

Bijlage 1: AVG Governance

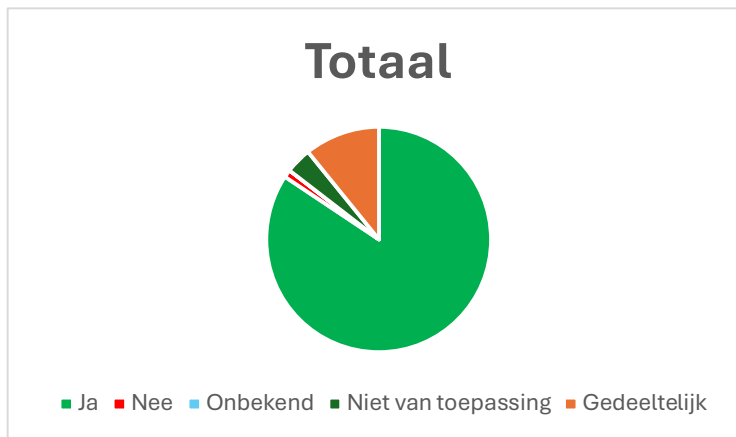
1. Privacy Control Framework

De Algemene Verordening Gegevensbescherming (hierna AVG) vereist voortdurende inspanningen om controle te verkrijgen en te behouden. Daarom is het belangrijk om te kijken waar het GBTwente nu staat, en waar de organisatie heen wil in relatie tot de AVG.

Voor de terugblik op 2025 is, evenals voorgaande jaren sinds 2019, gebruik gemaakt van het Privacy Control Framework¹. Hierbij worden vragen verdeeld over 7 categorieën.

Deze categorieën zijn:

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



Figuur 1: Totaalscore Privacy Control Framework

Deze 7 categorieën helpen om een groot deel van de gegevensbescherming te regelen en geven houvast bij het opzetten van de belangrijkste onderdelen om beter aan de AVG te voldoen.

In de tabel hieronder worden de verschillende totaalscores weergegeven (afgezet tegen de scores van voorgaande jaren):

Voldoen aan eis / afspraak	2019	2022	2023	2024	2025	Vershil 2025 met 2024:
Aantal keer Ja	141	162	163	163	157	omlaag
Aantal keer Nee	16	6	4	4	2	omlaag
Aantal keer Niet van toepassing	5	6	7	7	7	Gelijk
Aantal keer Gedeeltelijk	24	12	12	12	20	Omhoog

GBTwente scoort op een paar eisen nog een nee, maar voor het grootste gedeelte een ja of gedeeltelijk (zie ook figuur 1).

Enkele scores zijn aangepast van 'ja' naar 'gedeeltelijk'. Dit komt doordat verschillende documenten geactualiseerd moeten worden en de beschreven PDCA-cyclus in de praktijk niet helemaal werkbaar

¹ Een Excel-format van de VNG, waarbij de verschillende eisen vanuit de AVG vertaald worden in 200 vragen. Per vraag moet je invullen of je daar wel, niet of gedeeltelijk aan voldoet. Ook kun je aangeven dat een vraag niet van toepassing is voor jouw organisatie.

De vragenlijst is opgesteld voor gemeenten, maar kan ook voor een organisatie als het GBTwente worden gebruikt.

blijkt. Het actueel houden van het verwerkingenregister blijft een belangrijk aandachtspunt. Daarnaast verloopt het aanmeld-, afmeld- en wijzigingsproces niet altijd soepel.

2. Datalekken

In 2025 zijn er 30 meldingen als datalek gekwalificeerd. In 2024 waren dit er 39 en in 2023 in totaal 31.

Het doel is niet om helemaal naar nul datalekken te gaan, maar om ze op tijd te signaleren en maatregelen te treffen waar nodig.

In de tabel hieronder wordt per kwartaal beschreven welk soort datalek heeft plaatsgevonden.²

Aard van het datalek	Q1	Q2	Q3	Q4	2025
Persoonsgegevens van verkeerde persoons zichtbaar in portaal		1			1
Persoonsgegevens per ongeluk gepubliceerd					
Dossier op verkeerde persoons geboekt					
Apparaat of gegevensdrager kwijtgeraakt of gestolen			1		1
Persoonsgegevens mondeling gedeeld met onbevoegde ontvanger					
Post of mail verkeerd verstuurd of geopend door onbevoegde	7	6	4	3	20
Datalek bij externe verwerker					
Verkeerde persoon geselecteerd in brief of mail	2				2
Verkeerde adres of gegevens geselecteerd		1	2	2	5
Onbevoegd persoon heeft toegang tot persoonsgegevens			1		1
Totaal	9	8	8	5	30

Er zijn 3 datalekken bij de autoriteit persoonsgegevens gemeld. Het gaat in die gevallen voornamelijk om dwangbevelen of huurvorderingsbrieven die verkeerd verstuurd of bezorgd zijn. Door de aard de brief worden deze datalekken wel beschouwd als risico voor de persoonlijke levenssfeer van een betrokkene en moeten daarom ook aan de AP worden gemeld. De AP heeft geen contact gezocht na het maken van deze meldingen. Daarnaast zijn de betrokkene ook op de hoogte gesteld van de datalekken.

In 2025 heeft er een oefening plaatsgevonden over hoe om te gaan met een cyberaanval. In de voorgaande jaren heeft dit ook plaatsgevonden. Daarnaast vindt er elke vier weken een vergadering van het Cybercrisisteam plaats.

Vanaf 1 januari 2026 is de nieuwe procedure beveiligingsincidenten en datalekken in werking getreden. Vanaf die datum worden de datalekken voor Berkelland en Bronckhorst eveneens afgehandeld door GBTwente en niet meer door de Functionaris Gegevensbescherming van deze gemeenten, omdat zij nu zijn aangesloten bij de GR. Dit houdt in dat de verantwoordelijkheid voor het melden bij de AP en/of betrokkene(n) nu ook bij GBTwente ligt.

² In het document 'Overzicht beveiligingsincidenten en datalekken GBTwente 2025' staat de volledige lijst met datalekken en beveiligingsincidenten.

In de vernieuwde procedure beveiligingsincidenten en datalekken is de verantwoordelijkheid voor de beslissing om een datalek te melden bij de AP en/of betrokkene(n) formeel belegd bij de managers van de taakvelden.

3. Uitoefenen rechten door betrokkene

Personen hebben privacyrechten zodra een organisatie hun persoonsgegevens verwerkt. Deze rechten zijn bedoeld om mensen controle te geven over hun eigen gegevens. Een van deze rechten is het inzagerecht, waarmee een persoon inzicht krijgt in welke gegevens GBTwente over hen verwerkt.

In 2025 is er geen inzageverzoek geweest of zijn andere rechten van betrokkene uitgevoerd. (in 2024 waren er 3 inzageverzoeken en 2023 waren dit er ook 3)

Er is een AVG-portaal ingericht waar betrokkenen hun AVG-rechten kunnen uitoefenen. Het portaal zorgt ervoor dat verzoeken sneller kunnen worden afgehandeld, omdat de identificatiestap via DigiD verloopt. Daarnaast zorgt het portaal ervoor dat betrokkenen eenvoudiger een verzoek kunnen indienen.

4. Bewustwording

In 2025 zijn er verschillende activiteiten georganiseerd om de bewustwording te vergroten:

- Tijdens de introductiedag voor nieuwe medewerkers wordt aandacht besteed aan privacy en informatiebeveiliging door middel van een presentatie. Hierbij komen onder meer de basisprincipes van de AVG, het omgaan met datalekken en veilig mailen aan bod. Ook thema's op het gebied van informatiebeveiliging worden behandeld. Om de betrokkenheid te vergroten, is deze presentatie in 2025 interactiever ingericht.
- In 2024 is een verplichte e-learning beschikbaar gesteld voor alle medewerkers. Deze e-learning richt zich op onderwerpen zoals de AVG, social engineering, wachtwoordbeheer en phishing. Het uitgangspunt was dat iedere medewerker de modules in 2025 volgens planning zou afronden. Dit is niet behaald, aangezien de verplichte lessen gemiddeld voor 70 procent zijn afgerond
- Voor interne communicatie is op Insite een aparte groep *Informatiebeveiliging & Privacy* ingericht. Deelname aan deze groep is verplicht voor alle medewerkers. Via deze groep worden relevante ontwikkelingen en aandachtspunten gedeeld.
- Periodiek, per kwartaal, wordt inzicht gegeven in het aantal datalekken en beveiligingsincidenten aan het MT. De terugkoppeling vindt plaats tijdens de terugkoppeling moment binnen de verschillende taakvelden. Daarnaast is, op verzoek van de manager van de taakvelden Belastingen & Invordering en Databeheer & Heffen, een gerichte presentatie over datalekken verzorgd. Omdat de FG is gepositioneerd binnen het taakveld Strategie & Bedrijfsvoering, worden de datalekken binnen dit taakveld ieder kwartaal door de FG toegelicht.

5. Vooruitblik 2026 en verder

Hieronder worden verschillende onderwerpen belicht die in 2026 van belang zijn om de organisatie beter in control te houden:

AI en algoritmes

AI en algoritmen spelen een steeds grotere rol binnen organisaties en bieden kansen voor een efficiëntere en effectievere dienstverlening. Ook GBTwente heeft de ambitie om AI te gaan gebruiken. Tegelijkertijd kunnen deze technologieën risico's met zich meebrengen voor de privacy en de persoonlijke levenssfeer van betrokkenen. De organisatie moet daarom een goede balans vinden tussen technologische ontwikkeling en een zorgvuldige omgang met persoonsgegevens.

Met de inwerkingtreding van de Artificial Intelligence Act (AI Act) wordt van organisaties verwacht dat zij investeren in de AI-geletterdheid van medewerkers. Binnen de organisatie is hier al deels invulling aan gegeven door het organiseren van kennissessies. Het is belangrijk dat deze AI-geletterdheid blijft meegroeien met de wijze waarop AI binnen de organisatie wordt ingezet.

Actualiseren beleidsstukken en verwerkingenregister

De beleidsdocumenten *Rechten van betrokkenen* en *Privacybeleid*, evenals het verwerkingenregister, dienen te worden geactualiseerd. Deze documenten dateren uit 2022 en 2023. Inmiddels is gebleken dat niet alle inhoud nog actueel of juist is, dan wel dat de beschreven processen in de praktijk niet (volledig) uitvoerbaar zijn

FG-rol

De Autoriteit Persoonsgegevens heeft meerdere keren aangegeven strenger te zullen controleren op de juiste invulling van de FG-rol.³ Een FG moet een onafhankelijke positie binnen de organisatie innemen om zijn toezichthoudende functie goed te kunnen uitvoeren. Momenteel bevindt de FG zich voornamelijk in een uitvoerende rol, hetgeen mogelijk leidt tot belangenverstrengeling.

Voor een zuivere rolafbakening en om beter te voldoen aan wet- en regelgeving moet worden onderzocht in hoeverre de huidige rolverdeling kan blijven bestaan.

GBTwente kiest er voor nu voor, gezien omvang van de organisatie de grootte van de taken, de huidige invulling van de FG in stand te laten.

³ [Brieven aan Breda en Doesburg over gegevensbescherming | Autoriteit Persoonsgegevens](#) In de brieven staan de bevindingen van de AP. Ook geeft de AP de gemeenten enkele aanbevelingen mee, bijvoorbeeld over het verwerkingsregister, DPIA's en de positionering van de functionaris gegevensbescherming (FG).