betrouwbaar

Zwolle

Jaarverslag functionaris voor gegevensbescherming 2024

Verslag voor de Gemeenteraad

Inhoudsopgave

Inleiding

De functionaris gegevensbescherming (FG) houdt toezicht op de naleving van wetgeving en beleid met betrekking tot de bescherming van persoonsgegevens. Daarnaast kan hij gevraagd en ongevraagd advies geven. Jaarlijks brengt hij verslag uit aan de verschillende bestuursorganen binnen de gemeente, zoals de Gemeenteraad. Voor u ligt het jaarverslag over 2024.

Waarover leest u in dit jaarverslag?

Wat zijn de wettelijke privacyvereisten?
Een verwerking van persoonsgegevens moet voldoen aan wettelijke vereisten. Deze worden in dit jaarverslag toegelicht.

Welke bijzonderheden waren er in 2024?
Dit jaarverslag gaat over de verwerkingen waarvoor de gemeenteraad verwerkingsverantwoordelijke is:

- Verwerken van persoonsgegevens van (burger)raadsleden en derden
- Publiceren van stukken op de website
- Streamen, opnemen en beschikbaar houden van beelden van raadsvergaderingen

Voor iedere verwerking worden bijzonderheden toegelicht.

Wat zijn belangrijke privacyontwikkelingen?
In dit jaarverslag geven wij achtergrond bij een aantal ontwikkelingen die van groot belang zijn voor de bescherming van persoonsgegevens.

Welk handelingsperspectief heeft de raad?
De gemeenteraad heeft een belangrijke rol bij het zorgen voor een informatieveilig en privacyvriendelijke gemeente. In dit jaarverslag geven we de raad een 'privacy toolkit' die kan helpen om die rol op een goede wijze te vervullen.

Wettelijk kader

Regels over de verwerking van persoonsgegevens zijn vastgelegd in de Algemene Verordening Persoonsgegevens (AVG). Sinds de komst van AVG in 2018 zijn de privacyregels overal in de Europese Unie gelijk. De AVG beschrijft waaraan organisaties die persoonsgegevens verwerken zich moeten houden. Personen van wie persoonsgegevens worden verwerkt hebben door de AVG meer rechten gekregen.

Algemene privacyvereisten

De gemeenteraad is verwerkingsverantwoordelijke voor verschillende verwerkingen van persoonsgegevens. De gemeenteraad is er daarmee voor verantwoordelijk dat die verwerkingen voldoen aan de vereisten van de AVG:

- Behoorlijkheid, rechtmatigheid en transparantie: de verwerking van persoonsgegevens moet een wettelijke grondslag hebben en voor betrokkenen moet helder zijn waarvoor hun persoonsgegevens worden verwerkt.
- Doelbinding: persoonsgegevens mogen alleen voor welbepaalde, legitieme en specifieke doelen gebruikt worden.
- Dataminimalisatie: het is niet toegestaan om meer persoonsgegevens te verwerken dan noodzakelijk.
- Juistheid: verwerkte persoonsgegevens moeten juist en actueel zijn.
- Opslagbeperking: persoonsgegevens mogen niet langer worden verwerkt dan noodzakelijk.
- Integriteit en vertrouwelijkheid: persoonsgegevens moeten beschermd zijn door passende beveiligingsmaatregelen.
- Verantwoording: een organisatie die persoonsgegevens verwerkt moet kunnen aantonen dat zij aan privacyregels voldoet.

Meldplicht datalekken

'Datalek' is de veelgebruikte term voor 'inbreuk in verband met persoonsgegevens'. De AVG geeft de volgende definitie: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.'

Een datalek moet gemeld worden bij de Autoriteit persoonsgegevens (AP) 'tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen' . Als de inbreuk een hoog risico vormt voor degene van wie gegevens zijn gelekt, dan moet deze betrokkene op de hoogte gesteld worden van het datalek.

Rechten betrokkenen

Een verwerkingsverantwoordelijke moet er voor zorgen dat de persoon van wie gegevens worden verwerkt (de betrokkene) een beroep kan doen op zijn privacyrechten: het recht op inzage, rectificatie, verwijdering, beperking van de verwerking, bezwaar en op overdraagbaarheid van de persoonsgegevens. Het doel van deze rechten is om betrokkenen in staat te stellen controle te houden over de verwerking van persoonsgegevens.

AVG- verzoeken kunnen worden ingediend via Mijn Loket, of per post of via e-mail. Op de afhandeling is de Algemene wet bestuursrecht (Awb) van toepassing. Een besluit om een verzoek in te willigen is dan ook een besluit in de zin van de Awb, waartegen bezwaar kan worden gemaakt.

Bijzonderheden verwerkingen raad 2024

Bijzonderheden kunnen te maken hebben met het wettelijke privacykader. Uit onderzoek kan bijvoorbeeld blijken dat een verwerking niet volledig aan de eisen voldoet. Daarnaast geldt een datalek of een ingediend AVG-verzoeken ook als een 'bijzonderheid'.

Verwerken gegevens (burger)raadsleden en derden

Het gaat hier voornamelijk over de verwerking van contactgegevens. Daarnaast houdt de griffie een overzicht bij van nevenfuncties van raadsleden en commissieleden.

In 2024 is een datalek ontstaan bij het informeren van geïnteresseerden over de raadsagenda. De aankondiging van de agenda werd per mail verstuurd naar medewerkers van Zwolle, inwoners, zakelijke relaties en fractieleden. De adressen van betrokkenen stonden zichtbaar in de e-mail. Dit datalek is gemeld bij de Autoriteit Persoonsgegevens. Ook zijn betrokkenen geïnformeerd.

Publiceren van stukken op internet

Uitgangspunt bij de publicatie van (beleidsstukken) is dat persoonsgegevens niet mogen worden gepubliceerd, tenzij er sprake is van medewerkers die vanuit hun functie in de openbaarheid treden. Dit betekent dat bijvoorbeeld de naam van een gemeenteraadslid of een wethouder wél openbaar mag worden, maar de naam van een informant uit de ambtelijke organisatie niet. Voor ingekomen brieven en e-mails van inwoners geldt dat anonimiseren het beleidsuitgangspunt is.

In 2024 hebben zich geen bijzonderheden voorgedaan.

Verwerken beelden raadsvergadering

Het live uitzenden van raadsvergaderingen is gericht op de toegankelijkheid en openbaarheid en transparantie van de gemeenteraad. Dit zijn belangrijke doelen. Tegelijkertijd moet wel de bescherming van persoonsgegevens van betrokkenen in ogenschouw gehouden worden. Het is noodzakelijk is dat betrokkenen vooraf geïnformeerd worden over de opnames en het live uitzenden.

Naar aanleiding van signalen vanuit de raad over het gebruik van cookies en trackers op de website met raadsinformatie heeft de betreffende IT-leverancier in 2024 aanvullende informatie opgesteld in de vorm van een privacy- en cookieverklaring. Deze verklaringen voldoen nog niet volledig aan wettelijke vereisten. De leverancier is opnieuw benaderd met het verzoek om noodzakelijke verbeteringen door te voeren.

Actuele ontwikkelingen

Maatschappelijke en technologische ontwikkelingen hebben grote impact op de bescherming van persoonsgegvens. In dit hoofdstuk lichten we twee belangrijke ontwikklingen toe: Artificial intelligence en Cyber security.

Artificial intelligence (AI)

Sinds de komst van ChatGPT in 2022 is AI in het middelpunt van de publieke belangstelling komen te staan. Naast taalmodellen zoals ChatGPT en CoPilot zijn ook verschillende systemen beschikbaar gekomen om gemakkelijk beelden te creëren of te manipuleren. Dit heeft geleid tot veel optimisme over de mogelijkheden van kunstmatige intelligentie, maar ook tot minstens evenveel zorgen over de risico's van deze nieuwe technologie voor de mens.

Vanaf 2018 heeft de Europese Commissie een voorstel voor het reguleren van AI in voorbereiding. Doel hiervan was het versterken van de positie van de EU bij de ontwikkeling van AI én het zorgdragen dat AI ten dienste van de mens en de samenleving komt. Op 1 augustus 2024 is het uiteindelijke commissievoorstel in werking getreden: de AI-verordening.

De AI-verordening maakt onderscheid tussen verschillende risiconiveaus voor AI-systemen en geeft dwingende voorschriften voor elk van deze niveaus. Systemen met een onacceptabel risico zijn verboden, voor systemen met een hoog of beperkt risico gelden voorwaarden, en systemen met een minimaal risico worden niet gereguleerd. Voor zogenaamde 'general purpose AI', zoals ChatGPT en CoPilot, zijn afzonderlijke regels vastgesteld. De AI-act geldt overigens niet alleen voor aanbieders van AI, maar ook voor importeurs en distributeurs, organisaties die AI gebruiken en voor fabrikanten die AI in hun producten gebruiken.

De bepalingen van de AI-verordening zijn niet allemaal direct van toepassing. Vanaf februari 2025 zijn verschillende AI-systemen, zoals systemen die mensen manipuleren of misleiden, verboden. Ook zijn werkgevers verplicht om medewerkers AI-geletterd te maken, zodat iedereen gelijkelijk kan profiteren van de mogelijkheden van AI. In augustus 2025 zullen eisen voor 'general purpose AI' in werking treden. Vanaf 2026 zullen stapsgewijs ook de regels voor AI-systemen met een hoog risico van toepassing worden.

Cybersecurity

Onze grote afhankelijkheid van IT en de toename van cyberrisico's vragen om een hoog niveau van informatiebeveiliging. De snelle ontwikkeling van AI en van superkrachtige computers maakt dat de uitdagingen voor informatiebeveiligers groter zijn dan ooit. Organisaties moeten kunnen inspelen op snelle technologische ontwikkelingen. Dit vraagt om voldoende specialistische kennis én volwassen risicomanagement.

De Europese Raad heeft in 2022 de NIS2-richtlijn vastgesteld. Met deze richtlijn worden EU-lidstaten gedwongen om op vergelijkbare wijze informatiebeveiligingswetgeving te implementeren. Binnen Nederland gebeurt dit met de Cyberbeveiligingswet die naar verwachting in 2025 in werking zal treden.

Voor gemeenten betekent dit dat zij een wettelijke zorgplicht krijgen voor digitale veiligheid. Gemeenten worden verplicht om te voldoen aan de Baseline Informatiebeveiliging Overheid 2 (BIO2). Deze norm is vooral gericht op de organisatie van informatiebeveiliging en op goed functionerend risicomanagement. Daarnaast schrijft de norm een aantal specifieke overheidsmaatregelen voor.

Privacy toolkit voor de raad

Hulpmiddelen en checklists

De Autoriteit Persoonsgegevens publiceerde in 2023 een drietal brochures voor raadsleden over de bescherming van persoonsgegevens:

- gemeenten_en_privacy_-_wat_kun_u_als_raadslid_doen_-.pdf
- gemeenten_en_privacy_-_inzet_van_technologie.pdf
- gemeenten_en_privacy_-_samenwerkingsverbanden.pdf

De VNG publiceerde in 2023 een checklist waarin werd toegelicht wat raadsleden kunnen doen om de digitale weerbaarheid van de gemeente te versterken:

- checklist-raadsleden-digitale-veiligheid.pdf

In 2024 verscheen een publicatie van de Nederlandse Vereniging voor Raadsleden over de rol van raad bij informatieveiligheid binnen de gemeente:

- De raad als sleutelbewaarder van de digitale voordeur | Nederlandse Vereniging voor Raadsleden

De FG en de gemeenteraad

De FG is niet alleen toezichthouder, maar ook adviseur met betrekking tot persoonsgegevens. Dit betekent dat de raad de FG kan benaderen met vragen over de bescherming van persoonsgegevens.