

## Privacybeleid 2024 Gemeente Almelo

### 1 Inleiding

#### 1.1 Achtergrond

Gemeente Almelo hecht grote waarde aan een beheerste en integere omgang met persoonsgegevens, waarbij het belang van haar inwoners en medewerkers centraal staat.

Binnen de gemeente worden veel verschillende en soms complexe diensten verleend of uitgevoerd waarbij dagelijks op grote schaal persoonsgegevens worden verwerkt. Gegevens worden bijvoorbeeld ingezien, verzonden naar anderen, aangepast, opgeslagen of verwijderd.

Om de privacy van alle hierbij betrokken personen te kunnen beschermen is het noodzakelijk dat de verwerking van persoonsgegevens zorgvuldig en in overeenstemming met de relevante wet- en regelgeving gebeurt.

Ten dienste daarvan is privacybeleid (hierna: *Beleid*) opgesteld, dat bijdraagt aan een adequate bescherming en verantwoorde omgang met persoonsgegevens en het verantwoorden daarvan.

#### 1.2 Reikwijdte

Dit *Beleid* is van toepassing op:

- Alle gestructureerde persoonsgegevens die gemeente Almelo verwerkt of laat verwerken, zowel fysiek als digitaal, zowel intern als extern;
- Alle taken en processen waarin persoonsgegevens worden verwerkt waar gemeente Almelo verantwoordelijk voor is;
- Alle personen en/of organisaties (zowel intern als extern) die persoonsgegevens gemeente Almelo verwerken;
- Alle organisatorische, procedurele en technische maatregelen ter bescherming van persoonsgegevens.

#### 1.3 Werking van dit document

• De uitgangspunten rondom de verwerking van persoonsgegevens zijn gebaseerd op de Algemene Verordening Gegevensbescherming (hierna: *AVG*) en de Wet politiegegevens (hierna: *Wpg*). Wanneer er wordt gesproken over gegevens, betreffen dit zowel politiegegevens als overige persoonsgegevens, tenzij anders aangegeven.

Vanzelfsprekend voldoet gemeente Almelo aan eventuele aanvullende eisen die worden opgelegd vanuit wetgeving of die gemeente Almelo contractueel heeft afgesproken met derden.

• Gemeente Almelo hanteert met betrekking tot deze uitgangspunten het principe "pas toe of leg uit". Afwijkingen van de uitgangspunten dienen voorgelegd te worden aan het college.

• De uitgangspunten in dit *Beleid* zijn richtinggevend (parapluregels) en geen vervanging voor het inrichten en implementeren van meer gedetailleerde en specifiek beheersmaatregelen op basis van gerichte risico-overwegingen per proces, systeem of applicatie.

• De kosten van beheersmaatregelen moeten passen bij de risico's die de gemeente Almelo loopt. Hierbij geniet een technische oplossing altijd de voorkeur boven gedragsvoorschriften.

• Het college van Burgemeester en Wethouders (hierna: het college) en de directie bevorderen de communicatie en bewustwording rondom privacy zodat zowel interne als externe gebruikers hun verantwoordelijkheden rondom gegevensbescherming begrijpen en nakomen.

#### 1.4 Gerelateerde documenten

Dit *Beleid* hangt samen met de laatst vastgestelde versies van volgende documenten:

- Strategisch (INT-77330) en tactisch (INT-87858) informatiebeveiligingsbeleid
- *Beleid* Wet politiegegevens (INT-90612)

## 2 Beleidsuitgangspunten

### 2.1 Algemeen

- Gegevens worden alleen verwerkt met een wettelijke grondslag.
- Alle verwerkingen van gegevens zijn opgenomen in een verwerkingsregister.
- Alle medewerkers, zowel intern als extern, hebben een schriftelijk vastgelegde geheimhoudingsplicht.
- Gegevens zijn beschermd tegen onbevoegden.
- Gegevens worden enkel verwerkt indien dit noodzakelijk en rechtmatig is en zolang de verwerking plaatsvindt in lijn met het doel.
- Gegevens worden niet langer bewaard dan wettelijk vastgelegd of noodzakelijk.
- Gegevens worden gedeeld met medewerkers of derden die dit nodig hebben.

### 2.2 Governance

- Voor het waarborgen van gegevensbescherming is een managementcyclus opgesteld.
- Kwetsbaarheden, bedreigingen en incidenten worden gemeld en gerapporteerd.
- Vereiste verwerkersovereenkomsten worden afgesloten en beheerd.
- Op dienstverleners die namens gemeente Almelo gegevens verwerken wordt toegezien.
- Ontwikkelingen in privacywet- en regelgeving zijn inzichtelijk.
- Op verwerkingen van persoonsgegevens wordt toegezien op het gebied van relevante wettelijke uitgangspunten.

### 2.3 Organisatie

- Een Functionaris Gegevensbescherming is aangesteld.
- Taken en verantwoordelijkheden rondom gegevensbescherming zijn belegd.
- Toegang tot informatie wordt beperkt tot noodzakelijke informatie.

### 2.4 Processen

- Een proces is ingericht voor de juiste afhandeling van datalekken.
- Een proces is ingericht voor de juiste afhandeling van rechtenverzoeken.
- Systemen en processen zijn zodanig ingericht dat ze niet meer gegevens verwerken dan noodzakelijk voor het doel.
- Mogelijk hoge risico's m.b.t. de bescherming van gegevens worden geïdentificeerd, beoordeeld en aantoonbaar gemitigeerd.
- Binnen een week wordt het doel van de verwerking van de politiegegevens vastgelegd ten behoeve van het onderzoek.

### 2.5 Communicatie & bewustzijn

- Websites en andere kanalen voor externe bezoekers hebben een privacyverklaring.
- Communicatie over privacy is begrijpelijk, transparant en relevant.
- Medewerkers worden getraind op de omgang met gegevens.

## 2.1 Algemeen

<b>Omschrijving</b>	<b>Gegevens worden alleen verwerkt met een wettelijke grondslag</b>
Reden	Alle verwerkingen van gegevens zonder grondslag zijn onrechtmatig
Toelichting	Indien wij gegevens verwerken in de rol van Verwerker, dient de Verwerkingsverantwoordelijke een wettelijke grondslag te hebben
<b>Omschrijving</b>	<b>Alle verwerkingen van gegevens zijn opgenomen in een verwerkingsregister</b>
Reden	Wettelijk vereiste
Toelichting	Dit uitgangspunt betekent dat er een verwerkingsregister is opgesteld en up-to-date wordt gehouden.
<b>Omschrijving</b>	<b>Alle medewerkers, zowel intern als extern, hebben een schriftelijk vastgelegde geheimhoudingsplicht</b>
Reden	De aard van de gegevens en het belang van privacy voor de inwoners veronderstelt een hoge mate van integriteit
Toelichting	
<b>Omschrijving</b>	<b>Gegevens zijn beschermd tegen onbevoegden</b>
Reden	Om de privacy van de betrokkenen te waarborgen en de risico's voor de gemeente Almelo in geval van verlies, diefstal en ongewenste wijzigingen te mitigeren, is bescherming noodzakelijk
Toelichting	De eisen rondom de beveiliging van gegevens zijn nader uitgewerkt in het informatiebeveiligingsbeleid en onderliggende of aanverwante stukken
<b>Omschrijving</b>	<b>Gegevens worden enkel verwerkt indien dit noodzakelijk en rechtmatig is en zolang de verwerking plaatsvindt in lijn met het doel</b>
Reden	Wettelijk vereiste
Toelichting	-
<b>Omschrijving</b>	<b>Gegevens worden niet langer bewaard dan wettelijk vastgelegd of noodzakelijk</b>
Reden	Wettelijk vereiste
Toelichting	Politiegegevens hebben specifieke, bij wet vastgelegde bewaartermijnen. Overige persoonsgegevens mogen bij wet niet langer dan noodzakelijk worden bewaard
<b>Omschrijving</b>	<b>Gegevens worden gedeeld met medewerkers of derden die dit nodig hebben</b>
Reden	Noodzakelijk voor een juiste uitvoering van werkzaamheden
Toelichting	Gegevens worden gedeeld met medewerkers die deze gegevens nodig hebben voor hun werkzaamheden (need to know principe). Ook mogen politiegegevens worden gedeeld met instanties die binnen de Wpg vallen (free flow principe).

## 2.2 Governance

<b>Omschrijving</b>	<b>Voor het waarborgen van gegevensbescherming is een managementcyclus ingericht</b>
Reden	Gegevensbescherming is een on-going proces dat geborgd dient te zijn in een PDCA-cyclus
Toelichting	Voor dit uitgangspunt moeten de volgende zaken zijn ingericht:  PDCA-cyclus van dit Beleid en overige privacygerelateerde documenten (zoals privacyverklaring, procedures) over een periode van 4 jaar

Periodiek rapportage over alle hoge risico's op het gebied van gegevensbescherming aan de directie

<b>Omschrijving</b>	<b>Kwetsbaarheden, bedreigingen en incidenten worden gemeld en gerapporteerd</b>
Reden	Kwetsbaarheden, bedreigingen en incidenten moeten zo snel mogelijk opgelost op gemitigeerd worden, en naar de toekomst worden voorkomen
Toelichting	Voor dit uitgangspunt moeten de volgende zaken zijn ingericht:  Registratieproces en-systeem voor datalekken en overige bijzonderheden Periodieke rapportage aan de directie over kwetsbaarheden, incidenten en bedreigingen Gedetailleerde terugkoppeling aan leiding over ontstaan en opvolging van belangrijke incidenten

<b>Omschrijving</b>	<b>Vereiste verwerkersovereenkomsten worden afgesloten</b>
Reden	Afspraken over de verwerking van gegevens moeten vastgelegd worden waarbij de zeggenschap over de gegevens bij de Verwerkingsverantwoordelijke blijft liggen
Toelichting	-

<b>Omschrijving</b>	<b>Op dienstverleners die namens gemeente Almelo gegevens verwerken wordt toegezien</b>
Reden	Goed opdrachtgeverschap Risicobeheerder binnen uitbestede en ingehuurde diensten
Toelichting	Voor dit uitgangspunt moet zijn ingericht: Proces audit/beoordeling dienstverleners

<b>Omschrijving</b>	<b>Ontwikkelingen in privacywet- en regelgeving zijn inzichtelijk</b>
Reden	Vorkomen non-compliance Vorbereiden op opkomende risico's
Toelichting	Zowel de AVG als de Wpg zijn relatief nieuwe wetten met een aantal open normen. Jurisprudentie en bijvoorbeeld standpunten van toezichthouders moeten uit gaan wijzen hoe eventuele onduidelijkheden in de wet nader geïnterpreteerd moeten worden

<b>Omschrijving</b>	<b>Op verwerkingen van persoonsgegevens wordt toegezien op het gebied van relevante wettelijke uitgangspunten</b>
Reden	Wettelijke vereiste
Toelichting	Audit vindt plaats door externe- en interne privacy audits. De audit ziet op wettelijke verplichtingen van de AVG en de Wpg.

## 2.3 Organisatie

<b>Omschrijving</b>	<b>Een Functionaris Gegevensbescherming is aangesteld</b>
Reden	Wettelijk vereiste
Toelichting	De Functionaris Gegevensbescherming (FG) houdt toezicht op en adviseert over de naleving van zowel de AVG als de Wpg binnen gemeente Almelo

<b>Omschrijving</b>	<b>Taken en verantwoordelijkheden rondom gegevensbescherming zijn belegd</b>
Reden	Aanbrengen van organisatorische rol- en functiescheiding Aanwezig hebben van noodzakelijke specialismen rondom risicomanagement, gegevensbescherming en informatiebeveiliging Wettelijk vereiste
Toelichting	De volgende rollen zijn minimaal vereist: FG; Bevoegd functionaris i.h.k.v. de Wpg Privacy Officer (C)ISO; Risicomanager(s)
<b>Omschrijving</b>	<b>Toegang tot informatie wordt beperkt tot noodzakelijke informatie</b>
Reden	Voorkomen van ongewenste functievermenging Voorkomen van ongeoorloofde toegang tot systemen en gegevens
Toelichting	De eisen rondom logische toegang en autorisatie zijn uitgewerkt in aanvullende documentatie.

## 2.4 Processen

<b>Omschrijving</b>	<b>Een proces is ingericht voor de juiste afhandeling van datalekken</b>
Reden	Processen geven richting aan een beheerste bedrijfsvoering en zijn noodzakelijk bij de beheersing van de risico's op het gebied van gegevensbescherming. Schendingen van wetgeving en contractuele verplichtingen worden voorkomen.
Toelichting	De Verwerkingsverantwoordelijke moet datalekken binnen 72 uur bij de externe toezichthouder melden. Een snelle en juiste afhandeling is daarom noodzakelijk.
<b>Omschrijving</b>	<b>Een proces is ingericht voor de juiste afhandeling van rechtenverzoeken</b>
Reden	Processen geven richting aan een beheerste bedrijfsvoering en zijn noodzakelijk bij de beheersing van de risico's op het gebied van gegevensbescherming. Schending van wetgeving wordt voorkomen.
Toelichting	Rechten van betrokkenen zijn wettelijk vastgelegd. Een tijdige en juiste afhandeling is daarom van belang.
<b>Omschrijving</b>	<b>Systemen en processen zijn zodanig ingericht dat ze niet meer gegevens verwerken dan noodzakelijk</b>
Reden	Wettelijk vereiste
Toelichting	Al direct bij systeem- en procesontwerp en vormen van redesign moet aantoonbaar rekening worden gehouden met optimale bescherming van persoonsgegevens (privacy by design).
<b>Omschrijving</b>	<b>Mogelijk hoge risico's m.b.t. gegevensbescherming worden geïdentificeerd, beoordeeld en aantoonbaar gemitigeerd</b>
Reden	Wettelijk vereiste
Toelichting	Risico's moeten in kaart worden gebracht (bijvoorbeeld middels DPIA's/GEB's. Hoge risico's moeten worden gemitigeerd.
<b>Omschrijving</b>	<b>Binnen een week wordt het doel van de verwerking van de politiegegevens vastgelegd ten behoeve van het onderzoek</b>

Reden Wettelijk vereiste

Toelichting

## 2.5 Communicatie en bewustzijn

**Omschrijving** Websites en andere kanalen voor externe bezoekers hebben een privacyverklaring

Reden Voldoen aan wettelijke informatieplicht

Toelichting Websites zijn vaak het eerste en zichtbaarste communicatiekanaal met externen. Hier moet dan ook direct aan de informatieplicht worden voldaan.

**Omschrijving** Communicatie over privacy is begrijpelijk, transparant en relevant

Reden Voldoen aan wettelijke informatieplicht

Toelichting Dit uitgangspunt impliceert dat er verschillende inhoud en wordt gebruikt bij verschillende kanalen, afgestemd op de doelgroep (inwoners, leveranciers, medewerkers, sollicitanten, etc.).

**Omschrijving** Medewerkers worden getraind op de omgang met gegevens

Reden Verkleinen van het kans op incidenten

Toelichting Bij het waarborgen van privacy en het beschermen van gegevens, is de grootste afhankelijkheid het menselijk handelen. Een groot bewustzijn bij medewerkers over hoe om te gaan met persoonsgegevens is daarom van essentieel belang.

Binnen bepaalde domeinen moet er specifieke aandacht worden besteed aan de Wpg.

## Slotbepalingen

1. Deze nota treedt in werking na vaststelling door het college.
2. Het Privacybeleid 2018-2021 komt met de vaststelling van deze nota te vervallen.

### Versie:

Privacybeleid 2024 Gemeente Almelo v1.0

### Toezichthouder:

Functionaris Gegevensbescherming

#### 1. Inhoud

1 Inleiding 3

1.1 Achtergrond 3

1.2 Reikwijdte 3

1.3 Werking van dit document 3

1.4 Gerelateerde documenten 4

#### 2 Beleidsuitgangspunten 5

2.1 Algemeen 6

2.2 Governance 7

2.3 Organisatie 9

2.4 Processen 10

2.5 Communicatie en bewustzijn 11

Slotbepalingen 11

