

## Privacyverordening gemeente Utrecht

### VERORDENING VAN UTRECHT 2016, NR. 22 (raadsbesluit van 22 september 2016)

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 Wet bescherming persoonsgegevens (hierna: de Wet). De in de Wet 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, op grond van de Wet bevoegd om toe te zien op de verwerking van persoonsgegevens overeenkomstig het bij en krachtens de Wet bepaalde (voorheen: College bescherming persoonsgegevens).
  - c. CIO: Chief Information Officer, zijnde de concernmanager informatievoorziening en procesmanagement.
  - d. CISO: Chief Information Security Officer, zijnde het hoofd informatiebeveiliging, aangewezen door het college van burgemeester en wethouders.
  - e. Dataminimalisatie: alleen de informatie die noodzakelijk is voor de uitvoering van wettelijke taken wordt opgeslagen.
  - f. IRM-er: integraal resultaatsverantwoordelijk manager, verantwoordelijk voor een organisatieonderdeel van de gemeente Utrecht, of daarmee gelijk te stellen functies.
  - g. Privacy impact assessment (PIA): 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.
  - h. Pseudonimiseren: een procedure waarmee identificerende gegevens met behulp van een bepaald algoritme in een dataset worden vervangen door versleutelde gegevens (het pseudoniem).
  - 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 Verantwoordelijke

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

#### Artikel 3 Functionaris voor de gegevensbescherming

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

#### Artikel 4 Contactpersoon voor de gegevensbescherming

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 nieuwe of aangepaste verwerkingen in het licht van de meldplicht en andere verplichtingen.
- c. Het opstellen van en het houden van toezicht op het gebruik van privacyprotocollen voor verwerkingen die onder verantwoordelijkheid van het organisatieonderdeel plaatsvinden.
- d. De informatiebeveiliging van het organisatieonderdeel. Hieronder vallen in ieder geval:
  - i. Informatiebeveiligingsbeleid van Utrecht opnemen en doorvoeren in contracten met bewerkers en leveranciers;
  - ii. Alle handelingen aangaande de meldplicht datalekken die het organisatieonderdeel aangaan.

#### **Artikel 5 Privacy impact assessment (PIA)**

1. Voordat een beslissing wordt genomen over nieuwe of wijzigingen van bestaande bewerkingen, wordt door middel van een PIA aangetoond dat de privacy voldoende is gewaarborgd en worden de al dan niet te nemen maatregelen gemotiveerd.
2. De functionaris voor de gegevensbescherming geeft over de PIA een bindend advies.
3. De PIA 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 Wbp en deze verordening.
2. Een openbare 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 gemeente 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 gegevensbescherming die de aanvraag zal beoordelen in het kader van de wet en 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 in de openbare ruimte of waarbij de openbare ruimte geheel of gedeeltelijk in beeld wordt gebracht ten behoeve van de openbare orde of veiligheid 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 de 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 de gegevensbescherming en de CISO beoordelen of het datalek meldingswaardig is, als bedoeld in de Wet.
4. De functionaris voor de gegevensbescherming meldt een meldingswaardig datalek direct aan de Autoriteit Persoonsgegevens.
5. De IRM-er is verantwoordelijk voor de onverwijld 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 de gegevensbescherming over alle bevoegdheden die daarvoor redelijkerwijs noodzakelijk zijn. Ingeval van twijfel of verschil van mening daaromtrent beslist de functionaris voor de gegevensbescherming, de CIO gehoord hebbende.
2. De verantwoordelijke en de personen die bij een verwerking van persoonsgegevens zijn betrokken verstrekken desgevraagd de functionaris voor de gegevensbescherming alle inlichtingen en verlenen alle overige medewerking die hij voor de uitoefening van zijn taak behoeft.
3. De functionaris voor de gegevensbescherming heeft toegang tot alle ruimten, waar een verwerking van persoonsgegevens plaatsvindt. De functionaris voor de 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 de 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 de 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 de gegevensbescherming kan voor zijn onderzoek gebruik maken van de diensten van derden.
3. De functionaris voor de gegevensbescherming deelt zijn bevindingen aan de Verantwoordelijke mede en geeft zo nodig aanbevelingen.
4. De bevindingen van de functionaris voor de gegevensbescherming alsmede de aanbevelingen zijn naderhand te raadplegen via de website van de gemeente. De functionaris voor de gegevensbescherming kan dit achterwege laten vanwege dringende redenen.

### **Artikel 12 Openbaar register verwerkingen**

De functionaris voor de 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 de 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 35 van de Wet en volgende worden centraal uitgevoerd onder verantwoordelijkheid van de CIO.
2. Bij uitoefening van de taken wordt de functionaris voor de gegevensbescherming betrokken.
3. Een betrokkene kan een verzoek zoals beschreven in artikel 35 eerste lid van de Wet ook via andere gangbare publieksdienstverleningskanalen van de gemeente Utrecht doen.  
Dit verzoek is geldig ongeacht het middel waarmee het verzoek wordt gedaan.

#### **Artikel 15 Intrekking oude regeling**

Op het moment van inwerkingtreding van deze verordening wordt de Privacyverordening gemeente Utrecht (Gemeenteblad van Utrecht 2003, nr. 39) ingetrokken.

#### **Artikel 16 Inwerkingtreding**

Deze verordening treedt in werking met ingang van de dag na de datum van haar bekendmaking.

#### **Artikel 17 Citeertitel**

Deze verordening wordt aangehaald als: Privacyverordening gemeente Utrecht.

*Aldus besloten in de openbare vergadering van de raad, gehouden op 22 september 2016*

*De griffier,*

*mevr. Mr. M. van Hall*

*De burgemeester,*

*J.H.C. van Zanen*

## Toelichting

### Artikel 1 Definitie en begripsbepalingen

Pseudonimiseren is noodzakelijk indien datasets vergeleken moeten worden. Dit wordt bijvoorbeeld gedaan binnen het sociaal domein. De gemeente wil de zorg die wordt geboden door de instellingen controleren door gericht onderzoek waarbij vaak meerdere datasets worden gebruikt.

### Artikel 2 Verantwoordelijke

Het college van burgemeester en wethouders dan wel de burgemeester zijn, iedere vanuit hun eigen bevoegdheid, te allen tijde verantwoordelijke voor de verwerkingen en bewerkingen die door of namens de gemeente worden uitgevoerd.

### Artikel 3 Functionaris voor de gegevensbescherming

De gemeente heeft een functionaris voor de gegevensbescherming (FG) benoemd die verantwoordelijk is voor het toezicht op privacy en de borging er van. Hij kan het college van burgemeester en wethouders, de burgemeester en de gemeenteraad gevraagd en ongevraagd advies geven over privacy-aangelegenheden. De FG heeft verregaande bevoegdheden op grond van de Wbp. In artikel 63 lid 2 wordt zijn onafhankelijke rol benadrukt:

De functionaris kan wat betreft de uitoefening van zijn functie geen aanwijzingen ontvangen van de verantwoordelijke of van de organisatie die hem heeft benoemd. Hij ondervindt geen nadeel van de uitoefening van zijn taak. De verantwoordelijke stelt de functionaris in de gelegenheid zijn taak naar behoren te vervullen. De functionaris kan de kantonrechter verzoeken te bepalen dat de verantwoordelijke gevolgd dient te geven aan hetgeen in de tweede volzin is bepaald.

Hoewel de FG een eigen rol kent, treedt hij altijd in overleg met de CIO over geconstateerde gebreken of onjuistheden in het systeem van verwerkingen.

Tot de taken van de functionaris behoren in ieder geval:

- a. Toezicht op de verwerking van persoonsgegevens door de gemeente Utrecht.
- b. Gevraagd en ongevraagd signaleren, adviseren en informeren over zaken aangaande de Wet, deze verordening en overige onderwerpen die de privacy betreffen.
- c. Toezicht houden op het gemeentelijk privacy- en beveiligingsbeleid door middel van advisering en controles.
- d. Inventarisatie van de verwerkingsprocessen en beheren van meldingen van verwerkingen in het register van de AP.
- e. Verantwoordelijke voor de coördinatie van de werkprocessen in geval van datalekken en het beheren van het logboek inzake datalekken.
- f. Aanspreekpunt en contactpersoon aangaande privacy, zowel intern als extern.

### Artikel 4 Contactpersoon voor de gegevensbescherming

De contactpersoon voor de gegevensbescherming is iemand die werkzaam is binnen de gemeente onder verantwoordelijkheid van de IRM-er van een organisatieonderdeel. Hij is verantwoordelijk voor borging van de privacy en informatiebeveiliging bij het betreffende organisatieonderdeel. De contactpersonen hebben regelmatig overleg met de CISO en zorgen voor eenduidige uitvoering van het privacy- en informatiebeveiligingsbeleid door het organisatieonderdeel.

### Artikel 5 Privacy Impact Assessment (PIA)

Alvorens wordt besloten om een verwerking van persoonsgegevens aan te vangen of te wijzigen, wordt door het organisatieonderdeel een privacy impact assessment (PIA) uitgevoerd. Uitgangspunt bij een PIA is dat afhankelijk van de verwerking passende waarborgen worden ingebouwd (Privacy by design). Bij iedere verwerking van persoonsgegevens wordt dataminimalisatie toegepast. Daarnaast worden binnen die minimale dataset - waar mogelijk - de persoonsgegevens eerst geanonimiseerd en de overige persoonsgegevens worden gepseudonimiseerd. Deze keuzes worden onderbouwd voorgelegd aan de CISO, die mede beslist over de inhoud van de PIA.

De PIA legt in de eerste plaats de risico's bloot van projecten waarbinnen wordt gewerkt met persoonsgegevens, en het draagt bij aan het vermijden of verminderen van deze privacy risico's. Op basis van de antwoorden die worden gegeven in de PIA wordt op systematische wijze inzichtelijk gemaakt of er een kans is dat de privacy van de betrokkene wordt geschaad, hoe groot deze kans is en op welke gebieden dit speelt.

De PIA doet dit op een gestructureerde wijze:

- De mogelijk (negatieve) gevolgen van het gebruik van persoonsgegevens voor de betrokkenen personen en organisaties in kaart te brengen.
- De risico's voor de betrokken personen en organisaties zoveel mogelijk te lokaliseren.

Op basis van de uitkomsten van de PIA kan de gemeente gericht acties ondernemen om deze risico's te verminderen. Door het gebruik van de PIA kan bescherming van persoonsgegevens op een gestructureerde manier onderdeel uitmaken van de belangenafweging en besluitvorming over een project.

De PIA is openbaar met inachtneming van de Wet openbaarheid van bestuur. In ieder geval worden de volgende gegevens van verwerkingen via de website bekend gemaakt:

- a. de reden om de persoonsgegevens te bewaren;
- b. bewaartermijnen en een motivering waarom voor die bewaartermijn gekozen is met zo mogelijk een verwijzing naar het wettelijk kader;
- c. mogelijke uitzonderingen op de gekozen bewaartermijn met uiteenzetting van de voorwaarden waaronder langer bewaard kan worden;
- d. een verwijzing naar de persoon bij wie een betrokkene een verzoek kan indienen als hij in zake wil hebben in verwerkingen die hem aangaan;

Er zal gebruik worden gemaakt van de PIA die door de InformatieBeveiligingsDienst wordt aanbevolen. De IBD is onderdeel van het Kwaliteitsinstituut Nederlandse Gemeenten (van de VNG).

De FG ziet toe op het proces en geeft een bindend advies over de PIA.

#### Artikel 6 Open data

Om het begrip Open data te definiëren is aansluiting gezocht bij het Platform Open Data. Zij omschrijft open data als data die vrij gebruikt kunnen worden, hergebruikt kunnen worden en opnieuw verspreid kunnen worden door iedereen - onderworpen enkel, in het uiterste geval, aan de eis tot het toeschrijven en gelijk delen. Kenmerken van open data:

- Beschikbaarheid en Toegankelijkheid: De data moet in zijn geheel beschikbaar zijn, en voor niet-meer dan een redelijke productieprijs, bij voorkeur door middel van downloaden via het internet. De data moet ook beschikbaar zijn in een handige en modificeerbare vorm.
- Hergebruik en herverspreiding: de data moet aangeboden worden onder voorwaarden die hergebruik en herverspreiding toestaan, daarbij ook het samenvoegen met andere datasets inbegrepen.
- Universele deelname: iedereen moet kunnen gebruiken, hergebruiken en herverspreiden - er moet geen discriminatie bestaan tegen velden van een bepaalde onderneming, of tegen personen of groepen. Bijvoorbeeld, 'niet-commerciële' beperkingen die 'commerciële' gebruik voorkomen, of beperkingen voor het gebruiken van de data voor bepaalde doeleinden (e.g. alleen in het onderwijs), zijn niet toegestaan.

De gemeente heeft veel data die onder voorwaarden opengesteld kan worden voor een breed publiek. Hier zijn ook verschillende redenen voor aan te wijzen:

- data waar (overheids-)organisaties over beschikken vertegenwoordigen waarde voor anderen;
- veel verschillende groepen mensen en organisaties kunnen profiteren van de beschikbaarheid van open data, inclusief de overheid zelf;
- het is onmogelijk om precies te voorspellen hoe en waar de waarde van deze data zal ontstaan in de toekomst. De aard van innovatie is dat ontwikkelingen vaak uit onverwachte hoek komen.

Economisch gezien is open data ook van groot belang. Verscheidene onderzoeken hebben de economische waarde van open data geschat op miljarden Euro.

De overheid heeft ook een taak als het gaat om hergebruik van overheidsgegevens. In de Wet hergebruik van overheidsgegevens zijn voorwaarden bepaald waaronder hergebruik kan plaatsvinden.

De Privacyverordening 2016 stelt de eisen voor de gemeente Utrecht waaraan het gebruik van open data moet voldoen. Hergebruik is immers niet altijd wenselijk of toelaatbaar. Naast beperkingen door wet- en regelgeving is het ook niet de bedoeling dat gegevens waarin persoonsgegevens zijn verwerkt worden hergebruikt en daarmee beschikbaar gesteld als open data.

De gemeente biedt via een website inmiddels haar open data aan. Een afnemer moet van de status van de data uit kunnen gaan en dat de data voldoen aan bepaalde kwaliteitseisen. Dit is immers ook van belang voor de toepassing waarvoor hij de open data gebruikt. Er is geen wettelijke verplichting om datasets bij te houden en te actualiseren bij het aanbieden ervan. Daarom is in de Privacyverordening 2016 de verplichting opgenomen dat het betreffende organisatieonderdeel aangeeft welke status de dataset heeft.

#### Artikel 7 Big data en tracking

Dit artikel is bedoeld om de mogelijkheden van tracking en big data te kaderen voor de gemeente. Big data en tracking kunnen van onschatbare waarde zijn voor de organisatie. Het gebruik ervan mag echter niet leiden tot hetherleidbaar zijn van personen. Hierbij geldt de volgende volgorde: op een dataset vindt eerst dataminimalisatie plaats, vervolgens wordt anonimiseren zoveel mogelijk toegepast en alleen als het noodzakelijk is om datasets te vergelijken wordt pseudonimiseren toegepast. Doel van tracking is om publieksstromen (aantallen) in kaart te brengen en daarop eventuele regulerende maatregelen te kunnen treffen. Een voorbeeld hiervan is het kunnen monitoren en in goede banen leiden van grote publieksstromen tijdens Koningsdag (crowd management).

Voor big data en tracking is het niet nodig dat persoonsgegevens kenbaar zijn. Het is ook nadrukkelijk niet de bedoeling dat de persoonsgegevens voor andere doeleinden dan deze worden gebruikt. Big data en tracking van mobiele gegevensdragers wordt uitsluitend toegepast als de privacy van de individu

kan worden gewaarborgd. Daar waar gegevens tot personen herleidbare informatie leidt of kan leiden wordt deze informatie onherkenbaar gemaakt op zodanige wijze dat herleiding niet meer mogelijk is. Gelet op de grootschaligheid van big data biedt deze Verordening een extra waarborg voor de veilige verwerking van de persoonsgegevens. Het verzamelen van de (persoons)gegevens voor bigdata mag niet door dezelfde personen worden uitgevoerd als degenen die het onderzoek met behulp van die (gepseudonimiseerde) gegevens uitvoeren. De verzamelde gegevens worden geanonimiseerd of gepseudonimiseerd door de bronhouder, de geautoriseerde persoon namens gemeente. De versleutelde dataset wordt door de bronhouder aan de onderzoeker toegestuurd. De onderzoeker krijgt zodoende datasets die voorhem niet meer herleidbaar zijn naar persoonsgegevens. Hij krijgt geen beschikking over het (onversleutelde) brondocument.

Het verschil tussen anonimiseren en pseudonimiseren van persoonsgegevens ziet met name op de bruikbaarheid van deze gegevens voor het vergelijken van databestanden. Bij anonimiseren worden alle persoonsgegevens verwijderd uit de dataset. Hierdoor zijn personen, adressen of plaatsen niet meer te herleiden. Wanneer de gemeente uit verschillende datasets een analyse wil (laten) maken van een wijk is dat met een geanonimiseerde dataset niet mogelijk. De relevante gegevens zijn dan immers uit de dataset verdwenen. Dan is pseudonimisering noodzakelijk.

Bij pseudonimisering worden de persoonsgegevens (door toepassing van een algoritme) vervangen door bijvoorbeeld een nummer. Hierdoor zijn de persoonsgegevens niet meer te herleiden. Maar door toepassing van het algoritme kunnen wel meerdere datasets naast elkaar gebruikt worden voor een gerichte analyse van bijvoorbeeld een wijk, zonder dat er persoonsgegevens worden verwerkt. Ook voormeerjarige onderzoeken waarbij datasets over meerdere jaren vergeleken moeten worden biedt pseudonimisering de (enige) mogelijkheid om onderzoek veilig uit te voeren.

De geanonimiseerde en/of gepseudonimiseerde datasets zijn altijd kopieën van de bronbestanden. De gemeente heeft immers een wettelijke taak om bepaalde (persoons)gegevens te bewaren gedurende een langere termijn. Dat een dataset wordt geanonimiseerd en/of gepseudonimiseerd ten behoeve van een onderzoek gedurende die bewaartermijn doet daaraan niet af. Het is daarom niet toegestaan om het bronbestand na anonimisering te vernietigen. Uitsluitend na ommekomst van de bewaartermijn wordt het bronbestand vernietigd.

#### Artikel 8 Cameratoezicht en camerabewaking

Cameratoezicht vindt plaats op basis van artikel 151 subc van de Gemeentewet. Hoe Utrecht hiermee omgaat is uitgewerkt in het "Beleidskader cameratoezicht". Deze verordening zet het beleidskader niet opzij. Enkel wordt door lid 1 van artikel 8 verduidelijkt dat er sprake kan zijn van cameratoezicht, met een wettelijke basis. Een uitsnede van het Beleidskader cameratoezicht:

"De inzet van cameratoezicht moet evenredig zijn in relatie tot het doel (proportionaliteit) en mag nooit eendoel op zich zijn. Het inzetten van cameratoezicht is één van de zwaarste middelen dat in aanvulling op een pakket aan maatregelen kan worden ingezet. Vast moet staan dat het doel niet op een minder ingrijpende wijze kan worden bereikt (subsidiariteit). Door een analyse te maken van de veiligheidssituatie van een locatie wordt bekeken welke maatregelen een bijdrage kunnen leveren om het probleem aan te pakken. Het inzetten van cameratoezicht is altijd een besluit van de burgemeester, afgestemd met de Driehoek (burgemeester, hoofd van politie, officier van justitie). Het is een tijdelijke maatregel waarbij periodiek wordt geëvalueerd waar de camera's hangen, met welk doel ze op die locatie geplaatst zijn en of zij nog steeds bijdragen aan dat doel. Die doelen zijn maatwerk en verschillen per gebied. Het cameratoezicht in Utrecht voldoet aan alle wettelijke richtlijnen die voor deze inzet gelden (zie: wettelijke richtlijnen p. 15). De camerabeelden zijn door fysieke, softwarematige en organisatorische maatregelen beveiligd. Ze mogen alleen onder directe politieaansturing door een kleine groep opgeleide en gescreende functionarissen worden bekeken. De beelden worden 28 dagen opgeslagen en daarna automatisch gewist. In die 28 dagen kan de politie beelden van strafbare feiten terugzoeken en gebruiken voor opsporing. Met de camera's kan niet in woningen worden gekeken. Er wordt met software een grijs vlak over de woning gelegd dat meedraait als de camera beweegt ('blinking'). Opgeslagen beelden vallen onder de Wet Politiegegevens."

Naast toezicht camera's zijn er ook talloze andere camera's. Bijvoorbeeld camera's ter bewaking van eigendommen, verkeerstelcamera's, camera's voor de ingang van een parkeergarage, kentekenherkenningscamera's, etc.

Camerabewaking in iemands eigendom is altijd mogelijk: kom je als dief een huis binnen dan moet je niet raar opkijken als je gefilmd wordt. Anders wordt het als de openbare ruimte wordt mee gefilmd en persoonsgegevens op die manier worden verkregen. De openbare ruimte is van iedereen maar de eigendom ervan ligt veelal bij de gemeente.

Omdat bij camerabewaking vaak ook (een deel van) de openbare weg wordt gefilmd is de gemeente partij. Zij moet voor het filmen toestemming verlenen en daarbij komt dat die toestemming niet altijd wettelijk geregeld is (doelbinding). De gemeente moet verzoeken van bedrijvencollectieven, winkelcentra en gelijke partijen om camerabewaking te installeren afwegen aan de hand van alle

belangen en de Wet. Bij bijvoorbeeld bedrijvencollectieven die bedrijventerreinen laten filmen ter voorkoming van vernieling en diefstal speelt het algemeen belang een rol. Hier kan de gemeente worden gevraagd om toestemming voor het filmen van een deel van de openbare ruimte.

Om voor de inwoners duidelijkheid te geven hoe omgegaan wordt met camerabewaking in de openbare ruimte moet een kader worden gesteld. Gekozen is om een convenant verplicht te stellen zodat voor gemeente altijd duidelijk is wat een camera doet in een bepaald gebied.

Deaanvragers kunnen een cameraplan overleggen met een motivering waarom camerabewaking voor het gevraagde doel past binnen de Wet en de Privacyverordening 2016. Omdat het openbare ruimte betreft moeten de aanvragers ook de voorwaarden van de gemeente volgen die op de camerabewaking van toepassing worden. Daarom wordt altijd eenconvenant gesloten indien er sprake is van camerabewaking door derden waarbij de openbare ruimte wordt gefilmd.

Voorwaarden kunnen bijvoorbeeld zijn: bij het gebruik van camera's in combinatie met opslag van het beeldmateriaal is in veel gevallen sprake van het verwerken van persoonsgegevens. Hierbij wordt de duur van de opslag van de verzamelde beelden in tijd zodanig beperkt dat dit overeenkomt met het doel van de verwerking.

Bij inzet van camera's moet voorafgaand aan de plaatsing worden bepaald voor welk doel de camera wordt ingezet, de duur van de inzet, de bewaartermijn van de beelden alsmede de toegang tot de beelden. Beelden zijn uitsluitend toegankelijk voor hiertoe geautoriseerde personen en worden niet aan anderen verstrekt.

Alleenindien beelden dusdanig vaag worden opgeslagen waardoor directe of indirecte herkenning van personen niet meer mogelijk is (ook niet door middel van achteraf uit te voeren beeldverbeteringstechnieken) is er geen sprake van verwerken van persoonsgegevens.

Ook bij camera inzet voor andere gemeentelijke doeleinden dient voorafgaand aan deze inzet de impact op de privacy duidelijk te zijn. Bijvoorbeeld als bij verkeerskundig onderzoek gebruik wordt gemaakt van camera's.

#### Artikel 9 Datalek

Op 1 januari 2016 is de Wet bescherming persoonsgegevens gewijzigd als gevolg van de Wet meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid van de Autoriteit Persoonsgegevens (hierna te noemen AP). Belangrijk gevolg hiervan is dat organisaties verplicht zijn om een inbreuk op de beveiliging te melden, wanneer het lekken een ernstig nadelig gevolg kan hebben op de bescherming van verwerkte persoonsgegevens. De melding moet aan de AP worden gedaan. In sommige gevallen moeten zelfs de betrokkenen op de hoogte worden gebracht wiens persoonsgegevens zijn gelekt, namelijk als de inbreuk ongunstige gevolgen voor de betrokkenen met zich mee brengt. Indien de regels niet of onvoldoende worden nageleefd kan de AP een forse boete opleggen.

Zowel private als publieke organisaties worden verplicht om inbreuken in de beveiliging die leiden tot verlies, misbruik of diefstal, te melden bij de AP, indien het lekken een ernstig nadelig gevolg kan hebben op de bescherming van verwerkte persoonsgegevens. Melding dient binnen 72 uur plaats te vinden. Melden mag ook later maar dan moet gemotiveerd worden waarom de melding is uitgesteld. Daarnaast moet ook degene wiens persoonsgegevens het betreft een melding krijgen, wanneer er (waarschijnlijk) sprake zal zijn van ongunstige gevolgen voor zijn/haar privacy.

#### Wat is een datalek?

Er is sprake van een datalek als het gaat om een beveiligingslek waarbij persoonsgegevens in handen vallen van derden die geen toegang tot diepersoonsgegevens zouden mogen hebben. Persoonsgegevens zijn alle gegevens die direct of indirect naar personen zijn te herleiden. Een datalek is het gevolg van een beveiligingsprobleem of een gebruikersfout. In de meeste gevallen gaat het om uitgelekte computerbestanden, al kan een gestolen geprinte klantenlijst evengoed een datalek vormen. Illegaal verkregen bedrijfsgegevens over een productieproces of marktstrategie betreffen kostbare informatie, maar vallen niet onder de gangbare definitie van datalek.

#### Wanneer is er sprake van inbreuk op de beveiliging?

Een inbreuk op de beveiliging hoeft niet te betekenen dat de beveiliging is tekortgeschoten. Denkbaar is dat de beveiliging op zich van voldoende niveau is, maar dat de beveiligingsmaatregelen worden omzeild. In de toelichting bij de wet worden als voorbeeld genoemd: een hack van een ICT-systeem dat persoonsgegevens bevat en de diefstal van een laptop of mobiele telefoon uit een afgesloten kluisje. Daarnaast kan de inbreuk op de beveiliging het gevolg zijn van een tekortschietende beveiliging. Dat is bijvoorbeeld het geval als bepaalde bestanden niet goed beveiligd zijn geweest of als er menselijke fouten zijn gemaakt.

Als voorbeelden kunnen worden genoemd: het slordig omgaan met wachtwoorden, papieren dossiers die als oud papier worden aangeboden, het kwijtraken van apparaten of gegevensdragers met privacygevoelige informatie, een USB-stick, laptop, tablet, telefoon. Ook het onversleuteld elektronisch uitwisselen van privacygevoelige informatie valt hieronder, bijvoorbeeld via e-mail of andere onbeveiligde verbindingen.

Op de hierboven genoemde situaties is de meldplicht van toepassing. Uitsluitend wanneer de getroffen voorzieningen niet specifiek bedoeld zijn voor de beveiliging van persoonsgegevens hoeft geen mel-



ding te worden gedaan. In de toelichting bij de wet wordt het voorbeeld genoemd van een gebouw dat afbrandt als gevolg van blikseminslag, waarbij persoonsgegevens verloren zijn gegaan.

Degemeente verwerkt veel persoonsgegevens van inwoners om haar taken uit te kunnen oefenen. Inwoners hebben recht op bescherming van hun persoonsgegevens. Daarom is de gemeente verplicht om persoonsgegevens goed te beveiligen. Met de meldplicht wordt bijgedragen aan het behoud en herstel van vertrouwen in de omgang met persoonsgegevens.

Ook voor partijen die in opdracht van de gemeente persoonsgegevens verwerken (bewerkers) brengt dewet indirect verplichtingen met zich mee. Denk bijvoorbeeld aan leveranciers van ICT-systemen.

Hierdienen schriftelijke afspraken over te zijn gemaakt, zodat bij een eventueel datalek de gemeente onmiddellijk wordt ingelicht door de dienstverlener teneinde te bepalen of er daadwerkelijk een datalekmelding moet worden gedaan. De leverancier zal de gemeente dan per ommegaande moeten waarschuwen als zij een inbreuk vaststelt.

De Autoriteit Persoonsgegevens kan bij nalatigheid om aan haar te melden, een boete opleggen als genoemd in artikel 66 van de wet.

NB: deze boete staat los vande boete die geldt voor het dataleken zelf. Afhankelijk van de aard en omvang van het datalek kan de AP hiervoor een boete opleggen als genoemd in artikel 66 vande wet.

#### Wie meldt een datalek?

Iedereen kan aan de gemeente Utrecht een datalek melden. Zowel interne medewerkers als andere personen die een mogelijk datalek constateren kunnen via de website van de gemeente Utrecht een melding doen via een daarvoor gecreëerde link naar een invultabel.

#### Meldingsplicht of niet

Niet elk datalek moet bij de AP worden gemeld. Nodeloze meldingen moeten worden voorkomen. Er dient aan bepaalde criteria te worden voldaan. De FG zal samen met de CISO bepalen of een melding aande AP noodzakelijk is aan de hand van criteria die door de AP zijn vastgesteld.

DeFG houdt een overzicht bij van de datalekken. Dit overzicht wordt, vanuit archief technisch oogpunt, permanent bewaard. De meldingsdossiers (meldingsformulier en andere relevante stukken) over de datalekken worden gedurende zeven jaar na het vervallen van het belang bewaard.

#### Artikel 10 Toezicht

DeFG is belast met het toezicht op alle privacyaspecten binnen de gemeente Utrecht. Hij beoordeelt zelfstandig of de gemeente voldoet aan de Wet en deze verordening. Zijn bevoegdheden zijn verstrekkend, hij kan in het uiterste geval een beslissing overrulen. Dit zal alleen het geval zijn als duidelijk is dat de Autoriteit Persoonsgegevens ook niet kan instemmen met de betreffende beslissing op privacy gebied.

De FG zal bij een privacy issue altijd eerst via de lijn proberen de situatie op te lossen. Vervolgens zal de IRM-er worden gevraagd de beslissing aan te passen en ten slotte zal interventie plaatsvinden met degemeentesecretaris. Hoewel de FG een eigen rol kent, treedt hij wel altijd in overleg met de CIO over geconstateerde gebreken of onjuistheden in het systeem van verwerkingen.

#### Artikel 11 Onderzoek

De FG kan een onderzoek instellen naar (schendingen van) privacyaspecten door de gemeente Utrecht. Hij kan hiervoor derden inschakelen die vertrouwelijk met de persoonsgegevenskwestie om kunnen gaan, zoals bijvoorbeeld een accountant die vanuit zijn professie een geheimhoudingsplicht kent. Het onderzoek en mogelijke aanbevelingen worden openbaar gemaakt via de website. Er kunnen dringende redenen zijn om openbaarmaking voorsnog achterwege te laten, zoals bijvoorbeeld in het geval het college eerst verregaande maatregelen moet treffen om een mogelijke privacy schending te voorkomen.

#### Artikel 12 Openbaar register verwerkingen

Aan de Autoriteit Persoonsgegevens worden op dit moment nieuwe verwerkingen gemeld. Deze worden op de lijst van verwerkingen geplaatst bij de AP. Als het op grond van de AVG verplicht wordt om zelf deze verwerkingen op een lijst te plaatsen dan kan dat ook.

#### Artikel 13 Logboek datalekken

De FG houdt samen me de CISO een logboek bij van datalekken. Het logboekis openbaar. De FG houdt bij opname in het register rekening met de belangen die bij openbaarmaking zijn gemoeid. Er kunnen bijvoorbeeld redenen zijn omopenbaarmaking aan te houden, zoals bijvoorbeeld bij een ernstig datalek dat eerst moet worden gedicht.

#### Artikel 14 Rechten betrokkene

Betrokkenen kunnen de gemeente verzoeken om inzage te geven in de verwerkingen van hun persoonsgegevens. Dit kan zowel schriftelijk als via een door de gemeente in te richten website met informatie over de verwerking van persoonsgegevens door gemeente. Op deze site zullen naast de PIA's, meldingen van verwerkingen en logboeken van datalekken, ook een pagina worden toegevoegd



waarmee betrokkenen actief kunnen communiceren met de gemeente over privacy-aangelegenheden. Op die manier kunnen meldingen van vermeende datalekken, vragen over PIA's, klachten, rechten als opvragen, wijziging, vernietiging van persoonsgegevens ook laagdrempelig worden gedaan.