

Toezicht Algemene Verordening Gegevensbescherming 2022

V_20230401

Inleiding en samenvatting

De Functionaris gegevensbescherming (FG) rapporteert in dit verslag over het uitgevoerde toezicht op de Algemene Verordening Gegevensbescherming (AVG) in 2022. De AVG zorgt voor een verhoogde aandacht voor een rechtmatige en zorgvuldige verwerking van persoonsgegevens in alle domeinen. Voor de bescherming van persoonsgegevens door BOA's die opsporingstaken doen is sinds 2019 een speciale privacywet; de Wet politiegegevens (Wpg) .

Het college van Burgemeester en Wethouders (college) is verantwoordelijk voor het merendeel van de verwerkingen van persoonsgegevens in onze gemeente. Daarnaast zijn de gemeenteraad en de burgemeester verantwoordelijk voor een beperkt aantal verwerkingen. In de AVG en Wpg zijn zij de 'verwerkingsverantwoordelijke'. Deze verantwoordelijkheid brengt verplichtingen met zich mee. In dit rapport beoordeelt de FG als onafhankelijk toezichthouder in hoeverre de gemeente als verwerkingsverantwoordelijke aan de verplichtingen in het kader van de AVG voldoet¹. De Functionaris Gegevensbescherming (FG) adviseert daarbij – gevraagd en ongevraagd - over een juiste toepassing². Daarom noemt de FG in dit rapport de bevindingen, aandachtspunten en adviezen.

De FG rapporteert in dit jaarverslag 2022 over:

1. AVG-Toezichtskalender 2022
2. De Wet Politiegegevens (Wpg)
3. Organisatorische inbedding privacy
4. Klacht en vraag inwoners
5. Rechten van betrokkenen
6. Datalekken
7. Data protection Impact Assessments (DPIA)
8. Register van verwerkingen

1. AVG-Toezichtskalender 2022

In de FG-jaarkalender 2022³ staan de volgende onderzoeken voor 2022:

Q1: Bevestigingen aan het Inlichtingenbureau door de gemeente. De Autoriteit Persoonsgegevens (AP) heeft in een brief aan de VNG kenbaar gemaakt de indruk te hebben dat gemeenten mogelijk teveel en te frequent persoonsgerelateerde informatie over (uitkeringsgerechtigde) inwoners uitvragen. De AP gaat hier streng op toezien.

Q2: Processen jeugd, met name informatieplicht naar betrokkenen en transparantie

Q3: Bewustzijn medewerkers m.b.t. datalekken

Q4: Privacy- volwassenheid organisatiebreed en AVG processen

¹ Artikel 39, lid 1 onder b AVG

² Artikel 39, lid 1, onder a AVG

³ B&W 1 maart 2022, DT 10 februari 2022

Onderzoeken Q3 en Q4 zijn niet uitgevoerd. Daarvoor had de FG door de extra inzet voor de gemeenten Staphorst, Meppel en Zwartewaterland geen capaciteit⁴. Voor onderzoek Q4 privacy-volwassenheid organisatiebreed en AVG-processen ontbreekt een actueel inzicht. Tot 2021 werd hiervoor het IBD/VNG-borginsgdocument gebruikt. Daar is van afgestapt, omdat de thema's door de organisatie niet worden herkend. Omdat er wel behoefte is om de mate van privacyvolwassenheid in beeld te hebben en de verplichte AVG-processen en -producten te monitoren is in 2022 besloten een bij de gemeente gebruikte managementtool voor informatiebeveiliging uit te breiden met een privacymanagementdeel. De invulling van dit privacymanagementdeel is nog niet gerealiseerd noch gepland.

Advies:

1. Privacymanagementtool te laten inrichten en gebruiken voor een overzicht van de privacy-volwassenheid van de organisatie en de verplichte AVG- processen en - producten.

Reactie DT: Opnemen in Jaarplan privacy, informatiebeveiliging en informatiebeheer voor 2024.

Q1 Bevragingen Inlichtingenbureau

De FG heeft geoordeeld dat de gemeente Steenwijkerland voldoende maatregelen heeft getroffen om bij de bevragingen aan het Inlichtingenbureau (IB) te kunnen voldoen aan de AVG.

Q2 Transparantie in jeugdprocessen

De FG ziet dat binnen de jeugdprocessen nog onvoldoende opzet aanwezig is om te kunnen voldoen aan de AVG-beginselen van informatieplicht en transparantie en doet aanbevelingen, waaronder:

- Privacyverklaring over gegevensverwerkingen in jeugdprocessen
- In werkprocessen/werkinstructie vastleggen hoe en dat betrokkenen tijdig worden geïnformeerd over het verwerken van persoonsgegevens en de AVG-rechten

Deze aanbevelingen zijn door het Team Sociaal Domein overgenomen.

2. De FG en de Wet politiegegevens

Per 1 januari 2019 is de Wet Politiegegevens (Wpg) in werking getreden. In de Wpg is voor werkgevers van BOA's die opsporingstaken verrichten de verplichting opgenomen om elk jaar een interne audit te doen en één keer in de vier jaar een externe audit en de resultaten van de externe audit te delen met de Autoriteit Persoonsgegevens (AP). In 2022 heeft de gemeente Steenwijkerland de externe Wpg-audit laten doen en daarop een verbeterplan gemaakt. Dit wordt nu uitgevoerd en in 2023 geheraudit. Uit de audit blijkt o.a. dat voor de Wpg ook een FG moet worden aangesteld, die elk jaar een verslag met bevindingen opstelt over de naleving van de Wpg , deze deelt met de gemeente en een verplichte adviesrol heeft bij de Wpg-DPIA's. De huidige AVG-FG kan dit doen. Ze is ook nog niet aangewezen als FG voor de AVG.

Advies:

2. Voor het verplichte toezicht uit de Wet politiegegevens (Wpg) en de AVG de huidige AVG-FG aan te laten wijzen en hiervoor aanwijzingsbesluiten voor te leggen aan het college en de burgemeester.

4 Vanaf 2018 hadden de gemeenten Staphorst, Steenwijkerland, Westerveld en Zwartewaterland een samenwerking voor twee FG's. Na vertrek van de tweede FG medio 2021 is de FG van Steenwijkerland ingezet voor de vier gemeenten en Meppel kwam daar tijdelijk bij. Deze samenwerking met Staphorst en Zwartewaterland is in september 2022 beëindigd.

Reactie DT: de aanwijzingsbesluiten FG voor de AVG en FG voor de Wpg voorleggen aan het college respectievelijk de burgemeester.

3. Organisatorische inbedding privacy

Voor een goede en juiste uitvoering van de AVG is het van belang dat eenieder binnen de organisatie op de hoogte is van wie welke taken, verantwoordelijkheden en bevoegdheden heeft. Eind 2022 is de organisatorische inbedding van privacy en informatieveiligheid binnen de gemeente opnieuw vastgelegd in een nieuwe privacygovernance⁵. Deze privacy governance verbetert het eigenaarschap over privacy en informatieveiligheid en legt dit bij het management: Elke leidinggevende (eerste lijn) is ervoor verantwoordelijk om de privacymaatregelen binnen diens eenheid te implementeren. Hierbij worden ze ondersteund door I-adviseurs.

In de nieuwe privacygovernance zijn ook de taken, verantwoordelijkheden en bevoegdheden binnen het privacyteam nader geduid. De privacy officer en Chief Information Security Officer (CISO) adviseren de organisatie als de tweede lijn. Zij rapporteren hierover separaat met een jaarplan, auditplan en verslag. De FG richt zich met name op toezicht in de derde lijn en maakt elk jaar een toezichtsplan en een verslag.

4. Klacht en vraag inwoners

De AVG verplicht gemeenten om de contactgegevens van de FG te publiceren zodat betrokkenen contact kunnen opnemen met deze functionaris. In 2022 hebben twee personen van deze mogelijkheid gebruik gemaakt. Er is een klacht en een vraag over de AVG door de FG onderzocht en afgehandeld. De klacht was dat een medewerker van de gemeente persoonlijke gegevens van betrokkene onterecht zou hebben gedeeld met een externe overheidsinstantie. De FG heeft geoordeeld dat de klacht terecht is. De onbevoegde ontvangende instantie is verzocht de gegevensdeling als niet verzonden te beschouwen. De FG heeft dit met de teamleider van de medewerker besproken, waarop de teamleider de casus binnen het team (anoniem) heeft besproken. De vraag kwam van een burger met een geheim adres, niet wonend in Steenwijkerland. De vraag was waarom er binnen de gemeentelijke organisatie van Steenwijkerland een bevraging is gedaan naar diens erkend geheime adres. Dit was een automatische bevraging bij het archiveren van een ouder dossier.

5. Rechten van betrokkenen

De burger heeft op basis van de AVG verschillende rechten om controle te houden over diens persoonsgegevens. Dit worden de rechten van betrokkenen genoemd. De gemeente moet deze verzoeken als verwerkingsverantwoordelijke afhandelen. Jaarlijks worden in Steenwijkerland ongeveer acht inzageverzoeken behandeld. Er is één AVG-inzage verzoek geweest in 2022. Binnen het sociaal domein waren vier tot acht inzageverzoeken vanuit de Jeugdwet (JW) en Wet Maatschappelijke Ondersteuning (WMO). Het kan onduidelijk zijn wat de relevante wet is voor een inzageverzoek: AVG, JW, WMO of Participatiewet. In 2022 is afgesproken een eenduidige afdoening bevorderen. De privacy officer wordt betrokken bij inzageverzoeken in het sociaal domein en bespreekt deze met de behandelaar binnen het sociaal domein.

⁵ DT 22-12-2022

6. Datalekken 2022

Er zijn in 2022 13 incidenten intern gemeld, waarvan 12 datalekken; geen ervan is gemeld aan Autoriteit Persoonsgegevens, omdat deze niet dermate risicovol waren, en vier zijn gemeld aan betrokkenen. Dit zijn minder datalekken dan voorgaande jaren en bij vergelijkbare gemeenten. De meeste komen door verkeerde adressering per post of mail. Dit kan vervelend zijn voor de betrokkenen, zeker als het gaat om gevoelige informatie of kwetsbare personen. Daarom is het belangrijk dat medewerkers ook in 2023 gewezen worden op de risico's bij het versturen van persoonsgegevens.

Overzicht datalekken 2022		
Onderwerp	Oorzaak	Maatregelen
1. Geen anonimiseren van emailadressen en telefoonnummers van bezwaarmakers documenten	Vergeten Onveilig menselijk handelen, onzorgvuldig	Betrokkene is in kennis gesteld Eenmalige fout: Normaal gesproken worden de documenten juist geanonimiseerd
2. Ongegronde gegevensdeling over een persoon met externe instantie	Onbewust dat deze informatie niet gedeeld mocht worden	Externe instantie is verzocht de informatie niet te gebruiken Anoniem besproken binnen het team om de bewustwording te vergroten en herhaling te voorkomen Melden aan betrokkene
3. Foutieve koppeling in het zaakstelsel van een verkeerde persoon aan een zaak	Onbewust onveilig handelen	Document is aan de juiste zaak toegevoegd Melder is geïnformeerd
4. Werkmap vergeten mee te nemen met naam en contactgegevens organisatie evenement	Onzorgvuldig	Map is geplaatst op verlorenofgevonden.nl, maar is niet terecht gekomen
5, 6, 7, 8, 9 onjuist email adres verzonden	5. Onjuist emailadres in mail en formulier gebruikt 6. Onjuist emailadres 7 en 8. automatische verkeerde aanvulling e-mail-adres 9 in thuiswerkomgeving werkt internet blijkbaar niet optimaal	5 en 7. Correctieverzoek met tweede mail. Ontvanger heeft bevestigd de mail te verwijderen 6 en 8 Onjuiste ontvanger deed zelf melding en heeft de mail verwijderd 9. Telefonisch contact met onbevoegde ontvanger om mail te verwijderen

10. Per abuis naam opgenomen in openbaar document over aangevraagde vergunningen boven € 30.000	Onbewust	Betrokkene is geïnformeerd Redactionele wijziging in het document binnen anderhalve week In het vervolg zal de kolom "aanvrager" niet worden opgenomen
11. Verkeerde persoonsgegevens doorgegeven aan een externe	Onzorgvuldigheid door werkproces: twee zaken tegelijk	Externe heeft de gegevens verwijderd na een verzoek daartoe van de gemeente
12. Verkeerd adres van betrokkene in systeem ingevuld	Kan niet worden gereset door beperkingen in software	Betrokkene is geïnformeerd Afhandeling gaat via de mail

Aandachtspunt:

- Bij het onderzoek ook kijken naar achterliggende oorzaken waardoor er onzorgvuldig of onbewust gehandeld is zodat ook meer structurele maatregelen kunnen worden genomen. Bijvoorbeeld: kennisachterstand - wist betrokkene het niet - of is de werkdruk (te) hoog?

Advies:

3. Bij het onderzoek naar incidenten en datalekken verder na te laten gaan wat de achterliggende oorzaak is van het onzorgvuldig of onbewust handelen.

Reactie DT:

In het Jaarplan privacy, informatiebeveiliging en informatiebeheer 2023 is opgenomen dat datalekken/beveiligingsincidenten op leer- en verbeterpunten worden geanalyseerd.

7. Data Protection Impact Assessment (DPIA)

De gemeente is in bepaalde gevallen verplicht een gegevensbeschermingseffectbeoordeling (ook wel DPIA: data protection impact assessment genoemd) uit te voeren. Dat geldt voor verwerkingen van persoonsgegevens met een hoog risico. Met een DPIA scant de gemeente de privacyrisico's en geeft maatregelen aan waarmee deze worden ondervangen. Hiermee wordt privacy onderdeel van de belangenafweging. Na het doorlopen van een DPIA dient het advies van de FG te worden ingewonnen.

In 2022 zijn drie DPIA's om advies voorgelegd aan de FG:

1. Digitaal internet rechercheren OOV (pilot)
2. Wet Inburgering
3. Drone toezicht handhaving

Dit zijn alle drie nieuwe op te starten verwerkingen/ontwikkelingen. Voor bestaande hoogrisicovolle verwerkingen moeten ook DPIA's worden gedaan. De planning daarvan is nu nog niet in beeld.

Aandachtspunten:

- In een organisatie met de grootte van Steenwijkerland is het niet aannemelijk dat drie DPIA's dekkend is voor de nieuwe verwerkingen met een hoog risico.

- Er moet inzichtelijk worden gemaakt op welke bestaande en op te starten verwerkingen DPIA's moeten worden gedaan en wat hiervan de planning is.

Advies:

4. Laat een overzicht met DPIA's voor 2023 e.v. opstellen aan de hand van een risicoclassificatie van de verwerkingen.

Reactie DT: Opnemen in Jaarplan privacy, informatiebeveiliging en informatiebeheer voor 2024.

8. Register van verwerkingen

Werkprocessen waarin persoonsgegevens worden verwerkt moeten zijn vastgelegd in een Register. Het doel van dit register is inzicht hebben in de structurele verwerkingen van persoonsgegevens en de stromen van persoonsgegevens binnen de organisatie. In Steenwijkerland is het afgelopen jaar het Register van Verwerkingen opnieuw ingevuld en daarmee up to date. Dat is een heel mooie inhaalslag! Tijdens het onderzoek naar jeugdprocessen bleek echter dat het Register nog niet eenvoudig in te zien is en dat de informatie daarin nog niet door alle organisatieonderdelen actief wordt beheerd. Veel gemeenten hebben het Register gepubliceerd op hun website, zodat inwoners/relaties kunnen zien welke verwerkingen met persoonsgegevens de gemeente doet. In Steenwijkerland is dit nog niet zo.

Aandachtspunt:

- Publicatie van het Register van verwerkingen om betrokkenen inzicht te bieden in de verwerkingen van de gemeente. Dit doen wanneer het beheer geregeld is waarmee geborgd is dat het Register actueel is.

Advies:

5. Het beheer van het Register van Verwerkingen te laten beleggen binnen de organisatie zodat het up-to-date is en blijft.

Reactie DT: Het beheren en actualiseren van het Document Structuurplan/Register van verwerkingen is in het Jaarplan privacy, informatiebeveiliging en informatiebeheer 2023 belegd bij de teamleider I&A.