

Privacyreglement Veiligheidsregio Brabant-Noord

In dit reglement laat Veiligheidsregio Brabant Noord (hierna: VRBN) zien op welke manier zij dagelijks omgaat met persoonsgegevens en privacy en wat er wettelijk wel en niet verantwoord is.

Privacy speelt een belangrijke rol in de relatie tussen de burger, bedrijven en de overheid. VRBN heeft de verantwoordelijkheid over persoonsgegevens en gegevensuitwisseling op alle terreinen waar ze actief is.

VRBN is verplicht om zorgvuldig en veilig, proportioneel en vertrouwelijk om te gaan met het verzamelen, bewaren en beheer van persoonsgegevens van medewerkers, vrijwilligers, externe partijen en burgers. 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. Daarom vinden wij het belangrijk om transparant te zijn over de manier waarop wij met persoonsgegevens omgaan, en de privacy waarborgen.

1. Wetgeving en definities

Op 25 mei 2018 trad de Europese Verordening, de Algemene Verordening Gegevensbescherming (AVG), in werking, samen met de uitvoeringswet. De AVG zorgt onder andere voor versterking en uitbreiding van de privacy-rechten met meer verantwoordelijkheden voor organisaties.

De volgende begrippen worden in de AVG gebruikt (Artikel 4, AVG):

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). Naast gewone persoonsgegevens kent de wet ook bijzondere persoonsgegevens. Dit zijn gegevens die gaan over gevoelige onderwerpen, zoals etnische achtergrond of politieke voorkeuren.

Gegevensbeschermingseffectbeoordeling

Met een gegevensbeschermingseffectbeoordeling worden de effecten en risico's van de nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. Dit wordt ook wel een Privacy Impact Assessment (PIA) of Data Protection Impact Assessment (DPIA) genoemd.

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: 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 VRBN plaatsvinden.

3. Verantwoordelijke

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

4. Toepassing van de AVG

Verwerkingen (Artikel 4, AVG)

De verwerking van persoonsgegevens is elke handeling of elk geheel van handelingen met persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde processen.

Volgens de AVG vallen de volgende handelingen onder het begrip 'verwerking':

- Verzamelen, vastleggen en ordenen.
- Bewaren, bijwerken en wijzigen.
- Opvragen, raadplegen, gebruiken.
- Verstrekken door middel van doorzending.
- Verspreiding of enige andere vorm van ter beschikkingstellen.
- Samenbrengen, met elkaar in verband brengen.
- Afschermen, uitwissen of vernietigen van gegevens.

Uit deze opsomming blijkt dat alles wat met een persoonsgegeven gedaan wordt een verwerking is.

Doeleinden (Artikel 5, AVG)

Volgens de wet mogen persoonsgegevens alleen verzameld worden als daarvoor een doel is vastgesteld. Het doel moet uitdrukkelijk omschreven en gerechtvaardigd zijn. De gegevens mogen niet voor andere doelen verwerkt worden. Voor de uitvoering van sommige wetten zijn de doelen voor het verwerken in de wet al vastgelegd, net als de persoonsgegevens die gevraagd en verwerkt mogen worden.

Rechtmatige grondslag (Artikel 6, AVG)

De wet zegt dat er voor elke verwerking van persoonsgegevens een rechtmatige grondslag uit de wet van toepassing moet zijn. Dat betekent dat de verwerking alleen mag plaatsvinden:

- Om een verplichting na te komen die in de wet staat.
- Voor de uitvoering van een overeenkomst waar de betrokkene onderdeel van is of was.
- Om een ernstige bedreiging voor de gezondheid van de betrokkene te bestrijden.
- Voor de goede vervulling van de wettelijke taken.
- Wanneer de betrokkene toestemming heeft gegeven voor de specifieke verwerking.

Wijze van verwerking

De hoofdregel van de verwerking van persoonsgegevens is dat het alleen toegestaan is in overeenstemming met de wet, en op een zorgvuldige wijze. Persoonsgegevens worden zoveel mogelijk verzameld bij de betrokkene zelf. De wet gaat uit van subsidiariteit. Dit betekent dat verwerking alleen is toegestaan wanneer het doel niet op een andere manier kan worden bereikt.

In de wet wordt ook gesproken over proportionaliteit. Dit betekent dat persoonsgegevens alleen mogen worden verwerkt als dit in verhouding staat tot het doel. Wanneer met geen, of minder (belastende), persoonsgegevens hetzelfde doel bereikt kan worden moet daar altijd voor gekozen worden.

Doorgifte (Artikelen 44 t/m 50, AVG)

VRBN geeft geen persoonsgegevens door aan een land buiten de Europese Economische Ruimte (EER) of 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.

5. Transparantie en communicatie

Wet openbaarheid van bestuur (Wob)

Via de Wob (en straks wellicht de Wet Open Overheid) kan een verzoek om informatie worden ingediend bij VRBN. Bij het verzoek bekijkt VRBN 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.

Wet hergebruik van overheidsinformatie

De Wet hergebruik van overheidsinformatie regelt het op verzoek verstrekken van overheidsinformatie voor hergebruik. Bij het verzoek bekijkt VRBN 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.

Informatieplicht (Artikelen 13 en 14, AVG)

VRBN informeert betrokkenen over het verwerken van persoonsgegevens.

Wanneer betrokkenen gegevens aan VRBN verstrekken, worden zij op de hoogte gesteld van de manier waarop VRBN met persoonsgegevens om zal gaan. De betrokkene wordt niet nogmaals geïnformeerd als hij/zij al weet dat VRBN 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 voor de eerste keer worden verwerkt.

Verwijdering

VRBN bewaart de persoonsgegevens niet langer dan nodig is voor de uitvoering van wettelijke taken, of zoals vastgelegd in de Archiefwet. Wanneer nog persoonsgegevens opgeslagen zijn die niet langer nodig zijn voor het bereiken van het doel, dan 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.

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:**

Betrokkene heeft het recht om aan VRBN te vragen of zijn/haar persoonsgegevens worden verwerkt.

- **Inzagerecht:**

Betrokkene heeft de mogelijkheid om te controleren of, welke en op welke manier, zijn/haar gegevens worden verwerkt.

- **Correctierecht:**

Als duidelijk wordt dat de gegevens niet kloppen, kan de betrokkene een verzoek indienen bij VRBN om dit te corrigeren.

- **Recht van verzet:**

Betrokkene heeft het recht aan VRBN te vragen om zijn/haar persoonsgegevens niet meer te gebruiken. VRBN zal hieraan voldoen, tenzij er gerechtvaardigde gronden zijn voor de verwerking.

- **Recht om vergeten te worden:**

In gevallen waar de betrokkene toestemming heeft gegeven om gegevens te verwerken, heeft de betrokkene het recht om de persoonsgegevens te laten verwijderen. VRBN zal hieraan voldoen, tenzij er gerechtvaardigde gronden zijn voor de verwerking.

- **Recht op bezwaar:**

Betrokkenen hebben het recht om bezwaar te maken tegen de verwerking van zijn/haar persoonsgegevens. VRBN zal hieraan voldoen, tenzij er gerechtvaardigde gronden zijn voor de verwerking.

Indienen van verzoek

Om gebruik te maken van zijn/haar rechten kan de betrokkene een verzoek indienen bij de Functionaris Gegevensbescherming van VRBN via e-mail: fg@vrbn.nl.

VRBN 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. Binnen vier weken zal VRBN laten weten wat er met het verzoek gaat gebeuren. Als het verzoek niet wordt opgevolgd is er de mogelijkheid om bezwaar te maken bij VRBN, of een klacht in te dienen bij de Autoriteit Persoonsgegevens (AP). Aan de hand van een verzoek kan VRBN aanvullende informatie opvragen om zeker te zijn van de identiteit van betrokkene.

6. Geautomatiseerde verwerkingen

Profileren (Artikel 22, AVG)

Profileren vindt plaats wanneer 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. Voorbeelden van persoonlijke aspecten kunnen zijn; financiële situatie, interesses, gedrag of locatie.

Om profileren wat duidelijker te maken gebruiken we het volgende voorbeeld:

Wanneer een bezoeker op de VRBN-website naar een bepaalde dienst kijkt, mag VRBN geen actie ondernemen om de dienst aan te bieden. VRBN mag wel bekijken hoe vaak een bepaalde dienst bekeken is, maar dus niet specifiek gericht adverteren. Daarnaast geeft de wet aan dat geen besluit mag worden genomen op basis van profileren.

VRBN maakt geen gebruik van profileren. Zoals hierboven aangegeven mag VRBN 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.

Big data en tracking

Door middel van Big data onderzoek en tracking mogen alleen gegevens verwerkt worden wanneer deze niet herleidbaar zijn tot een natuurlijk persoon. Daarnaast worden ze alleen verzameld voor onderzoek dat door, of namens, VRBN wordt uitgevoerd. De verzamelde gegevens door Big data onderzoek en tracking zijn alleen de gegevens die door geautoriseerde personen zijn verzameld. Wanneer de gegevens worden omgezet in een dataset zal dataminimalisatie worden toegepast. Dit betekent dat alleen de data die echt nodig is voor het behalen van het doel gebruikt zullen worden. Daarnaast kunnen persoonsgegevens gepseudonimiseerd (versleuteld) worden, zodat zij in eerste instantie niet herleidbaar zijn tot een persoon.

VRBN maakt gebruik van Big data en tracking. Dit doen wij op de volgende punten:

- Bedrijfsvoering (PIOFACH taken)
- Operationele toepassingen
- Business Intelligence
- Regionaal risicoprofiel

Inzet van camera's

VRBN heeft een wettelijke taak in het kader van de crisis- en rampbestrijding. In dat kader kan vanuit de levensreddende noodzaak gebruik worden gemaakt van camera's, terwijl 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 de Functionaris Gegevensbescherming (FG) van VRBN via het e-mailadres: fg@vrbn.nl.

Door VRBN wordt onder bepaalde omstandigheden aanvullend gebruik gemaakt van allerlei soorten camera's. Door de elektronische en digitale ontwikkelingen is dit in dit reglement niet in een limitatieve opsomming te omvatten. Echter 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. Waar nodig zal er aanvullende regelgeving worden opgesteld, zodat VRBN bij gebruik van een bepaalde camera ook aanvullende beperkingen, vereisten of afspraken vastlegt.

7. Plichten van de Veiligheidsregio Brabant Noord

Register van verwerkingen (Artikel 30, AVG)

VRBN is verantwoordelijk voor het aanleggen van een register van alle verwerkingen waarvan VRBN de verwerkingsverantwoordelijke is. Een register bevat een beschrijving van wat er tijdens een verwerking plaatsvindt en welke gegevens daarvoor worden gebruikt, namelijk:

- 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.

Gegevensbeschermingseffectbeoordeling (PIA of DPIA genoemd, Artikel 35, AVG)

Met een gegevensbeschermingseffectbeoordeling worden de effecten en risico's van nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. VRBN voert deze uit wanneer bijvoorbeeld een geautomatiseerde verwerking, een grootschalige verwerking, of wanneer een grootschalige monitoring van openbare ruimten plaatsvindt. Dit geldt in het bijzonder bij verwerkingen waarbij nieuwe technologieën worden gebruikt.

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

De FG is betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. De taken van de functionaris zijn informeren, adviseren, toezicht houden, bewustwording creëren, en optreden als contactpersoon voor de Autoriteit Persoonsgegevens (AP). Het is niet de bedoeling dat de functionaris 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 de FG gemeld voordat de verwerking begint. De FG 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 de functionaris gegevensbescherming van VRBN via fg@vrbn.nl.

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.

Aan de hand van het protocol datalek beoordelen de Functionaris Gegevensbescherming (FG) 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.

Wanneer er een aan de Autoriteit Persoonsgegevens te melden datalek heeft plaatsgevonden, dan meldt VRBN dit zonder onredelijke vertraging, uiterlijk 72 uur nadat kennis van de inbreuk is vernomen, aan de Autoriteit Persoonsgegevens. Als dit later dan 72 uur is wordt 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 VRBN dit aan de betrokkenen in eenvoudige en duidelijke taal. Om toekomstige datalekken te voorkomen worden bestaande datalekken geëvalueerd.

Afsluiting

Als VRBN een wettelijke verplichting niet nakomt kan de betrokkene een klacht indienen bij de FG via fg@vrbn.nl. Deze zal vervolgens via de klachtenregeling van VRBN 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.