FG-verslag 2025

Gemeente Raalte



Aan: het bestuur van de gemeente Raalte
Van: Lucas Klekamp, functionaris gegevensbescherming (FG)

25 februari 2026

Gemeente Raalte

Beoordeling

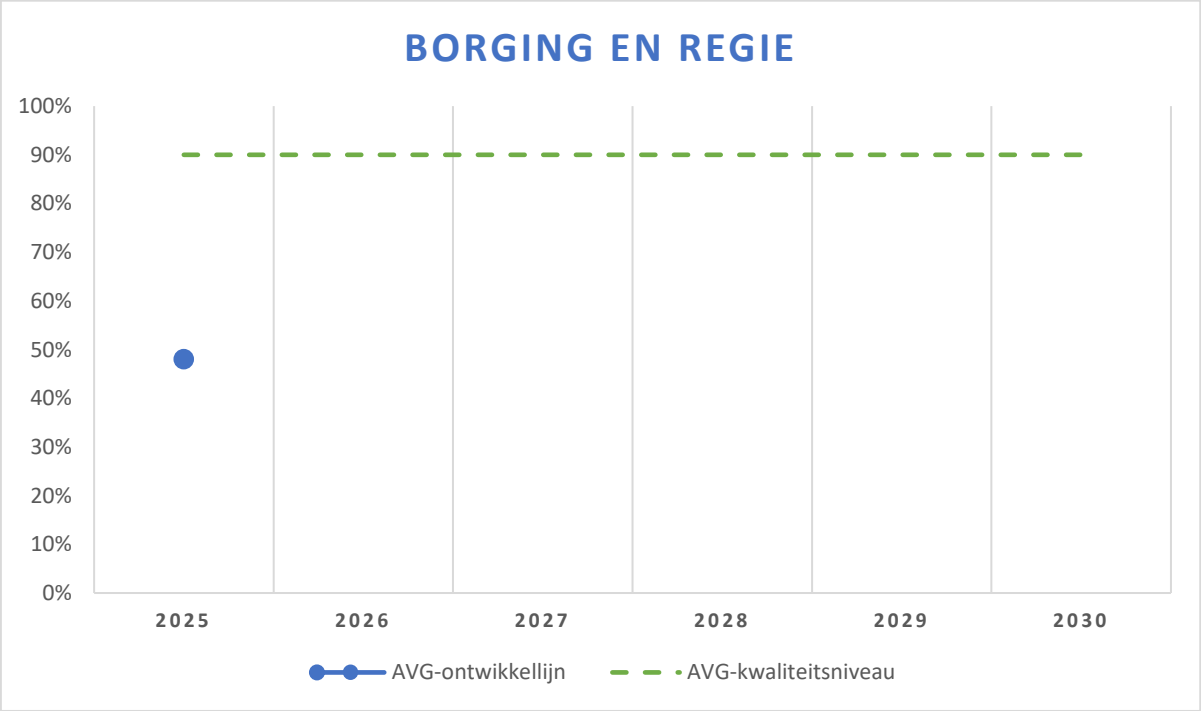
Jaarlijks breng ik verslag uit van de naleving van de Algemene Verordening Gegevensbescherming (AVG)[1] door gemeente Raalte. Voor u ligt het verslag over 2025.

De AVG gaat over de doelmatigheid en doeltreffendheid van praktische waarborgen rondom de gemeentelijke bedrijfsprocessen die afhankelijk zijn van persoonsgegevens. Die praktische waarborgen zijn bedoeld om personen (meestal inwoners) passend te beschermen tegen de keerzijden van de gegevensverwerking. Bij keerzijden kunt u denken aan het registreren van onjuiste informatie over mensen, het onterecht wel óf niet delen van persoonsgegevens met anderen, het niet voldoende beveiligen van gebruikte systemen of het inzetten van discriminerende algoritmes. Allemaal vormen van gebrekkige gegevensverwerking die daadwerkelijke gevolgen voor mensen kunnen hebben. De Toeslagenaffaire en het datalek bij Bevolkingsonderzoek Nederland zijn voorbeelden die het maatschappelijk belang illustreren.

Vanaf dit jaar hanteer ik een nieuwe methode[2] om de mate van naleving te beoordelen en te visualiseren. De gemeente wordt getoetst op de naleving van de AVG op basis van tien toetspunten die logischerwijs uit de AVG voortvloeien. Dit leidt tot een percentage, de jaarscore.
U kunt deze eerste keer zien als een nulmeting.

De jaarscore geef ik hieronder weer in de grafiek. Ieder jaar krijgt de gemeente opnieuw een score en zal er een ontwikkellijn ontstaan. Een 100% score is lastig vol te houden. Bij een score onder de 90% is bijsturing nodig. Op pagina 5 wordt deze methode verder toegelicht.

Voor 2025 komt gemeente Raalte op een jaarscore van **48%.**



[1] Waar van toepassing ziet dit verslag ook op de naleving van de Wet Politiegegevens. Ten behoeve van de leesbaarheid hanteer ik alleen het begrip 'AVG'.
[2] Deze methode is ontwikkeld door Privacy Management Partners en wordt ook bij een aantal andere gemeenten gebruikt door de FG.

FG-advies voor de komende periode

Voor het laten stijgen van de ontwikkellijn zijn mijn drie belangrijkste adviezen:

1. Waarborg de beschikbaarheid van voldoende 2e lijn-ondersteuning (privacy officers).
2. Stel een werkprogramma op met lange termijn doelen wat zich richt op het bereiken van een volwassen organisatiecultuur naar AVG-maatstaven en praktische oplossingen voor maatschappelijk verantwoorde gegevensverwerking (passende maatregelen om personen te beschermen).
3. Richt interne verantwoordingslijnen in m.b.t. AVG-beleidsvoering tussen domeinmanagers, directie en bestuur.

Overig advies treft u aan in de rechterkolom op pagina 6.

Toelichting

De AVG is niet zozeer een privacywet, maar het beschermt personen tegen de risico's van gegevensverwerking. De gemeente draait voor het grootste gedeelte om gegevensverwerking. Zonder gegevensverwerking immers geen gemeentebelastingen, burgerzaken, dienstverlening in het sociaal domein, werkgeverschap, fraudeonderzoek, datagedreven werken etc. De kunst is om op bestuurlijk niveau AVG-conform te sturen, zodat op uitvoeringsniveau alles in orde komt én in orde blijft.

Om op het AVG-kwaliteitsniveau te komen is een helder beleidskader onmisbaar. Dit vormt het fundament. Een goed beleidskader bevat een AVG-managementaanpak dat wordt gekenmerkt door een duidelijke verdeling van rollen en verantwoordelijkheden, risicosturing en afdwingbaarheid.
Positief is te noemen dat gemeente Raalte in 2025 haar Privacybeleidskader uit 2018 heeft geactualiseerd. Zowel in het MT als in het college is hier uitgebreid aandacht voor geweest. Dit schept vertrouwen en zal hopelijk leiden tot een aanpak die beter aansluit bij de bedoeling van de AVG.
Ook heeft het MT geactualiseerde procedures omtrent AVG-verzoeken (zoals verzoeken om inzage of verwijdering) en het afhandelen van datalekken vastgesteld. Dit zal naar verwachting helpen om deze processen beter te laten verlopen.

Om de AVG-beleidsvoering handen en voeten te geven is slagvaardige 2e lijn-ondersteuning (in de vorm van privacy officers) noodzakelijk. De gemeente heeft moeite om voldoende 2e lijn-ondersteuning te borgen. Raalte deelt de beschikbare capaciteit aan privacy officers met gemeenten Deventer en Olst-Wijhe. Ook in 2025 waren de privacy officers niet volledig bezet. Hierdoor blijft de gemeente te veel hangen in de waan van de dag. Dit betekent dat de capaciteit voornamelijk gaat naar vraaggestuurde ondersteuning aan de gemeenteorganisatie, de afhandeling van intern gemelde datalekken en van AVG-verzoeken. Hierdoor bleven inwoners gelukkig onverminderd toegang houden tot AVG-dienstverlening, maar tegelijkertijd lukt het de gemeente onvoldoende om op een gestructureerde wijze te werken aan het optimaliseren van de gemeentelijke werkprocessen. Dit betekent concreet dat het uitvoeren van DPIA's[3] (AVG risico-analyses) op hoog risico processen achterblijft. DPIA's zijn instrumenteel om te bepalen welke beschermende maatregelen binnen een specifiek werkproces passend zijn.

Naar verwachting heeft de gemeente nog enkele jaren nodig om over de volle breedte op het kwaliteitsniveau van de AVG te komen. In het nieuwe Privacybeleidskader heeft het college de ambitie uitgesproken om in 2030 dat kwaliteitsniveau bereikt te hebben. De haalbaarheid hiervan is niet alleen afhankelijk van voldoende capaciteit aan privacy officers, maar is met name ook afhankelijk van bestuurlijk support en interne verantwoordingsafspraken tussen directie en domeinmanagers. Het is zaak om de afspraken op papier (Privacybeleidskader) in de praktijk te brengen en daarmee het eigenaarschap op alle niveaus van de organisatie te borgen.

Daarnaast zal de gemeente moeten prioriteren; niet alles kan tegelijk. Het opstellen van een meerjarenplan/werkprogramma helpt om risico gebaseerd en planmatig de nodige verbeteringen in gang te zetten en te groeien naar een volwassener organisatiecultuur.

[3] Data Protection Impact Assessments (art. 35 AVG en art. 4c Wet Politiegegevens)

Verantwoording

De functionaris gegevensbescherming (FG) is wettelijk toezichthouder naar Europees recht op de interne naleving van de AVG, gerelateerde wet- en regelgeving en het gemeentelijk gegevensbeschermingsbeleid. Het FG-verslag ondersteunt de verantwoording door het college van B&W aan de raad en eventueel anderen. Daarnaast beschikt de accountant op deze manier over een in onafhankelijkheid afgegeven beoordeling van de gemeentelijke AVG-beleidsvoering.

Voor de beoordeling van de mate waarin de gemeente aan de AVG voldoet hanteer ik hierna tien toetspunten (prestatie-indicatoren) op bestuurlijk niveau die zijn voorzien van de volgende symbolen:



Afwezig of niet aantoonbaar



In aanzet aanwezig en aantoonbaar



Substantieel aanwezig en aantoonbaar



Grotendeels aanwezig en aantoonbaar



Volledig aanwezig en aantoonbaar

Ze zijn geplaatst in drie kolommen:

- **Opzet:** De aanpak klopt op papier – er is goed over nagedacht.
- **Bestaan:** De aanpak is volgens plan in praktijk gebracht – de gemeente heeft daadwerkelijk in passende gegevensbescherming voorzien.
- **Werking:** De aanpak blijkt ook in de praktijk doelmatig en doeltreffend.

Alle symbolen behoren volledig donkerblauw te zijn. Naar AVG-maatstaven doet het gemeentebestuur er dan al het nodige aan om behoorlijk bestuur te betrachten in het digitale tijdperk. Inwoners, medewerkers en andere doelgroepen kunnen dan rekenen op een mensgerichte aanpak. Het gemeentebestuur waarborgt dan AVG-rechtsbescherming.

Oordeelsvorming vloeit voort uit gesprekken, documenten, periodiek overleg, adviesaanvragen (bijvoorbeeld bij DPIA's), zo nodig klachtonderzoek of ander contact.

De gemeente verdient punten via de symbolen, die tegelijk ook percentages verbeelden. Percentages in de opzet-kolom tellen 1 keer, in de bestaan-kolom 2 keer en in de werking-kolom 3 keer. Op deze manier kom ik tot een gewogen gemiddelde, de jaarscore.

Toetspunten	Opzet	Bestaan	Werking	Advies
1. Beleid *Bestuurlijke borging AVG-rechtsbescherming*				1. Breng het geactualiseerde privacybeleidskader in de praktijk door interne verantwoordingslijnen in te richten m.b.t de AVG-beleidsvoering tussen domeinmanagers, directie en bestuur.
2. Regie en support *Ondersteuning door een slagvaardig AVG-ondersteuningsteam*				1. Waarborg de beschikbaarheid van voldoende 2e lijn-ondersteuning (privacy officers). 2. Houd in de gaten of de huidige capaciteit voor privacy officers op de langere termijn voldoende is. 3. Blijf de samenwerking van multidisciplinaire deskundigheid binnen afdeling Digitalisering & Data (Deventer) stimuleren.
3. Toezicht *Onafhankelijk toezicht en expertise*				1. Betrek de FG naar behoren en tijdig bij alle bestuurlijke besluitvorming waar bescherming van persoonsgegevens aandacht behoeft.
4. Werkprogramma *Meerjarenplan*				1. Stel een werkprogramma op met lange termijn doelen wat zich richt op het bereiken van een volwassen organisatiecultuur en praktische oplossingen voor maatschappelijk verantwoorde gegevensverwerking (passende maatregelen om personen te beschermen). 2. Laat directie/MT op basis van prioriteitstelling en het werkprogramma een jaarplan opstellen met de acties voor de korte termijn. Zorg dat deze acties concreet en meetbaar worden beschreven (SMART). Neem waar nodig proceseigenaren hierin mee. 3. Laat de privacy officers periodiek verslag doen aan directie/MT over het behalen van de in het jaarplan gestelde doelen en eventuele knelpunten.
5. Binnenshuis *Kwaliteit van eigen werkprocessen en informatieverwerking op orde*				1. Voer DPIA's uit op risicovolle werkprocessen om te komen tot passende maatregelen. 2. Zorg dat de gemeentelijke processen zijn terug te vinden in het verwerkingsregister en gebruik het register als centraal overzicht om regie te houden op de uitvoering van de DPIA's.
6. Buitenshuis *Uitbesteding en deelname in samenwerkingsverbanden op orde (ketenregie)*				1. Gebruik de DPIA-systematiek om ook risico's bij uitbesteding en ketensamenwerking in kaart te brengen. Dit zodat aantoonbaar kan worden voorzien in passende afspraken om personen te beschermen. 2. Zorg dat ook uitbestede taken en processen in samenwerkingsverbanden waar de gemeente een (gezamenlijke) verwerkingsverantwoordelijkheid heeft, voorkomen in het verwerkingsregister.
7. Verzoeken, klachten en incidenten *Veerkracht en servicegerichtheid*				1. Zorg dat de nieuwe vastgestelde procedure voor AVG-verzoeken goed landt binnen de domeinen en bij proceseigenaren, zodat verzoeken binnen de wettelijke termijn afgehandeld worden. 2. Zorg voor een overzichtelijkere datalekkenadministratie, zodat deze indien nodig gemakkelijk gedeeld kan worden met de Autoriteit Persoonsgegevens.
8. Communicatie en training/opleiding *Cultuur, begrip en draagvlak*				1. Zorg voor meer doelgroepgerichte interne en externe communicatie over de verwerking van persoonsgegevens door de gemeente. 2. Stel een i-basistraining verplicht voor nieuwe medewerkers. 3. Geef proceseigenaren passende training zodat ze hun verantwoordelijkheden kunnen waarmaken. Waarborg dat personeelswisselingen niet kunnen leiden tot een kennisgat.
9. Informatiebeveiliging *Beschikbare, betrouwbare en veilige informatievoorzieningen*				1. Geef risicomanagement vorm door middel van het inrichten van een information security management systeem (ISMS). Betrek hierbij de proceseigenaren. 2. Implementeer aanvullende beveiligingsmaatregelen die voortvloeien uit de Cyberbeveiligingswet. Heb hierbij specifiek aandacht voor dataclassificatie.
10. Budget *Financiële middelen*				1. Stel voldoende budget beschikbaar via de jaarbegroting en de budgetten van de domeinen die persoonsgegevens verwerken, om verbeteringen op voorgaande punten te realiseren. 2. Heb specifiek aandacht voor voldoende budget voor 2e lijn-ondersteuning (privacy officers).