

Bekendmaking Algemeen privacybeleid gemeente Steenbergen

1 Inleiding

De gemeente Steenbergen verwerkt persoonsgegevens voor de goede uitvoering van haar publiekrechtelijke taken en in het kader van de bedrijfsvoering. De gemeente verzamelt en bewerkt persoonsgegevens voor de dienstverlening aan inwoners en bedrijven. Als gevolg van de decentralisaties van de Jeugdwet, Wmo 2015 en de Participatiewet beschikt de gemeente Steenbergen over nieuwe klantgroepen en dus nieuwe (bijzondere) persoonsgegevens. De beschikking over deze gegevens vormt een nieuwe belangrijke verantwoordelijkheid. Daarnaast zal de gemeente door deze taakuitbreiding vaker persoonsgegevens willen uitwisselen met andere instanties. De complexiteit van de bescherming van de persoonlijke levenssfeer van inwoners van de gemeente is hiermee toegenomen.

De gemeente vindt het belangrijk dat inwoners kunnen vertrouwen op een veilige verwerking van persoonsgegevens. Bescherming van persoonsgegevens is immers een grondrecht. Burgers hebben er recht op dat persoonsgegevens op een rechtmatige manier worden verwerkt. Uitgangspunt is dat de gemeente zorgvuldig en veilig, proportioneel en vertrouwelijk omgaat met persoonsgegevens. Een zorgvuldige omgang met de gegevens van burgers is van groot belang voor het vertrouwen van burgers in de overheid. De gemeente geeft met dit algemene privacybeleid verdere invulling aan de verplichtingen en bevoegdheden die uit de privacywetgeving voortvloeit. De Algemene Verordening Gegevensbescherming en andere bij specifieke wet geregelde privacyregimes vormen het formele kader van de gemeente Steenbergen. Naast dit algemene privacybeleid, is er ook aanvullend beleid opgesteld voor het sociaal domein.

2 Uitgangspunten

Het gemeentelijk privacybeleid is van toepassing op alle taken en verwerkingsprocessen waar persoonsgegevens worden verwerkt en waar de gemeente Steenbergen voor verantwoordelijk is. Bij het verwerken van persoonsgegevens worden de volgende uitgangspunten in acht genomen:

1. Gegevens van burgers worden binnen de kaders van de geldende wet- en regelgeving en op behoorlijke en zorgvuldige wijze verwerkt.
2. De inbreuk op de eerbiediging van de persoonlijke levenssfeer van de burger wordt zoveel mogelijk beperkt (subsidiariteit).
3. De inbreuk op de belangen van de burger mag niet onevenredig zijn in verhouding tot het met de verwerking te dienen doel (proportionaliteit).
4. Gegevens worden enkel gebruikt voor het met de verwerking te dienen doel en kunnen alleen worden gebruikt voor andere doelen of worden gedeeld voor zover de wet dat toestaat. De gemeente streeft naar minimale gegevensverwerking. Waar mogelijk worden minder of geen persoonsgegevens verwerkt.
5. Persoonsgegevens worden niet langer bewaard dan noodzakelijk.
6. In geval van samenwerking met derden, dan wel verstrekking van persoonsgegevens aan derden, worden afspraken gemaakt over de eisen en voorwaarden waar gegevensuitwisseling aan moet voldoen.
7. De burger wordt op een proactieve en transparante wijze geïnformeerd over de verwerking van persoonsgegevens door de gemeente. De gemeente geeft in voorkomend geval gehoor aan inzagen/of correctieverzoeken, dan wel verwijderingverzoeken. Afhandeling van klachten gebeurt op een laagdrempelige, toegankelijke wijze.
8. De gemeente borgt middels technische en organisatorische maatregelen dat onbevoegde toegang en onbevoegd gebruik van gegevens wordt voorkomen.
9. Bij aanschaf, inrichting of ontwikkeling van producten of diensten houdt de gemeente rekening met de eerbiediging van de persoonlijke levenssfeer van burgers.
10. Beveiligingsincidenten waar potentieel persoonsgegevens bij betrokken zijn worden direct gemeld bij de Functionaris voor de gegevensbescherming.

3 Het wettelijk kader

Het recht op eerbiediging van de persoonlijke levenssfeer bij het verwerken van persoonsgegevens is een grondrecht. Het recht op privacy is niet alleen nationaal als grondrecht erkend, maar ook internationaal in onder andere het Europees Verdrag voor de Rechten van de Mens en het Internationaal kinderrechtenverdrag.

1 Europese privacywetgeving

De huidige privacywetgeving, de Wet Bescherming Persoonsgegevens (hierna: de WBP), is gebaseerd op de Europese privacyrichtlijn uit 1995. De WBP vereist dat het College van B&W borgt dat de personen over wie de gemeente gegevens bijhoudt, op een passende manier beschermt worden tegen risico's van de informatiemaatschappij. De WBP werd opgesteld toen het internet en de technische mogelijkheden die het gebruik van internet biedt, nog in de kinderschoenen stond. Daarom is de Europese privacywetgeving de afgelopen jaren herzien.

Op 24 mei 2016 is de Algemene verordening gegevensbescherming (hierna: AVG) in werking getreden. De AVG zal vanaf 25 mei 2018 direct van toepassing zijn en, vanaf die datum, de Wet Bescherming Persoonsgegevens vervangen. De snelle technologische ontwikkelingen, de grote hoeveelheid beschikbare data en de aanzienlijke toename van de grensoverschrijdende stromen van persoonsgegevens heeft geleid tot harmonisatie van het Europees Unierecht met betrekking tot de bescherming van persoonsgegevens.

Het begrip persoonsgegevens omvat alle gegevens die een natuurlijk identificeerbaar persoon betreffen. NAW-gegevens, Burgerservicenummers, e-mail, maar ook kentekens en IP-adressen kunnen als persoonsgegeven worden aangemerkt, omdat deze kunnen leiden tot een persoon.

De AVG zorgt voor een versterking en uitbreiding van privacyrechten en brengt meer verantwoordelijkheden voor organisaties. De gemeente dient aan te (kunnen) tonen dat er is voldaan aan de wettelijke vereisten omtrent gegevensbescherming. Elke verwerking van persoonsgegevens dient behoorlijk en rechtmatig te geschieden en voor burgers dient het transparant te zijn dat hen betreffende persoonsgegevens worden verzameld, gebruikt of geraadpleegd. Persoonsgegevens mogen enkel worden verwerkt indien het doel van de verwerking niet redelijkerwijs op een andere wijze kan worden verwezenlijkt.

De opslagperiode dient niet langer te zijn dan noodzakelijk voor het doel waar de persoonsgegevens voor zijn verzameld. Wanneer er geen concrete bewaartermijn in de wet is opgenomen voor een bepaald gegeven, bijvoorbeeld op grond van belastingwetgeving of op grond van de Archiefwet, betekent dit dat de gegevens vernietigd moeten worden als zij niet meer nodig zijn.

2 Grondslagen gegevensverwerking

De gemeente Steenbergen verwerkt enkel gegevens indien aan ten minste een van de onderstaande voorwaarden is voldaan:

1. Er is sprake van expliciete toestemming van de betrokkene;
2. Er is sprake van een overeenkomst;
3. Er is sprake van een wettelijke plicht;
4. Er is sprake van een vitaal belang van de betrokkene;
5. Er is sprake van een publiekrechtelijke taak;
6. Er is sprake van een gerechtvaardigd belang dat boven het privacybelang van betrokkene staat.

Bijzondere persoonsgegevens zijn gegevens die betrekking hebben op iemand godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele voorkeur en/of strafrechtelijk verleden.

Deze persoonsgegevens worden door de gemeente Steenbergen met extra zorgvuldigheid beveiligd en verwerkt.

De gemeente Steenbergen verzamelt en verwerkt persoonsgegevens enkel voor een bepaald doel. Dit doel is specifiek en nadrukkelijk beschreven in het documentatieregister. Daarnaast wordt de verwerking getoetst aan het proportionaliteitsbeginsel en het subsidiariteitsbeginsel. Dit houdt in dat de verwerking in verhouding staat met het beoogde doel en er enkel gegevens worden verwerkt indien dit niet op een minder ingrijpende wijze kan worden bereikt.

3 Sectorspecifieke wetgeving

De voorwaarden en eisen die zowel de WBP als de AVG stellen, fungeren als parapluwetgeving: bijna alle sectoren, instellingen en bedrijven in Nederland dienen eraan te voldoen. Naast dit algemeen wettelijk kader zijn er in sectorspecifieke wetten aanvullende regels opgenomen omtrent gegevensuitwisseling en het waarborgen van privacy. De Jeugdwet, de Wet Basisregistratie Personen, de Participatiewet en de WMO 2015 zijn voorbeelden van dergelijke wetgeving met specifieke aanvullende eisen. De gemeente Steenbergen heeft nadere beleidsregels en protocollen opgesteld omtrent het verwerken van persoonsgegevens in het sociaal domein.

4 Governance

Privacy is voor een belangrijk deel een zaak van bewustwording, cultuur en communicatie. Bestuur, ambtenaar en hulpverlener moeten zich bij de uitoefening van hun werk voortdurend bewust zijn van het belang van het waarborgen van de eerbiediging van de persoonlijke levenssfeer van de burger. De gemeente zal dit bewustwordingsproces ondersteunen door het ontwikkelen van privacyprotocollen en afwegingskaders en het geven van trainingen.

1 De eindverantwoordelijkheid

Het college van Burgemeester en Wethouders is in het merendeel van de verwerkingen verwerkingsverantwoordelijk voor de zorgvuldigheid van de gegevensverwerking die door of namens de gemeente plaats vindt. Er zijn echter ook verwerkingen waar enkel de burgemeester of de gemeenteraad de eindverantwoordelijkheid draagt.

Het College is voor de wijze waarop het invulling geeft aan het privacybeleid verantwoording verschuldigd aan de Gemeenteraad. Om privacy goed te borgen in de organisatie is het van belang dat er in de lijnorganisatie genoeg aandacht is voor dit onderwerp. De rollen en verantwoordelijkheden dienen te worden bepaald en vastgelegd.

1. Het College stelt het gemeentelijk privacybeleid vast met inachtneming van de aanbevelingen van de functionaris voor de gegevensbescherming en bevordert de beschikbaarheid van voldoende middelen om privacybescherming passend te waarborgen.
2. Het College wijst een functionaris voor de gegevensbescherming (hierna: FG) aan voor onafhankelijk toezicht op de uitvoering van het privacybeleid conform artikel 37 van de Algemene Verordening Gegevensbescherming.
3. Het college stelt een Privacybeheerder aan voor het adviseren over praktische privacyvraagstukken binnen de organisatie.
4. Het college wijst uit haar midden een portefeuillehouder privacy & gegevensbescherming aan die bestuurlijk verantwoordelijk is voor de uitvoering van het gemeentelijk privacybeleid en voor controle op de naleving van afspraken. De feitelijke uitvoering wordt opgedragen aan de functionaris voor de gegevensbescherming.
5. De portefeuillehouder privacy ziet toe op de ontwikkeling en uitvoering van themagericht privacybeleid. De privacybeheerder en de FG rapporteren minstens één keer per jaar aan de portefeuillehouder over de resultaten die zij hieromtrent hebben bereikt. Privacy vormt een onderdeel van het planning en control proces van de gemeente. De portefeuillehouder informeert de Raad binnen de jaarlijkse planning en control cyclus over het privacybeleid binnen de gemeente.

2 Intern: Advies, controle en Toezicht

Door de functies advies en controle te scheiden, wordt voorkomen dat de Functionaris voor de gegevensbescherming toezicht moet houden op zijn eigen werk en waarborgt de gemeente haar geloofwaardigheid en betrouwbaarheid. Dit komt de kwaliteit ten goede.

- a. Functionaris voor de gegevensbescherming
De Functionaris voor de gegevensbescherming fungeert als onafhankelijke interne toezichthouder. Hij ziet toe op de naleving van de Verordening, andere privacywetgeving en het beleid van de gemeente Steenbergen met betrekking tot de bescherming van persoonsgegevens, inclusief de toewijzing van verantwoordelijkheden, bewustmaking en opleiding van de medewerkers. Om deze taak uit te voeren heeft de Functionaris voor de gegevensbescherming controlebevoegdheden, zoals nader bepaald in de Regeling toezichtbevoegdheden Functionaris voor de gegevensbescherming. Daarnaast geeft hij advies omtrent de uit te voeren gegevensbeschermingseffectbeoordelingen en ziet toe op de uitvoering hiervan. De Functionaris rapporteert zo nodig rechtstreeks aan het College.
- b. de Privacybeheerder
Binnen de gemeente wordt een Privacybeheerder aangesteld. De privacybeheerder vormt de vraagbaak binnen de gemeente voor privacyvraagstukken, geeft advies omtrent de uitvoering en draagt bij aan kennisverspreiding en cultuur. Tevens actualiseert de privacybeheerder het register van verwerkingen en controleert de verwerkingen op rechtmatigheid.

3 Privacy op de werkvloer

Alle medewerkers van de gemeente Steenbergen dienen bij te dragen aan de eerbiediging van de persoonlijke levenssfeer bij de verwerking van persoonsgegevens. Privacy dient dan ook ingebed te zijn in de door hen te hanteren werkwijze(n). De gemeente werkt actief aan het optimaliseren van kennis

omtrent privacy en een transparante procesuitvoering. Individuele casussen, bevindingen en vragen omtrent dit onderwerp worden voorgelegd aan de Privacybeheerder.

De leidinggevenden zien toe op de naleving van wet- en regelgeving en het privacybeleid. De leidinggevende zorgt ervoor dat de FG naar behoren en tijdig wordt geïnformeerd en betrokken bij gelegenheden die verband houden met de bescherming van persoonsgegevens, zodat de FG zijn taken adequaat kan uitvoeren. Wanneer persoonsgegevens tussen de verschillende afdelingen worden uitgewisseld worden hier afspraken over gemaakt.

4 Informatieveiligheid

De gemeente neemt passende technische en organisatorische maatregelen teneinde persoonsgegevens te beveiligen tegen verlies, onbevoegde toegang of onrechtmatige verwerking. Hoe gevoeliger de informatie is, des te hoger het beveiligingsniveau. Daarnaast besteedt de gemeente Steenbergen reeds bij de ontwikkeling en aanschaf van producten en diensten aandacht aan privacy verhogende maatregelen.

In 2017 is het informatieveiligheidsbeleid vastgesteld, waarin kaders en maatregelen voor de beveiliging van (persoons)gegevens zijn opgenomen. Het beschermingsniveau van data wordt uitgedrukt in classificatieniveaus voor beschikbaarheid, integriteit en vertrouwelijkheid van informatie:

- Beschikbaarheid: hoeveel en wanneer data toegankelijk is en gebruikt kan worden.
- Integriteit: het in overeenstemming zijn van informatie met de werkelijkheid en dat niets ten onrechte is achtergehouden of verdwenen.
- Vertrouwelijkheid: de bevoegdheden en de mogelijkheden tot muteren, kopiëren, toevoegen, vernietigen of kennismaken van informatie voor een gedefinieerde groep van gerechtigden.

Met het toekennen van classificatieniveaus aan data en/of informatiesystemen is van groot belang, omdat daarmee het vereiste beschermingsniveau kenbaar gemaakt wordt. In het geval zich – ondanks de getroffen maatregelen – een beveiligingsincident voor doet waarbij persoonsgegevens zijn betrokken, wordt dit direct gemeld bij de FG. Onder een dergelijk beveiligingsincident valt onbevoegde toegang of kennisname van persoonsgegevens, dan wel verlies of onjuiste vernietiging van bestanden welke persoonsgegevens bevat.

5 Uitwisseling met en (intergemeentelijke) samenwerking met derden

Met het oog op de bescherming van persoonsgegevens maakt de gemeente Steenbergen met externe partijen afspraken omtrent de omgang met privacy. Dit kan in bijvoorbeeld convenanten of verwerkersovereenkomsten. Deze afspraken voldoen aan de wet.

1 Convenanten

Indien de gemeente Steenbergen structureel informatie uitwisselt of samenwerkt met externe organisaties of andere gemeenten, maakt de gemeente Steenbergen vooraf duidelijke afspraken over de gegevensuitwisseling in de vorm van een convenant.

2 Verwerkersovereenkomst¹

Als de gemeente Steenbergen een externe vraagt voor haar gegevens te verwerken is het College verplicht met die externe een verwerkersovereenkomst te sluiten. In de verwerkersovereenkomst worden afspraken gemaakt omtrent de waarborgen en beveiliging van persoonsgegevens. De FG ziet toe op de naleving van de verwerkersovereenkomst.

6 Maatregelen

Om de privacy van haar burgers optimaal te kunnen waarborgen voert de gemeente Steenbergen een gegevensbeschermingseffectbeoordeling uit als dit nodig is en houdt zij een register van verwerkingen bij.

1 Gegevensbeschermingseffectbeoordeling²

Bij de invoering van nieuw beleid of regelgeving of bij het gebruik van nieuwe technologieën houdt de gemeente Steenbergen rekening met de bescherming van de persoonlijke levenssfeer door een gegevensbeschermingseffectbeoordeling uit te voeren. Het college besluit van geval tot geval over de noodzaak daarvoor.

De volgende indicatoren zullen daarbij als toetsingskader worden gehanteerd:

1) In de Wbp wordt een dergelijke overeenkomst aangeduid als bewerkersovereenkomst.

2) Ook wel Data Protection Impact Assessment genoemd (DPIA)

- een nieuwe gemeentelijke taak;
- aanleg van een groot databestand;
- verwerking van bijzondere persoonsgegevens;
- aanschaf van een nieuw ICT-systeem;
- systematische gegevensuitwisseling met een externe.

In het geval sprake is van één of meerdere indicatoren, kan de uitvoering van een (externe) PIA in de rede liggen.

In de gegevensbeschermingseffectbeoordeling komt ten minste naar voren:

- Een systematische beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden;
- Een beoordeling van de noodzaak en de evenredigheid van de verwerkingen;
- Een beoordeling van de risico's voor de rechten en vrijheden van burgers;
- De beoogde maatregelen om de risico's aan te pakken

Wanneer het effect van een verwerking beoordeeld is, wordt de Functionaris voor Gegevensbescherming geraadpleegd en om advies gevraagd.

2 Register van verwerkingen

De gemeente Steenbergen houdt een register van verwerkingen bij met alle verwerkingsactiviteiten van persoonsgegevens per proces³. De privacybeheerder controleert en actualiseert het register. Onder andere de doeleinden van de verwerkingen, de categorieën van persoonsgegevens, derden ontvangen en de rechtmatige grondslag worden hierin opgenomen.

7 Positie en rechten van de burger

Transparantie richting de burgers staat bij de gemeente Steenbergen voorop. Naast informatie over de doeleinden van de verwerkingen, de categorieën van de verwerkte gegevens, de herkomst van de gegevens en de ontvangers verstrekt de gemeente ook informatie over de mogelijkheid van geautomatiseerde besluitvorming, alsmede de bewaartermijnen en klachtrechten. Burgers hebben de volgende rechten:

- Recht op informatie: Betrokkenen hebben het recht om aan de gemeente te vragen of zijn/haar persoonsgegevens worden verwerkt;
- Inzagerecht: Betrokkenen hebben de mogelijkheid om te controleren of, en op welke manier, zijn/haar gegevens worden verwerkt;
- Correctierecht: Als duidelijk wordt dat de gegevens niet kloppen, kan de betrokkene een verzoek indienen bij de gemeente om dit te corrigeren;
- Recht van verzet: Betrokkenen hebben het recht aan de gemeente te vragen om hun persoonsgegevens niet meer te gebruiken;
- Recht om vergeten te worden: In gevallen waar de betrokkene toestemming heeft gegeven om gegevens te verwerken, heeft de betrokkene het recht om de persoonsgegevens te laten verwijderen.
- Recht op bezwaar: Betrokkenen hebben het recht om bezwaar aan te maken tegen de verwerking van zijn/haar persoonsgegevens. De gemeente zal hieraan voldoen, tenzij er gerechtvaardigde gronden zijn voor de verwerking.

Klachten en verzoeken met betrekking tot de bescherming van de persoonlijke levenssfeer worden direct doorgegeven aan de afdeling waar de klacht betrekking op heeft. Dit kan zowel schriftelijk als via de e-mail ingediend worden. De leidinggevende is verantwoordelijk voor de afwikkeling en het treffen van verbetermaatregelen. Daarnaast wordt de klacht doorgegeven aan de Functionaris voor de gegevensbescherming, alwaar deze wordt geregistreerd. Burgers die – ondanks de gevolgde procedure - niet tevreden zijn over de wijze van afwikkeling van zijn of haar klachten kunnen zich rechtstreeks beklagen bij de Functionaris voor de gegevensbescherming.

3) Register overeenkomstig artikel 30 Avg