

## Privacybeleid 2024-2026

Versie november 2023

### 1. Inleiding

De gemeente Altena behandelt mensen met respect. Privacy staat bij ons daarom hoog in het vaandel. Dit privacybeleid dient daarbij als een kapstok. Het doel van dit privacybeleid is om te beschrijven hoe wij aantoonbaar op een juiste wijze omgaan met persoonsgegevens. De Algemene Verordening Gegevensbescherming (hierna: AVG) is daarbij het centrale kader. Dit biedt ons belangrijke houvast voor de wijze waarop wij omgaan met persoonsgegevens. Het beleid is geschreven voor alle inwoners, partners en onze medewerkers. Het beleid heeft betrekking op de (onderdelen van de) gemeente Altena als bestuursorgaan en als werkgever. Dit stuk beschrijft de context van het beleid, de doelen en de uitgangspunten voor ons handelen. Daarmee maken we inhoudelijke keuzes binnen de kaders van de AVG en verwante sector wet- en regelgeving.

Digitalisering en de toepassing van nieuwe technologieën leiden tot veranderingen in de samenleving. Hierdoor verschuiven ook de verwachtingen die inwoners hebben van de gemeentelijke dienstverlening. Denk aan het beheer van de openbare ruimte, het toezicht en de handhaving. Het gebruik van gegevens speelt een belangrijke rol bij het waarmaken van die verwachtingen. Wij hechten veel waarde aan een zorgvuldige verwerking van informatie, zeker als het gaat om persoonsgegevens. Persoonsgegevens dienen goed te worden beschermd door middel van de juiste maatregelen wat betreft Informatieveiligheid. In de Baseline Informatiebeveiliging Overheid (BIO), die van toepassing is op de gemeente Altena, zijn normen bepaald voor informatieveiligheid. Deze zijn nader uitgewerkt in informatiebeveiligingsbeleid.

In dit privacybeleid wordt beschreven hoe de gemeente invulling geeft aan de centrale privacy uitgangspunten en de verplichtingen die de AVG met zich meebrengt. Dit beleid is vervolgens in de organisatie nader uitgewerkt in operationeel beleid en werkinstructies voor een juiste implementatie. In dit stuk wordt geschreven over de gemeente, ons of wij. Dit refereert altijd aan de gemeente Altena.

Dit beleid geldt tot en met 2026, en wordt elke drie jaar geëvalueerd. Dit kan ook eerder zijn, als dit nodig is.

#### 1.1 Ambities

De afgelopen jaren heeft de gemeente Altena hard gewerkt om te voldoen aan de privacy wet- en regelgeving. Hierbij zijn externe experts ingehuurd en is intern meer budget vrijgekomen voor dit thema. Zo is aan de hand van het CIP-model, nader omschreven in hoofdstuk 5, gekeken naar het privacy volwassenheidsniveau binnen de gemeente. Begin 2021 was het volwassenheidsniveau overwegend niveau 2, maar nog niet organisatie breed.

Onze doelstelling is om te groeien naar een privacy volwassenheidsniveau 3 op alle privacy thema's in 2027 in de gehele organisatie. Op het moment dat deze ambitie is bereikt, zal de gemeente haar ambitie verhogen naar niveau 4. Dit privacybeleid vormt de basis voor de gemeente Altena om deze ambitie waar te maken. Aan de hand van dit beleid zal er een privacy compliance risicobeheersingsraamwerk opgezet worden. Op deze manier kan doorlopend worden bijgehouden waar de gemeente staat.

#### 1.2 Scope van dit beleid

Het privacybeleid omvat de gehele datastroom van persoonsgegevens binnen de gemeente. Van het genereren of verzamelen van persoonsgegevens, het dagelijks gebruik ervan en de gegevensopslag tot en met de archivering en vernietiging van persoonsgegevens. Dit privacybeleid is bindend voor de gehele organisatie (inclusief de bestuursorganen) van de gemeente Altena.

Dit beleid wordt nader uitgewerkt in operationeel beleid, werkinstructies en richtlijnen. Deze uitwerkingen worden vastgesteld door het directieteam van de gemeente. Wanneer sprake is van Verwerkers of samenwerking gelden dezelfde uitgangspunten. Diezelfde uitgangspunten vormen het kader bij de selectie van leveranciers c.q. verwerkers. Hiervoor maken wij contractuele afspraken die we ook kunnen toetsen bij de uitvoering van de werkzaamheden. Het beleid is ook van toepassing in geval van uitwisseling van informatie met andere gemeenten en organisaties bij de uitbesteding van publieke taken aan externe partijen.

Het beleid strekt zich ook uit over de verwerkingen van persoonsgegevens op grond van de wet Basisregistratie Personen (BRP) en op de verwerkingen waarop de Archiefwet van toepassing is. Uiteraard voor zover deze specifieke wet- en regelgeving geen afwijkende eisen stellen.

### **1.3 Definities**

In het privacybeleid worden de volgende definities gehanteerd:

#### ***Algemene Verordening Gegevensbescherming (AVG)***

Algemene Verordening Gegevensbescherming (EU 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens).

#### ***Betrokkene(n)***

De persoon op wie de persoonsgegevens betrekking hebben. De betrokkene is degene van wie de persoonsgegevens worden verwerkt. Dit kan gaan om een inwoner, ondernemer, ambtenaar of contactpersoon van een (keten)partner.

#### ***Datalek***

Een datalek is persoonlijke informatie (zoals namen, adressen of financiële gegevens) die per ongeluk of opzettelijk wordt blootgesteld aan onbevoegden, wat de privacy en veiligheid van mensen in gevaar brengt.

#### ***Data Protection Impact Assessment (DPIA)***

In het Nederlands vertaald naar gegevensbeschermingseffectbeoordeling, maar de gangbare term is DPIA. Dit is een instrument om vooraf de privacy risico's van een gegevensverwerking in kaart te brengen en vervolgens maatregelen te kunnen nemen om de risico's te verkleinen. Een DPIA is een beoordeling over het effect van de (nieuwe of aangepaste) verwerking op de bescherming van de persoonsgegevens en is verplicht als een gegevensverwerking waarschijnlijk een hoog privacy risico oplevert voor de betrokkenen. De beoordeling bevat tenminste een inschatting van de risico's van de verwerking en de vereiste beheersmaatregelen om tekortkomingen op te lossen.

#### ***DPIA-Toets***

Een model om te beoordelen of een DPIA verplicht is of niet.

#### ***Functionaris Gegevensbescherming (FG)***

Een onafhankelijke en deskundige interne toezichthouder en adviseur met wettelijke taken en bevoegdheden. De FG houdt binnen de organisatie toezicht op de toepassing en naleving van alle privacy wet- en regelgeving waaronder de Algemene Verordening Gegevensbescherming (AVG).

#### ***Privacy Team***

Binnen de gemeente zijn meerdere rollen belegd met controle en aanpassing van het privacybeleid. Onder het Privacy Team wordt onder meer verstaan de Privacy Officer(s), CISO en de FG.

#### ***Persoonsgegevens***

Informatie uit data die direct of indirect betrekking heeft op een levend persoon.

Denk hierbij aan naam, adres, geboortedatum. Naast deze gewone persoonsgegevens kent de wet ook bijzondere persoonsgegevens. Deze gegevens gaan over gevoelige onderwerpen, zoals etnische achtergrond, politieke voorkeur of gezondheid.

#### ***Verwerker***

De organisatie, of persoon, die in opdracht en ten behoeve van de verwerkingsverantwoordelijke bepaalde onderdelen van of de gehele verwerking voor zijn rekening neemt.

#### ***Verwerkersovereenkomst***

Een overeenkomst waarin de afspraken staan hoe een verwerker met de persoonsgegevens moet omgaan bij verwerkingen in opdracht en ten behoeve van de verwerkingsverantwoordelijke.

#### ***Verwerking***

Alles wat je met persoonsgegevens kan doen; "het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, doorzenden, verspreiden, beschikbaar stellen, samenbrengen, met elkaar in verband brengen, afschermen, wissen en vernietigen van gegevens."

#### ***Verwerkingsverantwoordelijke***

De organisatie, of persoon, die bepaalt waarom de verwerking van persoonsgegevens plaatsvindt en vaststelt met welke middelen dat gebeurt.

## 2. Belangenafweging

Bij verwerking van persoonsgegevens zijn vaak diverse belangen gemoeid. Dat vraagt om een zorgvuldige afweging. Naast het belang van de individuele inwoner, is er het publieke (algemeen) belang en zijn er belangen van inwoners ten opzichte van elkaar.

- **Belang van de inwoner:** een inwoner wil dat zijn persoonsgegevens veilig en betrouwbaar worden verwerkt. Daarnaast moeten wij transparant zijn over wat wij met die informatie doen. De wensen kunnen wel van verschillend karakter zijn. Aan de ene kant heeft de inwoner er belang bij dat zo min mogelijk gegevens worden opgeslagen en niet langer worden bewaard dan noodzakelijk. Aan de andere kant verwacht de inwoner efficiënte dienstverlening, waarbij wij niet naar de bekende weg vragen.
- **Publiek belang:** wij voeren op diverse gebieden wettelijke- en bestuurlijke taken uit. Denk hierbij aan onder andere in het sociaal domein, openbare orde en veiligheid of burgerzaken. Om deze taken goed te volbrengen is het noodzakelijk dat er persoonsgegevens worden verwerkt.
- **Belangen van inwoners ten opzichte van elkaar:** de bescherming van de rechten van de ene inwoner kan ingrijpende gevolgen hebben voor de belangen en de rechten van de ander.

Voordat persoonsgegevens worden verwerkt vindt er een belangenafweging plaats. Daarbij worden de privacy uitgangspunten als beschreven in hoofdstuk 3 meegewogen. De gemeente maakt een analyse, zodat de risico's van de verwerking vooraf inzichtelijk zijn. Na een onderbouwde belangenafweging wordt besloten of de gegevensverwerking kan plaatsvinden. Daarbij worden risico's zoveel mogelijk verkleind met de juiste maatregelen. Dit wordt nader uitgewerkt in paragraaf 4.2.

## 3. Privacy uitgangspunten

De AVG omschrijft een aantal uitgangspunten die centraal staan in dit beleid. De gemeente Altena hanteert hierbij de centrale uitgangspunten van *Rechtmatigheid*, *Behoorlijkheid* en *Transparantie* om invulling te geven aan alle uitgangspunten die de AVG stelt. Hieronder worden deze uitgangspunten omschreven en de wijze waarop wij deze concreet invulling geven binnen onze organisatie.

### 3.1 Rechtmatigheid

Wij gaan uit van de geldende wet- en regelgeving voor gegevensverwerking en hanteren de AVG als basis. Voor verwerking van persoonsgegevens moet er altijd een wettelijke grondslag bestaan.

Het kan zijn dat wij persoonsgegevens vaker moeten gebruiken. Dit kan alleen als dat doel verenigbaar is met de oorspronkelijke verzameldoelstellingen. Mocht blijken dat het niet verenigbaar is dan zal worden gekeken naar een rechtmatige grondslag. Dit wordt getoetst bij ons Privacy Team.

Wij leggen alleen persoonsgegevens vast als dit noodzakelijk is voor het specifieke doel van de verwerking. Het kan zijn dat de wet dit ons verplicht of dat het nodig is om de belangen van betrokkenen te beschermen. Dit wordt voor de verwerking concreet gemaakt en vastgelegd in het verwerkingsregister.

Diverse gemeentelijke taken vereisen het gebruik van persoonsgegevens. In deze gevallen is het doel in de wet vastgelegd. Tevens wordt in het verwerkingsregister per verwerking bijgehouden op welke grondslag en met welk doel dit gerechtvaardigd is.

Bij de gegevensverwerking wordt rekening gehouden met de beginselen van proportionaliteit en subsidiariteit. Wij vragen slechts die informatie die noodzakelijk is om het beoogde doel te bereiken. Daarbij gebruiken wij altijd de minst ingrijpende methode voor de betrokkenen.

### 3.2 Behoorlijkheid

Wij hanteren het principe van minimale gegevensverwerking. Dit wil zeggen dat er geen gegevens worden gevraagd die niet nodig zijn voor het vastgestelde doel. Hiermee geven wij invulling aan het principe van dataminimalisatie. Zo richten wij onze systemen op een wijze in zodat niet te veel informatie wordt gevraagd. Denk aan online formulieren die geen overbodige invulvakjes hanteren. Verder zijn er werkinstructies en periodieke data-“opschoonacties” om het dataminimalisatie principe te waarborgen.

Wij hanteren het beginsel van éénmalige vastlegging, meervoudig gebruik: gegevens die bekend zijn, worden niet nodeloos opnieuw gevraagd. Dit betekent ook zo veel mogelijk gebruik maken van zogenoemde brongegevens, zoals die zijn opgenomen in het stelsel van basisregistraties. Dit is slechts mogelijk als hier een wettelijke grondslag en een verenigbaar doel voor is. De grondslag en verenigbaarheid wordt niet op werknemer-niveau bepaald. Dit wordt op teamniveau vastgelegd middels werkinstructies en autorisaties om heldere kaders te schetsen voor onze medewerkers.

Persoonsgegevens worden niet langer bewaard dan noodzakelijk is. De noodzakelijkheid is voor ons altijd gerelateerd aan het doeleinde waarvoor de betreffende persoonsgegevens zijn verzameld. Vaak is dit op basis van wettelijke bewaartermijnen. Wanneer de wet hier niet in voorziet staan de bewaartermijnen beschreven in ons verwerkingsregister. De gemeente Altena bewaart persoonsgegevens in ieder geval in overeenstemming met de "Selectielijst gemeenten en intergemeentelijke organen 2020". De interne organisatie heeft toegang tot het verwerkingsregister om de bewaartermijnen te raadplegen. Verder zijn er werkinstructies voor het gebruik van dit register.

Alleen functionarissen (ambtenaren, externen, leveranciers, convenantpartners) waarvoor het voor de directe taakuitoefening noodzakelijk is, hebben inzage in persoonsgegevens. Deze gegevens worden vertrouwelijk behandeld. Verder hebben wij een autorisatiebeleid zodat slechts medewerkers toegang hebben tot de gegevens die hier ook echt een doel voor hebben.

Er wordt gewerkt met geheimhoudingsverklaringen voor externen en leveranciers. Met externe (keten)partners worden overeenkomsten (convenanten) afgesloten.

Persoonsgegevens worden goed beveiligd opgeslagen zodat ze adequaat zijn beschermd tegen misbruik, verlies, onbevoegde toegang en bewerking. Door gebruik te maken van privacy by design wordt al tijdens de ontwikkeling van producten en diensten (zoals informatiesystemen) aandacht aan privacy verhogende maatregelen geschonken.

Het is voor zowel ons als de inwoners van belang dat persoonsgegevens actueel en correct zijn. Er worden diverse projecten en processen periodiek uitgevoerd om de basisregistratie personen actueel en juist te houden. Dit is tevens een wettelijke verantwoordelijkheid.

### **3.3 Transparantie**

Iedereen heeft het recht om te vragen welke persoonsgegevens de gemeente Altena over hem/haar heeft verzameld en waarvoor deze worden gebruikt. Dit gebeurt onder meer door onze privacyverklaring op de website. Verder wordt per team bekeken hoe betrokkenen op een passende wijze worden geïnformeerd. Dit is vastgelegd in werkinstructies om te voldoen aan de informatieplicht onder de AVG.

Inwoners hebben de mogelijkheid om te vragen waarom en welke persoonsgegevens wij van hen verwerken. In de basis verstrekken wij de gevraagde informatie tenzij de wet anders aangeeft. Verder kunnen inwoners om verbetering, aanvulling of verwijdering van persoonsgegevens verzoeken. Dit verzoek wordt gehonoreerd, tenzij ook hier weer de wet anders heeft bepaald.

Om recht te doen aan verzoeken van betrokkenen hebben wij een Procedure rechten van betrokkenen vastgesteld. Hierin is beschreven op welke wijze verzoeken van betrokkenen door ons worden afgehandeld. Hier wordt ook omschreven wie daarbij welke taken en verantwoordelijkheden heeft. In nadere interne beleidsstukken is uitgewerkt hoe betrokkenen tijdig geïnformeerd worden over deze procedure.

Wij zijn transparant over het type persoonsgegevens dat wij voor een specifiek doel met derden delen. Daarbij kan het zijn dat er een uitzondering is wanneer er belangen zijn, genoemd in wet- of regelgeving, die zich daartegen verzetten. Type persoonsgegevens worden bijgehouden in het verwerkingsregister en zijn opvraagbaar.

Wij zijn open en transparant over hoe wij met persoonsgegevens omgaan. Door de waarborg dat afwijkingen van dit beleidskader beargumenteerd worden voorgelegd aan het Privacy Team. Indien nodig zal de interne toezichthouder (de FG) escaleren naar het college en/of de burgemeester. Zo wordt maximaal invulling gegeven aan transparantie richting inwoners en de raad.

## **4. Algemene Verordening Gegevensbescherming**

De AVG legt diverse verplichtingen op aan gemeenten. Hieronder worden deze verplichtingen omschreven inclusief de feitelijke uitwerking daarvan binnen onze organisatie. Dit geeft tevens weer hoe wij verdere invulling geven aan de privacy uitgangspunten als omschreven in het vorige hoofdstuk.

### **4.1 Het verwerkingsregister**

Binnen de gemeente werken wij met veel processen en dus ook diverse verwerkingen van persoonsgegevens. Middels een verwerkingsregister wordt precies bijgehouden waar welke verwerkingen plaats vinden. In dit register staat de volgende informatie vermeld:

- De naam en contactgegevens van de vertegenwoordiger namens de gemeente Altena, de FG en eventuele andere organisaties waarmee de gemeente Altena gezamenlijk verwerkingsverantwoordelijke is;

- De doelen en grondslagen van de verwerkingen;
- Een beschrijving van de categorieën van betrokkenen en de categorieën persoonsgegevens;
- Een beschrijving van de ontvangers van de persoonsgegevens;
- Indien van toepassing, een beschrijving van het delen van persoonsgegevens aan derde landen;
- De bewaartermijnen;
- Een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

Het Privacy Team beheert het verwerkingsregister. Proceseigenaren binnen de teams zijn verantwoordelijk voor het opnemen van nieuwe verwerkingen in het verwerkingsregister, maar ook voor het controleren van bestaande verwerkingen. Het register wordt jaarlijks generiek gecontroleerd en geactualiseerd. Zij worden hierbij geadviseerd door de Privacy Officer(s). De FG controleert of het register volledig en up-to-date is. Middels een memo worden de rollen en verantwoordelijkheden ten aanzien van het beheer van het register van verwerkingsactiviteiten vastgelegd.

#### 4.2 Data Protection Impact Assessment (DPIA)

De gemeente staat niet stil en wij zijn altijd in ontwikkeling. Zo worden processen en systemen periodiek aangepast. Daardoor kan er sprake zijn van een nieuwe verwerking of wijziging van een bestaande verwerking. Om de privacy risico's in kaart te brengen voor een juiste belangenafweging voeren wij vooraf een DPIA-Toets uit. De uitvoering van de DPIA-Toets valt onder de verantwoordelijkheid van de teammanager. Deze kan een DPIA-verantwoordelijke binnen het proces aanwijzen. Aan de hand van de uitgevoerde DPIA-Toets worden voor zowel informatiebeveiliging als privacy, een risico-inventarisatie uitgevoerd.

Op basis van de uitgevoerde DPIA-Toets wordt bepaald of voor een afzonderlijke verwerking een hoog risico bestaat. Is dit niet het geval, dan kan een privacy advies van het Privacy Team volstaan. Wanneer een verwerking wel een hoog privacy risico voor betrokkenen met zich meebrengt wordt er eerst een DPIA uitgevoerd. Een DPIA geeft inzicht in welke maatregelen getroffen moeten worden om het risico te verkleinen naar een minimaal en acceptabel niveau. Hiermee wordt invulling gegeven aan een juiste belangenafweging.

De gemeente Altena hanteert hiervoor een standaard DPIA-model. Proceseigenaren zijn verantwoordelijk voor de uitvoering van een DPIA voor een verwerking met een hoog privacy risico. De gemeente hanteert hierbij een handreiking ter verduidelijking voor de DPIA verantwoordelijke. Het Privacy Team ondersteunt en adviseert bij de uitvoering hiervan. De FG geeft advies over de uitgevoerde DPIA.

Het DPIA-proces wordt nader uitgewerkt in een procedure, zodat het voor alle betrokkenen duidelijk is hoe een DPIA moet worden doorlopen.

Het Privacy Team houdt een register bij van uitgevoerde DPIA's en monitort de voortgang van het DPIA-proces. Er wordt gekeken naar de geïmplementeerde beheersmaatregelen en gerapporteerd aan de FG.

Processen kunnen regelmatig worden aangepast met mogelijke effecten op de verwerking. Als er een wijziging in het proces wordt doorgevoerd is het noodzakelijk om een eerder uitgevoerde DPIA te herzien en te kijken of de wijziging ook nieuwe risico's met zich meebrengt. Kleine risico's kunnen groter worden, maar grote risico's kunnen ook kleiner worden. Dit wordt meegenomen bij een herijking van een DPIA.

#### 4.3 Privacy by Design & Privacy by Default

De gemeente hanteert de principes van *Gegevensbescherming door ontwerp* en *Gegevensbescherming door standaardinstellingen* op haar verwerkingen.

*Gegevensbescherming door ontwerp*: houdt in dat er bij het ontwerpen van producten en diensten voor wordt gezorgd dat persoonsgegevens goed worden beschermd. Bij de inrichting van het proces en/of bouw van het systeem wordt bijvoorbeeld gekeken naar de benodigde technische en organisatorische maatregelen. Privacy wordt aan het begin voor de uitvoer van projecten meegenomen. Dit wordt gewaarborgd door een Privacy Officer mee te laten kijken in de voorfase van een project. De FG ziet er op toe dat dit ook gebeurt.

*Gegevensbescherming door standaardinstellingen*: houdt in dat de standaardinstellingen van een programma ingesteld dienen te worden op de meest privacy vriendelijke manier. Zoals beschreven in paragraaf 4.2 geldt voor de gemeente Altena dat voor een nieuwe verwerking of een wijziging in een bestaande verwerking een DPIA-Toets uitgevoerd dient te worden. Door deze toets wordt aan de voorkant helder of een uitgebreidere DPIA noodzakelijk is. Bij het uitvoeren van een DPIA worden de voor *Gegevensbescherming door ontwerp* en *Gegevensbescherming door standaardinstellingen* noodzakelijke aspecten (bijvoorbeeld dataminimalisatie en bewaartermijnen) meegenomen in de

voorgenomen verwerking. Zo worden in formulieren geen gegevens gevraagd die overbodig zijn. Dit helpt tevens mee aan het principe van dataminimalisatie. Op deze manier wordt geborgd dat nieuwe verwerkingen conform de normen van *Gegevensbescherming door ontwerp* en *Gegevensbescherming door standaardinstellingen* worden ingericht.

Kortom betekent dit dat de procesverantwoordelijke privacy in zijn processen en applicaties betreft, en altijd de meest privacyvriendelijke optie kiest als dat mogelijk is.

#### 4.4 Datalekken

Een datalek heeft potentieel een grote impact op betrokkenen en ons als organisatie. Er worden daarom meerdere processen, systemen en acties ingezet om datalekken te voorkomen. Volledig uitsluiten is onmogelijk, maar wij zetten ons in om een cultuur te creëren waarin het snel melden van mogelijke datalekken wordt gestimuleerd. Het kan namelijk zo zijn dat een datalek gemeld moet worden bij de Autoriteit Persoonsgegevens (hierna: AP) en/of betrokkenen binnen 72 uur. Indien wij niet of niet tijdig melden lopen wij een risico op een boete van de AP. Deze kan oplopen tot een maximum van 20 miljoen euro of 4% van een jaaromzet. Los van een morele verplichting is er dus ook een financieel risico wanneer niet wordt voldaan aan de meldplicht.

Om te voldoen aan bovengenoemde verplichtingen is er een *procedure datalekken* opgesteld. Hier staat beschreven op welke wijze datalekken worden afgehandeld en wie daarbij welke taken en verantwoordelijkheden heeft. In deze procedure staat ook beschreven hoe en wanneer een datalek dient te worden gemeld bij de AP en/of betrokkenen. Daarnaast ontvangen onze medewerkers meerdere malen per jaar informatie over dit thema om de bewustwording op peil te houden. Tevens staat de gemeente Altena voor een open en veilige cultuur zodat medewerkers zich veilig voelen om datalekken te melden. Dit wordt bevorderd door de bestuurders. Tot slot staan op het interne portaal van de gemeente Altena diverse aanvullende bronnen ten aanzien van het melden van datalekken.

Om te blijven anticiperen op mogelijke risico's wordt er een intern datalekregister bijgehouden waarin alle geconstateerde beveiligingsincidenten worden geregistreerd. Hierin wordt vastgelegd of het beveiligingsincident heeft geleid tot een datalek en indien dat het geval is, het datalek ook is gemeld bij de toezichthouder en/of de betrokkenen. Jaarlijks wordt het datalekregister geëvalueerd om trends bij te houden en structurele verbeteringen intern door te voeren. Tevens worden gevoelige datalekken direct geëvalueerd om zo dringende aanpassingen gelijk door te voeren in de organisatie.

#### 4.5 Functionaris Gegevensbescherming (FG)

De gemeente Altena is een overheidsinstantie die structureel en op grote schaal persoonsgegevens verwerkt, waaronder bijzondere persoonsgegevens. Het is in dit geval een wettelijke verplichting een FG aan te stellen.

De FG is als interne toezichthouder betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. De gemeente heeft er voor gekozen om de rol van FG intern te beleggen. Samen met de Privacy Officer(s) vormt hij het Privacy Team.

De FG is een onafhankelijke toezichthouder die gevraagd en ongevraagd advies geeft op het gebied van de AVG. De FG voert jaarlijks een interne audit uit en maakt daarbij een FG-toezichtplan. De FG rapporteert jaarlijks over de naleving van privacy wet- en regelgeving aan het college van B&W. De FG heeft onder meer de volgende wettelijke taken:

- Informatievoorziening;
- Toezicht op de implementatie van de privacy wet- en regelgeving;
- Contactpersoon voor de Autoriteit Persoonsgegevens;
- Periodieke verslaglegging aan college van B&W over de uitvoering van zijn taken;
- Het zorg dragen voor een juiste afwikkeling van de vragen of klachten van Betrokkenen;
- Adviseren en beoordelen van uitgevoerde DPIA's.

#### 4.6 Beveiliging

Op grond van de AVG dienen organisaties passende technische en organisatorische maatregelen te nemen om de persoonsgegevens die zij verwerkt, te beveiligen. De gemeente Altena heeft een Strategisch en Tactisch Informatiebeveiligingsbeleid opgesteld waarin is beschreven op welke wijze invulling is gegeven aan de passende beveiliging van persoonsgegevens. Tevens is er een CISO aangesteld, conform het functieprofiel van de IBD. De CISO staat voor Chief Information Security Officer, die verantwoordelijk is voor informatiebeveiliging(sbeleid). Voor meer informatie daarover wordt verwezen naar het Informatiebeveiligingsbeleid.

#### 4.7 Gegevens delen met derden

Wanneer er sprake is van structurele of gevoelige gegevensuitwisseling met derde partijen, worden er afspraken gemaakt over de gegevensuitwisseling. Deze afspraken voldoen tenminste aan de AVG en worden vastgelegd in een onderlinge regeling, samenwerkingsovereenkomst (convenant), een gegevensuitwisselingsovereenkomst of een verwerkersovereenkomst. De gemeente Altena sluit zich aan bij de sjablonen van de VNG.

Er is een model verwerkersovereenkomst aanwezig dat inhoudelijk voldoet aan de eisen die de AVG daaraan stelt. Verwerkers worden bijgehouden in het verwerkingsregister van de gemeente Altena. De ondertekende versies van de verwerkersovereenkomsten behoren bij de proceseigenaren te zijn gearchiveerd. De gemeente Altena gebruikt zoveel mogelijk landelijke standaarden en richtlijnen om de contractuele verplichtingen te regelen met derden. Dit is uitgewerkt in werkinstructies en gewaarborgd in het inkooptraject.

Met betrekking tot doorgifte hanteert de gemeente het uitgangspunt dat persoonsgegevens niet worden doorgegeven aan een bedrijf of vestiging in een land buiten de Europese Economische Ruimte (EER), tenzij deze doorgifte aantoonbaar rechtmatig is, en strikt noodzakelijk. Rechtmatigheid wordt aangetoond in een van de volgende vier gevallen:

- Een adequaatheidsbesluit;
- Passende waarborgen middels een modelcontract (Standard Contractual Clauses);
- Binding corporate rules (BCR);
- Specifieke uitzonderingen.

#### 5. Risico's

Het privacy control framework van de gemeente Altena is vormgegeven door de Privacy baseline en het Privacy volwassenheidsmodel van het Centrum Informatiebeveiliging en Privacybescherming (CIP). Dit dient als het beoordelingskader voor het waarborgen van privacy compliance binnen de gemeente. De Privacy baseline en het Privacy volwassenheidsmodel van het CIP geven invulling aan het normenkader voor het duiden van privacy risico's en de daarbij behorende beheersmaatregelen binnen de gemeente Altena. Hierbij houden wij nauwlettend nieuwe methodieken en modellen in de gaten wanneer deze specifiek zijn opgesteld voor gemeenten, zoals het borgingsproduct van de VNG. In de basis zal de essentie gelijk blijven, maar kan de vorm en benaming tussentijds wijzigen mits dit geen wezenlijke impact heeft op de praktijk.

Op basis van de Privacy baseline en het Privacy volwassenheidsmodel zal de gemeente Altena kerncontrolepunten en bijbehorende werkprogramma's vaststellen.

Bij het niet voldoen aan de relevante wet- en regelgeving is het College van B&W wettelijk aansprakelijk. Niet voldoen kan leiden tot:

- Klachten van betrokkenen;
- Verlies van vertrouwen in de (lokale) overheid;
- Imago schade voor de gemeentelijke organisatie;
- Datalekken;
- Schadevergoedingen;
- Onderzoeken, dwangmaatregelen en (hoge) bestuurlijke boetes.

De risico's van schending van de privacy voor betrokken personen variëren van ongemak, substantiële benadeling, ernstige sociale beschadiging of gevaren voor de gezondheid en de persoonlijke veiligheid. Dit beleid in combinatie met het informatiebeveiligingsbeleid en de stukken waarnaar wordt verwezen, hebben als doel deze risico's te verkleinen.

#### 6. Taken & verantwoordelijken

Het College is verantwoordelijk voor het naleven van de uitgangspunten uit de privacy wet- en regelgeving en de kaders voor het verantwoord omgaan met persoonsgegevens. Dit is gelijk aan de 10 informatiebeveiligingsprincipes. De gemeente heeft de verantwoordingsplicht om te kunnen aantonen dat deze uitgangspunten en kaders worden nageleefd. Elke medewerker binnen onze organisatie is in diverse mate verantwoordelijk voor de juiste naleving en implementatie van dit privacybeleid. Wij hanteren hiervoor het zogeheten 'Three Lines of Defense' model. Hieronder wordt dit principe kort toegelicht. De concrete interne taakverdeling om dit te borgen is vastgelegd in interne instructies.

De teammanagers dragen de eerstelijnsverantwoordelijkheid. Zij zijn daarmee een onmisbare en noodzakelijke schakel om namens het College (als interne eindverantwoordelijke), te voldoen aan pri-

vacy wet- en regelgeving. Deze interne verantwoordelijkheid dragen teammanagers voor de verwerkingsprocessen die binnen hun teams plaatsvinden. Deze interne verantwoordelijkheid heeft vooral betrekking op de uitvoering van de verplichtingen uit o.a. de AVG en sectorale wetgeving die op het team van toepassing is. Elk team zal een privacyambassadeur aanwijzen. Deze ambtenaar zal fungeren als het eerste aanspreekpunt als het gaat om privacyvraagstukken. Bij complexe vraagstukken of escalatie zal het Privacy Team worden ingeschakeld.

Wij hebben een team van privacy professionals dat het College ondersteunt in de beleidsuitvoering van privacy. Dit team wordt het Privacy Team genoemd. Zij zorgen dat er centraal inzicht is in de naleving van privacy wet- en regelgeving binnen alle organisatieonderdelen en bestuursorganen van de gemeente. Daarnaast draagt het Privacy Team door middel van advisering en monitoring een tweedelijnsverantwoordelijkheid voor de naleving van de privacy wet- en regelgeving binnen de gemeente. Op deze wijze draagt het Privacy Team actief bij aan de door het College geambieerde privacy volwassenheidsniveau.

Ten slotte is er de FG die controleert of het samenspel tussen de eerste en tweede lijn soepel functioneert. Daarover velt hij een objectief en onafhankelijk oordeel met mogelijkheden tot verbetering. De FG speelt een rol in alle lijnen, maar met de voornaamste focus op de derde lijn. Belangrijk punt daarbij is dat de FG zowel een rol speelt in de advisering als in de controle. Wanneer er een mogelijk conflict tussen advies- en controlebevoegdheid betreft, doet de FG een stap terug. De FG draagt geen verantwoordelijkheid voor o.a. het beleid, DPIA's of instructies. Dit ligt bij de verwerkingsverantwoordelijke.

## 7. Bewustwording

Een hoge mate van bewustwording bij alle medewerkers is van essentieel belang om dit privacybeleid goed uit te voeren. Wij verwachten dat elke medewerker een adequaat niveau van bewustwording heeft als het gaat om privacy en informatiebeveiliging. Er zijn diverse (online) middelen om de bewustwording van medewerkers te vergroten. Zo is gewaarborgd dat medewerkers weten wanneer er sprake is van (bijzondere) persoonsgegevens en gewone gegevens. Hier wordt aandacht aan besteed in o.a. een digitale leeromgeving en via berichtgeving op interne portalen. Het volgen van het programma via de digitale leeromgeving is verplicht. Zo komen periodiek onder meer de volgende thema's aan bod:

- Herkennen en melden van een datalek;
- Het kwalificeren van persoonsgegevens en overige informatie;
- Het informeren van de betrokkenen;
- Het uitvoeren van een DPIA;

In het kader van bewustwording is de teammanager verantwoordelijk voor informerende en voorlichtende activiteiten op het gebied van privacy binnen zijn/haar team. Hierbij is in ieder geval de meldplicht datalekken een terugkerend onderwerp is. Verder worden nieuwe medewerkers gemotiveerd om binnen 3 maanden na indiensttreding een digitale training te volgen. Zo wordt de bewustwording gelijk tot het minimale vereiste niveau gebracht. Het Privacy Team in combinatie met de afdeling communicatie stellen ieder jaar een jaarplanning op om de bewustwording organisatie breed op peil te houden.

## 8. Uitwerking en evaluatie

De uitwerking van dit privacybeleid verloopt volgens de PDCA-methodiek (Plan-Do-Check-Act). Dit betekent dat het beleid is vastgesteld volgens een cyclisch proces. De Privacy Officer heeft dit jaar het privacy beleid opnieuw opgesteld. Hierbij zijn uitgebreide voorbereidingen getroffen en is gekeken naar de huidige bedrijfsvoering van de gemeente. Hierbij is ook gekeken naar het informatiebeveiligingsbeleid. Dit privacybeleid is vervolgens voorgelegd bij de FG en de verantwoordelijke teammanager voor advies alvorens het is vastgesteld door het College. Dit is vervolgens door de gehele organisatie gecommuniceerd via diverse kanalen.

Dit privacybeleid wordt door het Privacy Team uitgewerkt in specifiek uitvoeringsbeleid, nadere richtlijnen en/of werkinstructies. Het Privacy Team werkt hiervoor nauw samen met de andere afdelingen van de gemeente. Eens in de drie jaar, of eerder indien daar aanleiding toe is, wordt dit privacybeleid geëvalueerd en aangepast. Dit beleid heeft geen verlooptdatum.

Specifiek uitvoeringsbeleid, richtlijnen en werkinstructies worden jaarlijks door het verantwoordelijke lijnmanagement geëvalueerd. Hierover dient door het lijnmanagement te worden gerapporteerd aan het Privacy Team. Al deze stukken maken integraal deel uit van het beleid, waardoor het beleid een geïntegreerde structuur krijgt. Alle stukken samen vormen het privacyhandboek.

In 2026 zal dit proces wederom worden herhaald, mocht eerdere herziening niet noodzakelijk zijn. Hierbij zal wederom dit cyclisch proces worden toegepast.



## **Inwerkingtreding**

Het privacybeleid treedt in werking per 1 januari 2024.

*Het college van burgemeester en wethouders,*

*de interim secretaris,  
drs. R.J.M. van Wuijtswinkel MPA*

*de burgemeester,  
drs. E.B.A. Lichtenberg MCM*