gemeente eijsden-margraten

GEMEENTEBLAD

Officiële uitgave van de gemeente Eijsden-Margraten

Nr. 109639

25 mei

2018

Rectificatie Besluit van het college van burgemeester en wethouders van de gemeente Eijsden-Margraten houdende regels omtrent privacybeleid Privacybeleid gemeente Eijsden-Margraten 2018

1. Inleiding

1.1 Algemeen

Overheidsorganisaties verzamelen en gebruiken veel persoonsgegevens, noodzakelijk voor hun taakuitvoering en zijn verantwoordelijk voor de bescherming van deze persoonsgegevens.

De bescherming van persoonsgegevens speelt een steeds belangrijkere rol door de:

- technologie die zich steeds sneller ontwikkelt;
- toename in dataverkeer;
- toename in het verzamelen en delen van gegevens;
- risico's van cybercrime;
- samenleving die steeds kritischer wordt;
- behoefte en rechten van inwoners om inzicht in de verwerking van zijn of haar persoonsgegevens;
- toename van de hoeveelheid gevoelige informatie van personen (bijvoorbeeld jeugdzorg, maatschappelijke ondersteuning, de zorg voor chronisch zieken, ouderen en gehandicapten, leerlingzaken).

Iedereen heeft recht op correcte, veilige en betrouwbare informatieverwerking en moet erop kunnen vertrouwen dat de gemeente zorgvuldig met deze gegevens omgaat.

1.2 Reikwijdte en afbakening privacy

Binnen de gemeente Eijsden-Margraten wordt veel gewerkt met persoonsgegevens van burgers, medewerkers en (keten)partners. Persoonsgegevens worden voornamelijk verzameld bij de inwoners voor het goed uitvoeren van de gemeentelijke wettelijke taken. Men moet erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig met de persoonsgegevens omgaat. In deze tijd gaat ook de gemeente 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 gemeente is zich hier van bewust en zorgt dat de privacy gewaarborgd blijft, onder andere door maatregelen op het gebied van informatiebeveiliging, dataminimalisatie, transparantie en gebruikerscontrole. Het bestuur en management spelen een cruciale rol bij het waarborgen van privacy.

De gemeente Eijsden-Margraten geeft middels dit beleid een duidelijke richting aan privacy en laat zien dat zij de privacy waarborgt, beschermt en handhaaft. Dit beleid is van toepassing op de gehele organisatie, alle processen, onderdelen, objecten en gegevensverzamelingen van de gemeente. Dit privacybeleid van gemeente Eijsden-Margraten is in lijn met het algemene beleid van de gemeente en de relevante lokale, regionale, nationale en Europese wet- en regelgeving.

Onder persoonsgegevens verstaan we alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"). Dit betekent dat informatie direct over iemand gaat of naar deze persoon te herleiden is.

Er is al snel sprake van 'verwerken' van persoonsgegevens. Verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, combineren, afschermen, wissen of vernietigen van gegevens valt allemaal onder het verwerken van persoonsgegevens.

Verdere definities met betrekking tot de verwerking van persoonsgegevens zijn opgenomen in de Algemene Verordening Gegevensbescherming (hierna te noemen: de AVG).

1.3 Scope

Het privacybeleid is van toepassing op:

- alle processen en informatiesystemen waarbinnen persoonsgegevens worden verwerkt;

- alle ruimten en devices die door gemeenteambtenaren worden gebruikt waar(op) persoonsgegevens worden verwerkt;
- alle geldende normen en regels op het gebied van privacy.

1.4 Opbouw privacybeleid

Het privacybeleid geldt als algemeen beleid, waarin de kaders met de risico's en maatregelen worden beschreven om te voldoen aan de geldende wet- en regelgeving. Voor bepaalde domeinen kan het op termijn nodig zijn om aanvullend een specifiek privacybeleid vast te stellen.

1.5 Juridisch kader

De bescherming van de privacy bij de verwerking van persoonsgegevens is een grondrecht. Dit is geregeld in:

- Grondwet (artikel 10);
- Handvest van de grondrechten van de Europese Unie (EHRM);
- Europees Verdrag voor de Rechten van de Mens (EVRM);
- Internationaal Kinderrechtenverdrag (IVRK).

De belangrijkste wet die op dit moment invulling geeft aan de bescherming van de privacy van personen bij de verwerking van persoonsgegevens is de AVG.

Verder is ook in specifieke regelgeving invulling gegeven aan de bescherming van de privacy bij de verwerking van persoonsgegevens zoals:

- Wet maatschappelijke ondersteuning (WMO)
- Jeugdwet
- Basisregistratie Personen (BRP)

Informatiebeveiliging en de bescherming van persoonsgegevens zijn onlosmakelijk met elkaar verbonden. Informatiebeveiliging is een randvoorwaarde voor de borging van privacy bij de verwerking van persoonsgegevens. In het vastgestelde Informatiebeveiligingsbeleid van de gemeente Eijsden-Margraten zijn maatregelen genoemd alle persoonsgegevens te beschermen.

2. Privacybeleid

2.1 Doelstelling

Doel van het privacybeleid is het beschrijven van kaders voor het verantwoord omgaan met persoonsgegevens en de borging van de privacyrechten van personen waarvan de gemeente Eijsden-Margraten persoonsgegevens verwerkt.

Het privacybeleid draagt bij aan bij:

- de privacybescherming van personen van wie de gemeente Eijsden-Margraten gegevens verwerkt of laat verwerken;
- het maatschappelijk vertrouwen en draagvlak;
- de beheersing van gemeentelijke afbreuk- en aansprakelijkheidsrisico's;
- in het met vertrouwen verantwoording af kunnen leggen aan de raad, waar nodig de Autoriteit Persoonsgegevens;
- in het kunnen inspelen op wettelijke en technologische ontwikkelingen.

2.2 Uitgangspunten

Een ieder die werkzaam is binnen onze organisatie is verantwoordelijk voor het verantwoord omgaan met persoonsgegevens en het waarborgen van de privacyrechten van personen. Het is belangrijk om persoonsgegevens rechtmatig, behoorlijk en transparant te verwerken.

De uitgangspunten hierbij zijn:

- betrokkene is vooraf in eenvoudige en duidelijk taal geïnformeerd dat zijn/haar persoonsgegevens worden verwerkt en voor welk doel;
- uitsluitend persoonsgegevens die noodzakelijk zijn voor het doel worden verwerkt;
- persoonsgegevens zijn correct en actueel;

- verzoeken van betrokkene op het gebied van rechten zoals ‘het recht om vergeten te worden’, ‘recht op inzage’, ‘recht op rectificatie’ worden opgevolgd;
- als identificatie niet meer noodzakelijk is voor het doel, dan moeten de persoonsgegevens worden verwijderd of geanonimiseerd;
- persoonsgegevens zijn beveiligd door middel van technische en organisatorische maatregelen.

Het college van burgemeester en wethouders is verantwoordelijk voor de naleving van deze uitgangspunten en moet dit kunnen aantonen.

2.2 Risico’s

Bij schending van de privacy is het college wettelijk aansprakelijk. Het verwijtbaar onvoldoende beschermen van persoonsgegevens en het niet naleven van privacywet- en regelgeving kan leiden tot:

- het betalen van schadevergoeding. Elke benadeelde heeft hier recht op;
- reputatieschade en herstelkosten. Deze kunnen fors zijn en leiden tot verlies van vertrouwen in de overheid;
- onderzoeken, dwangmaatregelen en hoge bestuurlijke boetes. Bij overtreding van de Wbp/ AVG kan de Autoriteit Persoonsgegevens (de landelijke toezichthouder) een boete opleggen.

Binnen bepaalde domeinen wordt er gewerkt met zeer gevoelige (bijzondere) persoonsgegevens zoals medische gegevens, gegevens over iemands financiële situatie of strafrechtelijke gegevens. Voorbeelden zijn het sociale domeinen, burgerzaken. De risico’s zijn hier hoger.

De risico’s van schending van de privacy voor personen variëren van ongemak, substantiële benadeling, ernstige sociale beschadiging of gevaren voor de gezondheid en de persoonlijke veiligheid.

Om de risico’s te beperken zijn maatregelen getroffen. Deze maatregelen zijn beschreven in hoofdstuk 4.

2.3 Evaluatie

Het privacybeleid wordt jaarlijks geëvalueerd. Hierover wordt gerapporteerd in de PDCA-cyclus. Indien noodzakelijk vindt bijstelling van het privacybeleid plaats.

3. Taken en verantwoordelijkheden

3.1 Doelstelling

De bescherming van de privacy van betrokkenen beleggen bij de verantwoordelijke personen.

3.2 Afbakening rollen en verantwoordelijkheden

Het college is eindverantwoordelijk, maar iedereen binnen de organisatie is verantwoordelijk voor de bescherming van de privacy van betrokkenen. Onderstaande tabel brengt de verantwoordelijkheden in beeld:

Feitelijk verantwoordelijk	• directie • afdelingshoofd/proceseigenaar/projectleider • alle medewerkers (inclusief inhuur/externen)
Eindverantwoordelijk	• college van burgemeester en wethouders • alle colleges bij gezamenlijk opdrachtgeverschap
Uitvoerend	• afdelingshoofd/proceseigenaar/projectleider • alle medewerkers (inclusief inhuur/externen)
Adviserend, controlerend	• privacyteam (FG, CISO en privacy beheerders)
Geïnformeerd	• gemeenteraad (privacy rechtelijk geen controlerende taak maar op basis van de Gemeentewet en de decentralisatiewetgeving een bestuurlijke toezichttaak) • belanghebbenden

3.3 Het college van B&W
Het college van B&W:

- is eindverantwoordelijk om te waarborgen dat persoonsgegevens worden beschermd in overeenstemming met wet- en regelgeving en op een behoorlijke en zorgvuldige manier. Er is een directe relatie met de beginselen van behoorlijk bestuur;
- stelt kaders voor de bescherming van de privacy op basis van wet- en regelgeving.

3.4 Het privacyteam
De bewaking van de privacyrichtlijnen en de voortgang van het plan van aanpak zullen worden opgepakt door een intern privacyteam, bestaande uit de volgende rollen:

- De Functionaris Gegevensbescherming (Concerncontroller);
- De CISO (beleidsadviseur informatiemanagement);
- De privacybeheerders (kwaliteitsmedewerker KCC en de adviseur informatiemanagement).

Het privacyteam zal aansluiten bij de bestaande werkgroep informatiebeveiliging.

3.4.1 De functionaris voor gegevensbescherming (FG):
- is onafhankelijk toezichthouder op de toepassing van de AVG en krijgt geen instructies over de uitvoering van de taken;
- levert een belangrijke bijdrage aan juist gebruik van persoonsgegevens door de organisatie;
- is aangewezen op grond van zijn professionele kwaliteiten, deskundigheid op het gebied van de wetgeving en de praktijk;
- mag werkzaam zijn voor meerdere organisaties;
- heeft toegang tot alle persoonsgegevens in de organisatie en de verwerkingsactiviteiten daarvan;
- wordt betrokken bij alles wat verband houdt met de bescherming van persoonsgegevens;
- is verplicht tot geheimhouding en vertrouwelijkheid.

De FG heeft minimaal de volgende taken en bevoegdheden:

- informeert en adviseert over de verplichtingen die de organisatie heeft met betrekking tot de bescherming van persoonsgegevens;
- ziet toe op de naleving van wet- en regelgeving en het door het college vastgestelde beleid met betrekking tot de bescherming van persoonsgegevens;
- ziet toe op het toewijzen van verantwoordelijkheden, bewustmaking en opleiding van de organisatie op het gebied van de bescherming van persoonsgegevens;
- geeft advies over Privacy Impact Analyses (PIA, zie paragraaf 4.2.4);
- werkt samen met en treed op als contactpersoon voor de Autoriteit Persoonsgegevens;
- in samenspraak met de CISO en Privavacybeheerders evalueren van het privacybeleid, opstellen van voorstellen tot implementatie en aanpassingen van het privacybeleid;
- rechtstreeks rapporteren aan het college.

Voorts neemt de FG regelmatig deel aan de MO-overleggen en rapporteert jaarlijks aan het college over zijn activiteiten als toezichthouder.

3.4.2 De privacybeheerder.
- bevordert en adviseert de organisatie gevraagd en ongevraagd over de bescherming van persoonsgegevens;
- controleert en evalueert de naleving van wet- en regelgeving en het door het college vastgestelde beleid met betrekking tot de bescherming van persoonsgegevens;
- verzorgt rapportages over de status;
- evalueert, in samenspraak met de FG, het privacybeleid, doet voorstellen tot implementatie en aanpassingen van het privacybeleid;
- rapporteert rechtstreeks aan de FG en de zijn leidinggevende directie.

3.4.3 De CISO (Certified Information Security Officer)
De CISO coördineert alle activiteiten op het gebied van informatiebeveiliging. Informatiebeveiliging en periodieke controle hierop is randvoorwaarde om aan de privacyrichtlijnen te kunnen voldoen. Adviseert de FG en de privacybeheerders en legt verantwoording af aan de directie en het college.

3.5 De directie
De directie is verantwoordelijk voor kaderstelling en sturing:

- stuurt op concern risico's;
- controleert of de getroffen maatregelen voldoende bescherming bieden om de privacy van betrokkenen te beschermen;
- beoordeelt periodiek het privacybeleid op basis van de evaluatie en aanpassingen van het privacybeleid en –plan van het privacyteam;
- zorgt dat de FG naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens.

3.6 De organisatie
Alle medewerkers (inclusief inhuur/externen) zijn verantwoordelijk voor de bescherming van de privacy van betrokkenen. Dat betekent dat iedereen zorgt voor een rechtmatige, behoorlijke en transparante verwerking van persoonsgegevens (zie paragraaf 2.2).

3.6.1 Afdelingshoofd
- stelt, indien nodig, voor het betreffende organisatieonderdeel een specifiek privacybeleid op, vraagt hierover advies aan het privacyteam en legt het aan het college voor ter vaststelling. Dit specifieke privacybeleid maakt onderdeel uit van dit overkoepelende privacy-beleid;
- zorgt voor naleving van wet-, regelgeving en het privacybeleid (rechtmatige, behoorlijke en transparante verwerking, bewustwording, gebruikt en evalueert PIA's, past 'Privacy bij design/default' toe en zorgt voor registratie van verwerkingsactiviteiten etc.);
- rapporteert aan de directie over naleving van wet- en regelgeving en het privacybeleid;
- zorgt dat de FG naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens;
- maakt afspraken met andere organisatieonderdelen over het borgen van de privacy in geval van informatie die stroomt tussen verschillende organisatieonderdelen.

4. Maatregelen

4.1 Doelstelling
Met de maatregelen beschreven in dit hoofdstuk kunnen de doelstellingen van het privacybeleid worden gehaald en de risico's worden beperkt. Het privacyteam bewaakt de in- en uitvoering van privacymaatregelen.

4.2 Maatregelen
Onderstaande maatregelen zijn getroffen om persoonsgegevens rechtmatig, behoorlijk en transparant te kunnen verwerken, volgens geldende wet- en regelgeving.

4.2.1 Transparantie
Betrokkenen krijgen vooraf duidelijke informatie (via de website en de dienstverlening (telefonisch, schriftelijk, email)) over de verwerking van hun persoonsgegevens en het doel van de verwerking.

4.2.2 Naleving van het informatiebeveiligingsbeleid
Op basis van het informatiebeveiligingsbeleid zijn maatregelen getroffen om de bescherming van persoonsgegevens te waarborgen. Informatieveiligheid is een eerste voorwaarde voor gegevensbescherming in het kader van privacy. Dit wordt gecoördineerd door de CISO.

4.2.3 Bewustwording
De mens is de zwakste schakel in de omgang met persoonsgegevens. Bewustwording is essentieel voor het borgen van privacy in de organisatie. Het is belangrijk dat iedereen die werkt met privacygevoelige informatie zich bewust is van het belang om hier zorgvuldig mee om te gaan. Doorlopend wordt er aandacht geschonken aan de bewustwording.

4.2.4 Register van verwerkingsactiviteiten
Er wordt een register bijgehouden met alle verwerkingsactiviteiten van persoonsgegevens per proces. Hierin worden onder andere de doeleinden van de verwerkingen, categorieën van betrokkenen en persoonsgegevens, derden ontvangers, bewaartermijn en maatregelen opgenomen.

4.2.5 Privacy impact analyses (PIA's)
Voor (veranderingen in) processen, diensten en producten en informatiesystemen, waar persoonsgegevens worden verwerkt, worden PIA's uitgevoerd. De AVG noemt dit een gegevensbeschermingseffectbeoordeling. Systematisch worden verwerkingen van persoonsgegevens, doeleinden, risico's en (voorgenomen) maatregelen beschreven. Het doel is om de impact van de verwerkingen op de bescherming van persoonsgegevens in kaart te brengen.

Per PIA wordt advies aan de FG gevraagd. Als uit een PIA blijkt dat er sprake is van risicovolle verwerkingen wordt de Autoriteit Persoonsgegevens op de hoogte gesteld. De Autoriteit Persoonsgegevens maakt het overzicht met risicovolle verwerkingen openbaar.

4.2.6 Privacy by design of privacy by default

Privacy by design houdt in dat vanaf het ontwerpen van een nieuw of aangepast proces, product, dienst of informatiesysteem wordt nagedacht over:

- het rechtmatig, behoorlijk en transparant verwerken van persoonsgegevens (paragraaf 2.2) en de maatregelen die hiervoor nodig zijn.

Privacy by default betekent dat de standaard instellingen in systemen zijn ingesteld om maximale privacy bescherming te borgen. De AVG noemt dit 'Gegevensbescherming door ontwerp en standaardinstellingen'.

Bij het toepassen van Privacy by design en – default wordt advies aan de FG gevraagd.

4.2.7 Verwerkersovereenkomst
Er worden verwerkersovereenkomsten afgesloten met bewerkers. Een verwerkersovereenkomst is wettelijk verplicht als het verwerken van persoonsgegevens aan een andere partij wordt uitbesteed. Er worden afspraken gemaakt over:

- de doeleinden waarvoor de gegevens mogen worden verwerkt;
- hoe de bewerker met de persoonsgegevens moet omgaan;
- welke beveiligingsmaatregelen moeten worden genomen;
- welke vormen van toezicht de eigenaar van de gegevens mag uitoefenen;
- de geheimhoudingsplicht;
- inschakeling van derden en onderaannemers;
- locatie van de data;
- aansprakelijkheid in geval van schade door het niet naleven van regelgeving.

4.2.8 Meldplicht datalekken
Datalekken worden intern via de cyclusdocumenten en indien nodig bij de Autoriteit Persoonsgegevens en de betrokkene(n) gemeld.
De meldplicht datalekken houdt in dat een ernstig data lek direct moet worden gemeld bij de Autoriteit Persoonsgegevens. Er is sprake van een ernstig data lek als persoonsgegevens:

- van gevoelige aard in handen (kunnen) vallen van derden die geen toegang tot die gegevens zouden mogen hebben;
- onjuist of onrechtmatig verwijderd zijn;
- niet juist en tijdig vernietigd zijn.

Een datalek moet aan de betrokkene(n) worden gemeld als de inbreuk waarschijnlijk ongunstige gevolgen heeft voor zijn of haar privéleven.

4.2.9 Toezicht en rapportage
Het privacyteam beoordeelt de naleving van het privacybeleid en rapporteert hierover in de cyclusdocumenten aan het college, directie en de raad. De directie, lijnmanagers en medewerkers worden waar nodig geïnformeerd. De rapportage zal tegelijkertijd plaatsvinden met de rapportage omtrent beveiligingsincidenten.

4.2.10 Bekendmaking en inwerkingtreding
Het privacybeleid treedt in werking de dag na publicatie in het gemeenteblad.