Gemeente Utrecht

GEMEENTEBLAD

Officiële uitgave van de gemeente Utrecht

Nr. 205921

27 september

2018

Privacyverordening gemeente Utrecht

De raad van de gemeente Utrecht;
Gelet op artikel 149 Gemeentewet

BESLUIT
vast te stellen de volgende

PRIVACYVERORDENING gemeente Utrecht

Artikel 1 Definitie en begripsbepalingen

1. Deze verordening strekt tot nadere uitwerking van de Algemene Verordening Gegevensbescherming (hierna: de Verordening). De in de Verordening opgenomen definities en overige normen zijn onverkort van toepassing.
2. Deze verordening verstaat onder:
a. Anonimiseren: persoonsgegevens die voor een taakuitvoering niet meer noodzakelijk zijn, worden verwijderd uit een dataset. De dataset bevat dan enkel geanonimiseerde gegevens, die wel worden bewaard voor bijvoorbeeld onderzoeksdoeleinden of om te gebruiken als open data.
b. AP: de Autoriteit Persoonsgegevens: Is de toezichthoudende autoriteit verantwoordelijk voor het toezicht op de toepassing van de Verordening teneinde de grondrechten en fundamentele vrijheden van natuurlijke personen in verband met de verwerking van hun persoonsgegevens te beschermen en het vrije verkeer van persoonsgegevens binnen de Unie te vergemakkelijken.
c. Big data: een of meer datasets, zowel ongestructureerd als gestructureerd, die door middel van koppeling of hergebruik geschikt zijn voor analyse doeleinden, zoals bijvoorbeeld beleidsonderzoek, gedragsonderzoek, of wetenschappelijk onderzoek.
d. CIO: Chief Information Officer, zijnde de concernmanager informatievoorziening en procesmanagement.
e. CISO: Chief Information Security Officer, zijnde het hoofd informatiebeveiliging, aangewezen door het college van burgemeester en wethouders.
f. Dataminimalisatie: bij het verzamelen en verwerken van persoonsgegevens mogen niet meer gegevens worden gebruikt dan nodig is om het doel waarvoor ze gebruikt zullen worden te bereiken.
g. DISO: Decentrale Information Security Officer zijnde de door de IRM-er aangewezen contactpersoon voor gegevensbescherming die belast is met de coördinatie en uitvoering van het privacy- en beveiligingsbeleid van het betreffende organisatieonderdeel
h. IRM-er: integraal resultaatsverantwoordelijk manager, verantwoordelijk voor een organisatieonderdeel van de gemeente Utrecht, of daarmee gelijk te stellen functies.
i. Data protection impact assessment (DPIA/gegevensbeschermingseffectbeoordeling): een analyse van de gevolgen voor privacy als een project, beleid, dienst, product of ander initiatief wordt gestart of ingevoerd en het nemen van eventueel noodzakelijke mitigerende acties om een negatieve impact te voorkomen dan wel te verkleinen.
j. Pseudonimiseren: het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om er voor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld.
k. Tracking: het volgen van mobiele datadragers zoals telefoons, bijvoorbeeld door Wifi- of bluetooth apparatuur waarbij (persoons)gegevens worden verzameld uit die datadragers.

Artikel 2 Verantwoordelijke

De verantwoordelijke voor de verwerking van persoonsgegevens, zoals bedoeld in de Verordening, is het college van burgemeester en wethouders, respectievelijk de burgemeester.

Artikel 3 Functionaris voor gegevensbescherming

Het college van burgemeester en wethouders benoemt een functionaris voor gegevensbescherming, zoals bedoeld in de Verordening, die belast is met toezicht op het privacy- en beveiligingsbeleid van de gemeente.

Artikel 4 Contactpersoon voor gegevensbescherming (DISO)

1. Elk organisatieonderdeel heeft een contactpersoon die belast is met de coördinatie en uitvoering van het privacy- en beveiligingsbeleid van het betreffende organisatieonderdeel.

2. Tot de taken van de contactpersoon behoren in ieder geval:
a. Het onderhouden en aanvullen van de groslijst met alle verwerkingen die binnen het organisatieonderdeel zijn geïnventariseerd.
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 privacy protocollen voor verwerkingen die onder verantwoordelijkheid van het organisatieonderdeel plaatsvinden.
d. De informatiebeveiliging van het organisatieonderdeel. Hieronder vallen in ieder geval:
i. Informatiebeveiligingsbeleid van de gemeente Utrecht opnemen en doorvoeren in contracten met bewerkers en leveranciers;
ii. Alle handelingen aangaande de meldplicht datalekken die het organisatieonderdeel aangaan.

Artikel 5 Data protection impact assessment (DPIA/gegevensbeschermingseffectbeoordeling)
1. Indien naar oordeel van de DISO van het verantwoordelijke organisatieonderdeel sprake is van een verwerking, die gelet op de aard en de omvang, de context en de doeleinden een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen dan wordt door middel van een DPIA aangetoond dat de privacy voldoende is gewaarborgd en worden de al dan niet te nemen maatregelen gemotiveerd.
2. De functionaris voor gegevensbescherming geeft over de DPIA een bindend advies aan de IRM-er.
3. De DPIA wordt openbaar gemaakt nadat de beslissing als bedoeld onder lid 1 is genomen.

Artikel 6 Open data
1. Hergebruik van gegevens zoals bedoeld in de wet hergebruik van overheidsgegevens via het aanbieden van open data gebeurt met inachtneming van de Verordening 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 7 Big data en tracking
1. Gegevens in big data en tracking mogen alleen worden verzameld, opgeslagen en gedeeld, als ze niet herleidbaar zijn tot een persoon en worden alleen verzameld voor onderzoek dat door of namens de gemeente Utrecht 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 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.

Artikel 8 Cameratoezicht, camerabewaking en overige inzet van camera's
1. Cameratoezicht ten behoeve van het toezicht op een openbare plaats, als bedoeld in artikel 1 van de Wet openbare manifestaties en overeenkomstig artikel 151c van de Gemeentewet en openbare parkeerplaatsen of openbare parkeerterreinen als bedoeld in artikel 2:5 lid 2 van de Algemene Plaatselijke Verordening vindt alleen door of namens de gemeente plaats, na een daartoe strekkend besluit van de burgemeester.
2. Camerabewaking kan tevens door particuliere bedrijven worden uitgeoefend onder voorwaarde dat indien er camera's in de openbare ruimte worden geplaatst dan wel delen van de openbare ruimte in beeld worden gebracht, er een daartoe strekkend besluit door of namens het college van burgemeester en wethouders is genomen en er een convenant met de verantwoordelijke is gesloten voorafgaande aan de verwerking.
3. Het convenant zoals bedoeld in het tweede lid gaat in ieder geval in op:
-de grondslag voor de verwerking van persoonsgegevens;
-het verzamel- en verwerkingsdoel;
-de organisatorische en technische maatregelen die worden getroffen tegen verlies of onrechtmatige verwerking;
-de bewaartermijn;
-de wijze waarop voldaan wordt aan de meldplicht datalekken.
4. Bij inzet van camera's voor andere gemeentelijke doeleinden dient voorafgaand aan deze inzet advies te worden gevraagd aan de functionaris voor gegevensbescherming.

Artikel 9 Datalek
1. Geconstateerde datalekken worden terstond gemeld bij de functionaris voor de gegevensbescherming.
2. De IRM-er is verantwoordelijk voor het dichten van het datalek in samenwerking met de CISO.
3. De functionaris voor gegevensbescherming en de CISO beoordelen of het datalek meldingswaardig is, als bedoeld in de Verordening.
4. De functionaris voor gegevensbescherming meldt een meldingswaardig datalek direct aan de Autoriteit Persoonsgegevens.
5. De IRM-er is verantwoordelijk voor de onverwijlde melding naar betrokkene(n) wiens persoonsgegevens zijn gelekt.
6. De CISO ziet er samen met de CIO op toe dat het datalek op adequate wijze wordt gedicht.

Artikel 10 Toezicht
1. Voor de uitoefening van zijn toezichthoudende functie beschikt de functionaris voor gegevensbescherming over alle bevoegdheden die daarvoor redelijkerwijs noodzakelijk zijn. Ingeval van twijfel of verschil van mening daaromtrent beslist de functionaris voor gegevensbescherming, de CIO gehoord hebbende.
2. De verantwoordelijke 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.
3. De functionaris voor gegevensbescherming heeft toegang tot alle ruimten, waar een verwerking van persoonsgegevens plaatsvindt. De functionaris voor gegevensbescherming is bevoegd apparatuur, programmatuur, gegevensbestanden, boeken en bescheiden te onderzoeken en zich de werking van apparatuur en programmatuur te doen tonen.
4. De functionaris voor gegevensbescherming rapporteert over zijn bevindingen aan het college van burgemeester en wethouders. Hij geeft aanbevelingen over te nemen maatregelen, die een goede werking van de verwerking van persoonsgegevens moeten helpen waarborgen.

Artikel 11 Onderzoek
1. 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.
2. De functionaris voor gegevensbescherming kan voor zijn onderzoek gebruik maken van de diensten van derden.
3. De functionaris voor gegevensbescherming deelt zijn bevindingen aan de Verantwoordelijke mede en geeft zo nodig aanbevelingen.
4. De bevindingen van de functionaris voor gegevensbescherming alsmede de aanbevelingen zijn naderhand te raadplegen via de website van de gemeente. De functionaris voor gegevensbescherming kan dit achterwege laten vanwege dringende redenen.

Artikel 12 Openbaar register verwerkingen
De functionaris voor gegevensbescherming schrijft namens de verantwoordelijke de verwerkingen van persoonsgegevens waarvoor meld- of registratieplicht geldt bij in het daartoe bestemde register.

Artikel 13 Logboek datalekken
1. De functionaris voor gegevensbescherming houdt namens de verantwoordelijke een logboek bij waarin datalekken zijn opgenomen.
2. In het logboek worden in ieder geval de volgende gegevens vermeld:
a. Het onderwerp van het datalek.
b. De datum van het datalek;
c. De duur van het datalek;
d. de aard van de inbreuk;
e. de instanties waar meer informatie over de inbreuk kan worden verkregen;
f. de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk gevolgen te beperken.
g. een beschrijving van de gevolgen voor de verwerkte persoonsgegevens;
h. de maatregelen die de gemeente heeft getroffen of voorstelt te treffen om deze gevolgen te verhelpen;
i. de kennisgeving aan betrokkenen.

Artikel 14 Rechten betrokkene
1. De taken zoals omschreven in artikel 15 t/m 20 van de Verordening en volgende worden centraal uitgevoerd onder verantwoordelijkheid van de CIO.
2. Bij uitoefening van de taken wordt de functionaris voor gegevensbescherming betrokken.

3. Een betrokkene kan een verzoek in het kader van artikel 15 en verder van de Verordening ook via andere gangbare publieksdienstverleningskanalen van de gemeente Utrecht doen. Dit verzoek is geldig ongeacht het middel waarmee het verzoek wordt gedaan.

Artikel 15 Vervallen oude regeling
De Privacyverordening gemeente Utrecht (Gemeenteblad van Utrecht 2016, nr. 135657) komt op 25 mei 2018 van rechtswege te vervallen gelet op artikel 122 Gemeentewet.

Artikel 16 Inwerkingtreding
Deze verordening treedt, op grond van artikel 4 lid 2 Verordening Raadgevend Referendum, 5 weken na bekendmaking in werking.

Artikel 17 Citeertitel
Deze verordening wordt aangehaald als: Privacyverordening gemeente Utrecht.

Aldus besloten in de openbare vergadering van de raad, gehouden op 20 september 2018,
De griffier, De burgemeester,
mevr. Mr. M. van Hall J.H.C. van Zanen