JAARVERSLAG AVG / WPG 2024

GEMEENTE NOARD EAST FRYSLÂN

Toezicht Algemene Verordening Gegevensbescherming / Wet politiegegevens

Bevindingen en aanbevelingen van de Functionaris Gegevensbescherming

Inhoud

INLEIDING 3

1 TOETSINGSKADER 4

1.1 WETTELIJK KADER 4
1.2 BORGINGSPRODUCT IBD 4

2 BELANGRIJKSTE BEVINDINGEN 5

3 ONTWIKKELINGEN EN BELANGRIJKE GEBEURTENISSEN 6

3.1 NOARDEAST-FRYSLÂN EN DANTUMADIEL 6
3.2 WET POLITIEGEGEVENS 6
3.3 AUTORITEIT PERSOONSGEGEVENS 7
3.4 VOORUITBLIK: UITBREIDING WETGEVING 7

4 VERPLICHTINGEN ONDER DE AVG EN WPG 9

4.1 FUNCTIONARIS GEGEVENSBESCHERMING 9
4.2 PRIVACYBELEID 9
4.3 REGISTER VAN VERWERKINGSACTIVITEITEN 10
4.4 DATA PROTECTION IMPACT ASSESSMENTS 10
4.5 REGISTRATIE EN MELDPLICHT DATALEKKEN 10
4.6 RECHTEN VAN BETROKKENEN, BEZWAARSCHRIFTEN EN KLACHTEN 11

BIJLAGE: OVERZICHT VAN AANBEVELINGEN 12

BIJLAGE: VERKLARENDE WOORDENLIJST 2

Inleiding

In 2018 is de Algemene Verordening Gegevensbescherming[1] (AVG) in werking getreden. De AVG zorgt voor een verhoogde aandacht voor een rechtmatige verwerking van persoonsgegevens. De overheid heeft hierin een belangrijke voorbeeldfunctie. Gemeenten verwerken immers bij de uitoefening van hun taken veel informatie. Niet alleen persoonlijke informatie van eigen inwoners, maar ook van andere burgers, medewerkers, externen en zakenrelaties.

De AVG beschrijft het wettelijk kader voor het verwerken van persoonsgegevens. Daarnaast heeft de gemeente ook te maken met tal van privacyregels in sectorspecifieke wetgeving. De Wet politiegegevens (Wpg) is van toepassing op de verwerking van persoonsgegevens door de bijzonder opsporingsambtenaar (boa) in het kader van zijn opsporingstaak. De Wpg stelt net als de AVG verschillende eisen aan die verwerkingen, zoals het aanwijzen van een interne toezichthouder, de registers voor verwerkingen en datalekken. Dit alles heeft gevolgen voor de inrichting van processen en systemen in en van de gemeente.

Organisaties zijn verantwoordingsplichtig voor naleving van de privacywetgeving. zij moet aan kunnen tonen dat zij aan de wettelijk vereisten voldoet. De kern is de plicht voor de verwerkingsverantwoordelijke om voorafgaand aan, tijdens en én na de verwerking van persoonsgegevens aantoonbaar een passende set van organisatorische, procedurele en technische maatregelen te hebben[2].

De AVG raakt vrijwel alle processen van de van gemeente. Dit vloeit voort uit de taken die de gemeente voor inwoners en andere betrokkenen uitvoert. Zonder persoonsgegevens kan de gemeente haar taken niet uitvoeren. Het aantoonbaar voldoen aan de AVG draagt in belangrijke mate bij aan een betrouwbare overheid.

Voor u ligt het verslag van de bevindingen over het jaar 2024 van de Functionaris voor Gegevensbescherming (FG). Deze is binnen de gemeente Noardeast-Fryslân belast met het houden van onafhankelijk intern toezicht op de naleving van de AVG en de Wpg. Tot de taken[3] van de FG behoort ten minste het adviseren en informeren van de verwerkingsverantwoordelijke over zijn verplichtingen uit hoofde van de wet- en regelgeving (gevraagd én ongevraagd) en het toezien op de naleving daarvan.

De FG brengt rechtstreeks verslag uit aan de hoogste leidinggevende. Deze rapportage geeft een beeld van de stand van zaken van de naleving van de AVG door de organisatie. Het rapport schetst een aantal belangrijke ontwikkelingen, trends en gebeurtenissen in 2024. Daarbij doe ik concrete aanbevelingen voor verdere borging van de AVG-compliancy. Het gaat daarbij om de verwerkingen van persoonsgegevens die onder de verantwoordelijkheid van het college van burgemeester en wethouders, de burgemeester en de gemeenteraad worden uitgevoerd.

Rudy Cuperus
Functionaris Gegevensbescherming Noardeast-Fryslân en Dantumadiel
April 2025

Leeswijzer

Hoofdstuk 1 beschrijft het toetsingskader. Hoofdstuk 2 beschrijft de belangrijkste bevindingen in het verslagjaar. Hoofdstuk 3 beschrijft een aantal ontwikkelingen en belangrijke gebeurtenissen die de gemeente raken. In hoofdstuk 3 lopen we langs de basisverplichtingen die de AVG aan de verwerkingsverantwoordelijke oplegt. Met deze verplichtingen kan hij aantonen dat hij aan de vereisten voldoet (verantwoordingsplicht).

[1] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG

[2] Artikel 5 en 24 AVG
[3] Artikel 39 AVG, artikel 36 Wpg

1 Toetsingskader

1.1 Wettelijk kader

De basis is de Europese Algemene Verordening Gegevensbescherming (AVG) die sinds 2018 van kracht is. Een aantal bevoegdheden is uitgewerkt in de Nederlandse Uitvoeringswet AVG (UAVG). Voor de opsporingstaak van bijzonder opsporingsambtenaren (boa's) stelt de Wet politiegegevens (Wpg) de kaders. In verschillende materiewetgeving zijn bepalingen over verwerkingen van persoonsgegevens opgenomen. In gemeentelijk privacybeleid geeft de gemeente aan hoe zij uitvoering geeft aan de eisen die de AVG en de Wpg stellen.

1.2 Borgingsproduct IBD

De Informatiebeveiligingsdienst (IBD/VNG) heeft een toetsingskader opgesteld waarmee gemeenten inzicht kunnen krijgen in de mate waarin zij voldoen aan de AVG[4]. Het kader toetst uitsluitende de onderwerpen die de IBD als noodzakelijk beschouwt om aan de AVG te voldoen. Het toetsingskader is opgebouwd uit zeven thema's waarop getoetst wordt.

Beleid	De organisatie heeft processen en bijbehorende verantwoordelijkheden en risico's in kaart gebracht en vastgelegd in beleidsstukken. Deze stukken moeten voor alle werknemers vindbaar en begrijpelijk zijn.
Processen	De organisatie heeft alle processen waarbinnen persoonsgegevens worden verwerkt in kaart gebracht. De beschrijving van deze processen wordt actueel gehouden, werkinstructies worden nageleefd en processen met een hoog risico worden getoetst op juistheid.
Organisatorische inbedding	De organisatie heeft een FG aangesteld en kan zich voor inhoudelijke vraagstukken tot een intern privacyteam richten. Er wordt doorlopend aan bewustwording gedaan.
Rechten van betrokkenen	De organisatie voldoet aan alle wettelijke eisen die er zijn op het gebied van rechten van betrokkenen. De organisatie is transparant over hoe en welke persoonsgegevens verwerkt worden.
Samenwerking	De organisatie heeft in kaart gebracht met wie zij samenwerkt en heeft daarbij passende afspraken gemaakt. Deze afspraken worden door de betrokken partijen nageleefd.
Gegevens-bescherming	Hoewel pas echt een beeld kan worden geschetst van de stand van zaken op het gebied van gegevensbescherming middels de Baseline Informatiebeveiliging Overheid, zijn privacy en gegevensbescherming niet geheel los van elkaar te trekken. Een aantal informatiebeveiligingsaspecten met een duidelijke privacycomponent zijn dan ook in het Borgingsproduct opgenomen. Denk bijvoorbeeld aan de handelswijze bij datalekken. De CISO kan helpen bij het beoordelen van de mate waarin aan de bij dit thema opgenomen maatregelen wordt voldaan. Wanneer deze maatregelen voldoende zijn geïmplementeerd houdt dat dus niet automatisch in dat organisatie volledig aan de BIO voldoet.
Verantwoording	De organisatie evalueert de naleving van de AVG en rapporteert over de voortgang.

De thema's zijn onderverdeeld in 28 onderwerpen en 155 beheersmaatregelen. De stelregel is dat de burger recht heeft op passende bescherming van zijn privacy, ongeacht in welke gemeente hij woont. Daarom behoort iedere gemeente volgens de IBD 100% van de criteria uit het toetsingskader na te leven, tenzij zij gemotiveerd kan uitleggen dat een bepaald criterium niet van toepassing is (pas-toe-of-leg-uit). Dan is er sprake van een volwassenheidsniveau waarbij procedures en processen volledig zijn geïmplementeerd en beoordelingen worden uitgevoerd om de doeltreffendheid te beoordelen.

[4] https://www.informatiebeveiligingsdienst.nl/avg-borgingsproduct-3-0/

2 Belangrijkste bevindingen

Gegevensbescherming is geen kwestie van eenmalig een lijst afvinken. Een organisatie moet continue aan de vereisten voldoen. Dit hoofdstuk beschrijft de belangrijkste bevindingen van de FG.

De basis is nog niet op orde: verwerkingsregister en DPIA's

In 2024 hebben de FG en de privacy-officer met alle clusterhoofden gesproken over het register van verwerkingsactiviteiten voor hun organisatieonderdeel. In 2024 hebben twee clusters het register bijgewerkt en aangeleverd. Met de andere clusters worden in 2025 opnieuw afspraken ingepland om het register te bespreken.

Vervolgens moet voor iedere verwerking bepaald worden of een Data Protection Impact Assessment (DPIA) verplicht of noodzakelijk is om de risico's die aan de verwerking verbonden zijn te inventariseren, en de maatregelen te treffen die nodig zijn om die risico's zoveel mogelijk weg te nemen.

Aanbeveling
Zorg dat het register van verwerkingsactiviteiten wordt gecontroleerd, aangevuld. Wijs de verwerkingen in het register aan het juiste organisatieonderdeel (cluster en eenheid) toe.

Aanbeveling
- Zorg dat voor iedere verwerking in het register van verwerkingsactiviteiten beoordeeld wordt of een DPIA noodzakelijk en/of verplicht is.
- Voer voorafgaand aan het inzetten van cameratoezicht in de openbare ruimte een DPIA uit.

Aanbeveling
- Beoordeel op welke onderdelen domeinspecifiek privacybeleid nodig is en stel dit vast.
- Stel conform het privacybeleid tweejaarlijks het werkprogramma privacybeleidsvoering op en vast.

Versterking van het privacyteam

De FG van Noardeast-Fryslân werkt vanaf 2024 14,4 uur per week voor de gemeente Dantumadiel op basis van een dienstverleningsovereenkomst. Hierdoor resteren nog 21,6 FG-uren voor Noardeast-Fryslân.

Vanaf 2024 is de formatie uitgebreid met een privacy-officer voor 0,72 fte (26 uur). Van 1 februari tot 1 oktober is een privacy-officer in dienst geweest. Vanaf 1 februari 2025 is de functie weer ingevuld.

Met de aanstelling van een privacy-officer zijn de uitvoerende en toezichthoudende taken gescheiden. De FG zal zich richten op zijn toezichthoudende taken. In het functieboek moet de functie Adviseur Gegevensbescherming vervangen worden door de functiebeschrijvingen en -waarderingen van de FG en de privacy-officer.

Aanbeveling
Pas in het functieboek de functie Adviseur Gegevensbescherming aan door de taken van de FG en de privacy-officer te scheiden.

Aandacht voor de privacy-audits voor de Wet politiegegevens

In 2025 zijn boa-werkgevers verplicht om de vierjaarlijkse externe privacy-audit over de jaren 2021 tot en met 2024 uit te voeren en de resultaten daarvan vóór 1 maart 2026 met de AP te delen. De AP kan handhavende maatregelen treffen wanneer een organisatie onvoldoende aan de normen voldoet.

De auditscores zijn tot nu toe onvoldoende geweest. De interne audit over 2024 is nog niet uitgevoerd. Door deze in 2025 op alle onderwerpen uit te voeren kunnen de verbeterpunten zichtbaar worden. Door deze verbeterpunten in de resterende maanden van 2025 op te pakken kan de externe audit verbeteringen laten zien.

Voor het uitvoeren van de audits en het realiseren van verbeteringen is geld en tijd nodig. De gemeente heeft geen medewerker(s) in dienst die aan de gestelde eisen voor de auditor voldoen. Om noodzakelijke verbeteringen te realiseren is interne capaciteit nodig.

Aanbeveling
Borg dat de organisatie tijdig voldoet aan de in- en externe audit-verplichtingen van de Wet politiegegevens.

3 Ontwikkelingen en belangrijke gebeurtenissen

Ook in 2024 zijn er de nodige ontwikkelingen geweest op het gebied van bescherming van persoonsgegevens. Dit hoofdstuk beschrijft deze ontwikkelingen.

3.1 Noardeast-Fryslân en Dantumadiel

Op 1 januari 2024 was de ontvlechting van de ambtelijke samenwerking tussen Noardeast-Fryslân en Dantumadiel formeel een feit. In de eerste maanden van 2024 zijn de laatste activiteiten om de ontvlechting af te ronden uitgevoerd. De ontvlechting van de applicaties binnen het Sociaal Domein is voor de zomer afgerond.

De accountant constateerde in de Managementletter 2024 dat Noardeast-Fryslân een achterstand op de verdere implementatie van de AVG kent. Hij acht het noodzakelijk om deze achterstand op korte termijn in te lopen om calamiteiten op AVG-gebied te voorkomen.

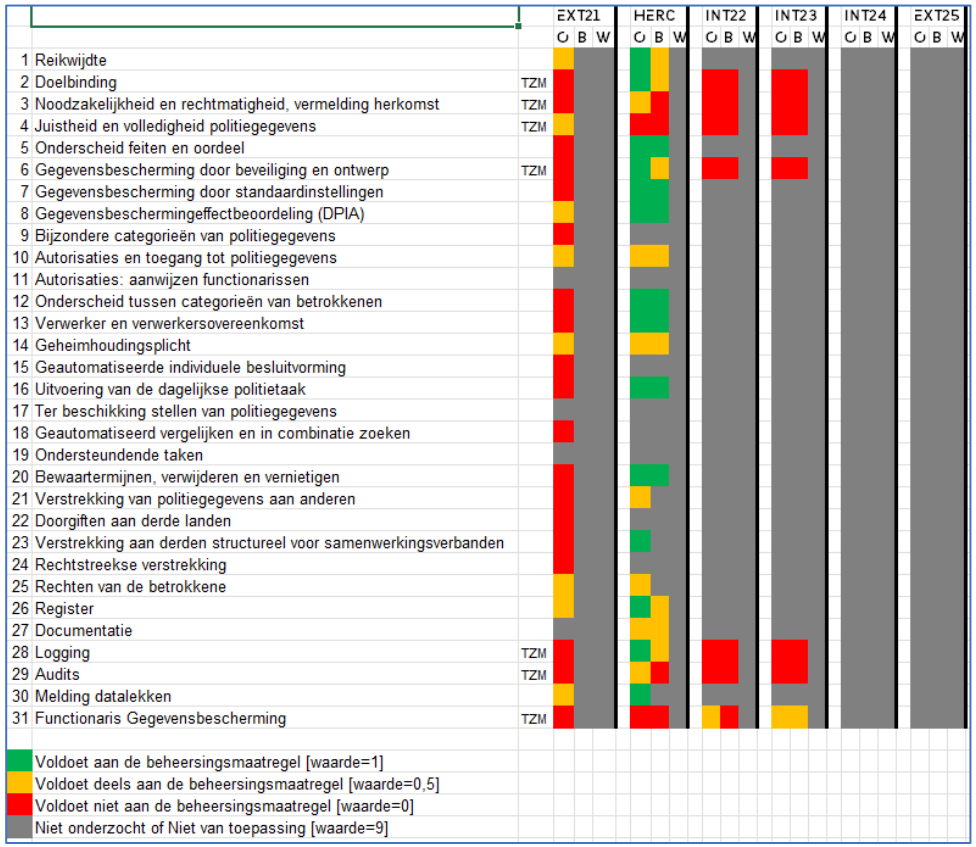
- Noardeast-Fryslân heeft de eerste algoritmes gepubliceerd in het landelijke algoritmeregister.
- In mei 2024 hebben de FG en de privacy-officer een presentatie aan het ODC gegeven over gegevensbescherming.
- In september 2024 heeft Noardeast-Fryslân de tabletop-oefening van de IBD gespeeld. Hierbij wordt in kaart gebracht wat de gevolgen van een ransomware-aanval voor de dienstverlening en bedrijfsvoering kunnen zijn.
- In november 2024 hebben i-adviseurs en projectleiders een cursus gevolgd waarin zij geleerd hebben hoe zij informatiebeveiliging en privacy in hun projecten kunnen integreren en beheren.

3.2 Wet politiegegevens

In 2022 heeft de externe privacy-audit Wet Politiegegevens over de periode 2019 tot en met 2021 plaatsgevonden. Deze audit liet zien dat we op vrijwel alle onderdelen niet voldoen aan de gestelde voorwaarden. De audit toetst opzet (zijn maatregelen beschreven), bestaan (zijn maatregelen geïmplementeerd) en werking (worden maatregelen toegepast) van maatregelen. Van alle beheersmaatregelen kon de opzet niet of beperkt worden aangetoond. De auditor heeft daarom het bestaan en werking van de maatregelen niet kunnen toetsen.

Voor de tekortkomingen heeft het college een verbeterplan opgesteld. In 2024 heeft de auditor de hercontrole uitgevoerd. De hercontrole liet verbeteringen zien, maar er waren nog beheersmaatregelen waarvan opzet en bestaan niet of onvoldoende zijn aangetoond.

De interne audit over 2023 is in december 2024 uitgevoerd. In deze audit zijn zeven toezichtmaatregelen getoetst. Omdat er in 2023 weinig tot geen verbeteringen zijn gerealiseerd zijn is het resultaat van deze interne audit vrijwel gelijk aan de resultaten van de externe audit.



De interne audits gelden als voorbereiding op de externe privacy-audit. In 2025 zijn boa-werkgevers verplicht om de vierjaarlijkse externe privacy-audit over de jaren 2021 tot en met 2024 uit te voeren en de resultaten daarvan met de AP te delen. De boa-werkgevers hebben tot 1 maart 2026 de tijd om de resultaten van die audit door te geven. De AP heeft de lat voor de auditresultaten hoog gelegd. Organisaties hebben meerdere jaren tijd gehad om aan de beheersmaatregelen

te voldoen. De AP kan handhavende maatregelen treffen wanneer een organisatie hier niet (genoeg) aan voldoet[5].

De interne audit over 2024 is nog niet uitgevoerd. Door deze alsnog in de eerste helft van 2025 op alle onderwerpen uit te voeren kunnen de verbeterpunten zichtbaar worden. Door deze verbeterpunten in de resterende maanden van 2025 op te pakken kan de externe audit verbeteringen laten zien.

Voor het uitvoeren van de audits en het realiseren van verbeteringen is geld en tijd nodig. De gemeente heeft geen medewerker(s) in dienst die aan de gestelde eisen voor de auditor voldoen. Om de noodzakelijke verbeteringen te realiseren is interne capaciteit nodig.

Aanbeveling
Borg dat de organisatie tijdig voldoet aan de in- en externe audit-verplichtingen van de Wet politiegegevens.

3.3 Autoriteit Persoonsgegevens

Bescherming van persoonsgegevens (privacy) is een grondrecht. De Autoriteit Persoonsgegevens (AP) is de onafhankelijke toezichthouder in Nederland die dit grondrecht bewaakt. De AP houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens. Onder toezicht vallen diverse activiteiten, zoals onderzoek doen en behandelen van privacyklachten. Andere belangrijke taken van de AP zijn adviseren over nieuwe wet- en regelgeving, voorlichting geven over de privacywetgeving en internationale taken.

Sectorbeeld Overheid

In 2024 heeft de AP het “Sectorbeeld Overheid” gepubliceerd[6]. De AP ziet dat de overheid wel stappen zet, maar nog altijd worstelt om aan de privacywetgeving te voldoen.

In het algemeen ziet de AP dat DPIA’s vaak niet of kwalitatief niet goed worden uitgevoerd. En privacy wordt te vaak nog gezien als slechts een onderdeel van een afweging waarbij andere belangen meer gewicht krijgen. Bestuurders hebben onvoldoende kennis waardoor zij niet altijd de goede besluiten nemen.

Bij gemeenten ziet de AP dat vooral in het sociaal domein, het zorgdomein en het veiligheidsdomein de behoefte bestaat om gegevens met elkaar te delen en aan elkaar te koppelen. Dit mag alleen als daar een juridische grondslag voor is. Bij samenwerkingsverbanden is niet altijd duidelijk welke privacypositie de partijen innemen en wie waarvoor verantwoordelijk is.

Vooral het sociaal domein is kwetsbaar voor AVG-overtredingen. Daar worden veel gevoelige gegevens over gezondheid en de financiële situatie van burgers verwerkt. De wetgeving is niet altijd toereikend om te doen wat in het belang is van de burger. Daarnaast worden in het sociaal domein en bij criminaliteitsbestrijding algoritmes gebruikt om fraude op te sporen en burgers hierop te profileren.

Gemeenten zoeken de grenzen van de AVG en lijken daar vaker overheen te gaan. Soms door een gebrek aan kennis, maar soms ook moedwillig omdat de AVG als belemmering wordt gezien. Aan de andere kant bestaat handelingsverlegenheid omdat de AVG ten onrechte als belemmering wordt gezien. Het is vooral voor kleinere gemeenten een opgave om alles over de AVG te weten en deze goed toe te passen.

Gemeenten moeten transparanter zijn over de doelen en manieren waarop zij persoonsgegevens van burgers verwerken. Publiceren van het register van verwerkingsactiviteiten en algoritmes kunnen bijdragen aan het verhogen van het vertrouwen in de overheid.

3.4 Vooruitblik: uitbreiding wetgeving

Het gegevensbeschermingsrecht is volop in ontwikkeling. De komende jaren worden er zowel nationaal als op Europees niveau nieuwe wetgeving verwacht. Een deel van deze wetgeving zal ook effecten hebben voor de gemeente en daarmee ook op gegevensbescherming. Bijvoorbeeld bij de inrichting van systemen en werkprocessen.

Wet gegevensverwerking door samenwerkingsverbanden (Wgs)

Het wetsvoorstel[7] wil een juridische basis bieden voor de verwerking van persoonsgegevens door samenwerkingsverbanden tussen bestuursorganen en private partijen. Deze partijen verwerken gezamenlijk (persoons)gegevens voor zwaarwegende algemene belangen, zoals bestrijden van fraude en georganiseerde criminaliteit. De wet is op 1 maart 2025 in werking getreden.

[5] https://www.autoriteitpersoonsgegevens.nl/actueel/privacyproof-werken-boa-werkgevers-iets-verbeterd

[6] https://www.autoriteitpersoonsgegevens.nl/documenten/sectorbeeld-overheid

[7] https://www.eerstekamer.nl/wetsvoorstel/35447_wet_gegevensverwerking_door

Wet aanpak meervoudige problematiek sociaal domein (Wams)

Dit wetsvoorstel met betrekking tot het sociaal domein geeft gemeenten de mogelijkheid om bij meervoudige problematiek breed en integraal te werken[8]. Het geeft een juridische grondslag om noodzakelijke persoonsgegevens domeinoverstijgend te kunnen delen, verzamelen en verwerken.

De Tweede Kamer heeft het wetsvoorstel na de val van het kabinet in 2023 controversieel verklaard. Hierdoor is het onduidelijk of en wanneer dit wetsvoorstel wordt behandeld, wat het eindresultaat wordt en wanneer deze in werking kan treden. Dat betekent dat er binnen het sociaal domein nog steeds geen grondslagen bestaan om domeinoverstijgend persoonsgegevens te mogen delen.

Artificial Intelligence Act (AI)

Op 1 augustus 2024 is de Artificial Intelligence Act (AI-Act) in werking getreden. Deze Europese verordening bevat voorschriften voor vrijwel ieder gebruik van algoritmen, autonome systemen en robots. De regels gelden voor iedereen die AI ontwikkelt of gebruikt. De definitie van AI komt neer op een autonoom systeem dat gebaseerd op input van buitenaf een uitvoer genereert (zoals een besluit, aanbeveling, tekst of afbeelding) waarbij die uitvoer direct invloed heeft op de omgeving. De gebruikte technologie is niet relevant. De verplichtingen uit de AI-Act treden treden gefaseerd in werking. De eerste eisen gelden vanaf februari 2025.

De VNG[9] vindt het belangrijk dat gemeenten de mogelijkheid krijgen om generatieve AI in te zetten. Hierbij moet een evenwichtige benadering worden gekozen, waarbij innovatie gestimuleerd wordt binnen bestaande wettelijke kaders. We moedigen dan ook aan dat gemeenten op een verantwoorde manier en binnen beschermde omgevingen kunnen experimenteren. Gemeenten moeten daarbij uiteraard bestaande wet- en regelgeving naleven, bijvoorbeeld met betrekking tot de bescherming van persoonsgegevens en het werken met ethische gedragsregels. In dat kader hebben gemeenten antwoord nodig op de vraag welke leveranciers en toepassingen voldoen aan deze regelgeving. Dit inzicht ontbreekt op dit moment.

- De Informatiebeveiligingsdienst (IBD/VNG) heeft een Handreiking AI[10] gepubliceerd.
- Het ODC heeft in september 2024 richtlijnen voor het gebruik van ChatGPT en andere GenAI vastgesteld.

[8] https://www.eerstekamer.nl/wetsvoorstel/36295_wet_aanpak_meervoudige
[9] https://vng.nl/nieuws/vng-reageert-op-kamerbrief-generatieve-ai
[10] www.informatiebeveiligingsdienst.nl/nieuws/ibd-publiceert-handreiking-ai/

4 Verplichtingen onder de AVG en Wpg

De AVG bevat verplichtingen waar de verwerkingsverantwoordelijke moet voldoen om aan te tonen dat zij handelt in overeenstemming met de regelgeving. In dit hoofdstuk lopen we langs die verplichtingen.

4.1 Functionaris Gegevensbescherming

De (minimaal) vereiste taken van de Functionaris Gegevensbescherming (FG) zoals deze in artikel 39 AVG en artikel 36 Wpg zijn vastgelegd:

- toezien op naleving AVG en Wpg en beleid met betrekking tot bescherming van persoonsgegevens;
- informeren en adviseren over verplichtingen op grond van gegevensbeschermingsrecht;
- adviseren over DPIA's en toezien op de uitvoering hiervan;
- optreden als contactpersoon voor de Autoriteit Persoonsgegevens.

De FG neemt deel aan verschillende interne overleggen, zoals het Strategisch Informatieoverleg (SIO), de Ondernemingsraad en de Experttafel SSC. Er is maandelijks overleg met de FG's van de Friese gemeenten. Er is onregelmatig overleg met FG's van de noordelijke gemeenten (Drenthe, Friesland en Groningen).

De verwerkingsverantwoordelijk moet de FG in staat stellen zijn deskundigheid in stand te houden. De FG heeft in 2024 cursussen en trainingen gevolgd:

- Privacy versus Artificial Intelligence
- Privacywetgeving voor boa's
- Training Audits voor de Wet politiegegevens
- Training Pseudonimisering en Anonimisering

De FG is lid van het Nederlands Genootschap van Functionarissen voor Gegevensbescherming (NGFG, de onafhankelijke beroepsorganisatie voor en van FG's). Het NGFG richt zich op het bevorderen van de kwaliteit van de beroepsgroep en het behartigen van de collectieve belangen van FG's.

In 2024 is landelijk gewerkt aan de totstandkoming van het Nederlands Register voor FG's (NRFG). In 2025 wordt verder gewerkt aan de kwaliteitsnormen die voor inschrijving in het register gaan gelden.

4.1.1 Formatie voor gegevensbescherming

Tot en met 2023 was binnen Noardeast-Fryslân één medewerker die zowel de FG- als de PO-taken uitvoert. Het combineren van deze twee functies kan tot een belangenconflict leiden. Met de aanstelling van een privacy-officer per 1 januari 2024 zijn de uitvoerende en toezichthoudende taken gescheiden. De FG zal zich richten op zijn toezichthoudende taken. In het functieboek moet de functie Adviseur Gegevensbescherming vervangen worden door de functiebeschrijvingen van de FG en de privacy-officer.

Aanbeveling
Pas in het functieboek de functie Adviseur Gegevensbescherming aan door de taken van de FG en de privacy-officer te scheiden.

De dienstverlening aan Dantumadiel voor de FG-taken (0,4 fte) legt vanaf 2024 beslag op de beschikbare FG-uren voor Noardeast-Fryslân. Hierdoor resteren nog 0,6 fte (21,6 uren) voor de FG-taken voor Noardeast-Fryslân.

4.2 Privacybeleid

De AVG vereist[11] dat de verwerkingsverantwoordelijke privacybeleid vaststelt dat in verhouding staat tot de verwerkingsactiviteiten. Het algemene privacybeleid is inhoudelijk in 2018 voor het laatst beschreven. Het beleid schrijft voor dat het iedere twee jaar wordt geëvalueerd en waar nodig bijgesteld. De evaluatie is tot op heden vooruit geschoven in afwachting van een organisatiewijziging waardoor bepaalde rollen en taken mogelijk anders beschreven en toegewezen zouden moeten worden.

Het privacybeleid is in 2024 geëvalueerd. Daarbij zijn ook de vereisten die de Wpg stelt in het beleid opgenomen. Dit volgt uit het verbeterplan in het kader van de privacy-audit.

Voor verwerkingen die qua "*aard, omvang, context en doel*" meer risico ("*qua waarschijnlijkheid en ernst*") kunnen inhouden voor de rechten van betrokkenen kan het nodig zijn om specifiek beleid vast te stellen en uit te voeren. Denk hierbij bijvoorbeeld aan het Sociaal Domein waar veel -vaak bijzondere- persoonsgegevens worden verwerkt. Er is geen domeinspecifiek privacybeleid, en er zijn nog geen beoordelingen geweest of voor een domein specifiek privacybeleid noodzakelijk is.

Op grond van het privacybeleid stelt het college, respectievelijk de burgemeester, tweejaarlijks het werkprogramma privacybeleidsvoering vast, mede op basis van

[11] Artikel 24 lid 2 AVG

de FG-rapportage en de aanbevelingen die hij hierin doet. Het werkprogramma draagt bij aan gestructureerde verdere verbetering, implementatie en compliance. Een dergelijk werkprogramma is tot op heden niet op- en vastgesteld.

Aanbeveling
- Beoordeel op welke onderdelen domeinspecifiek privacybeleid nodig is en stel dit vast.
- Stel conform het privacybeleid tweejaarlijks het werkprogramma privacybeleidsvoering op en vast.

4.3 Register van verwerkingsactiviteiten

De gemeente moet een register van verwerkingsactiviteiten bijhouden met daarin alle verwerkingen waarbij persoonsgegevens worden gebruikt. Dit register geeft inzicht in alle processen en vormt daarom de basis van waaruit andere AVG-thema's kunnen worden opgepakt:

- contractmanagement: het register maakt inzichtelijk met welke externe partijen we samenwerken en waarbij wij en/of de externe partijen persoonsgegevens verwerken.
- risicomanagement: door gegevens over de laatst uitgevoerde Quickscan en/of DPIA te registreren draagt dit bij aan een PDCA-cyclus.
- incidentmanagement: bij een datalek en andere informatieveiligheidsincidenten hebben we een overzicht van de verwerkingen en partijen die bij het incident betrokken (kunnen) zijn.
- transparantie: met een juist en actueel register krijgen we niet alleen zelf inzicht in welke persoonsgegevens wij verwerken, maar hebben onze burgers, relaties en medewerkers dat ook.

Het register vermeldt voor iedere verwerking wie deze uitvoert, op welke grondslag(en) deze is gebaseerd, hoe deze is beveiligd en hoe lang we gegevens bewaren. Ook zien we per verwerking van wie de gegevens afkomstig zijn en aan wie we de persoonsgegevens verstrekken.

In 2024 hebben de FG en de privacy-officer met alle clusterhoofden gesproken over het register voor hun organisatieonderdeel. In 2024 hebben twee clusters het register bijgewerkt en aangeleverd.

Aanbeveling
Zorg dat het register van verwerkingsactiviteiten wordt gecontroleerd, aangevuld. Wijs de verwerkingen in het register aan het juiste organisatieonderdeel (cluster en eenheid) toe.

4.4 Data Protection Impact Assessments

De AVG kent de verplichting om een DPIA (Data Protection Impact Assessment) of, de Nederlandse term, een gegevensbeschermingseffectbeoordeling uit te voeren voor verwerkingen met een hoog risico. Met deze analyses worden de risico's voor de betrokkenen bij een verwerking in kaart gebracht, evenals de maatregelen om deze risico's zoveel mogelijk weg te nemen. Wanneer die risico's niet kunnen worden weggenomen is er sprake van een hoog restrisico. In dat geval moet de verwerking voor de start van het proces of activiteit worden voorgelegd aan de Autoriteit Persoonsgegevens.

In 2024 zijn twee DPIA's gestart: gebruik van bodycams door boa's, en gebruik van de AFAS Pocket App.

De organisatie heeft onvoldoende zicht op de risico's bij de verwerking van persoonsgegevens

De Autoriteit Persoonsgegevens heeft een aantal typen verwerkingen benoemd waarvoor een DPIA verplicht is gesteld. De organisatie heeft tot nu toe vrijwel geen DPIA's of een quickscan daarvoor uitgevoerd. Bij de actualisatie van het Register van Verwerkingsactiviteiten (zie §2.1) is aan de proceseigenaren gevraagd om voor iedere verwerking een Quickscan-DPIA in te vullen. Hieraan is in de meeste gevallen geen opvolging gegeven.

Er worden vrijwel geen DPIA's of een quickscans daarvoor uitgevoerd. De organisatie heeft daarom onvoldoende zicht welke de meest risicovolle verwerkingen zijn en welke maatregelen genomen moeten zijn/worden om die risico's weg te nemen.

Aanbeveling
- Zorg dat voor iedere verwerking in het register van verwerkingsactiviteiten beoordeeld wordt of een DPIA noodzakelijk en/of verplicht is.
- Voer voorafgaand aan het inzetten van cameratoezicht in de openbare ruimte een DPIA uit.

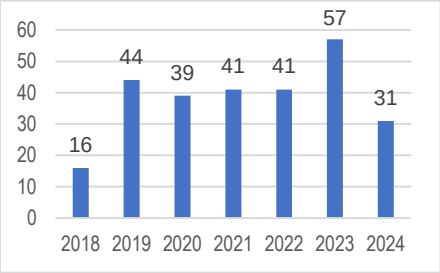
4.5 Registratie en meldplicht datalekken

Bij een datalek gaat het om het vrijkomen, wijzigen of vernietigen van persoonsgegevens zonder dat dit onze bedoeling is. De gemeente moet alle datalekken -ongeacht de ernst- opnemen in een datalekregister. Datalekken zijn niet alleen een risico voor de organisatie, maar vooral ook voor de personen die het betreft. Datalekken moeten daarom goed en snel worden afgehandeld. Dit omvat tevens het nemen van maatregelen om het datalek te dichten om de schade zo beperkt mogelijk te houden en het nemen van preventieve maatregelen om

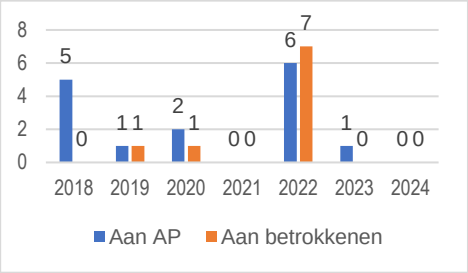
datalekken in de toekomst te voorkomen. Ongeacht de mate van impact van het datalek moet dit per individueel datalek, worden vastgelegd in het datalekregister van de gemeente.

In 2024 zijn 31 AVG-datalekken gemeld. In 6 gevallen zijn persoonsgegevens naar verkeerde ontvangers gestuurd (mail en brieven). In 1 geval is een gegevensdrager gestolen. De overige meldingen betroffen voornamelijk meldingen van kwijtgeraakte toegangspassen. Dit zijn in strikte zin niet altijd datalekken, maar met een gevonden pas kan de vinder toegang krijgen tot de werkruimten en de informatie die daar verwerkt wordt.

Een ernstig datalek moet uiterlijk binnen 72 uur na ontdekking worden gemeld bij de Autoriteit Persoonsgegevens (AP) en aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt). In 2024 is geen datalek aan de AP en/of betrokkenen gemeld.



Datalekken (intern gemeld)



Gemelde datalekken aan AP / betrokkenen

4.6 Rechten van betrokkenen, bezwaarschriften en klachten

Onder de AVG zijn de rechten van betrokkenen versterkt. Deze houden onder meer in dat betrokkenen inzage kunnen krijgen in hun eigen persoonsgegevens, zijn gegevens niet verder te verwerken, of om zijn persoonsgegevens te laten corrigeren of wissen.

- In 2024 zijn 7 verzoeken voor inzage op grond van de AVG ingediend.
- In 2024 is 1 verzoek voor verwijdering van persoonsgegevens ingediend. Dit verzoek is ingewilligd omdat de betreffende persoonsgegevens niet langer noodzakelijk waren.
- In 2024 is 1 bezwaarschrift ingediend tegen het besluit op een inzageverzoek. Dit bezwaarschrift is ongegrond verklaard.
- In 2024 is één klacht ingediend tegen de verwerking van persoonsgegevens door de gemeente Noardeast-Fryslân. Deze klacht was gegrond. De betrokkene heeft daarbij een schadevergoeding geëist. De schadevergoeding is in 2025 betaald.
- Er zijn geen verzoeken tot inzage, correctie of verwijdering of klachten op grond van de Wpg ingediend.

Bijlage: overzicht van aanbevelingen

Aanbeveling	Jaarverslag	Stand van zaken	
Privacybeleid			
• Beoordeel op welke onderdelen domeinspecifiek privacybeleid nodig is en stel dit vast.	2021 2022 2023 2024	• ODC 2 september 2024: opvolging door privacy-officer.	
• Leg de werkwijze voor het standaard en periodiek opvragen van gegevens bij het Inlichtingenbureau vast, bij voorkeur in DPIA's. Vraag geen gegevens op die niet strikt noodzakelijk zijn of niet worden gebruikt. Vraag ook niet standaard van alle betrokkenen gegevens op, tenzij dit aantoonbaar noodzakelijk en proportioneel is.	2022 2023	• In december 2021 heb ik de toenmalige teamleiders en directieleden geadviseerd om de effectiviteit van de bevragingen van het IB vast te stellen, om beleid en richtlijnen vast te stellen en een DPIA op de gegevensverwerking uit te voeren (2021-116132). In 2023 is per signaal vastgesteld met welke frequentie deze worden opgehaald bij het IB. • ODC 2 september 2024: opvolging door clusterhoofd Bedriuwsfiering Gebietsteams. • Er is nog geen DPIA uitgevoerd. Bij het IB kunnen basis-DPIA's worden opgevraagd die als basis kunnen dienen voor de gemeentelijke DPIA.	
• Stel conform het privacybeleid het tweejaarlijkse werkprogramma privacybeleidsvoering op en vast.	2024		
Register van verwerkingsactiviteiten			
• Zorg dat het verwerkingenregister wordt gecontroleerd en aangevuld. • Wijs de verwerkingen in het register aan het juiste organisatieonderdeel (cluster en eenheid) toe.	2021 2022 2023 2024	• ODC 2 september 2024: verwerkingsregister agenderen voor de kwartaalgesprekken. • In 2024 zijn alle clusterhoofden door de PO en FG benaderd om het register te controleren en aan te vullen. Twee clusters hebben hier in 2024 aan voldaan.	
DPIA			
• Zorg dat voor iedere verwerking in het register van verwerkingsactiviteiten beoordeeld wordt of een DPIA noodzakelijk en/of verplicht is.	2021 2022 2023 2024	• ODC 2 september 2024: opvolging door privacy-officer.	
Wet politiegegevens			
• Borg dat de organisatie tijdig voldoet aan de in- en externe audit-verplichtingen van de Wet politiegegevens.	2024	• ODC 2 september 2024: opvolging door privacy-officer.	
Diversen			
• Pas in het functieboek de functie Adviseur Gegevensbescherming aan door de taken van de FG en de privacy-officer te scheiden.	2024		

Op grond van het privacybeleid stelt het college tweejaarlijks het werkprogramma privacybeleidsvoering vast, mede op basis van de rapportage van de FG en de aanbevelingen die hij hierin doet.

	Groei, verbetering
	Stilstand, consolidatie
	Achteruitgang

Bijlage: verklarende woordenlijst

Autoriteit Persoonsgegevens (AP)
Bescherming van persoonsgegevens is een grondrecht van iedereen. De Autoriteit Persoonsgegevens (AP) is de onafhankelijke toezichthouder in Nederland die dit grondrecht bewaakt[12]. En ervoor zorgt dat bedrijven en organisaties zich aan de privacywetgeving houden.

AVG/GDPR
Algemene Verordening Gegevensbescherming (voluit: "Verordening (EU) 2016/679 van het Europees Parlement en de raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming)"). De AVG wordt internationaal aangeduid als de GDPR (General Data Protection Regulation).

Betrokkene(n)
De perso(o)n(en) waarvan de persoonsgegevens worden verwerkt.

Chief Information Security Officer (CISO)
De CISO is een op het vakgebied informatiebeveiliging deskundige functionaris die het complete spectrum aan informatiebeveiliging kan overzien en coördineren. Zonder informatiebeveiliging kan er geen sprake zijn van gegevensbescherming.

Datalek
Bij een datalek gaat het om het vrijkomen, wijzigen of vernietigen van persoonsgegevens, zonder dat dit de bedoeling is. Er is dus sprake van een datalek als er persoonsgegevens in handen vallen van personen of organisaties die geen toegang tot die gegevens zouden mogen hebben. Ook wanneer persoonsgegevens verloren zijn geraakt, is er een datalek. De meest voorkomende datalekken betreffen verkeerd verstuurde e-mail.

Datalek, meldplicht
Als een datalek ernstige nadelige gevolgen kan hebben voor de persoonlijke levenssfeer van betrokkenen, moet de gemeente het datalek binnen 72 uur na ontdekkingmelden bij de Autoriteit Persoonsgegevens. Dit wordt de meldplicht van datalekken genoemd.
Gemeenten moeten betrokkene(n) informeren over een datalek wanneer het waarschijnlijk is dat de inbreuk resulteert in een hoog risico voor de rechten en vrijheden van de betrokkene(n) zodat zij eventueel voorzorgsmaatregelen kunnen treffen.

Datalek, register
De gemeente moet alle datalekken documenteren in een register: het datalekkenregister. Met deze documentatie moet de Autoriteit Persoonsgegevens kunnen controleren of de gemeente aan de meldplicht heeft voldaan.

DPIA (Data Protection Impact Assessment)
Dit is een Engelse term die (strikt genomen) in de Avg vervangen is door de term DPIA, oftewel Data Protection Impact Assessment. De Nederlandse term is 'gevensbeschermingseffectbeoordeling'. Een DPIA is een instrument om privacy risico's van een gegevensverwerking in kaart te brengen. En vervolgens maatregelen te kunnen nemen om de risico's te verkleinen. Een DPIA is verplicht voor 'risicovolle verwerkingen'. De Avg geeft aan voor welke categorieën van verwerkingen een DPIA verplicht is. Daarnaast heeft de Autoriteit Persoonsgegevens een aanvullend overzicht opgesteld waarin is geconcretiseerd in welke gevallen de organisatie verplicht is een DPIA uit te voeren.

Functionaris Gegevensbescherming (FG)
De FG houdt het toezicht binnen een organisatie op de correcte uitvoering van de verwerking volgens de Avg. Een FG is verplicht bij overheden en publieke organisaties.

Opzet, bestaan en werking
Een audit toetst opzet (zijn maatregelen beschreven), bestaan (zijn maatregelen geïmplementeerd) en werking (worden maatregelen over een periode van ten minste twaalf maanden toegepast).

Persoonsgegeven
Een persoonsgegeven is alle informatie, op wat voor manier ook, die iets zegt over een persoon. Daar is al snel sprake van: naam, (mail)adres, woonplaats, geboortedatum, geslacht, functie, inhoud van e-mails, surfgedrag, loginnamen, wachtwoorden, IP-adressen, tracking cookies enz. enz. Niet alleen geschreven tekst kan een persoonsgegeven zijn, ook beeld en geluid kunnen persoonsgegevens zijn.

Politiegegevens
De Wet politiegegevens (Wpg) is van toepassing op de verwerking van persoonsgegevens door de bijzonder opsporingsambtenaar (boa) in het kader van zijn opsporingstaak. Politiegegevens zijn persoonsgegevens die onder het regime van de Wpg worden verwerkt.

Privacy by default en design
Privacy by default betekent dat standaardinstellingen zo privacy-vriendelijk mogelijk zijn ingesteld. Privacy by design betekent dat er bijvoorbeeld bij het ontwerpen van een informatiesysteem of nieuw product rekening gehouden wordt met privacy (design). Met andere woorden: het pro-actief borgen van gegevensbescherming in beleid, procedures en processen. Dit zijn wettelijke verplichting onder de Avg.

Rechten van betrokkenen
Onder de Avg hebben mensen mogelijkheden om voor zichzelf op te komen als hun persoonsgegevens worden verwerkt. Het gaat om de volgende rechten:

- Inzage: het recht van mensen om de persoonsgegevens die de gemeente van hen verwerkt in te zien.

[12] https://www.autoriteitpersoonsgegevens.nl/nl/over-privacy/het-werk-van-de-ap

- Rectificatie en aanvulling: het recht om de persoonsgegevens die de gemeente verwerkt te wijzigen.
- Verwijdering: het desgevraagd wissen van persoonsgegevens van betrokkene.
- VVergetelheid: het recht om ‘vergeten’ te worden. Dat wil zeggen dat iedere koppeling naar of kopie van de gegevens worden gewist.
- Beperking van de verwerking: het recht om minder gegevens te laten verwerken.
- In de situatie van geautomatiseerde besluitvorming en profilering: het recht op een menselijke blik bij besluiten.
- Dataportabiliteit: het recht om persoonsgegevens over te dragen. Het houdt in dat mensen het recht hebben om de persoonsgegevens te ontvangen die een organisatie van hen heeft. Zo kunnen zij hun gegevens bijvoorbeeld makkelijk doorgeven aan een andere leverancier van dezelfde soort dienst.
- Bezwaar te maken tegen de gegevensverwerking.
- Duidelijke informatie over wat de gemeente met hun persoonsgegevens doet.

UAVG
De AVG is rechtstreeks van toepassing in Nederland. Daar waar de AVG ruimte laat voor nationale keuzes bij de uitvoering van de AVG, zijn deze ingevuld in de Uitvoeringswet AVG (UAVG).

Verantwoordingsplicht
De AVG legt de verantwoordelijkheid bij de gemeente als organisatie om aan te tonen dat de gemeente aan de privacyregels voldoet. Verantwoordelijkheid is het vermogen om compliance met de AVG aan te tonen. Dit is dus voor verantwoordelijken en verwerkers verplicht. De verantwoording kan vormgegeven worden door het bijhouden van de verschillende registers: verwerkingsregister, datalekken, verwerkersovereenkomsten etc.

Verwerken / verwerking
Dit is alles wat de gemeente doet met persoonsgegevens. Het omvat de hele levenscyclus van informatie, en alles wat je doet of zou kunnen doen met persoonsgegevens. Bijvoorbeeld: verzamelen, vastleggen, ordenen, structureren, opslaan, wijzigen, opvragen, raadplegen, gebruiken, verstrekken, verspreiden, combineren, afschermen of wissen enz. enz.

Verwerker
Een derde die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt.

Verwerkersovereenkomst
Dit is een overeenkomst tussen verantwoordelijke en verwerker, waarin de verantwoordelijkheden en afspraken over de verwerking worden vastgelegd.De overeenkomst regelt vaak algemene zaken zoals aansprakelijkheid, plus een bijlage waarin de specifieke kenmerken rondom de verwerking worden benoemd.

(Verwerkings)verantwoordelijke
Dit is een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Voor de gemeente zijn dit meestal het college en de burgemeester.

Verwerkingsregister
De gemeente is verplicht een register bij te houden van alle verwerkingen van persoonsgegevens. Dit register moet continu actueel worden gehouden. In het verwerkingsregister staan onder meer de verwerkingsdoeleinden, beschrijving van de categorieën betrokkenen en van de categorieën persoonsgegevens, de beoogde bewaartermijnen (de termijnen waarbinnen de persoonsgegevens moeten worden gewist) en een beschrijving van de wijze waarop de gegevens beveiligd zijn.