Gemeente Oldenzaal

GEMEENTEBLAD

Officiële uitgave van de gemeente Oldenzaal

Nr. 250554

30 september 2020

Verordening van de gemeenteraad van de gemeente Oldenzaal houdende regels omtrent de privacy (Privacyverordening 2020)

De raad van de gemeente Oldenzaal;

gelezen het voorstel van het college van burgemeester en wethouders van 4 februari 2020, nr. 5/3, reg.nr. INTB-19-04335;

gelet op artikel 149 van de Gemeentewet;

b e s l u i t :
vast te stellen de navolgende Privacyverordening 2020

Artikel 1 Definitie en begripsbepalingen

De begripsbepalingen bedoeld in artikel 4 van de Algemene verordening gegevensbescherming (hierna te noemen: AVG) zijn van overeenkomstige toepassing op deze verordening.

a. FG = Functionaris voor de Gegevensbescherming.
b. AP = Autoriteit Persoonsgegevens.
c. Big data= hiervan spreekt men als een verzameling gegevens uit traditionele en digitale bronnen binnen en buiten de organisatie gebruikt worden als bron voor verdere analyse dan waar deze gegevens oorspronkelijk voor zijn verzameld.
d. Tracking = het creëren, verzamelen en bijhouden van informatie betreffende het gedrag en gebruik van informatie, waaronder het volgen van menselijk gedrag.
e. Pseudonomiseren = met pseudonimiseren worden persoonsgegevens getransformeerd in een dataset die niet meer direct herleidbaar is tot een persoon. Om dit te doen worden de direct identificeerbare elementen van een persoonsgegeven vervangen door andere gegevens, zoals een nummer.
f. Anonimiseren = het (al dan niet gedeeltelijk) verwijderen van persoonsgegevens.
g. DPIA=gegevensbeschermingseffectbeoordeling (data protection impact assessment). Dit is een instrument om vooraf de privacy risico's van een gegevensverwerking in kaart te brengen. En om daarna maatregelen te kunnen nemen om de risico's te verkleinen.

Artikel 2 Reikwijdte

Deze verordening gaat over de verwerking van persoonsgegevens door of namens het college van burgemeester en wethouders, de burgemeester en de raad van de gemeente Oldenzaal, ieder voor zover het hun bevoegdheid betreft.

Artikel 3 Functionaris voor de Gegevensbescherming

Het college van burgemeester en wethouders, de burgemeester en de raad wijzen gezamenlijk een FG aan, die ten minste belast is met de taken als genoemd in artikel 39 van de AVG. Hieronder is mede begrepen het toezien op de uitwerking van het privacybeleid.

Artikel 4 Taken van de Functionaris voor de Gegevensbescherming

Tot de taken van de FG behoren in ieder geval:

a. Het onderhouden en aanvullen van het verwerkingenregister.
b. Het zorg dragen voor het afsluiten van verwerkersovereenkomsten indien noodzakelijk en een deugdelijke registratie van deze overeenkomsten.
c. Het beoordelen van verwerkingen en het eventueel uitvoeren van DPIA's.
d. Het opstellen van en het houden van toezicht op het gebruik van privacy protocollen voor verwerkingen die onder verantwoordelijkheid van de gemeente plaatsvinden.
e. Alle handelingen aangaande de meldplicht datalekken die de gemeente aangaan.

Artikel 5 Data Protection impact assessment (DPIA / gegevensbeschermingseffectbeoordeling)

1. Indien naar het oordeel van de FG 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 FG zorgt ervoor dat bij het uitvoeren van een DPIA de richtlijnen van de AP waaronder begrepen de "AP lijst van verwerkingen waarvoor een DPIA verplicht is" in acht worden genomen.
3. De FG geeft over de DPIA een bindend advies.

Gemeente Oldenzaal

Artikel 6 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 Oldenzaal 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 FG 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.

Artikel 7 Inzet van camera's

1. Camerabewaking door particuliere bedrijven wordt 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.
2. Het convenant zoals bedoeld in het tweede lid gaat in ieder geval in op:
   a. de grondslag voor de verwerking van persoonsgegevens;
   b. het verzamel- en verwerkingsdoel;
   c. de organisatorische en technische maatregelen die worden getroffen tegen verlies of onrechtmatige verwerking;
   d. bewaartermijn;
   e. de wijze waarop voldaan wordt aan de meldplicht datalekken.
3. Bij inzet van camera's dient voorafgaand aan deze inzet advies te worden gevraagd aan de FG.

Artikel 8 Datalek

1. Geconstateerde datalekken worden terstond gemeld bij de FG conform het proces datalekken. De FG 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.
3. De FG is verantwoordelijk voor het dichten van het datalek in samenwerking met de CISO.
4. De FG, de CISO en de PO (privacy officer) beoordelen of het datalek meldingswaardig is, als bedoeld in de Algemene Verordening Gegevensbescherming.
5. De FG meldt een meldingswaardig datalek direct aan de Autoriteit Persoonsgegevens, doch uiterlijk binnen 72 uur na kennisname.
6. De FG is bij een meldingswaardig datalek verantwoordelijk voor de onverwijlde melding naar betrokkene(n) wiens persoonsgegevens zijn gelekt.

Artikel 9 Toezicht en onderzoek

1. Voor de uitoefening van zijn toezichthoudende functie beschikt de FG over alle bevoegdheden die daarvoor redelijkerwijs noodzakelijk zijn. De FG is aangewezen als toezichthouder zoals bedoeld in artikel 5:11 Awb en mag daardoor gebruik maken van de bevoegdheden opgenomen in titel 5.2 Awb.
2. De FG 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.
3. De FG rapporteert over zijn bevindingen aan het college van burgemeester en wethouders. Hij geeft aanbevelingen over te nemen maatregelen die een goede verwerking van persoons-gegevens moeten helpen waarborgen.

Artikel 10 dataminimalisatie en beveiligingsbeleid

1. De verwerkingsverantwoordelijke streeft naar dataminimalisatie en richt processen zodanig in dat alleen de gegevens gevraagd wordt die benodigd zijn. Nadat een proces is afgerond worden gegevens zoveel mogelijk verwijderd tenzij deze bewaard moeten worden om te voldoen aan een wettelijke verplichting.
2. De verwerkingsverantwoordelijke stelt bewaartermijnen op van verschillende documenten en systemen ten behoeve van het uitgangspunt genoemd onder lid 1.
3. Het college stelt een autorisatiebeleid vast waarin bepaald is wie toegang heeft tot welke gegevens. Tevens is hierin bepaald op welke wijze geborgd wordt dat medewerkers niet onrechtmatig toegang hebben of krijgen tot gegevens die zij niet nodig hebben bij het uitvoeren van hun taak.

Artikel 11 Rechten betrokkene

De taken zoals omschreven in Hoofdstuk 3 van de AVG worden centraal uitgevoerd door het college. Bij uitoefening van de taken wordt de FG indien nodig betrokken.

Artikel 12 Inwerkingtreding en citeertitel

1. Deze verordening treedt in werking op 1 januari 2020.
2. Deze verordening wordt aangehaald als: Privacyverordening 2020.

Vastgesteld in de openbare vergadering van 21 september 2020,

de griffier,
J.H. Brokers

de voorzitter,
P.G. Welman

Toelichting behorende bij de Privacyverordening 2020 (vastgesteld bij raadsbesluit van 21 september 2020, nr. 1022)

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 Reikwijdte

De Raad, het college van burgemeester en wethouders dan wel de burgemeester zijn, iedere vanuit hun eigenbevoegdheid, te allen tijde verantwoordelijke voor de verwerkingen en bewerkingen die door of namens de gemeente worden uitgevoerd. Om hierin geen verschillen te laten ontstaan wijzen zij gezamenlijk een FG aan die zorg draagt voor toezicht op de naleving van de AVG.

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 AVG. In artikel 38 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. Hoewel de FG een eigen rol kent, treedt hij altijd in overleg met de CISO over geconstateerde gebreken of onjuistheden in het systeem van verwerkingen.

Artikel 4 Taken van de Functionaris voor de Gegevensbescherming

De taken en de positie van de FG zijn vastgelegd in artikel 37 tot en met 39 van de AVG. Deze taken zijn niet opgenomen in deze verordening omdat hogere regelgeving voorgaat. In dit artikel zijn de taken opgenomen die de FG daarnaast heeft bij de gemeente Oldenzaal.

Artikel 5 Data Protection Impact Assessment (DPIA/gegevensbeschermingseffectbeoordeling)

Voordat wordt besloten tot een verwerking van persoonsgegevens die een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, wordt een gegevensbeschermingseffectbeoordeling uitgevoerd. Uitgangspunt bij een gegevensbeschermingseffectbeoordeling is dat afhankelijk van de

verwerking passende waarborgen worden ingebouwd (Privacy by design). Bij iedere verwerking van persoonsgegevens wordt dataminimalisatie toegepast. De gegevensbeschermingseffectbeoordeling 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 gegevensbeschermingseffectbeoordeling 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.

Artikel 6 Big data en tracking
Dit artikel is bedoeld om de mogelijkheden van tracking en big data in 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 het herleidbaar zijn van personen. Hierbij geldt de volgende volgordelijkheid: op een dataset vindt eerst dataminimalisatie plaats, vervolgens wordt anonimisering 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.

Het verzamelen van de (persoons)gegevens voor big data 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 voor hem 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 voor meerjarige 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 7 Inzet van camera's
Cameratoezicht vindt plaats op basis van artikel 151 sub c van de Gemeentewet.

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, kenteken-herkenningscamera's, etc.

Camerabewaking van 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.

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 de gemeente altijd duidelijk is wat een camera doet in een bepaald gebied.

De aanvragers kunnen een cameraplan overleggen met een motivering waarom camerabewaking voor het gevraagde doel past binnen de AVG. 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 een convenant gesloten indien er sprake is van camerabewaking door derden waarbij de openbare ruimte wordt gefilmd.

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. Er moet altijd voorafgaand aan de plaatsing en het maken van opnamen een gegevensbeschermingseffectbeoordeling worden uitgevoerd.

Artikel 8 Datalek
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 die persoonsgegevens zouden mogen hebben of dat persoonsgegevens onbedoeld onherroepelijk zijn vernietigd. 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. Essentieel is dat het moet gaan om persoonsgegevens.

De gemeente 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 De wet indirect verplichtingen met zich mee. Denk bijvoorbeeld aan leveranciers van ICT-systemen. Hier dienen 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.

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 en de PO (Privacy Officer) bepalen of een melding aan de AP noodzakelijk is aan de hand van criteria die door de AP zijn vastgesteld. Op basis van deze criteria wordt ook vastgesteld of een betrokkene moet worden geïnformeerd. De FG houdt een overzicht bij van de datalekken

Artikel 9 Toezicht en onderzoek
De FG is belast met het toezicht op alle privacyaspecten binnen de gemeente Oldenzaal. Hij beoordeelt zelfstandig of de gemeente voldoet aan de AVG en deze verordening. Zijn bevoegdheden zijn vastgelegd in de AVG. Daarnaast is de FG toezichthouder zoals bedoeld in de Awb.

De FG kan een onderzoek instellen naar (schendingen van) privacyaspecten door de gemeente Oldenzaal. Hij kan hiervoor derden inschakelen die vertrouwelijk met de persoonsgegevenskwestie om kunnen gaan, zoals bijvoorbeeld een accountant die vanuit zijn professie een geheimhoudingsplicht kent.

Artikel 10 Dataminimalisatie en beveiligingsbeleid
In artikel 5 AVG zijn de beginselen opgenomen waaraan de verwerking van persoonsgegevens moet voldoen. Onderdeel hiervan is het uitgangspunt van dataminimalisatie. Hoe hieraan invulling wordt gegeven is in dit artikel vastgelegd. In het autorisatiebeleid is bepaald op welke wijze met autorisaties wordt omgegaan.

Artikel 11 Rechten betrokkene
Betrokkenen kunnen de gemeente onder meer verzoeken om inzage te geven in de verwerkingen van hun persoonsgegevens. De rechten van betrokkenen zijn geregeld in hoofdstuk 3 van de AVG.