PRIVACYBELEID GEMEENTE ALMELO 2018 - 2021

Gebaseerd op de Algemene Verordening Gegevensbescherming (AVG)

Nota 02 Intern - 63102

Vastgesteld door GO dd. 07-02-2019

INHOUDSOPGAVE

1 INLEIDING

1.1 Algemeen

Iedereen heeft recht op privacy. Gemeenten verzamelen en gebruiken veel persoonsgegevens. Deze gegevens zijn nodig voor het uitvoeren van taken. De gemeente is verantwoordelijk voor de bescherming van deze persoonsgegevens.

De bescherming van persoonsgegevens speelt een steeds belangrijkere rol door de:

- technologie die zich steeds sneller ontwikkelt,
- toename in dataverkeer,
- toename in het verzamelen en delen van gegevens,
- risico's van cybercrime,
- samenleving die steeds kritischer wordt,
- behoefte en rechten van inwoners om inzicht in de verwerking van zijn of haar persoonsgegevens,
- toename van de hoeveelheid gevoelige informatie van personen (bijvoorbeeld jeugdzorg, maatschappelijke ondersteuning, de zorg voor chronisch zieken, ouderen en gehandicapten, leerlingzaken).

Iedereen heeft recht op correcte, veilige en betrouwbare informatieverwerking en moet erop kunnen vertrouwen dat de gemeente zorgvuldig met deze gegevens omgaat.

1.2 Reikwijdte en afbakening privacy

Het gemeentelijk privacybeleid is van toepassing op alle taken en processen waar de gemeente voor verantwoordelijk is. Het privacybeleid heeft betrekking op de persoonsgegevens van personen van wie de gemeente Almelo gegevens verwerkt (of laat verwerken).

Onder persoonsgegevens verstaan we alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"). Dit betekent dat informatie direct over iemand gaat of naar deze persoon te herleiden is.

Er is al snel sprake van 'verwerken' van persoonsgegevens. Verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen,

combineren, afschermen, wissen of vernietigen van gegevens valt allemaal onder het verwerken van persoonsgegevens.

Verdere definities met betrekking tot de verwerking van persoonsgegevens zijn opgenomen in de Algemene Verordening Gegevensbescherming (AVG)

Dit privacybeleid is van toepassing op:

- alle processen waarbinnen persoonsgegevens worden verwerkt,
- informatiesystemen die de gemeente gebruikt waarin persoonsgegevens worden verwerkt,
- alle ruimten en devices die door gemeenteambtenaren worden gebruikt waar(op) persoonsgegevens worden verwerkt,
- alle geldende normen en regels op het gebied van privacy.

1.3 Opbouw privacybeleid

Het privacybeleid geldt als algemeen beleid. Hierin zijn de kaders met de risico's en maatregelen beschreven, om te voldoen aan wet- en regelgeving. Voor bepaalde domeinen kan het nodig zijn om aanvullend een specifiek privacybeleid vast te stellen. Denk hierbij aan het sociaal domein, publiekszaken, leerlingzaken, schuldsanering, belastingen. Daarnaast wordt er ten behoeve van de medewerkers van de gemeente Almelo een praktische handreiking opgesteld en beschikt de gemeente over een 'Privacyreglement Gebruik Elektronische Communicatiemiddelen 2018' en een 'Privacyreglement DNO'.

1.4 Wetten en regels

De juridische grondslag voor privacy is terug te vinden in wet- en regelgeving. De bescherming van de privacy bij de verwerking van persoonsgegevens is een grondrecht. Dit is geregeld in:

- Grondwet (artikel 10)
- Handvest van de grondrechten van de Europese Unie (EHRM)
- Europees Verdrag voor de Rechten van de Mens (EVRM)
- Internationaal Kinderrechtenverdrag (IVRK)

De belangrijkste wet die op dit moment invulling geeft aan de bescherming van de privacy van personen bij de verwerking van persoonsgegevens is de Wet Bescherming Persoonsgegevens (Wbp). De Europese Algemene Verordening Gegevensbescherming en de Uitvoeringswet Algemene Verordening Gegevensbescherming vervangen op 25 mei 2018 de Wbp.

Verder is ook in specifieke regelgeving invulling gegeven aan de bescherming van de privacy bij de verwerking van persoonsgegevens zoals:

- Wet maatschappelijke ondersteuning (Wmo)
- Jeugdwet
- Basisregistratie Personen (BRP)

Informatiebeveiliging en de bescherming van persoonsgegevens zijn onlosmakelijk met elkaar verbonden. Informatiebeveiliging is een randvoorwaarde voor de borging van privacy bij de verwerking van persoonsgegevens. In het document Informatiebeveiligingsbeleid van de gemeente Almelo zijn maatregelen opgenomen om alle gegevens te beschermen.

2 PRIVACYBELEID

2.1 Doelstelling

Doel van dit privacybeleid is het beschrijven van kaders voor het verantwoord omgaan met persoonsgegevens en het waarborgen van de privacyrechten van personen waarvan de gemeente Almelo persoonsgegevens verwerkt.

2.2 Uitgangspunten

Iedereen werkzaam binnen de organisatie is verantwoordelijk voor het verantwoord omgaan met persoonsgegevens en het waarborgen van de privacyrechten van personen. Het is belangrijk om persoonsgegevens rechtmatig, behoorlijk en transparant te verwerken. De uitgangspunten hierbij zijn:

- De verwerking is noodzakelijk:
  * op basis van de wet of een overeenkomst,
  * bij bescherming van de vitale belangen,
  * voor een taak in het algemeen belang of voor de uitoefening van het openbaar gezag.
- Betrokkene is vooraf in eenvoudige en duidelijk taal geïnformeerd dat zijn/haar persoonsgegevens worden verwerkt en voor welk doel. Het is voldoende dit eenmalig bij de start van de werkzaamheden te doen.
- Alleen persoonsgegevens die noodzakelijk zijn voor het doel worden verwerkt;
- Persoonsgegevens zijn correct en actueel.

- Verzoeken van betrokkene op het gebied van rechten zoals 'het recht om vergeten te worden', 'recht op inzage', 'recht op rectificatie' worden in beginsel opgevolgd.
- Als identificatie niet meer noodzakelijk is voor het doel, dan moeten de persoonsgegevens worden verwijderd of geanonimiseerd.
- Persoonsgegevens zijn beveiligd door middel van technische en organisatorische maatregelen.
- Toestemming voor het verwerken van persoonsgegeven wordt alleen in uitzonderingssituaties gevraagd indien een andere grondslag niet mogelijk is. Betrokkenen zijn dan 'vrij' om hun toestemming te geven of te weigeren. Toestemming moet verder 'specifiek' en 'tijdgebonden' zijn. Toestemmingen worden altijd schriftelijk verleend en worden in een aparte registratie bijgehouden. Toestemming is bijvoorbeeld nodig voor het doorbreken van het medisch beroepsgeheim voor het opvragen van benodigde informatie bij een arts of specialist.

Het college van B&W is verantwoordelijk voor het naleven van deze uitgangspunten en moet dit kunnen aantonen.

2.3 Risico's

Bij schending van de privacy is het college van B&W wettelijk aansprakelijk. Het verwijtbaar onvoldoende beschermen van persoonsgegevens en het niet naleven van privacywet- en regelgeving kan leiden tot:

- het betalen van schadevergoeding. Elke benadeelde heeft hier recht op,
- reputatieschade en herstelkosten. Deze kunnen fors zijn en leiden tot verlies van vertrouwen in de overheid,
- onderzoeken, dwangmaatregelen en hoge bestuurlijke boetes. Bij overtreding van de AVG kan de Autoriteit Persoonsgegevens (de landelijke toezichthouder) een boete opleggen. Onder de AVG kan de boete oplopen tot maximaal € 20.000.000.

Binnen bepaalde domeinen wordt er gewerkt met zeer gevoelige (bijzondere) persoonsgegevens zoals medische gegevens, gegevens over iemands financiële situatie of strafrechtelijke gegevens. Voorbeelden zijn het sociale domein, leerlingzaken, burgerzaken. De risico's zijn hier hoger.
De risico's van schending van de privacy voor personen variëren van ongemak, substantiële benadeling, ernstige sociale beschadiging of gevaren voor de gezondheid en de persoonlijke veiligheid.
Om de risico's te beperken zijn maatregelen getroffen. Deze maatregelen zijn beschreven in hoofdstuk 4.

2.4 Evaluatie

Dit privacybeleid treedt in werking na vaststelling door het college van burgemeesters en wethouders. Het beleid wordt jaarlijks geëvalueerd en minimaal na 3 jaar, of als er belangrijke wijzigingen zijn, bijgesteld. Hierover wordt gerapporteerd in de cyclusdocumenten. De ondernemingsraad heeft volgens artikel 27 lid 1k van de (WOR) instemmingsrecht op elke regeling (dus ook het privacybeleid) die te maken heeft met het verwerken en beschermen van persoonsgegevens van medewerkers in de organisatie.

3 TAKEN EN VERANTWOORDELIJKHEDEN

3.1 Doelstelling

De bescherming van de privacy van betrokkenen beleggen bij de verantwoordelijke personen.

3.2 Afbakening rollen en verantwoordelijkheden

Het college van B&W is eindverantwoordelijk, maar iedereen binnen de organisatie is verantwoordelijk voor de bescherming van de privacy van betrokkenen. Onderstaande tabel brengt de verantwoordelijkheden in beeld aan de hand van het RASCI-model:

RASCI-model	**Verantwoordelijkheid**	**rol**
R	Responsible / Feitelijk verantwoordelijk	- Directie - Teammanager /proceseigenaar / projectleider - Alle medewerkers (incl. inhuur / externen)
A	Accountable / Eindverantwoordelijk	- College van B&W - Alle colleges bij gezamenlijk opdrachtgeverschap
S	Supporting / Uitvoerend	- Teammanager /proceseigenaar / projectleider - Alle medewerkers (incl. inhuur / externen)
C	Consulted / Adviserend, controlerend	- Chief Information Security Officer / Functionaris Gegevensbescherming

RASCI-model	Verantwoordelijkheid	rol
I	Informed / Geïnformeerd	- Gemeenteraad (privacy rechtelijk geen controlerende taak maar op basis van de Gemeentewet en de decentralisatiewetgeving een bestuurlijke toezichttaak) - Functionaris Gegevensbescherming (toezichthouder)

3.3 College van B&W

- is eindverantwoordelijk om te waarborgen dat persoonsgegevens worden beschermd in overeenstemming met wet- en regelgeving en op een behoorlijke en zorgvuldige manier. Er is een directe relatie met de beginselen van behoorlijk bestuur,
- stelt kaders voor de bescherming van de privacy op basis van wet- en regelgeving.

3.3.1 Functionaris voor de gegevensbescherming

- krijgt genoeg middelen ter beschikking om zijn taken goed te vervullen,
- is onafhankelijk toezichthouder op de toepassing van de AVG en krijgt binnen de organisatie geen instructies over de uitvoering van de taken,
- levert een belangrijke bijdrage aan juist gebruik van persoonsgegevens door de organisatie,
- is aangewezen door het college van B&W op grond van zijn professionele kwaliteiten, deskundigheid op het gebied van de wetgeving en de praktijk,
- mag naast zijn FG-taken eventueel andere taken of functies vervullen, maar er mag geen sprake zijn van belangenverstrengeling,
- mag werkzaam zijn voor meerdere organisaties,
- is verplicht zijn contactgegevens openbaar te maken,
- heeft toegang tot alle persoonsgegevens in de organisatie en de verwerkingsactiviteiten daarvan,
- wordt betrokken bij alles wat verband houdt met de bescherming van persoonsgegevens,
- krijgt eerst een melding van de verwerking van persoonsgegevens van de manager voordat de verwerking begint,
- is verplicht tot geheimhouding en vertrouwelijkheid.

De FG heeft minimaal de volgende taken en bevoegdheden:

- informeert en adviseert over de verplichtingen die de organisatie heeft met betrekking tot de bescherming van persoonsgegevens,
- ziet toe op de naleving van wet- en regelgeving en het door het college vastgestelde beleid met betrekking tot de bescherming van persoonsgegevens,
- ziet toe op het toewijzen van verantwoordelijkheden, bewustmaking en opleiding van de organisatie op het gebied van de bescherming van persoonsgegevens,

- actualiseert in overleg met de verantwoordelijk proceseigenaar / teammanager het 'Register van Verwerkingen',
- adviseert over en bepaalt voor welke verwerkingen een Privacy Impact Assessment (PIA, zie paragraaf 4.2.5) uitgevoerd moet worden,
- heeft een toetsende rol bij uitgevoerde PIA's,
- werkt samen met en treedt op als contactpersoon voor de Autoriteit Persoonsgegevens,
- evalueert jaarlijks het privacybeleid doet voorstellen tot implementatie en aanpassingen van het privacybeleid,
- rapporteert rechtstreeks aan het college van B&W.

3.3.2 Chief Information Security Officer (CISO)

- adviseert over informatiebeveiliging bij de uitvoering van PIA's o.g.v. zijn taken, genoemd in het '*Informatiebeveiligingsbeleid – gemeente Almelo 2018 – 2021*',
- adviseert over informatiebeveiliging bij beveiligingsincidenten o.g.v. de meldplicht datalekken.

3.4 Directie

- is verantwoordelijk voor kaderstelling en sturing,
- stuurt op gestelde kaders,
- controleert of de getroffen maatregelen voldoende bescherming bieden om de privacy van betrokkenen te beschermen,
- beoordeelt periodiek het privacybeleid op basis van de evaluatie en aanpassingen van het privacybeleid en –plan van de werkgroep privacy,
- draagt, conform artikel 38 lid 2 van de AVG, er zorg voor dat de FG over voldoende middelen (waaronder tijd) ter beschikking wordt gesteld voor het vervullen van zijn taken en het in stand houden van zijn deskundigheid.

3.5 De organisatie

Alle medewerkers (inclusief inhuur/externen) zijn verantwoordelijk voor de bescherming van de privacy van betrokkenen. Dat betekent dat iedereen zorgt voor een rechtmatige, behoorlijke en transparante verwerking van persoonsgegevens (zie paragraaf 2.2) alsook dat gelet wordt op de uitgangspunten subsidiariteit en proportionaliteit.

3.5.1 Teammanager / proceseigenaar / projectleider

- stelt, indien nodig, voor het betreffende organisatieonderdeel een specifiek privacybeleid op, vraagt hierover advies aan de werkgroep privacy en legt het aan het college voor ter vaststelling. Dit specifieke privacybeleid maakt onderdeel uit van dit overkoepelende privacybeleid,
- voert voor verwerkingen met een hoog risico, in samenspraak met de FG, Privacy Impact Assessments uit,
- zorgt voor naleving van wet-, regelgeving en het privacybeleid (rechtmatige, behoorlijke en transparante verwerking, bewustwording, gebruikt en evalueert PIA's, past 'Privacy by Design/Default' toe en is verantwoordelijk voor registratie van verwerkingsactiviteiten etc.),
- zorgt dat de FG naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens,
- maakt afspraken met andere organisatieonderdelen over het borgen van de privacy in geval van informatie die stroomt tussen verschillende organisatieonderdelen,
- leidinggevenden hebben het mandaat om namens het college verzoeken van burgers ('rechten van betrokkenen') af te handelen.

4 BEHEERSMAATREGELEN

4.1 Doelstelling

Iedereen heeft recht op privacy. Gemeenten verzamelen en gebruiken veel persoonsgegevens. Deze gegevens zijn nodig voor het uitvoeren van taken. De gemeente is verantwoordelijk voor de bescherming van deze persoonsgegevens. Met de maatregelen beschreven in dit hoofdstuk kunnen de doelstellingen van het privacybeleid worden gehaald en de risico's worden beperkt.

4.2 Maatregelen

Onderstaande maatregelen zijn getroffen om persoonsgegevens rechtmatig, behoorlijk en transparant te kunnen verwerken, volgens geldende wet- en regelgeving.

4.2.1 Transparantie

Betrokkenen krijgen vooraf duidelijke informatie (via de website en de dienstverlening (telefonisch, schriftelijk, email) over de verwerking van hun persoonsgegevens, het doel van de verwerking en hun rechten.

4.2.2 Naleving van het informatiebeveiligingsbeleid

Op basis van het informatiebeveiligingsbeleid zijn maatregelen getroffen om de bescherming van persoonsgegevens te waarborgen. Informatieveiligheid is een eerste voorwaarde voor gegevensbescherming in het kader van privacy.

4.2.3 Bewustwording

De mens is de belangrijkste factor in de omgang met persoonsgegevens. Bewustwording is essentieel voor het borgen van privacy in de organisatie. Het is belangrijk dat iedereen die werkt met privacygevoelige informatie zich bewust is van het belang om hier zorgvuldig mee om te gaan. Doorlopend wordt er aandacht geschonken aan de bewustwording.

4.2.4 Register van Verwerkingen

Er wordt een register bijgehouden met alle verwerkingsactiviteiten van persoonsgegevens per proces (art 30 AVG). Hierin worden onder andere de doeleinden van de verwerkingen, categorieën van betrokkenen en persoonsgegevens, derden ontvangers, bewaartermijn en beveiligingsmaatregelen opgenomen.

4.2.5 Privacy Impact Assessments (PIA's)

Voor (veranderingen in) processen, diensten en producten en informatiesystemen, waar persoonsgegevens worden verwerkt, kunnen PIA's worden uitgevoerd. De AVG noemt dit een Gegevensbeschermingseffectbeoordeling (artikel 35 AVG).

Systematisch worden verwerkingen van persoonsgegevens, doeleinden, risico's en (voorgenomen) maatregelen beschreven. Het doel is om de impact van de verwerkingen op de bescherming van persoonsgegevens in kaart te brengen. Het uitvoeren van een PIA is niet altijd verplicht. In geval van hogere risico's (bijvoorbeeld bij de verwerking van bijzondere persoonsgegevens, grootschalige verwerkingen, verwerkingen van bijzondere kwetsbare doelgroepen zoals jongeren, etc.) is een PIA verplicht.
Per PIA wordt advies aan de FG gevraagd. Als uit een PIA blijkt dat er sprake is van risicovolle verwerkingen zonder dat het mogelijk is hier maatregelen tegen te nemen wordt de Autoriteit Persoonsgegevens op de hoogte gesteld. De Autoriteit Persoonsgegevens maakt het overzicht met risicovolle verwerkingen openbaar.

4.2.6 Privacy by Design / Privacy by Default

Privacy by Design houdt in dat vanaf het ontwerpen van een nieuw of aangepast proces, product, dienst of informatiesysteem wordt nagedacht over:

- het rechtmatig, behoorlijk en transparant verwerken van persoonsgegevens (paragraaf 2.2),
- de maatregelen die hiervoor nodig zijn.

Privacy by Default betekent dat de standaard instellingen in systemen zijn ingesteld om maximale privacy bescherming te borgen. De AVG noemt dit 'Gegevensbescherming door ontwerp en standaardinstellingen'.
Bij het toepassen van Privacy by Design/Default wordt advies aan de FG gevraagd.

4.2.7 Verwerkersovereenkomst

Er zijn verwerkersovereenkomsten afgesloten met verwerkers. Een verwerkersovereenkomst is wettelijk verplicht als het verwerken van persoonsgegevens aan een andere partij wordt uitbesteed. Er worden afspraken gemaakt over:

- de doeleinden waarvoor de gegevens mogen worden verwerkt,
- hoe de verwerker met de persoonsgegevens moet omgaan,
- welke beveiligingsmaatregelen moeten worden genomen,
- welke vormen van toezicht de eigenaar van de gegevens mag uitoefenen,
- de geheimhoudingsplicht,
- inschakeling van derden en onderaannemers,
- locatie van de data,
- aansprakelijkheid in geval van schade door het niet naleven van regelgeving
- het vernietigen van persoonsgegevens na beëindiging van de overeenkomst.

4.2.8 Meldplicht datalekken

Datalekken worden intern via de cyclusdocumenten en indien nodig bij de Autoriteit Persoonsgegevens en de betrokkene(n) gemeld.

De meldplicht datalekken houdt in dat een ernstig datalek binnen 72 uur moet worden gemeld bij de Autoriteit Persoonsgegevens. Er is sprake van een ernstig datalek als persoonsgegevens:

- van gevoelige aard in handen (kunnen) vallen van derden die geen toegang tot die gegevens zouden mogen hebben,
- onjuist of onrechtmatig verwijderd zijn,
- niet juist en tijdig vernietigd zijn.

Een datalek moet aan de betrokkene(n) worden gemeld als de inbreuk waarschijnlijk ongunstige gevolgen heeft voor zijn of haar privéleven.

4.2.9 Toezicht en rapportage

De FG beoordeelt de naleving van het privacybeleid en rapporteert hierover in de cyclusdocumenten aan het college en de raad. De directie, lijnmanagers en medewerkers worden waar nodig geïnformeerd.

4.2.10 Klacht

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 klachtenregeling niets over zegt, beslist het verantwoordelijk bestuursorgaan van de gemeente.