FG-JAARVERSLAG 2025

Bestemd voor:

- Het college van Burgemeester en Wethouders van de gemeente Druten
- Het college van Burgemeester en Wethouders van de gemeente Wijchen
- Het bestuur en de directie van de Werkorganisatie Druten Wijchen

Datum: 15 juni 2026
Auteur: Functionaris Gegevensbescherming

Inhoud

1. Inleiding
De Functionaris Gegevensbescherming (FG) fungeert binnen de Werkorganisatie Druten Wijchen (WDW) als onafhankelijke toezichthouder en adviseur over de naleving van Algemene Verordening Gegevensbescherming (AVG) en de Wet politiegegevens (Wpg).

Ook is de FG contactpunt voor de Autoriteit Persoonsgegevens (AP) en aanspreekpunt voor betrokkenen (inwoners, medewerkers en andere personen waarvan de gemeenten of de WDW gegevens verwerkt). De wettelijke taken en bevoegdheden van de FG zijn opgenomen in artikel 38 en 39 van de AVG.

Op 1 mei 2025 is een nieuwe (startend) Functionaris Gegevensbescherming (FG) begonnen bij de Werkorganisatie Druten Wijchen. Deze FG heeft in het afgelopen jaar met een nieuwe blik naar de rol van FG en de inrichting van de privacy organisatie (privacy governance) van de WDW gekeken. Hierbij heeft zij hierbij geconstateerd dat er door haar voorgangster een mooie basis is gelegd voor privacy en persoons-gegevensbescherming. Maar ook dat het is het tijd voor een volgende stap. Privacy moet echt onderdeel worden van het dagelijks werk, het privacy-by-design principe moet meer toegepast gaan worden binnen de organisatie en er moet een privacy planning- en control cyclus worden ingericht. Hierdoor kan de organisatie beter doorgroeien naar een gedegen en meer volwassen ingerichte privacy organisatie, welke weerbaar is voor toekomstige ontwikkelingen.

2. Managementsamenvatting
Dit jaarverslag beschrijft de stand van zaken rond privacy en gegevensbescherming binnen de WDW over 2025. Het verslag is opgesteld door de FG en heeft als doel om bestuur en management inzicht te geven in de naleving van de AVG en Wpg, de belangrijkste risico’s en de ontwikkelrichting van de privacy governance.

In 2025 is het toezicht door de FG beperkt van omvang geweest. Dit hangt samen met de start van een nieuwe FG, het ontbreken van een Privacy Officer (PO) en het bestaan van rolconflicten tussen toezicht en uitvoering. Daardoor is het toezicht vooral reactief ingericht en is nog geen sprake van een structureel, risico gestuurd toezichtkader of periodieke rapportage aan het managementteam.

Tegelijkertijd is een basis aanwezig waarop kan worden voortgebouwd. Er is zicht op datalekken, DPIA’s worden uitgevoerd bij risicovolle verwerkingen en de organisatie toont in de praktijk bereidheid om zorgvuldig met persoonsgegevens om te gaan. Met de komst van PO’s in 2026 ontstaan randvoorwaarden om de scheiding tussen uitvoering, advies en toezicht beter te borgen en het toezicht verder te professionaliseren.

De FG ziet 2025 daarmee als een overgangsjaar, waarin is gewerkt aan rolverheldering en positionering, met als doel om vanaf 2026 te komen tot meer structureel en aantoonbaar toezicht.

3. FG- Jaarverslag 2025

3.1 Doel
Met dit jaarverslag wil de FG inzicht te geven in de belangrijkste activiteiten en bevindingen op het gebied van privacy en verbeterpunten voor het komende jaar te benoemen. Privacy is een gezamenlijke verantwoordelijkheid van de organisatie. Dit verslag helpt om transparant te zijn richting bestuur, management en inwoners. Het laat zien waar we staan en waar we naartoe werken.

3.2 AVG compliance en privacy governance
De FG-rol is sinds de invoering van de AVG in 2018 relatief nieuw en in veel organisaties nog in ontwikkeling, ook binnen de WDW. In de afgelopen jaren is een basis gelegd voor een AVG-conforme werkwijze. Door de toenemende complexiteit van

gegevensverwerking en de nadruk op aantoonbaarheid is echter een volgende ontwikkelstap noodzakelijk.

Een duidelijkere scheiding tussen uitvoerende privacy taken en het onafhankelijke toezicht door de FG is daarbij essentieel. Omdat er in de loop van 2026 twee Privacy Officers starten ziet FG duidelijk mogelijkheden om de privacy organisatie verder te professionaliseren. Door verantwoordelijkheden geleidelijk breder in de organisatie te verankeren, kan WDW doorgroeien naar een meer volwassen werkwijze op het gebied van privacy en gegevensbescherming, met meer privacy bewustzijn en minder afhankelijkheid van FG en PO.

3.2.1 Richtlijnen voor FG-advies en DPIA-besluitvorming

Een FG mag op grond van de AVG altijd advies uitbrengen. Dit kan zowel op verzoek als op eigen initiatief. De FG mag daarbij in principe zelf bepalen op welke wijze dat advies wordt gegeven. Om die reden bestaan binnen de organisatie geen vaste procedures voor het geven van gevraagd en ongevraagd FG-advies aan managers of de directie.

Het ontbreken van een duidelijke interne richtlijn kan er echter toe leiden dat voor management en directie niet altijd helder is hoe zij moeten handelen wanneer zij het niet eens zijn met een advies van de FG, of hoe dit zorgvuldig moet worden vastgelegd. Maar ook dat het voor de medewerkers niet duidelijk is hoe en wanneer de beslissing op een FG-advies wordt genomen. Een duidelijke richtlijn helpt om verwachtingen, verantwoordelijkheden en de manier van besluitvorming inzichtelijk te maken.

Daarnaast ontbreken binnen de organisatie afspraken over wat er gebeurt ná het FG-advies bij een DPIA. Hierdoor bestaat het risico dat DPIA’s onvolledig worden afgerond, dat rollen door elkaar gaan lopen of dat het bestuur niet aantoonbaar kan maken dat het zorgvuldig heeft gehandeld.

In het komende jaar wordt door de privacy organisatie dus worden gewerkt aan heldere richtlijnen die het MT kan vaststellen voor:

- Het geven van gevraagd en ongevraagd FG-advies;
- Het vastleggen van deze adviezen en eventuele daarop genomen besluiten;
- De besluitvorming na een DPIA-advies, inclusief de rol van directie en proceseigenaren.

3.3 Onafhankelijkheid FG

De toezichthoudende taak van de FG is in 2025 beperkt uitvoerbaar geweest door rolconflicten die voortkwamen uit een te grote betrokkenheid van de FG bij uitvoerende werkzaamheden. Dat betekent ook dat de onafhankelijke rol van de FG in de huidige praktijk niet is geborgd.

Concreet betekent dit dat de FG in 2025 toezicht heeft gehouden op het verwerkingsregister en het datalekkenregister, maar ook betrokken is bij het bijhouden daarvan. Dit heeft geleid tot een rolconflict en dat is niet in lijn met de onafhankelijkheid die van de FG wordt gevraagd (AVG art. 38–39). Daarnaast heeft de FG ook Woo-verzoeken met privacyaspecten af moeten handelen, maar de FG mag alleen adviseren over de privacy aspecten van een Woo-verzoek en mag toezien op naleving, maar mag geen besluiten nemen in Woo-procedures. Het laten afhandelen van Woo-verzoeken door de FG levert een rolconflict op dat niet in lijn is met de onafhankelijkheid die van de FG wordt gevraagd en in strijd is met artikel 38 en 39 van de AVG.

Deze voorbeelden hebben afgelopen jaar geen acute verstoringen opgeleverd, maar een rolconflict duidt wel op onvoldoende aantoonbare naleving van de AVG en Wpg. Vanuit toezichtperspectief is dit geen wenselijke situatie, omdat de FG onafhankelijk moet kunnen toezien. Zeker wanneer het openbare stukken betreft, zoals Woo-verzoeken en beleidsstukken, die moeten worden opgesteld en behandeld, kan een rolconflict gevolgen

hebben. Het risico lijkt misschien klein, maar wanneer raadsleden of inwoners het vertrouwen in de (onafhankelijkheid van de) FG verliezen, heeft een rolconflict een groot gevolg. Dit kan politiek gevoelig kan liggen of kan leiden tot imagoschade voor de organisatie en voor de FG persoonlijk. Het is daarom een goede stap dat er twee PO starten in de loop van 2026 zodat dit soort rolconflicten in de toekomst niet meer ontstaan en de positionering van de FG goed is geborgd.

3.4 Toezichtplan en risicomanagement

In het afgelopen verslagjaar is het toezicht op de naleving van de AVG en de bredere gegevensbeschermingskaders beperkt van omvang geweest. Dit hangt samen met het feit dat de FG in dit jaar nieuw is gestart en tijd nodig had om de positie, rol en onafhankelijke taak binnen de organisatie te verduidelijken en te verankeren. Daarnaast is sprake geweest van meerdere rolconflicten, onder meer door de combinatie van toezichttaken met uitvoerende of adviserende betrokkenheid op het gebied van informatieveiligheid. Dit heeft de ruimte voor structureel en risico gestuurd toezicht beperkt.

Verder ontbrak afgelopen jaar een PO, waardoor de scheiding tussen beleidsvoorbereiding, uitvoering en onafhankelijk toezicht onvoldoende was ingebed. Als gevolg hiervan heeft de FG het toezicht voornamelijk reactief ingericht, op basis van lopende dossiers, signalen uit DPIA's, datalekmeldingen en ad-hoc vragen. Er is nog geen uitgewerkt toezichtplan en er vond geen structurele rapportage plaats richting het managementteam. Dit is voor de FG een verbeterpunt om in het komende jaar op te pakken, zodat de FG ook meer ruimte krijgt om toezichtbevindingen periodiek te bespreken met het MT en het MT inzage te geven op de manier waarop de FG het toezicht wil vormgeven.

3.6 Suwinet

Omdat Suwinet zeer privacygevoelige informatie bevat moet het gebruik van Suwinet voldoen aan de bij de wet gestelde privacy- en beveiligingseisen (o.a. de Baseline Informatiebeveiliging Overheid). Of de gemeente voldoet aan deze eisen wordt door een externe auditor jaarlijks getoetst in de Suwinet audit. Ook afgelopen jaar heeft een audit plaatsgevonden en de WDW is geslaagd voor deze audit. De auditor heeft hierbij wel een aantal aandachtpunten aangedragen zoals o.a. het vaststellen van een bewustwordingsplan en meer bewustwording specifiek voor de Suwinet gebruikers.

Maar ook bij Suwinet constateert de FG een rolconflict dat in strijd is met artikel 38 en 29 van de AVG. De rol van Security Officer (SO) Suwinet ligt namelijk ook bij de FG. Dat betekent dat de FG onafhankelijk toezicht moet houden op de eigen uitvoerende rol van SO Suwinet. Omdat dit ook een ongewenste situatie is, wordt komend jaar bekeken hoe deze rol bij de PO kan worden belegd.

3.7 Wet politie gegevens (Wpg)

De Wet politiegegevens (Wpg) regelt hoe persoonsgegevens mogen worden verwerkt door opsporingsinstanties. Hieronder vallen ook gemeenten die werken met buitengewoon opsporingsambtenaren (boa's).

Om naleving van deze wet te borgen, is iedere organisatie die onder de Wpg valt verplicht om jaarlijks een interne Wpg-audit uit te voeren en eens per vier jaar een externe Wpg-audit te laten uitvoeren door een onafhankelijke auditor. Het rapport van de externe audit wordt aangeboden aan de Autoriteit Persoonsgegevens (AP).

De Werkorganisatie Druten Wijchen heeft in het verslagjaar zowel een interne als een externe Wpg-audit laten uitvoeren. Uit de auditresultaten blijkt dat voor een groot deel van de getoetste normen de vereisten op orde zijn en dat grotendeels wordt voldaan aan de eisen van de Wpg.

Uit het auditrapport komt ook naar voren dat voor een aantal Wpg-verwerkingen nog geen DPIA's zijn uitgevoerd, terwijl deze wel vereist zijn. Met de komst van de PO kan samen met de proceseigenaren een inventarisatie worden gemaakt van ontbrekende DPIA's binnen de organisatie. Op basis daarvan kan worden vastgesteld welke DPIA's prioriteit hebben voor uitvoering.

3.8 Artificial Intelligence (AI) en privacy

AI wordt binnen overheden in toenemende mate ingezet of verkend. AI raakt echter niet alleen privacy, maar ook andere domeinen zoals informatiebeveiliging, IT-architectuur, juridische kaders, ethiek, inkoop en besluitvorming. Daarnaast stelt de aankomende Europese AI-verordening (AI Act) eisen aan governance, risicobeheersing, transparantie en toezicht.

Vanuit haar adviserende en toezichthoudende rol constateert de functionaris voor gegevensbescherming FG binnen de WDW momenteel geen structurele werkgroep of stuurgroep is ingericht waarin deze verschillende disciplines gezamenlijk vertegenwoordigd zijn. Hierdoor ontbreekt een integrale en organisatiebrede benadering van AI-vraagstukken binnen de WDW.

De rol van de FG bij AI is beperkt tot het adviseren over en het toezicht houden op de verwerking van persoonsgegevens binnen AI-toepassingen. Voor een integrale, organisatiebrede en AI Act-conforme aanpak is een multidisciplinaire governance-structuur noodzakelijk, waarin naast privacy ook technische, juridische, organisatorische en ethische aspecten zijn belegd. De FG signaleert dit als aandachtspunt voor verdere ontwikkeling.

3.8.1 AI-governance en de IAMA

Binnen de organisatie neemt het gebruik van algoritmen en AI-toepassingen toe, waardoor uitvoering van de IAMA (Impact Assessment Mensenrechten en Algoritmen) noodzakelijk is. De IAMA betreft een uitvoerende, multidisciplinaire beoordeling die moet worden belegd binnen de lijnorganisatie, met betrokkenheid van beleidsmatige, juridische, technische en data-expertise. Het beleggen van deze taak bij de FG is niet verenigbaar met de onafhankelijkheid zoals vereist in artikel 38 AVG en toegelicht door de Autoriteit Persoonsgegevens.

Voor een zorgvuldige uitvoering en besluitvorming is een AI governancestructuur of stuurgroep noodzakelijk waarin de benodigde expertise samenkomt. Het is van belang dat dit in de organisatie duidelijk belegd wordt, zodat de IAMA's op een juiste en rechtmatige wijze worden uitgevoerd.

4.0 Cijfers en aantallen

In dit onderdeel van het jaarverslag zijn cijfers en aantallen opgenomen van de Data Protection Impact Assessments (DPIA's), datalekken en aantal keren dat een burger gebruik heeft gemaakt van de rechten die zijn opgenomen in de AVG.

4.0.1 Data Protection Impact Assessment (DPIA)

Een Data Protection Impact Assessment (DPIA) is een uitgebreide risicoanalyse die verplicht is bij verwerkingen met een hoog privacy risico (AVG, artikel 35). Het doel van een DPIA is om de gevolgen van gegevensverwerking voor betrokkenen inzichtelijk te maken en passende maatregelen vast te stellen om privacy risico's te voorkomen of te beperken.

Om te bepalen of een DPIA nodig is, maakt de organisatie gebruik van een pré-DPIA (een korte vragenlijst of checklist). De uitkomst van een pré-DPIA kan zijn dat geen volledige DPIA noodzakelijk is, of dat alsnog een volledige DPIA moet worden uitgevoerd door de betrokken proceseigenaar. Ook bij grote wijzigingen in bestaande processen kan het noodzakelijk zijn om een DPIA uit te voeren of een bestaande DPIA opnieuw te

beoordelen. De PO heeft hierbij een ondersteunende rol richting de proceseigenaar. De FG vervult een adviserende en toezichthoudende rol.

Binnen de WDW is de basis aanwezig voor het uitvoeren van een pré-DPIA en een DPIA. Tegelijkertijd constateert de FG dat blijvende aandacht nodig is voor het tijdig en structureel uitvoeren van een (pre) DPIA. Met de komst van een PO kan worden nagedacht over een gerichte verbeteraanpak, inclusief een inhaalslag voor DPIA's.

Daarnaast constateert de FG dat een DPIA in de praktijk niet altijd wordt uitgevoerd doordat proceseigenaren hiervoor onvoldoende tijd en kennis hebben. Hierdoor krijgt de DPIA soms onvoldoende prioriteit, terwijl dit instrument belangrijke inzichten oplevert voor het bestuur in privacy risico's en te treffen maatregelen. Bovendien draagt het uitvoeren van een DPIA bij aan bewustwording van privacy risico's bij proceseigenaren.

Hieronder wordt een overzicht getoond de pre DPIA's en DPIA's die in 2025 zijn gedaan met daarbij de status van de DPIA op het moment van opstellen van het FG-jaarverslag:

Onderwerp	**Pre DPIA of DPIA**	**Status**
Gebruik Duo fietsen	Pre DPIA	Geen DPIA nodig, procedure opgesteld
Monitoren gelden volwassensportfonds	Pre DPIA	Geen DPIA nodig, procedure opgesteld
Gebiedsaanpak Wijchen-Zuid	DPIA	Afgerond, verwerking gestart
Cameratoezicht Touwslagerbaan	DPIA	Afgerond, verwerking gestart
Verbetering dienstverlening	DPIA	Loopt, verwerking nog niet gestart
Onderzoek uit de Armoede	DPIA	Afgerond, verwerking gestart
Groene groei – energieadvies met videobeelden	DPIA	Loopt, verwerking nog niet gestart

4.0.2 Rechten van betrokkene

In 2025 zijn bij de WDW twee verzoeken van betrokkenen ingediend tot uitoefening van hun rechten (zoals inzage, rectificatie, verwijdering, beperking of bezwaar).

Recht	**Aantal**	**Opmerking**
Recht op vergetelheid	1	Geen bijzonderheden
Recht op inzage	4	Geen bijzonderheden

Deze verzoeken zijn afgehandeld door de afdeling AJZ, waarbij de FG als toezichthouder is betrokken. De onafhankelijkheid van de FG binnen dit proces is hiermee goed geborgd. Het is wel zo dat het proces nog niet formeel is beschreven in een werkinstructie of procedure en dat er in de praktijk twee privacy juristen zijn de weten hoe een verzoek moet worden afgehandeld. Om de continuïteit te borgen en een aantoonbaar proces te hebben adviseert de FG om het proces te vast te leggen in een procesbeschrijving met daarin een rol- en taakafbakening.

De conclusie van de FG is dat het proces in de basis goed werkt en de onafhankelijkheid van de FG is geborgd, maar dat formaliseren van het proces in de aantoonbaarheid, consistentie en continuïteit verhoogd.

4.0.3 Datalekken

In de periode januari t/m december 2025 zijn binnen de Werkorganisatie Druten Wijchen acht datalekken geregistreerd in het incidentenregister. Bij twee van de geregistreerde datalekken, die door inwoners zelf waren gemeld, bleek uit nader onderzoek dat het niet

om een datalek ging. Alle overige meldingen zijn ook beoordeeld en waar nodig zijn maatregelen getroffen, zoals het informeren van betrokkenen en het verbeteren van werkprocessen.

In geen van de gevallen is melding gedaan aan de Autoriteit Persoonsgegevens (AP), omdat de inschatting van de risico's voor betrokkenen daarvoor onder de meldingsdrempel bleef.

	Datalekken 2025	**Impact**	**Meldingsplicht AP**
1	Er was door de burger een fout mailadres doorgegeven bij het doen van een huwelijksmelding en daarom is de communicatie over het huwelijk naar dit foute mailadres gegaan.	Laag	Nee
2	Er zijn de namen van leerlingen bij begeleiders/intern begeleiders van scholen terecht gekomen. Deze namen stonden op de agenda om te bespreken en normaal staan hier alleen initialen. Het betreft hier alleen de namen er is verder geen informatie of stukken en alle ontvangers zijn professionals binnen de scholen. Allen waren bij 1 of 2 leerlingen zelf betrokken.	Laag	Nee
3	In een interne mailing aan leden van de PV is per ongeluk de cc gebruikt en niet de bcc. Er waren ook een aantal privé mailadressen die hierin stonden.	Laag	Nee
4	Er zijn 06-nummers van de voorzitters van de stembureaus meegestuurd naar een journalist in het document met de de opkomstcijfers.	Laag	Nee
5	Onderzoeksverslag naar de verkeerde client gestuurd	Laag	Nee
6	Onderzoeksverslag naar de verkeerde client gestuurd	Laag	Nee
7	Mogelijk onrechtmatig lekken van gegevens door de gemeente aan een VVE	Onderzocht geconstateerd geen datalek	Nee
8	Mogelijk onrechtmatig lekken van gegevens aan een isolatie advies bedrijf	Onderzocht geconstateerd geen datalek	Nee

De conclusie van de FG is dat medewerkers in de praktijk vaak tijdig en correct handelen. Tegelijk blijft aandacht nodig voor het herkennen van datalekken en het tijdig melden. Een niet-herkend of te laat gemeld datalek kan risico's opleveren voor zowel betrokkenen als de organisatie. Daarom is het belangrijk dat bewustwording en handelingsperspectief (wat te doen bij een incident) structureel worden geborgd.

5. Conclusie

Het jaar 2025 kenmerkt zich als een opstart- en overgangsjaar voor het privacy toezicht binnen de Werkorganisatie Druten Wijchen. Door de start van een nieuwe FG, het ontbreken van een PO en bestaande rolconflicten is het toezicht beperkt en vooral reactief ingericht geweest. Er is in dit verslagjaar nog geen gewerkt toezichtplan vastgesteld en er is geen structurele rapportagecyclus richting het managementteam ingericht.

In 2025 is nog geen gebruikgemaakt van het VNG/IBD AVG-borgingsproduct als formeel toetsings- en toezichtinstrument. De FG ziet dit borgingsproduct echter als een belangrijk hulpmiddel om het toezicht risico gestuurd, transparant en herhaalbaar in te richten.

Zodra de PO zijn gestart en de scheiding tussen uitvoering en toezicht beter is geborgd, kan dit instrument worden ingezet om de volwassenheid van privacy governance systematisch te meten en hierover te rapporteren.

De FG beschouwt 2025 als een jaar van positionering en bewustwording. De aandachtspunten en signalen in dit verslag vormen een basis voor verdere professionalisering van toezicht en risicomanagement in de komende jaren, met behoud van de onafhankelijke rol van de FG zoals bedoeld in artikel 38 en 39 van de AVG.