provincie Drenthe

Jaarrapportage Gegevensbescherming van de Functionaris Gegevensbescherming (FG) 2025

Datum
20 januari 2026

Documentgegevens
Versie : 1.0

Inhoud

Voorwoord

De provincie Drenthe werkt met persoonsgegevens. Waar nodig worden door de provincie Drenthe persoonsgegevens verwerkt voor het goed kunnen uitvoeren van wettelijke medebewindstaken, autonome taken of voor de provinciale bedrijfsvoering. Hierbij gaat het om gegevens van zowel externe personen, zoals inwoners en contactpersonen van andere overheden, bedrijven en instellingen, als van interne personen, zoals bestuurders en werknemers. De provincie Drenthe dient zorgvuldig om te gaan met persoonsgegevens. In de Algemene verordening gegevensbescherming (AVG) en de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG) wordt hiertoe het wettelijk kader beschreven.

De AVG en de UAVG geven echter niet voor elk privacyvraagstuk een pasklaar antwoord. De Europese en landelijke wetgeving bevatten normen, die samen een afwegingskader geven. Aan de hand van het wettelijk afwegingskader moet de provincie Drenthe steeds beoordelen of een bepaalde verwerking van persoonsgegevens is toegestaan, en zo ja, onder welke voorwaarden.

Het merendeel van de verwerkingen van persoonsgegevens binnen de provincie vinden plaats onder de verantwoordelijkheid van het college van Gedeputeerde Staten (GS). Provinciale Staten (PS) controleert dit en is zelfstandig verantwoordelijk voor de verwerkingen van persoonsgegevens door statenleden en de Statengriffie.

De Autoriteit Persoonsgegevens (AP) houdt extern toezicht op de naleving van de privacyregels in Nederland. Het interne toezicht voert de Functionaris Gegevensbescherming (FG) uit. Sinds 1 maart 2025 vervul ik die rol. Als FG heb ik als taak toezicht te houden op en te adviseren over de toepassing en naleving van de AVG door de provincie Drenthe. De organisatie zelf draagt zorg voor het realiseren van de privacybeschermende maatregelen.

Ik heb in 2025 een overall-beeld gevormd en heb mij gefocust op een advies aan de directie voor een gestructureerd groeipad om te komen tot een volwassenheidsniveau op het gebied van privacybescherming dat passend is voor de provincie.

Deze jaarrapportage is besproken met de provincie secretaris, de concerncontroller, de CISO (Chief Information Security Officer), de provinciearchivaris, de Statengriffier en informatiemanager van de Statengriffie.

Assen, 20 januari 2026

L. Pilon

Functionaris Gegevensbescherming (FG) van de provincie Drenthe

1. Inleiding

Privacy is inmiddels een breed maatschappelijk veelbesproken thema geworden en heeft zich ontworsteld aan het imago van een hinderlijke bijkomstigheid en het inzetten van procedurele en technische maatregelen. Waar de aandacht aanvankelijk vooral uitging naar het risico op reputatieschade, juridische gevolgen, boetes en schadeclaims, wordt goede privacy borging nu steeds meer gezien als onderdeel van excellente dienstverlening en het bevorderen van vertrouwen van de burger in de overheid.
Aantoonbaar voldoen aan de relevante wet- en regelgeving is geen afvinklijst, maar een continu proces. Privacy risico's blijven evolueren in een digitale wereld waarin gegevens steeds centraler staan. De toename van digitale diensten, geavanceerde technologieën en data gedreven processen brengen nieuwe uitdagingen met zich mee voor de bescherming van persoonsgegevens. Onzorgvuldige omgang met informatie, cyberdreigingen en onduidelijke verantwoordelijkheden kunnen leiden tot verlies van vertrouwen en gegevens en leiden tot hoge kosten en reputatieschade. In deze rapportage wordt belicht hoe de Provincie Drenthe deze risico's beheerst en inzet op transparantie, beveiliging en naleving van privacywetgeving.

De zeven belangrijkste risico's zijn:

Privacy Risico	**Beschrijving van het risico**	**Maatregelen**	**Toelichting op de maatregelen**
1. Onrechtmatige verwerking van persoonsgegevens	Verwerking zonder wettelijke grondslag of verdere verwerking dan noodzakelijk.	Verwerkingsregister bijhouden DPIA uitvoeren bij risicovolle verwerkingen Juridische toetsing van verwerkingsgrondslagen	Zorgen ervoor dat elke verwerking van persoonsgegevens wordt vastgelegd, beoordeeld op risico's en juridisch getoetst op geldige grondslagen.
2. Onvoldoende transparantie richting betrokkenen	Betrokkenen weten niet wat er met hun gegevens gebeurt.	Privacyverklaring publiceren, actueel houden en ernaar handelen. Mechanismen voor het uitoefenen van rechten (inzage, correctie, verwijdering)	Zorgen voor duidelijke communicatie en faciliteren de rechten van betrokkenen op hun persoonsgegevens.
3. Onvoldoende beveiliging van persoonsgegevens	Datalekken door technische of organisatorische tekortkomingen.	Toegangsbeheer (autorisatie, authenticatie) Encryptie van gevoelige data Patchmanagement en monitoring Incidentmanagementproces (inclusief datalekken)	Beschermen persoonsgegevens tegen ongeautoriseerde toegang en zorgen voor snelle detectie en afhandeling van beveiligingsincidenten.
4. Bewaren van gegevens langer dan noodzakelijk	Overtreding van de bewaartermijnen.	Opslagbeperking Dataretentiebeleid Automatische verwijdering of archivering Periodieke review van opgeslagen data	Zorgen ervoor dat persoonsgegevens niet langer worden bewaard dan nodig is voor het doel waarvoor ze zijn verzameld.
5. Verstrekking aan derden zonder juiste afspraken	Ongecontroleerde doorgifte aan verwerkers of andere partijen.	Verwerkersovereenkomsten Doorgiftebeleid (ook buiten EU)	Zorgen voor duidelijke afspraken en transparantie over doorgifte van persoonsgegevens aan derden.

6. Gebrek aan bewustzijn en training	Medewerkers handelen (vaak onbewust) in strijd met privacyregels.	Privacy awareness trainingen E-learning modules Regelmatige communicatie over privacybeleid	Vergroten van het bewustzijn van medewerkers en zorgen voor naleving van privacyregels in de praktijk.
7. Niet voldoen aan rechten van betrokkenen	Niet tijdig of volledig reageren op verzoeken.	Opslagbeperking Procedure voor afhandeling van verzoeken	Zorgen voor een volledige, gestructureerde en tijdige afhandeling van verzoeken van betrokkenen.

1.2 Opbouw document

Per onderwerp wordt ingegaan op de vraag in hoeverre de fundamentele zaken op orde zijn om de provincie in staat te stellen om voortdurend aan privacy wet- en regelgeving te voldoen. Er wordt met symbolen een oordeel gegeven over de stand van zaken van het afgelopen jaar en er worden aanbevelingen gedaan.

Achtereenvolgens komen de volgende onderwerpen aan bod.

- Beleid
- Processen
- Organisatorische inbedding
- Rechten van betrokkenen
- Samenwerking
- Gegevensbescherming
- Verantwoording

Deze onderwerpen zijn van toepassing op de verwerkingen van persoonsgegevens onder de verantwoordelijkheid van GS én PS. Maar omdat PS op onderdelen afwijkt, is er een apart hoofdstuk voor PS opgenomen. Ditzelfde geldt voor de verwerkingen van politiegegevens die niet onder de AVG vallen maar onder de Wpg (Wet politiegegevens). Ook hiervoor is een apart hoofdstuk opgenomen.

Legenda van de symbolen:

- Op schema. Oordeel over afgelopen jaar is goed. Alle nodige acties zijn opgepakt en werkzaam
- In te halen achterstand. Oordeel over afgelopen jaar is voldoende. Alle of een deel van de nodige acties zijn in gang gezet of deels werkzaam
- Aandacht vereist van management. Oordeel over afgelopen jaar is onvoldoende. De nodige acties zijn nog niet of niet voldoende opgepakt dan wel in gang gezet.
- Geen oordeel gegeven of op dit moment geen oordeel mogelijk.

2. Privacybeleid

Het privacybeleid is een kader waarin de provincie aangeeft aan welke principes zij zich houdt bij de verwerking van persoonsgegevens. Het laat zien hoe de provincie wenst om te gaan met persoonsgegevens en welke maatregelen zij treft om te voldoen aan de relevante wet- en regelgeving.

2.1 Stand van zaken afgelopen jaar

Onderdeel	Oordeel 2020	Oordeel 2021	Geen oordeel 2022 t/m 2024	Oordeel 2025
Er is een actueel Beleidskader privacy provincie Drenthe				
Het beleid is dekkend en toereikend				
Er is een actuele privacyverklaring, zowel extern als intern en deze wordt toegepast				
Er is een actueel protocol meldplicht datalekken				

De provincie heeft een actueel en vastgesteld privacybeleid. Het is een overkoepelende, richtinggevende visie op het privacybeleid van de provincie Drenthe. Het biedt kaders voor alle onderliggende (beleids)documenten en/of (beheers)maatregelen die de provincie Drenthe opstelt dan wel neemt op het terrein van de bescherming van privacy. Het privacybeleid is van toepassing op alle taken en processen waar Provinciale Staten (PS) en Gedeputeerde Staten (GS) van de provincie Drenthe verantwoordelijk voor zijn en heeft betrekking op de persoonsgegevens van personen van wie de provincie Drenthe gegevens verwerkt (of laat verwerken), voor zover dit onder het gezag van PS of GS valt.

Op de volgende onderwerpen zijn specifieke regelingen of protocollen opgesteld:
- Privacyprotocol cameratoezicht
- Privacyverklaring medewerkers
- Gebruiksreglement bedrijfsmiddelen
- Handleiding Privacy by design
- Protocol melding datalekken

Zoals in de inleiding weergegeven blijven privacy risico's evolueren in een digitale wereld. Het gebruik van AI is zo'n ontwikkeling. Door middel van het project AI Readiness binnen het programma digitalisering wordt gewerkt aan AI-beleid wat past binnen de kaders van het privacybeleid van de provincie Drenthe. Het AI-kader is wel opgesteld en gepubliceerd op het digitale plein.

Het thema Communicatie monitort actief op de aanwezigheid van een privacyverklaring op satellietwebsites. Dit zijn kleinere websites die erop gericht zijn om de hoofdwebsite te ondersteunen en worden ingezet om specifieke doelgroepen te bereiken. Op 15 van de 62 satellietwebsites ontbreekt de privacyverklaring. De website eigenaren worden benaderd om een link naar de privacyverklaring te maken.

3. Processen

De verwerkingen van persoonsgegevens door de provincie Drenthe dienen te voldoen aan de AVG. Dit houdt in dat de provincie de werkprocessen waarin persoonsgegevens verwerkt worden moet toetsen en inrichten volgens de volgende beginselen: behoorlijkheid, transparantie, doelbinding, dataminimalisatie, opslagbeperking, juistheid, integriteit en vertrouwelijkheid.

1. Er mogen alleen persoonsgegevens verwerkt worden als daar een grondslag uit de AVG voor is. Grondslagen zijn: Gerechtvaardigd belang, Algemeen belang, Wettelijke verplichting, Uitvoeren overeenkomst, Vitaal belang of Toestemming. Verwerkingen moeten worden vastgelegd in het verwerkingsregister.

2. Voor elke verzameling en/of verwerking van persoonsgegevens is doelbinding nodig, die wordt vastgelegd in het verwerkingsregister. Volgens de AVG mogen persoonsgegevens alleen verzameld en/of verwerkt worden als daarvoor een gerechtvaardigd doel is vastgesteld; er is zogenoemde doelbinding.

3. Bij het verzamelen en/of verwerken van persoonsgegevens moet de hoeveelheid en het soort gegevens zoveel mogelijk geminimaliseerd worden. Alleen de persoonsgegevens die noodzakelijk zijn voor het doel van de verzameling en/of verwerking worden verzameld en/of verwerkt.

4. Persoonsgegevens mogen niet langer bewaard worden dan strikt noodzakelijk voor de dienstverlening of wettelijke verplichting. De bewaartermijn wordt vastgelegd in het verwerkingsregister.

5. Persoonsgegevens moeten passend beveiligd worden volgens het geldende informatiebeveiligingsbeleid. De beveiligingsmaatregelen en categorieën ontvangers van persoonsgegevens worden vastgelegd in het verwerkingsregister.

6. In het geval van doorgifte van persoonsgegevens aan derden als verwerker moet de verwerker formeel garanties afgeven waarmee aangetoond kan worden dat ook bij doorgifte van gegevens verwerkt wordt volgens de AVG. Dit wordt vastgelegd in een verwerkersovereenkomst.

7. Alleen persoonsgegevens die van een goede kwaliteit ofwel juist en actueel zijn mogen worden verwerkt.

8. De verwerkingsverantwoordelijke moet transparant zijn over de wijze en de reden waarom persoonsgegevens verwerkt worden. En heeft een informatieplicht richting betrokkenen en betrokkenen hebben de nodige rechten.

9. Er moet extra zorgvuldig omgegaan worden met geautomatiseerde verwerkingen van persoonsgegevens, zoals in het geval van profilering, het verzamelen van big data, tracking en tracing en het inzetten van camera's.

10. Bij het ontwerpen en inrichten van processen en systemen van gegevensverzameling en/of -verwerking hoort privacy by design en privacy by default uitgangspunt te zijn. Privacy by design houdt in dat er al bij het ontwerpen van producten en diensten voor wordt gezorgd dat persoonsgegevens goed worden beschermd. Privacy by default houdt in dat de meest privacy vriendelijke standaardinstellingen worden gebruikt.

11. Bij risicovolle verzamelingen en verwerkingen van persoonsgegevens dient vooraf een data protection impact assessment (DPIA) uitgevoerd te worden om de privacy risico's in kaart te brengen. En vervolgens maatregelen te kunnen nemen om de risico's te verkleinen.

12. Er moet een verwerkingsregister bijgehouden worden met daarin alle verwerkingen waarvoor de organisatie verwerkingsverantwoordelijk is.

13. Datalekken worden gemeld bij de Autoriteit Persoonsgegevens (AP) en informeert de betrokkene, tenzij hiervoor een uitzondering geldt. Er is sprake van een datalek wanneer persoonsgegevens (mogelijk) in handen vallen van derden die geen toegang tot die gegevens mogen hebben.

3.1 Stand van zaken afgelopen jaar

Onderdeel	Oordeel 2020	Oordeel 2021	Geen oordeel 2022 t/m 2024	Oordeel 2025
Er is een actueel verwerkingsregister	🟡	🟢		🟢
Er is een standaard verwerkersovereenkomst	○	○		🟢
Er is zijn formats voor het uitvoeren van een pre-DPIA en DPIA	○	○		🟢
Bij risicovolle verzamelingen en/of verwerkingen van persoonsgegevens worden vooraf DPIA's uitgevoerd	🟢	🟢		🔴
Er wordt privacy by design en privacy by default toegepast bij het ontwerpen en inrichten van processen en systemen van gegevensverzameling en/of -verwerking	🟡	🟡		🟡
Er is een ingericht changeproces	○	○		🟢
Er is een protocol melding datalekken	🟢	🟢		🟢
Risicovolle verwerkingen zijn gedefinieerd en er zijn steekproeven naar het voldoen aan de beginselen van art. 5 AVG op uitgevoerd.	○	○		○

Verwerkingsregister
De provincie Drenthe beschikt over een verwerkingsregister. In 2025 is deze geactualiseerd.
Het verwerkingsregister is een belangrijk instrument om nieuwe verwerkingen te toetsen en in te richten volgens de AVG. De privacy ambassadeurs (1e contactpersonen binnen de thema's op het gebied van privacy) spelen hierbij een belangrijke rol. Zij zouden moeten weten of er sprake is van een nieuwe verwerking van persoonsgegevens binnen hun thema en samen met de privacy officers de verwerkingen vooraf moeten toetsen. Toetsen op de aanwezigheid van een grondslag voor de verwerking, doelbinding, dataminimalisatie, bewaartermijnen, opslag en beveiliging, of er een verwerkersovereenkomst nodig is en of er een DPIA uitgevoerd moet worden.
Bij het ontwerpen en inrichten van processen en systemen moeten vooraf alle privacyaspecten meegenomen en afgewogen worden. Dit geheel valt onder Privacy by design. Niet alle Privacy ambassadeurs worden door collega's binnen het thema meegenomen in nieuwe ontwikkelingen of nemen hierin een actieve houding aan zodat het risico bestaat dat nieuwe verwerkingen onrechtmatig zijn.

Processen
Rechtmatige verwerking van persoonsgegevens wordt gefaciliteerd door diverse ingerichte processen. Het protocol melding datalekken biedt waarborgen voor een zorgvuldige behandeling van datalekken. Het inkoopproces biedt waarborgen voor het afsluiten van verwerkersovereenkomsten. De provincie gebruikt in beginsel een eigen verwerkersovereenkomst gebaseerd op het VNG model.

Er is in 2025 vanuit het accountmanagement en changemanagement een nieuw proces ingericht rondom het beoordelen van wijzigingen die bij het thema Informatie, Data & Automatisering (ID&A) binnenkomen. Deze werkwijze is een belangrijke stap naar een gestructureerd en uniform beoordelingsproces waarin alle relevante expertises op het juiste moment worden betrokken. Privacy is hier één van.

Dat privacy procesmatig gefaciliteerd is, wil niet zeggen dat er niet buiten procedures omgewerkt wordt. Er is ruimte voor verbetering. Niet alle nieuwe verwerkingen lopen via het inkoopproces, changeproces of via privacy ambassadeurs of privacy officers. Het feit dat thema's kunnen inkopen vanuit hun budgettaire mandaat kan in de hand werken dat pas later privacyvraagstukken in beeld komen. De privacy officers zijn dan niet of pas later aangehaakt bij de aanschaf van een product/applicatie of het vormen van een dataverzameling.

DPIA's (Dataprotection impact assessments)
Risico-inschatting bij verwerkingen van persoonsgegevens vindt vaak achteraf plaats in plaats van vooraf. Dit kan ertoe leiden dat de principes van privacy by design en privacy by default (de meest privacy vriendelijke standaardinstellingen) niet worden toegepast. Dat het oordeel over 2025 rood is komt doordat de norm is aangescherpt van het uitvoeren van een DPIA naar het vooraf uitvoeren van een DPIA en doordat er in 2025 geen DPIA's zijn afgerond. Er zijn wel twee DPIA's in behandeling.

Er is een pre-DPIA checklist beschikbaar om vooraf snel te beoordelen of een verwerking risicovol is en of een DPIA moet worden uitgevoerd. Ook is er een format voor het uitvoeren van de daadwerkelijke DPIA. Het is onduidelijk voor welke processen een DPIA verplicht is en nog moet worden uitgevoerd.

Informatiebeheer
Grip op informatiebeheer is cruciaal voor het waarborgen van privacy. De provincie hanteert het principe 'open tenzij'. In theorie betekent dit dat openbare en intern openbare informatie voor iedereen beschikbaar is om integraal te kunnen werken. Vertrouwelijke en geheime informatie valt hier niet onder. Persoonsgegevens behoren in de basis tot de categorie vertrouwelijk.
In de praktijk ontbreekt echter classificatie en labeling van data. Hierdoor hebben vaak te veel medewerkers toegang tot vertrouwelijke gegevens. Bovendien worden persoonsgegevens regelmatig opgeslagen in openbare SharePoint-bibliotheken, zoals kopieën van rijbewijzen of identiteitsbewijzen. Dit heeft in 2025 geleid tot meerdere datalekken. Het opslaan van dergelijke gegevens is in de meeste gevallen onrechtmatig en brengt, zelfs wanneer het rechtmatig gebeurt, aanzienlijke risico's mee voor betrokkenen.
In 2025 is vanuit informatiebeheer is een inventarisatie uitgevoerd bij themamanagers over het aantal SharePoint-sites en het gebruik van persoonsgegevens. Daarnaast werkt het thema Informatie, Data & Automatisering aan een duurzame technische oplossing voor het labelen van data, die naar verwachting in 2026 beschikbaar komt.

Daarbij is bij de technische inrichting van SharePoint slechts ten dele rekening gehouden met de AVG. Van elke bewerking wordt een nieuwe versie van een document onder water bewaard waardoor iedereen van elkaar precies kan zien wie wat wanneer heeft gedaan.

3.2 Aanbevelingen

.

- Breng in beeld voor welke processen een DPIA is uitgevoerd en voor welke dit nog noodzakelijk is.
- Rond de dataclassificatie in 2026 af.

4. Organisatorische inbedding

Voor een goede en juiste uitvoering van het privacybeleid is het van belang dat iedereen binnen de organisatie op de hoogte is van de beginselen van de AVG en het belang van privacy. Organisatorische inbedding betekent het toewijzen van taken, verantwoordelijkheden en bevoegdheden en bewustzijn creëren.

4.1 Stand van zaken afgelopen jaar

Onderdeel	Oordeel 2020	Oordeel 2021	Geen oordeel 2022 t/m 2024	Oordeel 2025
De verdeling van taken, verantwoordelijkheden en bevoegdheden rondom privacy is duidelijk beschreven en werkt zoals het bedoeld is				
Nieuwe bestuurders en medewerkers leggen een (ambts)eed af (in het kader van het integriteitsbeleid), waarin aandacht wordt besteed aan de omgang met (privacygevoelige) gegevens				
Er is voldoende (aandacht voor) privacybewustzijn in de organisatie, mede gevormd door iBewustzijn, gekoppeld aan het informatiebeveiligingsbeleid en informatiebeheer				

<u>Verdeling taken en verantwoordelijkheden</u>
Het college van GS is bestuurlijk verantwoordelijk voor het privacybeleid. PS heeft in voorkomende gevallen ook een bestuurlijke (vooral kader stellende en controlerende) rol wat betreft het privacybeleid van de provincie en is verantwoordelijk voor de verwerkingen van persoonsgegevens binnen de Statengriffie.

De provinciesecretaris is ambtelijk eindverantwoordelijk voor het privacybeleid in de organisatie. De Statengriffier voor de verwerkingen door de Statengriffie. Dit werkt zoals het bedoeld is.

De verdere verdeling van taken, verantwoordelijkheden en bevoegdheden rondom privacy is duidelijk beschreven maar werkt niet overal zoals het bedoeld is.
Bescherming van de privacy is namelijk primair een lijnverantwoordelijkheid (1e lijn). Het privacybeleid maakt onderdeel uit van het integraal management. De domeinmanager is verantwoordelijk voor de informatiebeveiliging binnen zijn/haar domein, de themamanager binnen zijn/haar thema en proces(sen). De belangrijkste taak ligt in het toezien op naleving van beleid in de werkzaamheden van de medewerker. Per thema is er een medewerker die privacy ambassadeur is. De privacy ambassadeur fungeert als privacy-aanspreekpunt voor de collega's uit het thema, de privacy officer en de FG.

Eigenaarschap op privacy wordt in de lijn niet overal gevoeld. Niet alle privacy ambassadeurs worden voldoende gesteund door hun themamanager, krijgen voldoende tijd voor het uitvoeren van privacy taken of nemen een proactieve houding aan. Hierdoor bestaat het risico dat nieuwe verwerkingen onrechtmatig zijn of niet voldoen aan de eisen die de wet eraan stelt. Het advies 'Implementatie en borging van privacy' van de FG, dat op 17 november 2025 is vastgesteld door de directie, bevat aanbevelingen om de privacy governance te verbeteren. Privacy governance betekent dat de taken en verantwoordelijkheden die voortvloeien uit de AVG in de gehele organisatie zijn belegd en ingebed.

In november 2025 is voor een periode van een half jaar een kwartiermaker privacy officer aangesteld met als taak om het belang van privacy bewust handelen, en wat daarin van de lijn verwacht wordt, uit te dragen en de privacy governance naar een hoger niveau te tillen.

De privacy officer (2e lijn) is verantwoordelijk voor het ontwikkelen en implementeren van beleid en procedures met betrekking tot de bescherming van persoonsgegevens en ondersteunt de 1e lijn. Dit werkt zoals het bedoeld is maar privacy is een onderwerp wat de juristen naast hun dagelijkse werkzaamheden oppakken. Een dedicated privacy officer ontbreekt. De kwartiermaker privacy officer heeft als taak om met een advies te komen voor de aanstelling en positionering van een privacy officer.

De FG (3e lijn) is een onafhankelijke toezichthouder die de naleving van de AVG bewaakt. Daarnaast geeft de FG gevraagd en ongevraagd advies over privacy rechten. Dit voor zowel medewerkers van de provincie Drenthe als de inwoners van de provincie. De rollen van FG en privacy officer zijn gescheiden. De provincie heeft een FG aangewezen om toezicht te houden op de verwerkingen van persoonsgegevens die onder de AVG en Wpg (Wet politiegegevens) vallen.

De persoonlijke verantwoordelijkheid van bestuurders en medewerkers van de provincie Drenthe ten aanzien van het privacybeleid is vastgelegd in gedragscodes, het integriteitsbeleid en het gebruiksreglement bedrijfsmiddelen. Daarnaast legt iedereen een (ambts)eed af. Vanaf 2026 is een VOG verplicht bij indiensttreding en overgang naar een als kwetsbaar gedefinieerde functie.

Ondanks de hernieuwde aandacht is het oordeel over 2025 oranje gebleven omdat het gezien de tijd te kort is voor het oordeel groen.

Bewustwording
Er is aandacht voor bewustwording. De privacy officers bezoeken jaarlijks alle thema's om de bewustwording verder te bevorderen. Het blijft bij sommige thema's echter lastig om aan tafel te komen. Vanaf 2025 biedt de organisatie e-learningen aan op het gebied van informatiebeveiliging en privacy. De trainingen zijn niet verplicht om te volgen. 55 á 60% van de medewerkers heeft de e-learningen gevolgd.

Informatiebeheer
Naast deze activiteiten is het belangrijk dat medewerkers ook in praktische zin weten hoe ze met informatie en gegevens moeten omgaan. Bijvoorbeeld welke informatie moet op welke manier waar opgeslagen worden. Daarom is in 2025 gestart met het programma CPI (Cybersecurity, Privacy en Informatiebeheer) met als één van de doelen dat medewerkers vanaf de eerste week weten hoe om te gaan met informatie en gegevens en managers gefaciliteerd worden om hier sturing aan te geven.

4.2. Aanbevelingen

- Verbeter de privacy governance. Privacy governance betekent dat de taken en verantwoordelijkheden die voortvloeien uit de AVG in de gehele organisatie zijn belegd en ingebed.
- Laat het programma CPI de regie nemen in het omgaan met informatie en gegevens door het ontwikkelen van verplichte trainingen op het gebied van informatiebeheer, informatiebeveiliging en privacy voor iedereen

Als medewerkers weten wat er verwacht wordt en managers hun verantwoordelijkheid voelen, hun kennis en gemaakt afspraken uitdragen, zal daarmee het volgen van de processen (genoemd in paragraaf 3.1) verbeteren. Ook kunnen de privacy ambassadeurs hun rol dan beter pakken.

5. Rechten van betrokkenen

De AVG stelt betrokkenen in staat om via een aantal rechten controle en invloed uit te oefenen over zijn of haar persoonsgegevens. De provincie heeft de plicht om de betrokkenen te wijzen op deze rechten en om ervoor te zorgen dat de betrokken deze rechten ook daadwerkelijk kunnen uitvoeren.

De rechten van betrokkenen bestaan uit:

- Recht op informatie: betrokkenen hebben het recht om te vragen of zijn/haar persoonsgegevens worden verwerkt.
- Recht op inzage: betrokkenen hebben de mogelijkheid om te controleren of, en op welke manier, zijn/haar gegevens worden verwerkt.
- Recht op correctie: als duidelijk wordt dat de gegevens niet kloppen, kan de betrokkene een verzoek indienen om dit te corrigeren.
- Recht op dataportabiliteit: dit is het recht om gegevens van betrokkene mee te nemen naar een andere organisatie of daar naartoe over te laten dragen.
- Recht op beperking van de verwerking: het recht om minder gegevens te laten verwerken.
- Recht van verzet: betrokkenen hebben het recht om te vragen om hun persoonsgegevens niet meer te gebruiken.
- Recht om vergeten te worden (ook wel: recht op vergetelheid): in gevallen waar de betrokkene toestemming heeft gegeven om gegevens te verwerken, heeft de betrokkene het recht om de persoonsgegevens te laten verwijderen.
- Recht op een menselijke blik bij besluiten. Dit betreft het recht van betrokkenen om niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking gebaseerd besluit waaraan rechtgevolgen zijn verbonden of waarbij sprake is van profilering.
- Recht op bezwaar (ook wel: klachtrecht): betrokkenen hebben het recht om bezwaar te maken tegen de verwerking van zijn/haar persoonsgegevens. De betrokkene kan een klacht indienen over het gebruik van diens persoonsgegevens. Als de betrokkene en de provincie er onderling niet uitkomen, kan betrokkene een klacht indienen bij de AP.

Om gebruik te maken van zijn/haar rechten kan de betrokkene een verzoek indienen. Als het verzoek niet wordt opgevolgd, kan betrokkene bezwaar (ex artikel 7.1. Algemene wet bestuursrecht (Awb)) maken bij de provincie Drenthe of een klacht indienen bij de AP.

Betrokkenen die een klacht hebben over de omgang met persoonsgegevens kunnen ook een klacht indienen bij de FG. De FG heeft een ombudsfunctie.

5.1 Stand van zaken afgelopen jaar

Onderdeel	Oordeel 2020	Oordeel 2021	Geen oordeel 2022 t/m 2024	Oordeel 2025
Verzoeken die betrokkenen hebben gedaan op grond van hun rechten worden adequaat, volgens de regels afgehandeld				

Het aanvraagproces is een gestructureerd digitaal proces. Betrokkenen kunnen een aanvraag doen via de website en inloggen met DigiD zodat de identiteit direct is vastgesteld. Dit hoeft niet, betrokkene kan ook een afspraak maken om zich te identificeren. Afgelopen jaar is één klacht is bij FG ingediend en één verzoek om verwijdering speelde bij PS. Beide verzoeken zijn binnen de termijn afgehandeld. Het proces is goed ingericht maar het opzoeken van de informatie in de (veelheid aan) systemen blijft een uitdaging.

Er worden door de provincie Drenthe geen beslissingen over betrokkene genomen door volledig geautomatiseerde besluitvorming.

6. Samenwerking

De provincie Drenthe werkt op meerdere beleidsterreinen, in diverse rollen en hoedanigheden, samen met (mede)overheden en private organisaties. Daarbij kan sprake zijn van een verwerking van persoonsgegevens tussen partijen: ontvangen van persoonsgegevens, verzenden van persoonsgegevens, maar ook het opslaan van en inzage hebben in persoonsgegevens vallen onder dit begrip. Deze verwerkingen dienen ook te voldoen aan de AVG. De provincie Drenthe dient dan ook afspraken te maken met andere partijen.

Bij doorgifte aan een derde partij als verwerker moeten er afdoende garanties zijn dat er verwerkt wordt volgens de AVG. De verwerker moet passende technische en organisatorische maatregelen treffen zodat deze voldoet aan de AVG en de bescherming van de rechten van de betrokkene gewaarborgd is. Deze afspraken worden vastgelegd in een verwerkersovereenkomst

Soms kan ook sprake zijn van een gedeelde verantwoordelijkheid voor de gegevensverwerking – de zogenaamde gezamenlijke verwerkingsverantwoordelijkheid. In die gevallen dient voor gegevensverwerking een voorziening te worden getroffen als bedoeld in artikel 26 van AVG – een regeling die voorziet in nakoming van de verplichtingen uit de AVG.

6.1 Stand van zaken afgelopen jaar

Onderdeel	Oordeel 2020	Oordeel 2021	Geen oordeel 2022 t/m 2024	Oordeel 2025
Voor elke verwerking door een derde partij sluit de provincie Drenthe een verwerkersovereenkomst af volgens de regels	○	○		●
Er is een overzicht van verwerkingsovereenkomsten	●	●		●
Voor relaties die een gezamenlijke verwerkingsverantwoordelijkheid tot gevolg hebben, is een toereikende regeling	●	●		●

De provincie beschikt over een eigen model verwerkersovereenkomst die gebruikt wordt. De meeste relaties van verwerker en verwerkingsverantwoordelijke komen vanuit het inkoopproces, bijvoorbeeld bij de aanschaf van software. Op het moment dat het een cloudoplossing betreft is duidelijk dat er sprake is van een verwerker. Het afsluiten van een verwerkingsovereenkomst is onderdeel van het inkoopproces. Echter, het komt ook voor dat er sprake is van een verwerking van persoonsgegevens onder de verantwoordelijkheid en zeggenschap van de provincie die niet formeel geregeld zijn en zonder dat er sprake is van een inkoopsituatie. In die gevallen is het niet altijd bekend dat het afsluiten van een verwerkersovereenkomst noodzakelijk is. Het kan daarom voorkomen dat het wordt gemist en is ook lastig te controleren omdat er geen centrale sturing en registratie is op het afsluiten van verwerkersovereenkomsten.

In voorkomende gevallen is geen zeggenschapsrelatie maar een gezamenlijke verwerkingsverantwoordelijkheid met een partner. Voorbeelden hiervan zijn samenwerkingen met andere overheden dan wel wanneer uitvoerende taken met een mate van uitvoeringsvrijheid worden belegd bij een andere organisatie. De AVG voorziet in de mogelijkheid om in dat geval een ‘artikel 26’ regeling op te stellen waarin afspraken staan om rollen en verantwoordelijkheden te verdelen, zoals waar de bevoegdheid neergelegd wordt om beveiligingsincidenten te melden. Dit is gebeurd voor de samenwerking tussen SNN en de provincies Groningen, Friesland en Drenthe. Ook met het Drents

energieloket is een overeenkomst afgesloten waarin afspraken staan over de verwerking van persoonsgegevens.
De relaties met uitvoerende partijen zijn echter steeds complexer geworden, denk hierbij aan het Fix-team en het Flex-team voor de uitvoering van het RES (Regionale Energie Strategieën) programma. Niet altijd is duidelijk wie de verwerkingsverantwoordelijke entiteit is of worden afspraken gemaakt over de opslag van data of het hanteren van de uitgangspunten bij gegevensverwerkingen. Niet qua techniek, beveiliging of toezicht.

6.2. Aanbevelingen

- Besteed in het kader het verbeteren van de privacy governance binnen de thema's aandacht aan de verplichting tot het afsluiten van verwerkersovereenkomsten. Als de changeprocedure bekend is en privacy ambassadeurs in staat zijn hun rol goed te vervullen, volgt in voorkomende gevallen het afsluiten van verwerkingsovereenkomsten.
- Hou de verhoudingen tussen de provincie en uitvoerende organisaties tegen het licht en maak afspraken over de verwerking en het toezicht op de verwerking van persoonsgegevens.

7. Beveiliging

Vanuit het algemene behoorlijkheidsbeginsel, het integriteitsbeginsel en het vertrouwelijkheidsbeginsel moet de provincie Drenthe passende technische en organisatorische maatregelen nemen voor de beveiliging van persoonsgegevens. In het Beleidskader informatiebeveiliging 2025-2029 heeft de provincie de kaders voor de beschermende maatregelen beschreven op het gebied van informatie(verwerking). Een goede informatiebeveiliging geeft meer bescherming van de privacy. Daarnaast geldt er onder de AVG een meldplicht datalekken. Dit houdt in dat incidenten, waaronder inbreuken op de persoonlijke levenssfeer van betrokkenen onder omstandigheden gemeld dienen te worden aan de AP en/of de betrokkene(n). Het bijhouden van een register van datalekken die zijn opgetreden is verplicht.

7.1 Stand van zaken afgelopen jaar

Onderdeel	Oordeel 2020	Oordeel 2021	Geen oordeel 2022 t/m 2024	Oordeel 2025
Er is een actueel Beleidskader informatiebeveiliging van de provincie Drenthe				
Er is een actueel register van datalekken die zijn opgetreden				
Alle datalekken, voor zover van toepassing, zijn volgens de regels waar nodig gemeld aan de AP en de betrokkene(n)				
Voor alle datalekken, voor zover van toepassing, zijn mitigerende maatregelen getroffen				

Het Beleidskader informatiebeveiliging is in 2025 opgesteld en vastgesteld.

Het proces datalekken is laagdrempelig en goed functionerend opgezet. Dit proces is vastgelegd in het protocol datalekken.
In de bijlage is een overzicht opgenomen van de datalekken in het afgelopen jaar. Hierin is opgenomen of het betreffende datalek wel of niet is gemeld aan de AP en de betrokkene(n) en welke maatregelen de organisatie heeft genomen om de negatieve effecten van het datalek (verder) te voorkomen dan wel te reduceren, de zogenoemde mitigerende maatregelen.

Opvallend is het, voor een organisatie met de omvang zoals die van de provincie Drenthe, lage aantal datalekken:16 in totaal. Daardoor ontstaat het vermoeden dat er meer incidenten zijn, maar men niet op de hoogte is van de meldplicht. In 2025 is één datalek bij PS gemeld aan de Autoriteit Persoonsgegevens.

Een intern datalek wat al jaren voortduurt is dat er persoonsgegevens in openbare Sharepointbibliotheken opgeslagen worden én voor iedere medewerkers van de provincie toegankelijk zijn. Dit gaat niet alleen om NAW-gegevens maar ook om kopieën van rijbewijzen, identiteitsbewijzen, CV's etc. Initiatieven om dit te verwijderen en ervoor te zorgen dat de bibliotheken vervolgens ook schoon blijven, hebben tot nu toe niet tot een significante daling geleid, hoewel de indruk bestaat dat de groei ervan wel minder is ten opzichte van de jaren ervoor.

De FG en CISO hebben een zeer nauwe samenwerking en beide zien een positieve trend in de groei in volwassenheid op het gebied van informatiebeveiliging. Inzicht en urgentiebesef bij het management vraagt over de hele linie om verbetering.

8. Verantwoording

De AVG legt de verantwoordelijkheid bij de organisatie zelf om aantoonbaar te maken dat deze voldoet aan de privacyregels. Door te voldoen aan de verantwoordingsplicht, levert de organisatie een belangrijke bijdrage aan de bescherming van het grondrecht van mensen op privacy. Dit betekent dat GS en PS aan moeten kunnen tonen dat verwerkingen van persoonsgegevens voldoen aan de beginselen van de AVG en aan de relevante wet- en regelgeving.

8.1 Stand van zaken afgelopen jaar

Onderdeel	Oordeel 2020	Oordeel 2021	2022 t/m 2024	Oordeel 2025
Er is adequate jaarlijkse lijnverantwoording richting directie.	🔴	🔴	Geen oordeel	🟡
Er is een adequate cyclus van rapportagemomenten door de FG	🟡	🟢	🔴	🟢

Het onderwerp privacy en informatiehuishouding is aan de orde geweest in de managementgesprekken tussen de domeinen bedrijfsvoering en bestuur en organisatie met de directie. Ook is in 2025 door de lijn een reflectie aan directie gerapporteerd over de onderdelen uit het sectorbeeld van de AP en daaruit is het programma CPI voortgekomen.

Binnen de provincie Drenthe is geen sprake van een structurele (schriftelijke) verantwoording vanuit alle thema's of programma's richting directie.

De FG heeft over de jaren 2022, 2023 en 2024 geen jaarrapportage gemaakt. De provincie secretaris is wel door middel van gesprekken op de hoogte gehouden, maar hier is geen verslaglegging van. Vanaf 2025 wordt wel weer een jaarverslag gemaakt waarmee de progressie of stagnatie in de tijd inzichtelijk wordt gemaakt.
Over de rapportagemomenten hebben de portefeuillehouder, provinciesecretaris en de FG afgesproken om mee te lopen met de reguliere planning en control cyclus. Dit houdt in dat de rapportage gegevensbescherming meeloopt met de jaarstukken en de FG tijdens de interim rapportage rapporteert over de mate van compliancy aan de AVG. Dit zijn ook de momenten dat de portefeuillehouder, GS, het presidium van PS en de OR geïnformeerd worden. De provinciesecretaris en Statengriffier worden voorafgaand aan deze twee formele momenten geïnformeerd.

Overleg tussen de FG met de provinciesecretaris, Statengriffier en portefeuillehouder vindt verder plaats als de actualiteit daar aanleiding toe geeft.

8.2 Aanbevelingen

- Stuur vanuit de directie op een adequate jaarlijkse lijnverantwoording om zicht te krijgen op de decentrale uitvoering van de AVG.

9. Provinciale Staten

De AVG legt de verantwoordelijkheid bij de organisatie zelf om aantoonbaar te maken dat deze voldoet aan de privacyregels. Dit speelt ook bij de Provinciale Staten als bestuursorgaan. Daar rust een zelfstandige verantwoordelijkheid om aan de AVG te voldoen.

De Statengriffier als eerstverantwoordelijke voor de uitvoering van de zorgplicht op het gebied van gegevensbescherming binnen PS, is in 2025 en de jaren daaraan voorafgaand beperkt gefaciliteerd en geïnformeerd door de FG en de ambtelijke organisatie van GS om op een structurele en effectieve wijze invulling te geven aan de verplichtingen die voortvloeien uit de AVG.
Anderzijds was de organisatorische capaciteit van de Statengriffie onvoldoende om hier invulling aan te geven. In 2025 is een belangrijke stap gezet door binnen de formatie van de Statengriffie te investeren in nieuwe rollen, waaronder een strategisch informatiemanager en een jurist met privacy in het takenpakket waardoor PS structureel beter in staat is om de compliance opgave te dragen.

Dit heeft geleid tot een situatie waarin PS in onvoldoende mate kon beschikken over de inhoudelijke en organisatorische randvoorwaarden om deze verantwoordelijkheid adequaat uit te voeren.
De uitdaging voor 2026 is om deze nieuwe capaciteit te verbinden met de specialistische kennis die bij de ambtelijke organisatie van GS aanwezig is, zoals expertise in privacy, informatieveiligheid en informatiemanagement, zodat PS beschikt over een volwaardige en duurzame ondersteuning bij het realiseren van AVG-compliancy.

Desondanks zijn de basisvoorzieningen voor een groot deel op orde. Het privacybeleid is van toepassing op alle bestuursorganen van de provincie en PS is daar waar het kan aangesloten bij de systematiek van GS

9.1 Stand van zaken afgelopen jaar

Onderdeel	Oordeel 2020	Oordeel 2021	Geen oordeel 2022 t/m 2024	Oordeel 2025
Provinciale Staten hebben basis voorzieningen om te voldoen aan de AVG.	🟡	🟡		🟡
De website van het Drents parlement bevat een privacyverklaring of een link naar de privacyverklaring van de provincie Drenthe	○	○		🔴
Het gebruik van opnames door het Drents parlement wordt uitgelegd op de website van het Drents parlement	○	○		🟢
Er is een richtlijn voor het anonimiseren	○	○		🔴
Statenleden werken in de beveiligde ICT omgeving	○	○		🟢
Statenleden worden bij installatie én via het Statenportaal geïnformeerd over het beleidskader privacy, de gedragscode en de omgang met privéapparaten.	🟢	🟢		🟢
De Statengriffie rapporteert jaarlijks aan het presidium van PS	○	○		🔴

Basisvoorzieningen
Basisvoorzieningen zijn bijvoorbeeld een register van verwerkingen, een privacy verklaring, standaarden voor verwerkersovereenkomsten of DPIA's en ingerichte AVG-processen zoals het proces meldplicht datalekken.

PS beschikt over een actueel register van verwerkingen. Deze is in 2025 geactualiseerd. Daar waar het kan zijn de standaarden en processen die GS gebruikt ook van toepassing op PS. Dit is het geval bij de standaarden voor het uitvoeren van DPIA's en voor het proces melden datalekken. Datalekken kunnen worden gemeld bij de Servicedesk. Ook de afhandeling van AVG-verzoeken van betrokkenen volgt het proces van GS.
De ICT en aanschaf van software wordt gefaciliteerd door de ambtelijke organisatie van GS waarmee het afsluiten van verwerkersovereenkomsten met software leveranciers ook ondervangen wordt.

PS communiceert op haar website nog niet welke rechten betrokkenen hebben, hoe deze uit te oefenen en heeft geen eigen voorziening getroffen voor het indienen van AVG-verzoeken. De rechten van betrokkenen staan in de privacyverklaring van de provincie Drenthe, maar die ontbreekt nog op de website van het Drents parlement.

Staten Informatiesysteem (SIS)
Commissie en Statenvergaderingen van het Drents parlement worden uitgezonden. Bij binnenkomst van de Statenzaal worden bezoekers geattendeerd op de opnames.
Deze audio- en videowebcasts worden opgeslagen in het SIS en gepubliceerd op de website van het Drents parlement. Het SIS wordt ook gebruikt voor de documentopslag. Ten aanzien van het in blijvend in goede geordende en toegankelijke staat bewaren van Stateninformatie loopt een actie om alle verslagen (opnames en stukken ouder dan 10 jaar) en alle andere daarvoor in aanmerking komende stukken over te brengen naar het e-depot.
Statenleden beschikken over een laptop die in beheer is bij thema ID&A en gebruiken het SIS voor het raadplegen van de Stateninformatie.

Anonimiseren
Voor publicatie moeten persoonsgegevens geanonimiseerd worden. PS communiceert via de website niet expliciet dat ze bij publicatie de persoonsgegevens zal anonimiseren en er is geen richtlijn voor het anonimiseren en verwerken van persoonsgegevens door de Statengriffie.

Het anonimiseren gebeurt handmatig. Mede naar aanleiding van een drietal datalekken waarbij per abuis persoonsgegevens op de website zijn gepubliceerd, gaat de Statengriffie per 2026 over tot het gebruik van anonimiserings-software. De inzet van slimme AI en taaltechnieken minimaliseert het risico op datalekken door onzorgvuldig handmatig anonimiseren. De licenties hiervoor zijn in 2025 aangeschaft.

Bewustwording
Voor een goede en juiste uitvoering is het van belang dat niet alleen de Statengriffie maar ook de statenleden zelf op de hoogte zijn van de beginselen van de AVG en hoe privacy bewust en informatieveilig te handelen. De Statengriffie gaat met ingang van 2026 de e-learningen op het gebied van informatiebeveiliging en privacy volgen die al ingezet worden bij GS.

Voor statenleden is van belang dat ze werken in de aangeboden beveiligde ICT-omgeving en geen gegevens opslaan op privéapparaten of persoonlijke mailaccounts. Dit zorgt ervoor dat aan de beginselen opslagbeperking, minimale gegevensverwerking en passende beveiliging van de AVG kan worden voldaan en zorgt voor een verkleining van het risico op datalekken.

9.2 Aanbevelingen

- Zet in overleg met de ambtelijke organisatie van GS een actieve lijn op zodat de Statengriffie (proactief) gefaciliteerd wordt op het gebied van privacy, informatiebeveiliging en informatiebeheer. Dit helpt de Statengriffier om aan de zorgplicht te voldoen.

- Governance: beschrijf de taken en rollen van de informatiemanager en jurist op het gebied van privacy en leg vast wie in geval van afwezigheid van de Statengriffier AVG verantwoordelijke is.
- Stel een richtlijn anonimiseren op. De Statengriffie heeft te maken met de soms lastige afweging ten aanzien van de transparantie van politieke besluitvorming versus de eerbiediging van de privacy van inwoners op het gebied van het publiceren van documenten. Een richtlijn voor het publiceren en verwerken van persoonsgegevens kan Statengriffiemedewerkers helpen om een goede afweging te maken en gedeeld worden met het presidium en statenleden. Advies is ook om met de ambtelijke organisatie van GS een werkwijze af te spreken dat documenten voor PS zoveel mogelijk (ook) publiceerbaar (lees geanonimiseerd) aan de Statengriffie aangeboden worden.
- Verwijs op de website van het Drents parlement naar de privacyverklaring op de website van de provincie Drenthe,
- Train statenleden op het informatieveilig en privacybewust handelen. Ter bescherming van de persoonsgegevens van inwoners maar ook ter bescherming van de statenleden zelf. Bestuurders bevinden zich per definitie in een kwetsbare positie als het gaat om slachtoffer te worden van de geraffineerde sluimerende aanwezigheid van georganiseerde (cyber) criminaliteit en ondermijnende activiteiten.
  Informeer over de gevaren en risico's van social mediagebruik, digitale intimidatie, bedreiging en chantage en de do's en don'ts op het gebied van informatieveilig werken. Laat ook onderwerpen als het gebruik van berichtendiensten bijvoorbeeld Whatsapp, het belang van het tijdig uitvoeren van beveiligingsupdates, het beperken van opslag van gegevens voor het statenwerk op privé apparaten en privé mail, en het beveiligen van privé apparaten onderdeel zijn van de trainingen.

.

10. Wet politiegegevens (Wpg)

De provincie Drenthe heeft medewerkers in dienst die taken verrichten in de rol van Bijzonder Opsporingsambtenaar (boa). Deze medewerkers voeren taken uit die vallen binnen de Wet politiegegevens (Wpg). Boa's mogen de grondslagen uit artikel 8 (dagelijkse politietaak), artikel 9 (handhaving van de rechtsorde in een bepaald geval) en artikel 13 (ondersteunende taken) van de Wpg gebruiken. Vanuit de Wpg is er een jaarlijkse interne auditverplichting voor de verwerkingsverantwoordelijke en om de vier jaar moet een externe audit uitgevoerd worden. In 2025 is de externe audit uitgevoerd en het resultaat van het assurance-onderzoek gaat naar de Autoriteit Persoonsgegevens. De FG heeft een aanvullende toezichts- en jaarlijkse rapportageverplichting. Het toetsingsverslag 2025 van de FG is meegenomen in de externe audit.

De externe auditor heeft twee aanbevelingen gedaan ter verdere optimalisatie van de interne beheersing. Er kan worden geconcludeerd dat binnen de provincie op zorgvuldige wijze wordt omgegaan met politiegegevens en dat de bestaande structuur in de basis robuust is. De genoemde verbeterpunten zijn vooral gericht op het verder formaliseren en aantoonbaar maken van al ingezette maatregelen.

Bevinding 1: Controle op autorisaties in het Boa Registratie Systeem (BRS)
De auditor heeft vastgesteld dat het BRS beschikt over een systeem van autorisaties dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid. De auditor merkt op dat minimaal tweemaal per jaar een controle op toegangsrechten dient plaats te vinden.

Bevinding 2: Auditplanning en uitvoering interne audits
De auditor constateert dat voor 2023 en 2024 een interne audit (interimcontrole) is uitgevoerd, maar dat over 2022 geen interne audit heeft plaatsgevonden. Ook wordt aanbevolen om een meerjarig auditplan op te stellen waarin per jaar is vastgelegd welke Wpg-onderwerpen worden getoetst.

De provincie heeft op 9 december 2025de aanbevelingen onderschreven. Het management zal zorgen voor de halfjaarlijkse autorisatiecontrole en een meerjarig auditplan, waarin per kalenderjaar de te toetsen Wpg-onderwerpen worden benoemd.

.

11. Conclusie

De provincie Drenthe beschikt over de noodzakelijke fundamenten voor gegevensbescherming en voldoet in opzet en bestaan grotendeels aan de AVG. Het privacybeleid is actueel en toereikend en ondersteunt de uitvoering binnen zowel GS als PS. In het beleid wordt helder uiteengezet aan welke principes de provincie zich houdt bij de verwerking van persoonsgegevens, op welke wijze hiermee wordt omgegaan en welke maatregelen zijn getroffen om te voldoen aan de geldende wet- en regelgeving. Alle relevante thema's zijn in het beleid opgenomen. Daarnaast is het Beleidskader informatiebeveiliging 2025–2029 vastgesteld en is het verwerkingsregister in 2025 geactualiseerd, waarmee de basis op orde is.

Tegelijkertijd vraagt de praktische toepassing om versterking. Het advies 'Implementatie en borging Privacy' van de FG, waarin verbeteracties op het gebied van governance en compliance worden aangereikt om de praktische toepassing en duurzaamheidsborging van het bestaande beleid te versterken, is volop in uitvoering.

Op procesniveau zijn randvoorwaarden aanwezig maar deze routes worden niet altijd consequent doorlopen. DPIA's worden te vaak achteraf uitgevoerd waardoor er geen rekening wordt gehouden met privacy by design en privacy by default

De belangrijkste structurele risico's liggen bij informatiebeheer: het ontbreken van dataclassificatie en labeling, te ruime toegangsrechten, willekeurige opslag van documenten en niet voldoen aan de wettelijke eisen voor wat betreft de archivering. De provincie Drenthe is hierin niet uniek. In het Sectorbeeld van oktober 2024 roept de Autoriteit Persoonsgegevens overheden op om kritisch naar de informatiehuishouding te kijken omdat het voldoen aan privacywetgeving sterk verband houdt met de algemene kwaliteit van de informatiehuishouding.

De in gang gezette inventarisatie binnen thema's en de technische oplossing voor datalabeling zijn belangrijke stappen, maar vragen om aanvullende organisatorische borging en een duidelijk handelingsperspectief voor medewerkers in de opslag van data in het algemeen en persoonsgegevens in het bijzonder.
.
Qua governance en bewustwording zijn rollen en verantwoordelijkheden beschreven: 1e lijn, procesverantwoordelijke, 2e lijn, privacy officer en 3e lijn, FG. In de uitvoering wordt eigenaarschap niet overal gevoeld en zijn privacy-ambassadeurs niet altijd tijdig aangehaakt bij nieuwe ontwikkelingen. De kwartiermaker privacy officer en het programma CPI (Cybersecurity, Privacy en Informatiebeheer) zijn van start gegaan om dit te verbeteren.
De afspraak om mee te lopen met de planning- en-control-cyclus voor rapportage vergroot de voorspelbaarheid van sturing en verantwoording.

Voor Provinciale Staten zijn de basisvoorzieningen in lijn met GS. Aandacht is nodig om de nieuwe capaciteit bij de Statengriffie te verbinden met de specialistische kennis die bij de ambtelijke organisatie van GS aanwezig is, de rollen en taken op het gebied van privacy te beschrijven en de publicatieprocessen (anonimiseren, metadata) te verbeteren. De geplande inzet van anonimiserings-software is cruciaal om datalekken bij publicatie te voorkomen.

Binnen de Wpg-context (boa's) is het beeld positief. De externe audit in 2025 concludeert dat zorgvuldig wordt omgegaan met politiegegevens, met verbeterpunten rond autorisatiecontroles en een meerjarig auditplan die inmiddels zijn onderschreven.

Samenvattend: De basis is gelegd. Met de uitvoering van het FG-advies "Implementatie en borging van privacy" zet de provincie de stap van 'opzet en bestaan' naar duurzame werking in de praktijk, waarmee privacybescherming aantoonbaar wordt geborgd en het vertrouwen van inwoners en partners verder wordt versterkt. Het resultaat hangt echter voor een groot deel af van het privacy bewustzijn van bestuurders, managers en medewerkers. Het is daarom van belang dit bewustzijn actief en structureel te bevorderen, voorbeeldgedrag te tonen en te sturen op de naleving van organisatorische en procedurele maatregelen op het gebied van de bescherming van persoonsgegevens.

Bijlage Overzicht datalekken

Overzicht van de gemelde datalekken in het jaar 2025. Hierin is opgenomen of het betreffende datalek wel of niet is gemeld aan de AP en/of de betrokkene(n) en welke maatregelen de organisatie heeft genomen om de negatieve effecten van het datalek (verder) te voorkomen dan wel te reduceren.

Melding	Soort	Actie	AP melding
M2509 0402	CV's in open SharePoint bibliotheek van Thema CMV	Verwijderd	Nee
M2508 0366	Datalek bevolkingsondersoek door gebruik Eurofins	Gebruik Eurofins databestanden gestopt totdat na onderzoek duidelijk was dat er geen kwetsbaarheid was bij de provincie.	Nee
M2506 1003	Namen op lijst ingekomen stukken op de website van Drents parlement.nl .	Verwijderd	Ja
M2507 1206	Metadate met persoonsgegevens op de website van Drents parlement	In behandeling	Nee
M2506 0145	Brief naar verkeerde ontvanger verstuurd	Ontvanger verzoecht de brief te vernietigen	Nee
M2511 1428	Kopie paspoort op Sharepoint Thema Bodem	Verwijderd	Nee
M2509 0181	Namen op lijst ingekomen stukken op de website van Drents parlement.nl .	Verwijderd.	Nee
M2512 1477	Publicatie naam in besluit op Website Provincie Drenthe	Verwijderd	Nee
M2511 1667	Bij Woo besluiten de KIX barcode niet verwijderd waardoor na omzetting beperkte persoonsgegevens zichtbaar zouden kunnen zijn.	Diverse besluiten aangepast. In de historische dossiers kunnen nog KIX codes staan. Zeer laag risico en beperkte impact	Nee
M2508 0388	Namen medewerkers op de website van Drents parlement.nl .	Namen geanonimiseerd	Nee
M2506 0078	Mail naar verkeerde ontvangers	Gemeld aan betrokkenen	Nee
M2504 0315	POB van medewerker zichtbaar in openbare Sharepoint bibliotheek	Verwijderd	Nee
M2502 1732	Mobiele telefoon gestolen	Verwijderd	Nee
M2506 0460	Onbekende gebruiker in Cisco beheer portaal	Rechten ingetrokken en geen activiteit van gebruiker te zien	Nee
M2504 0967	Metadata zichtbaar op publicatiewebsites Rijk	De door ons geuplode bestanden zijn gecheckt.	Nee
M2502 0879	Via Stack zijn mappen gedeeld	Geheel Stack wordt uitgefaseerd	Nee