

Privacy beleid 2020-2023 Gemeente Drimmelen

Vastgesteld op 15 oktober 2019
door het College van B&W

Privacy beleid Gemeente Drimmelen

1. Inleiding

De Nederlandse Grondwet (artikel 10) en Verdragen bevatten regels over de manier waarop de gemeente met persoonsgegevens om kan en om mág gaan. In de hele Europese Unie geldt sinds 25 mei 2018 één en dezelfde privacywetgeving: de Algemene verordening gegevensbescherming (hierna: AVG). De Wet bescherming persoonsgegevens (Wbp) geldt niet meer. De AVG stelt regels voor het mogen verwerken van persoonsgegevens. Onder verwerking van persoonsgegevens wordt onder meer verstaan het verzamelen, vastleggen, opvragen en vernietigen van gegevens.

De gemeente Drimmelen heeft (het verwerken van) persoonsgegevens nodig om haar taken goed uit te kunnen voeren. Zonder de verwerking van persoonsgegevens is het onmogelijk om bijvoorbeeld aan een burger een uitkering te verstrekken of een vergunning te verlenen. De burger moet er hierbij op kunnen vertrouwen dat de gemeente zorgvuldig en veilig met persoonsgegevens omgaat.

Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds meer digitale overheid stellen andere eisen aan de bescherming van gegevens en privacy. Een verwerking van persoonsgegevens brengt risico's mee. Zo kan de verwerking er toe leiden dat de gemeente informatie van de burger te weten komt die een te grote inbreuk maakt op de persoonlijke levenssfeer van de burger. Dat risico kan vergroot worden naarmate er meerdere soorten persoonsgegevens worden verzameld. Dit is met name van toepassing op het verwerken van bijzondere persoonsgegevens zoals gezondheidsgegevens. Tevens bestaat bijvoorbeeld het risico dat verzamelde persoonsgegevens bekend raken bij derden die daar niks mee te maken hebben. Dit kunnen burgers zijn of medewerkers die niet bij de verwerking betrokken zijn. Dat zou tot (identiteits)fraude kunnen leiden. Hierbij kan het voorkomen dat de burger zich in zijn of haar rechten geschonden voelt als de informatie bekend wordt bij anderen.

De gemeente Drimmelen 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.

Dit privacy beleid gaat met name over hoe om te gaan met persoonsgegevens. Om de verzamelde persoonsgegevens zo goed mogelijk te beveiligen heeft de gemeente tevens een Informatiebeveiligingsbeleid vastgesteld. In dit beleid zijn de strategische, tactische en operationele maatregelen uitgewerkt over hoe de gemeente zorgt voor afdoende veiligheidsmaatregelen met betrekking tot het afschermen en zorgvuldig omgaan met persoonsgegevens zowel in digitale als in analoge (fysieke) vorm.

2. Reikwijdte

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

3. Wettelijke kaders voor de omgang met gegevens

Het College van Burgemeester en Wethouders is verantwoordelijk voor het integraal opstellen en uitvoeren van het onderhavige privacy beleid.

Hiervoor gelden onder andere de volgende wettelijke kaders:

- de Algemene Verordening Gegevensbescherming (AVG);
- de Uitvoeringswet Algemene Verordening Gegevensbescherming;
- het Informatiebeveiligingsbeleid welke vastgesteld door het College van Burgemeester en Wethouders;
- de Code voor Informatiebeveiliging (NEN/ISO 27002);
- de Baseline Informatiebeveiliging Gemeenten (vanaf 1 januari 2020 de Baseline Informatiebeveiliging Overheid geheten).

De volgende begrippen worden in de AVG gebruikt (artikel 4 AVG) en worden als zodanig ook gehanteerd in dit beleid:

Betrokkene:

De persoon op wie de persoonsgegevens betrekking hebben. De betrokkene is degene van wie de gegevens worden verwerkt.

Verwerker:

De persoon of organisatie die de persoonsgegevens verwerkt in opdracht van een andere persoon of organisatie.

Persoonsgegevens:

Alle gegevens die gaan over mensen en waaraan je een mens als individu kunt herkennen. Het gaat hierbij niet alleen om vertrouwelijke gegevens, zoals over iemands gezondheid, maar om ieder gegeven dat te herleiden is tot een bepaald persoon (bijvoorbeeld; naam, adres, geboortedatum). Naast gewone persoonsgegevens kent de wet ook bijzondere persoonsgegevens. Dit zijn gegevens die gaan over gevoelige onderwerpen, zoals etnische achtergrond, politieke voorkeuren. Het Burgerservicenummer (BSN) is onder de AVG geen bijzonder persoonsgegeven maar gelet op zijn aard een zeer gevoelig persoonsgegeven.

Gegevensbeschermingseffectbeoordeling:

Met een gegevensbeschermingseffectbeoordeling worden de effecten en risico's van de nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. Dit heet ook wel een Privacy Impact Assessment (PIA).

Verwerkingsverantwoordelijke:

Een persoon of instantie die alleen, of samen met een ander, het doel en de middelen voor de verwerking van persoonsgegevens vaststelt.

Verwerking:

Een verwerking is alles wat je met een persoonsgegeven doet, zoals: vastleggen, bewaren, verzamelen, bij elkaar voegen, verstrekken aan een ander, en vernietigen.

4. Uitgangspunten

De gemeente gaat op een veilige manier met persoonsgegevens om en respecteert de privacy van betrokkenen. De gemeente houdt zich hierbij aan de volgende uitgangspunten:

Rechtmatigheid, behoorlijkheid, transparantie

Persoonsgegevens worden in overeenstemming met de wet en regelgeving op behoorlijke en zorgvuldige wijze verwerkt.

Grondslag en doelbinding

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

Dataminimalisatie

De gemeente verwerkt alleen de persoonsgegevens die minimaal noodzakelijk zijn voor het vooraf bepaalde doel. De gemeente streeft naar minimale gegevensverwerking. Waar mogelijk worden zo min mogelijk persoonsgegevens verwerkt.

Bewaartermijn

Persoonsgegevens worden niet langer bewaard dan nodig is voor het doel waarvoor de gegevens zijn verzameld of worden gebruikt. Het bewaren van persoonsgegevens kan nodig zijn om de gemeentelijke taken goed uit te kunnen oefenen of om wettelijke verplichtingen te kunnen naleven.

Integriteit en vertrouwelijkheid

De gemeente 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 gemeente voor passende beveiliging van persoonsgegevens. Deze beveiliging is vastgelegd in het informatiebeveiligingsbeleid van de gemeente Drimmelen.

Delen met derden

In het geval van samenwerking met externe partijen, waarbij sprake is van verwerking, maakt de gemeente afspraken over de eisen waar gegevensuitwisseling aan moet voldoen. Deze afspraken voldoen aan de wet. De gemeente controleert deze afspraken jaarlijks.

Subsidiariteit

Voor het bereiken van het doel waarvoor de persoonsgegevens worden verwerkt, wordt inbreuk op de persoonlijke levenssfeer van de betrokken inwoner zoveel mogelijk beperkt.

Proportionaliteit

De inbreuk op de belangen van de betrokkene mag niet onevenredig zijn in verhouding tot het met de verwerking te dienen doel.

Rechten van betrokkenen

De gemeente respecteert en honoreert waar mogelijk de rechten van betrokkenen bedoeld in de artikelen 15 tot en met 22 van de AVG en richt daar de systemen, processen en interne organisatie op in. In uitzonderingsituatie zoals het excessief opvragen van gegevens of het ter bescherming van zwaarderwegende rechten van anderen kan een verzoek om gegevens worden geweigerd.

De volgende rechten van betrokkenen volgen uit de AVG:

- Recht op informatie: Betrokkenen hebben het recht om aan de gemeente te vragen of zijn/haar persoonsgegevens worden verwerkt. De gemeente dient te communiceren in een beknopte en transparante, begrijpelijke en gemakkelijk toegankelijke manier. De informatie moet in duidelijke en eenvoudige taal worden opgesteld, en moet in principe kosteloos worden verstrekt.
- Inzagerecht: Betrokkenen hebben de mogelijkheid om te controleren of, en op welke manier, zijn/haar gegevens en welke worden verwerkt. Tevens kunnen betrokkenen kosteloos een kopie van de verwerkte persoonsgegevens krijgen.
- Correctierecht: Als duidelijk wordt dat door de gemeente verwerkte persoonsgegevens niet kloppen, kunnen de betrokkenen een verzoek indienen bij de gemeente om dit te corrigeren of aan te vullen.
- Recht van verzet/beperking: Betrokkenen hebben het recht aan de gemeente te vragen om hun persoonsgegevens niet meer te gebruiken of te beperken.
- Recht om vergeten te worden: In gevallen waar de betrokkenen toestemming hebben gegeven om gegevens te verwerken, hebben de betrokkenen in een aantal gevallen het recht om de persoonsgegevens te laten verwijderen.
- Recht op bezwaar: Betrokkenen hebben het recht om bezwaar te maken tegen de verwerking van zijn/haar persoonsgegevens. De gemeente zal hieraan voldoen, tenzij er dwingende gerechtvaardigde gronden zijn voor de verwerking.

De gemeente stelt een procedure op voor het omgaan met verzoeken die zien op de rechten van betrokkenen.

Om gebruik te maken van zijn/haar rechten kan de betrokkene een verzoek daartoe indienen bij de gemeente. Dit verzoek kan digitaal (middels DigiD) of schriftelijk ingediend worden. Indien het verzoek schriftelijk wordt ingediend stelt de gemeente de identiteit van de indiener vast. De gemeente heeft vier weken de tijd, vanaf de ontvangst van het verzoek, om te beoordelen of het verzoek gerechtvaardigd is. Binnen vier weken zal de gemeente laten weten wat er met het verzoek gaat gebeuren. Indien het verzoek niet binnen 4 weken afgehandeld kan worden, heeft de gemeente de mogelijkheid de termijn van 4 weken met twee maanden te verlengen.

Als het verzoek niet wordt opgevolgd is er de mogelijkheid om bezwaar te maken bij de gemeente, of een klacht in te dienen bij de Autoriteit Persoonsgegevens (AP). Aan de hand van een verzoek kan de gemeente aanvullende informatie opvragen om zeker te zijn van de identiteit van de verzoeker.

5. Geautomatiseerde verwerkingen

Profilering (Artikel 22 AVG)

Uitgangspunt in de AVG is dat betrokkenen het recht hebben niet te worden onderworpen aan uitsluitend geautomatiseerde besluitvorming (waaronder profilering), als daaraan rechtsgevolgen voor de betrokkenen zijn verbonden of het besluit hen in aanmerkelijke mate treft.

Profilering vindt plaats wanneer er een geautomatiseerde verwerking van persoonsgegevens plaatsvindt waarbij aan de hand van persoonsgegevens naar bepaalde persoonlijke aspecten van een persoon wordt gekeken om deze persoon te categoriseren en te analyseren, of om zaken te kunnen voorspellen. Voorbeelden van persoonlijke aspecten kunnen zijn; financiële situatie, interesses, gedrag of locatie.

Om profilering wat duidelijker te maken gebruiken we het volgende voorbeeld: wanneer een bezoeker op de gemeentelijke website naar een bepaalde dienst kijkt, mag de gemeente geen actie ondernemen om die dienst aan te bieden.

Gemeenten mogen wel bekijken hoe vaak een bepaalde dienst bekeken is, maar dus niet specifiek gericht adverteren, wat binnen de gemeente Drimmelen dan ook niet plaatsvindt.

Big data en tracking

Door middel van big data onderzoek en tracking mogen alleen gegevens verwerkt worden wanneer deze niet herleidbaar zijn tot een natuurlijk persoon. Daarnaast worden ze alleen verzameld voor onderzoek dat door, of namens, de gemeente wordt uitgevoerd. De verzamelde gegevens door big data onderzoek en tracking zijn alleen de gegevens die door geautoriseerde personen zijn verzameld. Wanneer de gegevens worden omgezet in een dataset zal dataminimalisatie worden toegepast. Dit betekent dat alleen de data die echt noodzakelijk is voor het behalen van het doel waarvoor ze verzameld/verwerkt wordt gebruikt zal worden. Daarnaast kunnen persoonsgegevens gepseudonimiseerd worden zodat zij niet herleidbaar zijn tot een persoon.

De gemeente Drimmelen maakt op dit moment geen gebruik van big data en tracking.

6. Inzet van camera's

Binnen de gemeente wordt onder bepaalde omstandigheden gebruik gemaakt van cameratoezicht, zoals vastgelegd in de Gemeentewet. Cameratoezicht wordt onder andere gebruikt voor het vergroten van de veiligheid op en rond openbare ruimten indien dat noodzakelijk is. De gemeente maakt ook gebruik van cameratoezicht in en om de gemeentelijke gebouwen. Camera's kunnen een grote inbreuk maken op de privacy van diegene die gefilmd worden. Om de privacy zo goed mogelijk te waarborgen worden camera's alleen ingezet wanneer er geen andere manieren zijn om het doel te bereiken en worden er eisen gesteld aan de inzet van camera's.

De gemeente kan gebruiken van cameratoezicht onder de volgende voorwaarden:

In artikel 151c van de Gemeentewet is bepaald dat het doel bij de toepassing van gemeentelijk cameratoezicht de noodzaak voor het kunnen handhaven van de openbare orde is. Hieronder valt ook de algemene bestuurlijke voorkoming van strafbare feiten die invloed hebben op de orde en rust in de gemeente.

Camerabewaking kan tevens door particuliere bedrijven worden uitgeoefend. Indien dit van toepassing is wordt er een daartoe strekkend besluit door of namens het College van Burgemeester en Wethouders genomen en wordt er een convenant met de verantwoordelijke gesloten voorafgaande aan de verwerking.

Een convenant zoals hierboven bedoeld 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. de bewaartermijn;
- e. de wijze waarop voldaan wordt aan de meldplicht datalekken.

7. Register van verwerkingen (Artikel 30 AVG)

De gemeente is verantwoordelijk voor het aanleggen van een register van alle verwerkingen waarvan de gemeente de verwerkingsverantwoordelijke is. Het register bevat een beschrijving van wat er tijdens een verwerking plaatsvindt, en welke gegevens daarvoor worden gebruikt, namelijk:

- De naam en contactgegevens van de verwerkingsverantwoordelijke en, mogelijk, de gezamenlijke verwerkingsverantwoordelijke;
- De doelen van de verwerking;
- Een beschrijving van het soort persoonsgegevens en de daarbij horende betrokkenen;
- Een beschrijving van de ontvangers van de persoonsgegevens;
- Indien van toepassing een beschrijving van het delen van persoonsgegevens aan een derde land of internationale organisatie;
- De termijnen waarin de verschillende persoonsgegevens moeten worden gewist;
- Een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

8. Datalekken (Artikel 33 en 34 AVG)

We spreken van een datalek wanneer persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens mogen hebben. Wanneer er een datalek heeft plaatsgevonden meldt de gemeente dit zonder onredelijke vertraging en, indien mogelijk, uiterlijk 72 uur nadat de gemeente kennis van de inbreuk heeft genomen aan de AP. Als dit later dan 72 uur is wordt er een motivering voor de vertraging bij de melding gevoegd. Het kan zijn dat de inbreuk een hoog risico meebrengt voor de rechten en vrijheden van de betrokkene(n). In dit geval meldt de gemeente dit aan de betrokkene(n) in eenvoudige en duidelijke taal. Om toekomstige datalekken te voorkomen worden bestaande datalekken geëvalueerd.

9. De Functionaris voor gegevensbescherming

De Functionaris Gegevensbescherming (FG) is verantwoordelijk voor het intern onafhankelijk toezicht op en adviseren van de organisatie over de juiste en zorgvuldige omgang met persoonsgegevens. Hierbij kan de FG rechtstreeks de AP inschakelen.

De gemeente heeft een eigen FG in dienst. De FG is betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. De taken van de functionaris zijn informeren, adviseren, toezicht houden, bewustwording creëren en optreden als contactpersoon van de AP. Het is uitdrukkelijk 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 FG is verantwoordelijk voor het structureel toetsen van de implementatie en de uitvoering van de wettelijke eisen en de gemeentelijke richtlijnen op het gebied van privacy. Voor vragen over privacy of over deze toelichting kunt u contact opnemen met de functionaris voor gegevensbescherming van gemeente.

De AP kan ook uit eigen beweging een onderzoek doen naar de naleving van de privacywetgeving. Daarnaast kan de AP op verzoek van belanghebbenden (zoals burgers of belangenorganisaties) een onderzoek instellen.

Dit privacy beleid treedt in werking na vaststelling door het College van Burgemeesters en Wethouders. Het beleid wordt tenminste iedere vier jaar geëvalueerd en indien nodig herzien. Aanpassingen van dit beleid worden aangekondigd via de website van de gemeente Drimmelen. De meest actuele versie van het beleid is te vinden op de website van de gemeente.

Aldus vastgesteld door burgemeester en wethouders van gemeente Drimmelen, op 15 oktober 2019

*E. Delissen,
gemeentesecretaris*

*G.L.C.M. de Kok
Burgemeester*

Disclaimer

Dit product is een eenvoudige en begrijpbare vertaling van de huidige privacywetgeving en gebaseerd op de AVG. Vanzelfsprekend is de toepasbare wet- en regelgeving altijd leidend en kunnen er geen rechten ontleend worden aan dit document.