

Gemeente Stein

Privacyreglement

Documentcode:	
Versie:	2.0
Versiedatum	05-06-2018
Gemaakt door:	Privacycoördinator / FG
Goedgekeurd door:	Managementteam / Gemeentesecretaris / College B&W

Versiegegevens

Datum	Versie	Gemaakt door	Omschrijving van de aanpassing
05-06-2018	1.0	Privacycoördinator	Basisdocument
07-06-2018	1.1	Privacycoördinator	Tekstuele aanpassingen na review PIT en FG
10-06-2018	2.0	Privacycoördinator	Definitieve versie

Inhoudsopgave

PRIVACYREGLEMENT GEMEENTE STEIN	4
1. DE STEINSE AANPAK	4
2. WETGEVING EN DEFINITIES	4
3. REIKWIJDTE	5
4. VERANTWOORDELIJKE VOOR DE VERWERKING	5
5. VERWERKINGEN (ARTIKEL 4, AVG)	6
6. DOELEINDEN (ARTIKEL 5, AVG)	6
7. RECHTMATIGE GRONDSLAG (ARTIKEL 6, AVG)	7
8. WIJZE VAN VERWERKING	8
8.1. ORGANISATORISCHE MAATREGELEN	8
8.2. BEVEILIGING	8
8.3. MELDEN VERWERKINGEN	9
9. DOORGIFTE AAN DERDEN	9
10. TRANSPARANTIE EN COMMUNICATIE	9
10.1. WET OPENBAARHEID VAN BESTUUR (WOB)	9
10.2. WET HERGEBRUIK VAN OVERHEIDSINFORMATIE	9
10.3. INFORMATIEPLICHT	10
10.4. VERWIJDERING	10
10.5. RECHTEN VAN BETROKKENEN (ARTIKEL 13 T/M 20, AVG)	10
10.6. INDIENEN VAN VERZOEK	10
11. GEAUTOMATISEERDE VERWERKINGEN	11
11.1. PROFILERING (ARTIKEL 22, AVG)	11
11.2. BIG DATA EN TRACKING	11
11.3. INZET VAN CAMERA'S	11
12. PLICHTEN VAN DE GEMEENTE	11
12.1. REGISTER VAN VERWERKINGEN (ARTIKEL 30, AVG)	11

12.2.	BEWAARTERMIJNEN.....	11
12.3.	MELDPLICHT DATALEKKEN (ARTIKEL 33, 34 AVG).....	12
12.4.	VERWERKERSOVEREENKOMST.....	12
12.5.	DATA PROTECTION IMPACT ASSESSMENT (DPIA) (ARTIKEL 35, AVG)	12
12.6.	PRIVACY BY DESIGN EN PRIVACY BY DEFAULT	13
12.7.	FUNCTIONARIS VOOR DE GEGEVENSBECHERMING (ARTIKEL 37 T/M 39, AVG)	13
12.8.	VERANTWOORDELIJKHEID	13
13.	AFSLUITING	14
14.	SLOTBEPALING	14
15.	FORMELE VASTSTELLING	14

Privacyreglement Gemeente Stein

Privacy speelt een belangrijke rol in de relatie tussen de burger en de overheid en staat daarmee hoog op de bestuurlijke agenda. Gemeenten hebben de verantwoordelijkheid over persoonsgegevens en gegevensuitwisseling op alle terreinen waar ze actief zijn. Gemeenten zijn verplicht om zorgvuldig en veilig, proportioneel en vertrouwelijk om te gaan met het verzamelen, bewaren en beheren van persoonsgegevens van burgers. Maar óók voor de verwerking van persoonsgegevens van het personeel en sollicitanten (P&O). Dat geldt voor alle gemeentelijke taken. Goed en zorgvuldig omgaan met persoonsgegevens is een dagelijkse bezigheid van gemeenten. Het beschermen van de privacy is complex, en wordt steeds complexer door technologische ontwikkelingen, de decentralisaties, grote uitdagingen op het terrein van veiligheid en nieuwe Europese wetgeving. Daarom vinden wij het belangrijk om transparant te zijn over de manier waarop wij met persoonsgegevens omgaan, en de privacy waarborgen.

1. De Steinse aanpak

De Gemeente Stein respecteert en beschermt de privacy en persoonsgegevens van haar burgers. In de uitoefening van haar publiekrechtelijke taak houdt zij zich aan de wet en zoekt waar mogelijk de ruimte om de privacybelangen van zowel de burger als de doelstellingen van de gemeente naar beste inzicht te behartigen.

Als Gemeente Stein vinden wij het belangrijk dat onze medewerkers privacybewust zijn. Dit verkleint de kans op onjuist gebruik van gegevens, lekken en nadelige gevolgen zoals boetes en negatieve publiciteit. Daarnaast tonen we hiermee aan dat wij als gemeente beschikken over medewerkers die bewust zijn van de risico's bij het werken met persoonsgegevens. Om privacybewust te worden en uiteindelijk ook te zijn, zorgt de gemeente voor bewustwordingscampagnes, kennissessies en workshops op het gebied van privacy en omgaan met persoonsgegevens. Tevens stelt de gemeente diverse handleidingen, factsheets en overige materialen ter beschikking om de medewerker in hun werkzaamheden handvatten te bieden bij het verwerken van de persoonsgegevens waarmee zij werken.

2. Wetgeving en definities

Vanaf 25 mei 2018 is de Europese Verordening; de Algemene Verordening Gegevensbescherming (AVG), in werking getreden, samen met de uitvoeringswet. De AVG bouwt voort op de Wbp en zorgt onder andere voor versterking en uitbreiding van de privacyrechten met meer verantwoordelijkheden voor organisaties.

De volgende begrippen worden in de AVG gebruikt (Artikel 4, AVG):

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

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 of het Burgerservicenummer (BSN). Deze gegevens mogen in principe niet worden verwerkt. Of alleen worden gebruikt bij uitdrukkelijke toestemming van de betrokkene, wanneer de gegevens door de betrokkene duidelijk openbaar zijn gemaakt of wanneer de wet het toestaat.

Data Protection Impact Assessment (DPIA): in het Nederlands gegevensbeschermingseffectbeoordeling genoemd. Met een Data Protection Impact Assessment worden de effecten en risico's van de nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy.

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

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

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

Overige wetgeving om in het bijzonder rekening mee te houden:

Wet openbaarheid van bestuur (Wob): Via de Wob (en straks wellicht de Wet Open Overheid) kun je een verzoek om informatie indienen bij de gemeente. Bij het verzoek bekijkt de gemeente altijd of het antwoord geen inbreuk maakt op de persoonlijke levenssfeer van betrokkenen. In principe worden geen persoonsgegevens verstrekt.

Wet hergebruik van overheidsinformatie: De Wet hergebruik van overheidsinformatie regelt het op verzoek verstrekken van overheidsinformatie voor hergebruik. Bij het verzoek bekijkt de gemeente altijd of het antwoord geen inbreuk maakt op de persoonlijke levenssfeer van betrokkenen. In principe worden geen persoonsgegevens verstrekt.

3. Reikwijdte

Het reglement is van toepassing op alle verwerkingen van persoonsgegevens door alle bestuursorganen van de gemeente. Oftewel: voor alle verwerkingen die binnen de gemeente plaatsvinden.

4. Verantwoordelijke voor de verwerking

De bestuursorganen van de gemeente (Burgemeester, het college van Burgemeesters en Wethouders en de Raad) zijn allemaal, ieder voor hun verwerkingen door of namens de gemeente worden uitgevoerd, verantwoordelijk.

5. Verwerkingen (Artikel 4, AVG)

De verwerking van persoonsgegevens is elke handeling of elk geheel van handelingen met persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde processen. Let wel, het wettelijk kader van de Wbp en de AVG als opvolger, ziet niet op de specifieke verwerkingen die wij als gemeente verrichten in het kader van de uitvoering van de basisregistratie personen (BRP). Hiervoor is de Wet BRP van toepassing.

In de AVG valt onder een verwerking:

- Verzamelen, vastleggen en ordenen;
- Bewaren, bijwerken en wijzigen;
- Opvragen, raadplegen, gebruiken;
- Verstrekken door middel van doorzending;
- Verspreiding of enige andere vorm van ter beschikkingstellen;
- Samenbrengen, met elkaar in verband brengen;
- Afschermen, uitwissen of vernietigen van gegevens.

Uit deze opsomming blijkt dat alles wat je met een persoonsgegeven doet een verwerking is.

6. Doeleinden (Artikel 5, AVG)

Algemeen uitgangspunt is dat persoonsgegevens alleen verzameld worden als daarvoor een doel bestaat. Dit doel moet welbepaald, duidelijk omschreven en gerechtvaardigd zijn. Ook moet steeds nagegaan worden of het verwerken van persoonsgegevens noodzakelijk is voor het doel. De verwerkingsdoelen zijn het 'waarom' van het verwerken van persoonsgegevens. Doelen zijn van belang voor verschillende normen. Denk hierbij aan onder andere het bepalen wie verantwoordelijk is voor de verwerking van persoonsgegevens. Of de vraag of het delen van deze gegevens met andere organisaties is toegestaan. Ook zijn doelen van belang voor het vaststellen van bewaartermijnen en het informeren van de burger. Zo weet je hoe lang het nodig is om de persoonsgegevens te bewaren of waar je burgers over moet informeren.

Voor de uitvoering van diverse wetten (denk aan de Wmo en Participatiewet) zal in die wet dikwijls zijn aangegeven welke persoonsgegevens nodig zijn en dus verwerkt mogen worden. Denk aan de Jeugdwet waar de doelen voor het verwerken in de wet al zijn vastgelegd, net als de persoonsgegevens die gevraagd en verwerkt mogen worden. Daar waar over verwerking van persoonsgegevens in bijzondere wetgeving niets is geregeld, gelden de regels van de AVG (en de daarmee samenhangende Uitvoeringswet AVG).

Een belangrijke eis is dat doelen vooraf specifiek geformuleerd moeten zijn. De doelen mogen dus niet te ruim en vaag omschreven zijn of achteraf bepaald worden. Verwerking voor een ander doel dan het oorspronkelijke doel is alleen onder strikte voorwaarden toegestaan. Zo zal er een directe relatie moeten zijn met het doel waarvoor de persoonsgegevens eerder zijn verzameld. Ook moet men rekening houden met de soort gegevens. Algemeen geldt: hoe gevoeliger het gegeven, hoe minder snel er sprake is van verenigbaar gebruik en de gegevens niet verder mogen worden verwerkt. Dus niet mogen worden gebruikt voor een ander doel dan waarvoor deze eerder zijn verzameld. Ook moet men rekening houden met de gevolgen van de beoogde verwerking voor de betrokkene. Denk hierbij

aan het vooraf inlichten van de burger over het doel waarvoor de gegevens worden gebruikt als de burger zijn persoonsgegevens aan de gemeente geeft. Bijvoorbeeld voor de aanvraag van een parkeer- of bouwvergunning.

7. Rechtmatige grondslag (Artikel 6, AVG)

De wet zegt dat er voor elke verwerking van persoonsgegevens een rechtmatige grondslag uit de wet van toepassing moet zijn. Dit betekent dat we als gemeente moeten verantwoorden op basis waarvan we persoonsgegevens van bijvoorbeeld een burger verwerken. Een uitzondering hierop is het hiervoor besproken geval waarin persoonsgegevens worden verwerkt voor een ander doel dan het doel waarvoor ze zijn verzameld. Dit is onder strikte voorwaarden toegestaan. Een goed voorbeeld hiervan is het verder gebruiken van de gegevens voor wetenschappelijk onderzoek en statistiek.

Iedere verwerking van persoonsgegevens moet kunnen worden gebaseerd op één van de volgende zes grondslagen:

1. De betrokkene heeft voor de verwerking zijn ondubbelzinnige toestemming verleend;
2. De gegevensverwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, waarbij ook rekening moet worden gehouden met de onderhandelingsfase;
3. De gegevensverwerking is noodzakelijk om een wettelijke verplichting na te komen waaraan de gemeente onderworpen is;
4. De gegevensverwerking is noodzakelijk ter vrijwaring van een vitaal belang van de betrokkene (in het kader van leven of dood, bijvoorbeeld delen van gegevens bij opname spoedeisende hulp);
5. De gegevensverwerking is noodzakelijk voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt, of
6. De gegevensverwerking is noodzakelijk voor de behartiging van het gerechtvaardigde belang van de gemeente of van een derde aan wie de gegevens worden verstrekt. Maar als het belang op bescherming van zijn privacy voor de betrokkene zwaarder weegt, dan is het verwerken van gegevens op grond van een gerechtvaardigd belang niet van toepassing.

Voor alle grondslagen zal er altijd een noodzaak moeten zijn om die gegevens te verwerken. Of het verwerken van bepaalde gegevens noodzakelijk is, moet altijd gemotiveerd worden.

Van de zes grondslagen zijn voor de gemeente in de praktijk de wettelijke grondslag en de goede vervulling van een publiekrechtelijke taak leidend. Doordat er tussen de gemeente en de burger een afhankelijkheidsrelatie bestaat, zal de grondslag toestemming zelden kunnen worden gebruikt. Voor veel voorzieningen moet de burger aankloppen bij de gemeente en is de burger dus afhankelijk. Alleen in uitzonderlijke situaties is toestemming van de burger een grondslag.

Voor de interne bedrijfsvoering van de gemeente, voor de medewerkers dus, speelt ook de grondslag gerechtvaardigd belang een rol. Denk hierbij aan de vraag of de gemeente het recht heeft om e-mail, internet- en telefoongebruik door medewerkers te controleren. Het gerechtvaardigd belang mag nooit als reden van de verwerking van gegevens van burgers worden gebruikt.

8. Wijze van verwerking

De hoofdregel van de verwerking van persoonsgegevens is dat het alleen toegestaan is in overeenstemming met de wet, en op een zorgvuldige wijze. Persoonsgegevens worden zoveel mogelijk verzameld bij de betrokkene zelf. De wet gaat uit van subsidiariteit. Dit betekent dat verwerking alleen is toegestaan wanneer het doel niet op een andere manier kan worden bereikt. In de wet wordt ook gesproken over proportionaliteit. Dit betekent dat persoonsgegevens alleen mogen worden verwerkt als dit in verhouding staat tot het doel. Wanneer met geen, of minder (belastende), persoonsgegevens hetzelfde doel bereikt kan worden moet daar altijd voor gekozen worden.

Persoonsgegevens moeten dus juist, ter zake dienend, up-to-date en niet bovenmatig veel zijn in het licht van het doel van de verwerking. Dit betekent dat alleen die persoonsgegevens mogen worden gebruikt die strikt noodzakelijk zijn voor het doel van de verwerking. Wanneer het bijvoorbeeld voldoende is om iemands contactgegevens te gebruiken, is het niet nodig om ook een pasfoto en BSN te vragen. Sowieso gelden voor het gebruik van het BSN strenge regels. Wanneer ook met anonieme gegevens volstaan kan worden, mogen geen herleidbare persoonsgegevens gebruikt worden.

8.1. Organisatorische maatregelen

Niet alleen zorgt de gemeente ervoor dat de persoonsgegevens kloppen en volledig zijn voordat ze verwerkt worden. Deze gegevens worden alleen verwerkt door personen met een geheimhoudingsplicht. Ook is het van belang dat de personen die daadwerkelijk werken met deze gegevens weten wat hun verantwoordelijkheid is. En hoe ze zorgvuldig om moeten gaan met persoonsgegevens. Het is dus belangrijk dat de medewerkers van de gemeente zich bewust zijn van de regels en gedragsnormen rondom privacy. Deze organisatorische maatregelen dragen ook bij aan een bewustwording binnen de gemeente. Denk hierbij aan het ontwikkelen van specifieke privacy protocollen en afwegingskaders. Maar ook in de vorm van het ondersteunen van de medewerkers door privacy trainingen en kennissessies. De medewerkers moeten zich bewust zijn van het belang van privacy. Zo moeten zij persoonsgegevens verwerken zoals is bepaald in het algemeen privacybeleid, algemeen privacyreglement en de bijbehorende privacyregelingen.

8.2. Beveiliging

Daarnaast beveiligt de gemeente alle persoonsgegevens. Dit moet voorkomen dat de persoonsgegevens kunnen worden ingezien of gewijzigd door iemand die daar geen recht toe heeft. Als uitgangspunt geldt dat naarmate de risico's van de verwerking hoger liggen er betere beveiligingsmaatregelen moeten worden getroffen. De gemeente heeft hiervoor een specifiek beleid opgesteld in de vorm van het Informatiebeveiligingsbeleid. Het is aan de gemeente om te bepalen hoe de persoonsgegevens organisatorisch en technisch moeten worden beveiligd. Hoe de gemeente dit doet staat in het informatiebeveiligingsbeleid van de gemeente en in een eventueel aanvullend beveiligingsplan specifiek opgesteld voor een proces of registratie.

In ieder geval wordt de toegang en het gebruik van de systemen ten behoeve van de BRP en Suwinet gelogd. Middels steekproeven wordt gecontroleerd of het gebruik van de systemen en de verwerking van persoonsgegevens in lijn is met de wet- en regelgeving, het privacybeleid en dit reglement. Ook voor overige systemen wordt gebruik gemaakt van het loggen van gegevens. Indien daar aanleiding

toe is, zal ook hier worden gecontroleerd of de systemen en verwerking van persoonsgegevens worden gebruikt conform de wet- en regelgeving, het privacybeleid en dit reglement.

8.3. Melden verwerkingen

Onder de AVG heeft de gemeente een verantwoordingsplicht, wat inhoudt dat de verwerkingen gemeld dienen te worden bij de functionaris gegevensbescherming. Het bijhouden van een register van verwerkingsactiviteiten is onderdeel van onze verantwoordingsplicht. Hiermee kan de gemeente aantonen dat het in overeenstemming met de AVG handelt.

De gemeente kan het register ook nodig hebben als betrokkenen hun privacyrechten uitoefenen. Als zij ons vragen hun gegevens te corrigeren of te verwijderen, moet de gemeente dit doorgeven aan de organisaties waarmee we hun gegevens hebben gedeeld.

9. Doorgifte aan derden

Persoonsgegevens mogen in principe niet worden doorgegeven naar een organisatie in een land buiten de Europese Unie (EU). Dit komt omdat binnen de EU een goede bescherming voor de persoonsgegevens is, en daarbuiten niet in alle gevallen. Onder doorgifte wordt o.a. verstaan: het opslaan (bijvoorbeeld in de Cloud) of het ter beschikking stellen aan een organisatie buiten de EU. De gemeente geeft alleen persoonsgegevens door aan een land buiten de Europese Economische Ruimte (EER) of een internationale organisatie op grond van goedgekeurde afspraken door de Europese Commissie.

10. Transparantie en communicatie

10.1. Wet openbaarheid van bestuur (Wob)

Via de Wob (en straks wellicht de Wet Open Overheid) kan een verzoek om informatie ingediend worden bij de gemeente. Bij het verzoek kijkt de gemeente altijd of het antwoord geen inbreuk maakt op de persoonlijke levenssfeer van betrokkenen. In principe worden geen persoonsgegevens verstrekt.

10.2. Wet hergebruik van overheidsinformatie

De gemeente informeert betrokkenen over het verwerken van persoonsgegevens. Wanneer betrokkenen gegevens aan de gemeente geven, worden zij op de hoogte gesteld van de manier waarop de gemeente met persoonsgegevens om zal gaan. De betrokkene wordt niet nogmaals geïnformeerd als hij/zij al weet dat de gemeente persoonsgegevens van hem/haar verzamelt en verwerkt, en weet waarom en voor welk doel dat gebeurt.

Wanneer de gegevens via een andere weg verkregen worden, dus buiten de betrokkene om, wordt de betrokkene geïnformeerd op het moment dat deze voor de eerste keer worden verwerkt.

10.3. Informatieplicht

De gemeente informeert betrokkenen over het verwerken van persoonsgegevens. Wanneer betrokkenen gegevens aan de gemeente geven, worden zij op de hoogte gesteld van de manier waarop de gemeente met persoonsgegevens om zal gaan. De betrokkene wordt niet nogmaals geïnformeerd als hij/zij al weet dat de gemeente persoonsgegevens van hem/haar verzamelt en verwerkt, en weet waarom en voor welk doel dat gebeurt.

Wanneer de gegevens via een andere weg verkregen worden, dus buiten de betrokkene om, wordt de betrokkene geïnformeerd op het moment dat deze voor de eerste keer worden verwerkt.

10.4. Verwijdering

De gemeente bewaart de persoonsgegevens niet langer dan nodig is voor de uitvoering van gemeentelijke taken, of zoals vastgelegd in de Archiefwet. Wanneer er nog persoonsgegevens opgeslagen zijn die niet langer nodig zijn voor het bereiken van het doel worden deze zo snel mogelijk verwijderd. Dit houdt in dat deze gegevens vernietigd worden, of zo worden aangepast dat de informatie niet meer gebruikt kan worden om iemand te identificeren.

10.5. Rechten van betrokkenen (Artikel 13 t/m 20, AVG)

De wet bepaalt niet alleen de plichten van degenen die de persoonsgegevens verwerken, maar bepaalt ook de rechten van de personen van wie de gegevens worden verwerkt. Deze rechten worden ook wel de rechten van betrokkenen genoemd, en bestaan uit 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. De gemeente zal hieraan voldoen, tenzij er gerechtvaardigde gronden zijn voor de verwerking.
- 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.

10.6. Indienen van verzoek

Om gebruik te maken van zijn/haar rechten kan de betrokkene een verzoek indienen. Bij ontvangst van een verzoek kan de gemeente aanvullende informatie opvragen om zeker te zijn van de identiteit van de betrokkene. De gemeente heeft vier weken de tijd, vanaf de ontvangst van het verzoek, om een besluit te nemen op het verzoek. Als het verzoek niet wordt gehonoreerd, is er de mogelijkheid om bezwaar te maken bij de gemeente, of een klacht in te dienen bij de Autoriteit Persoonsgegevens (AP).

11. Geautomatiseerde verwerkingen

11.1. Profileren (Artikel 22, AVG)

Profileren 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.

11.2. 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 nodig is voor het behalen van het doel gebruikt zullen worden. Daarnaast kunnen persoonsgegevens gepseudonimiseerd worden zodat zij niet herleidbaar zijn tot een persoon.

11.3. 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 straat. 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 in ons aanwijzingsbesluit.

12. Plichten van de gemeente

12.1. Register van verwerkingen (Artikel 30, AVG)

Met de inwerkingtreding van de AVG is de gemeente verplicht om te documenteren welke persoonsgegevens worden verwerkt, wat het doel ervan is, van wie of waar deze gegevens afkomstig zijn en met wie deze gegevens worden gedeeld. Daarnaast moeten we per verwerking documenteren en verantwoorden op basis van welke wettelijke grondslag de gemeente deze persoonsgegevens verwerkt.

12.2. Bewaartermijnen

De gemeente bewaart de persoonsgegevens niet langer dan nodig is voor de uitvoering van gemeentelijke taken, of zoals vastgelegd in de Archiefwet. In de AVG worden geen bewaartermijnen genoemd. De hoofdregel is: bewaren mag zolang het nodig is voor het doel van de verwerking.

In een aantal wetten zijn specifieke bewaartermijnen opgenomen voor bepaalde persoonsgegevens. Als geen bewaartermijn aanwezig is dan moet goed kunnen worden onderbouwd waarom

persoonsgegevens voor een bepaalde termijn worden bewaard. Wanneer er nog persoonsgegevens opgeslagen zijn die niet langer nodig zijn voor het bereiken van het doel worden deze zo snel mogelijk verwijderd. Na afloop van de bewaartermijnen moeten de persoonsgegevens worden vernietigd of geanonimiseerd. Dit geldt niet alleen voor de gegevens zelf, maar ook voor kopieën en back-ups. Voor alle persoonsgegevens geldt dat de vernietiging onomkeerbaar moet zijn. Het gaat dus niet om het plaatsen van de bestanden in de prullenbak en de prullenbak legen, maar bijvoorbeeld om het overschrijven van data met nullen, enen en willekeurige karakters (data wiping).

12.3. Meldplicht datalekken (Artikel 33, 34 AVG)

De meldplicht datalekken houdt in dat de gemeente zo snel mogelijk (binnen 72 uur) een melding doet bij de AP zodra een ernstig datalek zich heeft voorgedaan. Een datalek is een inbreuk op de beveiliging, die flinke nadelige gevolgen heeft voor de burger of voor de bescherming van de persoonsgegevens. Denk hierbij aan een kwijtgeraakte USB-stick met persoonsgegevens, een gestolen laptop of een inbraak op het netwerk (hack). Als de kans bestaat dat het datalek nadelige gevolgen zou kunnen hebben voor burgers, dan moet de gemeente het datalek daarnaast óók melden bij de betrokken burgers. Daarnaast moet de burger worden geïnformeerd over welke maatregelen wij als gemeente nemen om de risico's en schade te beperken.

Naast het melden moeten wij ook alle datalekken documenteren. Met deze documentatie moet de Autoriteit Persoonsgegevens niet alleen kunnen controleren of wij als gemeente aan de meldplicht hebben voldaan, maar ook onze afwegingen om wel of niet te melden transparant te kunnen beoordelen.

12.4. Verwerkersovereenkomst

Verwerkersovereenkomsten moeten iedere keer worden afgesloten wanneer derden – ook wel verwerkers genoemd – in opdracht van de gemeente persoonsgegevens verwerken. Te denken valt aan een instantie op het gebied van schuldhulpverlening die van de gemeente de opdracht krijgt de schuldenproblematiek aan te pakken. Hiervoor krijgt de instantie toegang tot deze specifieke gemeentelijke gegevens. Uiteraard moeten er juridische afspraken worden gemaakt over hoe deze instantie moet omgaan met de gegevens die zij van de gemeente krijgt. Denk hierbij aan welke gegevens men nodig heeft om de taak uit te oefenen. De manier waarop de organisatie de gegevens heeft beveiligd en wat zij moet doen als er een datalek is. De gemeente heeft een standaard verwerkersovereenkomst beschikbaar gesteld die in al deze gevallen moet worden gebruikt.

12.5. Data Protection Impact Assessment (DPIA) (Artikel 35, AVG)

Met een DPIA worden de effecten en risico's van nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. Dit geldt in het bijzonder bij verwerkingen waarbij nieuwe technologieën worden gebruikt. De gemeente Stein voert deze alleen uit wanneer:

1. Er een (geautomatiseerde) verwerking plaatsvindt met een hoog risico,
2. Er een (geautomatiseerde) verwerking plaatsvindt waarvan de Autoriteit Persoonsgegevens heeft aangegeven dat daarvoor een DPIA verplicht is;
3. Een grootschalige verwerking plaatsvindt;
4. Of wanneer er een grootschalige monitoring van openbare ruimten plaatsvindt.

12.6. Privacy by Design en Privacy by Default

Bij de aanschaf of ontwikkeling van producten, systemen en/of inrichting van processen moet altijd rekening worden gehouden met de bescherming van persoonsgegevens. We noemen dit Privacy by Design en Privacy by Default. Voor alle producten, systemen of processen moeten de technische en organisatorische maatregelen ervoor zorgen dat standaard alleen die gegevens worden gebruikt die nodig zijn voor het doel. Als blijkt dat bij een systeem gevoelige of bijzondere persoonsgegevens worden verwerkt en dit mogelijk een hoog privacyrisico met zich meebrengt, zijn we verplicht om een Data Protection Impact Assessment (DPIA) uit te voeren.

12.7. Functionaris voor de gegevensbescherming (Artikel 37 t/m 39, AVG)

De gemeente heeft een functionaris voor de gegevensbescherming (FG) aangesteld. Door het aanstellen van een FG wordt een belangrijke stap gezet in de manier waarop de gemeente aan haar burgers wil uitdragen dat zij serieus omgaat met de verwerking van persoonsgegevens. De aanwijzing van een FG wordt voor de gemeente onder de AVG verplicht. 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. De gemeente stelt ook een FG aan om daarmee het eigen toezicht en controle te organiseren. Hij heeft een belangrijke coördinerende rol en adviseert over oplossingen over privacy. De FG houdt vanuit een onafhankelijke positie intern toezicht op de manier waarop door de gemeente wordt omgegaan met persoonsgegevens. Belangrijk is ook dat hij vroegtijdig betrokken wordt bij de inrichting van processen. En als laatste is de FG het formele aanspreekpunt voor burgers als zij hun rechten als betrokkene willen uitoefenen. Het is 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.

Voor vragen over privacy of over deze toelichting kunt u contact opnemen met de functionaris voor gegevensbescherming van de gemeente Stein via: info@gemeentestein.nl

12.8. Verantwoordelijkheid

De afdeling, respectievelijk team, is verantwoordelijk voor de wijze waarop zij persoonsgegevens verwerkt. De FG of de medewerkers belast met privacy, zoals de privacy officer, kunnen adviseren of oordelen dat een bepaalde gegevensverwerking niet conform het beleid en het reglement wordt uitgevoerd.

Als de aanwijzing(en) door de FG ten aanzien van de desbetreffende gegevensverwerking niet binnen een redelijke termijn wordt opgevolgd, wordt het volgende escalatiemodel gehanteerd:

1. De leidinggevende van het desbetreffende team wordt geïnformeerd en de opvolging wordt zijn / haar verantwoordelijkheid;

Bij het niet opvolgen van de aanwijzing wordt:

2. De manager van de desbetreffende afdeling wordt geïnformeerd en de opvolging wordt zijn / haar verantwoordelijkheid;

Bij het niet opvolgen van de aanwijzing wordt:

3. De algemeen directeur wordt geïnformeerd en de opvolging wordt zijn / haar verantwoordelijkheid;

Bij het niet opvolgen van de aanwijzing wordt:

4. Het college geïnformeerd.

13. Afsluiting

Als de gemeente een wettelijke verplichting niet nakomt kan de betrokkene een klacht indienen. Deze zal via de klachtenregeling van de gemeente worden behandeld. In gevallen waar de regeling niets over zegt, beslist het verantwoordelijke bestuursorgaan van de gemeente.

14. Slotbepaling

Dit reglement treedt in werking op de dag na die van bekendmaking.

Dit reglement kan worden aangehaald als 'Privacyreglement Gemeente Stein'.

15. Formele vaststelling

Burgemeester en wethouders van de gemeente Stein heeft dit document formeel vastgesteld in de collegevergadering van 14 mei 2019.

