

## **Besluit van de gemeenschappelijke regeling van 1Stroom houdende regels omtrent privacy**

In dit reglement laat de gemeenschappelijke regeling 1Stroom 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 en de overheid en staat daarmee hoog op de bestuurlijke agenda. Gemeenten<sup>1</sup> hebben de verantwoordelijkheid over persoonsgegevens en gegevensuitwisseling op alle terreinen waar ze actief zijn. Gemeenten zijn verplicht om zorgvuldig en veilig, proportioneel en vertrouwelijk om te gaan met het verzamelen, bewaren en beheren van persoonsgegevens van burgers. Dat geldt voor taken als de bijhouding van de basisadministraties, openbare orde en veiligheid en het sociaal domein. Goed en zorgvuldig omgaan met persoonsgegevens is een dagelijkse bezigheid van gemeenten. Het beschermen van de privacy is complex, en wordt steeds complexer door technologische ontwikkelingen, de decentralisaties, grote uitdagingen op het terrein van veiligheid en de 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**

De Algemene Verordening Gegevensbescherming (de AVG) regelt op dit moment het juridische kader voor de omgang met persoonsgegevens in Nederland. Op 25 mei 2018 is de AVG samen met de uitvoeringswet (de UAVG) in werking getreden. De AVG bouwt voort op de Wet Bescherming Persoonsgegevens (de Wbp) en zorgt onder andere voor versterking en uitbreiding van de privacyrechten van onze inwoners met meer verantwoordelijkheden voor onze organisatie en de ketenpartners. 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 persoonsgegevens 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, politieke voorkeur of het Burgerservicenummer (BSN).

#### Gegevensbeschermingseffectbeoordeling

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

#### 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 je met een persoonsgegeven doet, zoals: vastleggen, bewaren, verzamelen, bij elkaar voegen, verstrekken aan een ander en vernietigen.

### **2. Reikwijdte**

Het reglement is van toepassing op alle verwerkingen van persoonsgegevens door alle bestuursorganen van de gemeente. Oftewel: voor alle verwerkingen die binnen de gemeenschappelijke regeling van 1Stroom plaatsvinden.

1 ) Met gemeenten c.q. gemeente wordt in dit Privacyreglement ook de Gemeenschappelijke Regeling 1Stroom bedoeld.

### 3. Verantwoordelijke

De bestuursorganen van de gemeente zijn allemaal verantwoordelijken voor de verwerkingen die door of namens de gemeente worden uitgevoerd. De bestuursorganen van de gemeente zijn onder andere de burgemeester, het college van Burgemeesters en Wethouders (college van B&W) en de Raad. Een groot aantal taken en bevoegdheden van de hierboven genoemde bestuursorganen zijn gemandateerd aan de directie of de medewerkers van de Gemeenschappelijke Regeling 1Stroom (Mandaatregeling 1Stroom).

### 4. 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. In de AVG valt onder een verwerking:

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

Uit deze opsomming blijkt dat alles wat je met een persoonsgegeven doet een verwerking is.

#### Doeleinden (Artikel 5, AVG)

Volgens de AVG 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, zoals bijvoorbeeld de Jeugdwet, zijn de doelen voor het verwerken al in de specifieke wet vastgelegd, net als de persoonsgegevens die gevraagd en verwerkt mogen worden.

#### Rechtmatige grondslag (Artikel 6, AVG)

De AVG 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:

- a. Om een verplichting na te komen die in de wet staat;
- b. Voor de uitvoering van een overeenkomst waar de betrokkene onderdeel van is;
- c. Om een ernstige bedreiging voor de gezondheid van de betrokkene te bestrijden;
- d. Voor de goede vervulling van de gemeentelijke taak (algemeen belang / openbaar gezag);
- e. Wanneer de betrokkene toestemming heeft gegeven voor de specifieke verwerking;
- f. Voor de behartiging van de gerechtvaardigde belangen van de gemeente.

#### 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. In het belang van de zorgvuldigheid worden de volgende uitgangspunten in acht genomen:

- a. De persoonsgegevens worden zoveel mogelijk verzameld bij de betrokkene zelf;
- b. De verwerking is alleen toegestaan wanneer het doel niet op een andere manier kan worden bereikt (subsidiariteit);
- c. De persoonsgegevens mogen alleen verwerkt worden 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 (proportionaliteit);
- d. De organisatie zorgt ervoor dat de persoonsgegevens kloppen en volledig zijn voordat ze verwerkt worden;
- e. De gegevens worden alleen verwerkt door personen met een geheimhoudingsplicht;
- f. De organisatie zorgt voor een adequaat beveiligingsniveau van alle persoonsgegevens, zodat de persoonsgegevens niet kunnen worden ingezien of gewijzigd door iemand die daar geen recht toe heeft.

Hoe de organisatie dit doet staat in het informatiebeveiligingsbeleid van de twee gemeenten en in het eventueel aanvullend beveiligingsplan, specifiek opgesteld voor een proces of registratie. De gemeenschappelijke regeling 1Stroom voert de dagelijkse werkzaamheden uit in overeenstemming met het informatiebeveiligingsbeleid van de twee gemeenten.

### Doorgifte (Artikel 44 t/m 50, AVG)

De organisatie van 1Stroom geeft alleen persoonsgegevens door aan een land buiten de Europese Economische Ruimte (EER) of een internationale organisatie op grond van goedgekeurde afspraken door de Europese Commissie.

## **5. Transparantie en communicatie**

### Wet openbaarheid van bestuur ( Wob )

Via de Wob (en straks wellicht de Wet Open Overheid) kan men een verzoek om informatie indienen bij de gemeente. Bij het verzoek bekijkt de organisatie altijd of het antwoord geen inbreuk maakt op de persoonlijke levenssfeer van betrokkenen. In principe worden geen persoonsgegevens verstrekt.

### Wet hergebruik van overheidsinformatie

De Wet hergebruik van overheidsinformatie regelt het op verzoek verstrekken van overheidsinformatie voor hergebruik. Bij het verzoek bekijkt de organisatie altijd of het antwoord geen inbreuk maakt op de persoonlijke levenssfeer van betrokkenen. In principe worden geen persoonsgegevens verstrekt.

### Informatieplicht (Artikel 13 en 14, AVG)

De organisatie informeert betrokkenen over het verwerken van persoonsgegevens. Wanneer betrokkenen gegevens aan de organisatie verstrekken, worden zij op de hoogte gesteld van de manier waarop de organisatie met de verstrekte persoonsgegevens om zal gaan.

### Verwijdering

De organisatie bewaart de persoonsgegevens niet langer dan nodig is voor de uitvoering van gemeentelijke taken, of zoals vastgelegd in de Archiefwet. Wanneer er nog persoonsgegevens opgeslagen zijn die niet langer nodig zijn voor het bereiken van het doel waarvoor ze verstrekt zijn, dan worden deze persoonsgegevens 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 (Artikel 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:

- a. Recht op informatie: Betrokkenen hebben het recht om aan de organisatie te vragen of zijn/haar persoonsgegevens worden verwerkt;
- b. Inzagerecht: Betrokkenen hebben de mogelijkheid om te controleren of, en op welke manier, zijn/haar gegevens worden verwerkt;
- c. Correctierecht: Als duidelijk wordt dat de gegevens niet kloppen, kan de betrokkene een verzoek indienen bij de organisatie om dit te corrigeren;
- d. Recht van verzet: Betrokkenen hebben het recht aan de organisatie te vragen om hun persoonsgegevens niet meer te gebruiken;
- e. 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;
- f. Recht op bezwaar: Betrokkenen hebben het recht om bezwaar aan te maken tegen de verwerking van zijn/haar persoonsgegevens. De organisatie zal aan het verzoek om de persoonsgegevens niet te verwerken 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. Dit verzoek kan zowel schriftelijk als via de e-mail ingediend worden. De organisatie heeft vier weken de tijd, vanaf de ontvangst van het verzoek, om te beoordelen of het verzoek gerechtvaardigd is. Binnen vier weken zal de organisatie laten weten wat er met het verzoek gaat gebeuren. Als het verzoek niet wordt opgevolgd, bestaat er nog de mogelijkheid om bezwaar te maken bij de gemeente, of een klacht in te dienen bij de Autoriteit Persoonsgegevens (AP). Aan de hand van een verzoek kan de organisatie aanvullende informatie opvragen om zeker te zijn van de identiteit van de betrokkene.

## **6. Geautomatiseerde verwerkingen**

### Profilering (Artikel 22, AVG)

De gemeenschappelijke regeling 1Stroom kan gebruik maken profilering, echter alleen indien er sprake is van de volgende drie gevallen:

- a. noodzakelijk is voor de totstandkoming of uitvoering van een overeenkomst tussen de betrokkene en de verwerkingsverantwoordelijke;
- b. is toegestaan bij een bepaling van de Europese Unie of een lidstaat die op de verwerkingsverantwoordelijke van toepassing is en die ook voorziet in passende maatregelen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene; of
- c. berust op de uitdrukkelijke toestemming van de betrokkene.

#### Big data en tracking

De gemeenschappelijke regeling 1Stroom kan gebruik maken van Big data voor onderzoek onder de volgende voorwaarden:

- a. Door middel van Big data onderzoek en tracking mogen alleen gegevens verwerkt worden wanneer deze niet herleidbaar zijn tot een natuurlijk persoon;
- b. De gegevens worden alleen verzameld voor onderzoek dat door, of namens, de organisatie wordt uitgevoerd;
- c. De verzamelde gegevens door Big data onderzoek en tracking zijn alleen de gegevens die door geautoriseerde personen zijn verzameld;
- e. Wanneer de gegevens worden omgezet in een dataset zal dataminimalisatie worden toegepast. Dit betekent dat alleen de data die echt nodig zijn voor het behalen van het doel gebruikt zullen worden;
- f. De persoonsgegevens worden gepseudonimiseerd worden, zodat zij niet herleidbaar zijn tot een persoon.

#### Inzet van camera's

Binnen de gemeenschappelijke regeling 1Stroom kan onder bepaalde omstandigheden gebruik gemaakt worden van cameratoezicht, zoals vastgelegd in artikel 151c van de Gemeentewet. Cameratoezicht door de organisatie is slechts toegestaan in de volgende vier gevallen:

- a. De handhaving van de openbare orde en veiligheid op straat;
- b. De beveiliging van gemeentelijke eigendommen;
- c. De handhaving van de verkeersveiligheid;
- d. De opsporing van criminaliteit.

### **7. Plichten van de gemeenschappelijke regeling 1Stroom**

#### Register van verwerkingen (Artikel 30, AVG)

De gemeenschappelijke regeling 1Stroom is verantwoordelijk voor het aanleggen van een register van alle verwerkingen waarvan de gemeenschappelijke regeling 1Stroom de verwerkingsverantwoordelijke is. Elk register bevat een beschrijving van wat er tijdens een verwerking plaatsvindt en welke gegevens daarvoor worden gebruikt, namelijk:

- a. De naam en contactgegevens van de verwerkingsverantwoordelijke en, mogelijk, de gezamenlijke verwerkingsverantwoordelijke;
- b. De doelen van de verwerking;
- c. Een beschrijving van het soort persoonsgegevens en de daarbij horende betrokkenen;
- d. Een beschrijving van de ontvangers van de persoonsgegevens;
- e. Een beschrijving van het delen van persoonsgegevens aan een derde land of internationale organisatie;
- f. De termijnen waarin de verschillende persoonsgegevens moeten worden gewist;
- g. Een algemene beschrijving van de beveiligingsmaatregelen.

#### Gegevensbeschermingseffectbeoordeling (Artikel 35, AVG)

De organisatie voert een gegevenseffectbeoordeling uit in de volgende gevallen:

- a. Wanneer er sprake is van een geautomatiseerde verwerking, een grootschalige verwerking, of
- b. Wanneer er sprake is van een grootschalige monitoring van openbare ruimten.

#### Aanstellen van een Functionaris voor gegevensbescherming (FG) (Artikel 37 t/m 39, AVG)

De gemeenschappelijke regeling heeft een Functionaris Gegevensbescherming aangesteld.

#### 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 er een datalek heeft plaatsgevonden onderneemt de organisatie de volgende acties:

- a. Indien van toepassing meldt de organisatie het datalek zonder onredelijke vertraging, uiterlijk 72 uur nadat er kennis van de inbreuk is vernomen aan de Autoriteit Persoonsgegevens;
- b. Als de melding later dan 72 uur wordt doorgegeven, wordt de motivering voor de vertraging bij de melding gevoegd;
- c. Indien het datalek een hoog risico met zich mee brengt voor de rechten en vrijheden van betrokkene, dan meldt de organisatie dit aan de betrokkene in eenvoudige en duidelijke taal;
- d. Om toekomstige datalekken te voorkomen worden de bestaande datalekken geëvalueerd met als doel om een vergelijkbaar datalek in de toekomst te voorkomen.

#### Klachten en bezwaren

Als de gemeenschappelijke regeling 1Stroom een wettelijke verplichting niet nakomt, kan de betrokkene een klacht indienen. Deze zal via de bestaande klachtenregeling van de organisatie worden behandeld. Bij de behandeling van de klacht kan de Functionaris Gegevensbescherming om advies worden gevraagd (ombudsfunctie). In onvoorziene gevallen waar dit reglement niets over zegt, beslist het verantwoordelijke bestuursorgaan van de gemeenschappelijke Regeling 1Stroom.

### **8. Inwerkingtreding**

Dit privacyreglement treedt in werking één dag na de bekendmaking.

*Aldus vastgesteld door het dagelijks bestuur van de gemeenschappelijke regeling 1Stroom op 21 februari 2019.*

*Het dagelijks bestuur van de gemeenschappelijke regeling van 1Stroom,*

*drs. H.B.I. (Rik) de Lange  
(voorzitter)*

*ing. C.J. (Chris) Papjes  
(secretaris)*

## **Artikelsgewijze toelichting**

### **Artikel 5: Informatieplicht**

De informatieplicht kan 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 organisatie 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.

### **Artikel 6: Profilering**

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. Voorbeelden van persoonlijke aspecten kunnen zijn; financiële situatie, interesses, gedrag of locatie. Profiling bij de overheid kan een vorm van risicomanagement zijn, zoals bij grenscontroles.

### **Artikel 6: Big data en tracking**

De technologie om grote hoeveelheden data te verzamelen, op te slaan en te analyseren, wordt steeds betaalbaarder en makkelijker in het gebruik. Dat leidt ertoe dat organisaties steeds meer verschillende soorten gegevens kunnen verzamelen. Daarnaast is het makkelijker dan vroeger om bestanden met zeer verschillende indelingen en van heel verschillende oorsprong te koppelen. In de gecombineerde 'big data' kunnen nieuwe soorten statistische verbanden worden ontdekt, die in kleinere of eenzijdiger verzamelingen niet zouden opvallen.

Het pseudonimiseren van persoonsgegevens is een methode om met persoonsgegevens te werken zonder daarbij te weten over welke personen de gegevens gaan. Het pseudonimiseren van

persoonsgegevens zorgt er namelijk voor dat gegevens alleen nog herleidbaar zijn tot een specifiek persoon als er gebruik wordt gemaakt van aanvullende gegevens. Bij pseudonimisering is het van belang dat er voldoende technische en organisatorische maatregelen zijn genomen, zodat onbevoegden de koppeling met het bestand met aanvullende gegevens niet kunnen maken. Het koppelen van bestaande bestanden en het zoeken naar nieuwe verbanden, betekent vaak dat gegevens voor een nieuw doeleinde worden verwerkt. Wat niet voorzien was toen de oorspronkelijke bestanden werden aangelegd.

De overheid kan bigdata-analyses bijvoorbeeld inzetten om epidemieën te bestrijden of fraudeurs op te sporen.

#### **Artikel 6: Inzet van camera's**

Het gebruik van camera's kan een grote inbreuk maken op de privacy van diegene die gefilmd worden. Om de privacy zo goed mogelijk te waarborgen worden camera's alleen ingezet wanneer er geen andere manieren zijn om het doel te bereiken en worden er eisen gesteld aan de inzet van camera's. Het gebruik van camera's door particulieren op de openbare weg is alleen mogelijk na toestemming van het college van B&W. Daarvoor wordt er een convenant afgesloten tussen de particulieren en het bestuursorgaan waarin o.a. de grondslag, het doel, de maatregelen tegen verlies, en de bewaartermijn in opgenomen worden.

De enige verplichting voor het gebruik van camera's is het op duidelijke wijze kenbaar maken wanneer iemand zich in het camera gebied bevindt. Wettelijk is het niet verplicht om via andere kanalen aan te geven waar de organisatie haar camera's heeft hangen, maar het geeft daarmee wel meer transparantie richting de burger. In de privacyverklaring op de website van de gemeenschappelijke regeling 1Stroom worden daarom de locaties benoemd waar de organisatie gebruik maakt van cameratoezicht.

#### **Artikel 7: Gegevensbeschermingseffectbeoordeling (PIA)**

Met een gegevensbeschermingseffectbeoordeling worden de effecten en risico's van nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. Dit geldt in het bijzonder bij verwerkingen waarbij nieuwe technologieën worden gebruikt.

#### **Artikel 7: Datalekken**

Bij een datalek is er sprake van een inbreuk op de beveiliging van persoonsgegevens waarbij deze zijn blootgesteld aan verlies of onrechtmatige verwerking ervan. Daarbij kan men denken aan de volgende situaties:

- a. Een medewerker verliest een laptop met onversleutelde persoonsgegevens;
- b. Een bedrijf krijgt te maken met een hack, waarbij persoonsgegevens worden ontvreemd;
- c. De envelop met een verzameling van documenten met persoonsgegevens wordt per ongeluk niet versnipperd, maar in de vuilnisbak gegooid.

#### **Artikel 7: Functionaris Gegevensbescherming (FG)**

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 van de AP. Het is niet de bedoeling dat de functionaris de taken op het gebied van bescherming van de privacy van de afdelingen overneemt. De teams 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 gemeentelijke richtlijnen op het gebied van privacy. Voor vragen over privacy of over deze toelichting kunt u contact opnemen met de Functionaris Gegevensbescherming van gemeenschappelijke regeling 1Stroom via [privacy@1stroom.nl](mailto:privacy@1stroom.nl).