

Bescherming van persoonsgegevens in Papendrecht

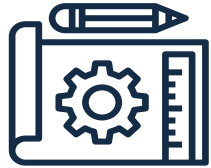
Presentatie onderzoeksresultaten
gemeenteraad Papendrecht
9 januari 2025

Inhoud



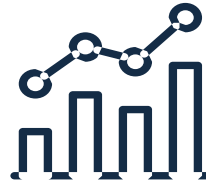
01

**Aanleiding,
vraagstelling en
aanpak**



02

**AVG en Wpg in het
kort**



03

**Bevindingen beleid
AVG en Wpg in
Papendrecht**



04

**Bevindingen
uitvoering AVG en
Wpg in
Papendrecht**



05

**Conclusie en
aanbevelingen
gemeenteraad en
college B&W**



Onderzoeksvraag

“Hoe wordt de privacy van de Papendrechtse inwoners beschermd en wordt er adequaat gebruik gemaakt van de AVG en Wpg, ook gelet op derden aan wie de uitvoering van beleid is uitbesteed, of met wie anderszins persoonsgegevens worden gedeeld?

En op welke wijze wordt de gemeenteraad in staat gesteld de privacybescherming periodiek te controleren?”

Onderzoeksaanpak



PBLQ

- ▶ **Startbijeenkomst** met vertegenwoordigers van de ambtelijke organisatie om het onderzoek toe te lichten en praktisch zaken te bespreken
- ▶ **Documentstudie m.b.t. bescherming van persoonsgegevens op papier** zoals het privacybeleid, raadsstukken en -vragen, klachten, register van verwerkingen, verwerkersovereenkomsten met andere organisaties etc.
- ▶ **Interviews** met sleutelpersonen zoals de FG, CISO, portefeuillehouder, gemeentesecretaris, vertegenwoordiger van de OR, medewerkers uit sociaal domein en Wpg-domein (BOA's)
- ▶ **Sessie met de raad** aan de hand van een fictieve casus over de rol van de raad (controlerend, sturend, kaderstellend) ten aanzien van de bescherming van persoonsgegevens
- ▶ **Workshop** in de vorm van een mini-PIA met toezicht en handhaving mbt de Wpg, waarbij heel concreet gekeken is hoe in de praktijk wordt gewerkt
- ▶ **Convergentiesessie met medewerkers van de organisatie** om concept bevindingen te bespreken: meer inzicht en meer draagvlak
- ▶ **Ambtelijk wederhoor** schriftelijk en in een mondeling gesprek met de ambtelijke organisatie voor wederzijds begrip en draagvlak
- ▶ **Bestuurlijk wederhoor:** zie de stukken voor deze vergadering
- ▶ **Onderzoekperiode:** maart t/m juni, wederhoor in de zomerperiode

AVG en Wpg op hoofdlijnen

AVG op hoofdlijnen

- ▶ Europese regelgeving die rechtstreeks werkt, van toepassing sinds 2018
- ▶ Doel = bescherming persoonsgegevens: gemeente mag alleen persoonsgegevens van burgers verzamelen en gebruiken wanneer daar een belang mee is gemoeid dat dit in voldoende mate rechtvaardigt. Gegevens mogen bovendien niet zomaar voor een ander doel worden gebruikt dan waarvoor ze in eerste instantie zijn verzameld.
- ▶ De belangrijkste verplichtingen voor een gemeente zijn:
 - Werken cf Privacy by Design: bij het bedenken van een proces of dienst al zorgen dat persoonsgegevens goed worden beschermd en niet meer wordt verwerkt of langer bewaard dan nodig
 - Functionaris Gegevensbescherming. Privacy Officer is strikt genomen niet verplicht, wel zeer aanbevolen
 - Data Protection Impact Assessment (DPIA): voor nieuwe verwerking van persoonsgegevens vooraf privacyrisico's in kaart brengen en maatregelen nemen om deze te mitigeren.
 - Register van verwerkingen volledig en op orde hebben
 - Adequate informatiebeveiliging ter bescherming van persoonsgegevens (technische en organisatorische maatregelen)
 - Burgers voldoende toegankelijk en begrijpelijk informeren over hun rechten ogv de AVG (zoals inzage en correctie), en over wat de gemeente precies doet met hun persoonsgegevens
 - Als taken worden uitgevoerd door andere organisatie dan gemeente zelf: zorgen dat ook deze organisatie zorgvuldig omgaat met persoonsgegevens, bijvoorbeeld door het sluiten van een verwerkersovereenkomst

Wpg op hoofdlijnen

- ▶ Specifieke regels voor verwerking van politiegegevens: persoonsgegevens die worden verwerkt bij het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten
- ▶ Voor gemeenten van toepassing op het werk van de bijzonder opsporingsambtenaren (BOA's), zoals wanneer deze een boete geven
- ▶ Overlapt inhoudelijk voor een groot deel met de AVG
- ▶ Maar meer is expliciet wettelijk bepaald, zoals wie verantwoordelijk is voor verwerking gegevens en hoe lang je ze mag bewaren
- ▶ Aanvullende verplichtingen, zoals bijhouden wie welke gegevens gebruikt (logging)
- ▶ Leent zich goed voor automatisering, belangrijkste middel om te voldoen is beschikken over software die aan de Wpg voldoet en deze op de juiste manier gebruiken
- ▶ Verplicht uitvoeren periodieke audit (1x per jaar intern, 1x per 4 jaar extern)

Voor AVG en Wpg geldt: voldoen = aantoonbaar voldoen!

Wat kan er gebeuren wanneer je niet aantoonbaar voldoet?

AP intensificeert toezicht op Eindhoven

17 november 2023

Boete van 30.000 euro voor gemeente Voorschoten

Zorgen over intern toezicht gemeente Amsterdam

08 mei 2023 Thema: [Gemeenten](#)

De Autoriteit Persoonsgegevens (AP) heeft wethouders Van Buren (P&O) en Scholtes (ICT) gevraagd om namens het college van B en W van de gemeente Amsterdam naar de AP te komen om uitleg te geven over de positie van hun interne privacytoezichthouder. De AP maakt zich zorgen of de onafhankelijkheid van het interne toezicht bij de gemeente Amsterdam wel goed genoeg is geregeld.

PBLQ

Datalek gemeente Amsterdam: geheime lijst met namen van radicale moslims verstuurd

Boete gemeente Enschede om wifitracking

29 april 2021 Thema's: [Wifi en bluetooth](#), [Gemeenten](#)

De Autoriteit Persoonsgegevens (AP) geeft de gemeente Enschede een boete van 600.000 euro, omdat de gemeente wifitracking gebruikte in de

Datalek bij gemeente Den Bosch: inwoners ontvangt persoonsgegevens van 23.000 personen

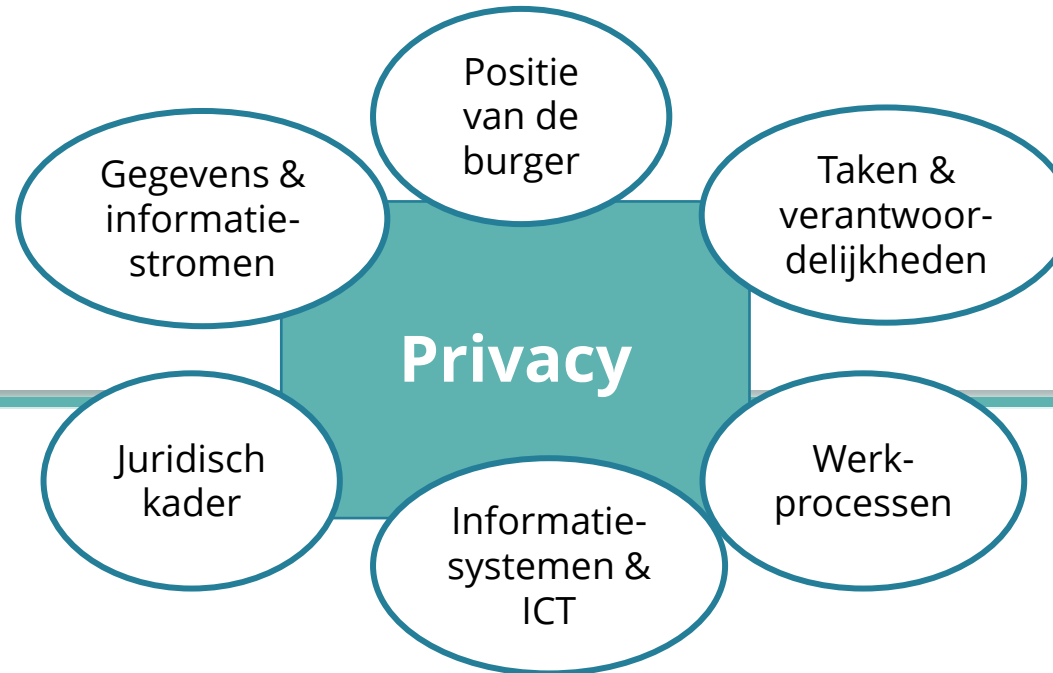
Bevindingen

Privacy is niet alleen een juridisch onderwerp



1. Privacy & privacybeleid

Balans tussen:
- Rechten van inwoners
- Taakuitoefening overheid



2. Meer dan een juridisch vraagstuk



3. Privacy is een gespreksonderwerp

Breed binnen de organisatie
& met ketenpartners

Beleid en werkprocessen AVG en Wpg in Papendrecht

- ▶ AVG-conform privacybeleid is aanwezig en vastgesteld door gemeenteraad
 - Nieuwe (concept)beleid voor Drechtsteden is een flinke verbetering t.o.v. geldende versie, bijvoorbeeld m.b.t. verdeling van taken en verantwoordelijkheden op het gebied van privacy en de mate waarin werkprocessen goed zijn uitgewerkt
 - Maar ook het geldende beleid is in principe genoeg om aan de AVG te kunnen voldoen
- ▶ Er is nog geen vastgesteld beleid voor Wpg
 - Er is wel concept-Wpg-beleid aanwezig, maar dit is nog niet vastgesteld of in de praktijk gebracht
- ▶ Er zijn vastgestelde werkprocessen voor omgang met rechten van betrokkenen (zoals recht op inzage)
- ▶ Privacyverklaring op de website is actueel en voldoet
- ▶ Raad ontvangt via ENSIA-rapportages en jaarstukken hoofdzakelijk procesmatige informatie over AVG en Wpg, maar weinig tot geen inhoudelijke informatie over eventuele risico's en genomen maatregelen

Uitvoering AVG in Papendrecht [1]

- ▶ Weinig klachten van inwoners (2 die ongegrond bleken), ook weinig verzoeken inwoners ovg hun rechten
- ▶ Weinig datalekken (3 tot 5 per jaar) in vergelijking met andere gemeenten, de lekken die er waren zijn cf geldende procedure afgehandeld
- ▶ Uitvoering taken door andere organisaties dan Papendrecht gedekt door eigen verwerkingsverantwoordelijkheid uitvoeringsorganisatie (igv gemeenschappelijke regeling zoals Drechtsteden) of verwerkersovereenkomst
- ▶ Samenwerking met FG sterk verbeterd
- ▶ (Na)scholing mbt AVG voor medewerkers wordt jaarlijks uitgevoerd in de vorm van een maand van de informatiebeveiliging en privacy obv vrijwillige deelname
- ▶ Medewerkers zijn goed op de hoogte van het privacybeleid en tonen zich betrokken en verantwoordelijk, ze zijn zich bewust van de noodzaak AVG-conform te handelen en doen daar ook hun best voor
- ▶ IB op orde

Uitvoering AVG in Papendrecht [2]

Maar ook:

- ▶ Serieuze achterstanden in uitvoering vereiste AVG-maatregelen door langdurig capaciteitsgebrek binnen de organisatie
 - Voor veel gegevensverwerkingen nog geen DPIA uitgevoerd, omgang met DPIA's bovendien niet altijd even correct
 - Achterstand bij uitvoering maatregelen uit FG-adviezen, betrokkenheid FG op een aantal punten nog *ad hoc*
 - Nog geen functionerende Plan-Do-Check-Act-cyclus op het gebied van bescherming van persoonsgegevens (niet rechtstreeks verplicht o.g.v. de AVG, maar wel aanbevolen manier van werken)
- ▶ Nascholing medewerkers gemeente is weinig functiespecifiek, alleen obv vrijwilligheid en is onvoldoende geïntegreerd in reguliere werkprocessen medewerkers
- ▶ Bescherming persoonsgegevens door verwerkers namens gemeente wordt niet verder in de gaten gehouden
- ▶ Weinig actieve informatieverstrekking aan inwoners Papendrecht over hun rechten / verwerking van hun gegevens
- ▶ Verbetertraject is ingezet en heeft voorzichtig resultaat, maar nog niet mogelijk om vast te stellen wanneer hiermee wel aan AVG voldaan wordt

Uitvoering Wpg in Papendrecht

- ▶ In externe audit begin 2022 is geconstateerd dat door BOA's gebruikte software niet voldoet aan Wpg
- ▶ Dit was t.t.v. ons onderzoek nog niet opgelost omdat nieuwe software nog niet was uitgerold
 - Inkooptraject nieuwe software duurde erg lang, zowel t.g.v. het inkoopproces zelf als vertraging rond uitvoering DPIA
 - Nieuwe software is inmiddels wel ingekocht en voldoet aan Wpg, deze zou nu operationeel moeten zijn (beoogde datum uitrol was tweede helft 2024)
 - Overstap op nieuwe software leverde risico op dat gegevens die in oude software stonden zouden verdwijnen, wij hebben in ons onderzoek niet vastgesteld of dit in voldoende mate is opgelost
- ▶ Daarom waren in de tussentijd ook geen aanvullende interne Wpg-audits uitgevoerd, want zonder nieuwe software was het voor Papendrecht sowieso niet mogelijk om aan de Wpg te voldoen
- ▶ Inzet is nu om bij volgende interne Wpg-audit wel te kunnen voldoen

Conclusies en aanbevelingen

Conclusies

- ▶ Privacybeleid voldoet aan AVG, maar wordt wel beter wanneer het nieuwe beleid wordt vastgesteld
- ▶ In de praktijk wordt niet altijd aantoonbaar volgens dit beleid gewerkt en zijn er achterstanden in de uitvoering, vooral mbt DPIA's. Ook worden aanbevolen / afgesproken verbetermaatregelen niet altijd of pas na langere tijd opgevolgd.
- ▶ Voor Wpg voldoen zowel beleid als uitvoering niet, zoals in 2022 is vastgesteld. De gemeente heeft de nodige verbeteringen in gang gezet om tijdens de volgende audit wel te voldoen, waarvan de belangrijkste een nieuw informatiesysteem en het Wpg-beleid zijn.
- ▶ Er is beperkte betrokkenheid van de gemeenteraad bij het onderwerp. De gemeenteraad wordt met name op procesniveau geïnformeerd over privacy en gegevensbescherming en beschikt over onvoldoende informatie om adequaat te kunnen sturen en controleren.

Aanbevelingen aan de gemeenteraad

- 1 Neem een pro-actievere (kaderstellende) rol aan ten aanzien van de bescherming van persoonsgegevens en het privacy- en Wpg-beleid en besluit mee over strategische uitgangspunten en ambitieniveaus.
- 2 Zorg voor een betere informatiepositie door het beleid en de verbeteringen van de gemeente periodiek te beoordelen.
- 3 Spreek minimaal jaarlijks over privacy (AVG én Wpg).

Aanbevelingen aan het college van B&W

1	Zet de reeds ingezette verbeteringen, waaronder het nieuwe privacy- en Wpg-beleid en het inlopen van de achterstand bij de uitvoering zoals m.b.t. DPIA's, onverminderd door. Zorg daarbij voor voldoende capaciteit.
2	Zorg voor een periodieke rapportage over de voortgang met betrekking tot het privacy- en Wpg-beleid, de uitvoering van DPIA's en het opvolgen van FG-adviezen, en stuur bij waar nodig.
3	Beoordeel en evalueer het privacy- en Wpg-beleid jaarlijks en leg de resultaten hiervan vast.
4	Besteed meer aandacht aan de bescherming van persoonsgegevens bij gemeenschappelijke regelingen, samenwerkingspartners of verwerkers in de praktijk door afspraken en waarborgen uit verwerkersovereenkomsten periodiek te toetsen door middel van rapportage of onderzoeken.