

Algemeen privacybeleid
gemeente Asten 2018

Bezoekadres Koningsplein 3 | 5721 GJ Asten

Postadres Postbus 290 | 5720 AG Asten

T (0493) 671 212 | F (0493) 671 213

www.asten.nl | gemeente@asten.nl

ALGEMEEN PRIVACYBELEID (AVG) GEMEENTE ASTEN

Inhoud

1. Inleiding	3
2. Uitgangspunten	3
3. Rollen en bevoegdheden	4
Bestuur	4
- College van B&W	4
- Gemeenteraad	4
Organisatie	5
- Functionaris voor de Gegevensbescherming (FG)	5
- Privacy-Officer	5
- Chief Information Security Officer (CISO)	5
- Management en medewerkers	5
4. Informatiebeveiliging	6
5. Uitwisseling met derden	6
6. Maatregelen	7
7. Rechten van betrokkenen	8

Vastgesteld door college van burgemeester en wethouders dd 15 mei 2018

1. Inleiding

De gemeente Asten verwerkt persoonsgegevens van inwoners, medewerkers en contactgegevens van zakelijke partners. Persoonsgegevens worden gebruikt voor de dienstverlening aan inwoners en bedrijven, het uitvoeren van wettelijke taken en in het kader van de bedrijfsvoering. Door een uitbreiding van de digitale gegevensverwerking en doordat er steeds meer wettelijke taken bij de gemeente worden ondergebracht, worden er andere eisen aan de bescherming van gegevens en privacy gesteld.

De gemeente Asten vindt een betrouwbare dienstverlening, waarin inwoners open en respectvol worden behandeld belangrijk. Goede bescherming van persoonsgegevens is daarbij cruciaal. Inwoners kunnen er op vertrouwen dat de gemeente zorgvuldig, veilig en vertrouwelijk omgaat met persoonsgegevens.

Er zijn veel wetten, besluiten en regelingen die de verwerking van persoonsgegevens regelen. Voor de gemeente zijn belangrijke wetten:

- Wet bescherming persoonsgegevens (Wbp)(vanaf 25 mei 2018 de Algemene Verordening Gegevensbescherming (AVG));
- Wet basisregistratie personen (Wet BRP).

De gemeente geeft met dit privacybeleid invulling aan de verplichtingen en bevoegdheden die voortvloeien uit de Wbp, vanaf 25 mei 2018 de AVG. De gemeente laat met het privacybeleid zien dat zij de privacy waarborgt, beschermt en handhaaft. De Wet BRP kent een eigen stelsel van regels.

2. Uitgangspunten

Het gemeentelijk privacybeleid is van toepassing op alle taken en verwerkingsprocessen waarin persoonsgegevens worden verwerkt en waar de gemeente Asten voor verantwoordelijk is.

Bij persoonsgegevens gaat het om alle informatie over een persoon. Ook gegevens die indirect iets over iemand zeggen, zijn persoonsgegevens. Voor de hand liggende gegevens zijn iemands naam, adres en woonplaats. Maar ook telefoonnummers en postcodes met huisnummers zijn persoonsgegevens. Gevoelige gegevens als iemands ras (bijvoorbeeld een foto), godsdienst of gezondheid worden ook wel bijzondere persoonsgegevens genoemd. Deze zijn door de wetgever extra beschermd. Het Burgerservicenummer is vergelijkbaar aan een bijzonder persoonsgegeven. Dit mag alleen verwerkt worden als daar een wettelijke grondslag voor is.

Bij het verwerken van persoonsgegevens worden de volgende uitgangspunten in acht genomen:

- Persoonsgegevens worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt.
- De gemeente Asten verzamelt en verwerkt persoonsgegevens enkel voor een bepaald doel en met een rechtvaardige grondslag.* Het doel is specifiek en nadrukkelijk beschreven in het register van verwerkingen. Daarnaast wordt de verwerking getoetst aan het proportionaliteitsbeginsel en het subsidiariteitsbeginsel. Dit houdt in dat de verwerking in verhouding staat tot het beoogde doel en er enkel gegevens worden verwerkt indien het beoogde doel niet op een minder ingrijpende wijze kan worden bereikt.

- Betrokkenen worden geïnformeerd over de verwerking van hun persoonsgegevens via de privacyverklaring op de website. De gemeente geeft in voorkomend geval gehoor aan inzage- en/of correctieverzoeken, dan wel verwijderingsverzoeken. Afhandeling van klachten gebeurt op een laagdrempelige, toegankelijke wijze.
- De gemeente zorgt er voor dat persoonsgegevens correct en actueel zijn.
- Persoonsgegevens worden niet langer bewaard dan noodzakelijk en worden daarna vernietigd. Het bewaren van gegevens kan nodig zijn om taken goed uit te kunnen oefenen. De gemeente houdt zich aan de wettelijke verplichtingen.
- 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. Persoonsgegevens worden alleen gedeeld als dat strikt noodzakelijk is voor de uitvoering van wettelijke taken.
- De gemeente borgt middels technische en organisatorische maatregelen passende beveiliging van persoonsgegevens. Deze beveiliging is vastgelegd in het informatiebeveiligingsbeleid.
- Bij aanschaf, inrichting of ontwikkeling van producten of diensten houdt de gemeente rekening met de bescherming van persoonsgegevens.

*Grondslagen gegevensverwerking

De gemeente Asten verwerkt enkel gegevens indien is voldaan aan ten minste een van de onderstaande voorwaarden en er sprake is van:

- een publiekrechtelijke taak;
- een wettelijke plicht;
- een overeenkomst;
- expliciete toestemming van de betrokkene;
- een vitaal belang van de betrokkene.

3. Rollen en bevoegdheden

Privacy is voor een belangrijk deel een zaak van bewustwording, cultuur en communicatie. Bestuur, management en medewerkers zijn zich bij de uitoefening van hun werk voortdurend bewust van het belang van bescherming van de privacy.

Bestuur

College van B&W

- Is verantwoordelijk voor de naleving van privacywetgeving en voert proactief privacybeleid op basis van afweging van belangen en risico's bij de verwerking van persoonsgegevens. In evenwicht dus: behoorlijk, zorgvuldig en in overeenstemming met de wet.
- Stelt beleid vast voor de bescherming van de privacy op basis van wet- en regelgeving.
- Legt over de privacy beleidsuitvoering verantwoording af aan de raad.
- Draagt zorg voor de documentatie van beleid en maatregelen zodat het op ieder moment maatschappelijk en juridisch uitleg kan geven over de deugdelijkheid van de aanpak.
- Houdt een register van de gegevensverwerkingen bij.
- Wijst de Functionaris voor de gegevensbescherming als interne toezichthouder aan.

Gemeenteraad

- Heeft een toezichthoudende rol op basis van de controlerende taak die de Gemeentewet aan de gemeenteraad toekent.

Organisatie

De taken en bevoegdheden in het kader van privacy worden belegd bij onderstaande functies:

Functionaris voor de gegevensbescherming (FG)

De Functionaris voor de gegevensbescherming (FG) is een wettelijk verplichte functie. De FG fungeert als onafhankelijke interne toezichthouder en heeft van de wetgever vijf taken gekregen:

- Intern toezicht op de toepassing van de AVG.
- Bevorderen van bewustzijn over de AVG in de organisatie.
- Adviesrol op het gebied van de AVG met name omtrent het uit te voeren Privacy Impact Assessment (PIA) (zie pag. 6).
- Optreden als contactpersoon en samenwerkingspartner naar de Autoriteit Persoonsgegevens, waaronder de verantwoordelijkheid voor de melding van datalekken bij de Autoriteit Persoonsgegevens.
- De FG rapporteert zo nodig rechtstreeks aan het college.

Privacy-Officer (PO)

De Privacy-Officer (PO) geeft uitvoering aan het privacybeleid in de organisatie. Deze rol wordt vervuld door de juridisch controller met ondersteuning van de medewerker juridische kwaliteitszorg. Taken die bij deze rol horen zijn:

- De belangrijkste adviseur binnen de organisatie over privacy.
- Coördineren en opstellen van privacy-beleid.
- Coördineren en uitvoeren van actiepunten uit het privacy-beleid.
- Coördineren en afhandelen van verzoeken van burgers met betrekking tot de privacyrechten, als inzage in of correctie van persoonsgegevens.
- Rapportage naar management, college van B&W en gemeenteraad over privacy.

Door de functies advies (PO) en controle (FG) te scheiden, wordt voorkomen dat de FG toezicht moet houden op zijn eigen werk. Dit komt de kwaliteit ten goede.

Chief Information Security Officer (CISO)

De CISO houdt zich bezig met de inrichting van de informatiebeveiliging op basis van de Baseline Informatiebeveiliging Gemeenten (BIG). Dit houdt in dat informatiebeveiliging wordt ingericht, waarbij de prioritering wordt gebaseerd op basis van de grootste risico's voor de dienstverlening van de gemeente. De taken van de CISO zijn verdeeld over de volgende aspecten van informatiebeveiliging:

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

Management en medewerkers

Privacy dient ingebed te zijn in de door de medewerkers 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 PO en of FG. De leidinggevenden zien toe op de naleving van wet- en regelgeving, het privacybeleid en het informatiebeveiligingsbeleid.

4. Informatiebeveiliging

In 2016 is het informatiebeveiligingsbeleid vastgesteld. Het beleid is het kader voor passende technische, fysieke en organisatorische maatregelen om gemeentelijke informatie te beschermen en te waarborgen dat de gemeente Asten voldoet aan relevante wet- en regelgeving.

Informatiebeveiliging betreft de processen die ingericht worden om de gemeentelijke processen, de gebruikte informatiesystemen en de daarin opgeslagen gegevens te beschermen tegen vernietiging, verlies, diefstal en onbevoegden.

De informatiebeveiliging heeft betrekking op:

Beschikbaarheid/continuïteit

Het zorg dragen voor het beschikbaar zijn van informatie en informatieverwerkende bedrijfsmiddelen op de juiste tijd en plaats voor gebruikers.

Exclusiviteit/vertrouwelijkheid

Het beschermen van informatie tegen kennisname en mutatie door onbevoegden.

Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn.

Integriteit/betrouwbaarheid

Het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking.

In het geval zich - ondanks de getroffen maatregelen - een incident voordoet waarbij persoonsgegevens zijn betrokken, wordt dit direct gemeld aan de CISO.

5. Uitwisseling met derden

Bij de uitvoering van haar gemeentelijke taken werkt de gemeente Asten veel samen met externe partijen zoals andere overheden, gemeenschappelijke regelingen, softwareleveranciers en adviesbureaus. Met het oog op de bescherming van persoonsgegevens maakt de gemeente Asten met deze externe partijen afspraken over de omgang met privacy.

Voor zover de samenwerkingspartners worden aangemerkt als verwerker sluit de gemeente met deze partij een zogenaamde verwerkersovereenkomst. In de verwerkersovereenkomst worden afspraken gemaakt over het waarborgen van privacyverplichtingen en beveiliging van persoonsgegevens. Wanneer samenwerkingspartners worden aangemerkt als verwerkingsverantwoordelijke worden de afspraken over de omgang met persoonsgegevens vastgelegd in een overeenkomst omtrent persoonsgegevens, algemene inkoopvoorwaarden, bestaande samenwerkingsovereenkomsten, convenanten, gemeenschappelijke regelingen, etc. De Privacy-Officer ziet toe op de naleving van de gemaakte afspraken.

6. Maatregelen

Onderstaande maatregelen zijn getroffen om de privacy te kunnen waarborgen:

1. Informatieplicht
Betrokkenen krijgen vooraf duidelijke informatie via de privacyverklaring op de website en de dienstverlening (telefonisch, schriftelijk, e-mail) over de verwerking van hun persoonsgegevens en het doel van de verwerking.
2. Bewustwording
Bewustwording is essentieel voor het borgen van privacy in de organisatie. Er wordt doorlopend aandacht geschonken aan de bewustwording van privacy in de organisatie.
3. Register van verwerkingen
Een register van verwerkingen met alle verwerkingsactiviteiten van persoonsgegevens wordt bijgehouden.
4. Privacy Impact Assessment (PIA)
Bij de invoering van nieuw beleid of regelgeving of bij het gebruik van nieuwe technologieën houdt de gemeente Asten rekening met de bescherming van persoonsgegevens door een PIA uit te voeren.
5. Het melden van incidenten informatieveiligheid
Er is een procedure voor het melden van incidenten informatieveiligheid. Deze procedure ziet ook toe op het **melden van datalekken**. Er wordt een register bijgehouden van gemelde incidenten.
6. Toezichtrapportage en evaluatie
Periodiek wordt gecontroleerd of beleid en dagelijkse praktijk overeenkomen. Samen met de Privacy-Officer bepaalt team control periodiek of een privacy-audit wordt uitgevoerd in aanvulling op het toezicht door de FG.
Jaarlijks legt het college in de paragraaf bedrijfsvoering in begroting en jaarrekening verantwoording af aan de raad waar het gaat over de risico's en beheersmaatregelen met betrekking tot het privacybeleid. Het privacybeleid wordt na twee jaar geëvalueerd.

Nadere toelichting PIA

Met een (externe) PIA worden de effecten en risico's van nieuwe of bestaande risicovolle verwerkingen beoordeeld op de bescherming van de privacy. De gemeente voert deze uit wanneer er een geautomatiseerde verwerking, een grootschalige verwerking of wanneer er een grootschalige monitoring van openbare ruimten plaatsvindt.

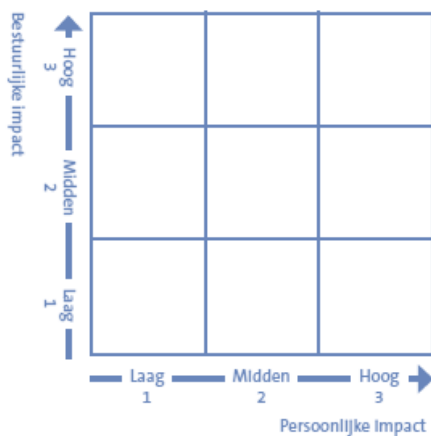
De volgende indicatoren zullen daarbij als toetsingskader worden gehanteerd:

- 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 de PIA is ten minste opgenomen:

- 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 personen.
- De beoogde maatregelen om de risico's te beperken.

PIA-scores worden bepaald aan de hand van de hieronder afgebeelde matrix. Hoe hoger de score, hoe robuuster de beheersmaatregelen moeten zijn om de privacy te waarborgen.



7. Rechten van betrokkenen

Door de Algemene Verordening Gegevensbescherming krijgt men meer mogelijkheden om voor zichzelf op te komen als persoonsgegevens verwerkt worden. Betrokkenen hebben de volgende rechten:

1. Recht op informatie
De gemeente heeft de algemene plicht om publiek te informeren over gegevensverwerkingen; wat er met persoonsgegevens gebeurt en waarom.
2. Inzagerecht
De mogelijkheid om in te zien of en op welke manier, zijn/haar gegevens worden verwerkt;.
3. Recht op correctie en verwijdering
Als duidelijk wordt dat de gegevens niet kloppen, kunnen betrokkenen een verzoek indienen bij de gemeente om dit te corrigeren. Dat houdt in dat zij mogen vragen hun persoonsgegevens te verbeteren, aan te vullen, te verwijderen of af te schermen.
4. Recht om vergeten te worden
Wanneer persoonsgegevens openbaar zijn gemaakt, bijvoorbeeld door online te zetten, hebben betrokkenen het recht om vergeten te worden, zodat koppelingen naar en kopieën van de gegevens gewist worden.
5. Recht op beperking
Het recht om in bepaalde gevallen aan de gemeente te vragen om hun persoonsgegevens tijdelijk niet meer te gebruiken.
6. Recht op dataportabiliteit
Betrokkenen hebben het recht op overdraagbaarheid van gegevens.
7. Recht van bezwaar
Het recht om bezwaar te maken tegen de verwerking van zijn/haar persoonsgegevens. De gemeente zal hieraan voldoen, tenzij er gerechtvaardigde gronden zijn voor de verwerking.
8. Recht om niet onderworpen te worden aan geautomatiseerde individuele besluitvorming waaronder profilering
Het recht op een menselijke blik bij besluitvorming.

Verzoeken met betrekking tot bovenstaande rechten en bezwaren kunnen schriftelijk en digitaal worden ingediend bij de FG via het emailadres gemeente@asten.nl ter attentie van FG. Deze verzoeken worden geregistreerd en de afhandeling wordt verantwoord.