebruik van. Het risico dat burgers in de knel komen is groot als de overheid verkeerd omgaat met persoonsgegevens. Vooral omdat het vaak verplicht is om gegevens af te staan aan de overheid. Bovendien heeft de overheid een voorbeeldfunctie als het gaat om de verantwoorde omgang met persoonsgegevens. Daarom ziet de AP hier komend jaar extra op toe.

2.3.2 inspectie AP

In mei 2025 heeft de AP aangekondigd steekproefsgewijs bij gemeentes op inspectie te gaan en vooral na te gaan of voldaan is aan de vereisten uit de AVG voor wat betreft het register van verwerkingen, de positie en onafhankelijkheid van de FG en uitvoering van DPIA's. Een privacy 'apk' werd geadviseerd, zodat met gemeentesecretaris, CIO, concerndirecteur, CISO, FG en PO de bedoelde onderwerpen doorgenomen zijn. Daarbij is geconstateerd dat voldaan wordt aan de AVG, Wpg, actualiteit en volledigheid van het register en de DPIA's. Ook heeft de FG binnen de organisatie voldoende draagvlak en autoriteit. Verder is afgesproken om jaarlijks een privacy 'apk' te doen. Dit wordt vanaf 2026 opgenomen in de P&C cyclus.

In 2025 is de AP overigens niet op inspectie gekomen bij de gemeente Barneveld, maar als dat bijvoorbeeld het komende jaar wel het geval is, kan mede aan de hand van dit jaarverslag aangetoond worden in welke mate de gemeente voldoet aan de AVG en de Wpg.

3. GOVERNANCE

3.1 Governance algemeen

Er is een duidelijke structuur aangaande de governance aanwezig wat betreft de uitvoering van de AVG. Er zijn een Chief Information Security Officer (CISO), een Privacy Officer (PO) en een Functionaris Gegevensbescherming (FG) aangewezen door het college. Deze onderlinge relaties en verantwoordingen blijken uit het door het college vastgestelde en op 1 mei 2023 in werking getreden herziene Privacybeleid. Hiermee wordt voldaan aan artikel 5 lid 2 van de AVG dat bepaalt dat een organisatie dient aan te kunnen tonen 'in control' te zijn aangaande de uitvoering van de AVG.

3.2 Verantwoording Functionaris gegevensbescherming

Overzicht uitgevoerde werkzaamheden in 2025:

- In 2025 zijn de uit de in 2024 uitgevoerde Data Protection Impact Assessments (DPIA's) voortvloeiende acties opgepakt en uitgevoerd.

- Het Register van Verwerkingen is zowel voor AVG als voor Wpg in 2025 volledig geactualiseerd.
- De voorgaande jaren is aan de hand van het IBD borgingsdocument de borging van privacy en informatiebeveiliging beoordeeld en zijn de resultaten geëvalueerd ten opzichte van het jaar daarvoor. In oktober 2024 is een nieuwe applicatie aangeschaft, waarin alle normenkaders verwerkt zijn die op de gemeente van toepassing (kunnen) zijn. In 2025 is de borging uitgevoerd in de nieuwe applicatie waarna een beoordeling kan plaatsvinden. De daaruit voortkomende acties worden vervolgens in 2026 verder opgepakt [Zie verder bij 3.5].
- Voor de Wpg is een interne audit uitgevoerd. Ook is een externe audit uitgevoerd in 2025 [zie verder bij 4.3].

3.3 Verantwoording Privacy Officer

Overzicht uitgevoerde werkzaamheden in 2025:

DPIA's	In 2025 zijn een aantal DPIA's uitgevoerd op risicovolle processen, zoals de verwerking van persoonsgegevens bij de uitvoering van de Wvvgz en de Wet zorg en dwang, de verwerking van persoonsgegevens bij het tijdelijk huisverbod, de overgang naar de applicatie ZorgNed, en hebben herijkingen plaatsgevonden van de DPIA's cameratoezicht, schuldhulpverlening en vroegsignalering.
Bewustwording privacy en informatiebeveiliging	- Er zijn trainingen voor (nieuwe) medewerkers verzorgd. - Periodiek is een nieuwsbericht op intranet gezet. - Er is een project in gang gezet voor verplichte training en bewustwording voor alle medewerkers van de gemeente Barneveld. Het verplicht stellen van de training is langs de Ondernemingsraad geweest en de training zal begin 2026 ingevoerd worden.
Wet politiegegevens	Door de PO is, in samenwerking met de inhoudelijke collega's een interne audit uitgevoerd op de verwerking van politiegegevens.
Privacy en Publiekszaken	In overleg met Publiekszaken is ondersteuning geboden bij privacyvraagstukken (verstrekken gegevens uit de BRP).
Actualisering register van verwerkingen	Nieuwe processen worden toegevoegd en wijzigingen in processen worden in het register doorgevoerd. Daarnaast is het register in 2025 volledig gecontroleerd en geactualiseerd.
Ondersteunen bij ontwikkelingen in de organisatie	Bij ontwikkelingen in de organisatie is de privacyregelgeving meegenomen en neemt waar nodig de PO deel aan (implementatie) projecten.
Inzageverzoeken	De meeste inzageverzoeken hebben betrekking op het sociaal domein en publiekszaken en zijn door de Privacy Officer afgehandeld in samenwerking met een betrokken collega.
Datalekken	Inbreuken in verband met privacy zijn geregistreerd. Datalekken zijn gemeld bij de AP.

Overige werkzaamheden	Naast de hierboven genoemde werkzaamheden zijn door de PO de volgende werkzaamheden verricht: - Toetsen/ opstellen verwerkersovereenkomsten - Toetsen/ opstellen convenanten - Behandelen privacyvraagstukken - Signaleringsfunctie in organisatie - Sparringpartner voor de organisatie
-----------------------	---

3.4 Verantwoording CISO

Overzicht van uitgevoerde werkzaamheden in 2025:

Bewustwording privacy en informatiebeveiliging	- Samen met de PO zijn maandelijks workshops voor nieuwe medewerkers verzorgd. - Op verzoek zijn de CISO of PO bij teamoverleggen aanwezig geweest. - De CISO neemt periodiek deel aan afdelingsoverleggen binnen en buiten I&A. - Ter versterking van bewustwording wordt tooling ingericht die <i>alle</i> medewerkers bereikt, niet alleen nieuwe medewerkers.
Zelfevaluatie BRP/PNIK	De gemeente heeft de jaarlijkse verantwoording afgerond over informatiebeveiliging rond BRP / Pnik.
Zelfevaluatie ENSIA	De gemeente heeft verantwoording afgedragen over informatiebeveiliging door middel van ENSIA (Eenduidige Normatiek Single Information Audit). Hierin vallen onder andere BAG, BGT, DigiD, Suwinet. Daarbij worden DigiD, Suwinet en de ENSIA-verantwoording getoetst door een externe RE/RA auditor.
BIO	Controleren en evalueren van de huidige set maatregelen. Voorbereidingen getroffen voor de invoering van BIO-2.
TISO	Er is per 2026 structureel formatie toegevoegd voor een Technical Information Security Officer ter ondersteuning van de CISO.
Informatiebeveiligingsbeleid	Het informatiebeveiligingsbeleid uit 2024 wordt gecontinueerd tot aan de invoering van de Cyberbeveiligingswet. In 2026 zal een nieuw informatiebeveiligingsbeleid worden geschreven dat aansluit bij de nieuwe wetgeving.
Cyberbeveiligingswet (Cbw / NIS2)	Medio 2026 wordt de nieuwe Cyberbeveiligingswet van kracht. Implementatie van extra maatregelen (technisch en organisatorisch) wordt voorbereid.

3.5 Borging

Sinds 2021 is het borgingsdocument van de VNG jaarlijks gebruikt om te beoordelen of wat betreft privacy en security voldaan wordt aan de gestelde normenkaders, die voornamelijk uit de BIO (Baseline Informatieveiligheid Overheid) voortkomen. In oktober 2024 is een nieuwe applicatie aangeschaft waarin alle normenkaders opgenomen zijn die op de gemeente van toepassing (kunnen) zijn.

Q4 2024 en Q1 2025 zijn gebruikt om de controle op borging in die nieuwe applicatie te verwerken. De basis die gebruikt is, is het resultaat van de laatstelijk uitgevoerde controle op de borging uit Q1 2024. Ook al was het nodig de applicatie eenmalig in te richten, betekent dat niet dat er geen beeld is van de stand van zaken en welke zaken opgepakt moeten gaan worden om (nog) beter te voldoen aan de voor privacy en security gestelde normen.

In Q1 van 2026 zal de borging wederom beoordeeld worden op stand van zaken, actualiteit en volledigheid, waaruit de actiepunten voor 2026 zullen voortkomen. Deze actiepunten kunnen dan vanaf Q2 2026 opgepakt worden.

4. WERKZAAMHEDEN EN BEVINDINGEN

4.1 Privacybeleid

Op 1 april 2018 is het Privacybeleid in werking getreden. Op 30 mei 2018 is de gemeenteraad hierover geïnformeerd. Dit beleid implementeert de uitgangspunten en verplichtingen uit de AVG. De uitgangspunten rechtmatigheid, behoorlijkheid, transparantie, doelbinding, subsidiariteit, proportionaliteit, dataminimalisatie en vertrouwelijkheid worden omgezet in alle werkprocessen waarbinnen persoonsgegevens worden verwerkt. Er is beleid gevormd op hoe om te gaan met de rechten van betrokkenen, meldplicht datalekken, de functies van FG, PO en CISO en de gegevensuitwisseling tussen verschillende domeinen en teams.

Zowel in 2021, 2022 als in 2023 heeft een herziening plaatsgevonden van het privacybeleid, waarbij in de beleidsherziening in 2023 ook de Wpg is opgenomen. Het nieuwe (herziene) privacybeleid is op 18 april 2023 vastgesteld door het college en is op 1 mei 2023 in werking getreden. De raad is hierover geïnformeerd en ook op de website van de Gemeente Barneveld is hier aandacht aan besteed. In 2025 is het privacybeleid beoordeeld, waarbij is geconcludeerd dat geen actualisatie nodig was in 2025. In 2026 zal dit opnieuw beoordeeld worden.

4.2 Thuiswerken

In de jaren 2020 tot en met 2022 waren er landelijk maatregelen afgekondigd ter bestrijding van Covid-19. Het thuiswerken heeft vanaf dat moment een enorme vlucht genomen en sinds 2023 wordt het hybride werken (deels thuis en deels op kantoor werken) veel toegepast. Dat zal ook de komende jaren zo blijven, omdat gebleken is dat dit goed werkt. Ook in 2025 is regelmatig aandacht gevraagd voor de risico's die thuiswerken met zich meebrengt, aangezien thuiswerken niet alleen nieuwe mogelijkheden biedt, maar ook risico's met zich meebrengt op het gebied van privacy en informatiebeveiliging.

Er is benadrukt dat de regels van privacy en informatiebeveiliging in acht genomen moeten worden. Vanuit privacy is aangegeven dat het ongewenst en ook strijdig met het privacybeleid is dat medewerkers fysieke documenten meenemen met daarop persoonsgegevens of andere vertrouwelijke gegevens. Via de beveiligde netwerkomgeving zijn alle documenten beschikbaar.

Vanuit informatieveiligheid/-beveiliging zijn de regels voor thuiswerken nogmaals onder de aandacht gebracht, ook middels de verplichte workshops. Daarbij zijn medewerkers erop geattendeerd dat ze met vertrouwelijke gegevens en informatie werken. De thuiswerkregeling is in 2023 geactualiseerd en onder de aandacht gebracht van alle medewerkers.

4.3 Wpg- audit

4.3.1 Audits over 2021 tot en met 2024

Op grond van de Wpg moet elk jaar een interne audit worden uitgevoerd en één keer per vier jaar een externe audit. In 2022 is er een interne audit uitgevoerd voor de Wpg over het jaar 2021. In 2022 is ook een externe audit uitgevoerd voor de Wpg over de jaren 2019-2021. De audits hebben betrekking op de verwerking van politiegegevens door de buitengewone opsporingsambtenaren openbare ruimte en de leerplichtambtenaren. Uit de audits zijn een aantal verbeterpunten naar voren gekomen, die binnen een jaar doorgevoerd moeten worden. Hiervoor is begin 2023 een verbeterplan opgesteld en de actiepunten daarin zijn opgepakt en uitgevoerd. De externe audit over de hercontrole heeft eind 2023 plaatsgevonden en had een positief resultaat. In 2024 zijn de nog openstaande zaken verder opgepakt. In januari 2025 is de interne audit over 2024 uitgevoerd, waarbij onderstaande normen zijn beoordeeld:

2. Doelbinding
3. Noodzakelijkheid & rechtmatigheid, vermelding herkomst
4. Juistheid en volledigheid politiegegevens
5. Onderscheid feiten en persoonlijk oordeel
6. Gegevensbescherming door beveiliging en ontwerp
7. Gegevensbescherming door standaard-instellingen
9. Bijzondere categorieën van politiegegevens
12. Onderscheid tussen verschillende categorieën van betrokkenen
15. Geautomatiseerde individuele besluitvorming
16. Uitvoering van de dagelijkse politietaak
17. Ter beschikking stellen van politiegegevens binnen het WPG-domein
18. Geautomatiseerd vergelijken en in combinatie zoeken
20. Bewaartermijnen, verwijderen en vernietigen

Daarnaast zijn periodieke controles uitgevoerd op autorisaties, loggings, het monitoren van loggings en het verwerken van politiegegevens. De verwerkingen zijn steekproefsgewijs uitgevoerd.

4.3.2 Interne audit over 2025

Begin 2026 zal de interne audit over 2025 uitgevoerd worden, waarbij onderstaande normen worden beoordeeld:

21. Verstrekking van politiegegevens aan anderen dan politie en Koninklijke Marechaussee
23. Verstrekking aan derden structureel voor samenwerkingsverbanden
24. Rechtstreekse verstrekking
25. Informatie aan de betrokkene, recht op inzage, rectificatie en verwijdering.

Ook zijn in 2025 periodieke controles uitgevoerd op autorisaties, loggings, het monitoren van loggings en het verwerken van politiegegevens. De verwerkingen zijn steekproefsgewijs uitgevoerd. Daarvan zijn hieronder de uitgangspunten nader toegelicht en in de navolgende paragrafen zijn de controles verder uitgewerkt, waarbij de resultaten per controle zijn opgenomen.

Uitgangspunten autorisatie controle

Alleen daartoe bevoegde (en beëdigde) medewerkers mogen politiegegevens verwerken in de applicatie, waarbij een onderscheid is gemaakt in rollen en rechten tussen de verschillende functionarissen. Dit is van belang voor een rechtmatige verwerking en om het vier-ogen-principe op een correcte wijze in de applicatie uit te kunnen voeren. Dit wordt bij de controles beoordeeld.

Uitgangspunten logging controle

In tegenstelling tot de AVG kent de Wpg een verplichte logging. Dit volgt uit de EU-Richtlijn 2016/680. Artikel 25 uit de EU-Richtlijn is met ingang van 1 juli 2025 geïmplementeerd in artikel 32a in de Wpg, waarmee bepaald is dat verplicht gelogd wordt. De achterliggende gedachte is dat in het strafrecht de gegevens doorgaans gevoelig zijn en dat het grote gevolgen kan hebben als deze gegevens in de verkeerde handen terecht komen. Logging houdt dan ook in dat wordt vastgelegd wie toegang heeft gehad tot bestanden met politiegegevens en dat dit regelmatig wordt gecontroleerd. Zo kan worden nagegaan of iemand toegang heeft gehad tot politiegegevens, terwijl diegene daartoe onbevoegd was. De verwerkingsverantwoordelijke (werkgever van de boa) (en de verwerker) moeten het verzamelen, wijzigen, raadplegen, verstrekken en het vernietigen van politiegegevens vastleggen.

Uitgangspunten steekproef controle verwerking politiegegevens

In de Wet politiegegevens (Wpg) is bepaald dat jaarlijks een controle moet plaatsvinden op de verwerking van politiegegevens. De wijze van controle en de criteria aan de hand waarvan de controle plaatsvindt, zijn bepaald in het Controleprotocol.

Er worden jaarlijks veel processen-verbaal en halt-verwijzingen uitgeschreven. Om te kunnen beoordelen of dat op een zorgvuldige en rechtmatige wijze gebeurt, vindt door middel van een steekproef een controle plaats op het vastgestelde percentage te beoordelen zaken. In 2024 en voorgaande jaren is dat eenmaal in het jaar gedaan, maar vanaf 2025 wordt dat voor domein I tweemaal per jaar gedaan. Voor domein III blijft dat eenmaal per jaar, waarbij zaken uit het afgeronde voorgaande schooljaar worden beoordeeld.

4.3.2.1. Domein I (Openbare ruimte) controles april/mei 2025

Controle autorisaties

Op 12 mei 2025 is door Privacy Officer, samen met de BOA/bevoegd functionaris, de periodieke controle op de autorisaties in Citycontrol uitgevoerd. Daarbij is getoetst of de autorisatiematrix actueel is en of de in de applicatie toegekende rollen en rechten kloppen met de functies die medewerkers uitvoeren.

Vastgesteld is:

1. De gebruikers in Citycontrol komen overeen met de medewerkers die de werkzaamheden uitvoeren.
2. De geïmplementeerde autorisaties komen overeen met de toegekende autorisaties.
3. De aan de gebruikers toegekende rollen komen overeen met de toegekende autorisaties in Citycontrol. Toegang tot Wpg-gegevens is alleen ingesteld voor de specifieke rollen die deze toegang nodig hebben.

Er is geen opvolging omdat er geen onrechtmatigheden zijn geconstateerd.

Loggingen applicatie CityControl

In CityControl zijn alle Loggingen per zaak te zien, waarbij door vermelding van naam en tijd na te gaan is wie wat heeft gedaan. Daarbij is zichtbaar onder welk tabblad is gewerkt, maar niet wat daar is ingevoerd. Tevens is zichtbaar wat de zaakstatus is, als dit is aangepast.

Uitgevoerde controle op de logging

Uitgangspunt is dat de rechten en rollen van de verschillende medewerkers goed gescheiden zijn. Op 9 april 2025 is de controle op de logging uitgevoerd door de CISO, FG, BOA-coördinator en BOA/Bevoegd Functionaris op het HVC over de periode van 1 oktober 2024 tot en met 31 maart 2025. Tijdens de controle zijn met de BOA-coördinator en BOA/Bevoegd Functionaris de bevindingen van de vorige controle en welke opvolging hieraan is gegeven besproken.

Daarnaast heeft de Bevoegd Functionaris inzicht gegeven in CityControl:

- De rollen en bevoegdheden per collega;
- Rol AdminProfile;
- Aantal zaken over de periode van 1 oktober 2024 tot en met 31 maart 2025.

Bevindingen

Er zijn een aantal bevindingen naar voren gekomen uit de controle waarop aanbevelingen gedaan zijn voor verbetering om nog beter aan de Wpg te voldoen. Het controlemoment daarna zal de stand van zaken daarvan aan de orde komen. Het gaat om de volgende bevindingen:

1. De rollen en bevoegdheden per collega: werkwijze in- en uitdiensttreding en langdurige afwezigheid opnemen in werkprocesbeschrijving. De werkprocesbeschrijvingen zijn op 1 februari 2025 in gebruik genomen. Daarmee is deze bevinding afgerond.
2. Rol AdminProfile: leverancier geen toegang geven tot zaken. Daarin is geen verandering.

3. Casuïstiek bespreken in team overleggen: wanneer is sprake van AVG en wanneer van Wpg. Dit wordt opgepakt, zodat bij het volgende controlemoment de gang van zaken besproken kan worden.
4. Gebruik maken van 2f authenticatie bij inloggen op pc en handheld. Dit is geregeld en daarmee is deze bevinding afgerond.
5. Verwerkingen handheld zijn niet zichtbaar in loggingen. Hierover wordt nogmaals navraag gedaan bij de leverancier, zodat bij het volgende controlemoment de gang van zaken besproken kan worden.
6. Er wordt over nagedacht om ondermijningszaken extra af te schermen. In Q1 2025 is daar een besluit over genomen. Zodra dit in de applicatie is ingericht wordt de nieuwe werkwijze in een teamoverleg besproken. Is men mee bezig, zodat bij het volgende controlemoment de gang van zaken besproken kan worden.

Controle verwerking politiegegevens

Ieder proces-verbaal wordt door de boa zelf nagelopen op juistheid, volledigheid en rechtmatigheid. Daarnaast controleert de boa-coördinator maandelijks 10 processen-verbaal. Tweemaal per jaar controleert de FG 5% random gekozen processen-verbaal, uitgaande van 1000 processen-verbaal per jaar.

Controleperiode

Q4 2024 tot en met Q1 2025: van 1 oktober 2024 tot en met 31 maart 2025.

Omvang Steekproef

In het controleprotocol is de omvang van de steekproef bepaald op 50 processen-verbaal, waarbij als uitgangspunt ongeveer 1000 processen-verbaal per jaar geldt. Dat is 5%. Nu over de controleperiode 588 processen-verbaal zijn uitgeschreven, is er voor gekozen om 30 processen-verbaal in de steekproef mee te nemen (uitgaande van gemiddeld 1000 processen-verbaal over een jaar tijd). De steekproef is random geselecteerd. De controle is uitgevoerd op 16 april 2025, in bijzijn van BOA/Bevoegd Functionaris en BOA coördinator/Bevoegd Functionaris, omdat toegang tot CityControl nodig was om de documenten te kunnen inzien/controleren.

Bevindingen

Doordat foutieve parkeersituaties snel en vaak aangetroffen worden tijdens surveillancerondes komen dat soort bekeuringen/processen-verbaal het meest voor.

In nagenoeg alle zaken zijn alleen de noodzakelijke gegevens verwerkt. In veel gevallen waren er wel voertuiggegevens, kenteken, foto, locatie en aangetroffen overtreden situatie bekend, maar was er geen persoon aangetroffen, waardoor er geen persoonsgegevens verwerkt konden worden. Het CJIB heeft echter voldoende aan de hiervoor genoemde gegevens, waarmee het CJIB de kenteken/ voertuighouder eraan kan koppelen en die persoon of dat bedrijf een bekeuring kan sturen. Door de boa's worden daarom de persoonsgegevens niet opgevraagd via het kenteken, zodat zij niet meer persoon-/politiegegevens verwerken dan noodzakelijk. In de meeste zaken wordt een korte maar duidelijke omschrijving van de aangetroffen situatie vermeld [de 'reden van wetenschap'] en is sprake van een vrij kort of summier verhoor, indien er een persoon is aangetroffen of staande gehouden. Slechts in een van de gecontroleerde processen-verbaal is niet vermeld hoe de persoonsgegevens zijn vastgesteld, maar deze waren wel compleet.

Bij parkeren op laad- en losplekken is steeds tussen 5 tot 10 minuten gepost om te kunnen beoordelen of de bestuurder van het aangetroffen voertuig inderdaad bezig was met laad- en losactiviteiten.

Tijdens de controles van de processen-verbaal zijn geen onrechtmatige verwerkingen aangetroffen.

4.3.2.2. Domein III (Leerplicht) april, mei 2025

Controle autorisaties

Op 27 mei 2025 is door de privacy officer, samen met de functioneel beheerders de periodieke controle op de autorisaties in de applicatie Carel uitgevoerd. Daarbij is getoetst of de autorisatiematrix actueel is en of de in de applicatie toegekende rollen en rechten kloppen met de functies die medewerkers uitvoeren.

Vastgesteld is:

1. De gebruikers in Carel komen overeen met de medewerkers die de werkzaamheden uitvoeren.
2. De geïmplementeerde autorisaties komen overeen met de toegekende autorisaties.
3. De aan de gebruikers toegekende rollen komen overeen met de toegekende autorisaties in Carel. Toegang tot Wpg-gegevens is alleen ingesteld voor de specifieke rollen die deze toegang nodig hebben.

Er is geen opvolging omdat er geen onrechtmatigheden zijn geconstateerd.

Controle logging

De Gemeente Barneveld gebruikt sinds 2021 de applicatie Carel. In Carel worden standaard kolomnamen bij de Wpg logging gebruikt. Dit betreft één logbestand dat is gegenereerd. Onderstaande kolommen zijn zichtbaar in het logbestand.

Gebruiker	Tijdstip	Toegangs- reden	Verstrekking	Verstrekking aan	Persoons- nummer	Casus omschrijving	Begindatum casus	Document- naam
-----------	----------	--------------------	--------------	---------------------	---------------------	-----------------------	---------------------	-------------------

Op 17 april 2025 is door FG en de CISO de logging over Q4 2024 en Q1 2025 beoordeeld. Daarnaast zijn met de leerplichtambtenaar aan de hand van een steekproef een aantal loggings gecontroleerd. Tevens is bij deze controle inhoudelijk beoordeeld of de Halt- verwijzingen en Processen- verbaal voldoen aan de vereisten van juistheid, volledigheid, doelbinding, noodzaak en rechtmatigheid.

Bevindingen

Gebleken is dat alleen door bevoegde medewerkers Wpg zaken worden behandeld en verwerkt in de applicatie Carel. Geconstateerd is dat er enkele verwerkingen gedaan zijn buiten kantoortijden. Uit navraag bij de leerplichtambtenaar/boa blijkt dat er geen afspraken gemaakt zijn over tijdsblokken waarbinnen wel of niet in de applicatie gewerkt mag worden.

Bij deze en bij eerdere controles is geconstateerd dat zaken voor eigen gebruik of intern gebruik geraadpleegd wordt. Dat wordt gedaan om op uniforme wijze te werken, omdat de formats nog niet gereed zijn. In april 2025 werd aangegeven dat de formats worden gebouwd en vervolgens in Teams worden gehangen. Tijdens de controle is ook geconstateerd dat aan de vereisten van juistheid, volledigheid, doelbinding, noodzaak en rechtmatigheid wordt voldaan.

Conclusie

Geconcludeerd kan worden dat – voor zover dat aan de hand van de gegevens inzichtelijk is – op de juiste wijze gewerkt wordt in de applicatie Carel en dat de vijf daartoe bevoegde medewerkers die daarin Wpg-zaken behandelen daar voldoende bewust en zorgvuldig mee omgaan. Hier wordt zakelijk mee omgegaan. Een belangrijk punt van aandacht is dat er afspraken gemaakt moeten worden over de tijdsblokken waarbinnen in de applicatie Carel

persoons-/politiegegevens verwerkt mogen worden. De kolommen waarop gemonitord wordt, zijn voldoende om een goede beoordeling te kunnen maken. Meer of minder kolommen zijn niet nodig voor de monitoring.

4.3.2.3. Domein I (Openbare ruimte) november 2025

Controle autorisaties

Op 27 november 2025 is door de privacy officer, samen met de BOA/bevoegd functionaris, de periodieke controle op de autorisaties in de applicatie Citycontrol uitgevoerd. Daarbij is getoetst of de autorisatiematrix actueel is en of de in de applicatie toegekende rollen en rechten kloppen met de functies die medewerkers uitvoeren.

Vastgesteld is:

1. De gebruikers in Citycontrol komen overeen met de medewerkers die de werkzaamheden uitvoeren.
2. De geïmplementeerde autorisaties komen overeen met de toegekende autorisaties.
3. De aan de gebruikers toegekende rollen komen overeen met de toegekende autorisaties in Citycontrol. Toegang tot Wpg-gegevens is alleen ingesteld voor de specifieke rollen die deze toegang nodig hebben.

Er is geen opvolging omdat er geen onrechtmatigheden zijn geconstateerd.

Loggingen applicatie CityControl

In CityControl zijn alle Loggingen per zaak te zien, waarbij door vermelding van naam en tijd na te gaan is wie wat heeft gedaan. Daarbij is zichtbaar onder welk tabblad is gewerkt, maar niet wat daar is ingevoerd. Tevens is zichtbaar wat de zaakstatus is, als dit is aangepast.

Uitgevoerde controle op de logging

Uitgangspunt is dat de rechten en rollen van de verschillende medewerkers goed gescheiden zijn. Op 26 november 2025 is de controle op de logging uitgevoerd door de CISO, FG en BOA/Bevoegd Functionaris op het HVC over de periode van 1 april tot en met 30 september 2025. Tijdens de controle zijn met de BOA/Bevoegd Functionaris de bevindingen van de vorige controle en welke opvolging hieraan is gegeven besproken. Daarnaast heeft de Bevoegd Functionaris inzicht gegeven in CityControl:

- De rollen en bevoegdheden per collega;
- Rol AdminProfile;
- Aantal zaken over de periode van 1 april tot en met 30 september 2024.

Stand van zaken bevindingen

1. De concept werkinstructies/werkprocessen zijn besproken. Daarmee is deze bevinding afgerond.
2. Definitief geen toegang. Afgerond.
3. Afsproken is dat vanaf 1 januari 2025 3 keer per jaar (dus iedere 4 maanden) in een teamoverleg casuïstiek besproken wordt over wanneer er sprake is van AVG of Wpg. Wordt opgevolgd. Daarmee is deze bevinding afgerond.
4. Is ingesteld en daarmee is deze bevinding afgerond.
5. Logging / monitoring is mogelijk op verwerkingen in de backoffice (PC). Ook kunnen er rapportages gedraaid worden. Dit is nog niet mogelijk op frontoffice verwerkingen (handheld). Dit wordt nogmaals nagevraagd bij de leverancier (staat nog niet op hun planning). Heeft geen prioriteit bij leverancier, dus alert op blijven.
6. Er wordt over nagedacht om ondermijningszaken extra af te schermen. In Q1 2025 is daar een besluit over genomen worden. Nadat de applicatie is ingericht, wordt de nieuwe werkwijze in een teamoverleg besproken. Bij de controle in november 2025 is gebleken dat er een afzonderlijke applicatie gebruikt wordt voor ondermijningszaken. Dat is Pgax en alleen de boa's met aandachtsgebied ondermijning kunnen daarin zaken

verwerken. De andere boa's kunnen deze niet inzien. Begin januari 2026 is afgesproken dat uiterlijk 1 april 2026 er geen gebruik meer gemaakt wordt van gewone mail en alle correspondentie, vergaderingen en documenten in pgax plaatsvinden. Bij een volgende controle wordt dit geëvalueerd.

Controle verwerkingen politiegegevens

Ieder proces-verbaal wordt door de boa zelf nagelopen op juistheid, volledigheid en rechtmatigheid. Daarnaast controleert de BOA-Bevoegd Functionaris maandelijks 10 processen-verbaal. Tweemaal per jaar controleert de FG 5% random gekozen processen-verbaal, uitgaande van 1000 processen-verbaal per jaar.

Controleperiode

Q2 en Q3 2025: van 1 april tot en met 30 september 2025.

Omvang Steekproef

In het controleprotocol is de omvang van de steekproef bepaald op 50 processen-verbaal, waarbij als uitgangspunt ongeveer 1000 processen-verbaal per jaar geldt. Dat is 5%.

Nu over de controleperiode 1016 processen-verbaal zijn uitgeschreven, is er voor gekozen om 51 processen-verbaal in de steekproef mee te nemen (uitgaande van gemiddeld 1000 processen-verbaal over een jaar tijd). De steekproef is random geselecteerd.

Bevindingen

Doordat foutieve parkeersituaties snel en vaak aangetroffen worden tijdens surveillancerondes komen dat soort bekeuringen/processen-verbaal het meest voor.

In nagenoeg alle zaken zijn alleen de noodzakelijke gegevens verwerkt. In veel gevallen waren er wel voertuiggegevens, kenteken, foto, locatie en aangetroffen overtreden situatie bekend, maar was er geen persoon aangetroffen, waardoor er geen persoonsgegevens verwerkt konden worden. Het CJIB heeft echter voldoende aan de hiervoor genoemde gegevens, waarmee het CJIB de kenteken/voertuighouder eraan kan koppelen en die persoon of dat bedrijf een bekeuring kan sturen. In de meeste zaken wordt een korte maar duidelijke omschrijving van de aangetroffen situatie vermeld [de 'reden van wetenschap'] en is sprake van een vrij kort of summier verhoor, indien er een persoon is aangetroffen of staande gehouden.

Bij parkeren op laad- en losplekken is steeds tussen 5 tot 10 minuten gepost om te kunnen beoordelen of de bestuurder van het aangetroffen voertuig inderdaad bezig was met laad- en losactiviteiten

In een enkel proces verbaal is een verkeerde feitcode ingevoerd, waarbij het boetebedrag gelijk is aan een vergelijkbare situatie die bijna hetzelfde is. Daarbij gaat het vaak om een minimaal verschil, zodat de boete wel terecht is opgelegd. Hier zal in 2026 nog beter op gelet gaan worden.

Tijdens de controles van de processen-verbaal zijn geen onrechtmatige verwerkingen aangetroffen.

4.3.2.4. Domein III (Leerplicht) november 2025

Controle autorisaties

Op 10 november 2025 is door de privacy officer, samen met de functioneel beheerder, de periodieke controle op de autorisaties in de applicatie Carel uitgevoerd. Daarbij is getoetst of de autorisatiematrix actueel is en of de in de applicatie toegekende rollen en rechten kloppen met de functies die medewerkers uitvoeren.

Vastgesteld is:

1. De gebruikers in Carel komen overeen met de medewerkers die de werkzaamheden uitvoeren. Er staat nog één medewerker in Carel die op actief staat, maar niet meer bij de gemeente werkzaam is. De reden hiervoor is dat een aantal processen/taken nog overgedragen moeten worden. Deze medewerker heeft geen toegang meer tot Carel, omdat zij niet meer kan inloggen in de gemeentelijke omgeving.
2. De geïmplementeerde autorisaties komen overeen met de toegekende autorisaties.
3. De aan de gebruikers toegekende rollen komen overeen met de toegekende autorisaties in Carel. Toegang tot Wpg-gegevens is alleen ingesteld voor de specifieke rollen die deze toegang nodig hebben.

Er is geen opvolging omdat er geen onrechtmatigheden zijn geconstateerd.

Controle logging

Op 3 november 2025 is door FG samen met de CISO de logging over Q2 en Q3 2025 beoordeeld. Vervolgens is op 27 november 2025 door de FG met de leerplichtambtenaar aan de hand van een steekproef inhoudelijk beoordeeld of 10% van de Haltverwijzingen en Processen- verbaal over schooljaar 2024/2025 voldoen aan de vereisten van juistheid, volledigheid, doelbinding, noodzaak en rechtmatigheid. Over schooljaar 2024/2025 zijn twee random geselecteerde Halt-verwijzingen en vier random geselecteerde processen-verbaal opgenomen in de inhoudelijke beoordeling.

Bevindingen

Er zijn in Q2 2025 zes medewerkers en in Q3 2025 vijf medewerkers die bevoegd zijn om Wpg zaken te behandelen en te verwerken in de applicatie Carel. Een medewerker is in augustus vertrokken vanwege een andere baan. In de loggings van Q2 komt een enkele maal de naam van de applicatiebeheerder voor. Dat heeft te maken gehad met nieuwe bugs in de applicatie.

Geconstateerd is dat er enkele verwerkingen gedaan zijn buiten kantoortijden. Uit navraag bij de leerplichtambtenaar/boa blijkt dat er geen afspraken gemaakt zijn over tijdsblokken waarbinnen wel of niet in de applicatie gewerkt mag worden.

De hiervoor in paragraaf 4.3.2.2. genoemde kolommen geven de meest noodzakelijke zaken aan waar bij een logging op gemonitord kan worden. Deze loggegevens geven duidelijk aan door wie, wanneer en waarom een bepaald dossier is geopend en om wat voor soort zaak het gaat. Omdat het om Wpg-gegevens gaat, kan slechts sprake zijn van drie soorten zaken, namelijk Relatief verzuim, Halt-verwijzing en Proces-verbaal. Bij 24 verwerkingen is "Halt negatief afloopbericht" ingevuld als soort zaak. Dit is een niet eerder geconstateerde soort zaak. Uit navraag bij de leerplichtambtenaar/boa blijkt dat in afloopberichten vermeld wordt of een halt traject positief of negatief is geëindigd.

Verder valt op dat bij alle loggings is aangegeven 'voor eigen gebruik'. De opmerking 'intern gebruik' is niet aangetroffen zoals bij eerdere controlemomenten wel het geval was. Geconcludeerd wordt dat de raadplegingen 'voor eigen gebruik', zodra de formats in gebruik zijn, zullen blijven voorkomen, maar minder vaak. Op 16 oktober 2025 heeft de leerplichtambtenaar/boa medegedeeld dat er op dat moment de laatste hand gelegd wordt aan

de preventieve route waar deze documenten en formats deel van uitmaken. Naar verwachting zijn deze eind 2025 gereed.

Bij de vorige controle is geconstateerd dat wanneer er meer terugkoppeling aan Halt gaat worden gevraagd bij een negatief resultaat het wenselijk is dit ook vast te leggen in de werkinstructie (met daarbij een onderbouwing welke informatie wordt gevraagd en wat hiervan de noodzaak is). Uit de op 16 oktober 2025 ontvangen nadere toelichting blijkt dat op basis van herhaald licht school verzuim Halt overwogen wordt. Als Halt traject start, wordt in het kader van dat proces, daar het verzuim gemeld, als dat er is. Dit is niet nader omschreven maar vloeit voort uit de Leerplichtwet.

Tijdens de controle is ook geconstateerd dat aan de vereisten van juistheid, volledigheid, doelbinding, noodzaak en rechtmatigheid wordt voldaan.

Conclusie

Geconcludeerd kan worden dat – voor zover dat aan de hand van de gegevens inzichtelijk is – op de juiste wijze gewerkt wordt in de applicatie Carel en dat de zes/vijf daartoe bevoegde medewerkers die daarin Wpg-zaken behandelen daar voldoende bewust en zorgvuldig mee omgaan. Hier wordt zakelijk mee omgegaan. Een belangrijk punt van aandacht is dat er afspraken gemaakt moeten worden over de tijdsblokken waarbinnen in de applicatie Carel persoons-/politiegegevens verwerkt mogen worden. De kolommen waarop gemonitord wordt, zijn voldoende om een goede beoordeling te kunnen maken. Meer of minder kolommen zijn niet nodig voor de monitoring.

Controle verwerking politiegegevens

De interne controle op de naleving van de Leerplichtwet 1969, in Barneveld, ziet op twee handhavingsmaatregelen:

- Verwijzing naar Bureau Halt (Haltafdoening), gericht op de jongere tussen 12 en 18 jaar;
- Proces-verbaal voor openbaar ministerie, gericht op de jongere tussen 12 en 18 jaar en/of ouders-verzorgers.

Op deze handhavingsmaatregelen vindt toetsing plaats. Deze toetsing kent een ‘drietraps-model’. De eerste toetsing wordt uitgevoerd door de leerplichtambtenaar (tevens Boa), de tweede toetsing wordt uitgevoerd door een collega-leerplichtambtenaar (4-ogenprincipe) en in de derde toetsing wordt de voorgaande toetsing, steekproefsgewijs getoetst door de functionaris gegevensbescherming. Dit wordt gedaan aan de hand van een vragenformulier, waarin de vragen verduidelijkt en verbeterd zijn naar aanleiding van de vorige controle.

De toetsing richt zich op de volgende elementen en aspecten:

- Persoonsgegevens
- Verzuim
- Handhaving
- Haltafdoening
- Rechtmatigheid, noodzaak en doelbinding

Controleperiode

Schooljaar 2024/2025

Omvang Steekproef

In het controleprotocol is de omvang van de steekproef bepaald op 10%. In schooljaar 2024/2025 zijn 7 Halt-verwijzingen uitgeschreven, waarvan er twee zijn opgenomen in de

controle. In schooljaar 2024/2025 zijn 38 processen-verbaal uitgeschreven, waarvan er vier in de controle zijn opgenomen. De steekproef is random geselecteerd.

Controledatum

Halt-verwijzingen: deze beoordeling is uitgevoerd op 27 november 2025 in bijzijn van BOA/leerplichtambtenaar, omdat toegang tot Carel nodig was om de documenten te kunnen inzien/controleren. Processen-verbaal: deze beoordeling is uitgevoerd 27 november 2027 in bijzijn van BOA/leerplichtambtenaar, omdat toegang tot Carel nodig was om de documenten te kunnen inzien/controleren.

Bevindingen

Verificatie identiteit

Tijdens de uitvoering van de controle is gebleken dat de uit de vorige controle voortgekomen aanbeveling over de *Verificatie van de identiteit van de verdachte of jongere* onvoldoende wordt toegepast. Dat geldt zowel voor Halt-verwijzingen als voor processen-verbaal. Bij de controle op 27 november 2025 is gebleken dat het aangepaste formulier gaandeweg het vorige schooljaar is toegepast, waardoor nu in alle zaken is opgenomen dat er controle heeft plaatsgevonden van de identiteit van de verdachte of jongere en dat daarbij vermeld wordt op welke wijze dat is gedaan. Dit kan aan de hand van de oproepbrief zijn gecontroleerd of aan de hand van een identiteitsbewijs, waarbij alleen het soort document wordt vermeld. Daarmee is deze aanbeveling afgerond.

Indiening halt-verwijzing

Bij Halt-verwijzingen blijkt uit het formulier wel dat aan de jongere en diens ouder/voogd uitgelegd is wat een Halt-traject inhoudt en wat de consequenties zijn bij het niet positief afsluiten van een traject of in geval van recidive. Er blijkt echter niet uit of de Halt-verwijzing ingediend is bij Openbaar Ministerie en/of Bureau Halt Oost-Nederland. Eerder is aanbevolen dat dit verduidelijkt moet worden door het formulier Halt-verwijzing aan te passen en deze vraag daarin op te nemen. Bij de controle op 27 november 2025 is gebleken dat het formulier is aangepast. Daarmee is deze aanbeveling afgerond.

4.3.2.5. Domein I en III de technische en organisatorische maatregelen Wpg

De in november/december geplande jaarlijkse controle op de technische en organisatorische maatregelen Wpg is uitgesteld naar februari/maart 2026, omdat de Third Party Memoranda (TPM's) nog opgevraagd moesten worden en de leveranciers daarvoor een auditor moet inschakelen. De verwachting is dat de TPM voor Carel (Domein III) in februari 2026 beschikbaar komt. De TPM voor Sigmax (Domein I) is in december 2025 ontvangen.

4.3.3. Externe audit over 2024

In november 2025 is de vierjaarlijkse externe audit op de Wpg uitgevoerd door een auditor, waarbij de verwerking van Wpg-gegevens over de jaren 2022 t/m 2024 is beoordeeld. Eind november 2025 is het concept rapport ontvangen, waaruit wat verbeterpunten naar voren zijn gekomen. Omdat er wat onduidelijkheden in het rapport zitten en er een ander beoordelingskader is toegepast dan in voorgaande jaren is een verzoek tot verduidelijking gestuurd. In januari 2026 heeft een gesprek met de auditor plaatsgevonden, waarna het definitieve rapport in februari 2026 te verwachten is. De verbeterpunten worden daarna opgenomen in een verbeterplan en in het toezichtplan, zodat op de uitvoering daarvan toezien kan worden.

4.4 Register van verwerkingen

In 2025 is het register van verwerkingen zowel voor de AVG als voor de Wpg volledig geactualiseerd.

4.5 Meldingen datalekken

4.5.1 Cijfers AVG

In totaal zijn er in 2025 30 AVG beveiligingsincidenten geregistreerd bij de Gemeente Barneveld. Hiervan zijn 2 incidenten gemeld bij de AP. De AP registreert alle meldingen die door gemeenten gedaan worden. De AP reageert alleen in gevallen dat zij 'nader onderzoek' willen doen naar een door de gemeente gedane melding. In 2025 is daarvan geen sprake geweest. Ook heeft de AP geen waarschuwing gedaan of een dwangsom opgelegd aan de Gemeente Barneveld.

In een aantal gevallen is de betrokkene wiens gegevens zijn gelekt op de hoogte gesteld van het datalek. Uit een analyse van de datalekken is gebleken dat het van belang is om alert te blijven op het gebruik van de juiste contactgegevens van betrokkenen en mogelijke phishing, spoofing en hacks. Waar nodig zijn er technische maatregelen getroffen om de gebruikers te ondersteunen.

4.5.2 Cijfers Wpg

In 2025 zijn er geen Wpg beveiligingsincidenten gemeld bij de Gemeente Barneveld. De procedure meldplicht datalekken is in 2023 geactualiseerd en de Wpg is daar ook in opgenomen, omdat de procedure voorheen alleen zag op de AVG.

4.6 Rechten van betrokkenen

4.6.1 AVG verzoeken

Er zijn in 2025 18 verzoeken van betrokkenen op grond van de AVG binnengekomen. Er waren 2 verzoeken om verwijdering. De andere 16 verzoeken waren verzoeken tot inzage. De meeste verzoeken zijn toegewezen en 14 verzoeken hebben betrekking op het Sociaal Domein en Publiekszaken.

4.6.2 Wpg verzoeken

Er zijn in 2025 geen verzoeken gedaan op grond van de Wpg waarin betrokkenen een beroep op hun rechten deden.

4.7 Bewaartermijnen

In 2019 zijn digitale bezemdagen georganiseerd in verschillende teams en zijn teams actief geweest op het opschonen van mappen op netwerkschrijven en in e-mailboxen. Door de coronapandemie is er door de meeste medewerkers veel thuis gewerkt, waardoor het goed beveiligd thuiswerken meer prioriteit heeft gekregen dan het digitaal bezemen. Inmiddels is iedereen gewend geraakt aan het thuiswerken en weet men met welke privacy- en informatiebeveiligingsaspecten rekening gehouden moet worden.

Eind 2021 is het digitaal bezemen weer door enkele teams opgepakt en het was de bedoeling om dit in 2023 en 2024 voort te zetten, maar dat is niet gedaan. Het digitaal bezemen is daarom doorgeschoven naar 2025. In 2025 is dit echter beperkt opgepakt, omdat dit in 2026 in een breder verband, namelijk samen met de implementatie en de verdere uitrol van de actieve openbaarmakingsverplichtingen uit de Wet open overheid, opgepakt gaat worden.

4.8 Verwerkers en verwerkersovereenkomsten

Van alle leveranciers waarmee een verwerkersovereenkomst is afgesloten is een actueel overzicht. Bestaande verwerkers hebben niet gerapporteerd over incidenten. Verder weten medewerkers de Privacy Officer te vinden als ze twijfelen of een verwerkersovereenkomst moet

worden afgesloten en wordt een af te sluiten verwerkersovereenkomst ook altijd voorgelegd aan de Privacy Officer (en soms aanvullend aan de CISO) voor een inhoudelijke check.

Bij het afsluiten van verwerkersovereenkomsten met leveranciers wordt standaard de model verwerkersovereenkomst gehanteerd die verplicht is gesteld door de VNG/IBD. Dit is in 2025 bij alle verwerkersovereenkomsten gebeurd. Wel is in 2025 bij een verwerkersovereenkomst artikel 4.2. aangepast en is bij 3 overeenkomsten artikel 7 uitgebreider opgenomen. Bij een overeenkomst zijn meerdere artikelen aangepast. Bij iedere (door de verwerker gewenste) afwijking of aanpassing is steeds overleg gevoerd met de betreffende partij, de Privacy Officer, de FG en waar nodig ook met de CISO, waarna de verwerkersovereenkomst is goedgekeurd en vervolgens is afgesloten.

4.9 Privacy in het Sociaal Domein

Tussen de teams Samenleving, voornamelijk de juristen, de beleidsmedewerkers en de informatieadviseur, en de Privacy Officer is een goede samenwerking ontstaan. Indien nodig wordt tijdig de Privacy Officer geraadpleegd en om advies gevraagd.

4.10 Informatieveiligheid

In 2025 zijn grote wijzigingen doorgevoerd in de IT-infrastructuur van gemeente Barneveld. Hierdoor is veel aandacht en tijd van de CISO gegaan naar werk op operationeel niveau. Werk op strategisch niveau is daardoor vertraagd.

Ook is door de aanscherping van informatiebeveiligingsnormen het werk op het gebied van compliance sterk toegenomen. De directie en het bestuur hebben dit herkend en erkend. Besloten is om per 2026 formatie toe te wijzen voor ondersteuning van de CISO voor operationele taken.

De CISO heeft de jaarlijkse verantwoordingen in het kader van BAG, BGT, DigiD, Suwinet, ENSIA, BRP en PNIK opgeleverd.

4.11 Data Protection Impact Assessments

In 2025 zijn er DPIA's voor de onderstaande processen uitgevoerd:

1	Wet zorg en dwang en Wet verplichte ggz	Wet zorg en dwang en Wet verplichte ggz	Bestaand proces, Nieuwe verwerking
2	Tijdelijk huisverbod	Tijdelijk huisverbod	Bestaand proces, Nieuwe verwerking
3	Camera's gemeentelijke gebouwen	Camera's gemeentehuis	Nieuwe/gewijzigde verwerking
4	ZorgNed	Nieuwe applicatie voor Sociaal domein - Jeugd, Wmo en Regie	Nieuwe verwerking
5	Schuldhelpverlening	Vroegsignalering schuldhelp voorafgaand	Periodieke herziening
6	Schuldhelpverlening	Schuldhelpverlening	Periodieke herziening

In 2026 zullen er in ieder geval DPIA's voor de onderstaande processen worden uitgevoerd, waarbij dit voor de meeste processen een herziening en verdieping van de DPIA uit 2022 of 2023 betreft:

1	Wet Damocles	Bestuursrechtelijke handhaving	Periodieke herziening
2	Ondermijning- RIEC	Ondermijning	Periodieke herziening
3	Transcriberen keukentafelgesprekken	Transcriberen keukentafelgesprekken als aanvulling op DPIA Participatiewet	Aanvulling op DPIA Inkomen en Participatie
4	Handhaving boa's domein I	Handhaving boa's	Periodieke herziening
5	Leerplicht	Leerplicht (AVG en Wpg)	Periodieke herziening
6	Personeels- en salarisadministratie	Personeels- en salarisadministratie	Periodieke herziening. Dashboard mens-werk-geld meenemen in de DPIA.
7	Belastingen	Heffingen- en invorderingsadministratie Kwijtschelding gemeentelijke belastingen	Tijdens implementatie nieuwe applicatie/ Aanbesteding belastingapplicatie
8	Bodycams	Bodycams	Periodieke herziening
9	Leerlingenvervoer	Leerlingenvervoer	Periodieke herziening
10	Woonurgentie	Woonurgentie	Periodieke herziening
11	Telefonie- en contactcentrum KCC	Telefonie- en contactcentrum KCC	Periodieke herziening

Alle DPIA's vinden plaats aan de hand van een vragenlijst. Deze vragenlijst is gebaseerd op de vragenlijst van de beroepsvereniging voor IT-auditors NOREA en door de Privacy Officer aangepast en verder aangevuld. De vragenlijst ziet op zowel AVG als Wpg verwerkingen. Er wordt gevraagd naar onder andere de verwerkingsverantwoordelijke, de verwerkers, verwerkersovereenkomsten, nieuwe technieken, noodzaak van gegevensverwerking, aard van de persoons-/ politiegegevens (bijzonder of gevoelig), gegevensuitwisseling intern en extern, doelbinding, grondslag, transparantie, actualiteit, integriteit en beschikbaarheid van persoonsgegevens, rechten van betrokkenen, bewaartermijnen en beveiliging. Per proces wordt een rapportage opgesteld met bevindingen, conclusies en aanbevelingen, dat vervolgens aangevuld wordt met het advies van de FG.

Uit de in 2025 uitgevoerde DPIA's zijn maatregelen en aanbevelingen voortgekomen. Er zijn namelijk wat privacyrisico's geconstateerd. Dat houdt niet in dat er onzorgvuldig gewerkt wordt of dat medewerkers zich niet voldoende bewust zijn van het belang van een zorgvuldige

verwerking van persoons-/politiegegevens, maar ziet meer op het formeel vastleggen van werkprocesbeschrijvingen en werkinstructies. Ook komen er regelmatig technische/ICT-aspecten naar voren die niet direct opgelost kunnen worden, omdat een applicatie daarvoor (nog) niet voldoende toegerust is. In overleg met de leverancier en aanpassing van de applicatie of een aanbestedingen traject voor het aanschaffen van een upgrade of nieuwe applicatie kost tijd en daardoor is de onderstaande lijst langer en komt wellicht wat zorgwekkend over, maar er wordt nauwlettend op toegezien dat er – veelal met tussentijdse tijdelijke aanpassingen of handmatige oplossingen – toch AVG-/Wpg-proof gewerkt wordt.

In de in 2025 uitgevoerde DPIA's komen – samengevat – de volgende risico's naar voren:

- Er zijn geen afspraken gemaakt over controle op logging;
- De verwerking(en) is/zijn (nog) niet opgenomen in het register van verwerkingen of deze zijn onvoldoende actueel;
- De verwerkersovereenkomst is verouderd of (nog) niet ondertekend of afgesloten;
- Werkprocesbeschrijving/werkwijze/werkinstructie/richtlijn of protocol is/zijn verouderd en/of er blijkt onvoldoende uit welke persoons-/politiegegevens door wie opgevraagd, gedeeld en verwerkt mogen/moeten worden door zowel interne als externe partijen;
- Er wordt gebruik gemaakt van onbeveiligde mail;
- Er wordt gebruik gemaakt van het delen van gegevens via onbeveiligde usb-sticks;
- In de privacyverklaring op de website ontbreekt een (nieuwe) verwerking of bevat verouderde informatie;
- Medewerkers worden niet tijdig of onvoldoende geïnformeerd over een nieuwe verwerking;
- Er wordt gebruik gemaakt van 'echte' persoons-/politiegegevens in de testomgeving;
- Er is geen proces waarin is geregeld dat ouders geen toegang meer hebben tot het dossier als hun kind 16 jaar wordt;
- Toestemmingsverklaring is niet op de juiste grondslag gebaseerd;
- Er wordt een kopie ID-bewijs in het dossier opgeslagen terwijl dat niet noodzakelijk is, omdat verificatie voldoende is;
- Bij gebruik van whats app worden persoonsgegevens gedeeld, terwijl dit medium daar niet voor bedoeld is en daarvoor gebruik gemaakt moet worden van beveiligde mail (bij voorkeur vanuit de vak applicatie);
- Het informeren van betrokkenen ontbreekt op een aanvraagformulier;
- Op een aanvraagformulier wordt om toestemming gevraagd, maar het is onduidelijk waarvoor (gewone, bijzondere of gevoelige persoonsgegevens);
- In een vak applicatie zijn de bewaartermijnen niet goed ingeregeld, maar dit zal opgelost zijn zodra de nieuwe applicatie per 1 januari 2026 in gebruik genomen gaat worden;
- In een vak applicatie zijn de autorisaties te ruim geregeld, zodat meer medewerkers dan noodzakelijk gegevens kunnen inzien.

De volgende maatregelen zijn reeds genomen:

- Er zijn werkafspraken gemaakt over controle op logging;
- De verwerkingen is/zijn opgenomen in het register van verwerkingen;
- De verwerkersovereenkomst(en) is/zijn geactualiseerd, ondertekend en/of afgesloten;
- Er wordt gebruik gemaakt van een mailvoorziening binnen de vak applicatie of via pgax, zodat beveiligd gemaïld wordt.

Ook zijn er afspraken gemaakt over de termijn waarop andere maatregelen worden genomen zoals bijvoorbeeld in het geval dat wijzigingen in een werkprocesbeschrijving/werkwijze/werkinstructie/richtlijn of protocol opgenomen moeten worden, het opnemen van contact met de leverancier om de bewaartermijnen goed in te regelen of het maken van afspraken met

ketenpartners. Deze te nemen maatregelen kosten meer tijd, omdat er vaak meer interne en externe partijen bij betrokken zijn.

4.12 Bewustwording

Net als in voorgaande jaren, zijn er in 2025 workshops over Privacy en Informatiebeveiliging gehouden. Deze workshop is verplicht voor alle nieuwe medewerkers en wordt sinds 2023 in kleinere groepen gehouden voor een betere interactie. Belangrijk voor de bewustwording is ook de bekendheid en benaderbaarheid van de PO om als vraagbaak te fungeren. Hiervan is en wordt veel gebruik gemaakt.

In het najaar van 2025 is een tooling en een programma aangeschaft om het bewustzijn van de medewerkers op gebied van privacy en security te vergroten. Eind 2025/begin 2026 is de implementatie van deze tooling gepland en begin 2026 wordt gestart met enkele teams om dit uit te testen, voordat uitrol in de hele organisatie plaatsvindt.

4.13 Overige zaken

Er zijn een aantal andere zaken te melden over 2025. Dat zijn:

Onjuiste wijze van afhandelen registratiefase in Zaaksysteem

Bij het willen afsluiten van een afgehandelde/afgeronde zaak werd een terugkerende foutmelding gegeven die aangaf dat bepaalde kenmerken niet ingevuld zijn. Dit betrof o.a. geboortedatum, verklaring dat naar waarheid alles ingevuld is en de hoogte van een schadebedrag (betrof een aansprakelijkstelling). Dat zijn gegevens die alleen de indiener kan/mag en hoort in te vullen. In dit specifieke geval is dit door de medewerker ingevuld om de zaak af te kunnen sluiten en het niet mogelijk was dat de indiener het webformulier (achteraf) kon aanvullen met de ontbrekende gegevens. Het formulier was immers al ingestuurd en geregistreerd en is dan niet meer aan te passen. Daarom zijn geboortedatum 1-1-1900 en een fictief schadebedrag ingevuld met daarbij de opmerking dat deze gegevens incorrect zijn. Vervolgens is op voordracht van de FG door de applicatiebeheerder en de proceseigenaar uitgezocht waar de storing in zat en is dit verder opgelost, zodat dergelijke situaties niet meer voor mogen komen.

Onterechte inzage cv's bij benoeming commissieleden

Vanwege het eindigen van de termijnen van commissieleden is er een procedure gevolgd voor herbenoeming en benoeming van leden. De sollicitatie- en selectiecommissie heeft de cv's ingezien en beoordeeld en mede aan de hand van gesprekken zijn de gekozen en voorgedragen kandidaten opgenomen in het benoemingsbesluit. De benoeming door het college is alleen een formaliteit en zij hoeven die beoordeling niet over te doen. Het bijvoegen van cv's is niet nodig en ook vanuit de AVG niet gewenst.

Het college wenste echter tegen het advies van de FG in toch inzage in de gegevens van de geselecteerde en voorgedragen kandidaten. Als compromis zijn de cv's alsnog toegevoegd aan het collegevoorstel, maar de documenten zijn wel zodanig beveiligd en afgeschermd dat niemand buiten het college om deze documenten kon inzien.

4.14 Te verwachten ontwikkelingen wet- en regelgeving²

Hieronder zijn wetswijzigingen, waarin gegevensverwerking voorkomt en die in 2025 of 2026 in ontwikkeling zijn of in werking treden, opgenomen.

² Bij de totstandkoming van deze paragraaf is gebruik gemaakt van AI, omdat daarmee het doorzoeken van vele websites vergemakkelijkt kan worden. Daarop is vervolgens een check gedaan naar betrouwbaarheid en logica van de ontvangen zoekresultaten.

4.14.1 Inwerkingtreding Wet PARTA

Per 1 juli 2025 is de Wet gegevensverwerking Persoonsgerichte Aanpak Radicalisering en Terroristische Activiteiten (hierna: Wet PARTA) in werking getreden. De wet biedt duidelijkheid over taken, verantwoordelijkheden, grondslagen voor multilaterale gegevensverwerking en waarborgen voor gegevensbescherming die aansluiten bij de AVG.

Regiefunctie burgemeester

De burgemeester heeft op grond van de Wet PARTA de wettelijke taak om te zorgen voor het instand houden van een casusoverleg voor de persoonsgerichte aanpak van radicalisering en terroristische activiteiten (de zogenoemde regiefunctie).

Grondslag voor gegevensuitwisseling

De Wet PARTA geeft de juridische grondslag voor de gegevensuitwisseling, inclusief zogenoemde bijzondere persoonsgegevens, tussen organisaties die betrokken zijn bij een casus. De burgemeester en het college van burgemeester en wethouders, politie, het openbaar ministerie, reclasseringsinstellingen en de raad voor de kinderbescherming zijn aangewezen als reguliere deelnemers.

Aanvullende waarborgen voor gegevensbescherming

De wet regelt ook diverse aanvullende waarborgen voor een goede bescherming van de persoonsgegevens die de deelnemers aan de casusoverleggen verwerken. Deze vormen een aanvulling op de rechten en plichten uit de AVG, die nu al van toepassing zijn.

Continuering van bestaande praktijk

De wet continueert en legt de bestaande praktijk van de persoonsgerichte aanpak radicalisering vast. De wet sluit inhoudelijk zoveel mogelijk aan bij de Wet Gegevensverwerking door Samenwerkingsverbanden (WGS). Hieronder vallen de Zorg- en Veiligheidshuizen. Dus als een gemeente al een zorgvuldige werkwijze heeft voor de persoonsgerichte aanpak van radicalisering en terroristische activiteiten, dan is het niet nodig om deze aanpak helemaal anders te organiseren.

Ondersteuning voor kleinere gemeenten

Kleinere gemeenten kunnen voor de inrichting van de verplichting om een casusoverleg in stand te houden ondersteuning zoeken in de ervaring en faciliteiten van grotere gemeenten en/of regionale zorg- en veiligheidshuizen.

4.14.2 Wet Aanpak Meervoudige problematiek Sociaal Domein

De inwerkingtreding van de Wet Aanpak Meervoudige problematiek Sociaal Domein (Wams) stond gepland op 1 januari 2024. Maar uit een nieuwsbericht van de VNG van 22 november 2023 blijkt dat de focus van de handreikingen en checklists niet meer op het wetsvoorstel ligt, maar op het versterken van de aanpak van meervoudige problematiek in het sociaal domein. Dit omdat de wet op 12 september 2023 controversieel is verklaard, maar het wel verstandig is om alvast met het versterken van de aanpak van meervoudige problematiek aan de slag te gaan.

Het is de bedoeling dat in de Wet Wams de wettelijke borging van de regionale meldpunten wordt voorbereid. De Wet Wams betreft een aanpassing van de Wet maatschappelijke ondersteuning (Wmo) en regelt een basis voor gegevensdeling in het Sociaal Domein en een gemeentelijk meldpunt niet-acuut. Ook deze wet levert, naast nieuwe mogelijkheden, vanuit privacy & security risico's op, zodat bij implementatie betrokkenheid van de PO, CISO en FG van belang is. Vooralsnog is er nog geen duidelijkheid over de behandeling van dit wetsvoorstel, de datum van inwerkingtreding en de implementatie. Zodra het nieuwe kabinet gevormd is in 2024 zal dit wetsvoorstel weer opgepakt moeten gaan worden. De VNG adviseert gemeenten niet af te

wachten, maar al verder te gaan met de nodige voorbereidingen omdat het te verwachten is dat deze wet er wel komt, zij het met enige vertraging. In het jaar 2024 zijn hierin geen ontwikkelingen geweest en is er geen vervolg meer gekomen op het moment van controversieel verklaren van het wetsvoorstel.

In 2025 is het kabinet wederom gevallen en is er geen gevolg meer gekomen op het eerder controversieel verklaarde wetsvoorstel. In juli 2025 heeft de Tweede Kamer het voorstel nog niet geagendeerd. Wel is er een beleidsnota rond juli 2025 gepubliceerd en worden gemeenten ondersteund via VNG-activiteiten, als voorbereiding op mogelijke toekomstige inwerkingtreding. Het nieuwe kabinet is na de verkiezingen van oktober 2025 nog niet gevormd, zodat er begin 2026 nog geen ontwikkelingen te melden zijn.

4.14.3 aanpassingen AVG en AI Act (AI Verordening)

Er wordt een 7 of 8 stappen roadmap voor de uitvoering van de AVG geïntroduceerd. Dat bestaat uit de volgende onderdelen: identificeren van verwerkingsactiviteiten, DPIA's uitvoeren, wettelijke grondslagen vastleggen, dataminimalisatie optimaliseren, transparantie borgen, rechten van betrokkenen faciliteren en toezicht en 'proof of compliance' (documentatie, audits) instellen.

Ook is er een toekomstige versoepeling te verwachten die een vereenvoudiging inhoudt (voor mkb) via het Digital Omnibus-pakket³, inclusief versoepeling van gegevensregisters en DPIA-verplichtingen. Het Digital Omnibus pakket (november 2025) houdt o.a. in: herschrijven persoonsgegevensdefinitie, zodat enkel data te beschouwen is als identificeerbaar persoonsgegeven, en een 'incidentmeldings-single-point' wat het samenvoegen van meldingen onder AVG, NIS2, DORA⁴, DORA etc., met geharmoniseerde deadlines en formats inhoudt.

Daarnaast is sprake van uitstel AI Act verplichtingen⁵. De deadlines voor hoogrisico-AI zijn geschrapt en uitgesteld zijn tot eind 2027 of 2028. De fasen worden als volgt aangepast:

- Fase 1 (feb 2025): verbod op ongeoorloofde AI-toepassingen zoals sociale scoring, emotieherkenning, biometrische surveillance.
- Fase 2 (aug 2025): governanceverplichtingen voor General Purpose AI – risicoanalyses, bias-mitigatie, transparantie, menselijke overzicht.
- Voorbereiding 2026-2028: risicoklassificatie per AI-systeem, conformiteitsrapportages, kwaliteitsmanagement, documentatie & toezicht.

4.15 Evaluatie Toezichtplan 2025-2026

Met behulp van de in het Toezichtplan opgenomen actiepunten en planning is overzichtelijk welke zaken er op welk moment gecontroleerd moeten worden aan de hand van AVG, Wpg of gemaakte afspraken.

Weliswaar schuiven actiepunten – net als bij DPIA's – regelmatig op in de planning, maar de bewustwording van zaken die geregeld, gecontroleerd en afgestemd moeten worden is hoger dan in voorgaande jaren. De medewerking en het oppakken van bijvoorbeeld maatregelen uit DPIA's, uitgevoerde periodieke controles of uit een verbeterplan dat voortgekomen is uit een

³ [EU Digital Omnibus: How EU Data, Cyber, and AI Rules Will Shift | Insights | Jones Day](#)

⁴ DORA = Digital Operational Resilience Act. DORA is van toepassing op banken en verzekeraars en is niet direct relevant voor gemeenten.

⁵ [EU AI Act 2025: Practical Compliance Steps for Businesses](#)

intern of extern gehouden audit verloopt soepeler en men weet elkaar beter te vinden om zaken te bespreken en afspraken te maken over op te pakken actiepunten.

In dit jaarverslag wordt niet inhoudelijk ingegaan op de verschillende actiepunten, maar geconcludeerd kan worden dat het Toezichtplan behulpzaam is bij het overzicht houden en de samenwerking tussen verschillende functionarissen.

Enkele actiepunten die in 2025 niet afgerond konden worden, bijvoorbeeld door afhankelijkheid of planning van externe partijen, wordt aan het begin van 2026 opgepakt. De planning en actiepunten voor 2026 worden daarop aangepast. Evaluatie daarvan vindt plaats in het jaarverslag over 2026, waarna ook een toezichtplan voor 2027-2028 wordt opgesteld.

5. AANBEVELINGEN EN ACTIES

5.1 Aanbevelingen

Belang: het is belangrijk om het bewustzijn over het belang van het zorgvuldig omgaan met en verwerken van persoons-/politiegegevens blijvend onder de aandacht te houden bij de medewerkers. Daarbij is de combinatie privacy en informatieveiligheid een vast gegeven.

Aanbeveling: voor een blijvend bewustzijn regelmatig berichten op intranet plaatsen. Ook kan met de teamleiders afgesproken worden dat de Privacy Officer met enige regelmaat of incidenteel aanschuift bij teamoverleggen om in algemene zin of aan de hand van een specifieke casus het bewustzijn over het omgaan met persoons-/politiegegevens hoog te houden.

Vanuit informatieveiligheid blijft aandacht gevraagd worden voor het vergrendelen van het beeldscherm als de werkplek verlaten wordt. Verder is het van belang dat fysieke documenten veilig achter slot en grendel liggen en dat bezoekers tot aan de deur worden begeleid. Ook bij het thuiswerken moet worden gelet op het opbergen van documenten, omdat het niet de bedoeling is dat onbevoegden, denk aan huisgenoten of bezoekers, kennis kunnen nemen van vertrouwelijke informatie.

Om het bewustzijn te vergroten is in najaar 2025 een tooling en een programma aangeschaft voor bewustwordingstraining voor privacy en informatiebeveiliging voor nieuwe én bestaande medewerkers. In Q1 2026 zal gestart worden met een tweetal teams als testgroep. Als dat goed verloopt, wordt deze tooling in de hele organisatie uitgerold.

Belang: een andere passende technische en organisatorische maatregel ter beveiliging van persoonsgegevens is het bewust omgaan met chatrobots, omdat de uitkomsten daarvan niet allen even betrouwbaar zijn.

Aanbeveling: wat betreft de chatrobots is in 2024 en 2025 aanbevolen om alleen gebruik te maken van co-pilot (zakelijke versie), maar zonder dat daar persoonsgegevens en/of dossiers in verwerkt worden. Daarvoor is geen enkele chatrobot voldoende toegerust en daarmee onvoldoende betrouwbaar. Voor algemenere informatie kan een chatrobot een handige aanvulling/ handvatten bieden.

Belang: digitale mogelijkheden groeien en worden steeds diverser. AI speelt daarbij een belangrijke rol en het is van belang dat zorgvuldig omgegaan wordt met het toepassen van AI in de gemeentelijke dienstverlening. De bescherming van persoons-/politiegegevens moet goed geborgd zijn, voordat daar veelvuldig op de juiste wijze gebruik van gemaakt kan worden.

In 2025 is verder onderzoek gedaan naar (on)mogelijkheden en risico's van het gebruik van AI en is aangevangen met het opstellen van een algoritmeregister. In 2026 zal dit verder uitgewerkt worden en wordt de organisatie daar stapsgewijs bij betrokken. Ook zijn er in 2025 een aantal pilots gestart waarvan de evaluatie en het daarna wel of niet in gebruik nemen op de planning staat.

Aanbeveling: betrek de juiste stakeholders bij de ontwikkelingen en inzet van AI in de gemeentelijke dienstverlening. Evalueer de pilots voorafgaande aan het in gebruik nemen daarvan. En waar nodig voer een DPIA uit op de voorgenomen toepassing.

5.2 Acties voor 2026

In de voorgaande hoofdstukken is aangegeven welke werkzaamheden in 2025 zijn uitgevoerd en in paragraaf 5.1. worden de aanbevelingen genoemd. In deze laatste paragraaf wordt nader ingegaan op de acties die hiervoor al kort genoemd zijn. In 2026 worden de onderstaande acties opgepakt, waarover in het Jaarverslag FG 2026 gerapporteerd zal worden.

- DPIA's: evalueren van de opgepakte en uitgevoerde uit de rapportages voortgekomen aanbevelingen en maatregelen. Daarna toezien op de naleving ervan.
- DPIA's: uitvoeren DPIA's voor nieuwe/gewijzigde verwerkingen en herzien en actualiseren van uitgevoerde DPIA's in verband met de 3-jaarlijkse herziening.
- Actueel houden en aanpassen register van verwerkingen voor wat betreft AVG verwerkingen, na input uit uitgevoerde DPIA's.
- Uitvoering geven aan nog openstaande acties uit het verbeterplan Wpg;
- Uitvoeren jaarlijkse interne audit Wpg en meewerken aan het verbeterplan dat voortkomt uit de in 2025 uitgevoerde vierjaarlijks externe audit Wpg;
- Continue aandacht houden voor het belang van het afsluiten van verwerkersovereenkomsten (AVG en Wpg) en het overzicht actueel houden. Verouderde verwerkersovereenkomsten actualiseren en nieuwe verwerkersovereenkomsten afsluiten met nieuwe verwerkers.
- Vervolg workshops Privacy & Informatieveiligheid voor nieuwe medewerkers.
- Starten met uitrol van tooling en een programma voor bewustwordingstraining voor privacy en informatiebeveiliging voor nieuwe én bestaande medewerkers.
- Op verzoek aansluiten bij teamoverleggen om privacy binnen een bepaald vakgebied te bespreken.
- Uitvoeren van de zelfevaluatie/borging waarna beoordeling van de zelfevaluatie/borging gedaan kan worden en de daaruit voortkomende acties en verbeterpunten opgepakt en uitgezet kunnen worden in de organisatie. Vervolgens toezien op de naleving daarvan.
- Verbeteren bewustwording privacy en beeld van de privacyregelgeving positiever maken.
- Actueel houden en aanpassen register van verwerking voor wat betreft de Wpg verwerkingen, na input uitgevoerde Wpg controles.
- Evalueren van en adviseren over pilots waarin AI wordt toegepast, voordat besloten wordt dit toe te gaan passen in de dienstverlening.

BIJLAGE Autoriteit Persoonsgegevens Jaarplan 2025⁶

Citaat: “Heldere communicatie en uitleg om burgers beter te beschermen in een digitale wereld. Het beschermen van mensen in een digitale wereld: daar maakt de Autoriteit Persoonsgegevens (AP) zich sterk voor. Maatschappelijke, technologische en politieke ontwikkelingen – zowel binnen als buiten – hebben direct effect op ons werk. Organisaties verzamelen, verwerken en delen persoonsgegevens op grote schaal, en dit neemt alleen maar toe. Onder de juiste voorwaarden draagt dat bij aan innovatie en maatschappelijke vooruitgang. Het gebruiken van persoonsgegevens moet wel altijd rechtmatig, eerlijk en transparant gebeuren. Mensen moeten grip kunnen houden op hun persoonlijke gegevens. Want als dat niet gebeurt, dan kunnen mensen –bedoeld of onbedoeld– risico lopen op uitsluiting, manipulatie of discriminatie. Als AP houden we toezicht op de naleving van de regels door organisaties. Wij leggen uit wat er wél kan. Zo helpen we organisaties én burgers vooruit.

Toezicht houden betekent ook keuzes maken: ons toezichtveld wordt steeds groter en onze middelen zijn beperkt. Daarom hebben we onze fundamentele waarden bij het beschermen van persoonsgegevens vastgelegd: non-discriminatie, persoonlijke autonomie en vrijheid, en controleerbare en transparante macht. Door deze bril kijken we naar ons toezicht.

Begin 2025 verscheen de AP-evaluatie met aanbevelingen en adviezen voor onze plannen voor de komende jaren. Daar zijn we mee aan de slag gegaan. We zetten meer in op alternatieve interventies, zoals het uitleggen van de wet aan organisaties, en voorlichting. We leggen alleen boetes op als het nodig is. Zo beschermen we mensen in een digitale wereld. In 2025 besteden we, net als vorig jaar, extra aandacht aan deze vijf thema's:

Algoritmes & AI

Onze wereld wordt steeds digitaler en de mogelijkheden van [algoritmes en artificiële intelligentie](#) (AI) nemen snel toe. Dit biedt een hoop kansen, maar kan ook leiden tot onrechtmatige verwerking van gegevens, discriminatie, willekeur, gebrek aan transparantie of misleiding en manipulatie. We willen deze risico's voorkomen door onze grondrechten goed en proactief te beschermen. In 2025 verwachten we een intensivering van onze werkzaamheden op het gebied van algoritmes en AI. Hieraan werkt onder meer de Directie Coördinatie Algoritmes. Lees de [Werkagenda coördinerend AI- en algoritmetoezicht 2025](#) voor meer informatie.

Wat doen we onder andere in 2025?

- We publiceren de halfjaarlijkse Rapportage AI- & Algoritmerisico's Nederland (RAN) waarin we nieuwe ontwikkelingen voor AI en algoritmes duiden, risico's benoemen en inzoomen op specifieke toepassingen. We besteden extra aandacht aan het bereiken van specifieke doelgroepen, zoals bedrijven die algoritmes ontwikkelen of inzetten, onder meer door het organiseren van roadshows.
- Wij richten een wetenschappelijke commissie op, met onder andere expertise op het gebied van AI en algoritmes.
- We starten een netwerk van meldpunten om informatie over incidenten rond algoritmes en AI op te halen bij meldpunten en belangenorganisaties.
- We werken samen met andere toezichthouders in de voorbereiding op het toezicht op de AI-verordening en de lancering van de AI regulatory sandbox in 2026, waar organisaties AI-systemen in wording kunnen testen.

⁶ <https://www.autoriteitpersoonsgegevens.nl/over-de-autoriteit-persoonsgegevens/ap-jaarplan-2025>, volledig citaat overgenomen.

- We betrekken stakeholders via oproepen tot input en dialoogbijeenkomsten.
- Vanuit het gegevensbeschermingstoezicht ligt de focus op algoritmes en AI op verschillende aspecten van geautomatiseerde besluitvorming, zoals betekenisvolle menselijke tussenkomst, de rechten van betrokkenen, en de relatie met leveranciers van software. Hierover verwachten we informatie te publiceren met concrete handvaten voor organisaties om verantwoord met algoritmes en AI om te gaan.

Big Tech

Grote techbedrijven gebruiken de gegevens van hun gebruikers als brandstof. En dat is vaak niet in lijn met de Algemene verordening gegevensbescherming (AVG). Persoonsgegevens worden gebruikt om gericht reclames te kunnen aanbieden, AI-modellen te trainen en om gepersonaliseerde inhoud aan te bieden zodat gebruikers langer online blijven. Daarom is het van groot belang om hier scherp toezicht op te blijven houden. Burgers moeten de regie kunnen houden over hun persoonsgegevens. De AP blijft hier in 2025 aan werken, samen met andere (internationale) toezichthouders.

Wat doen we onder andere in 2025?

- We blijven (internationaal) onderzoek doen naar mogelijke overtredingen door grote techbedrijven.
- Samen met de andere Europese toezichthouders voorkomen we dat grote techbedrijven misbruik maken van de persoonsgegevens van Europese burgers bij het ontwikkelen en aanbieden van AI-modellen.
- In 2025 werken wij, samen met de Autoriteit Consument & Markt (ACM), aan het verder vormgeven van het toezicht op de Digitaaldienstenverordening (DSA). Zo kunnen we de fundamentele rechten van burgers nog beter beschermen.
- Persoonsgegevens zijn niet overal zo veilig als in de Europese Economische Ruimte (EER). Bedrijven die persoonsgegevens doorgeven naar buiten de EER moeten maatregelen treffen om een vergelijkbare bescherming te garanderen. De AP besteedt aandacht aan internationale doorgiften in onderzoeken, en werkt samen met Europese collega's om te controleren of bedrijven voldoende maatregelen hebben getroffen.

Vrijheid & veiligheid

Wij willen bijdragen aan een verdedigbare balans tussen vrijheid en veiligheid. Het zijn twee kanten van dezelfde medaille, waarbij veiligheid de vrijheid bevordert. Om de veiligheid te bewaken worden soms maatregelen genomen die de vrijheid inperken, zoals het delen van gegevens voor opsporing van strafbare feiten.

Wat doen we onder andere in 2025?

- Wij bouwen verder aan een meerjarig programma Vrijheid en veiligheid. Het gebruiken van gegevens is nodig om goed onderzoek uit te voeren bij de opsporing van strafbare feiten, het bewaken van de openbare orde en onze buitengrenzen. Dit moet zorgvuldig en binnen de grenzen van de wet gebeuren.
- Bij de inzet van nieuwe, risicovolle technologieën in het veiligheidsdomein adviseren we gevraagd en ongevraagd over wat wel en niet mag.
- We versterken ons toezicht op de politie om vanuit onze positie als toezichthouder te zorgen voor een verbeterde registratie, bewaring en rechtmatig gebruik van persoonsgegevens door de politie.

- We ontvangen al jaren veel klachten en tips over deurbelcamera's van particulieren. Burgers geven aan dat er inbreuk wordt gemaakt op hun persoonlijke levenssfeer. Daarom gaan we hier extra aandacht aan besteden en praktische handvaten voor veilig gebruik geven.
- We zetten een programma op om intensiever onderzoek te doen naar en toezicht te houden op grote Europese systemen en databases voor de bescherming van de buitengrenzen van het Schengengebied.
- We zijn nauw betrokken bij de implementatie van de nieuwe Europese anti-witwas regels.

Datahandel

Slimme producten en diensten genereren bergen waardevolle data, wat kan leiden tot de ongeoorloofde doorverkoop van persoonsgegevens. Dat gebeurt niet alleen in Nederland, maar ook internationaal. Dat mag niet en willen we een halt toe roepen.

Wat doen we onder andere in 2025?

- We zetten extra in op naleving van de regels voor datahandel. En geven voorlichting en uitleg over de juiste manier om met gegevens om te gaan, vooral gericht op het MKB.
- We zetten ook in op meer voorlichting aan consumenten over wat er met hun gegevens gebeurt en hoe ze hun privacyrechten kunnen uitoefenen.
- We geven prioriteit aan onderzoek naar klachten en datalekmeldingen die een duidelijke link hebben met datahandel.
- We komen dit jaar met de eerste resultaten van onze inspanningen op het gebied van datahandel.
- We blijven het ongeoorloofd online volgen van mensen, bijvoorbeeld via cookies en andere trackingmogelijkheden, op verschillende fronten aanpakken.

Digitale overheid

Centrale en lokale overheden, uitvoeringsorganisaties en politie en justitie beschikken over grote hoeveelheden - vaak gevoelige en bijzondere - persoonsgegevens van Nederlanders en maken hier veel gebruik van. Het risico dat burgers in de knel komen is groot als de overheid verkeerd omgaat met je persoonsgegevens. Vooral omdat het vaak verplicht is om gegevens af te staan aan de overheid. Bovendien heeft de overheid een voorbeeldfunctie als het gaat om de verantwoorde omgang met persoonsgegevens. Daarom zien we hier komend jaar extra op toe.

Wat doen we onder andere in 2025?

- We delen gevraagd en ongevraagd kennis over gegevensuitwisseling in het sociaal domein, daar waar mensen vaak geen andere keuze hebben dan het delen van hun gegevens. We besteden extra aandacht aan de bescherming van de persoonsgegevens van kinderen.
- We gaan in 2025 door met het reserveren van extra capaciteit om onderzoek te doen naar overheden en uitvoeringsorganisaties die persoonsgegevens van burgers gebruiken in algoritmes.
- De AP heeft het toezicht op de Belastingdienst geïntensiveerd. Daarmee verwacht de AP bij te dragen aan een duurzame verbetering van de bescherming van persoonsgegevens van Nederlandse burgers door de Belastingdienst. Onder meer wordt nagegaan of

risicoselecties zorgvuldig plaatsvinden en discriminatie wordt voorkomen. En of de privacyorganisatie toereikend is ingericht.

- We besteden opnieuw aandacht aan het delen van gegevens tussen verschillende onderdelen van de overheid en andere organisaties. Ook de risico's van het gebruik van algoritmes bij de overheid blijven we in de gaten houden, zoals discriminatie.

Wat doen we niet?

Keuzes maken betekent ook dat we andere dingen niet kunnen. Het budget en de capaciteit van de AP zijn immers beperkt. Dit kunnen we in 2025 niet optimaal:

- Alle datalekken de aandacht geven die ze verdienen, ondanks de mogelijke gevolgen voor de slachtoffers van deze datalekken.
- Alle klachten sneller afhandelen. Het duurt vaak meer dan een halfjaar voordat we een klacht kunnen oppakken. Ook snel inspringen op actuele issues lukt niet altijd.
- Proactief advies geven over wetgeving, zodat persoonsgegevens goed zijn beschermd in de wet.
- Sectoren die veel persoonsgegevens verwerken, zoals de zorg, onderwijs, energie, overheid en financiën, de aandacht geven die nodig is.

Financiering bij toenemend datagebruik

Het budget van de AP is afgelopen jaren telkens licht gegroeid, tot ca. €49 miljoen voor 2025 en verder. De financiering van het toezicht van de AP blijft daarmee echter ver achter op de hoge mate van digitalisering van Nederland.

De ernst van de situatie bepaalt de actie die we ondernemen. Daarvoor hebben wij een breed toezichtsinstrumentarium. Bij voorkeur gaan we eerst in gesprek, of geven we uitleg over de wet. Daar waar het nodig is, leggen we boetes op. Welk middel we kiezen, hangt af van de ernst van het probleem, de urgentie en het oordeel van onze professionals. Dit vraagt wel om de financiële, bestuurlijke en operationele armslag om steeds de juiste mensen, middelen en methodes te kunnen inzetten bij onze taak. De [Parlementaire Enquêtecommissie Fraudebeleid en Dienstverlening](#) kwam eerder ook tot deze conclusie.

Om onze taken goed te kunnen vervullen moet ons structurele budget groeien.

AP in vergelijking met andere toezichthouders

Gerealiseerd budget in 2024:

AP	AFM	NLA	ACM
47.4	142.7 (geraamd)	222	115.1

Cijfers uit 2024, bedragen in miljoenen euro.

AP= Autoriteit Persoonsgegevens, AFM = Autoriteit Financiële Markten, NLA = Nederlandse arbeidsinspectie, ACM = Autoriteit Consument & Markt.

Aanbevelingen en adviezen AP-evaluatie uitvoeren

In 2024 heeft een commissie van externe deskundigen, onder leiding van onafhankelijk voorzitter Paul Schnabel een breed evaluatieonderzoek uitgevoerd over de periode 2018-2024. In 2025 gaan we met de aanbevelingen en de adviezen van de AP-evaluatie aan de slag.

Er is een nadrukkelijke verduidelijking nodig van het AP-beleid over normen en handhaving. Met andere woorden: meer en helderdere communicatie over wat wel en niet mag. Dat betekent luisteren, en in gesprek gaan op een manier die rekening houdt met het eigen karakter en de identiteit van de partijen waar wij ons op richten. Een concreet voorbeeld van hoe we dat gesprek beter kunnen voeren, is het vaker uitzetten van consultaties. Zo kunnen we de ideeën en verwachtingen van de bij ons werkveld betrokken actoren in acht nemen in de uitvoering van ons toezicht.

De belangrijkste aanbeveling van de commissie herkennen wij goed: een andere tijd vraagt om een andere houding. Met inachtneming van de uitdagingen die we hebben ervaren in de eerste jaren van de AVG en de Richtlijn gegevensbescherming bij rechtshandhaving (RGR). We zijn hier in 2024 mee aan de slag gegaan, met name via een verbeterde informatievoorziening en actievere voorlichting naar organisaties, burgers en collega-experts. In 2025 zullen we nog meer investeren in onze lopende inspanningen, bijvoorbeeld in het verbeteren van de samenwerking met de functionarissen gegevensbescherming (FG's) van gegevens verzamelende en verwerkende organisaties en in de verdere ontwikkelingen van onze contacten met burgers.

De evaluatie laat zien dat de meeste winst is te boeken op het verder verbeteren en versnellen van het persoonlijk contact 'op ooghoogte', in onze toon en toelichting. Dat vertalen wij als 'helder op de inhoud, benaderbaar op de persoon'. Zo hebben we recent met VNO-NCW afgesproken dat we het komende jaar intensiever met brancheverenigingen zullen overleggen, zoals we ook al doen met de burger- en consumentenorganisaties.

Zo kunnen we de komende jaren zo goed mogelijk werk maken van het beschermen van mensen in een digitale wereld. En organisaties uitleggen wat er wél kan en stimuleren bij privacyvriendelijke innovaties. Zo helpen we de samenleving vooruit" [einde citaat].