

Privacyreglement Veiligheidsregio Noord- en Oost-Gelderland

De Veiligheidsregio Noord- en Oost-Gelderland (VNOG) werkt elke dag aan de veiligheid en gezondheid van inwoners. Daarbij worden ook persoonsgegevens verwerkt, zowel in de brandweer- en crisistaken, als in de interne bedrijfsvoering. Privacy speelt een belangrijke rol in de relatie tussen de burger, bedrijven en de overheid. In dit reglement leggen wij daarom uit hoe de VNOG omgaat met persoonsgegevens en hoe wij de privacy van medewerkers, vrijwilligers, ketenpartners en burgers beschermen.

De VNOG heeft de verantwoordelijkheid over persoonsgegevens en gegevensuitwisseling op alle terreinen waar ze actief is. De VNOG is verplicht om zorgvuldig en veilig, proportioneel en vertrouwelijk om te gaan met de persoonsgegevens van alle betrokkenen. Het beschermen van de privacy is complex, en wordt steeds complexer door technologische ontwikkelingen, grote uitdagingen op het terrein van veiligheid en (nieuwe) Europese wetgeving. Wij vinden het belangrijk om transparant te zijn over de manier waarop wij met persoonsgegevens omgaan, en de privacy waarborgen, zodat voor alle betrokkenen helder is wat van de VNOG verwacht kan worden.

Dit reglement is daarom relevant voor iedereen die met de VNOG te maken heeft. Wij willen hiermee inzicht geven in de rechten, plichten en waarborgen rondom privacy bij de VNOG, en laten zien hoe wij zorgvuldig met uw persoonsgegevens omgaan.

1. Wetgeving en definities

In dit reglement worden begrippen uit de Algemene Verordening Gegevensbescherming (AVG), gebruikt. De AVG zorgt onder andere voor versterking en uitbreiding van de privacy-rechten met meer verantwoordelijkheden voor organisaties.

Hieronder worden de belangrijkste begrippen uit de AVG versimpeld uitgelicht:

Betrokkene

De persoon op wie de persoonsgegevens betrekking hebben. De betrokkene is degene van wie de gegevens worden verwerkt.

Verwerker

De persoon of organisatie die de persoonsgegevens verwerkt in opdracht van een andere persoon of organisatie.

Persoonsgegevens

Alle gegevens die gaan over mensen en waaraan je een mens als individu kunt herkennen. Het gaat hierbij niet alleen om vertrouwelijke gegevens, zoals over iemands gezondheid, maar om ieder gegeven dat te herleiden is tot een bepaald persoon (bijvoorbeeld; naam, adres, geboortedatum, telefoonnummer of het Burgerservicenummer (BSN)). Naast gewone persoonsgegevens kent de AVG ook bijzondere persoonsgegevens. Dit zijn gegevens die gaan over gevoelige onderwerpen, zoals etnische achtergrond, politieke voorkeuren, gezondheidsgegevens of biometrische gegevens (vingerafdruk, gezichtsherkenning).

Verwerkingsverantwoordelijke

Een persoon of instantie die alleen, of samen met een ander, het doel en de middelen voor de verwerking van persoonsgegevens vaststelt.

Verwerking

Een verwerking is alles wat met een persoonsgegeven gedaan wordt, zoals bijvoorbeeld: vastleggen, bewaren, verzamelen, bij elkaar voegen, verstrekken aan derden en vernietigen.

2. Reikwijdte

Het reglement is van toepassing op alle verwerkingen van persoonsgegevens in relatie tot alle verwerkingsprocessen die binnen de VNOG plaatsvinden. Dit betreft verwerkingen bij:

- Uitvoering van wettelijke taken (brandweezorg, crisisbeheersing, GHOR)
- Bedrijfsvoering (HR, inkoop, ICT, planning & control)

- Samenwerking met gemeenten, ketenpartners en andere hulpdiensten
- Communicatie, voorlichting en publiekscontacten

Het reglement is van toepassing op medewerkers, vrijwilligers, stagiairs, leveranciers, ketenpartners, inwoners en andere mogelijke betrokkenen.

3. Verantwoordelijke

De bestuursorganen van de VNOG zijn allen verantwoordelijken voor de verwerkingen die door of namens de VNOG worden uitgevoerd. De bestuursorganen van de VNOG zijn onder andere de Voorzitter van de Veiligheidsregio, het Dagelijks Bestuur en het Algemeen Bestuur.

4. Toepassing van de AVG

Rechtmatige grondslag (Artikel 6, AVG)

De AVG verplicht dat er voor elke verwerking van persoonsgegevens een rechtmatige grondslag moet zijn.

Dat betekent dat de verwerking alleen mag plaatsvinden:

- Wanneer de betrokkene toestemming heeft gegeven voor de specifieke verwerking. Zoals bijvoorbeeld het ontvangen van de nieuwsbrief van de VNOG. Hierbij kan ten allen tijde de toestemming ingetrokken worden.
- Om een verplichting na te komen die in de wet staat. Hierbij kan gedacht worden aan het bijhouden van een financiële administratie, bijvoorbeeld bij het gebruik van dienstauto's.
- Voor de uitvoering van een overeenkomst waar de betrokkene onderdeel van is of was. Dit kan bijvoorbeeld wanneer VNOG een instructeur inhuurt.
- Wanneer dit nodig is voor het uitvoeren van een taak van algemeen belang. Zoals bijvoorbeeld bij crisisbeheersing of brandweerbijstand.
- Vanuit het gerechtvaardigd belang van VNOG. Denk hierbij aan cameratoezicht op locaties om de eigendommen van VNOG te beschermen.

Het Algemeen Bestuur van de VNOG heeft op 24 maart 2022 het gegevensbeschermingsbeleid vastgesteld. Deze en het daaruit voortvloeiende implementatieplan stellen dat onze medewerkers er voor moeten zorgen dat er zorgvuldig met persoonsgegevens omgegaan wordt. Hoe onze medewerkers dit dienen te doen staat ook omschreven in onze interne privacyhandleiding, die elke medewerker dient te lezen.

Persoonsgegevens worden alleen verwerkt door personen met een geheimhoudingsplicht. Daarnaast beveiligd de VNOG alle persoonsgegevens. Dit moet voorkomen dat de persoonsgegevens kunnen worden ingezien of gewijzigd door iemand die daar geen recht toe heeft. De VNOG volgt hiervoor de Baseline Informatiebeveiliging Overheid (BIO). Daarnaast heeft de VNOG ook een informatiebeveiligingsbeleid waarin aanvullende maatregelen zoals encryptie en toegangsbeveiliging zijn uitgewerkt.

Doorgifte (Artikelen 44 t/m 50, AVG)

De VNOG geeft geen persoonsgegevens door aan een land buiten de Europese Economische Ruimte (EER) of aan een internationale organisatie. Let wel, dit laat onverlet dat een gegevensverwerker waarmee een verwerkersovereenkomst is afgesloten de persoonsgegevens door een land buiten de EER of een internationale organisatie laat passeren/opslaan. Dit betekent dus dat in sommige gevallen persoonsgegevens van betrokkenen die voor de VNOG verwerkt worden, wel buiten de EER opgeslagen worden.

5. Transparantie en communicatie

Wet Open Overheid

Via de Wet Open Overheid kan een verzoek om informatie worden ingediend bij de VNOG. Bij het verzoek bekijkt de VNOG altijd of het antwoord geen inbreuk maakt op de persoonlijke levenssfeer van betrokkenen. In principe worden geen persoonsgegevens verstrekt. Waar nodig worden deze verwijderd of weggestreept. Dit gebeurt ook bij informatie die de VNOG actief openbaar maakt.

Wet hergebruik van overheidsinformatie

De Wet hergebruik van overheidsinformatie regelt het op verzoek verstrekken van overheidsinformatie voor hergebruik. Burgers en bedrijven kunnen bij VNOG een verzoek doen om openbare

overheidsinformatie op een duidelijke manier aan te leveren. Bij het verzoek bekijkt de VNOG altijd of het antwoord geen inbreuk maakt op de persoonlijke levenssfeer van betrokkenen. Er worden geen persoonsgegevens verstrekt. Waar nodig worden deze verwijderd of weggestreept.

Informatieplicht (Artikelen 13 en 14, AVG)

Bij de afhandeling van incidenten is er logischerwijs geen tijd om toestemming te vragen voor verwerking van persoonsgegevens. De VNOG informeert betrokkenen over het verwerken van persoonsgegevens daarom via de privacyverklaring op de website en via dit privacyregelement.

Wanneer betrokkenen gegevens aan de VNOG geven, worden zij op de hoogte gesteld van de manier waarop de VNOG met hun persoonsgegevens om zal gaan. Dit kan bij het aanmelden voor een training bijvoorbeeld via een formulier gebeuren. Vaak staat op de aanvraagformulieren vermeld welke gegevens zonder toestemming niet openbaar gemaakt zullen worden.

De betrokkene wordt niet nogmaals geïnformeerd als hij/zij al weet dat de VNOG persoonsgegevens van hem/haar verzamelt en verwerkt, en weet waarom en voor welk doel dat gebeurt.

Wanneer de gegevens via een andere weg verkregen worden, dus buiten de betrokkene om, wordt de betrokkene geïnformeerd op het moment dat deze gegevens voor de eerste keer worden verwerkt.

Verwijdering

De VNOG bewaart de persoonsgegevens niet langer dan nodig is voor de uitvoering van wettelijke taken, of zoals vastgelegd in de Archiefwet. Wanneer er nog persoonsgegevens opgeslagen zijn die niet langer nodig zijn voor het bereiken van het doel worden deze zo snel mogelijk verwijderd. Dit houdt in dat deze gegevens vernietigd worden, of zo worden aangepast dat de informatie niet meer gebruikt kan worden om iemand te identificeren.

De VNOG hanteert voor de bewaartermijnen de [selectielijst](#) van de Vereniging van Nederlandse Gemeenten (VNG).

Rechten van betrokkenen (Artikelen 13 t/m 20, AVG)

De wet bepaalt niet alleen de plichten van degenen die de persoonsgegevens verwerken, maar bepaalt ook de rechten van de personen van wie de gegevens worden verwerkt.

Deze rechten worden ook wel de rechten van betrokkenen genoemd, en bestaan uit de volgende rechten:

- **Recht op informatie:** De betrokkene heeft het recht om aan de VNOG te vragen of diens persoonsgegevens worden verwerkt.
- **Inzagerecht:** Betrokkene heeft de mogelijkheid om te controleren of, en op welke manier, diens persoonsgegevens worden verwerkt.
- **Correctierecht:** Als duidelijk wordt dat de persoonsgegevens niet kloppen, kan de betrokkene een verzoek indienen bij de VNOG om de persoonsgegevens te corrigeren.
- **Recht van beperking van de verwerking:** Betrokkene heeft het recht aan VNOG te vragen om diens persoonsgegevens niet meer te gebruiken. Hierbij zijn de persoonsgegevens wel beschikbaar, maar wordt gevraagd om ze tijdelijk niet meer te gebruiken, bijvoorbeeld tijdens het afwachten op de beoordeling van een bezwaar. VNOG zal hieraan voldoen, tenzij wij duidelijk aan kunnen tonen dat deze verwerking wel nodig is.
- **Recht op gegevenswissing:** In gevallen waar de betrokkene toestemming heeft gegeven om persoonsgegevens te verwerken, heeft de betrokkene het recht om de persoonsgegevens te laten verwijderen. De VNOG zal hieraan voldoen, tenzij er gerechtvaardigde gronden zijn voor de verwerking.
- **Recht op bezwaar:** De betrokkene heeft het recht om bezwaar te maken tegen de verwerking van diens persoonsgegevens als deze verwerking is gebaseerd op het uitvoeren van een taak van algemeen belang of een gerechtvaardigd belang. De VNOG zal hieraan voldoen, tenzij er dwingende gerechtvaardigde gronden zijn voor de verwerking die zwaarder wegen dan de belangen van de betrokkene.

- Recht op overdraagbaarheid van gegevens: Als de verwerking is gebaseerd op toestemming of voor de uitvoering van een overeenkomst, dan heeft de betrokkene het recht aan VNOG te vragen om diens gegevens over te dragen aan andere organisaties. De betrokkene kan ook diens eigen persoonsgegevens opvragen bij VNOG zodat de betrokkene zelf informatie gemakkelijk kan overdragen aan andere organisaties.

Indienen van een verzoek

Om gebruik te maken van zijn/haar rechten kan de betrokkene een verzoek indienen.

Dit verzoek kan zowel

- a. via directe e-mail (privacy-security@vnog.nl) ingediend worden;
- b. schriftelijk (Veiligheidsregio Noord- en Oost-Gelderland, t.a.v. team Privacy, Postbus 234 7300 AE Apeldoorn).

De VNOG heeft op basis van artikel 12 AVG, derde lid, vier weken de tijd, vanaf de ontvangst van het verzoek, om te beoordelen of het verzoek gerechtvaardigd is. Wij sturen zo snel mogelijk een ontvangstbevestiging met verdere informatie over hoe wij het verzoek behandelen.

Als het verzoek niet wordt opgevolgd is er de mogelijkheid om bezwaar te maken bij de VNOG, of een klacht in te dienen bij de Autoriteit Persoonsgegevens (AP). Aan de hand van een verzoek kan de VNOG aanvullende informatie opvragen om zeker te zijn van de identiteit van betrokkene. Hierbij vraagt VNOG de aanvrager om zich op locatie of online te identificeren. Dit doen wij om er zeker van te zijn dat degene die het verzoek doet, ook daadwerkelijk degene is van wie de persoonsgegevens opgevraagd worden. Zo voorkomen wij dat persoonsgegevens met een verkeerd persoon gedeeld worden. Na identificatie verwijderen wij de identiteitsgegevens zo snel mogelijk.

6. Geautomatiseerde verwerkingen

Profilering (Artikel 22, AVG)

Profilering vindt plaats wanneer er een geautomatiseerde verwerking van persoonsgegevens plaatsvindt waarbij aan de hand van persoonsgegevens naar bepaalde persoonlijke aspecten van een persoon wordt gekeken om deze persoon te categoriseren en te analyseren, of om zaken te kunnen voorspellen.

VNOG maakt geen gebruik van profilering. Daarnaast neemt de VNOG ook geen besluiten die uitsluitend zijn gebaseerd op geautomatiseerde verwerking of profilering. Zoals hierboven aangegeven mag de VNOG wel bekijken hoe vaak een bepaalde dienst bekeken is. Dit is dan ook wat de op de website gekoppelde zogenaamde 'cookies' doen en waar de websitebezoeker op wordt gewezen. De VNOG gebruikt cookies alleen voor noodzakelijke en analytische doeleinden. Meer hierover kunt u terugvinden in de [cookieverklaring](#) op de website van VNOG.

Inzet van camera's

De VNOG heeft een wettelijke taak in het kader van de crisis- en rampbestrijding. In dat kader kan er vanuit de levensreddende noodzaak gebruik worden gemaakt van camera's terwijl er logischerwijs vooraf geen toestemming van de gefilmde personen kan worden gevraagd. Ondanks deze ruimere wettelijke bevoegdheid zal ook bij dit cameragebruik gelden dat de privacy-waARBorgen vanuit de AVG worden nageleefd.

Dit houdt in dat rekening wordt gehouden met:

- doelbeperking (alleen gebruiken voor wettelijke doeleinden)
- gegevensbeperking (niet meer gegevens verzamelen dan nodig is voor wettelijke doeleinden)
- bewaarbeperking (gegevens niet langer bewaren dan noodzakelijkerwijs of wettelijk is toegestaan)
- integriteit en vertrouwelijkheid (gegevens zijn alleen toegankelijk voor diegenen die deze gegevens nodig hebben voor verwerking en zijn beschermd tegen verlies en diefstal)
- rechten van betrokkenen (indien gegevens ongewenst zijn verwerkt kunnen ze worden verwijderd)

Mocht een gefilmde persoon bezwaren hebben tegen de gemaakte camerabeelden, dan kan deze een verzoek tot vernietiging indienen bij team Privacy van de VNOG via het e-mailadres (privacy-security@vnog.nl).

Binnen de VNOG wordt onder bepaalde omstandigheden aanvullend gebruik gemaakt van allerlei soorten camera's. Door de digitale ontwikkelingen is dit in dit reglement niet in een beperkte opsomming te omvatten. Maar bij elke van deze ingezette of nieuw in te zetten camera's zullen de hierboven genoemde privacy-waarborgen van de AVG worden nagelopen, beoordeeld en nageleefd.

Voor camera's bij gebouwen van VNOG geldt dat de beelden die hier gemaakt worden alleen teruggekeken worden als hier een aanleiding voor is, en dat dit altijd gebeurt met een vierogenprincipe.

Waar nodig zal er aanvullende regelgeving worden opgesteld, zodat de VNOG bij gebruik van een bepaalde camera ook aanvullende beperkingen, vereisten of afspraken vastlegt.

Datawarehouse

VNOG heeft voor de verbetering van haar dienstverlening een datawarehouse waarin vanuit verschillende applicaties data verzameld wordt om verbeterde inzichten te krijgen. Hierin kunnen persoonsgegevens verwerkt worden voor zover dit noodzakelijk is voor de uitvoering van de wettelijke taken van VNOG. Hieronder worden gegevens uit de personeelsadministratie verwerkt, maar hierin worden ook gegevens uit de meldkamersystemen, waaronder de kladblokregels van incidenten, verwerkt. Voor rapportages die gemaakt worden met gegevens uit het datawarehouse wordt voorafgaand een privacytoets doorlopen waarin de noodzaak en privacygevoeligheid van de rapportage wordt beoordeeld. Waar mogelijk worden gegevens geanonimiseerd of alleen als statistieken beoordeeld.

Toegang tot gegevens in het datawarehouse is beperkt tot medewerkers die deze nodig hebben voor de uitvoering van hun werkzaamheden. Passende technische en organisatorische maatregelen zijn getroffen om de vertrouwelijkheid en integriteit van de gegevens te waarborgen. Verder wordt bij een verzoek van rechten van betrokkenen ook het datawarehouse doorzocht op gegevens van de betrokkene en waar nodig te verwijderen.

7. Plichten van de Veiligheidsregio Noord- en Oost-Gelderland

Register van verwerkingen (Artikel 30, AVG)

De VNOG is verantwoordelijk voor het aanleggen van een register van alle verwerkingen waarvan de VNOG de verwerkingsverantwoordelijke is. Op dit moment heeft de VNOG dit register niet extern gepubliceerd.

Het verwerkingsregister bevat een beschrijving van wat er tijdens een verwerking plaatsvindt, en welke gegevens daarvoor worden gebruikt, namelijk:

- Een omschrijving van het proces waarbij persoonsgegevens verwerkt worden
- De naam en contactgegevens van de verwerkingsverantwoordelijke en, mogelijk, de gezamenlijke verwerkingsverantwoordelijke
- De doelen van de verwerking
- Een beschrijving van het soort persoonsgegevens en de daarbij horende betrokkenen
- Een beschrijving van de ontvangers van de persoonsgegevens
- Een beschrijving van het delen van persoonsgegevens
- De termijnen waarin de verschillende persoonsgegevens moeten worden gewist
- Een algemene beschrijving van de beveiligingsmaatregelen

Aanstellen van een Functionaris Gegevensbescherming (FG) (Artikelen 37 t/m 39, AVG)

Het Dagelijks Bestuur (DB) van de VNOG heeft een FG aangesteld. Deze is geregistreerd als FG van de VNOG bij de Autoriteit Persoonsgegevens (AP) onder registratienummer FG000318. De FG heeft een onafhankelijke rol binnen de VNOG en is betrokken bij aangelegenheden die verband houden met de bescherming van persoonsgegevens. Hiervoor voert de FG ook interne audits uit. Daarnaast heeft het DB

een Privacy Officer (PO) aangesteld om de organisatie te ondersteunen bij de bescherming van persoonsgegevens. Gezamenlijk vormen deze functionarissen het team Privacy.

De taken van team Privacy zijn informeren, adviseren, toezicht houden, bewustwording creëren, en optreden als contactpersoon voor de Autoriteit Persoonsgegevens (AP). Hierbij heeft de Privacy Officer meer een uitvoerende en adviserende rol en heeft de FG een toezichthoudende rol. Het is niet de bedoeling dat het team de taken op het gebied van bescherming van de privacy van de afdelingen overneemt. De afdelingen hebben hun eigen verantwoordelijkheid in het goed omgaan met privacygevoelige gegevens. Een verwerking van persoonsgegevens wordt eerst aan het team Privacy gemeld voordat de verwerking begint. Het team Privacy is verantwoordelijk voor het structureel toetsen van de implementatie en de uitvoering van de wettelijke eisen en de richtlijnen op het gebied van privacy.

Voor vragen over privacy of over deze toelichting kunt u contact opnemen met team Privacy van de VNOG via privacy-security@vnog.nl dan wel telefonisch (088-310 4000).

Datalekken (Artikel 33,34, AVG)

We spreken van een datalek wanneer persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens mogen hebben, wanneer data onjuist is of als data niet beschikbaar is. VNOG beschikt over een vastgestelde datalekken procedure, waarnaar gehandeld wordt in het geval van een (vermoedelijk) datalek.

Aan de hand van een escalatieladder beoordelen de Privacy Officer (PO) en de Chief Information Security Officer (CISO) of er sprake is van:

- a. een beveiligingslek;
- b. een beveiligingsincident;
- c. een datalek;
- d. een aan de Autoriteit Persoonsgegevens te melden datalek;
- e. een aan de betrokkenen te melden datalek.

De Functionaris Gegevensbescherming (FG) geeft hierbij advies.

Wanneer er een aan de Autoriteit Persoonsgegevens te melden datalek heeft plaatsgevonden meldt de VNOG dit zonder onredelijke vertraging, uiterlijk 72 uur nadat er kennis van de inbreuk is vernomen, aan de Autoriteit Persoonsgegevens. Als dit later dan 72 uur is wordt er een motivering voor de vertraging bij de melding gevoegd.

Het kan zijn dat de inbreuk een hoog risico met zich meebrengt voor de rechten en vrijheden van de betrokkenen. In dit geval meldt de VNOG dit aan de betrokkenen in eenvoudige en duidelijke taal.

Alle meldingen die VNOG aanwijst als datalek, worden opgenomen in een datalekregister. Dit gebeurt ook wanneer VNOG een datalek als niet meldenswaardig bij de Autoriteit Persoonsgegevens beoordeelt. VNOG houdt het datalekregister intern bij en publiceert dit dus niet.

Om toekomstige datalekken te voorkomen worden bestaande datalekken geëvalueerd.

Afsluiting

Als de VNOG een wettelijke verplichting niet nakomt kan de betrokkene een klacht indienen bij de FG via privacy-security@vnog.nl. Deze zal vervolgens via de klachtenregeling van de VNOG worden behandeld.

Disclaimer: Dit product is een eenvoudige en begrijpbare vertaling van de huidige privacywetgeving en gebaseerd op de AVG. Vanzelfsprekend is de toepasbare wet- en regelgeving altijd leidend en kunnen er geen rechten dan wel aansprakelijkheid ontleend worden aan dit document.