Algemeen privacybeleid Gemeente Someren

Hoe gaat de gemeente Someren om met de verwerkingen van persoonsgegevens?

Algemeen privacybeleid Gemeente Someren

Hoe gaat de gemeente Someren om met de verwerkingen van persoonsgegevens?

Titel:	Algemeen privacybeleid Gemeente Someren
Versie:	170032337
Datum:	mei 2018
Zaaknummer:	SOM/2017/032337

1. Inleiding

Hoe gaat de gemeente Someren om met persoonsgegevens? Dit leest u in dit algemeen privacybeleid. Hierin leggen wij uit wat u van ons kunt verwachten ten aanzien van de bescherming van privacy. De gemeente is immers dagelijks bezig met het verwerken van persoonsgegevens van haar inwoners, haar medewerkers en haar zakelijke connecties. Dit doen we ter vervulling van onze gemeentelijke en wettelijke taken maar ook als werkgever en zakenrelatie.

Voor de bovengenoemde partijen is het van belang dat zij er op kunnen vertrouwen dat de gemeente Someren er alles aan doet om zorgvuldig en veilig te handelen tijdens het verwerken van persoonsgegevens. 100% Garantie tot waterdichte bescherming is helaas niet te geven. U mag er wel op vertrouwen dat wij zorgvuldig en vertrouwelijk omgaan met de persoonsgegevens en dat we ons inzetten om dit zo goed en veilig mogelijk te doen.

Wij willen u via deze nota informeren over hoe wij invulling geven aan de bevoegdheden en eisen vanuit de Europese Algemene Verordening Persoonsgegevens (AVG). Deze wet vervangt de Wet bescherming persoonsgegevens (Wbp) per 25 mei 2018. Overigens zijn niet alle verwerkingen onder deze wetgeving te scharen. De Wet registratie Persoonsgegevens (BRP) omvat een eigen stelsel aan regels.

2. Onze uitgangspunten

Ons privacybeleid passen wij toe op alle taken en verwerkingsprocessen waarin persoonsgegevens worden verwerkt en waar wij voor verantwoordelijk zijn. Onze medewerkers dragen de verantwoordelijkheid voor het correct omgaan met persoonsgegevens en het waarborgen van de privacyrechten van personen.

Ons college stelt de algemene uitgangspunten voor het Somerens privacybeleid vast. Burgers vinden het privacybeleid via onze site: gemeente@someren.nl. Wij maken afspraken met onze medewerkers via geheimhoudingsverklaringen, privacyprotocollen en integriteitsverklaringen. Met externe partijen leggen wij gemaakte afspraken vast in convenanten of zogenaamde verwerkersovereenkomsten. Hierin ligt besloten wat wij hebben afgesproken over de bescherming van de persoonsgegevens die worden verwerkt.

Persoonsgegevens geven informatie over een individu. Het gaat dan om alle informatie die te herleiden is tot een enkel persoon, zowel direct of indirect. Iemands naam en adres, maar ook een telefoonnummer, of een postcode in combinatie met een huisnummer kan een specifiek persoon duiden. Naast “gewone” persoonsgegevens zijn er “bijzondere” persoonsgegevens, zoals gegevens over iemands ras, godsdienst of burgerservicenummer. Met deze gegevens moet met nóg meer zorg worden omgegaan. Onder de AVG mogen deze gegevens in beginsel niet verwerkt worden tenzij sprake is van een uitzonderingsgrond. “Gewone” persoonsgegevens mogen verwerkt worden enkel en alleen als sprake is van:

1. een publiekrechtelijke taak of;
2. een wettelijke plicht of;
3. een overeenkomst of;
4. expliciete toestemming van de betrokkene of;

5. een vitaal belang van betrokkene.

Bij het verwerken van persoonsgegevens gaan wij uit van de volgende opgesomde basisprincipes.

1. Persoonsgegevens worden in overeenstemming met de wet, en op behoorlijke en zorgvuldige wijze verwerkt.
2. Wij verzamelen en verwerken persoonsgegevens alleen voor een bepaald doel en met een gerechtvaardigde grondslag. Dit betekent dat het doel specifiek en expliciet is vastgelegd in het register van verwerkingen. Wij toetsen de verwerking aan het proportionaliteits- en subsidiariteitsbeginsel. Met andere woorden: staat de verwerking in verhouding met het te dienen doel of kan het doel worden bereikt op een minder ingrijpende manier?
3. Wij informeren u over de verwerking van persoonsgegevens via onze privacyverklaring. Deze is te raadplegen via onze gemeentelijke site: www.someren.nl.
4. U kunt een verzoek indienen om inzage of correctie c.q aanvulling van uw persoonsgegevens of een verzoek tot verwijdering van bepaalde gegevens. Verzoeken worden echter niet automatisch gehonoreerd. Deze worden steeds inhoudelijk en juridisch beoordeelt.
5. Klachten over de wijze waarop wij omgaan met persoonsgegevens behandelen wij op een laagdrempelige en toegankelijke wijze.
6. Wij streven ernaar dat uw persoonsgegevens correct en actueel zijn.
7. Uw persoonsgegevens bewaren wij niet langer dan noodzakelijk. Dit betekent dat wij de gegevens bewaren zolang dat nodig is om de aangevraagde dienst, het product of het verzoek te beoordelen en afte handelen. Daarna worden die gegevens vernietigd. Gegevens die wij langer moeten bewaren wegens een wettelijke verplichting zijn hiervan uitgezonderd.
8. In het geval van samenwerking met derden, of het verstrekken van persoonsgegevens aan derden, maken wij afspraken over de eisen en voorwaarden waaraan de uitwisseling van gegevens moet voldoen. Het delen van persoonsgegevens geschied enkel als dit strikt noodzakelijk is voor de uitvoering van wettelijke taken.
9. Via technische en organisatorische maatregelen borgen wij een passende beveiliging van persoonsgegevens. Deze beveiliging is vastgelegd in ons informatiebeveiligingsbeleid.
10. Wij houden rekening met de bescherming van persoonsgegevens bij de aanschaf, inrichting of ontwikkeling van producten of diensten. Dit doen wij door ervoor te zorgen dat alleen de noodzakelijke personen toegang hebben tot de gegevens, dat de toegang tot de gegevens is afgeschermd én dat onze veiligheidsmaatregelen regelmatig worden gecontroleerd.

3. Rollen en bevoegdheden

Bewustwording van bestuur en medewerkers bepaalt voor een groot deel hoe privacy wordt verankerd binnen onze organisatie. Daarnaast spelen de cultuur en communicatie een rol. Onze organisatie brengt het onderwerp regelmatig onder de aandacht tijdens team- en afdelingsoverleggen. Op ons intranet wordt frequent informatie gepost over nieuwe ontwikkelingen op het gebied van privacy en privacy beveiliging.

Ieder gremium heeft bevoegdheden en heeft een eigen rol te vervullen; die zijn hieronder beknopt weergegeven.

Gemeentelijk bestuur

Het gemeentelijk bestuur is onderverdeeld in het college van burgemeester en wethouders en de gemeenteraad.

College

- Verantwoordelijk voor het naleven van privacywetgeving. Voert proactief privacybeleid op basis van afweging van belangen en risico's bij de verwerking van persoonsgegevens.
- Stelt beleid vast voor de bescherming van privacy op basis van wet- en regelgeving.
- Legt verantwoording aan de gemeenteraad af over het uitvoeren van het privacybeleid.
- Documenteert beleid en maatregelen ten behoeve van de aantoonplicht.
- Beheer en onderhoud van het register van verwerkingen.
- Wijst de Functionaris voor de gegevensbescherming als interne toezichthouder aan.

Gemeenteraad

- Vanuit de Gemeentewet heeft de gemeenteraad een controlerende taak en ziet hierop toe.

Ambtelijke organisatie

Binnen de ambtelijke organisatie zijn de taken en bevoegdheden rondom privacy onder gebracht bij de onderstaande functionarissen.

Functionaris voor de gegevensbescherming (FG)

De AVG stelt deze functie verplicht voor overheidsorganen. De FG opereert als onafhankelijke, interne toezichthouder. De wetgever heeft de volgende 5 taken aan de FG gegeven.

- Intern toezicht op naleving van de AVG.
- Het bevorderen van bewustzijn over de AVG in de organisatie.
- Adviesrol op het gebied van de AVG –primair naar management en bestuur- vooral over het uitvoeren van een Privacy Impact Assesment (PIA). Dit is een risicoanalyse die wordt gemaakt op het moment dat er bijzondere persoonsgegevens of persoonsgegeven op grote schaal worden verwerkt.
- Optreden als contactpersoon en samenwerkingspartner naar de Autoriteit Persoonsgevens (AP). Deze instantie controleert gemeenten op het correct naleven van de wet.
- De FG rapporteert als het nodig is rechtstreeks aan het college.

Privacy Officer

De PO voert het privacybeleid van de organisatie uit. De medewerker algemeen juridische zaken vervult momenteel deze rol. Taken die de functionaris uitvoert zijn de volgende.

- Adviseur op het vlak van privacy binnen onze organisatie, primair gericht naar de ambtelijke organisatie.
- Coördineert en stelt privacy beleid op.
- Coördineert en voert actiepunten uit het privacy beleid uit.
- Coördineert en handelt verzoeken van burgers omtrent privacy rechten uit, zoals verzoek om inzage, correctie/aanvulling of verwijdering van persoonsgegevens.
- Rapporteert over privacy aan het management, het college of de gemeenteraad.

Het scheiden van de functies, FG en PO voorkomt dat de FG zijn eigen werk moet controleren. Dit bevordert niet alleen de kwaliteit maar ook de integriteit.

Chief Information Security Officer (CISO)
De beveiliging van informatie is gebaseerd op de Baseline Informatiebeveiliging Gemeenten (BIG), een landelijke standaard voor gemeenten. De CISO is verantwoordelijk voor advisering over en coördinatie van de informatiebeveiliging. De taken van de CISO hebben betrekking op:

- beleid en coördinatie;
- controle en registratie;
- communicatie en voorlichting;
- advies en rapportage.

Management en medewerkers
Ons management en medewerkers zijn zich bewust van het belang van privacy. Dit belang werkt door in hun werkwijze. Wij zetten ons in om de aanwezige kennis te optimaliseren. Dit doen we door het inzetten van leermiddelen, zoals e-learning, bespreking van casuïstiek, al dan niet in samenwerking met de PO, CISO en/of de FG. Nieuwe medewerkers worden via een instructieprogramma op het door ons gewenste niveau gebracht. Hoewel de eindverantwoordelijkheid over de doel- en rechtmatigheid ten aanzien van naleving van wet- en regelgeving bij het management ligt, voelen wij ons hiervoor gezamenlijk verantwoordelijk.

4. Informatiebeveiliging

Ons informatiebeveiligingsbeleid is in 2015 vastgesteld en wordt in 2018 geactualiseerd. Hierin hebben we de pijlers beschreven die de beveiliging van informatie dragen. De technische, fysieke en organisatorische maatregelen die wij hebben getroffen om de informatie te beschermen en er voor te zorgen dat onze gemeente voldoet aan de eisen die er vanuit wet- en regelgeving worden gesteld.

Concreet betekent het beveiligen van informatie dat de processen en informatiesystemen en stromen met alle daarin opgeslagen gegevens worden beschermd tegen vernietiging, verlies, diefstal en onbevoegde toegang. Het is gericht op preventieve, detectieve, repressieve en correctieve maatregelen, met als doel zo optimaal mogelijk de informatie en de systemen te beveiligen.

Als zich ondanks al onze maatregelen en inspanningen toch een incident voordoet waarbij persoonsgegeven zijn betrokken dan wordt dit direct gemeld bij het Datalekteam. Dit team bestaat uit de CISO, de PO en de FG. Deze beoordelen de melding en ondernemen de nodige vervolgstappen.

5. Uitwisseling met externe partijen

Wij werken veel samen met externe partijen. Niet alleen via samenwerkingsverbanden maar ook partijen die als opdrachtnemer informatie namens ons verwerken. Denk bijvoorbeeld aan softwareleveranciers en adviesbureaus. Binnen deze verbanden hechten wij uiteraard ook veel belang aan de bescherming van persoonsgegevens. Hierover

maken wij afspraken met deze partijen die wij vervolgens vastleggen in onder meer convenanten, algemene voorwaarden, of zogenaamde verwerkingsovereenkomsten.

Via deze verwerkingsovereenkomsten liggen afspraken vast rondom de waarborgen van privacyverplichtingen en beveiliging van persoonsgegevens. Ons informatiebeveiligingsbeleid is in 2015 vastgesteld en wordt in 2018 geactualiseerd. Onze PO heeft het beheer en bewaking van de naleving van de gemaakte afspraken in het takenpakket.

6. Privacy waarborgmaatregelen

De onderstaande maatregelen hebben wij getroffen met als doel de persoonsgegevens rechtmatig, behoorlijk en transparant te kunnen verwerken, overeenkomstig de van toepassing zijnde wet- en regelgeving.

1. Transparantie

Betrokkene(n) 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.

2. Bewustwording

Van eminent belang voor het borgen van de privacy! Daarom hebben wij oog voor de bewustwording van privacy binnen onze organisatie.

3. Register van verwerkingen

Wij houden een register van verwerkingen bij waarin alle verwerkingsactiviteiten van persoonsgegevens zijn opgenomen. Dit register wordt periodiek bijgewerkt.

4. Privacy Impact Assessment (PIA)

Aandacht voor privacyrisico's op het moment dat er nieuwe technologieën worden gebruikt of als er nieuw beleid wordt ingevoerd. In dat geval voeren wij een PIA uit. Een PIA is een methode om bij risicovolle verwerkingen de mogelijke effecten op de privacy in kaart te brengen opdat hiertegen de juiste maatregelen kunnen worden getroffen om de die risico zo veel als mogelijk te minimaliseren.

5. Het melden van datalekken

Er is een procedure voor het melden van incidenten informatieveiligheid. Deze procedure ziet ook toe op het melden van datalekken. De gemelde incidenten worden opgenomen in een register.

6. Toezicht en evaluatie

Via audits controleert de FG of onze praktijk voldoet aan het beleid en wet- en regelgeving. Daarnaast legt het college jaarlijks verantwoording af aan de gemeenteraad over de risico's en beheersmaatregelen met betrekking tot het privacybeleid. Dit verloopt

via de begroting en jaarrekening onder de paragraaf bedrijfsvoering. Ons privacybeleid evalueren wij in 2020.

7. Externe partijen

Wij werken veel samen met externe partijen. Niet alleen via samenwerkingsverbanden maar ook partijen die als opdrachtnemer informatie namens ons verwerken. Denk bijvoorbeeld aan softwareleveranciers en adviesbureaus. Binnen deze verbanden hechten wij uiteraard ook veel belang aan de bescherming van persoonsgegevens. Hierover maken wij afspraken met deze partijen die wij vervolgens vastleggen in onder meer convenanten, algemene voorwaarden, of zogenaamde verwerkingsovereenkomsten

7. Rechten van betrokkenen

De rechten van betrokkenen zijn onder de vlag van AVG verruimd ten opzichte van de oude privacywetgeving. Welke rechten dat zijn staan hieronder opgesomd.

1. Recht op informatie

Wij moeten het publiek informeren over onze gegevensverwerkingen. Zij hebben het recht om te weten wat er met die gegevens gebeurd en waarom.

2. Recht op inzage

Via dit recht kan de betrokkene een verzoek indienen om in te zien of/en op welke manier zijn/haar gegevens worden verwerkt.

3. Recht op rectificatie en verwijdering

Betrokkenen kunnen een verzoek indienen om gegevens te corrigeren als duidelijk is dat er gegevens niet kloppen. Via dit verzoek kan worden gevraagd om persoonsgegeven te verbeteren, aan te vullen, te verwijderen of af te schermen.

4. Recht om vergeten te worden

Een verruiming ten opzichte van de oude wetgeving is het recht om vergeten te worden. Als persoonsgegevens openbaar zijn gemaakt dan kan een verzoek worden ingediend om vergeten te worden. Koppelingen en kopieën van de gegevens worden als het verzoek wordt ingewilligd, gewist. Ook hier geldt dat aan de voorwaarden die de AVG stelt is voldaan.

5. Recht op dataportabiliteit

Betrokkenen hebben het recht op overdraagbaarheid van gegevens. Dit betekent dat deze het recht heeft om gegevens te ontvangen die wij van de betrokkene hebben zodat hij/zij deze kan overdragen naar een andere organisatie. Indien gewenst dragen wij die gegevens rechtsreeks over aan die andere organisatie.

6. Recht op beperking

In bepaalde gevallen is er recht op het tijdelijk niet meer gebruiken van persoonsgegevens.

7. Recht van bezwaar

Er kan bezwaar gemaakt worden tegen de verwerking van zijn/haar persoonsgegevens wegens algemeen belang of een gerechtvaardigd belang. In dat geval moet de verwerking van de persoonsgegevens worden gestaakt, tenzij er dwingende gerechtvaardigde gronden voor de verwerking zijn die zwaarder wegen dan bijvoorbeeld het belang van de betrokkene.

8. Recht om niet onderworpen te worden aan geautomatiseerde individuele besluitvorming waaronder profilering

In dit geval moet het gaan om besluiten die op basis van automatisch verwerkte gegevens worden genomen mét consequenties voor de betrokkene. Iedereen heeft recht op een menselijke blik. Dit betekent dat als de betrokkene hierop een beroep doet dat het besluit opnieuw moet worden getoetst met die menselijke blik. Een voorbeeld hiervan is een verwerking van een sollicitatie via internet zonder menselijke tussenkomst.

Punt van aandacht!

Een beroep doen op een van de bovengenoemde rechten of bezwaren kan schriftelijk en digitaal worden ingediend ter attentie van de PO via het emailadres gemeente@someren.nl

Verzoeken en bezwaren worden geregistreerd en door de PO behandeld. Het verzoek wordt getoetst aan de wetgeving. Of het verzoek wordt ingewilligd hangt af van deze beoordeling en de individuele omstandigheden.
Tegen een eventuele (gemotiveerde) afwijzing staan bezwaar- en beroepsmogelijkheden open.

Gemeente
Someren

Postadres Postbus 290, 5710 AG Someren **Bezoekadres** Wilhelminaplein 1, 5711 EK Someren
Telefoon 0493 - 494 888 **Telefax** 0493 - 494 850 **E-mail** gemeente@someren.nl **Website** www.someren.nl