Gemeente Borger-Odoorn

GEMEENTEBLAD

Officiële uitgave van de gemeente Borger-Odoorn

Nr. 50220

1 maart

2019

Privacy beleid gemeente Borger-Odoorn

Privacy beleid gemeente Borger-Odoorn

Inleiding
Binnen de gemeente Borger-Odoorn wordt veel gewerkt met persoonsgegevens van klanten, medewerkers en (keten)partners. Persoonsgegevens worden voornamelijk verzameld bij de klanten voor het goed uitvoeren van de gemeentelijke wettelijke taken. De klant moet erop kunnen vertrouwen dat de gemeente Borger-Odoorn zorgvuldig en veilig met de persoonsgegevens omgaat. In deze tijd gaat ook de gemeente Borger-Odoorn 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 Borger-Odoorn is zich hier van bewust en zorgt dat de privacy gewaarborgd blijft, onder andere door maatregelen te nemen op het gebied van informatiebeveiliging, dataminimalisatie, transparantie en gebruikerscontrole.

Het bestuur en het management spelen een cruciale/belangrijke rol bij het waarborgen van privacy. De gemeente Borger-Odoorn 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 privacy beleid van de gemeente Borger-Odoorn is in lijn met het algemene beleid van de gemeente en de relevante lokale, regionale, nationale en Europese wet- en regelgeving. Naast dit privacy beleid stelt de gemeente Borger-Odoorn ook een privacy reglement vast en een reglement voor de taken en bevoegdheden van de Functionaris voor Gegevensbescherming.

Voor specifieke veel voorkomende processen, kunnen de betreffende afdelingen een specifiek beleid, reglement, protocol of procedure opstellen. Daarin kunnen zij aangeven hoe wordt omgegaan met privacygevoelige informatie. Deze meer specifieke beleidsstukken moeten voldoen aan de uitgangspunten van dit privacy beleid en het privacy reglement van de gemeente Borger-Odoorn.

1. Wettelijk kader

De gemeente Borger-Odoorn is verantwoordelijk voor het opstellen, uitvoeren en handhaven van het beleid. Hiervoor gelden onder andere de volgende wettelijke kaders:
- Europese Verordening: de Algemene Verordening Gegevensbescherming (AVG);
- Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG).

2. Naleving en toezicht op de verwerking van persoonsgegevens binnen de organisatie

2.1 Rol en taak college
Het college van burgemeester en wethouders, de burgemeester of de gemeenteraad zijn, ieder voor zover het een gegevensverwerking betreft in het kader van hun taak, eindverantwoordelijk voor het naleven van de AVG en het privacy beleid.

2.2 Rol en taak leidinggevenden
Leidinggevenden zijn verantwoordelijk voor de verwerkingen binnen zijn/haar team. Bij de uitvoering van de verwerkingen zijn zij zich bewust van de mogelijke inbreuk die dit kan maken op de persoonlijke levenssfeer van inwoners en handelen daar naar. Dit betekent dat zij de AVG naleven en handelen naar het privacy beleid en reglement van de gemeente.

2.3 Rol en taak medewerkers
Medewerkers zijn verantwoordelijk voor een zorgvuldige omgang met persoonsgegevens. Bij de uitvoering van hun taken zijn zij zich bewust van de mogelijke inbreuk die dit kan maken op de persoonlijke levenssfeer van inwoners en handelen daar naar. Dit betekent dat zij de AVG naleven en handelen naar het privacy beleid en reglement van de gemeente.

2.4 Rol en taak Functionaris voor de Gegevensbescherming
Op grond van de AVG is het voor de gemeente verplicht om een intern toezichthouder en adviseur aan te stellen; de Functionaris Gegevensbescherming (FG). De FG is een onafhankelijke toezichthouder die binnen de organisatie toezicht houdt op de naleving van de AVG en bovendien medewerkers, management en bestuur kan adviseren over vragen die zien op de naleving van de AVG. De FG

rapporteert over de wijze waarop de gemeente omgaat met de persoonsgegevens van de inwoners. Op de website van de gemeente worden de contactgegevens van de FG gepubliceerd. De FG geeft gevraagd en ongevraagd advies aan bestuur, management en medewerkers over onderwerpen die de verwerking van persoonsgegevens betreffen. De FG is de contactpersoon voor de Autoriteit Persoonsgegevens (AP). De FG is in de uitvoering van taken onafhankelijk en ontvangt geen instructies over de uitvoering van zijn taken. Over de taken en bevoegdheden van de FG is meer te lezen in het Reglement taken en bevoegdheden Functionaris voor Gegevensbescherming.

2.5 Rol en taak jurist privacy
De jurist privacy is het aanspreekpunt als het gaat om advies over de verwerking van persoonsgegevens en de uitleg van de AVG. De jurist privacy is tevens coördinator van het up to date houden van het register van verwerkingen. De jurist privacy heeft kennis van het gemeentelijk privacy beleid en de AVG.

2.6 Rol CISO
De verwerking van persoonsgegevens is onlosmakelijk verbonden met de beveiliging daarvan. Beveiliging van persoonsgegevens is een verantwoordelijkheid van iedere medewerker. Maar om er voor te zorgen dat er een samenhangend pakket aan maatregelen in de gemeente beschikbaar is ter waarborging van de vertrouwelijkheid, integriteit en beschikbaarheid van de informatie binnen een gemeente is er de CISO: Chief Information Security Officer. De CISO zal in samenwerking met de FG toezichthouden op en adviseren over de passende beveiliging van persoonsgegevens binnen de organisatie.

3. Beginselen AVG

De AVG verplicht de gemeente Borger-Odoorn om persoonsgegevens ‘in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze’ te verwerken. Dit privacy beleid is een invulling van artikel 24 lid 2 van de AVG. De gemeente gaat op een veilige manier met persoonsgegevens om en respecteert de privacy van betrokkenen. De gemeente houdt zich hierbij aan de volgende beginselen:

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

3.2 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 minder of geen persoonsgegevens verwerkt.

3.3 Bewaartermijn
De gemeente Borger-Odoorn bewaart de verzamelde persoonsgegevens niet langer dan strikt nodig is, of wettelijk geregeld is, om de doelen te realiseren waarvoor de gegevens zijn verzameld. Het bewaren van persoonsgegevens kan nodig zijn om de gemeentelijke taken goed uit te kunnen oefenen of om wettelijke verplichtingen te kunnen naleven. De meeste termijnen hiervoor liggen vast in de Archiefwet en andere wetten waar de termijnen zijn vastgesteld. Welke bewaartermijn van toepassing is op een verwerking is terug te vinden in het register van verwerkingen.

3.4 Integriteit en vertrouwelijkheid
De gemeente gaat zorgvuldig om met persoonsgegevens en behandelt deze vertrouwelijk. Zo worden persoonsgegevens alleen verwerkt door personen met een geheimhoudingsplicht of door personen die een integriteitsverklaring hebben ondertekend 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.

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

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

3.7 Rechten van betrokkenen
De gemeente honoreert alle rechten van betrokkenen.

4. Uitgangspunten beleid

Dit beleid gaat uit van de drie belangrijkste uitgangspunten voor de verwerking van persoonsgegevens op grond van de AVG: transparant, rechtmatig en behoorlijk en het afleggen van rekenschap. Deze beginselen zijn opgenomen in artikel 5 en 6 van de AVG en nader uitgewerkt in artikel 12 e.v. van de AVG. Onderstaand volgt een uiteenzetting op welke wijze de gemeente aan de uitgangspunten invulling geeft.

4.1 Transparant
4.1.1 Informatievoorziening voorafgaand aan verwerking
Voor elke verwerking van de gemeente is vooraf in begrijpelijke taal informatie beschikbaar over het doel van de verwerking, welke gegevens er worden vastgelegd, voor hoe lang en op welke wijze rechten kunnen worden uitgeoefend. Deze informatie is beschikbaar op het moment dat er klantcontact is, onafhankelijk of dit in persoon is of digitaal.

4.1.2 Register van verwerkingen
De gemeente beschikt, overeenkomstig artikel 30 van de AVG, over een register van verwerkingen. In dit actuele en volledige register wordt onder meer vastgelegd welke gegevensverwerkingen er onder verantwoordelijkheid van de gemeente plaatsvinden en per verwerking wordt aangegeven voor welk doel de verwerking is, over welke categorieën van personen het gaat en wie de ontvangers van die gegevens zijn. Het register van verwerkingen wordt door de gemeente openbaar gemaakt via de website.

4.1.3 Rechten van betrokkenen
Een ieder van wie persoonsgegevens worden verwerkt, heeft rechten welke in de AVG in hoofdstuk 3 zijn geregeld. De rechten van betrokkenen worden in het privacy reglement en de privacyverklaring nader toegelicht. De privacyverklaring is te raadplegen op de website van de gemeente Borger-Odoorn. Ook zal betrokkene actief worden gewezen op de mogelijkheid een klacht gerelateerd aan de AVG in te dienen bij de AP, indien het verzoek niet naar tevredenheid is afgehandeld.

4.2 Rechtmatig en behoorlijk
Met de digitalisering van dienstverlening en de uitbreiding van taken neemt het aantal persoonsgegevens dat door de gemeente wordt verwerkt toe. Het verwerken van (bijzondere) persoonsgegevens vraagt in alle gevallen een zorgvuldige afweging over of de verwerking noodzakelijk is en of de verwerking op grond van de AVG is toegestaan.

4.2.1 Gegevensbeschermingseffectbeoordeling
Wanneer een soort verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen wordt, overeenkomstig artikel 35 van de AVG, vóór de verwerking een gegevensbeschermingseffectbeoordeling gemaakt, ook wel een Data protection impact Assesment genoemd (DPIA). Bij het opstellen van de DPIA wordt een werkgroep samengesteld waarin in ieder geval de CISO en jurist privacy bij zijn betrokken. De FG kan desgewenst vooraf gevraagd worden om advies te verstrekken met betrekking tot de gegevensbeschermingseffectbeoordeling en toezien op de uitvoering daarvan in overeenstemming met artikel 35 van de AVG. De FG, jurist privacy en de CISO worden betrokken bij de uitkomsten van de DPIA. De uitkomsten van de DPIA worden meegewogen bij de beslissing voor het al dan niet aanvangen van de verwerking. Dat betekent dat altijd gemotiveerd wordt beargumenteerd welke keuzes worden gemaakt ten aanzien van de verwerking van persoonsgegevens. De keuzes zijn daarmee transparant en zijn onder andere voor de FG, de raad of de toezichthouder beschikbaar voor het uitoefenen van hun (controlerende) taken. Wanneer uit een DPIA blijkt dat de verwerking een hoog risico oplevert, en er geen maatregelen worden genomen om het risico te beperken, wordt voorafgaand aan de verwerking de AP geraadpleegd (artikel 36 lid 1 van de AVG).

4.2.2 Beveiliging; pas toe of leg uit
De persoonsgegevens waarover de gemeente beschikt worden passend beveiligd. Als uitgangspunt hiervoor hanteert de gemeente de Baseline Informatiebeveiliging voor Nederlandse Gemeenten (BIG). In de BIG staan verschillende technische en organisatorische maatregelen genoemd om persoonsgegevens te beveiligen tegen uiteenlopende risico's, zoals ongeautoriseerde toegang tot data, verlies van data of gijzeling van data (ransomware). Wat passend is, wordt mede bepaald door het soort persoonsgegeven, bijvoorbeeld een bijzonder persoonsgegeven, de mate van beschikbaarheid

en toepasbaarheid van de beveiligingsmaatregel, de kosten die verbonden zijn aan de maatregel in relatie tot de kans op het risico en de gevolgen voor betrokkenen indien de persoonsgegevens openbaar worden of juist vernietigd zijn. Persoonsgegevens worden, waar dit kan, versleuteld verzonden. Bijvoorbeeld door gebruik te maken van beveiligde diensten waarmee informatie kan worden verzonden. Ten aanzien van informatiebeveiliging hanteert de gemeente het ''pas toe of leg uit'' principe. In principe wordt de BIG integraal toegepast, tenzij op grond van bovenstaande criteria gemotiveerd tot een andere keuze wordt gekomen.

4.2.3 Privacy by design en Privacy by default
Bij het verwerken van persoonsgegevens is privacy by design en privacy by default het uitgangspunt (artikel 25 lid 1 en 2 van de AVG). Dat wil zeggen dat altijd wordt beoordeeld of het doel van de verwerking ook kan worden bereikt met het verwerken van minder persoonsgegevens of voor een kortere periode. Bij het ontwerp van een systeem of werkwijze wordt aandacht besteed aan de wijze waarop waarborgen voor de naleving van de AVG kunnen worden ingebouwd, zoals de toegang tot de persoonsgegevens en automatische archivering, verwijdering en vernietiging.

4.2.4 Derden
De gegevens van betrokkenen worden door de gemeente Borger-Odoorn alleen verstrekt, indien dit nodig is om te voldoen aan een wettelijke verplichting of voor de uitvoering van de overeenkomst met betrokkenen. De gemeente Borger-Odoorn sluit een verwerkersovereenkomst met organisaties (derden) die gegevens van betrokkenen in opdracht van de gemeente verwerken. In deze overeenkomst regelt de gemeente Borger-Odoorn hoe organisaties (derden) om moeten gaan met de beveiliging en vertrouwelijkheid van de gegevens. De gemeente blijft verantwoordelijk voor deze verwerkingen van de persoonsgegevens van betrokkenen.

4.2.5 Basisregistratie Personen
Persoonsgegevens uit de Basisregistratie Personen worden gedeeld met andere overheidsinstanties of instanties die de gegevens van betrokkenen nodig zijn voor de uitvoering van een wettelijke taak. Op de website van de Rijksoverheid is te zien welke organisaties gegevens uit de Basis Registratie Personen (BRP) krijgen en waarvoor deze gegevens worden gedeeld. In het Reglement gegevensverstrekking basisregistratie personen Borger-Odoorn is te lezen hoe wordt omgegaan met de gegevens uit de BRP.

4.3 Meldplicht datalekken
De gemeente meldt overeenkomstig de bepalingen uit de AVG datalekken bij de AP en, indien van toepassing, aan de betrokkenen die het betreft. De gemeente houdt, overeenkomstig artikel 33 lid 5 van de AVG een register bij van alle inbreuken (gemeld en niet gemeld bij de AP). Een overzicht van het aantal meldingen en klachten gerelateerd aan de AVG wordt opgenomen in het bedrijfsvoeringsprogramma.

4.4 Jaarlijkse verantwoording
Elk jaar stelt de ambtelijke organisatie een verantwoording op over het uitgevoerde beleid en haar uitgaven. In dit jaarverslag wordt met ingang van het verantwoordingsjaar 2018 ook verantwoording afgelegd over de wijze waarop de gemeente uitvoering heeft gegeven aan de AVG en haar privacy beleid en de wijze waarop zij rekenschap heeft afgelegd. Dit zal in het jaarverslag en de begroting worden opgenomen in de paragraaf 'bedrijfsvoering'.

5. Bekendmaking en inwerkingtreding

Dit beleid treedt in werking na vaststelling door het college van burgemeester en wethouders. Het beleid wordt geëvalueerd en, indien nodig, herzien. Als er belangrijke wijzigingen zijn, wordt het privacy beleid bijgesteld.

Exloo, 19 februari 2019