Gemeente Albrandswaard

GEMEENTEBLAD

Officiële uitgave van de gemeente Albrandswaard

Nr. 264385

31 oktober 2019

Privacybeleid van de gemeente Albrandswaard 2019/2020

Binnen de gemeente Albrandswaard wordt veel gewerkt met persoonsgegevens van burgers, medewerkers en (keten)partners. Persoonsgegevens worden verzameld voor het goed uitvoeren van de gemeentelijke taken. Onze inwoners moeten erop kunnen vertrouwen dat wij zorgvuldig en veilig met de persoonsgegevens omgaan. In deze tijd gaan ook gemeenten mee met nieuwe ontwikkelingen. Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds meer digitale overheid stellen andere eisen aan de bescherming van gegevens en privacy. Wij zijn ons hier van bewust en zorgen dat de privacy gewaarborgd blijft, onder andere door maatregelen op het gebied van informatiebeveiliging, dataminimalisatie, transparantie en gebruikerscontrole.

Wij geven met dit beleid een duidelijke richting aan de bescherming van persoonsgegevens. Dit beleid is van toepassing op de gehele organisatie, al onze processen, onderdelen, objecten en gegevensverzamelingen. Dit privacybeleid van de gemeente Albrandswaard is in lijn met het algemene beleid van de gemeente en de relevante lokale, regionale, nationale en Europese wet- en regelgeving.

Wettelijke kaders voor de omgang met persoonsgegevens
De gemeente is verantwoordelijk voor het opstellen, uitvoeren en handhaven van het beleid. Hiervoor gelden onder andere de volgende wettelijke kaders:

- De Algemene Verordening Gegevensbescherming (AVG)
- Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG)
- De Algemene wet bestuursrecht (Awb)
- De Wet Politiegegevens
- De Wet maatschappelijke ondersteuning 2015
- De Participatiewet
- De Jeugdwet

Wettelijke grondslag voor en reikwijdte van dit beleidsstuk
Dit beleid vloeit rechtstreeks voort uit het bepaalde in artikel 24, lid 2 AVG en hangt samen met het gemeentelijke informatieveiligheidsbeleid. Daar waar in andere beleidsstukken wordt afgeweken van dit algemene beleid dient dit nadrukkelijk te geschieden. Alleen in die gevallen wijkt dit algemene privacybeleid voor het bijzondere beleidsstuk.

Dit beleid is voor het overige gegrond op het bepaalde in Titel 4.3 van de Algemene wet bestuursrecht. Afwijking van hetgeen in dit privacy beleid is vastgelegd, is toegestaan in bijzondere gevallen. De afwijking van dit beleid wordt door het betrokken bestuursorgaan gemotiveerd. Van dit beleid maken de bijlagen zoals hieronder genoemd, onlosmakelijk onderdeel uit.

Uitgangspunten
Wij gaan op een veilige manier met persoonsgegevens om en respecteren de privacy van onze inwoners. Wij houden ons daarom aan de volgende uitgangspunten:

Rechtmatigheid, behoorlijkheid, transparantie
Persoonsgegevens worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt. Op ons rust echter een veelheid aan wettelijke verplichtingen op grond waarvan wij persoonsgegevens verwerken. Wij zorgen er voor dat betrokkenen daar inzicht in hebben. Wij zorgen er daarom voor dat het verwerkingsregister online beschikbaar is en actueel.

Grondslag en doelbinding
Wij zorgen er voor dat verwerkingen die binnen de gemeente plaatsvinden, altijd gestoeld zijn op een rechtmatige grondslag. Dat zal in ons geval veelal een wettelijke verplichting zijn. Wij zorgen er daarnaast natuurlijk ook voor dat wij gegevens niet voor een ander doel verwerken dan die waarvoor de gegevens zijn verzameld. Dat kan overigens anders zijn, wanneer wij in verband met een wettelijke verplichting die gegevens wel verder verwerken. Daarvan is bijvoorbeeld sprake bij de verplichtingen die wij hebben op grond van de Participatiewet. In die gevallen zorgen wij er voor dat de betrokkene op de hoogte is van wat er met de persoonsgegevens gebeurt.

Dataminimalisatie
De gemeente verwerkt alleen de persoonsgegevens die maximaal noodzakelijk zijn voor het vooraf bepaalde doel. Dat doel wordt doorgaans vastgesteld door wettelijke regelingen die wij uitvoeren. De gemeente streeft naar minimale gegevensverwerking. Waar mogelijk worden minder of geen persoonsgegevens verwerkt. Om dat te bereiken loopt de gemeente zijn processen doorlopend door en waakt op die wijze voor overbodige verwerking van persoonsgegevens.

Bewaartermijn
Het bewaren van persoonsgegevens kan nodig zijn om de gemeentelijke taken goed uit te kunnen oefenen of om wettelijke verplichtingen te kunnen naleven. Gemeenten zijn daarbij gebonden aan het bepaalde in de Archiefwet, de daarop gebaseerde besluiten en andere wetten. Hoe lang het noodzakelijk is om persoonsgegevens te bewaren hangt daarom af van het bepaalde in de archiefwet of bijzondere wetten, zoals de Wet basisregistratie personen of fiscale wet- en regelgeving. De bewaartermijn varieert daardoor fors. In ons verwerkingsregister hebben wij daarom per zaaksoort de wettelijke bewaartermijn opgenomen.

Integriteit en vertrouwelijkheid
Wij gaan zorgvuldig om met persoonsgegevens en behandelen deze vertrouwelijk. Zo worden persoonsgegevens alleen verwerkt door medewerkers met een wettelijke geheimhoudingsplicht en in beginsel slechts voor het doel waarvoor deze gegevens zijn verzameld. Daarbij zorgen wij voor passende beveiliging van persoonsgegevens. Deze beveiliging is voor de meeste gevallen vastgelegd in het door ons gehanteerde informatiebeveiligingsbeleid en het normenkader Baseline Informatiebeveiliging Gemeenten (BIG)[1] en Overheden (BIO).

Delen met derden
Het komt voor dat wij vrijwillig samenwerking met externe partijen. Dat is bijvoorbeeld het geval bij leveranciers van software applicaties. Er kan dan sprake zijn van gegevensverwerking, waaronder uitwisseling, verstrekking of ter beschikkingstelling van persoonsgegevens. In die gevallen maken wij afspraken over de eisen waar deze verwerking en de verdere omgang met persoonsgegevens aan moet voldoen. In die gevallen zorgen wij er voor dat de door die externe partijen te hanteren veiligheidsmaatregelen vergelijkbaar zijn met de eisen die op ons rusten als overheid. Wij zorgen er voor dat de afspraken die wij maken voldoen aan het bepaalde in de AVG. Wij evalueren de gemaakte afspraken met derden op regelmatige basis en passen deze indien nodig aan.

Wij delen overigens alle ontvangen persoonsgegevens met de BAR-organisatie. Alle medewerkers van de gemeente zijn daar in dienst. Wij zijn daardoor samen met de BAR-organisatie verantwoordelijk voor een rechtmatige verwerking van persoonsgegevens en de uitvoering van alle andere wettelijke taken. Wij houden hier getrapt (raad controleert het college en het college controleert de BAR) via het bestuur van de BAR-organisatie toezicht op.

Proportionaliteit
Bij het verwerken van persoonsgegevens moeten wij rekening houden met het doel daarvan en het belang van u als burger. Wij verwerken gegevens vrijwel altijd in het kader van een toegewezen wettelijke taak. Het doel van de verwerking is dan terug te voeren op die wettelijke taak. Wanneer een verwerking niet op een wettelijke taak is gebaseerd, dan maken wij dat duidelijk.

Subsidiariteit
Om het doel dat met de verwerking van persoonsgegevens te bereiken, houden wij de inbreuk op de persoonlijke levenssfeer van de burger zo beperkt mogelijk. Als een minder ingrijpende verwerking mogelijk is, dan streven wij er naar om voor die verwerking te kiezen.
Omdat gemeenten persoonsgegevens verwerken in het kader van de uitvoering van wettelijke taken, kan het zijn dat verwerkingen toch minder beperkt zijn. Dat kan bijvoorbeeld omdat de wet voorschrijft dat wij juist zo veel als mogelijk gegevens moeten verzamelen of dat wij gegevens verplicht moeten delen met andere overheden en instanties. In dat geval houden wij ons aan hetgeen de wetgever van ons vraagt.

Rechten van betrokkenen
Wij onderschrijven de rechten van betrokkenen zoals deze zijn gegeven op grond van de AVG en – in voorkomende gevallen – zoals die zijn gegeven in bijzondere wetten zoals de Wet basisregistraties personen. Wij dragen zorg voor de verwezenlijking daarvan. Wij leggen daarbij geen zwaardere eisen voor wat betreft de identificatie van een verzoeker op dan vereist op grond van artikel 12 AVG.

Wij nemen als uitgangspunt dat het bepaalde in de AVG voorgaat op hetgeen dat in Nederlandse wetgeving is opgenomen, voor zover daar op enigerlei wijze strijdigheid in bestaat. Voor wat betreft de opslag van persoonsgegevens gaat de gemeente uit van hetgeen bij of krachtens de Archiefwet of bijzondere wetgeving is bepaald. In overige gevallen worden de in het geding zijnde belangen gewogen.

Wij beseffen dat een transparante overheid soms schuurt met de zorg voor persoonsgegevens van inwoners. Wij zijn immers op grond van de (Grond)wet verplicht om informatie te openbaren of – op

1) https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2016/07/Strategische-Baseline-Informatiebeveiliging-Nederlandse-Gemeenten-v1.02.pdf

verzoek – openbaar te maken. Wij nemen daarbij tot uitgangspunt dat persoonsgegevens van individuele inwoners niet worden geopenbaard.
Dit kan alleen anders zijn wanneer de openbaarmaking van persoonsgegevens het belang van de publieke informatievoorziening dient, zoals bijvoorbeeld bij verslagen van openbare vergaderingen. Ook ingeval van een bijzondere verplichting – zoals die op ons rust in het kader van de Wet basisregistraties persoonsgegevens – kan, wanneer het doel dat met die bijzondere verplichting niet op een andere wijze kan worden bereikt, van dit uitgangspunt worden afgeweken.

Werking beleid
Dit privacybeleid treedt in werking op de dag na de bekendmaking daarvan en werkt terug tot aan 1 januari 2019. Het beleid wordt ieder jaar geëvalueerd en indien nodig herzien. Aanpassingen van dit beleid worden bekendgemaakt via het elektronisch gemeenteblad en gepubliceerd via de website van de gemeente. De meest actuele versie van het beleid is te vinden op de gemeentelijke website en op de site van de landelijke overheid.

Bijlagen
Bij dit beleidsstuk behoren een aantal bijlagen. Deze bijlagen kunnen niet los worden gezien van dit beleid en maken daar integraal onderdeel van uit. De bijlagen kunnen echter, met uitzondering van Bijlage 1, worden gewijzigd door de organen die deze hebben vastgesteld en in die gewijzigde vorm aan dit beleid worden gehecht. Deze bijlagen zijn:
1. Het Privacyreglement van de gemeente Albrandswaard.
2. Het convenant gegevensverwerking tussen de gemeente Albrandswaard en de BAR-organisatie.
3. Mandaatbesluit informatieveiligheid en privacy van de gemeente Albrandswaard.

Aldus vastgesteld door: De gemeenteraad van de gemeente Albrandswaard op 7 oktober 2019,

de griffier,
drs. Leendert Groenenboom

de burgemeester,
drs. Jolanda de Witte

Het college van burgemeester en wethouders van gemeente Albrandswaard op 16 juli 2019,

de secretaris,
Hans Cats

de burgemeester,
drs. Jolanda de Witte

De burgemeester van de gemeente Albrandswaard op 16 juli 2019,

De burgemeester,
drs. Jolanda de Witte

Bijlage 1 Privacyreglement

Privacyreglement Gemeente Albrandswaard
In dit reglement laten wij zien op welke manier wij dagelijks omgaan met persoonsgegevens en privacy van onze inwoners en anderen, en wat er wettelijk wel en niet verantwoord is. Dit reglement geldt als leidraad voor verwerkingen binnen de gemeentelijke organisatie.

Privacy speelt een belangrijke rol in de relatie tussen de burger en de overheid en staat daarmee hoog op onze agenda. Wij hebben als gemeente de verantwoordelijkheid over persoonsgegevens en gegevensuitwisseling op alle denkbare terreinen waar de overheid actief is. Wij zijn verplicht om zorgvuldig en veilig, proportioneel en vertrouwelijk om te gaan met het verzamelen, bewaren en beheren van persoonsgegevens. Dat geldt voor taken op het gebied van basisadministraties, openbare orde en veiligheid en het sociaal domein. Goed en zorgvuldig omgaan met persoonsgegevens is een dagelijkse bezigheid van gemeenten.

Het beschermen van de privacy is complex, en wordt steeds complexer door technologische ontwikkelingen, de decentralisaties, grote uitdagingen op het terrein van veiligheid en nieuwe Europese wetgeving. Daarom vinden wij het belangrijk om transparant te zijn over de manier waarop wij met persoonsgegevens omgaan en hoe wij de privacy waarborgen.

1. Wetgeving en definities
Op 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van toepassing geworden, samen met de Uitvoeringswet AVG. De AVG bouwt voort op de Wbp en zorgt onder andere voor versterking en uitbreiding van de privacyrechten met meer verantwoordelijkheden voor organisaties.

De volgende begrippen worden in de AVG gebruikt (Artikel 4, AVG):

Betrokkene: De betrokkene is degene van wie de gegevens worden verwerkt. Dat kan dus een inwoner zijn van de gemeente, maar het kan ook gaan om medewerkers van de gemeente.

Verwerker: De persoon of organisatie die de persoonsgegevens verwerkt in opdracht van een andere persoon of organisatie. Daarvan is bijvoorbeeld sprake wanneer wij een andere organisatie of een bedrijf inschakelen om bij een taak te ondersteunen of ten behoeve daarvan software te leveren.

Persoonsgegevens: Alle gegevens die gaan over mensen en waaraan je een mens als individu kunt herkennen.

Gegevensbeschermingseffectbeoordeling : Met een gegevensbeschermingseffectbeoordeling worden de effecten en risico's van de nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de persoonsgegevens.[2]

Verwerkingsverantwoordelijke: Een persoon of instantie die alleen, of samen met een ander, het doel en de middelen voor de verwerking van persoonsgegevens vaststelt. Meestal zijn wij dat als gemeente/overheid.

Verwerking: Een verwerking is alles wat je met een persoonsgegeven doet, zoals: vastleggen, bewaren, verzamelen, bij elkaar voegen, verstrekken aan een ander, of vernietigen.

2. Reikwijdte
Het reglement is van toepassing op alle verwerkingen van persoonsgegevens door alle bestuursorganen van de gemeente. Oftewel: voor alle verwerkingen die binnen de gemeente en de gemeentelijke organisatie plaatsvinden.

3. Verantwoordelijke
De bestuursorganen van de gemeente zijn allemaal verantwoordelijke voor de verwerkingen die door of namens de gemeente worden uitgevoerd. De bestuursorganen van de gemeente zijn onder andere de burgemeester, het college van Burgemeesters en Wethouders (college van B&W) en de Raad. Ook de gemeente als persoon kan verantwoordelijke zijn, bijvoorbeeld in geval van verwerkingen die plaatsvinden ter uitvoering van een overeenkomst.

Wij delen persoonsgegevens die aan ons worden verstrekt altijd met de BAR-organisatie. Alle medewerkers van de gemeente zijn immers in dienst van de BAR-organisatie en zij hebben de taak alle wettelijke taken en het beleid van de gemeente uit te voeren. Het is daarom onvermijdelijk dat gegevens altijd worden gedeeld met die BAR-organisatie. Dat doen wij in het kader van de uitoefening van onze

2) https://www.ibdgemeenten.nl/wp-content/uploads/2014/04/14-0404-Toelichting-PIA-v1.0.pdf

taak in het algemeen belang en in het kader van de uitoefening van het openbaar gezag, op grond van de Gemeenschappelijke regeling BAR-organisatie.

4. Verwerkingen (Artikel 4, AVG)
De verwerking van persoonsgegevens is elke handeling of elk geheel van handelingen met persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde processen. In de AVG valt onder een verwerking in ieder geval het:
- Verzamelen, vastleggen en ordenen
- Bewaren, bijwerken en wijzigen
- Opvragen, raadplegen, gebruiken
- Verstrekken door middel van doorzending
- Verspreiding of enige andere vorm van ter beschikkingstellen
- Samenbrengen, met elkaar in verband brengen
- Afschermen, uitwissen of vernietigen van gegevens

Uit deze opsomming blijkt dat alles wat je met een persoonsgegeven doet een verwerking is.

De gemeente verwerkt een veelheid aan soorten persoonsgegevens. Dat doen wij ofwel in het kader van aan ons opgedragen wettelijke taken, ofwel bij de uitvoering van taken in het algemeen belang. De soort gegevens die wij verwerken hangt daarmee af van de soort wettelijke taak. Welke gegevens wij precies verwerken voor welke taak, kunt u vinden in het verwerkingsregister. Wij zorgen er voor dat dit register beschikbaar is via de gemeentelijke site.

Als voorbeelden van soorten persoonsgegevens noemen wij (niet uitputtend):
- NAW gegevens (Naam, Adres, Woonplaats) bij bijvoorbeeld klachten of andere contactmomenten met de gemeente;
- Overige contactgegevens (e-mailadres, telefoonnummer e.d.);
- Gegevens over de gezondheid van inwoners, bijvoorbeeld bij de uitvoering van de Wmo 2015;
- Gegevens over de burgerlijke staat van inwoners en over de gezinssamenstelling (bij de uitvoering van de taken in het kader van de Wet basisregistratie personen, voorheen de GBA);
- Gegevens over financiële zaken, bijvoorbeeld bij de uitvoering van de Participatiewet.

In al deze gevallen moet worden voldaan aan de bepalingen in de AVG en is dit reglement van toepassing.

Doeleinden (Artikel 5, AVG)
Volgens de wet mogen wij persoonsgegevens alleen verzamelen als daarvoor een doel is vastgesteld. Het doel moet uitdrukkelijk omschreven en gerechtvaardigd zijn.
Wij mogen die gegevens in beginsel niet voor andere doelen verwerken. Wanneer wij persoonsgegevens wel voor een ander doel verwerken, dan gebeurt dat alleen wanneer het doel van die verwerking verenigbaar is met het oorspronkelijke doel en met inachtneming van het bepaalde in artikel 6, lid 4 AVG. Daarvan kan bijvoorbeeld sprake zijn wanneer gegevens die zijn verzameld in verband met de wettelijke taak het persoons- of Woz-register bij te houden, soms worden gebruikt voor het aanschrijven van (doel)groepen in verband met een andere taak in het algemeen belang: bijvoorbeeld het aanschrijven van inwoners in verband met werkzaamheden die plaats zullen vinden in de nabije leefomgeving. Of inwoners die de Aow gerechtigde leeftijd benaderen om hen te informeren over aanstaande of gewijzigde rechten die verband houden met het bereiken van die leeftijd. Dat is een verwerkingen die in het algemeen belang is, en daarmee voldoende aansluiten bij taken die gemeenten hebben.
De gemeente maakt in dergelijke gevallen echter altijd een afweging of het gebruik van dergelijke gegevens voor een ander doel, voldoende aansluit bij de taken en verplichtingen die de gemeente heeft.

Wij verwerken persoonsgegevens bijna altijd vanwege de doelmatige en rechtmatige uitvoering van een wettelijke taak of taak in het algemeen belang. Daarmee is in de meeste gevallen een gerechtvaardigde verwerking gegeven.
Voor de uitvoering van sommige wetten, zoals bijvoorbeeld de Jeugdwet, de Wmo en de Participatiewet zijn de doelen van het verwerken van persoonsgegevens ook in de wet vastgelegd, net als de persoonsgegevens die gevraagd en verwerkt mogen worden.

Het kan echter gebeuren dat wij persoonsgegevens verwerken op grond van een andere wettelijke grondslag, zoals toestemming (bijvoorbeeld bij nieuwsbrieven of enquêtes) of het gerechtvaardigd belang (bijvoorbeeld bezoekersregistratie of cameratoezicht in openbare ruimten). Wij geven het in die gevallen aan wanneer daar sprake van is.

Rechtmatige grondslag (Artikel 6, AVG)
De wet zegt dat er voor elke verwerking van persoonsgegevens een rechtmatige grondslag uit de wet van toepassing moet zijn. Dat betekent dat de verwerking alleen mag plaatsvinden:

- Om een verplichting na te komen die in de wet staat, zoals de nadrukkelijke verplichting voor gemeenten te zorgen voor een minimum inkomen (Participatiewet) of het afgeven van een gehandicaptenparkeerkaart (Wegenverkeerswet).
- Voor de uitvoering van een overeenkomst waar de betrokkene onderdeel is, zoals huurovereenkomsten voor ruimten of koopovereenkomsten voor bijvoorbeeld onroerende zaken.
- Voor de vervulling van een taak in het algemeen belang (wettelijke taken) of de uitoefening van het openbaar gezag, zoals wanneer sprake is van (feitelijke) handhaving van de openbare orde. Daarover meer onder het kopje 'Inzet van camera's'.
- Wanneer de betrokkene toestemming heeft gegeven voor de specifieke verwerking, zoals bij de verzending van nieuwsbrieven of het uitvoeren van enquêtes.

Wijze van verwerking
De hoofdregel van de verwerking van persoonsgegevens is dat het alleen toegestaan is in overeenstemming met de wet en op een zorgvuldige wijze. Persoonsgegevens worden zoveel mogelijk verzameld bij de betrokkene zelf. De wet gaat uit van subsidiariteit. Dat betekent dat een verwerking alleen is toegestaan wanneer het doel niet op een andere manier kan worden bereikt. In de wet wordt ook gesproken over proportionaliteit. Dit betekent dat persoonsgegevens alleen mogen worden verwerkt als dit in verhouding staat tot het doel. Wanneer zonder, of met minder (belastende), persoonsgegevens hetzelfde doel bereikt kan worden moet daarvoor gekozen worden.

Wij zorgen ervoor dat de persoonsgegevens kloppen en volledig zijn voordat ze verwerkt worden. Persoonsgegevens worden alleen verwerkt door medewerkers belast met de uitvoering van een (wettelijke) taak en met een geheimhoudingsplicht. Medewerkers van de gemeente hebben een dergelijke verplichting overigens op grond van de Ambtenarenwet en de Algemene wet bestuursrecht.

Daarnaast beveiligt de gemeente alle persoonsgegevens. Dit moet voorkomen dat de persoonsgegevens kunnen worden ingezien of gewijzigd door iemand die daar geen recht toe heeft. Hoe de gemeente daar vorm aan geeft staat in het informatiebeveiligingsbeleid van de gemeente, in de BIG en in een eventueel aanvullend beveiligingsplan specifiek opgesteld voor een proces of registratie.

Net als vele andere partijen maakt de gemeente gebruik van software en applicaties. Daarbij komt het voor dat persoonsgegevens worden gedeeld met derden, zoals softwareleveranciers en datacentra. De gemeente zorgt in die gevallen voor goede en duidelijke afspraken met die derden en controleert deze.

Doorgifte (Artikel 44 t/m 50, AVG)
De gemeente geeft geen persoonsgegevens door aan een land buiten de Europese Economische Ruimte (EER) of een internationale organisatie. Het kan wel voorkomen dat er gegevens van inwoners buiten de EER worden gebracht. Het gaat in dat geval om fraudeonderzoeken in het kader van de uitvoering van wettelijke taken. Dergelijk onderzoek doet de gemeente echter niet zelf, maar het UWV.

5. Transparantie en communicatie

Wet openbaarheid van bestuur (Wob)

Via de Wob[3] (en straks wellicht de Wet Open Overheid) kun je een verzoek om informatie indienen bij de gemeente. Bij het verzoek bekijken wij altijd of het gevraagde document geen inbreuk maakt op de persoonlijke levenssfeer van inwoners of andere derden. In beginsel worden in het kader van openbaarmakingen geen persoonsgegevens geopenbaard. In uitzonderingsgevallen vindt dat echter wel plaats, bijvoorbeeld omdat de publieke informatievoorziening daarom vraagt. Het belang van de openbaarheid weegt dan zwaarder dan het belang dat met de bescherming van de persoonlijke levenssfeer is gemoeid. De betrokkenen worden dan, voor zover zij bereikbaar zijn, in dat geval van tevoren op de hoogte gebracht.

Dit uitgangspunt geldt zowel voor wat betreft openbaarheid op verzoek als voor openbaarheid uit eigen beweging.

Wet hergebruik van overheidsinformatie

De Wet hergebruik van overheidsinformatie[4] regelt het op verzoek verstrekken van overheidsinformatie voor hergebruik, bijvoorbeeld gegevens uit bodemrapportages. Bij het verzoek bekijkt de gemeente altijd of het antwoord geen inbreuk maakt op de persoonlijke levenssfeer van betrokkenen. In principe worden geen persoonsgegevens voor hergebruik aan derden verstrekt.

3) http://wetten.overheid.nl/BWBR0005252/2016-10-01
4) http://wetten.overheid.nl/BWBR0036795/2016-10-01

Transparantie bij rechtsbescherming
Wij nemen als overheid besluiten waartegen bezwaar en beroep kan worden ingediend. Bezwaarzaken worden behandeld door de bezwaarschriftencommissie en beroepszaken door de rechtbank. In dergelijke dossiers kunnen natuurlijk ook persoonsgegevens voorkomen. Dat is geen probleem wanneer er sprake is van – bijvoorbeeld – een bezwaar tegen een persoonsgebonden beschikking, zoals bijvoorbeeld een besluit in verband met een uitkering. In dat geval zijn alleen de gegevens van degene die beschikking heeft gevraagd en daar bezwaar tegen maakt in het dossier opgenomen.

Wanneer er echter sprake is van een besluit waar meerdere belanghebbenden bij zijn betrokken, bijvoorbeeld wanneer er bezwaar wordt gemaakt tegen een aangevraagde omgevingsvergunning voor bouwen, kan er een probleem ontstaan op het gebied van de bescherming van persoonsgegevens. Op grond van het recht heeft de houder van een vergunning er immers recht op om te weten dat zijn vergunning is aangevraagd en wat daar de redenen voor zijn. Die rechtsverplichting kan ook een probleem zijn bij een handhavingsverzoek.

Wij kiezen er in een dergelijk geval voor om het recht op informatie voor rechtszoekenden voor te laten gaan op het recht op de bescherming van persoonsgegevens. Wij schonen dergelijke dossiers niet voor wat betreft de namen en gegevens van belanghebbenden. Wij schonen dergelijke dossiers wél voor wat betreft de persoonsgegevens derden belanghebbenden en betrokkenen wiens gegevens niet relevant zijn voor de behandeling van het bezwaar, dan wel het beroep.

Informatieplicht (Artikel 13, 14, AVG)
Wij informeren onze inwoners over het verwerken van persoonsgegevens. Op de gemeentelijke website staat bijvoorbeeld een privacyverklaring, ons verwerkingsregister en ook dit reglement dient dat doel. Wanneer betrokkenen gegevens aan ons verstrekken, worden zij op de hoogte gebracht van de manier waarop wij met persoonsgegevens om gaan. Dit kan bijvoorbeeld via een formulier gebeuren. Vaak staat op de aanvraagformulieren ook vermeld welke gegevens zonder toestemming niet openbaar zullen worden gemaakt. De betrokkene wordt niet nogmaals geïnformeerd als hij/zij al weet dat de gemeente persoonsgegevens van de betrokkene verzamelt en verwerkt, en weet waarom en voor welk doel dat gebeurt.

Wanneer de persoonsgegevens via een andere weg worden verkregen, dus buiten de betrokkene om, wordt de betrokkene geïnformeerd op het moment dat deze voor de eerste keer door ons worden verwerkt. Dat geldt overigens niet wanneer wij gegevens verkrijgen via andere overheden die verplicht zijn om deze gegevens met ons te delen, ofwel wij verplicht zijn deze gegevens van hen te vragen.[5] Daarvan is bijvoorbeeld sprake bij gegevensdelingen met de Belastingdienst of het Uwv. In die gevallen blijkt al uit de wet dat deze gegevensdelingen plaatsvinden en **informeren wij de betrokkene niet** afzonderlijk.

Verwijdering
Wij bewaren de persoonsgegevens niet langer dan nodig is voor de uitvoering van gemeentelijke taken, of zoals vastgelegd op grond van de Archiefwet. Wanneer er nog persoonsgegevens opgeslagen zijn die niet langer nodig zijn voor het bereiken van het doel, worden deze zo snel mogelijk verwijderd. Dit houdt in dat deze gegevens vernietigd worden, of zo worden aangepast dat de informatie niet meer gebruikt kan worden om iemand te identificeren en dus wordt geanonimiseerd.

Hoe lang gegevens mogen worden bewaard is niet altijd makkelijk te vinden. Daarom maken wij gebruik van een zaak- en archiefsysteem, waarin de wettelijke bewaartermijnen zijn opgenomen. Wij zorgen er daarom voor dat verkregen informatie zo veel als mogelijk binnen dat zaaksysteem worden opgeslagen. Wij dragen er daarnaast zorg voor dat gegevens zo min als mogelijk op andere plaatsen worden opgeslagen, zoals netwerkschijven en mobiele gegevensdragers (usb sticks e.d.).

In geval wij werken met systemen die niet geschikt zijn als bewaarplaats van (archiefwaardige) gegevens, zorgen wij er per geval voor dat gegevens niet langer dan noodzakelijk worden bewaard.

Rechten van betrokkenen (Artikel 13 t/m 20, AVG)
De wet bepaalt niet alleen de plichten van degenen die de persoonsgegevens verwerken, maar bepaalt ook de rechten van de personen over wie de persoonsgegevens worden verwerkt. Deze rechten worden ook wel de rechten van betrokkenen genoemd, en bestaan uit de volgende rechten:

- Recht op informatie: Betrokkenen hebben het recht om aan ons te vragen of zijn/haar persoonsgegevens worden verwerkt.
- Inzagerecht: Betrokkenen hebben de mogelijkheid om te controleren of, en op welke manier, zijn/haar gegevens worden verwerkt.

5) Zie voor meer informatie bijvoorbeeld: https://www.digitaleoverheid.nl/dossiers/basisregistraties/

- Correctierecht: Als duidelijk wordt dat de gegevens niet kloppen, kan de betrokkene een verzoek indienen bij de gemeente om dit te corrigeren.
- Recht op beperking van de verwerking: Betrokkenen hebben het recht aan de gemeente te vragen om hun persoonsgegevens niet meer te gebruiken.
- Recht om vergeten te worden: In gevallen waar de betrokkene toestemming heeft gegeven om persoonsgegevens te verwerken, heeft de betrokkene het recht om de persoonsgegevens te laten verwijderen.
- Recht op bezwaar: Betrokkenen hebben het recht om bezwaar te maken tegen de verwerking van zijn/haar persoonsgegevens. De gemeente zal hieraan voldoen, tenzij er gerechtvaardigde gronden zijn voor de verwerking.

Indienen van verzoek
Wanneer een inwoner gebruik wil maken van zijn of haar rechten, dan moet daartoe een verzoek worden ingediend (zie hiertoe artikel 34 UAVG). Dit verzoek kan zowel schriftelijk als via de formulieren via de gemeentelijke website ingediend worden. Wij moeten op zo'n verzoek binnen een maand beslissen. Als het verzoek niet wordt opgevolgd, is er de mogelijkheid om bezwaar te maken bij de gemeente, of een klacht in te dienen bij de Autoriteit Persoonsgegevens (AP).

Bij een verzoek om een van de rechten uit te oefenen, moeten wij in staat zijn de identiteit van de verzoeker vast te stellen. Dat kan gemakkelijk, wanneer er gebruik wordt gemaakt van een webformulier in combinatie met een inlog via DigiD. Wanneer een verzoek schriftelijk wordt ingediend, kan hierbij een kopie worden toegevoegd van een ID bewijs. In andere gevallen beoordelen wij of en in hoeverre aan deze identificatieplicht is voldaan.

6. Geautomatiseerde verwerkingen

Profilering (Artikel 22, AVG)
Profilering vindt plaats wanneer er een geautomatiseerde verwerking van persoonsgegevens plaatsvindt waarbij aan de hand van persoonsgegevens naar bepaalde persoonlijke aspecten van een persoon wordt gekeken om deze persoon te categoriseren en te analyseren, of om zaken te kunnen voorspellen. Voorbeelden van persoonlijke aspecten kunnen zijn; financiële situatie, interesses, gedrag of locatie.

Om profilering wat duidelijker te maken geven wij het volgende fictieve voorbeeld. Het kan voorkomen dat een bezoeker van onze website geregeld op bepaalde onderdelen klikt, bijvoorbeeld de vereisten voor een horecavergunning en die over schuldhulpverlening. Het is de gemeente dan niet toegestaan om – wanneer die bezoeker een aanvraag voor een horecavergunning indient – het profiel van die bezoeker met dat klikgedrag (wat wij overigens niet bijhouden) bij die aanvraag te betrekken. Meer concreet: het klikgedrag van een bezoeker op het onderdeel 'schuldhulpverlening' mag niet worden meegenomen bij de beoordeling van de aanvraag voor de horecavergunning.

Wij mogen wel bekijken hoe vaak een bepaalde dienst bekeken is, om die dienst te verbeteren. Wij mogen echter niet, aan de hand van de klicks op de site een profiel maken en gericht daarop acteren, voor zover dat van invloed is op de rechtspositie van een betrokkene. Daarnaast geeft de AVG aan dat er geen besluit mag worden genomen op basis van profilering, zonder dat daar op grond van een wettelijke bepaling toestemming voor is gegeven.

Wij maken overigens geen gebruik van profilering in deze zin.

Big data en tracking
Door middel van Big data onderzoek en tracking mogen alleen gegevens worden verwerkt wanneer deze niet herleidbaar zijn tot een natuurlijk persoon. Het gaat dan om louter statistische gegevens en niet meer om persoonsgegevens. Daarnaast worden deze gegevens alleen verzameld voor onderzoek dat door, of namens, ons wordt uitgevoerd.

Inzet van camera's
Binnen de gemeente wordt onder bepaalde omstandigheden gebruik gemaakt van cameratoezicht, zoals vastgelegd in de Gemeentewet en camerabewaking. Cameratoezicht wordt onder andere gebruikt voor het vergroten van de veiligheid op straat.[6] Camera's kunnen een grote inbreuk maken op de privacy van diegene 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.

Het gebruik van camera's door particulieren is alleen toegestaan om zaken en goederen te bewaken. Het is niet toegestaan om vanaf een particulier terrein de openbare weg te filmen, tenzij het niet anders

6) http://wetten.overheid.nl/BWBR0005416/2017-01-01

kan. In een dergelijk geval moet hier toestemming voor worden gevraagd aan het college. Dan worden er tussen hen en de betrokken eigenaar afspraken gemaakt (convenant). In die afspraken worden dan o.a. de grondslag, het doel, de maatregelen tegen verlies, en de bewaartermijn vastgelegd. Ook wijst het college de betrokken eigenaar dan op de verplichtingen die op hem rusten in het kader van de AVG.

Wij maken gebruik van cameratoezicht onder de volgende voorwaarden:

- Er moet sprake (geweest) zijn van regelmatige vernieling van in de openbare ruimte staande objecten of gebouwen.
- Er moet sprake zijn (geweest) van regelmatige verstoring van de openbare orde.

7. Plichten van de gemeente

Register van verwerkingen (Artikel 30, AVG)
Wij zijn verantwoordelijk voor het aanleggen van een register van alle verwerkingen waarvan de gemeente de verwerkingsverantwoordelijke is. Dat register bevat een beschrijving van wat er tijdens een verwerking plaatsvindt, en welke gegevens daarvoor worden gebruikt, namelijk:

- De naam en contactgegevens van de verwerkingsverantwoordelijke en, mogelijk, de gezamenlijke verwerkingsverantwoordelijke;
- De doelen van de verwerking;
- De rechtsgrond van de verwerking
- Een beschrijving van het soort persoonsgegevens en de daarbij horende betrokkenen;
- Een beschrijving van de ontvangers van de persoonsgegevens;
- Een beschrijving van het delen van persoonsgegevens aan een derde land of internationale organisatie;
- De wettelijke bewaartermijnen voor de verzamelde gegevens.

Een verwerkingsregister kan ook een algemene beschrijving van de technische en organisatorische maatregelen bevatten, zoals bedoeld in artikel 32 AVG. De gemeente kiest daar niet voor. De wijze waarop wij informatieveiligheid vormgeven is opgenomen in het gemeentelijk informatieveiligheidsbeleid en de BIG. De verwerkingen in het register sluiten daar vanzelfsprekend op aan. Dit register is overigens te vinden op de website van de gemeente.

Aanstellen van een Functionaris voor gegevensbescherming (FG) (Artikel 37 t/m 39, AVG)
Wij hebben een FG aangesteld. De FG is betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. De taken van de functionaris zijn informeren, adviseren, toezicht houden, bewustwording creëren, en optreden als contactpersoon van de AP.

Het is niet de bedoeling dat de functionaris de taken op het gebied van bescherming van de privacy van de organisatie overneemt. Wij hebben een eigen verantwoordelijkheid in het goed omgaan met de persoonsgegevens. De FG is verantwoordelijk voor het structureel toetsen van de implementatie en de uitvoering van de wettelijke eisen en de gemeentelijke richtlijnen op het gebied van privacy.

Voor vragen over privacy of andere zaken (zoals dit reglement) kan contact worden gezocht met onze Functionaris Gegevensbescherming. Dat kan via het mailadres FG@albrandswaard.nl.

Datalekken (Artikel 33 en 34, AVG)
We spreken van een datalek wanneer persoonsgegevens ongewild in handen vallen van derden die geen toegang tot die gegevens mogen hebben. Daar kan bijvoorbeeld al sprake van zijn wanneer een e-mail of een poststuk bij een verkeerde ontvanger terecht komt. Daar is ook sprake van bij een hack op een database.

Vermoedens van datalekken worden intern gemeld via Topdesk.[7] Een dergelijk vermoeden wordt dan beoordeeld door de CISO en de Privacy Officer en zo nodig gemeld bij de AP. Dat doen wij dan zonder onredelijke vertraging, uiterlijk 72 uur nadat er kennis van de inbreuk is vernomen. Als dit later dan 72 uur is, wordt er een motivering voor de vertraging bij de melding gevoegd. Het kan zijn dat de inbreuk een hoog risico met zich meebrengt voor de rechten en vrijheden van de betrokkenen. In dit geval melden wij dit aan de betrokkenen in eenvoudige en duidelijke taal. Om toekomstige datalekken te voorkomen worden bestaande datalekken geëvalueerd.

Het is niet altijd eenvoudig om een datalek te herkennen. Daarom is het van belang om bij een vermoeden van een datalek contact op te nemen met de betrokken functionarissen. Dat kan – voor burgers en andere derden – via de FG van de gemeente. Medewerkers kunnen een vermoedelijk datalek, zoals

7) Zie: https://intranet.bar-organisatie.nl/umbraco/weten-en-regelen/informatieveiligheid-en-privacy/datalek/.

aangegeven, melden via het intranet. Daar kun je ook voorbeelden vinden van datalekken. Ook is het niet zo dat ieder datalek bij de AP moet worden gemeld. Daarom is het goed om de beoordeling daarvan door onze specialisten te laten plaatsvinden.

Afsluiting
Als de gemeente een wettelijke verplichting niet nakomt, kan de betrokkene een klacht indienen. Deze zal via de klachtenregeling van de gemeente worden behandeld. In gevallen waar het reglement niets over zegt, beslist het verantwoordelijke bestuursorgaan van de gemeente.

Daarnaast kan een betrokkene klagen bij de Autoriteit Persoonsgegevens. Voor meer informatie daarover kunt u terecht op de site van de Autoriteit: https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/privacyrechten/klacht-indienen-bij-de-ap

Disclaimer:
Dit product is een eenvoudige en begrijpelijke vertaling van de huidige privacyregelgeving en gegrond op de AVG. Vanzelfsprekend is de toepasbare wet- en regelgeving altijd leidend en kunnen er geen rechten ontleend worden aan dit document.

Bijlage 2 Convenant gegevensverwerking tussen de gemeente Albrandswaard en de BAR-organisatie

Inleiding
Met de oprichting van de BAR-organisatie in 2014 is vrijwel al het gemeentelijk personeel in dienst getreden van de BAR-organisatie. Formeel is dat een derde ten opzichte van de gemeenten. Feitelijk is er echter nauwelijks onderscheid te maken tussen de gemeenten en de BAR-organisatie. Niettemin moeten wij uitgaan van de formele werkelijkheid: de BAR-organisatie als afzonderlijke organisatie.

Omdat er formeel sprake is van een andere organisatie, is het van belang om heldere afspraken te maken over de verdeling van verantwoordelijkheden. Dat voorkomt onduidelijkheid voor zowel de inwoners van de gemeenten, als voor de organisatie zélf. De noodzaak tot een dergelijke goede omschrijving wordt nog eens extra ingegeven door de vele eisen die voortvloeien uit de wet- en regelgeving in het kader van informatieveiligheid en privacy. Uit dat laatste vloeit voort, dat de gemeenten en de BAR-organisatie tezamen verantwoordelijke zijn voor de verwerking van persoonsgegevens. Dat komt omdat de colleges nog altijd dragers zijn van alle wettelijke bevoegdheden, maar deze bevoegdheden in zeer veel gevallen feitelijk – in mandaat – worden vervuld door de medewerkers van de BAR-organisatie. Daarbij wordt tevens gebruik gemaakt van het netwerk en de systemen van die BAR-organisatie.

Dit convenant is bedoeld om duidelijkheid te scheppen in de onderlinge verantwoordelijkheden. Duidelijkheid voor de interne organisatie. Die duidelijkheid moet ook worden gegeven op grond van artikel 26 van de AVG. Dit convenant volgt de structuur van dit artikel en geeft afspraken in hoofdlijnen weer. Bovendien zijn deze afspraken strikt beperkt tot de werking van de AVG en tot het daarmee samenhangende terrein van informatieveiligheid.

Dit convenant gaat niet over de verdeling van bevoegdheden in de zin van de Awb. Dat is binnen de verhouding geregeld via mandaten en daaraan kan dit stuk geen afbreuk doen. Dit convenant gaat uit de feitelijke situatie zoals deze is gegroeid sinds de oprichting van de BAR-organisatie. Met het vaststellen van dit convenant wordt de BAR-organisatie niet plotseling bevoegd om – net als de gemeenten – wettelijke taken zelfstandig uit te voeren. Dat blijft allemaal bij de gemeenten.

De wettelijke grondslag voor dit convenant is gelegen in het hiervoor aangehaalde artikel 26 AVG, de uitspraken van de jurisprudentie van het Europees Hof van Justitie van 5 juni 2018 en 10 juli 2018,[8] in samenhang met het bepaalde in artikel 4, lid 1 en artikel 5 van de Gemeenschappelijke Regeling BAR-organisatie.

1 Gezamenlijke verantwoordelijkheid

1.1 Gemeenten en de BAR-organisatie
De gemeenten en de BAR-organisatie zijn verantwoordelijk voor alle verwerkingen die plaatsvinden ten behoeve van de uitoefening van wettelijke taken, als bedoeld in artikel 4, lid 3 van de Gemeenschappelijke Regeling BAR-organisatie. De taken als bedoeld worden in veruit de meeste gevallen uitgevoerd door middel van elektronische dan wel geautomatiseerde systemen, die worden beheerd door het bestuur van de BAR-organisatie.

1.1.1 De beheerstaak van de BAR-organisatie
Het dagelijks bestuur van de BAR-organisatie heeft de taak de gehele ICT infrastructuur van de gemeenten en de BAR-organisatie te beheren en te beveiligen. Die infrastructuur omvat zowel hardware als software. Onder dat beheer wordt verstaan dat het bestuur er voor zorgdraagt dat afspraken over de beschikbaarheid, vertrouwelijkheid en integriteit van de infrastructuur en de daarop verwerkte data worden behaald. Het bestuur draagt zorg voor een efficiënte inkoop en beveiliging op het gebied van ICT en zorgt – daar waar noodzakelijk – voor afstemming met de betrokken organen van de gemeenten. Het bestuur van de gemeenten is aansprakelijk voor de op de ICT infrastructuur verwerkte en opgeslagen gegevens.

1.2 Interne verantwoording verwerkingen
Het dagelijks bestuur van de BAR-organisatie is ervoor verantwoordelijk om het bestuur van de gemeenten – indien er sprake is van beveiligingsincidenten – in algemene zin, dan wel in afzonderlijke gevallen van die incidenten op de hoogte te stellen. Het dagelijks bestuur heeft voor de uitoefening van deze taak een functionaris aangewezen. Die functionaris staat bekend als Chief Information Security Officer (CISO).

8) HvJ EU 5 juni 2018, C-210/16, ECLI:EU:C:2018:388 (Wirtschaftsakademie Schleswig-Holstein GmbH) en HvJ EU 10 juli 2018, C-25/17, ECLI:EU:C:2018:551 (Jehovan todistajat).

1.2.1 Externe verantwoording verwerkingen
Het bestuur van de gemeenten blijft voor haar inwoners de eerst aansprakelijke voor de verwerking van persoonsgegevens, ook wanneer deze verwerkingen plaatsvinden via de systemen die worden beheerd door het bestuur van de BAR-organisatie.

1.2.2 Externe verantwoording bij incidenten
Indien er sprake is van een beveiligingsmaatregel die dient ter voorkoming van het verlies van, de aantasting van of anderszins bescherming van persoonsgegevens of andere data die noodzakelijk blijkt voor de gemeentelijke dienstverlening, legt de voorzitter van het dagelijks bestuur van de BAR-organisatie daarover verklaringen af. Het gaat hierbij om eventuele publieke verklaringen die worden afgelegd ten behoeve van en namens de gemeenten en de BAR-organisatie. De voorzitter zorgt daarbij voor een doelmatige en effectieve communicatie en maakt daarbij gebruik van de op dat moment meest effectieve communicatiemiddelen.

1.3 Uitoefening rechten door burgers
Het bestuur van de gemeenten blijft te allen tijde het aanspreekpunt voor burgers. Het uitoefenen van de rechten die de inwoners toekomen, vindt plaats via het bestuur van de gemeenten. Verzoeken worden dus altijd ingediend bij de betreffende gemeente, maar worden feitelijk afgehandeld door de BAR-organisatie namens die gemeente. Hiervoor heeft de BAR-organisatie de nodige procedures ontwikkeld en in werking gesteld.

1.3.1 Uitoefening rechten door medewerkers BAR-organisatie
Het dagelijks bestuur van de BAR-organisatie is verantwoordelijk voor de uitoefening van de rechten van medewerkers. Verzoeken van medewerkers worden ingediend bij de BAR-organisatie.

1.3.1.1 Uitoefening rechten door andere medewerkers
Verzoeken van medewerkers van de gemeenten, met name die werkzaam zijn bij de griffies van de gemeenten en leden van organen van de gemeenten die geen deelnemers zijn aan de Gemeenschappelijke Regeling, vallen onder de verantwoordelijkheid van de betreffende gemeente. Dergelijke verzoeken worden dus gericht tot de gemeenten, maar worden feitelijk afgehandeld door de BAR-organisatie namens die gemeente.

2 Verantwoordelijkheid voor beveiligingsmaatregelen

2.1 Verantwoordelijkheid dagelijks bestuur
Het dagelijks bestuur van de BAR-organisatie is belast met het beheer van de gehele ICT-infrastructuur. Daaronder vallen in ieder geval alle hardware en alle gemeenschappelijke software en cloud-oplossingen. De gemeenten en de BAR-organisatie maken daar gezamenlijk gebruik van. Het dagelijks bestuur is verantwoordelijk voor het treffen en in standhouden van de noodzakelijk beveiligingsmaatregelen, gelet op het bepaalde in artikel 32 AVG, de BIG en de kaders in het informatieveiligheidsbeleid van de BAR-organisatie en de gemeenten. Het dagelijks bestuur draagt zorg voor tijdige maatregelen en voldoende budget voor deze taak.

2.2 Interne verantwoording beveiligingsmaatregelen
Het dagelijks bestuur draagt zorg voor de verantwoording aan het bestuur van de gemeenten ten aanzien van taak als bedoeld onder 2.1 en 2.2.1. De BAR-organisatie heeft hiertoe een functionaris: de CISO.

2.2.1 Externe verantwoording beveiligingsmaatregelen
Het dagelijks bestuur van de BAR-organisatie is verantwoordelijk voor de externe verantwoording voor wat betreft de beveiligingsmaatregelen. Daaronder vallen in ieder geval de ENSIA-verantwoording en de implementatie van de BIG, dan wel de rechtsopvolgers van deze verantwoordingssystemen. De coördinerende en ondersteunende taak rondom deze verantwoording belegt het dagelijks bestuur bij de CISO.

3 Het verwerkingsregister
Het dagelijks bestuur is verantwoordelijk voor het opstellen en het beheer van het verwerkingsregister als bedoeld in artikel 30 AVG. Dat register bevat alle verwerkingen die plaatsvinden binnen de BAR-organisatie en de gemeenten. Dat register ziet derhalve ook op verwerkingen die plaatsvinden door de organen van de gemeenten en geldt als gemeenschappelijk verwerkingsregister. Het dagelijks bestuur draagt zorg voor de verstrekking van het verwerkingsregister aan de toezichthouder en geeft daarbij aan dat die verstrekking plaatsvindt namens de gemeenten en de BAR-organisatie. Het dagelijks bestuur zorgt namens de gemeenten ook voor een passende en adequate openbaarmaking van dit register.

4 Verwerkers

4.1 Register van verwerkers
Het dagelijks bestuur van de BAR-organisatie draagt zorg voor een registratie van verwerkers die – op welke wijze dan ook – gegevens verwerken namens de gemeenten, dan wel de BAR-organisatie en gebonden zijn aan de aanwijzing van hen als bedoeld in artikel 28, lid 3 AVG.

4.2 Inschakelen verwerkers
De BAR-organisatie en de gemeenten schakelen geen verwerkers in die niet voldoen aan de eisen als bedoeld in artikel 28, lid 1 AVG. Het bestuur van de BAR-organisatie is verantwoordelijk voor de selectie van dergelijke verwerkers. Het inschakelen van verwerkers die niet aan het bepaalde in artikel 28, lid 1 AVG voldoen vindt alleen plaats na voorafgaande instemming van het betrokken orgaan van de gemeente(n). De inschakeling van verwerkers op een andere wijze dan hier omschreven komt voor rekening en risico van het bestuur van de betrokken organisatie.

5 Gegevensbeschermingseffectbeoordeling
Het dagelijks bestuur van de BAR-organisatie is verantwoordelijk voor de uitvoering van gegevensbeschermingseffectbeoordelingen als bedoeld in artikel 35 AVG. Het bestuur van de BAR-organisatie voert een dergelijke beoordeling uit bij de ingebruikneming van nieuwe systemen die een nieuwe vorm of verfijning van gegevensverwerking tot gevolg hebben. Deze verantwoordelijkheid vloeit voort uit het hiervoor bepaalde onder 2.1.

6 Taakverdeling bij toezicht

6.1 Taakverdeling bij regulier extern toezicht
Het toezicht op de naleving van de AVG is belegd bij de Autoriteit Persoonsgegevens (AP). Alle verwerkingsverantwoordelijken kunnen met toezichtshandelingen van die AP worden geconfronteerd. Om op vragen effectief en efficiënt te reageren is een verdeling van taken noodzakelijk. Uitgangspunt daarbij is dat de aangesproken organisatie naar de AP reageert. Het bestuur van de BAR-organisatie is echter voor een dergelijke reactie namens de aangesprokene verantwoordelijk. Omdat het niet is uitgesloten dat de reactie van één gemeente gevolgen kan hebben voor de andere gemeenten, is afstemming daarvan in het dagelijks bestuur van de BAR-organisatie voor de hand liggend.

6.2 Taakverdeling bij sancties: dwangsommen
Indien de AP overgaat tot het opleggen van sancties naar aanleiding van de toezichttaak, is het dagelijks bestuur van de BAR-organisatie ervoor verantwoordelijk dat:
a. Indien daar gronden voor bestaan tegen, een dwangsombesluit tijdig rechtsmiddelen aan te wenden. Het dagelijks bestuur besluit niet tot een dergelijke rechtshandeling zonder daaraan voorafgaande instemming van het betreffende bestuursorgaan. Het dagelijks bestuur is echter wel zonder die instemming bevoegd om pro-forma rechtsmiddelen aan te wenden teneinde fatale termijnen te stuiten;
b. De met een dwangsombesluit opgelegde maatregelen, ook ingeval er gronden zijn om het besluit aan te vechten, tijdig uit te voeren teneinde het verbeuren van dat besluit te voorkomen;
c. Overige opgelegde bestuurlijke maatregelen uit te voeren en daarover namens het betrokken bestuursorgaan aan de AP te rapporteren.

6.3 Taakverdeling bij sancties: boeten
Indien de AP overgaat tot het opleggen van een bestraffende sanctie naar aanleiding van de toezichttaak, is het dagelijks bestuur van de BAR-organisatie ervoor verantwoordelijk dat:
a. Indien daar gronden voor bestaan, tegen een bestraffende sanctie tijdig rechtsmiddelen aan te wenden. Het dagelijks bestuur besluit niet tot een dergelijke rechtshandeling zonder daaraan voorafgaande instemming van het betreffende bestuursorgaan. Het dagelijks bestuur is echter wel zonder die instemming bevoegd om pro-forma rechtsmiddelen aan te wenden teneinde fatale termijnen te stuiten;
b. De noodzakelijke organisatorische en technische maatregelen te nemen waarop de bestraffende sanctie ziet, teneinde een herhaling of verhoging daarvan te voorkomen;

De organisatie waartoe de bestraffende sanctie is gericht, blijft verantwoordelijk voor het tijdig voldoen daarvan. Het bestuur van de BAR-organisatie voert hiertoe de nodige correspondentie met de AP namens de betrokken organisatie.

6.4 Verhaal van kosten voor maatregelen en sancties
De gemeenten en de BAR-organisatie verhalen onderling de kosten die worden gemaakt als gevolg van opgelegde bestuurlijke maatregelen en of sancties in de hiervoor onder 6.2 en 6.3 bedoelde zin, op gelijke wijze als beschreven onder paragraaf 7.3.

7 Aansprakelijkheid

7.1 Onderlinge aansprakelijkheid
Gezamenlijke verantwoordelijkheid betekent – gelet op het bepaalde in artikel 82, lid 4 AVG – gezamenlijke aansprakelijkheid. Het bestuur van de BAR-organisatie zorgt voor een snelle en efficiënte afhandeling van schadeclaims van inwoners, als gevolg van een onrechtmatige handeling in de zin van de AVG. Het bestuur van de BAR-organisatie doet dat zowel op eigen titel als namens één of meer deelnemende gemeenten. Het bestuur van de BAR-organisatie draagt zorg voor een adequate verzekering van het risico dat is gemoeid met het verwerken van persoonsgegevens middels geautomatiseerde systemen.

7.2 Schadeoorzaak en vergoeding
Schade die het gevolg is van een inbreuk op de AVG veroorzaakt door één van de collectief gebruikte systemen, wordt door het bestuur van de BAR-organisatie vergoed. Dat geldt eveneens voor schade die wordt veroorzaakt door een feitelijke handeling van medewerkers in dienst van of werkzaam onder de verantwoordelijkheid van het dagelijks bestuur van de BAR-organisatie.

Schade die het gevolg is van een inbreuk op de verordening veroorzaakt door een door de BAR-organisatie beheerd systeem dat niet bedoeld is voor collectief gebruik wordt eveneens door het bestuur van de BAR-organisatie vergoed en verhaald bij de betrokken gemeente, tot wie het verzoek tot schadevergoeding was gericht.

7.3 Onderling verhaal
Uitgekeerde vergoeding van schade wordt – voor zover dit niet in het hier voorgaande afdoende is geregeld – in de gevallen als bedoeld onder 7.2, eerste volzin, onderling verhaald conform de gebruikelijke verdeelsleutel 1:2:2. Schade veroorzaakt door feitelijke handelingen van medewerkers in dienst van, dan wel werkzaam onder de verantwoordelijkheid van het dagelijks bestuur wordt niet verhaald bij de gemeenten.

Bijlage 3 Mandaatbesluit

Het college van burgemeester en wethouders, de burgemeester en de raad van de gemeente Albrandswaard, ieders voor zover het diens bevoegdheid betreft;

Gezien het besluit van d.d. 17 december 2013 (Mandaatregeling Albrandswaard);

Gezien het besluit van d.d. 3 juli 2018 (mandaatbesluit AVG Albrandswaard);

Gelet op het bepaalde in de Algemene verordening gegevensbescherming (Verordening EU 2016/679 van het Europees Parlement en de Raad van 27 april 2016, hierna: AVG) en Afdeling 10.1.1 van de Algemene wet bestuursrecht,

BESLUIT

1. Mandaat uitvoering AVG

1.1 Het hoofd van de afdeling waarbinnen persoonsgegevens worden verwerkt is gemandateerd, gemachtigd, dan wel gevolmachtigd om alle bevoegdheden uit te oefenen namens de verwerkingsverantwoordelijken binnen de gemeente Albrandswaard die voortvloeien uit de AVG.

1.2 Het bepaalde in lid 1 geldt niet voor wat betreft de uitoefening van de bevoegdheden uit de AVG die zijn opgenomen in Hoofdstuk III, Afdeling 2 van de AVG, zoals deze eerder zijn gemandateerd aan de hoofden van de afdelingen van de BAR-organisatie.

1.3 Het bepaalde in lid 1 geldt niet voor wat betreft de uitoefening van de bevoegdheden van artikel 32 van de AVG.

1.4 Het bepaalde in lid 1 geldt niet voor wat betreft de te geven reacties op handelingen en besluiten van de Autoriteit Persoonsgegevens, als bedoeld in artikel 83 AVG. Het bepaalde in artikel 1.1 is wel van toepassing op handelingen en besluiten van de Autoriteit Persoonsgegevens als bedoeld in artikel 58 AVG, met dien verstande dat te geven reacties vooraf worden besproken met de betrokken portefeuillehouder, dan wel gemeentesecretaris.

1.5 Het bepaalde in lid 1 is niet van toepassing op het bepaalde in Afdeling 4 van Hoofdstuk IV van de AVG (Functionaris Gegevensbescherming).

1.6 Het bepaalde in lid 1 is niet van toepassing op het bepaalde in artikel 24, lid 2 AVG.

1.7 In afwijking van het bepaalde in lid 1 is de manager van de afdeling Informatiemanagement bevoegd het verwerkingsregister als bedoeld in artikel 30 AVG vast te stellen en te actualiseren.

1.8 De bevoegdheid tot het sluiten van verwerkingsovereenkomsten als bedoeld in artikel 28 van de AVG wordt niet uitgeoefend zonder daaraan voorafgaand overleg met de betrokken portefeuillehouder, dan wel gemeentesecretaris.

1.9 De gemandateerde is bevoegd tot het afgeven van ondermandaat.

2. Bevoegdheid tot het treffen van technische en organisatorische maatregelen

2.1 De bevoegdheid en verantwoordelijkheid om namens de verwerkingsverantwoordelijke alle technische en organisatorische maatregelen te treffen als bedoeld in artikel 32 van de AVG, de BIG en het informatiebeveiligingsbeleid van de gemeente(n)/BAR-organisatie is belegd bij de manager van de betrokken afdeling.

2.2 De bevoegdheid als bedoeld in artikel 2.1 omvat niet het maken van de afwegingen als bedoeld in artikel 32, lid 1, 1e volzin AVG. Deze bevoegdheid wordt exclusief belegd bij de managers van de afdeling Automatisering en Informatiemanagement.

2.3 De bevoegden gaan niet over tot het nemen van risico's die groter zijn dan begroot, zonder daaraan voorafgaand overleg met de betrokken portefeuillehouder(s), dan wel gemeentesecretaris van de gemeente.

2.4 Bij de te nemen maatregelen als bedoeld in artikel 32 AVG, de BIG en het informatiebeveiligingsbeleid van de gemeente(n)/BAR-organisatie vraagt de bevoegde functionaris de Chief Information Security Officer (CISO) en de Privacy Officer om advies.

3. Bevoegdheden ENSIA

3.1 De bevoegdheid om namens het verantwoordelijke bestuursorgaan de ENSIA te coördineren wordt belegd bij de CISO. Die functionaris is in het kader van de ENSIA bevoegd om de daartoe noodzakelijke aanwijzingen aan het verantwoordelijke lijnmanagement te geven.

3.2 De CISO is bevoegd om namens het betrokken bestuursorgaan verantwoording af te leggen over de uitkomsten van de ENSIA.

3.3 De CISO is bevoegd om namens het betrokken bestuursorgaan de noodzakelijke (herstel)maatregelen te nemen die voorvloeien uit de uitkomsten van de ENSIA.

3.4 De CISO neemt geen maatregelen die daarvoor begrote bedragen overschrijden of die de daarvoor begrote bedragen dreigen te overschrijden. De CISO voert voorafgaande aan maatregelen als

bedoeld in voorgaande zin overleg met de betrokken portefeuillehouder(s), dan wel de gemeentesecretaris, dan wel het betrokken bestuursorgaan. Maatregelen als bedoeld in de eerste volzin kunnen pas worden genomen na verkregen instemming van de in de voorgaande zin genoemde betrokkenen.