

Privacybeleid Gemeente Westerwolde 2025-2029

Begrippenlijst

- a) **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 (bijv. naam, adres, geboortedatum). Naast gewone persoonsgegevens zijn er ook bijzondere persoonsgegevens. Die gaan over gevoelige onderwerpen, bijvoorbeeld etnische achtergrond, politieke voorkeuren en de gezondheid.
- b) **Politiegegevens:** Persoonsgegevens die worden verwerkt in het kader van de politietak, zoals bedoeld in de artikelen 3 en 4 van de Politiewet 2012.
- c) **AVG:** Verordening (EU) 2016/679 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (Algemene verordening gegevensbescherming).
- d) **Wpg:** Wet politiegegevens.
- e) **Verwerking:** Alle activiteiten die een organisatie kan uitvoeren met betrekking tot persoonsgegevens, vanaf het moment van verzameling tot en met het moment van verwijdering. Denk aan vastleggen, bewaren, verzamelen, bij elkaar voegen, verstrekken aan een ander, vernietigen en lezen.
- f) **Betrokkene:** De persoon op wie de persoonsgegevens betrekking hebben. De betrokkene is degene van wie de gegevens worden verwerkt.
- g) **Verwerkingsverantwoordelijke:** De normadressaat van de AVG. Deze partij bepaalt het doel en de middelen van de verwerking. Als de gemeente besluit 'waarom' en 'hoe' persoonsgegevens verwerkt worden, is zij de verwerkingsverantwoordelijke.
- h) **Verwerker:** Een derde partij die persoonsgegevens verwerkt namens de verwerkingsverantwoordelijke.
- i) **Functionaris Gegevensbescherming (FG):** De interne toezichthouder op het gebied van privacywetgeving.
- j) **Privacy Officer (PO) :** De juridisch adviseur op het gebied van privacywetgeving en hoeder van het privacybeleid van een organisatie.
- k) **DPIA:** Een hulpmiddel om de privacyrisico's van een verwerking vooraf te beoordelen, zodat de gemeente maatregelen kan treffen om deze risico's te verkleinen. Een DPIA is verplicht bij verwerkingen met een hoog risico.
- l) **Datalek:** een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens.
- m) **Geautomatiseerde besluitvorming:** Besluitvorming zonder of met beperkte menselijke tussenkomst.
- n) **Doorgifte:** Het overdragen of beschikbaar stellen van persoonsgegevens aan een organisatie, persoon of land buiten de Europese Economische Ruimte (EER).

1. Inleiding

Gemeente Westerwolde verwerkt een aanzienlijke hoeveelheid persoonsgegevens van haar burgers voor het leveren van diensten, het uitvoeren van gemeentelijke taken en het verzorgen van openbaar onderwijs. Daarnaast worden ook persoonsgegevens van medewerkers verwerkt in de rol van werkgever¹. Deze gegevens zijn essentieel voor het goed functioneren van de gemeentelijke organisatie en het bieden van de juiste zorg en ondersteuning aan inwoners.

Met de snelle technologische ontwikkelingen van de afgelopen jaren wordt het steeds noodzakelijker om zorgvuldig met persoonsgegevens om te gaan. Nieuwe digitale mogelijkheden bieden veel voordelen, maar stellen ook grotere eisen aan de manier waarop persoonsgegevens worden beschermd. Het is daarom van groot belang dat persoonsgegevens op een verantwoorde en veilige manier worden verwerkt. Om deze redenen heeft gemeente Westerwolde dit privacybeleid opgesteld.

1) Dit beleid is eveneens van toepassing op de verwerking van persoonsgegevens van (oud-)medewerkers van zowel de gemeentelijke organisatie als de openbare basisscholen. Dit omvat onder andere verwerkingen in het kader van verzuimregistratie, personeelsdossiers en applicatiemonitoring.

1.1 Doel

Dit beleid beschrijft hoe de bescherming van persoonsgegevens wordt gewaarborgd en biedt kaders voor het treffen van passende technische en organisatorische maatregelen om aantoonbaar te voldoen aan privacywetgeving zoals de AVG en Wpg.

1.2 Visie

Gemeente Westerwolde volgt vier leidende principes van dienstverlening. Dit is ten minste wat inwoners van de gemeente mogen verwachten:

1. *Onze taal is eerlijk, duidelijk en direct*
2. *We gaan respectvol met elkaar om*
3. *We durven voorbij de regels te kijken*
4. *We gaan naar de mensen toe*

Dit leidt tot de volgende visie op het gebied van privacy:

De gemeente streeft ernaar persoonsgegevens op een transparante, veilige en respectvolle manier te verwerken, waarbij het recht op privacy van elke burger wordt gewaarborgd. Er wordt actief geluisterd naar de zorgen van inwoners en gezocht naar innovatieve oplossingen die zowel de privacy beschermen als de dienstverlening verbeteren. Dit gebeurt met een duidelijke, eerlijke communicatie en een focus op het aanbieden van toegankelijke en gebruiksvriendelijke digitale diensten.

1.3 Scope

Dit privacybeleid is van toepassing op alle taken en processen waar de gemeente voor verantwoordelijk is, waaronder ook het Openbaar Onderwijs Westerwolde (OOW), en heeft betrekking op de persoonsgegevens van personen van wie gemeente Westerwolde gegevens verwerkt (of laat verwerken). Het beleid is richtinggevend en kaderstellend, en wordt aangevuld met onderwerpspecifieke beleidsdocumenten en werkinstructies.

1.4 Raakvlakken met andere beleidsthema's

Op zijn beurt vormt dit privacybeleid een specifieke aanvulling op het Strategisch gemeentebreed informatiebeveiligingsbeleid 2024-2026 (zie pagina 6). Dit bevat kaders om de beschikbaarheid, integriteit en vertrouwelijkheid van (persoons)gegevens binnen de gemeentelijke organisatie te waarborgen. Daarmee raakt het aan de bescherming van persoonsgegevens en is het onlosmakelijk verbonden met privacy. Daar waar het beleid elkaar raakt, zal in het Privacybeleid worden verwezen naar het Strategisch gemeentebreed informatiebeveiligingsbeleid.

2. Uitgangspunten en beleidsprincipes

2.1 Beginselen

Privacywetgeving is gebaseerd op zes basisprincipes, in de AVG 'beginselen' genoemd. Op de gemeente rust een verantwoordingsplicht, het zevende overkoepelende basisprincipe, wat inhoudt dat zij aantoonbaar aan deze basisprincipes moet voldoen. Gemeente Westerwolde onderschrijft de basisprincipes en verwerkt persoonsgegevens slechts in overeenstemming met de principes.

2.1.1 Rechtmatigheid, behoorlijkheid en transparantie

De verwerking van persoonsgegevens door de gemeente is rechtmatig, behoorlijk en transparant. Dit houdt in dat verwerking alleen plaatsvindt wanneer er een rechtmatige grondslag voor bestaat. Voor de gemeente is dit doorgaans een wettelijke verplichting of een taak van algemeen belang die zij moet vervullen. In situaties waarin geen wettelijke of contractuele verplichting geldt, vraagt de gemeente vooraf toestemming van de betrokkene voor de verwerking van diens persoonsgegevens. Voor de verwerking van politiegegevens geldt dat de gemeente alleen gegevens verwerkt als dit gebaseerd is op artikel 8, 9 of 13 Wpg.

Verder is de verwerking van persoonsgegevens op geen enkele manier nadelig, discriminerend, onverwacht of misleidend voor de betrokkenen, tenzij hiervoor een rechtvaardiging bestaat.

Voorafgaand aan iedere verwerking stelt de gemeente op een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke wijze en in duidelijke en eenvoudige taal de betrokkene op de hoogte van de verwerking van persoonsgegevens, inclusief de methoden en de doeleinden waarvoor deze gegevens worden gebruikt. Tevens worden zij op begrijpelijke wijze geïnformeerd over hun rechten en de stappen die ze kunnen nemen om deze rechten uit te oefenen. De gemeente geeft in algemene zin invulling aan deze informatieplicht door het beschikbaar stellen van een privacyverklaring op de website. Afwijkingen van de informatieplicht kunnen alleen plaatsvinden wanneer de wet dit uitdrukkelijk toestaat.

2.1.2 Doelbinding

De gemeente verwerkt persoonsgegevens alleen voor een specifiek en duidelijk omschreven doel en legt dit doel vast in het register van verwerkingen. Het doel bepaalt welke gegevens worden verwerkt en in welke mate. Er worden uitsluitend gegevens verzameld die strikt noodzakelijk zijn om het doel te bereiken, en waar mogelijk wordt gekozen voor een aanpak die minder impact heeft op de privacy van betrokkenen. De persoonsgegevens worden slechts voor een secundair doel verwerkt (verdere verwerking) indien dat doel verenigbaar is met het primaire doel van de verwerking. Voorafgaand aan iedere verdere verwerking van persoonsgegevens toetst de gemeente de mate waarin het secundaire doel verenigbaar is met het primaire doel.

Specifiek voor de verwerking van politiegegevens in het kader van artikel 9 Wpg geldt dat het doel van het onderzoek binnen een week, nadat is begonnen met de verwerking, schriftelijk wordt vastgelegd.

2.1.3 Dataminimalisatie

De gemeente verwerkt uitsluitend persoonsgegevens wanneer dit strikt noodzakelijk is. Bij het ontwerpen van een werkproces wordt eerst beoordeeld of het verzamelen van persoonsgegevens onmisbaar is voor het bereiken van het beoogde doel. Alleen de gegevens die echt noodzakelijk zijn, worden vervolgens verwerkt.

2.1.4 Juistheid

De gemeente zorgt ervoor dat de kwaliteit van de verwerkte persoonsgegevens op orde is. Dat houdt in dat de gegevens juist en volledig zijn. Daarom treft de gemeente passende maatregelen om onjuiste persoonsgegevens onverwijld te wissen of te rectificeren.

2.1.5 Opslagbeperking

De gemeente hanteert bewaartermijnen voor persoonsgegevens op basis van geldende wet- en regelgeving en specifieke selectielijsten. Deze lijsten, opgesteld conform de Archiefwet 1995, geven aan hoelang bepaalde documenten met persoonsgegevens bewaard moeten blijven.

Als er geen wettelijke richtlijnen of selectielijsten beschikbaar zijn, wordt de bewaartermijn bepaald aan de hand van wat noodzakelijk is voor het doel van de verwerking. Persoonsgegevens worden niet langer bewaard dan strikt noodzakelijk, tenzij deze volledig geanonimiseerd zijn, waardoor identificatie van personen onmogelijk wordt.

Voor het bewaren van politiegegevens hanteert de gemeente de bewaartermijnen uit artikel 8 en 9 Wpg.

2.1.6 Integriteit en vertrouwelijkheid

De gemeente treft zowel technische als organisatorische maatregelen om persoonsgegevens te beschermen tegen ongeautoriseerd gebruik of onrechtmatige verwerking. Hierbij wordt gehandeld volgens het Strategisch gemeentebreed informatiebeveiligingsbeleid.

2.2 Rechten van betrokkenen

Wanneer de gemeente persoonsgegevens verwerkt, hebben de betrokkenen een aantal wettelijke rechten, te weten:

- het recht van inzage;
- het recht op rectificatie;
- het recht op gegevenswissing;
- het recht op beperking van de verwerking;
- het recht op overdraagbaarheid van gegevens;
- en het recht van bezwaar.

De gemeente informeert de betrokkene zo snel mogelijk, maar uiterlijk binnen een maand na ontvangst van een verzoek tot gebruik van een recht, over de afhandeling ervan. Indien nodig, bijvoorbeeld vanwege de complexiteit van het verzoek of een groot aantal gelijktijdige verzoeken, kan deze termijn met maximaal twee maanden worden verlengd. De betrokkene wordt binnen een maand na ontvangst van het verzoek geïnformeerd over een eventuele verlenging van de termijn.

In uitzonderlijke situaties kan een inzageverzoek worden geweigerd, bijvoorbeeld wanneer het verzoek buitensporig of onredelijk is. Ook een verzoek tot verwijdering van persoonsgegevens kan worden geweigerd als de gegevens noodzakelijk zijn, bijvoorbeeld voor een juridische procedure.

Beslissingen op verzoeken worden beschouwd als besluiten in de zin van de Algemene wet bestuursrecht.

2.3 Convenanten en verwerkersovereenkomsten

Voor de uitgangspunten en beleidsprincipes die afspraken met verwerkers in het kader van de gemeentelijke organisatie betreffen, verwijst de gemeente naar het onderdeel Privacy van het Addendum inkoopbeleid gemeente Westerwolde 8 februari 2021 V2.0.

Voor verwerkersovereenkomsten die worden gesloten door Openbaar Onderwijs Westerwolde wordt gebruik gemaakt van de modelverwerkersovereenkomst van het Convenant Digitale Onderwijsmiddelen en Privacy 4.0.

Wanneer de gemeente samenwerkt met andere publieke of overheidsorganisaties om taken van algemeen belang uit te voeren, kunnen meerdere partijen verantwoordelijk zijn voor het verwerken van persoonsgegevens, samen of apart. Er worden dan passende overeenkomsten gesloten waarin de respectieve verantwoordelijkheden voor het naleven van de AVG worden vastgelegd. Externe partijen waarborgen hetzelfde niveau van gegevensbescherming als de gemeente.

2.4 Register van verwerkingen

De gemeente houdt een register bij van verwerkingen van persoonsgegevens waarvoor zij verantwoordelijk is. Daar worden diverse gegevens in vastgelegd, zoals:

- de naam en contactgegevens van de verwerkingsverantwoordelijke;
- de verwerkingsdoeleinden;
- een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
- de categorieën van ontvangers van de persoonsgegevens;
- de bewaartermijnen van persoonsgegevens;
- een algemene beschrijving van de beveiligingsmaatregelen.

Voor de verwerking van politiegegevens houdt de gemeente overeenkomstig artikel 31d Wpg een apart register bij.

2.5 Privacy by Design & Default

De gemeente zorgt ervoor dat bij de ontwikkeling en aanschaf van nieuwe diensten, systemen of processen privacy en gegevensbescherming altijd centraal staan. Dit wordt aangeduid als Privacy by Design. Bij het ontwerpen van deze nieuwe initiatieven worden concrete maatregelen genomen om de bescherming van persoonsgegevens te waarborgen. Bovendien hanteert de gemeente het principe van Privacy by Default, waarbij de standaardinstellingen altijd zo zijn ingesteld dat ze de privacy van de betrokkenen zoveel mogelijk beschermen.

2.5.1 DPIA's

Gemeente Westerwolde geeft invulling aan deze beginselen door onder andere bij de start of wijziging van iedere verwerking die een hoog risico inhoudt voor de rechten en vrijheden van betrokkenen een zogenoemde Data Protection Impact Assessment (DPIA) uit te voeren. Als uit de DPIA blijkt dat er risico's zijn verbonden aan de verwerking, zullen er passende maatregelen worden getroffen om de risico's te beperken. De afdelingsmanager is daarbij als proceseigenaar verantwoordelijk en wordt hierbij ondersteund door de PO. Bij de uitvoering van de DPIA wordt de FG altijd om advies gevraagd. Als blijkt dat er onvoldoende passende maatregelen genomen kunnen worden om de risico's bij de verwerking van de persoonsgegevens te beperken, zal er eerst overlegd worden met de Autoriteit Persoonsgegevens (AP) voordat er met de verwerking wordt gestart.

Bij risicovolle verwerkingen die medewerkers raken, worden de Ondernemingsraad voor de gemeentelijke organisatie en de Medezeggenschapsraad voor Openbaar Onderwijs Westerwolde structureel geconsulteerd en betrokken bij de DPIA.

2.6 Datalekken

Iedere medewerker van de gemeente is verplicht om een datalek of het vermoeden hiervan direct te melden volgens de geldende procedure. Ieder datalek dat een mogelijk risico inhoudt voor de betrokkene wordt binnen 72 uur gemeld bij de AP. De gemeente informeert de betrokkene over de gevolgen en eventuele maatregelen wanneer het datalek een hoog risico is voor de betrokkene. De PO, FG en CISO adviseren de verantwoordelijke afdelingsmanagers en/of betrokken medewerkers over de te treffen maatregelen, het melden van het datalek bij de AP en aan de betrokkenen. De afdelingsmanager is de eindverantwoordelijke voor de uitvoering van de maatregelen, de melding bij de AP en betrokkenen. Alle incidenten met persoonsgegevens worden vastgelegd in een register. Het incidentenregister moet actueel en volledig zijn en wordt aan het einde van ieder jaar verstrekt aan de accountant voor controle.

2.7 Doorgifte buiten de EER

Als de gemeente persoonsgegevens deelt met organisaties uit landen buiten de Europese Economische Ruimte (EER), gebeurt dit volgens de toepasselijke wet- en regelgeving. Dat betekent, via:

- een adequaatheidsbesluit – De Europese Commissie kan bepalen dat een land buiten de EER goede bescherming biedt, zodat de gegevens verstrekt mogen worden.
- passende maatregelen – Als er geen adequaatheidsbesluit is, moeten er extra maatregelen genomen worden, bijvoorbeeld door standaardcontracten die de bescherming regelen.
- of uitzonderingen – In uitzonderlijke gevallen, zoals met toestemming, mogen gegevens ook zonder extra maatregelen worden doorgegeven.

2.8 Geautomatiseerde besluitvorming

De gemeente maakt geen gebruik van profilering. Profilering is een geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd.

De gemeente voert statistisch onderzoek uit voor bijvoorbeeld de verbetering van haar dienstverlening. Deze gegevens worden alleen verzameld voor onderzoek dat door, of namens, de gemeente wordt uitgevoerd. Brongegevens die hiervoor gebruikt worden, worden omgezet tot een dataset die geen persoonsgegevens bevat en dus geanonimiseerd is.

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 degenen 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. De voorwaarden voor de inzet van cameratoezicht in en om het gemeentehuis zijn opgenomen in het Cameraprotocol, dat onderdeel is van het Personeelshandboek.

2.9 Bewustwording

De gemeente scherpert het bewustzijn in de gemeentelijke organisatie voortdurend aan, zodat kennis van risico's wordt verhoogd en (veilig en verantwoord) gedrag om (persoons)gegevens zorgvuldig te verwerken wordt aangemoedigd. Iedere medewerker wordt aantoonbaar geïnformeerd over het zorgvuldig omgaan met (persoons)gegevens, bijvoorbeeld via e-learnings, nano-learnings, cultuurvideo's, een phishingtest, pub-quiz, de publicatie van artikelen en nieuws via de hiervoor ingerichte digitale communicatiekanalen. De gemeente monitort periodiek het effect van haar bewustwordingscampagnes.

3. Borging van het privacybeleid

3.1 PDCA-cyclus

De gemeente hanteert een continue verbeteraanpak om de naleving van privacywetgeving en -beleid te waarborgen. Dit gebeurt door middel van een jaarlijkse PDCA-cyclus (Plan-Do-Check-Act).

Jaarlijkse cyclus

1. Jaarplan Privacy

Elk jaar start met het opstellen van een Jaarplan Privacy door de PO en de FG. In dit plan worden de te nemen verbetermaatregelen vastgesteld op basis van eerdere bevindingen, risicoanalyses en ontwikkelingen in wet- en regelgeving. Het Jaarplan Privacy is onderdeel van het actieplan informatieveiligheid zoals beschreven in paragraaf 1.3 van het Strategisch gemeentebreed informatiebeveiligingsbeleid.

2. Kwartaalrapportages

De FG rapporteert per kwartaal aan het bestuur over de voortgang van het Jaarplan Privacy en andere relevante ontwikkelingen binnen de gemeente.

3. Herijking van prioriteiten

Halverwege het jaar worden de gestelde prioriteiten geëvalueerd en, indien nodig, bijgesteld. Dit zorgt ervoor dat de gemeente wendbaar blijft en adequaat inspeelt op nieuwe risico's en ontwikkelingen.

4. Jaarverslag Privacy

Aan het einde van het jaar stelt de FG een Jaarverslag Privacy op. Hierin wordt gerapporteerd over de naleving van de AVG en Wpg, evenals over de voortgang en resultaten van de uitgevoerde verbetermaatregelen. Dit jaarverslag dient als input voor het nieuwe Jaarplan Privacy en wordt besproken met het bestuur.

3.2 Toepasselijke kaders

Voor het systematisch monitoren en borgen van de AVG-compliance binnen de gemeentelijke organisatie maakt de gemeente gebruik van het AVG Borgingsproduct van de Vereniging van Nederlandse Gemeenten (VNG).

Ten aanzien van de Openbaar Onderwijs Westerwolde wordt gebruikgemaakt van het Normenkader Informatiebeveiliging en Privacy voor het Funderend Onderwijs. Dit normenkader sluit specifiek aan bij de context van het primair onderwijs.

3.3 Audits

Sinds 2021 moet de gemeente op grond van de Wpg iedere vier jaar een externe privacy-audit laten uitvoeren op de naleving van de Wpg en hierover rapporteren aan de AP. Daarnaast moet er ieder jaar een interne audit uitgevoerd worden op de naleving van de Wpg. Dankzij deze audits kan worden vastgesteld of de gemeente bij de verwerkingen onder de Wpg voldoet aan de wettelijke eisen.

De jaarlijkse interne audit, vierjaarlijkse externe audit en eventuele hercontrole maken onderdeel uit van het jaarlijkse integrale auditplan zoals beschreven in paragraaf 1.4 van het Strategisch gemeentebreed informatiebeveiligingsbeleid.

4. Inwerkingtreding, evaluatie en herziening

Dit privacybeleid treedt in werking na vaststelling door het College van Burgemeester en Wethouders. Alvorens het College van Burgemeester en Wethouders overgaat tot vaststelling, wordt het privacybeleid eerst ter instemming voorgelegd aan de Ondernemingsraad en de Medezeggenschapsraad.

De gemeente zal steeds kijken of het beleid nog voldoet of zo nodig aangepast moet worden. Technologische, juridische en maatschappelijke ontwikkelingen op het gebied van privacy volgen elkaar immers snel op. In de regel wordt het privacybeleid in ieder geval elke vier jaar herzien. Indien zich eerder grote wijzigingen voordoen vindt actualisatie eerder plaats.

Bijlage 1. Overzicht noodzakelijke instrumenten en procedures

- Privacyverklaring gemeente Westerwolde
- Privacyverklaring Openbaar Onderwijs Westerwolde
- Procedure actualisatie privacyverklaring
- Procedure voor het afhandelen van verzoeken van betrokkenen
- Register van verwerkingen AVG
- Register van verwerkingen Wpg
- Procedure actualisatie register van verwerkingen
- Pre-DPIA & DPIA procedure
- Procedure afhandelen datalekken
- Werkinstructies Wpg