Gemeente Albrandswaard

GEMEENTEBLAD

Officiële uitgave van de gemeente Albrandswaard

Nr. 10232

12 januari 2026

Privacybeleid gemeente Albrandswaard 2025 - 2027

het college van burgemeester en wethouders van de gemeente Albrandswaard

Overwegende dat;

Ons college kaders heeft vastgesteld voor de privacy-borging van persoonsgegevens die door of namens de gemeente worden verwerkt bij de uitvoering van haar (wettelijke) taken;

Gelet op artikel 24, lid 2 Algemene verordening gegevensbescherming en artikel 160, lid 1 sub a en c Gemeentewet;

B E S L U I T vast te stellen

Privacybeleid gemeente Albrandswaard 2025 - 2027

Doel
Dit Strategisch Privacybeleid geeft richting aan de manier waarop binnen Gemeente Albrandswaard wordt gezorgd voor een adequate, zorgvuldige en rechtmatige omgang met persoonsgegevens van zowel burgers, inwoners en medewerkers (hierna: betrokkenen) en de borging daarvan. Dit privacybeleid beschrijft op hoofdlijnen (de 'wat) waar we binnen de Gemeente Albrandswaard de aankomende tijd de nadruk op leggen, mede richting gegeven door maatschappelijke ontwikkelingen en wet- en regelgeving. De daadwerkelijke uitvoering (de 'hoe') valt buiten de scope van dit beleid en zal in samenwerking met De BedrijfsvoeringsPartner (hierna DBP) worden vastgelegd in een uitvoeringsplan en in procedures en werkinstructies beschreven worden.

Doelgroep
In dit beleid wordt onder "medewerker" verstaan eenieder die namens een bestuursorgaan van de gemeente Albrandswaard op grond van een mandaat, machtiging of een geattribueerde bevoegdheid gegevens verwerkt ter uitvoering van de (wettelijke) taken van de gemeente.
Hieronder wordt in ieder geval begrepen:
- een ieder die op grond van een arbeids-, inhuur-, uitzendkracht-, detacheringsovereenkomst onder gezag staat van het college of het Bestuur van DBP (DBP);
- zelfstandigen zonder personeel (ZZP'ers);
- en Boa's, ambtenaren burgerlijke stand, leerplichtambtenaren, toezichthouders, heffings- en invorderingsambtenaren.

Toepasselijke regelgeving
Dit privacybeleid is opgesteld conform:

- de Algemene verordening gegevensbescherming (AVG), die aantoonbaarheid, evaluatie en aanpassing van de maatregelen (Art 24 lid 1) vereist en de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG);
- de Wet Politiegegevens, die nader is uitgewerkt in het Besluit Politiegegevens en het Besluit Politiegegevens Boa's;
- de volgende maatregelen uit de Baseline Informatiebeveiliging Overheid (BIO);
  - Control: 18.1.1; 18.1.3; 18.1.4;
  - Overheidsmaatregel: 18.1.3.1; 18.1.4.1; 18.1.4.2.

- de Archiefwet;
- sectorspecifieke wet- en regelgeving over de verwerking van persoonsgegevens;
- mandaatregelingen voor verlening van mandaat en volmacht aan functionarissen van Gemeente Albrandswaard en DBP.

Bereik
Dit privacybeleid is vastgesteld en van toepassing op alle medewerkers binnen onze gemeente en alle betrokkenen met wie Gemeente Albrandswaard werkt. Dit beleid draagt bij aan transparantie over de manier waarop we als gemeente omgaan met persoonsgegevens.

Dit privacybeleid is van toepassing op de Gemeente Albrandswaard en alle uit te voeren werkprocessen, organisatieonderdelen, objecten, informatiesystemen en gegevens(verwerkingen), inclusief gegevensverwerkingen door Gemeente Albrandswaard in opdracht van derden. Dit vraagt om nauwe samenwerking met DBP.

Dit beleid is opgesteld rekening houdende met privacy in het kader van de Algemene verordening gegevensbescherming (AVG) en andere relevante privacy wet- en regelgeving. De Wet Politiegegevens (Wpg) wordt eveneens behandeld, omdat de Gemeente Albrandswaard ook persoonsgegevens verwerkt die onder de Wpg vallen.

Griffie van gemeenteraad en verwerkingen gemeenteraad

Dit privacybeleid is eveneens van toepassing op de griffie van de gemeenteraad en op de verwerkingen van persoonsgegevens die door dit bestuursorgaan worden uitgevoerd, voor zover het beleid relevant is voor de taken en verantwoordelijkheden van de griffie.

De griffie conformeert zich aan de uitgangspunten en doelstellingen van dit privacybeleid, maar hanteert daarnaast eigen kaders en werkafspraken op het gebied van informatieveiligheid en privacy.

De griffie is zelfstandig verantwoordelijk voor een zorgvuldige omgang met persoonsgegevens binnen haar werkdomein, en draagt zorg voor een tijdige en adequate melding van eventuele datalekken

Verantwoordelijkheid en naleving
Het College van Burgemeester en Wethouders (B&W) van de gemeente Albrandswaard is verantwoordelijk voor de vaststelling van dit privacybeleid en de te stellen kaders.

Voor het bevorderen van de naleving van dit privacybeleid, de algehele communicatie en bewustwording (awareness) rondom privacy dragen zorg:

- ons College;
- het concernmanagement van de gemeente;
- het management van DBP (DBP);
- de proceseigenaren van de gemeente en DBP;
- de (Coördinerend) Privacy Officer(s) van DBP.

Beheer & herziening
Het inhoudelijke beheer van dit document berust bij de Coördinerend Privacy Officer (CPO) van DBP. Het privacybeleid wordt ten minste elke drie jaar herzien, of eerder indien omstandigheden en wet- en regelgeving daartoe vragen.

1: Inleiding

Gemeente Albrandswaard heeft een duidelijke visie gericht op een duurzame en aantrekkelijke leefomgeving, voor haar inwoners en ondernemers. Ze wil een plek bieden waar wonen, werken, recreëren en natuur hand in hand gaan, met oog voor toekomstige generaties. De kernwaarden nabijheid, eigenaarschap, opgavegerichtheid en betrouwbaarheid staan centraal. Daarbij hecht de gemeente veel waarde aan de actieve betrokkenheid van inwoners bij besluitvorming en ontwikkelingen binnen de gemeente.

De Gemeente Albrandswaard werkt met persoonsgegevens van betrokkenen, waaronder in sommige gevallen ook met gevoelige en bijzondere persoonsgegevens. Te denken valt aan het Burgerservicenummer (BSN), gegevens in de Basisregistratie personen (BRP), gezondheidsgegevens bij de uitvoering van de Wet maatschappelijke ondersteuning 2015 (Wmo) en de Jeugdwet en politiegegevens verwerkt door Boa's. Het waarborgen van de privacy van betrokkenen is daarbij belangrijk voor de rechtmatige uitvoering van gemeentelijke taken.

Persoonsgegevens zijn alle gegevens die direct of indirect naar een natuurlijk persoon te herleiden zijn. Dit omvat niet alleen gegevens waarbij personen met naam en toenaam worden genoemd, maar ook gegevens zoals postcodes, kentekens en cookies op een website. De kaders voor de verwerking van persoonsgegevens, en daarmee voor het waarborgen van de privacy van betrokkenen, worden voor Gemeente Albrandswaard gevormd door de Algemene Verordening Gegevensbescherming (AVG), de Uitvoeringswet AVG (UAVG) en de Wet Politiegegevens (Wpg). Deze wetten staan in het bredere kader van de bescherming van de persoonlijke levenssfeer als grondrecht, zoals vastgelegd in het Europees Verdrag voor de Rechten van de Mens (EVRM) en het Handvest van de Grondrechten van de Europese Unie (Handvest EU).

Het verwerken van persoonsgegevens omvat onder andere, maar is niet beperkt tot, het verzamelen, bewaren, raadplegen, gebruiken, verstrekken en vernietigen van informatie. Het waarborgen van privacy is noodzakelijk voor het goed functioneren van de werkprocessen van de Gemeente Albrandswaard

en de samenwerking met andere organisaties binnen de maatschappelijke context waarin de gemeente opereert.

Bij de bescherming van persoonsgegevens staat de betrokkene centraal. Gemeente Albrandswaard communiceert transparant met betrokkenen over hoe zij met persoonsgegevens omgaat en biedt ondersteuning bij vragen of klachten hierover. Betrokkenen moeten erop kunnen vertrouwen dat de gemeente zorgvuldig met persoonsgegevens omgaat. Nieuwe technologische ontwikkelingen die de bescherming en beveiliging van persoonsgegevens verbeteren, worden waar nodig toegepast. De gemeente streeft ernaar te handelen in overeenstemming met de privacybeginselen bij de verwerking van persoonsgegevens.

De Gemeente Albrandswaard wordt sinds 1 januari 2024 ondersteund op het gebied van privacy door DBP, om optimale bescherming van persoonsgegevens te kunnen waarborgen. DBP voert op grond van mandaten de bedrijfsvoeringstaken van de gemeente uit. Hier is onder andere het beheer van alle geautomatiseerde systemen, technische gegevensverwerking en de privacy-advisering in onder gebracht.

Rechtmatigheid, behoorlijkheid, transparantie
De gemeente Albrandswaard houdt zich aan de geldende privacywet- en regelgeving, waarbij de AVG als uitgangspunt dient. Voor het verwerken van persoonsgegevens binnen de gemeente moet er altijd een rechtmatige grondslag zijn.

Daarnaast hanteert de gemeente het principe van ‘éénmalige vastlegging, meervoudig gebruik’. Dit houdt in dat gegevens die al bekend zijn, niet onnodig opnieuw worden opgevraagd. Waar mogelijk wordt gebruikgemaakt van brongegevens uit het stelsel van basisregistraties.

De gemeente Albrandswaard erkent en respecteert de rechten van betrokkenen, zoals vastgelegd in de AVG en in specifieke wetten, zoals de Wet basisregistratie personen.

Transparantie is een belangrijk uitgangspunt: de gemeente is duidelijk over hoe zij met persoonsgegevens omgaat en welke gegevens zij met derden deelt binnen een specifiek doel, tenzij wettelijke of andere gerechtvaardigde belangen zich daartegen verzetten.

Persoonsgegevens van inwoners worden niet gedeeld met derden, tenzij dit noodzakelijk is voor publieke doeleinden en/of de uitvoering van specifieke wetgeving, zoals bij openbare vergaderingen, of in het sociaal domein. In sommige gevallen kan de gemeente wettelijk verplicht zijn om gegevens te verstrekken, maar dit gebeurt alleen wanneer er geen alternatieve manier is om het doel te bereiken.

Onder geen beding zullen persoonsgegevens voor commerciële doeleinden worden gebruikt.

Doelbinding
Gemeente Albrandswaard legt alleen persoonsgegevens vast als dit noodzakelijk is voor het doel van de verwerking.

Opslagbeperking
Persoonsgegevens worden niet langer bewaard dan strikt noodzakelijk is voor het doel waarvoor ze zijn verzameld of op grond van de bepalingen uit de Archiefwet. Voor elke verwerking wordt daarom een specifieke bewaartermijn vastgesteld, waarbij in sommige gevallen verschillende bewaartermijnen gelden voor diverse categorieën van gegevens. Deze termijnen worden vastgesteld op basis van de AVG, relevante sectorale wetgeving, de Archiefwet en de Selectielijst. Hierbij heeft de wetgeving voorrang boven de Selectielijst. De proceseigenaar is verantwoordelijk voor het binnen de wettelijke termijn archiveren of vernietigen van de persoonsgegevens.

Integriteit en vertrouwelijkheid
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’ besteedt Gemeente Albrandswaard al tijdens de ontwikkeling aandacht aan privacyverhogende maatregelen.

Alleen medewerkers voor wie het noodzakelijk is voor de uitvoering van hun directe taken, hebben toegang tot persoonsgegevens. Hierbij wordt gezorgd voor passende organisatorische en technische beveiligingsmaatregelen, zoals het bijhouden van logs (het registreren van handelingen die met de data worden uitgevoerd) wanneer dit vereist is. Daarnaast worden geheimhoudingsverklaringen gehanteerd voor externe partijen en leveranciers, en worden met externe partners samenwerkingsafspraken gemaakt via convenanten of verwerkersovereenkomsten.

Het uitgangspunt is dat de gemeente Albrandswaard geen gegevens buiten de Europese Economische Ruimte (EER) verwerkt en het haar leveranciers (verwerkers) niet toestaat om zonder de juiste waarborgen gegevens die in opdracht van de Gemeente Albrandswaard worden verwerkt, buiten de EER door te geven.

Dataminimalisatie
Gemeente Albrandswaard streeft naar minimale gegevensverwerking.

Alleen die persoonsgegevens worden verwerkt die in redelijke verhouding staan tot het doel van de verwerking. Als het doel kan worden bereikt met een minder ingrijpende verwerking, dan wordt ernaar gestreefd om voor die verwerking te kiezen. Op deze manier wordt de inbreuk op de persoonlijke levenssfeer van de betrokkene zo beperkt mogelijk.

Het uitgangspunt geldt dat Gemeente Albrandswaard geen bijzondere persoonsgegevens registreert die aanleiding kunnen geven tot discriminatie. Gemeente Albrandswaard registreert geen bijzondere persoonsgegevens over burgers waaruit bijvoorbeeld hun gezondheid, religieuze of levensbeschouwelijke overtuiging, politieke opvattingen, ras of etnische afkomst, of seksuele voorkeur blijkt. Uitzonderingen hierop zijn enkel mogelijk als de wet dit vereist, dit noodzakelijk is voor de uitvoering van de taken van de gemeente of wanneer het college en/of de burgemeester hiermee instemt. Ook hier geldt weer dat deze situaties gemotiveerd worden voorgelegd. Een wettelijke verplichting is er bijvoorbeeld bij het register van burgerlijke stand, ontheemden en vluchtelingen (registratie etnische afkomst), jeugdhulpverlening en Wmo.

Ambitie
De gemeente Albrandswaard streeft ernaar te voldoen aan de basisvereisten van de Algemene Verordening Gegevensbescherming (AVG) en heeft hiervoor haar ambitieniveau bepaald aan de hand van de vijf volwassenheidsniveaus die het Centrum Informatiebeveiliging en Privacybescherming (CIP) hanteert.

Het CIP is een publiek-private netwerkorganisatie die zich richt op het verbeteren van informatiebeveiliging en privacybescherming binnen de overheid. Het model van het CIP is voor de gemeente Albrandswaard een waardevol instrument, omdat het een gestructureerde en stapsgewijze aanpak biedt om volwassenheid op het gebied van privacybeheer te verbeteren.

Het gewenste ambitieniveau voor de gemeente Albrandswaard is niveau 3, wat inhoudt dat de gemeente voldoet aan de geldende wet- en regelgeving. Dit betekent dat de gemeente niet alleen de wettelijke eisen naleeft, maar ook actief inzicht heeft in de risico's die gepaard gaan met gegevensverwerking en deze bewust beheert op bestuurlijk niveau.

Om dit ambitieniveau te bereiken, onderneemt de gemeente de volgende stappen:

- Huidige situatie in kaart brengen: Het vaststellen van het huidige niveau van privacybeheer binnen de organisatie om te bepalen welke verbeteringen nodig zijn.
- Risicobeheer: Het verkrijgen van inzicht in de risico's die gepaard gaan met gegevensverwerking en het bewust beheren van deze risico's op bestuurlijk niveau.
- Integratie van privacy: Het structureel integreren van privacy in processen, systemen en beleid binnen de gemeente.

In overeenstemming met de AVG implementeert de gemeente passende organisatorische en technische maatregelen die aantoonbaar zijn. Dit omvat het vastleggen en communiceren van procedures en werkinstructies, zodat rollen en verantwoordelijkheden duidelijk zijn en er adequaat kan worden gehandeld.

Om deze ambitie waar te maken, werkt de gemeente samen met de DBP. Deze samenwerking richt zich op acties zoals het vergroten van kennis en bewustwording binnen de organisatie, het adviseren over passende technische en organisatorische maatregelen en het versterken van de samenwerking tussen het team Privacy en de proceseigenaren van de gemeente.

De DBP ondersteunt de gemeente Albrandswaard door te adviseren, te controleren en te rapporteren over de voortgang en naleving. Dit gebeurt onder andere door middel van kwartaalrapportages.
In lijn met de AVG vereist dit de implementatie van passende organisatorische en technische maatregelen, die bovendien aantoonbaar zijn. Dit omvat het vastleggen en communiceren van onderliggende procedures en werkinstructies, zodat rollen en verantwoordelijkheden helder zijn en er adequaat kan worden gehandeld.

Opbouw privacybeleid
Hoofdstuk 2 van het privacybeleid gaat in op de uitgangspunten van Gemeente Albrandswaard voor de zorgvuldige omgang met persoonsgegevens en de kaders waaruit deze uitgangspunten voortvloeien. Hoofdstuk 3 beschrijft de rollen en verantwoordelijkheden die betrokken zijn bij de bescherming van persoonsgegevens binnen Gemeente Albrandswaard. In hoofdstuk 4 wordt de aanpak op het gebied van privacy beschreven, waarna het beleid zich richt op de verschillende privacy onderwerpen (hoofdstuk 5). Tot slot gaat hoofdstuk 6 over de Wet Politiegegevens.

2. Uitgangspunten en Kaders

Wettelijk kader
De wettelijke kaders voor het verwerken van persoonsgegevens zijn voor de Gemeente Albrandswaard gegeven in:

- de Algemene Verordening Gegevensbescherming (AVG), die
  - het kunnen aantonen van het voldoen aan de AVG (art. 5 lid 2 AVG) vereist;
  - aantoonbaarheid, evaluatie en aanpassing van de maatregelen (Art 24 lid 1) vereist.

- de Uitvoeringswet AVG (UAVG).
- de Wet Politiegegevens, die nader is uitgewerkt in het Besluit Politiegegeven en het Besluit Politiegegevens Boa's.
- en wetten ten aanzien van de taakuitvoering van gemeenten, zoals bijvoorbeeld:
  - de wet Basisregistratie Personen (BRP);
  - de Wet structuur uitvoeringsorganisatie werk en inkomen (SUWI);
  - de Wet Maatschappelijke Ondersteuning (Wmo);
  - de Jeugdwet (Jw);
  - de Participatiewet (Pw);
  - de Archiefwet.

Daarnaast committeert Gemeente Albrandswaard zich voor het aspect van de beveiliging van persoonsgegevens (Art 5 lid 1 sub f en Art 32 AVG) aan de Baseline Informatiebeveiliging Overheid (BIO) die is vastgesteld voor alle overheidslagen en de verwerkersovereenkomst van de VNG. De BIO is gebaseerd op de beheersmaatregelen van de internationale norm ISO27001, die deels nader zijn uitgewerkt in overheidsmaatregelen. Voor het privacybeleid zijn met name de volgende maatregelen uit de BIO van belang:

- Control: 18.1.1; 18.1.3; 18.1.4;
- Overheidsmaatregel: 18.1.3.1; 18.1.4.1; 18.1.4.2.

Relatie tussen Privacy en Informatiebeveiliging
Betrokkenen hebben het recht op privacy en bescherming van hun persoonlijke gegevens. Dit betekent dat er zorgvuldig moet worden omgegaan met deze gegevens en dat ze goed beveiligd moeten worden. Ook moeten alle regels rondom privacy worden gerespecteerd. Het beschermen van persoonsgegevens is een belangrijk gebied waarin privacy en informatiebeveiliging samenkomen, omdat beide nodig zijn om ervoor te zorgen dat gegevens veilig blijven en niet zomaar toegankelijk zijn voor anderen.

Dit privacybeleid beschrijft hoe persoonsgegevens die worden verwerkt door of namens Gemeente Albrandswaard worden beschermd. Het borgen van de beveiliging van deze informatie is beschreven in een afzonderlijk informatieveiligheidsbeleid.

In de praktijk is er een nauwe samenwerking tussen informatiebeveiliging en privacy, bijvoorbeeld bij bewustwording en training van medewerkers, bij het adviseren over en beoordelen van nieuwe applicaties en bij de uitvoering van een risicoanalyse op een proces.

Risicomanagement
Gemeente Albrandswaard wil aantoonbaar voldoen aan wet- en regelgeving. De AVG vereist in dit kader passende organisatorische en technische beheersmaatregelen en aantoonbaarheid, evaluatie en aanpassing van de maatregelen en verplichtingen in de AVG (Art 5 lid 2 AVG; art 24 lid 1 AVG).

Gemeente Albrandswaard wil "in control" zijn, dat wil zeggen overzicht hebben van waar de risico's op het gebied van privacy liggen en deze risico's bewust nemen vanuit bestuurlijk niveau.

Het in kaart brengen van mogelijke privacyrisico's gebeurt aan de hand van risicoanalyses en zal vastgelegd worden in o.a. het Register van verwerkingen en het Algoritme register. De bevoegdheid van het College van B&W is om naar aanleiding van uitgevoerde risicoanalyses besluiten te nemen om risico's te accepteren, te beperken en te vermijden (door de verwerking te staken). Deze bevoegdheid is gemandateerd aan de ambtelijke organisatie AW en DBP in de vorm van de proceseigenaren, het verantwoordelijke cluster en het verantwoordelijke team. Zie de Mandaatbesluitregeling gemeente Albrandswaard voor medewerkers van de gemeente en De BedrijfsvoeringsPartner | Lokale wet- en regelgeving

Om het risicomanagement te versterken hanteert Gemeente Albrandswaard drie verdedigingslinies.

De eerste verdedigingslinie richt zich op het identificeren van mogelijke risico's tijdens de uitvoering van werkprocessen binnen de afdeling, onder verantwoordelijkheid van de lijnmanager. Dit omvat het in kaart brengen van hoogrisicoverwerkingen, het op orde brengen en documenteren van werkprocessen, het opstellen van passende werkinstructies en het werken volgens vastgelegde afspraken. Hieronder vallen ook integriteitsrichtlijnen bij werving, het uitvoeren van het personeelsbeleid en aansturing van medewerkers.

De tweede verdedigingslinie draait om de borging en controle van beheersmaatregelen binnen de lijn, uitgevoerd door bijvoorbeeld kwaliteitsfunctionarissen, rechtmatigheidscontrollers, teamleiders of privacy officers van DBP. Het doel is vast te stellen dat werkprocessen conform de afspraken verlopen, deze te evalueren en waar nodig aan te passen. Voor privacy wordt dit gecoördineerd door het Informatiebeveiliging & Privacy team van DBP, in samenwerking met de privacy officer(s), en uitgevoerd volgens een controleplan.

De derde verdedigingslinie bestaat uit interne audits uitgevoerd door het Team Control van de DBP. Deze omvatten Verbijzonderde Interne Controles (VIC), controles op basis van artikel 213a van de Gemeentewet en artikel 33 van de Wet Politiegegevens, en ENSIA-audits (onder andere ten behoeve van Suwinet, burgerlijke stand basisregistratie personen, DigiD). De audits evalueren de effectiviteit van de eerste en tweede linies en bieden onafhankelijke assurance over de interne controle en risicobeheersing, met aanbevelingen voor verbeteringen waar nodig.

Borging
De borging van het beheersen en verbeteren van privacy wordt meegenomen in de plan-do-check-act-cyclus en bestaat uit de volgende stappen:

Plan: Het inrichten en documenteren van beheersmaatregelen en de organisatiebrede aanpak van privacy voor Gemeente Albrandswaard, gebaseerd op geldende normen, wettelijke vereisten en risicobeoordelingen (in termen van interne controle: de 'opzet', 1e verdedigingslinie).

Do: Het aantonen van de uitvoering van de beheersmaatregelen en de organisatiebrede aanpak van privacy (in termen van interne controle: het 'bestaan', 1e verdedigingslinie).

Check: Het controleren en evalueren van de beheersmaatregelen en de organisatiebrede privacyaanpak. Hierbij worden criteria als volledige uitvoering en effectiviteit gehanteerd, waarbij ook de voortschrijdende ontwikkeling van technologie en nieuwe bedreigingen worden meegenomen. Dit omvat zowel interne als externe audits (de werking, 2e en 3e verdedigingslinie).

Act: Het aanpassen en/of verbeteren van de beheersmaatregelen en de privacyaanpak van Gemeente Albrandswaard op basis van de evaluatie (in termen van interne controle: de opzet en werking, 1e verdedigingslinie).

Beheersmaatregelen
Om te komen tot passende beheersmaatregelen wordt gebruik gemaakt van raamwerken met beheersmaatregelen om te waarborgen dat de wetgeving adequaat wordt afgedekt. Voorbeelden van beheersmaatregelen zijn het hebben van een up-to-date en volledig Register van verwerkingen en Algoritme register, het informeren van betrokkenen, het overeenkomen en beoordelen van verwerkersovereenkomsten en het uitvoeren van Data Protection Impact Assessments (DPIA's).

Externe partijen
Gemeente Albrandswaard verlangt van externe partijen die gegevens in opdracht van de organisatie verwerken en ketenpartners waarmee gegevens van betrokkenen worden uitgewisseld dat zij aantoonbaar voldoen aan een vergelijkbaar niveau van informatiebeveiliging en borging van privacy als Gemeente Albrandswaard zelf. Het gaat daarbij bijvoorbeeld om IT-leveranciers, maar ook ketenpartners in bijvoorbeeld Wmo en Jeugdzorg, zoals zorginstellingen. Dit wordt gewaarborgd in juridische privacy overeenkomsten.

Medewerkers
Wanneer dit beleid en/of beheersmaatregelen eisen stelt aan taken en verantwoordelijkheden van medewerkers dan worden deze opgenomen in aanvullende individuele afspraken, welke in specifieke procedures en werkinstructies staan, of zullen worden, opgenomen.

3. Rollen en verantwoordelijkheden

Het College van Burgemeester en Wethouders is bestuurlijk eindverantwoordelijk voor de privacy- en informatiebeveiligingsdoelstellingen van Gemeente Albrandswaard. Het College stelt het beleid vast en ziet toe op de realisatie hiervan via de uitvoerende lagen binnen de organisatie, zoals de directie en het lijnmanagement.

De directie van de gemeente en DBP zet de koers uit door het beleid om te zetten in doelstellingen, plannen en middelen en houdt toezicht op de naleving ervan. Het lijnmanagement is verantwoordelijk voor de integratie van dit beleid in de dagelijkse processen en zorgt voor de uitvoering en aansturing van medewerkers. Daarnaast is de directie verantwoordelijk voor de evaluatie en bijstelling van de aanpak van privacy en beheersingsmaatregelen. De uitvoering van privacy wordt ondersteund door:

- Alle medewerkers, die verantwoordelijk zijn voor het uitvoeren van het privacybeleid als onderdeel van hun professionele verantwoordelijkheid.
- Leidinggevenden/proceseigenaren van gemeente en DBP, die:
    - Verantwoordelijk zijn voor de uitvoering van het privacybeleid en de beheersmaatregelen binnen hun afdeling. Informatiesystemen en processen die door meerdere organisatieonderdelen worden gebruikt, vallen onder de verantwoordelijkheid van de systeemeigenaar;
    - Zorgen voor een adequate inrichting van werkprocessen en de aansturing van medewerkers (1e verdedigingslinie);
    - Toezien op de naleving van het beleid en het bevorderen van privacybewustzijn;
    - Onderdelen van beheersmaatregelen uitvoeren, zoals het bijhouden van het verwerkingenregister, het uitvoeren van DPIA's en risicoanalyses, en het beoordelen van toegangsrechten;
    - Relevante wettelijke, statutaire, regelgevende en contractuele eisen voor hun informatiesystemen vaststellen, documenteren en actueel houden;
    - Processpecifieke borgings-/controleactiviteiten uitvoeren, vaak samenhangend met processpecifieke applicaties;
    - Verantwoordelijk zijn voor het nemen van maatregelen om datalekken binnen hun afdeling te voorkomen.

- De Coördinerend Privacy Officer (CPO) van DBP, die:
    - Het opstellen, de uitvoering, evaluatie en bijstelling van het privacybeleid en de jaarlijkse verbetercycli coördineert;
    - De implementatie, uitvoering en borging van beheersmaatregelen coördineert en hierover rapporteert;
    - Over datalekken wordt rapporteert aan het management van de gemeente;
    - De afhandeling en evaluatie van datalekken en verzoeken van betrokkenen coördineert;
    - Privacybewustzijn bevordert in de gehele organisatie;
    - De activiteiten van PO's inhoudelijk coördineert.

- De Privacy Officer(s) (PO's) van DBP, die:
  - Op operationeel niveau gevraagd en ongevraagd adviseren;
  - Ondersteunen bij de uitvoering van het privacybeleid en het jaarplan;
  - Helpen bij de implementatie en uitvoering van beheersmaatregelen, zoals DPIA's, verzoeken van betrokkenen, de afhandeling en evaluatie van datalekken en het bevorderen van privacybewustzijn, en het bijhouden van het register van verwerkingen.

- De Functionaris Gegevensbescherming (FG) van DBP, die:
  - Gemeente Albrandswaard informeert en adviseert over de verplichtingen uit de AVG;
  - Toeziet op de naleving van de AVG binnen de gemeente;
  - Toeziet op de naleving van de Wpg binnen de gemeente;
  - Op verzoek advies geeft over risicoanalyses;
  - Samenwerkt met de toezichthouder (Autoriteit Persoonsgegevens);
  - Optreedt als contactpunt voor de Autoriteit Persoonsgegevens;
  - Rechtstreeks verslag uitbrengt aan het dagelijks bestuur van Gemeente Albrandswaard;
  - Jaarlijks een verslag met aanbevelingen opstelt.

- De Chief Information Security Officer (CISO) van DBP, die:
  - Het opstellen, de uitvoering, evaluatie en bijstelling van het informatiebeveiligingsbeleid en de jaarlijkse verbetercycli coördineert;
  - De implementatie, uitvoering en borging van beveiligingsmaatregelen coördineert;
  - Rapporteert over beveiligingsincidenten aan de Stuurgroep IV&P en rechtstreeks verslag kan doen aan de directie van Gemeente Albrandswaard;
  - De Stuurgroep IV&P en het management gevraagd en ongevraagd adviseert over informatiebeveiliging;
  - Beveiligingsincidenten registreert in een incidentenregister en de afhandeling en evaluatie hiervan coördineert;
  - Beveiligingsbewustzijn bevordert in de gehele organisatie.

- Team Control van DBP, die:
  - Interne audits coördineert, zoals de Verbijzonderde Interne Controles (VIC) en het onderzoeksplan doelmatigheid en doeltreffendheid op basis van artikel 213a van de Gemeentewet;
  - Externe audits coördineert, bijvoorbeeld de IT-audit in het kader van de controle van de jaarrekening.

- De rol van de interne controller: De controller van de gemeente Albrandswaard blijft op de hoogte van de processen. De controller wordt vooraf geïnformeerd over en betrokken bij nieuwe adviezen, rapportages en audits met betrekking tot Privacy & Informatiebeveiliging. De interne controller zorgt voor de juridische rechtmatigheidscontrole en de jaarlijkse rechtmatigheidsverantwoording.
- Gemeentesecretaris Albrandswaard: heeft de overkoepelende verantwoordelijkheid voor de dagelijkse uitvoering van informatieveiligheids- en privacymaatregelen.
- Chief Privacy Officer (CPO) DBP: verantwoordelijk voor de coördinatie van het privacybeleid binnen de gemeente.
- Clustermanager F&R: verantwoordelijk voor de integratie van informatieveiligheid en privacy in de gemeentelijke processen.
- Teamleider Control van DBP: verantwoordelijk voor de naleving en controle van de interne processen, waaronder privacy- en informatieveiligheidsbeleid.

4. De aanpak van Privacy

Om de borging van het privacybeleid en de daarvan afgeleide plannen te realiseren, doorloopt Gemeente Albrandswaard de onderstaande Plan, Do, Check, Act (PDCA)-cyclus, zowel organisatiebreed als per beheersmaatregel. Er wordt vanuit het IV&P-team binnen DBP samen met de Gemeente Albrandswaard een uitvoeringsplan opgesteld waarin ook het advies van de Functionaris Gegevensbescherming (FG) uit de jaarrapportage wordt meegenomen. Vervolgens worden het jaarplan en de bijbehorende beheersmaatregelen uitgevoerd en worden borgings-/controleacties uitgevoerd om vast te stellen of de beheersmaatregelen volledig zijn geïmplementeerd. Zo kijkt Gemeente Albrandswaard of deze effectief zijn en waar nodig, moeten worden bijgestuurd. Indien nodig kijkt Gemeente Albrandswaard naar herprioritering en/of aanvullende maatregelen waarbij aanbevelingen worden gedaan voor het verbeterplan.

Plan: Team IV&P binnen DBP stelt een jaarplan met verbeterpunten op, rekening houdend met Gemeente Albrandswaard-strategie en -doelstellingen, risico's, regelgeving (waaronder eventuele wijzigingen in de wetgeving), de stand van de techniek, beschikbare middelen, en het advies van de FG. Het plan bevat

meetbare doelen en een activiteitenplanning met rollen en verantwoordelijkheden, benodigde middelen, tijdslijnen en resultaten.

Do: Het jaarplan en de beheersmaatregelen worden uitgevoerd, waarbij beheersmaatregelen stapsgewijs worden ingevoerd en verbeterd. Onder de beheersmaatregelen vallen onder andere:

- Onderhouden en publiceren van het register van verwerkingen;
- Actief informeren van betrokkenen;
- Afhandelen van datalekken en verzoeken van betrokkenen;
- Afsluiten van verwerkersovereenkomsten met leveranciers en controle van de naleving daarvan;
- Naleven van bewerkings- en verwerkingstermijnen;
- Uitvoeren van DPIA's.

De uitvoering van het jaarplan en de beheersmaatregelen wordt bewaakt door de CPO van DBP, waarbij systeem- en proceseigenaren zorgen voor de naleving in de operationele processen.

Check: Borgings-/controleacties worden uitgevoerd om vast te stellen of de beheersmaatregelen volledig zijn geïmplementeerd en effectief zijn. De borgings-/controleacties worden opgenomen in een controleplan, zodat alle geïmplementeerde maatregelen passend worden afgedekt. Hier rapporteert de CPO van DBP elk kwartaal over, met inbegrip van datalekken en andere relevante gebeurtenissen aan de gemeentesecretaris en control van Albrandswaard.

Naast interne controles worden er, waar nodig, ook externe audits uitgevoerd om de effectiviteit en volledigheid van de beheersmaatregelen te evalueren. Deze audits worden uitgevoerd in overeenstemming met het jaarlijkse auditplan en in overeenstemming met control van Albrandswaard.

De FG geeft onafhankelijk advies over de naleving van de AVG tijdens de evaluaties in de Check-fase en rapporteert hierover aan het College van Burgemeester en Wethouders.

Act: Team IV&P zal bijsturen, herprioriteren en/of aanvullende maatregelen nemen of aanbevelingen doen voor het volgende verbeterplan op basis van de resultaten in de Check-fase, inclusief aanbevelingen uit interne en externe audits en incidentrapportages. Hiermee zorgt Gemeente Albrandswaard voor een continue verbetering van privacy.

5. Privacy beheersmaatregelen

Bewustwording en training

De CPO van DBP stelt jaarlijks, in samenwerking met de CISO, een bewustwordings- en trainingsplan voor Gemeente Albrandswaard en coördineert de uitvoering. Bij het opstellen van het bewustwordings- en trainingsplan wordt rekening gehouden met aanbevelingen van de FG en trends in bedreigingen en maatschappelijke ontwikkelingen.

Register van Verwerkingen

De gemeente Albrandswaard draagt de eindverantwoordelijkheid voor het onderhouden van een actueel en volledig register van verwerkingen binnen de interne werkprocessen. Hierbij zal ondersteuning worden geboden door DBP. Het is de taak van de gemeente om een up-to-date overzicht van de verwerkingsactiviteiten te leveren. In het register worden per verwerking de vereiste gegevens opgenomen, conform de AVG en Wpg. De gemeente streeft ernaar het register zo in te richten dat het gemakkelijk kan worden geraadpleegd bij verzoeken.

Data Protection Impact Assessment

Het uitgangspunt is dat voor (nieuwe) verwerkingen met een hoog privacyrisico binnen de gemeente Albrandswaard een Data Protection Impact Assessment (DPIA) wordt uitgevoerd. Hierbij wordt een integrale benadering gevolgd, waarbij niet alleen informatiebescherming maar ook informatiebeveiliging en informatiebeheer worden meegenomen. Op deze manier krijgt de gemeente een volledig overzicht van de risico's binnen een werkproces en de maatregelen die nodig zijn om deze te beperken. Dit is in overeenstemming met artikel 35 van de AVG, artikel 4c van de Wpg, en de richtlijnen van de gemeente Albrandswaard en de Autoriteit Persoonsgegevens.

Daarnaast kan de gemeente, op advies van DBP in de rol van FG, CPO of CISO, besluiten om een DPIA uit te voeren. De proceseigenaar is eindverantwoordelijk voor de uitvoering van de DPIA en wordt hierbij ondersteund door de relevante stakeholders.

Datalekken
Medewerkers zijn verplicht om datalekken, beveiligingsincidenten en kwetsbaarheden te melden. Datalekken binnen de gemeente Albrandswaard worden centraal geregistreerd via Topdesk en, indien nodig, Binnen de wettelijke termijn gerapporteerd aan de Autoriteit Persoonsgegevens (AP) en/of betrokkenen.

Alle meldingen worden vastgelegd in een datalekregister, waarin per melding wordt aangegeven of er sprake is van een datalek, of melding aan de AP en/of betrokkenen verplicht is, en een schriftelijke onderbouwing van het incident. Daarnaast wordt de mogelijke acceptatie van risico's door het management gedocumenteerd.

Elk datalek wordt geëvalueerd om passende maatregelen te nemen die herhaling voorkomen. Jaarlijks worden alle datalekken geanalyseerd om trends en patronen te identificeren, zodat verdere preventieve maatregelen getroffen kunnen worden. Dit proces sluit goed aan bij de PDCA-cyclus (Plan-Do-Check-Act).

Transparantie en Rechten van betrokkenen
Gemeente Albrandswaard informeert betrokkenen over de verwerking van hun persoonsgegevens en hun rechten. Het streven is om dit zo efficiënt mogelijk te doen door:

- Betrokkenen te informeren bij het eerste schriftelijke contact binnen een specifieke verwerking;
- Deze informatie duidelijk en uitgebreid op te nemen in de privacyverklaring op de website;
- Verzoeken van betrokkenen om hun rechten uit te oefenen binnen de wettelijke termijn en volgens de gemaakte afspraken binnen de Gemeente Albrandswaard af te handelen.

Geautomatiseerde besluitvorming, waaronder profilering
De gemeente Albrandswaard heeft als uitgangspunt geen gebruik te maken van geautomatiseerde besluitvorming, waaronder profilering, zoals bedoeld in artikel 22 van de AVG. Om dit te waarborgen, wordt via een Algoritmeregister inzicht gegeven in welke processen mogelijk algoritmes of profilering worden toegepast. Voor deze processen wordt een risicoanalyse uitgevoerd om de potentiële risico's te beoordelen, zoals beschreven in het onderdeel ‘risicomanagement’ hierboven.

6. Verwerking van politiegegevens

Uitgangspunten en bereik
De gemeente Albrandswaard volgt het model voor beheersmaatregelen dat is opgesteld voor Wpg-audits (Wet politiegegevens), zoals beschreven in bijlage 3 en 4 van de NOREA-handreiking voor privacy audits voor Buitengewoon Opsporingsambtenaren (boa’s). Deze NOREA-handreiking is een richtlijn opgesteld door NOREA, de beroepsorganisatie van IT-auditors in Nederland, en biedt specifieke richtlijnen en standaarden voor privacy-audits binnen het kader van de Wpg. Het document helpt organisaties de beveiliging van politiegegevens te waarborgen en ondersteunt bij het aantoonbaar naleven van de wettelijke privacy-eisen.

Indien een informatiesysteem wordt beheerd door een externe leverancier, zoals bij SaaS-oplossingen (Software as a Service), sluit de gemeente een verwerkersovereenkomst met de betreffende leverancier af. Deze overeenkomst waarborgt de bescherming van persoonsgegevens en bepaalt onder meer de verantwoordelijkheden van de leverancier ten aanzien van databeveiliging. Daarnaast is de leverancier verplicht een Third Party Memorandum (TPM) aan te leveren. Dit TPM-document, opgesteld volgens de NOREA-handreiking, biedt inzicht in de beveiligingsmaatregelen en de naleving van privacyrichtlijnen bij de leverancier.

Door gebruik te maken van deze NOREA-richtlijnen verzekert de gemeente Albrandswaard dat alle betrokken partijen voldoen aan de gestelde normen en richtlijnen voor de bescherming van politiegegevens en andere persoonsgegevens, conform de Wpg.

De verwerking van politiegegevens door de gemeente Albrandswaard is gebaseerd op artikel 8 van de Wpg (uitvoering van de dagelijkse politietaak) en de artikelen met betrekking tot het ter beschikking stellen en verstrekken van politiegegevens (artikelen 15-21 en 23-24). Daarnaast verwerkt de gemeente politiegegevens op basis van artikel 13 Wpg (ondersteunende taken), voor zover deze gegevens onder de verantwoordelijkheid van andere instanties vallen.

Gemeente Albrandswaard verwerkt geen gegevens op basis van de volgende artikelen van de Wpg:

- Artikel 9 Wpg (onderzoek in een specifiek geval), hoewel boa’s wel medewerking verlenen aan onderzoeken onder verantwoordelijkheid van de politie of andere opsporingsdiensten.
- Artikel 11 Wpg (geautomatiseerd vergelijken en zoeken in combinatie voor een onderzoek op basis van Artikel 9).

- Artikel 17a Wpg (doorgifte aan derde landen buiten de Europese Economische Ruimte). De gemeente maakt ook geen gebruik van geautomatiseerde besluitvorming, waaronder profilering zoals bedoeld in Artikel 7a Wpg.

De toegangsbeveiliging is zodanig ingericht dat alleen boa's en andere geautoriseerde personen toegang hebben tot de politiegegevens. Bij verzending worden de politiegegevens altijd versleuteld verstuurd.

Rollen, taken en bevoegdheden
De Privacy Officer van DBP beoordeelt jaarlijks of het bereik van de verwerking van politiegegevens is gewijzigd. Op basis hiervan worden dit beleid en het verwerkingenregister indien nodig aangepast.

De Teamleider van het team met Boa's is verantwoordelijk voor de implementatie en uitvoering van de Wpg. De taken omvatten onder andere:

- Medewerkers informeren over de handreiking en gedragsregels voor Boa's en toezicht hierop houden.
- Een overzicht bijhouden van geautoriseerden.
- Het actueel houden van het verwerkingenregister met betrekking tot het team.
- Bijhouden van een lijst met veel voorkomende verstrekkingen en de onderbouwing van de grondslagen hiervoor.
- Zorgdragen voor de bewaartermijnen van Art. 8 gegevens:
    - Na 1 jaar alleen beschikbaar voor gericht zoeken.
    - Na 5 jaar beschikbaar voor audits en klachtenprocedures.
    - Na 10 jaar vernietigd.

- Boa's en leerplichtambtenaren autoriseren voor verwerking politiegegevens volgens Wpg Art. 6, lid 3, 4, 5 via het "Autorisatie verwerking politiegegevens"-formulier en de autorisatiematrix vast te stellen.

De Teamleider Informatiebeheer van DBP heeft de bevoegdheid om medewerkers te autoriseren voor digitale verwerking justitiële gegevens op grond van artikel artikelen 9 tot en met 13 van de Wet justitiële en strafvorderlijke gegevens en het Besluit justitiële en strafvorderlijke gegevens:

Het college en de burgemeester nemen aanwijzings- en autorisatiebesluiten voor verwerken politiegegevens en justitiële informatie ten behoeve van: openbare orde en veiligheid, APV en bijzondere wetten en sociaal domein.

De Functionaris Gegevensbescherming (FG):

- Adviseert en informeert over de Wpg, waaronder DPIA's.
- Houdt toezicht op de uitvoering van de Wpg.
- Werkt samen met de AP en is het aanspreekpunt voor de AP.
- Stelt jaarlijks een verslag op met bevindingen.
- Voort controles uit.

Team Control van DBP coördineert interne en externe Wpg-audits.

Specifiek beleid cluster Veiligheid.
De gemeente Albrandswaard maakt gebruik van zowel bestuursrechtelijke als strafrechtelijke middelen voor toezicht en handhaving in de openbare ruimte. Boa's zijn hiervoor aangesteld en de Wpg is van toepassing.

Specifiek beleid leerplichtwet.
Naast bestuursrechtelijke middelen gebruikt de gemeente Albrandswaard strafrechtelijke instrumenten voor handhaving van de leerplichtwet, specifiek Art. 16 lid 5 en Art. 26. Boa's zijn aangesteld en de Wpg is van toepassing.

Specifiek beleid participatiewet
Voor toezicht en handhaving binnen de Participatiewet worden alleen bestuursrechtelijke middelen ingezet door de medewerker toezicht en handhaving . Boa's zijn hier niet aangesteld en de Wpg is niet van toepassing.

Inwerkingtreding en intrekking
"Privacybeleid gemeente Albrandswaard 2025 – 2027" treedt in werking de dag na publicatie Tegelijkertijd wordt ingetrokken "privacybeleid van de gemeente Albrandswaard 2019/2020".

Aldus besloten op 4 november 2025 november 2025,

College van burgemeester en wethouders van de gemeente Albrandswaard,

de secretaris,

de burgemeester,