

Privacy beleid (bescherming persoonsgegevens)

De gemeenten Alphen-Chaam, Baarle-Nassau en Gilze en Rijen en de ABG-organisatie (hierna gezamenlijk te noemen: de organisatie) hechten er grote waarde aan dat er binnen de organisatie zorgvuldig en respectvol omgegaan wordt met persoonsgegevens. De bescherming van persoonsgegevens is namelijk een belangrijke voorwaarde om het fundamentele recht op privacy van de betrokken personen te kunnen waarborgen. De organisatie werkt onderling dusdanig nauw samen dat er is besloten om een gelijkkludend Privacybeleid en Privacyreglement op te stellen en vast te stellen, wat van toepassing is op iedere individuele deelnemende partij binnen deze organisatie, maar tevens in gezamenlijkheid in die gevallen waarbij sprake is van gezamenlijke verwerkingsverantwoordelijkheid. Vandaar dat in dit (gezamenlijke) document wordt gesproken van 'organisatie' waaronder in het ene geval een van de deelnemende gemeenten kan worden begrepen, in het andere geval de ABG-organisatie en in voorkomende gevallen de al dan niet gehele samenwerking tussen de vier partijen.

Met persoonsgegevens worden gegevens bedoeld waarmee een persoon direct of indirect mee kan worden geïdentificeerd. Deze gegevens kunnen betrekking hebben op medewerkers, burgers, bezoekers en iedere andere natuurlijke persoon. Uiteraard worden persoonsgegevens enkel gebruikt als daar een specifieke reden voor is, zoals het verwerken van een paspoortaanvraag of het doorgeven van een verhuizing. Tevens worden er maatregelen in het leven geroepen om persoonsgegevens en het verwerkingsproces te beveiligen om te voorkomen dat gegevens op straat of bij de verkeerde persoon terecht komen. De organisatie hanteert de volgende uitgangspunten:

De organisatie:

- gaat voorzichtig en vertrouwelijk om met persoonsgegevens, houdt deze gegevens veilig en voorkomt dat ze worden gebruikt door onbevoegden of voor andere doeleinden dan aangegeven.
- is transparant over het verzamelen, gebruik, delen en opslaan van persoonsgegevens.
- verwerkt persoonsgegevens:
 - alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen.
 - op basis van een rechtvaardige (juridische) grondslag;
 - alleen gegevens die minimaal noodzakelijk zijn voor het vooraf bepaalde doel.
 - niet langer dan noodzakelijk en bewaart gegevens dan ook niet langer dan nodig.
 - in naleving van de toepasselijke wetgeving¹ en in samenwerking met relevante autoriteiten
 - in een gedegen balans tussen risicobeheer enerzijds en efficiëntie en praktische uitvoerbaarheid anderzijds
- houdt persoonsgegevens en verwerkingsprocessen veilig door het treffen van passende beveiligingsmaatregelen, hetgeen is vastgelegd in het informatiebeveiligingsbeleid.
- vergewist zich ervan dat externe partijen waarmee wordt samenwerkt dezelfde hoge standaarden hanteren waar het gegevensbescherming betreft door het maken van afspraken over de eisen waar gegevensuitwisseling aan moet voldoen.

¹ Met name de Wet Bescherming Persoonsgegevens (Wbp), vanaf 25 mei 2018 vervangen door de Europese Algemene Verordening Gegevensbescherming (AVG of GDPR) en de Nederlandse Uitvoeringswet AVG.



Baarle-Nassau
Baarle-Hertog

GEMEENTE

Gilze en Rijen



Dit privacy beleid treedt in werking na vaststelling door het college van burgemeesters en wethouders. Het beleid wordt iedere twee jaar geëvalueerd en indien nodig herzien. Aanpassingen van dit beleid worden aangekondigd via de digitale gemeentebleden. De meest actuele versie van het beleid is te vinden via de gemeentelijke websites van de gemeente Alphen-Chaam, Baarle-Nassau en Gilze en Rijen, alsmede via de website van de ABG-organisatie.

Privacy reglement (bescherming persoonsgegevens)

In dit reglement laat de organisatie zien op welke manier zij dagelijks omgaat met persoonsgegevens als noodzakelijke voorwaarde voor de bescherming van privacy, en wat er wettelijk wel en niet verantwoord is.

De bescherming van persoonsgegevens speelt een belangrijke rol in de relatie tussen burger en de overheid. Enerzijds moet de organisatie persoonsgegevens kunnen verwerken voor het uitvoeren van de dagelijkse taken (basisadministraties, openbare orde en veiligheid, en het sociaal domein), anderzijds kan onbehoorlijke gegevensbescherming het vertrouwen schaden dat de burger heeft in de organisatie. Het beschermen van persoonsgegevens staat daarmee hoog op de bestuurlijke agenda. Verwerkingsverantwoordelijken hebben de verantwoordelijkheid over persoonsgegevens en gegevensuitwisseling op alle terreinen waar ze actief zijn. Verwerkingsverantwoordelijken en verwerkers zijn verplicht om zorgvuldig en veilig, proportioneel en vertrouwelijk om te gaan met de persoonsgegevens van burgers. Dit betreft een dagelijkse bezigheid. 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 de privacy waarborgen.

1. Wetgeving en definities

Momenteel regelt de Wet bescherming persoonsgegevens (Wbp) het juridische kader voor de omgang met persoonsgegevens in Nederland. Op 25 mei 2018 vervalt de Wbp en treedt de Europese Algemene Verordening Gegevensbescherming (AVG) in werking, samen met de Nederlandse uitvoeringswet. De AVG zorgt onder andere voor verdere versterking en uitbreiding van de privacyrechten met meer verantwoordelijkheden voor organisaties.

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

Betrokkene: De persoon op wie de persoonsgegevens betrekking hebben. De betrokkene is degene van wie de gegevens worden verwerkt.

Verwerker: De persoon of organisatie die de persoonsgegevens verwerkt in opdracht van een andere persoon of organisatie.

Persoonsgegevens: Alle gegevens die gaan over mensen en waaraan je een mens als individu kunt herkennen. Het gaat hierbij niet alleen om vertrouwelijke gegevens, zoals over Bijvoorbeeld: naam, adres, geboortedatum, maar ook over ieder gegeven dat te herleiden is tot een bepaald persoon. Naast gewone persoonsgegevens kent de wet ook bijzondere persoonsgegevens. Dit zijn

gegevens die gaan over gevoelige onderwerpen, zoals etnische achtergrond, politieke voorkeuren of gezondheid.

Voor wat betreft het Burgerservicenummer (BSN) heeft de Nederlandse regering in de Uitvoeringswet AVG bepaald dat het BSN door overheidsinstellingen enkel mag worden verwerkt voor doeleinden uit hoofde van overheidstaken die per wet zijn geregeld.²

Gegevensbeschermingseffectbeoordeling: Met een gegevensbeschermingseffectbeoordeling worden de effecten en risico's van de nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. In de Europese terminologie heet dit een Data Protection Impact Assessment ook wel Privacy Impact Assessment (PIA) genoemd.³

Verwerkingsverantwoordelijke: Een persoon of instantie die alleen, of samen met een ander, het doel en de middelen voor de verwerking van persoonsgegevens vaststelt.

Verwerking: Een verwerking is alles wat je met een persoonsgegeven doet, zoals: verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

2. Reikwijdte

Het reglement is van toepassing op alle verwerkingen van persoonsgegevens door alle bestuursorganen van de organisatie. Oftewel: voor alle verwerkingen die binnen de gemeenten Alphen-Chaam, Baarle-Nassau en Gilze en Rijen, alsmede binnen de ABG-organisatie plaatsvinden.

3. Verantwoordelijke

De bestuursorganen van de gemeenten Alphen-Chaam, Baarle-Nassau en Gilze en Rijen zijn allemaal verantwoordelijken voor de verwerkingen die door of namens de betreffende gemeente worden uitgevoerd. De bestuursorganen van de gemeente zijn onder andere de burgemeester, het college van Burgemeesters en Wethouders (college van B&W), de gemeenteraad, de heffingsambtenaar en de invorderingsambtenaar. Daarnaast is het bestuur van de ABG-organisatie verwerkingsverantwoordelijke voor verwerkingen die door of namens de ABG-organisatie worden uitgevoerd, alsmede voor verwerkingen van persoonsgegevens afkomstig van een van de drie ABG-gemeenten waarbij de doeleinden en de middelen van de verwerkingen worden bepaald door de ABG-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:

- 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.

Doeleinden (Artikel 5, AVG)

² Artikel 10 Wet algemene bepalingen burgerservicenummer (Wabb), zie ook de MvT Uitvoeringswet AVG, p. 43.

³ <https://www.ibdgemeenten.nl/wp-content/uploads/2014/04/14-0404-Toelichting-PIA-v1.0.pdf> 6

Volgens de wet mogen persoonsgegevens alleen verzameld worden als daarvoor een doel is vastgesteld. Het doel moet uitdrukkelijk omschreven en gerechtvaardigd zijn. De gegevens mogen niet voor andere doelen verwerkt worden. Voor de uitvoering van sommige wetten, zoals bijvoorbeeld de Jeugdwet, zijn de doelen voor het verwerken in de wet al vastgelegd, net als de persoonsgegevens die gevraagd en verwerkt mogen worden.

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
- Voor de uitvoering van een overeenkomst waar de betrokkene onderdeel was
- Om een ernstige bedreiging voor de gezondheid van de betrokkene te bestrijden
- Voor de goede vervulling van de gemeentelijke taak
- Wanneer de betrokkene toestemming heeft gegeven voor de specifieke verwerking

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. Dit betekent dat 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 met geen, of minder (belastende), persoonsgegevens hetzelfde doel bereikt kan worden moet daar altijd voor gekozen worden.

De organisatie zorgt ervoor dat de persoonsgegevens kloppen en volledig zijn voordat ze verwerkt worden. Deze gegevens worden alleen verwerkt door personen met een geheimhoudingsplicht. Daarnaast beveiligd de organisatie alle persoonsgegevens. Dit moet voorkomen dat de persoonsgegevens kunnen worden ingezien of gewijzigd door iemand die daar geen recht toe heeft. Hoe de organisatie dit doet staat in het informatiebeveiligingsbeleid van de organisatie en in een eventueel aanvullend beveiligingsplan specifiek opgesteld voor een proces of registratie.

Doorgifte (Artikel 44 t/m 50, AVG)

Op de export van persoonsgegevens naar een EU-lidstaat zijn geen extra regels van toepassing. Daarentegen is doorgifte naar een land buiten de Europese Unie aan strenge regels onderworpen. De organisatie geeft alleen persoonsgegevens door aan een land buiten de Europese Economische Ruimte (EER) of een internationale organisatie op grond van goedgekeurde afspraken door de Europese Commissie.

5. Transparantie en communicatie

Wet openbaarheid van bestuur (Wob)

Via de Wob⁴ (en straks wellicht de Wet Open Overheid) kun je een verzoek om informatie indienen bij de organisatie. Bij het verzoek bekijkt de organisatie altijd of het antwoord geen inbreuk maakt op de persoonlijke levenssfeer van betrokkenen. In principe worden geen persoonsgegevens verstrekt.

Wet hergebruik van overheidsinformatie

De Wet hergebruik van overheidsinformatie⁵ regelt het op verzoek verstrekken van overheidsinformatie voor hergebruik. Bij het verzoek bekijkt de organisatie altijd of het antwoord geen inbreuk maakt op de persoonlijke levenssfeer van betrokkenen. In principe worden geen persoonsgegevens verstrekt.

⁴ <http://wetten.overheid.nl/BWBR0005252/2016-10-01>

⁵ <http://wetten.overheid.nl/BWBR0036795/2016-10-01>

Informatieplicht (Artikel 13,14, AVG)

De organisatie informeert betrokkenen over het verwerken van persoonsgegevens. Wanneer betrokkenen gegevens aan de organisatie geven, worden zij op de hoogte gesteld van de manier waarop de organisatie met persoonsgegevens om zal gaan. Dit kan bijvoorbeeld via een formulier gebeuren. Vaak staat op de aanvraagformulieren vermeld welke gegevens zonder toestemming niet openbaar gemaakt zullen worden. De betrokkene wordt niet nogmaals geïnformeerd als hij/zij al weet dat de organisatie persoonsgegevens van hem/haar verzamelt en verwerkt, en weet waarom en voor welk doel dat gebeurt.

Wanneer de gegevens via een andere weg verkregen worden, dus buiten de betrokkene om, wordt de betrokkene geïnformeerd op het moment dat deze voor de eerste keer worden verwerkt.

Verwijdering

De organisatie bewaart de persoonsgegevens niet langer dan nodig is voor de uitvoering van de gemeentelijke en organisatorische taken, of zoals vastgelegd in 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.

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

Indienen van verzoek

Om gebruik te maken van zijn/haar rechten kan de betrokkene een verzoek indienen. Dit verzoek kan zowel schriftelijk als via de e-mail ingediend worden. De organisatie heeft vier weken de tijd, vanaf de ontvangst van het verzoek, om te beoordelen of het verzoek gerechtvaardigd is. Binnen vier weken zal de organisatie laten weten wat er met het verzoek gaat gebeuren. Als het verzoek niet wordt opgevolgd is er de mogelijkheid om bezwaar te maken bij de organisatie, of een klacht in te dienen bij de Autoriteit Persoonsgegevens (AP). Aan de hand van een verzoek kan de organisatie aanvullende informatie opvragen om zeker te zijn van de identiteit van de betrokkene.

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 gebruiken we het volgende voorbeeld: Wanneer een bezoeker op de gemeentelijke website of website van de ABG-organisatie naar een bepaalde dienst kijkt, mag de organisatie geen actie ondernemen om de dienst aan te bieden. De organisatie mag wel bekijken hoe vaak een bepaalde dienst bekeken is, maar dus niet specifiek gericht adverteren. Daarnaast geeft de wet aan dat er in beginsel geen besluit mag worden genomen op basis van profilering. Dit is uitsluitend toegestaan indien en voor zover profilering is toegestaan door Nederlands/EU recht of, onder voorwaarden, indien profilering noodzakelijk is voor de uitvoering van een overeenkomst tussen de betrokkene en de verwerkingsverantwoordelijke, of de betrokkene toestemming heeft gegeven voor profilering.

Momenteel maakt de organisatie geen gebruik van profilering. Indien de organisatie besluit om wel van profilering gebruik te gaan maken dan worden uiteraard de daarvoor geldende regels en voorwaarden gerespecteerd.

Big data en tracking

Door middel van Big data onderzoek en tracking mogen alleen gegevens verwerkt worden wanneer deze niet herleidbaar zijn tot een natuurlijk persoon. Daarnaast worden ze alleen verzameld voor onderzoek dat door, of namens, de organisatie wordt uitgevoerd. De verzamelde gegevens door Big data onderzoek en tracking zijn alleen de gegevens die door geautoriseerde personen zijn verzameld. Wanneer de gegevens worden omgezet in een dataset zal dataminimalisatie worden toegepast. Dit betekent dat alleen de data die echt nodig is voor het behalen van het doel gebruikt zullen worden. Daarnaast worden persoonsgegevens indien mogelijk en noodzakelijk gepseudonimiseerd zodat zij niet herleidbaar zijn tot een persoon.

Inzet van camera's

Binnen de organisatie wordt onder bepaalde omstandigheden gebruik gemaakt van cameratoezicht, zoals vastgelegd in de Gemeentewet⁶. Cameratoezicht wordt onder andere gebruikt voor het vergroten van de veiligheid op straat. 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 op de openbare weg is alleen mogelijk door toestemming van de organisatie, zijnde meestal het college van B&W van de betreffende gemeente. Daarvoor wordt er een convenant afgesloten tussen de particulieren en de organisatie waarin o.a. de grondslag, het doel, de maatregelen tegen verlies, en de bewaartermijn in opgenomen worden.

De organisatie maakt gebruik van cameratoezicht onder de volgende voorwaarden:

- Voor de inzet van cameratoezicht dient aan de voorwaarden van proportionaliteit en subsidiariteit te worden voldaan.
- Proportionaliteit: de inzet van cameratoezicht is gerechtvaardigd gezien de omvang van de criminaliteit, de (on)veiligheid en/of overlast.

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

- Subsidiariteit: de inzet van cameratoezicht is gerechtvaardigd omdat het gewenste resultaat niet met minder ingrijpende middelen kan worden bereikt. Dit geldt ook voor het cameratoezicht zelf (aantal camera's, in beeld brengen bepaalde plaatsen en personen, wel of niet continu cameratoezicht).
- Er moet sprake zijn van een openbaar orde probleem omschreven in een analyse. Cameratoezicht moet aantoonbaar noodzakelijk zijn voor de handhaving van de openbare orde. Voor ieder nieuw aan te wijzen gebied moet een probleemanalyse zijn opgesteld.
- Andere maatregelen hebben onvoldoende effect. Andere maatregelen van zowel burgers, ondernemers en overheid hebben niet volstaan. In het cameratoezichtsgebied moeten al extra maatregelen zijn ingezet naast het reguliere politietoezicht en gemeentelijke handhaving. Ook andere maatregelen zoals het aanpassen van de openbare ruimte (openbare verlichting en groenvoorzieningen) moeten zijn uitgevoerd.
- Cameratoezicht is maatwerk en moet vanuit expliciete doelen worden ingezet. Op basis van de probleemanalyse worden de expliciete doelen, cameraposities en uitkijktijden vastgesteld. De doelen, cameraposities en uitkijktijden worden regelmatig gemonitord. De expliciete doelen geven aan wat er met het cameratoezicht bereikt moet worden, gericht op de specifieke problemen in het gebied.
- Cameratoezicht wordt regelmatig geëvalueerd. Bij het afwegingskader gaat hem om de factoren als de omvang en aard van het probleem, de ontwikkeling van het probleem, het gebruik van de beelden voor de aanpak van het probleem en de beoordeling van veiligheidsrisico's als camera's worden weggehaald.

7. Plichten van de gemeente

Register van verwerkingen (Artikel 30, AVG)

De organisatie is verantwoordelijk voor het aanleggen van een register van alle verwerkingen waarvan de organisatie de verwerkingsverantwoordelijke is. Het register bevat een beschrijving van wat er tijdens een verwerking plaatsvindt, en welke gegevens daarvoor worden gebruikt, en bevat tenminste:

- De naam en contactgegevens van de verwerkingsverantwoordelijke en, mogelijk, de gezamenlijke verwerkingsverantwoordelijke;
- De doelen 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 termijnen waarin de verschillende persoonsgegevens moeten worden gewist;
- Een algemene beschrijving van de beveiligingsmaatregelen.

Gegevensbeschermingseffectbeoordeling (Artikel 35, AVG)

Met een gegevensbeschermingseffectbeoordeling worden de effecten en risico's van nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. De organisatie voert deze uit wanneer er een geautomatiseerde verwerking, een grootschalige verwerking, of wanneer er een grootschalige monitoring van openbare ruimten plaatsvindt. Dit geldt in het bijzonder bij verwerkingen waarbij nieuwe technologieën worden gebruikt.

Aanstellen van een Functionaris voor gegevensbescherming (FG) (Artikel 37 t/m 39, AVG)

De organisatie heeft een FG aangesteld. Deze FG'r is werkzaam voor alle vier bij de organisatie betrokken partijen. 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 Autoriteit Persoonsgegevens (AP). De AP houdt toezicht op de verwerking van persoonsgegevens. Daarnaast adviseert de AP de regering met betrekking tot vraagstukken die te maken hebben met de verwerking van persoonsgegevens.

Privacybeleid en Privacyreglement Alphen-Chaam, Baarle-Nassau, Gilze en Rijen en de ABG-organisatie

Het is niet de bedoeling dat de functionaris de taken op het gebied van bescherming van de privacy van de afdelingen overneemt. De afdelingen hebben hun eigen verantwoordelijkheid in het goed omgaan met privacygevoelige gegevens. Een verwerking van persoonsgegevens wordt eerst aan de FG gemeld voordat de verwerking begint. 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.

Datalekken (Artikel 33,34, AVG)

We spreken van een datalek wanneer persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens mogen hebben. Wanneer er een datalek heeft plaatsgevonden meldt de organisatie dit zonder onredelijke vertraging, uiterlijk 72 uur nadat er kennis van de inbreuk is vernomen, aan het AP. 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 meldt de organisatie dit aan de betrokkenen in eenvoudige en duidelijke taal. Om toekomstige datalekken te voorkomen worden bestaande datalekken geëvalueerd.

Kortom:

Privacy is belangrijk. Dat vindt de organisatie ook. De organisatie verzamelt en verwerkt veel persoonsgegevens van burgers. Dat schept verplichtingen. De organisatie heeft daarom Privacy beleid en een Privacy reglement opgesteld. Dit beleid past de organisatie intern toe en ook in samenwerkingsverbanden met andere organisaties. Daarmee weet iedereen waar deze zich aan te houden heeft bij het beschermen van de persoonsgegevens van burgers. Ook voor de burger is het goed om te weten hoe de gemeente met diens persoonsgegevens omgaat. Het beleid en het reglement is dan ook bedoeld als handvat voor de burger om de organisatie te kunnen volgen en aanspreken op het zorgvuldig omgaan met diens persoonsgegevens.

Samengevat gaat de organisatie als volgt om met persoonsgegevens:

- De organisatie verwerkt alleen gegevens van en over haar medewerkers en haar burgers die strikt noodzakelijk zijn voor het uitvoeren van haar gemeentelijke en organisatorische taken.
- De organisatie informeert burgers over het opslaan van persoonsgegevens.
- De organisatie bewaart gegevens volgens de wettelijk geldende termijnen of anders altijd zo kort mogelijk en vernietigt deze daarna.
- De organisatie gaat terughoudend om met informatie van en over burgers. Medewerkers worden daarover geïnstrueerd.
- De organisatie gaat terughoudend om met informatie over haar medewerkers,
- De organisatie gaat bij handhaving terughoudend om met informatie van en over burgers.
- De organisatie deelt persoonsgegevens intern en extern alleen voor zover dat strikt noodzakelijk is voor de taakuitvoering.
- De organisatie zorgt ervoor dat persoonsgegevens niet voorkomen in verslagen.
- De organisatie deelt medische informatie van haar medewerkers en haar burgers alleen met toestemming van de medewerker of burger.
- De organisatie verstrekt op wettelijk verzoek van haar medewerkers of haar burgers de voor die medewerker of burger geregistreerde gegevens.
- Als de organisatie gegevens openbaart als gevolg van een wettelijk verzoek, stelt de ABG-organisatie alles in het werk om persoonsgegevens te anonimiseren.
- Als de organisatie zelf wettelijk gegevens openbaar moet maken, dan wordt de betrokken medewerker of burger eerst om toestemming voor publicatie gevraagd en wordt gegevensverstrekking tot een minimum beperkt.



Baarle-Nassau
Baarle-Hertog



- Als de organisatie gegevens ter inzage legt, dan wordt van betrokken burgers de gegevensverstrekking tot een minimum beperkt.
- De organisatie draagt via een intern protocol zorg voor het goed uitvoeren van bovenstaand beleid door medewerkers en samenwerkende instanties.
- De organisatie voert toezicht uit op het privacy beleid en de uitvoering ervan.

Afsluiting

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

Disclaimer:

Dit product is een eenvoudige en begrijpbare vertaling van de huidige privacywetgeving en gebaseerd op de AVG. Vanzelfsprekend is de toepasbare wet- en regelgeving altijd leidend en kunnen er geen rechten ontleend worden aan dit document.

Aldus vastgesteld door burgemeester en wethouders van gemeente Alphen-Chaam,
d.d.

mr. M.M. Hendrickx
secretaris

mr. J.W.M.S. Minses
burgemeester

Aldus vastgesteld door burgemeester en wethouders van gemeente Baarle-Nassau,
d.d.

Ir. J.C. Slagboom
secretaris

M.H.M.R. de Hoon-Veelenturf
burgemeester

Aldus vastgesteld door burgemeester en wethouders van gemeente Gilze en Rijen,
d.d.

drs. R. Wiersema
secretaris

dr. A.J.W. Boelhauer
burgemeester



Aldus vastgesteld door het bestuur van de ABG-organisatie,
d.d.

drs. R. Wiersema
algemeen directeur

dr. A.J.W. Boelhouwer
voorzitter