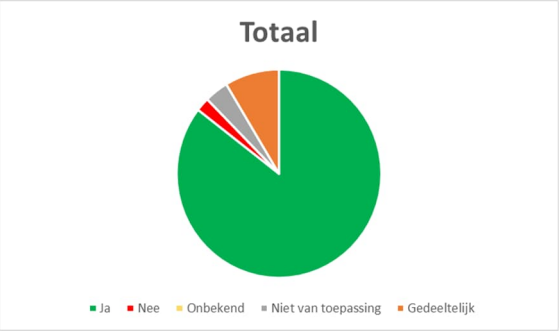
Bijlage 1: AVG Governance

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 2024 is, evenals voorgaande jaren sinds 2019, gebruik gemaakt van het Privacy Control Framework[1]. 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	Verschil 2024 met 2023:
Aantal keer Ja	141	162	163	163	Gelijk
Aantal keer Nee	16	6	4	2	Gelijk*
Aantal keer Niet van toepassing	5	6	7	7	Gelijk
Aantal keer Gedeeltelijk	24	12	12	14	Gelijk

GBTwente scoort op een paar eisen nog een nee, maar voor het grootste gedeelte een ja of gedeeltelijk (zie ook figuur 1). *Een paar punten zijn aangepast van 'nee' naar 'gedeeltelijk'. Dit komt vooral door de formulering van de vragen in het borgingsproduct. Strikt genomen zou dit als 'nee' kunnen worden beoordeeld, maar omdat we deze aspecten op een andere manier wel meenemen, zijn ze als 'gedeeltelijk' gemarkeerd.

Het is goed om in 2025 te evalueren of het Privacy Control Framework nog steeds de juiste tool is om in kaart te brengen hoe GBTwente voldoet aan de AVG en welke stappen er nog gezet moeten worden.

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.

2. Datalekken

In 2024 zijn er 39 meldingen als datalek gekwalificeerd. In 2023 waren dit er 31 en in 2022 in totaal 33. De stijging kan komen doordat er binnen de organisatie steeds meer bewustwording is over datalekken.

Het doel is dan ook 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.

Aard van het incident	Q 1	Q2	Q3	Q4	2024
Persoonsgegevens van verkeerde persoons zichtbaar in portaal			1		1
Persoonsgegevens per ongeluk gepubliceerd	1				1
Dossier op verkeerde persoons geboekt	2		1		3
Apparaat of gegevensdrager kwijtgeraakt of gestolen			1		1
Persoonsgegevens mondeling gedeeld met onbevoegde ontvanger				2	2
Post of mail verkeer verstuurd	8	8	4	10	30
Datalek bij externe verwerker		1			1
Totaal	11	9	7	12	39

Er is één datalek gemeld bij de Autoriteit Persoonsgegevens. Dit betrof de ransomware-aanval bij een leverancier. Dit datalek laat goed zien hoe groot de impact kan zijn op de organisatie wanneer een leverancier wordt gehackt.

GBTwente heeft in 2023 al een oefening gedaan over hoe om te gaan met een cyberaanval, en ook in 2024 heeft er een oefening plaatsgevonden. Daarnaast vindt er maandelijks een meeting plaats met het cybercrisisteam.

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 2024 zijn er drie inzageverzoeken geweest. (In 2023 waren dit er ook drie en in 2022 was dit er één). Inzageverzoeken hebben een termijn van één kalendermaand. Zodra een betrokkene een verzoek indient, start deze termijn. Dit betekent dat als de organisatie pas later aan de Functionaris Gegevensbescherming (FG) doorgeeft dat er een inzageverzoek is, er minder tijd overblijft om het verzoek te behandelen.

Er is een speciaal mailadres om de verzoeken in te dienen, maar dit mag ook via een andere weg. Hierdoor kan het voorkomen dat sommige verzoeken later pas in behandeling worden genomen. Tot op heden zijn alle verzoeken altijd binnen de gestelde termijn behandeld.

4. Bewustwording

In 2024 zijn er verschillende activiteiten georganiseerd om de bewustwording te vergroten:

- Er is een Lunch & Learn georganiseerd over de AVG. Daarnaast is er een presentatie gegeven over de Data Protection Impact Assessment (DPIA) om het MT en sleutelpersonen te informeren over wanneer een DPIA noodzakelijk kan zijn en wanneer advies moet worden gevraagd.
- Nieuwe medewerkers krijgen tijdens de introductiedag een presentatie vanuit Privacy & Informatiebeveiliging. Hierin worden de basisbeginselen van de AVG, datalekken en beveiligd mailen besproken. Daarnaast worden ook onderwerpen vanuit Informatiebeveiliging behandeld.
- Dit jaar wordt gebruikgemaakt van een e-learning. Medewerkers zijn verplicht deze lessen te volgen. De e-learning behandelt onder andere de AVG, social engineering, wachtwoordbeheer en phishing. Afgesproken is dat iedere medewerker in 2025 conform de planning de cursussen heeft gemaakt.
- Op Insite is een eigen groep aangemaakt (Informatiebeveiliging & Privacy), waar elke medewerker verplicht lid van is. In deze groep worden verschillende relevante onderwerpen besproken.
- Elk kwartaal wordt een overzicht gestuurd van de datalekken en beveiligingsincidenten. Op verzoek van het MT is de rapportage gewijzigd van een jaarlijkse naar een kwartaalrapportage. Daarnaast kwam vanuit de MT-leden de vraag om langs te gaan bij de verschillende taakvelden. Echter, dit heeft tot op heden nog niet plaatsgevonden.

5. Vooruitblik 2025 en verder

Hieronder worden verschillende onderwerpen belicht die in 2025 van belang zijn om de organisatie beter in control te houden:

Informatie Security Management Systeem (ISMS)

In 2024 is er een ISMS-tool aangeschaft om processen rondom privacy en gegevensbeheer beter te stroomlijnen. In 2025 wordt deze tool verder ingericht en geoptimaliseerd, zodat het zo effectief mogelijk kan worden ingezet.

De tool helpt om overzicht te houden op verschillende verplichtingen, zoals de eisen uit de AVG. Hierdoor wordt het makkelijker om aan deze regels te voldoen en sneller inzicht te krijgen in welke acties nodig zijn.

Bewaartermijnen

In 2024 is er een inzageverzoek geweest. Het bleek dat deze persoon langer dan noodzakelijk in de systemen stond. Een organisatie moet persoonsgegevens verwijderen zodra deze niet meer nodig zijn voor het doel waarvoor ze zijn verkregen (art. 5.1 lid c AVG). Het is belangrijk om te onderzoeken hoe de bewaartermijnen beter kunnen worden geregeld in de systemen.

AI en algoritmes

De opmars van AI biedt enorme kansen, maar deze technologische vooruitgang vraagt om een zorgvuldige aanpak waarbij de risico's goed in de gaten worden gehouden. Zonder een doordachte strategie kan het snel invoeren van AI tot problemen leiden. Denk bijvoorbeeld aan ethische kwesties, zoals het versterken van vooroordelen. Daarnaast zijn er praktische risico's, zoals systeemstoringen of cyberaanvallen, die belangrijke processen kunnen verstoren. Om deze risico's aan te pakken, is een integrale aanpak nodig die zowel de technische, ethische als juridische aspecten omvat.

Data-ethiek en privacy hoeven geen obstakels te zijn voor innovatie; ze vormen juist de basis voor duurzame en verantwoorde technologische vooruitgang. Daarnaast kan dit ook bijdragen aan het vergroten van het vertrouwen van inwoners in het gebruik van deze technologie.

Onlangs is de Artificial Intelligence Act (AI Act) ingegaan. Deze nieuwe wet geldt niet alleen voor organisaties die AI-modellen ontwikkelen, maar ook voor bedrijven en instellingen die ermee werken. Vanaf 2 februari 2025 moeten organisaties actief aan de slag met het bevorderen van AI-geletterdheid. Het is daarbij belangrijk om ook stil te staan bij de privacyrisico's, zodat medewerkers die in de toekomst met AI of algoritmes werken zich bewust zijn van de mogelijke impact en verantwoordelijkheden.

Business intelligence tools

Er wordt gebruikgemaakt van business intelligence-tools binnen GBTwente. Het is mogelijk dat soms meerdere gescheiden databases alsnog aan elkaar worden gekoppeld om zo tot meer en beter inzicht te komen. Dit kan bepaalde risico's met zich meebrengen vanuit privacyoogpunt. Daarom is het wenselijk om een beter beeld te krijgen van hoe en waarvoor deze tools worden gebruikt en, waar nodig, spelregels op te stellen voor het inrichten en werken met dit soort analyse- en rapportagetools.

Leveranciersmanagement

Een trend die werd geconstateerd, is dat hackers zich steeds meer richten op de leveranciers van gemeentelijke regelingen, gemeenten of andere grote organisaties. In 2024 hebben er verschillende hacks plaatsgevonden bij leveranciers van meerdere gemeenten, waarbij veel persoonsgegevens zijn gestolen. Ook de hack bij AddComm laat goed zien welke impact dit heeft op een organisatie. Dit benadrukt tevens het belang van een goed leveranciersmanagementbeleid en de uitvoering daarvan.