VEILIGHEIDSREGIO UTRECHT

BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 177

28 februari 2020

Officiële uitgave van de gemeenschappelijke regeling Veiligheidsregio Utrecht

Regeling van het algemeen bestuur van de Veiligheidsregio Utrecht houdende regels omtrent de bescherming van persoonsgegevens (Regeling bescherming persoonsgegevens VRU)

Het algemeen bestuur van de Veiligheidsregio Utrecht,

gelet op:
- de Algemene verordening gegevensbescherming (EU 2016/679) en de daarmee samenhangende wet- en regelgeving;
- de Gemeenschappelijke regeling VRU;
- de Organisatieverordening VRU 2015;

overwegende dat:
- de Veiligheidsregio Utrecht bij de uitvoering van haar taken persoonsgegevens verwerkt;
- het daarom van belang is om een regeling voor de bescherming van persoonsgegevens vast te stellen die duidelijkheid en kaders schept voor de verwerking van persoonsgegevens door de Veiligheidsregio Utrecht;
- dat het algemeen bestuur op 13 december 2013 de Algemene privacyregeling Veiligheidsregio Utrecht heeft vastgesteld;
- dat de Algemene verordening gegevensbescherming sinds 25 mei 2018 van toepassing is en daarmee de grondslag voor het verwerken van persoonsgegevens gewijzigd is;
- deze verordening strekt tot nadere uitwerking van de Algemene verordening gegevensbescherming;
- dat de Centrale Ondernemingsraad van de Veiligheidsregio Utrecht heeft ingestemd met deze regeling;

besluit:
1. de Algemene privacyregeling Veiligheidsregio Utrecht in te trekken en
2. vast te stellen de volgende:

Regeling bescherming persoonsgegevens VRU.

Artikel 1. Definities

1. De in de Algemene Verordening Gegevensbescherming (verder te noemen: AVG) opgenomen definities en overige normen zijn onverkort van toepassing op dit besluit.
2. Artikel 1 van de Organisatieverordening VRU 2015 is van toepassing op dit besluit.
   Daarnaast wordt in dit besluit verstaan onder:
   a. betrokkene: de persoon op wie de persoonsgegevens betrekking hebben, oftewel degene van wie de persoonsgegevens worden verwerkt;
   b. leden van het directieteam: het directieteam VRU zoals bedoeld in artikel 4 lid 1 Organisatieverordening VRU 2015;
   c. Autoriteit persoonsgegevens: de toezichthoudende autoriteit bedoeld in artikel 51 AVG;
   d. Functionaris voor gegevensbescherming: de functionaris bedoeld in artikel 37 e.v. AVG;
   e. big data: een hoeveelheid data waarbij sprake is van tenminste twee van de drie navolgende factoren:
   i. een grote hoeveelheid van data/gegevens die;
   ii. in principe ongestructureerd wordt opgeslagen, en
   iii. snel binnenkomen of kunnen worden opgevraagd;
   f. datalek: een ‘inbreuk in verband met persoonsgegevens’, bedoeld in artikel 33 AVG;
   g. gegevensbeschermingseffect¬beoordeling: de beoordeling van de effecten en risico’s van de nieuwe of bestaande verwerkingen op de bescherming van de privacy; ook wel een ‘Privacy Impact Assessment’ (PIA) of een ‘Data Protection Impact Assessment’ (DPIA) genoemd;
   h. anonimiseren: het transformeren van persoonsgegevens in een dataset die niet meer direct herleidbaar is tot een persoon;
   i. tracking: het volgen van mobiele datadragers zoals telefoons, bijvoorbeeld door Wifi- of bluetooth apparatuur waarbij (persoons)gegevens worden verzameld uit die datadragers.

Artikel 2. Doel van de regeling
Deze regeling schept een kader waarbinnen de verschillende verwerkingen van persoonsgegevens binnen de gehele VRU op eenduidige en rechtmatige wijze plaatsvinden.

Artikel 3. Reikwijdte
Deze regeling is van toepassing op het verwerken van persoonsgegevens door en namens de VRU.

Artikel 4. Verwerkingsverantwoordelijke
1. De verwerkingsverantwoordelijke voor de verwerking van persoonsgegevens, bedoeld in de AVG, is het dagelijks bestuur.
2. De leden van het directieteam zijn verantwoordelijk voor de verwerking van persoonsgegevens bij de uitvoering van de taken binnen hun organisatieonderdeel.

Artikel 5. Vastleggen doelen gegevensverwerking
1. Voor de verwerking van persoonsgegevens worden de grondslagen, doelen en voorschriften door of namens het dagelijks bestuur specifiek vastgelegd.
2. De verwerking van persoonsgegevens met een hoog risico, bedoeld in artikel 35 AVG, vindt slechts plaats op basis van een vooraf door het dagelijks bestuur vastgesteld reglement.

Artikel 6. Verantwoordelijkheden
1. De leden van het directieteam zijn met betrekking tot het eigen organisatieonderdeel verantwoordelijk voor in ieder geval:
   a. het aanleveren en actueel houden van de gegevens over de verwerkingen die onder zijn verantwoordelijkheid plaatsvinden, ten behoeve van het register zoals bedoeld in artikel 30 AVG;
   b. het beoordelen van verwerkingen en het eventueel uitvoeren van DPIA's;
   c. het opstellen van en het houden van toezicht op het gebruik van privacyreglementen voor verwerkingen die onder verantwoordelijkheid van het organisatieonderdeel plaatsvinden;
   d. het nemen van passende maatregelen die op grond van de AVG en de privacyreglementen noodzakelijk zijn;
   e. het afsluiten van verwerkersovereenkomsten zoals bedoeld in artikel 28 lid 3 AVG, en
   f. de informatiebeveiliging van het organisatieonderdeel. Hieronder valt in ieder geval:

i. het vaststellen van de autorisaties;
ii. het informatiebeveiligingsbeleid van de VRU opnemen en doorvoeren in contracten met verwerkers en leveranciers, en
iii. alle handelingen aangaande de meldplicht datalekken die het organisatieonderdeel aangaan.

2. Elk lid van het directieteam wijst voor het eigen organisatieonderdeel een of meer contactpersonen aan ten behoeve van de coördinatie en de uitvoering van het privacy- en beveiligingsbeleid van het betreffende organisatieonderdeel.

Artikel 7. Gegevensbeschermingseffectbeoordeling of DPIA
1. Voordat door of namens het dagelijks bestuur een beslissing wordt genomen over nieuwe of wijzigingen van bestaande verwerkingen die waarschijnlijk een hoog risico inhouden voor de rechten en vrijheden van natuurlijke personen, als bedoeld in artikel 35 AVG, wordt een gegevensbeschermingseffectbeoordeling uitgevoerd. Hiermee wordt zicht verkregen op de risico's van de betreffende verwerking voor de bescherming van de te verwerken persoonsgegevens. De resultaten van deze beoordeling worden vervolgens gebruikt om maatregelen te nemen om de risico's te beheersen.
2. Een gegevensbeschermingseffectbeoordeling is in ieder geval verplicht, als:
   a. er systematisch en uitgebreid persoonlijke aspecten geanalyseerd of geëvalueerd worden gebaseerd op geautomatiseerde verwerking, waaronder profiling, en daarop besluiten gebaseerd worden die gevolgen hebben voor personen;
   b. er op grote schaal bijzondere persoonsgegevens of strafrechtelijke gegevens verwerkt worden;
   c. er op grote schaal en systematisch mensen gevolgd worden in een publiek toegankelijk gebied (bijvoorbeeld door middel van cameratoezicht);
   d. de verwerking voorkomt op de vigerende lijst van verwerkingen waarvoor het uitvoeren van een DPIA verplicht is voordat begonnen wordt met de verwerking, zoals opgesteld door de Autoriteit Persoonsgegevens.

3. De functionaris voor gegevensbescherming adviseert het lid van het directieteam over de gegevensbeschermingseffectbeoordeling.
4. Door of namens het dagelijks bestuur wordt een procedure voor het uitvoeren van een gegevensbeschermingseffectbeoordeling vastgesteld.

Artikel 8. Open data

1. Hergebruik van gegevens als bedoeld in de Wet hergebruik van overheidsinformatie via het aanbieden van open data gebeurt met inachtneming van de AVG en deze verordening.
2. Een open dataset bevat geen gegevens die herleidbaar zijn naar een persoon.
3. Van open datasets wordt de status van de dataset voor de afnemer weergegeven op de site waarop de open datasets zijn te verkrijgen.

Artikel 9. Big data, tracking en pseudonimisering

1. Gegevens in big data en tracking mogen slechts worden verzameld, opgeslagen en gedeeld, als ze niet herleidbaar zijn tot een persoon en worden slechts verzameld voor onderzoek dat door of namens de VRU wordt uitgevoerd.
2. Voor big data en tracking wordt uitsluitend gebruik gemaakt van brongegevens die door daartoe geautoriseerde personen zijn verzameld.
3. Brongegevens die gebruikt worden voor big data toepassingen worden omgezet tot een dataset die geen persoonsgegevens bevat en dus geanonimiseerd is.
4. Indien het noodzakelijk is om van lid 3 af te wijken wordt vooraf toestemming aangevraagd bij de functionaris voor gegevensbescherming die de aanvraag zal beoordelen in het kader van de rechtmatigheid en de doelmatigheid. Alleen bij een goedgekeurde aanvraag mogen de gegevens worden gepseudonimiseerd in plaats van geanonimiseerd worden.
5. Onderzoek aan de hand van de dataset als bedoeld in lid 3, mag alleen door andere dan de in lid 2 bedoelde geautoriseerde personen worden uitgevoerd.
6. In afwijking van het derde lid kan door of namens het dagelijks bestuur worden beslist tot pseudonimisering van gegevens, indien daarvoor een noodzaak is. Deze beslissing wordt niet genomen dan nadat de functionaris voor gegevensbescherming hierover heeft geadviseerd.

Artikel 10. Datalek

1. Door of namens het dagelijks bestuur wordt een protocol datalekken vastgesteld, waarin verantwoordelijkheden en werkwijze zijn beschreven ten aanzien van het melden en afhandelen van datalekken.
2. Het protocol bevat ook verantwoordelijkheden en voorschriften voor de inhoud van een logboek datalekken.

Artikel 11. Geheimhoudingsplicht

De persoonsgegevens worden alleen verwerkt door personen die uit hoofde van ambt, beroep of wettelijk voorschrift, dan wel krachtens een overeenkomst tot geheimhouding zijn verplicht.

Artikel 12. Beveiliging

Het door het dagelijks bestuur vastgestelde informatiebeveiligingsbeleid bevat maatregelen die een passend beveiligingsniveau garanderen gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich mee brengen.

Artikel 13. Rechten betrokkene

Door of namens het dagelijks bestuur worden een Procedure verzoek uitoefening rechten betrokkenen en een Instructie behandeling verzoeken betrokkenen vastgesteld.

Artikel 14. Klachtenbehandeling

Klachten met betrekking tot de wijze waarop de VRU met persoonsgegevens om gaat kunnen worden ingediend conform de vigerende regeling van de VRU voor de behandeling van klachten.

Artikel 15. Functionaris voor gegevensbescherming

1. Door of namens het dagelijks bestuur wordt een functionaris voor gegevensbescherming benoemd, zoals bedoeld in artikel 37 AVG. De functionaris voor gegevensbescherming is verantwoordelijk voor het toezichthouden op de toepassing en naleving van de wet- en regelgeving met betrekking tot de verwerking van persoonsgegevens en het privacy- en beveiligingsbeleid van de VRU.
2. Voor de uitoefening van zijn functie beschikt de functionaris voor gegevensbescherming over alle bevoegdheden die daarvoor redelijkerwijs noodzakelijk zijn.
3. Het lid van het directieteam en de personen die bij een verwerking van persoonsgegevens zijn betrokken, verstrekken desgevraagd de functionaris voor gegevensbescherming alle inlichtingen en verlenen alle overige medewerking die hij voor de uitoefening van zijn taak behoeft.
4. De functionaris voor gegevensbescherming heeft toegang tot alle ruimten, waar een verwerking van persoonsgegevens plaatsvindt. De FG is bevoegd apparatuur, programmatuur, gegevensbestanden, boeken en bescheiden te onderzoeken en zich de werking van apparatuur en programmatuur te doen tonen.

5. De functionaris voor gegevensbescherming kan onafhankelijk, gevraagd en ongevraagd, zonder last of ruggenspraak, adviseren of informeren over onrechtmatigheden, risico's of onvolkomenheden aan:
   a. de algemeen directeur;
   b. het directieteam VRU en elk van zijn leden;
   c. het dagelijks bestuur, en
   d. de voorzitter.

6. De functionaris voor gegevensbescherming kan een onderzoek instellen naar de wijze waarop in verband met de verwerking van persoonsgegevens, in een bepaald geval dan wel in het algemeen belang, de persoonlijke levenssfeer wordt beschermd.
7. De functionaris voor gegevensbescherming kan voor zijn onderzoek gebruik maken van de diensten van derden.
8. De functionaris voor gegevensbescherming deelt zijn bevindingen aan de algemeen directeur of het betreffende lid van het directieteam mede en geeft zo nodig aanbevelingen. In bijzondere gevallen kan de FG zijn bevindingen ook aan het dagelijks bestuur of de voorzitter mededelen.
9. De functionaris voor gegevensbescherming hanteert het protocol datalekken zoals bedoeld in artikel 10.

Artikel 16. Slotbepalingen

1. Deze regeling treedt in werking op 1 maart 2020.
2. Reeds bestaande beslissingen die tot stand zijn gekomen onder de Algemene privacyregeling VRU worden tot wijziging daarvan beschouwd als waren zij tot stand gekomen onder deze regeling.
3. Deze regeling is vastgesteld door het algemeen bestuur, met dien verstande dat het dagelijks bestuur toekomstige wijzigingen van de regeling vaststelt.

Aldus vastgesteld door het algemeen bestuur,
Doorn, 10 februari 2020,

mr. J.H.C. van Zanen
voorzitter

dr. P.L.J. Bos
secretaris