DCMR milieudienst Rijnmond

BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 797
17 oktober 2019

Officiële uitgave van de gemeenschappelijke regeling DCMR Milieudienst Rijnmond

Privacybeleid DCMR Milieudienst Rijnmond Vastgesteld DB 26 september 2019

Inhoud

1. Inleiding

Binnen de DCMR Milieudienst Rijnmond (hierna DCMR) wordt gewerkt met persoonsgegevens van burgers, medewerkers en (keten)partners. Persoonsgegevens worden voornamelijk verzameld bij bedrijven en de burgers voor het goed uitvoeren van de wettelijke taken die de DCMR voor zijn opdrachtgevers uitvoert. De betrokkenen moeten erop kunnen vertrouwen dat de DCMR zorgvuldig en veilig met de persoonsgegevens omgaat.

In deze tijd gaat ook de DCMR mee met nieuwe ontwikkelingen. Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds meer digitale overheid stellen andere eisen aan de bescherming van gegevens en privacy. De DCMR is zich hiervan bewust en zorgt dat de privacy gewaarborgd blijft, onder andere door maatregelen op het gebied van informatiebeveiliging, dataminimalisatie, transparantie en gebruikerscontrole.

2. Reikwijdte

Het bestuur en management spelen een cruciale rol bij het waarborgen van privacy. De DCMR geeft door dit beleid richting aan de aanpak van privacy en laat zien dat zij de privacy waarborgt, beschermt en handhaaft.

Dit beleid is van toepassing op de verwerking van persoonsgegevens waarvoor de DCMR verantwoordelijk is, waaronder alle processen, onderdelen, objecten en gegevensverzamelingen van de DCMR.

3. Wettelijke kaders voor het omgaan met gegevens

De DCMR is verantwoordelijk voor het opstellen, uitvoeren en handhaven van het privacybeleid. Hiervoor gelden onder andere de volgende wettelijke kaders:

- De Algemene Verordening Gegevensbescherming (AVG);
- Uitvoeringswet Algemene Verordening Gegevensbescherming;
- Wet politiegegevens.

4. Verwerkingsverantwoordelijke

De AVG legt verplichtingen op aan de verwerkingsverantwoordelijke (degene die, alleen of samen met anderen, het doel en de middelen voor de verwerking van persoonsgegevens vaststelt) en de verwerker (degene die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt).

Gelet op het feit dat de DCMR in mandaat taken voor de deelnemers uitvoert, zou de vraag kunnen rijzen of de DCMR niet een verwerker is van de deelnemers. Om de volgende redenen beschouwen wij de DCMR als verwerkingsverantwoordelijke:

- de taken die de deelnemers bij de DCMR hebben neergelegd, betreffen niet het verwerken van persoonsgegevens op zichzelf. De DCMR wordt (moet worden) ingeschakeld vanwege haar expertise. Dat bij het uitvoeren van die taken persoonsgegevens worden verwerkt is een bijkomstigheid;
- de DCMR treedt naar buiten toe met een eigen gezicht en onder eigen naam op. Het beeld naar buiten zal daarom zijn dat de DCMR zelfstandig optreedt en 'verantwoordelijk' is.

DCMR beschouwt zich daarom als verwerkingsverantwoordelijke voor de verwerkingen van persoonsgegevens die door of namens de DCMR worden uitgevoerd.

5. Verplichtingen DCMR op grond van AVG

De verplichtingen die voor de DCMR voortvloeien uit de AVG zijn de volgende:

1. Het treffen van passende technische en organisatorische maatregelen:
a. Om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met de AVG wordt uitgevoerd. De maatregelen worden geëvalueerd en indien nodig geactualiseerd (plan-do-check-act). Gelet op de aard en omvang van de verwerkingsactiviteiten omvatten de maatregelen die de DCMR moet treffen ook een passend gegevensbeschermingsbeleid;
b. Die voldoen aan de beginselen van gegevensbescherming door ontwerp en gegevensbescherming door standaardinstellingen (privacy by design en by default);
c. Om een op het risico afgestemd beveiligingsniveau te waarborgen;
2. In geval een verwerker wordt ingeschakeld voor de verwerking van persoonsgegevens van de verwerkingsverantwoordelijke, het selecteren van een 'capabele' verwerker en het sluiten van een overeenkomst daarmee die voldoet aan de eisen van de AVG;
3. Het houden van een register van verwerkingsactiviteiten;
4. Het aanstellen van een functionaris voor gegevensbescherming;
5. Meldplicht datalekken (melding niet altijd verplicht);
6. Het uitvoeren van een gegevensbeschermingseffectbeoordeling van een nieuwe verwerking die waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van betrokkenen.

6. Uitgangspunten

De DCMR gaat op een veilige manier met persoonsgegevens om en respecteert de privacy van betrokkenen. De DCMR houdt zich hierbij aan de volgende - in de AVG vastgelegde - uitgangspunten:

Rechtmatigheid, behoorlijkheid, transparantie
Persoonsgegevens worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt.

Grondslag en doelbinding

De DCMR zorgt ervoor dat persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen worden verzameld en verwerkt. Persoonsgegevens worden alleen met een rechtvaardige grondslag verwerkt.

Dataminimalisatie
De DCMR verwerkt alleen de persoonsgegevens die minimaal noodzakelijk zijn voor het vooraf bepaalde doel. De DCMR streeft naar minimale gegevensverwerking. Waar mogelijk worden minder of geen persoonsgegevens verwerkt.

Bewaartermijnen
Persoonsgegevens worden niet langer bewaard dan nodig is. Het bewaren van persoonsgegevens kan nodig zijn om de DCMR-taken goed uit te kunnen oefenen of om wettelijke verplichtingen te kunnen naleven

Delen met derden
In het geval van samenwerking met externe partijen, waarbij sprake is van gegevensverwerking van persoonsgegevens, maakt de DCMR afspraken over de eisen waar gegevensuitwisseling aan moet voldoen. Deze afspraken voldoen aan de wet. De DCMR controleert of verwerkers van de DCMR de afspraken naleven.

Integriteit en vertrouwelijkheid

De DCMR gaat zorgvuldig om met persoonsgegevens en behandelt deze vertrouwelijk. Zo worden persoonsgegevens alleen verwerkt door personen met een geheimhoudingsplicht en voor het doel waarvoor deze gegevens zijn verzameld. Daarbij zorgt de DCMR voor passende beveiliging van persoonsgegevens.

Subsidiariteit en propor tionaliteit

De persoonsgegevens worden alleen verwerkt voor zover noodzakelijk voor het te bereiken doel. De inbreuk op de persoonlijke levenssfeer van de betrokken burger wordt zoveel mogelijk beperkt. De inbreuk op de belangen van de betrokkene is niet onevenredig in verhouding tot en met de verwerking te dienen doel.

7. Taken en verantwoordelijkheden

*

*) Wie	Verantwoordelijkheid
Algemeen bestuur	Het Algemeen bestuur oefent de controlefunctie uit en kan vanuit die rol controleren of de privacyregels en het privacybeleid worden nageleefd.
Dagelijks bestuur	Bestuurlijk verantwoordelijk voor het naleven van de privacyregels en het privacybeleid. Het dagelijks bestuur stelt het privacybeleid van de DCMR vast. Tenminste een keer per jaar is privacy een agendapunt in de vergadering van het dagelijks bestuur.
Directeur	De directeur is ambtelijk eindverantwoordelijk voor de verwerking van persoonsgegevens binnen de DCMR. Hij draagt zorg dat de organisatie voldoet en blijft voldoen aan de privacyregels en het privacybeleid en draagt zorg voor periodieke evaluatie. De directeur is het aanspreekpunt voor de FG.
Afdelingshoofden	De afdelingshoofden zijn verantwoordelijk voor de verwerking van persoonsgegevens overeenkomstig de AVG en het privacybeleid binnen hun afdeling.
Bureauhoofden	De bureauhoofden: zien toe op het naleven van de privacyregels en het gegevensbeschermingsbeleid binnen het bureau; dragen bij aan de bewustwording van het belang van gegevensbescherming bij medewerkers onder meer door privacy periodiek tijdens het bureauoverleg aan de orde te stellen; signaleren risico's, zwakke plekken in de beveiliging; dragen zorg voor bescherming digitale personele gegevens; dragen zorg voor de juiste autorisatie medewerkers t.b.v. toegang tot systemen; melden nieuwe verwerkingen bij het kernteam bescherming persoonsgegevens voordat met de nieuwe verwerking wordt gestart.
Systeemeigenaren	De systeemeigenaren dragen zorg voor de passende beveiligingsmaatregelen en signaleren beveiligingsrisico's met betrekking tot de betreffende systemen.
Medewerkers	De medewerkers: zorgen ervoor dat zij persoonsgegevens zorgvuldig verwerken in overeenstemming met het privacybeleid en de 10 regels voor privacybewustzijn; melden beveiligings- en datalekken wanneer zij deze signaleren; zijn op de hoogte van de regels van de DCMR voor privacybewustzijn
Kernteam bescherming persoonsgegevens	Binnen de DCMR functioneert het kernteam als eerste aanspreekpunt voor vragen, meldingen over privacy waaronder datalekken en nieuwe verwerkingen. Zij vormt het voorportaal voor de FG en beoordeelt welke punten direct door het kernteam kunnen worden opgepakt dan wel of deze moeten worden besproken met de FG. Het kernteam volgt de ontwikkelingen binnen de DCMR op het gebied van gegevensbewerkingen en draagt zorg voor: het afhandelen van verzoeken van betrokkenen; het actualiseren van het verwerkingenregister; het beoordelen of voorafgaand aan een nieuwe verwerking een gegevensbeschermingseffectbeoordeling moet worden uitgevoerd; het opstellen en adviseren over het selecteren van verwerkers en het aangaan van verwerkersovereenkomsten; het gevraagd en ongevraagd adviseren van de organisatie m.b.t. de bescherming van persoonsgegevens. Het kernteam is bemenst door de Juridisch controller, beleidsadviseur Personeel en Organisatie, adviseur Recordsmanagement, een Informatiebeveiligingsfunctionaris (ISO) en een Informatiemanager. Het kernteam komt periodiek bijeen onder voorzitterschap van de FG.
Functionaris voor gegevensbescherming	De DCMR heeft een FG aangesteld. De FG is betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. De taken van de functionaris zijn vastgelegd in de AVG en omvatten het informeren, adviseren, toezicht houden, bewustwording creëren, en optreden als contactpersoon van het Autoriteit persoonsgegevens.

8. Treffen van passende en organisatorische maatregelen

De DCMR draagt zorg voor het treffen van passende technische en organisatorische maatregelen:

a. Om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met de AVG wordt uitgevoerd. De maatregelen worden geëvalueerd en indien nodig geactualiseerd (plan-do-check-act).
b. Die voldoen aan de beginselen van gegevensbescherming door ontwerp en gegevensbescherming door standaardinstellingen (privacy by design en by default);
c. Om een op het risico afgestemd beveiligingsniveau te waarborgen;

Deze maatregelen zijn vastgelegd in het Beveiligingsbeleid DCMR.

9. Doorgifte

De DCMR geeft geen persoonsgegevens door met een land buiten de Europese Economische Ruimte (EER) of een internationale organisatie.

10. Bewaartermijnen

De DCMR bewaart de persoonsgegevens niet langer dan nodig is voor de uitvoering van zijn taken, of zoals vastgelegd in de selectielijsten conform de archiefwet.
Wanneer er nog persoonsgegevens opgeslagen zijn die niet langer nodig zijn voor het bereiken van het doel, 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.
De DCMR heeft de bewaartermijn vastgelegd in het register van verwerkingen.

11. **Inschakeling externe partijen, waaronder verwerkers**

Voor het inschakelen van externe partijen geldt het volgende:

- De verwerkingsverantwoordelijke gaat alleen in zee met 'capabele' verwerkers. Deze verwerkers bieden afdoende garanties met betrekking tot het toepassen van passende technische en organisatorische maatregelen.
- In het geval een verwerker wordt ingeschakeld wordt gehandeld in overeenstemming met het bepaalde in de AVG en wordt een verwerkersovereenkomst gesloten;
- Er is in contracten met externe partijen vastgelegd welke beveiligingsmaatregelen vereist zijn, dat deze door de externe partij zijn getroffen en worden nageleefd en dat beveiligingsincidenten onmiddellijk worden gerapporteerd. Ook wordt beschreven hoe die beveiligingsmaatregelen door de uitbestedende partij te controleren zijn (bijvoorbeeld audits en penetratietesten) en hoe het toezicht is geregeld.
- Er wordt een geheimhoudingsplicht opgelegd aan externe partijen en hun medewerkers die betrokken zijn bij de verwerking van persoonsgegevens van DCMR.
- Voorafgaand aan het afsluiten van een contract voor uitbesteding of externe inhuur is bepaald welke toegang (fysiek, netwerk of tot gegevens) de externe partij(en) moet(en) hebben om de in het contract overeen te komen opdracht uit te voeren en welke noodzakelijke beveiligingsmaatregelen hiervoor nodig zijn.

De verwerkers van DCMR zijn opgenomen in het register van verwerkingen.

12. **Informatie, toegang tot persoonsgegevens, uitoefening rechten betrokkenen**

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.

De taken en verantwoordelijkheden van de FG zijn in ieder geval:
Het informeren en adviseren van het bestuur en de directie en de verwerkers die namens de DCMR persoonsgegevens verwerken over hun verplichtingen uit hoofde van de AVG en andere EU wet- en regelgeving en nationale bepalingen over gegevensbescherming;
Het toezien op naleving van AVG, en andere EU wet- en regelgeving en nationale bepalingen betreffende gegevensbescherming;
Het toezien op naleving van het privacybeleid of de verwerker met betrekking tot de bescherming van persoonsgegevens;
Het toezien op toewijzing van verantwoordelijkheden, bewustmaking en opleiding van het bij de verwerking betrokken personeel en de betreffende audits;
Het geven van advies met betrekking tot de Privacy Impact Assessment (PIA) en het toezien of de uitvoering daarvan in overeenstemming is met de AVG.
Het samenwerken met de Autoriteit Persoonsgegevens;
Het optreden als contactpunt voor de Autoriteit Persoonsgegevens.

Op onze website is de privacyverklaring beschikbaar. Hiermee wordt voldaan aan onze informatieplicht. In de privacyverklaring wijzen we op de mogelijkheid voor betrokkenen hun rechten uit te oefenen. Wanneer een betrokkene een beroep doet op zijn rechten wordt het verzoek doorgestuurd naar het kernteam bescherming persoonsgegevens. Dit team draagt zorg voor de afhandeling.

Betrokkenen kunnen op grond van de AVG de volgende rechten uitoefenen:

- recht van inzage
- recht op rectificatie
- recht op wissen van gegevens
- recht op beperking van de verwerking
- recht van bezwaar
- recht op overdraagbaarheid
- recht om niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking gebaseerd besluit

Het recht op overdraagbaarheid geldt alleen wanneer de verwerking van persoonsgegevens plaatsvindt met toestemming van de betrokkene of op grond van een overeenkomst.
Betreft het persoonsgegevens die zijn verwerkt in het kader van bijvoorbeeld vergunningverlening of handhaving, dan bestaat het recht op overdraagbaarheid niet. Omdat binnen de DCMR geen sprake is van geautomatiseerde individuele besluitvorming, zal in de praktijk geen beroep op dit recht worden gedaan.

13. Verwerkingenregister

Een register is verplicht voor ondernemingen die tenminste 250 personen in dienst hebben. De DCMR heeft meer dan 250 personen in dienst en houdt dan ook een register bij.

14. Meldplicht datalekken

Datalekken hoeven niet altijd gemeld te worden bij de Autoriteit Persoonsgegevens (AP) of de betrokkenen. Alle datalekken worden wel gelogd.

15. Aanstellen functionaris voor gegevensbescherming

Overheidsinstanties en publieke organisaties zijn verplicht een functionaris voor gegevens-bescherming aan te stellen, onafhankelijk van het type gegevens dat ze verwerken.
Met een gegevensbeschermingseffectbeoordeling - ook wel privacy impact analyse (PIA) genoemd - worden de effecten en risico's van nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy.

De DCMR voert deze uit wanneer er een geautomatiseerde verwerking, een grootschalige verwerking, of wanneer er een grootschalige monitoring van openbare ruimten plaatsvindt. Dit geldt in het bijzonder bij verwerkingen waarbij nieuwe technologieën worden gebruikt.

DCMR maakt geen gebruik van profilering.
Het gegevensbeschermingsbeleid wordt tweejaarlijks geëvalueerd en zo nodig bijgesteld. Wanneer de omstandigheden daartoe aanleiding geven, zal het beleid ook tussentijds worden bijgesteld.

Aldus vastgesteld door het Dagelijks Bestuur van de DCMR Milieudienst Rijnmond

op 26 september 2019

De secretaris, De voorzitter,

M.M.H. de Hoog A.W. Bom-Lemstra