Alphen aan den Rijn

GEMEENTEBLAD

Officiële uitgave van de gemeente Alphen aan den Rijn

Nr. 160728

25 mei

2021

Algemeen privacybeleid Gemeente Alphen aan den Rijn

Het college van burgemeester en wethouders van Alphen aan den Rijn;

Gelet op de Algemene Verordening Gegevensbescherming (AVG);

B E S L U I T vast te stellen het:

Algemeen privacybeleid Gemeente Alphen aan den Rijn

Inhoud

AVG-proof privacybeleid: Leeswijzer

Dit beleidsstuk laat zich als volgt samenvatten : Risico gestuurde gegevensbescherming ten bate van efficiënte dienstverlening. Deze missie krijgt handen en voeten door een aantal concrete maatregelen die hier kort voor het voetlicht komen, maar later in hun context worden geplaatst. De component 'risicosturing' kent twee belangrijke maatregelen: In de eerste plaats worden alle afdelingen, afhankelijk van de risicofactor, geïnventariseerd, geregistreerd en van een rapportage met aanbevelingen voorzien. Bovendien heeft elk van deze afdelingen een medewerker met privacy taken als contactpersoon met een signaleringsfunctie. In de tweede plaats wordt bij elke nieuwe ontwikkeling de afweging gemaakt tussen rechtsbescherming en dienstverlening. Daar waar deze waarden conflicteren moet de keuze op het juiste niveau inzichtelijk worden gemaakt. Dit gebeurt, afhankelijk van de omvang, door middel van een beperkte effectenanalyse of een gestructureerde Data Protection Impact Assessment (DPIA). Een belangrijke maatregel ten behoeve van de rechtsbescherming is de aanstelling van de Functionaris Gegevensbescherming (FG). De cyclische controle van deze functionaris borgt de naleving van de AVG. Bij de implementatie van de AVG is intern gekozen voor een projectmatige aanpak, waarbij het volgende tijdpad is gehanteerd.

Grafische weergave implementatie AVG

Instellen intern privacy-netwerk (medewerkers met privacy taken) hoog risico	**Screening bestaande verwerkings-processen**	**Inventariseren hoog risicoverwerkingen, opname hiervan in register van verwerkingen**	**Aanstelling FG**	**Inventariseren laag risicoverwerkingen, opname hiervan in register van verwerkingen**

Vóór 25 mei 2018

Vaststellen AVG-proof Algemeen Privacybeleid

Na 25 mei 2018

Opnemen in Planning en Control cyclus

Voorlichting inwoners

Continu proces vanaf heden

Inventariseren en afsluiten verwerkingsovereenkomsten

1. Inleiding

Het algemeen privacybeleid dat voor u ligt is een herijking van het bestaande privacybeleid zoals de gemeente Alphen aan den Rijn het sinds 2015 hanteert. Onder het paraplubegrip 'privacy' wordt van alles verstaan(en misverstaan). Onder 'privacy' in de zin van dit beleidsstuk wordt verstaan de wijze waarop overheidsorganen omgaan met de persoonsgegevens van haar burgers. Het onderwerp is volop in beweging. De twee voornaamste ontwikkelingen op het gebied van wetgeving zijn de Algemene Verordening Gegevensbescherming (AVG) en de Wet op de inlichtingen- en veiligheidsdiensten (Wiv) . De aandacht voor deze ontwikkelingen is het logisch gevolg van het feit dat deze regelgeving een uitwerking is van een grondrecht. Dit grondrecht (artikel 10 GW) of 'mensenrecht' , in de woorden van het Europees Verdrag voor de Rechten van de Mens en de fundamentele vrijheden (artikel 8 EVRM) garandeert ieder persoon het recht op de eerbiediging van zijn of haar persoonlijke levenssfeer. De inperking van dit recht heeft de wetgever aan zeer strenge regels onderworpen.
De AVG is een Europese wet die het grondrecht vertaalt naar concrete normen voor organisaties die persoonsgegevens verwerken. De AVG volgt hiermee de Wet bescherming persoonsgegevens (Wbp) op. Deze nationale wetgeving kent grote overeenkomsten met de AVG, maar verschilt ervan waar het de verantwoordingsplicht betreft. De verantwoordingsplicht van de organisatie die de persoonsgegevens verwerkt is aangescherpt en wordt gesanctioneerd door aanzienlijk hogere boetes. Om Verscherpte eisen voor de verantwoordingsplicht, in combinatie met dreigende sancties wekken aanvankelijk de indruk dat de gemeentelijke dienstverlening verder aan banden wordt gelegd. Waar immers het delen en verwerken van data wordt beperkt ten behoeve van de gegevensbescherming, bemoeilijkt dit de soepele en efficiënte dienstverlening. Dit beleidsstuk beoogt onder andere deze oneigenlijke tegenstelling in de juiste context te plaatsen. Dit komt tot uitdrukking in de visie die de Gemeente Alphen aan den Rijn voorstaat met betrekking tot het beschermen van persoonsgegevens.
In dit algemeen privacybeleid wordt allereerst de missie met betrekking tot privacy naar voren gebracht. Rollen en verantwoordelijkheden worden benoemd in hoofdstuk 3. Er is speciale aandacht voor de rol van de Functionaris Gegevensbescherming (FG) die een centrale positie inneemt in de organisatie. In hoofdstuk 4 wordt het wettelijk kader geschetst waarbinnen de organisatie haar gegevensbescherming dient te borgen. Afzonderlijk behandelt dit hoofdstuk de beginselen waarop de wet is gestoeld, de uitputtende lijst grondslagen waarop de verwerkingen moeten zijn gebaseerd en de belangrijkste direct afdwingbare rechten. Voorts komt aan bod wat de gemeente doet om persoonsgegevens die zij met externe partijen deelt toch veilig en verantwoord te laten verlopen. Dit alles vergt intensieve samenwerking met de afdeling Informatisering en Automatisering. Hoofdstuk 6 besteedt aandacht aan de wisselwerking tussen de juridische en de informatie technische discipline.

2. Missie

2.1 Dilemma

De gemeente Alphen aan den Rijn wil voorop lopen in dienstverlening en vooruitstrevend zijn in technologische toepassingen. Waar deze wensen elkaar ontmoeten vormt zich de missie van de gemeente Alphen aan den Rijn. Als gemeentelijke organisatie verzamelt en bezitten wij een grote hoeveelheid data. Daar waar deze data de dienstverlening kunnen vereenvoudigen voor onze inwoners zou het mooi zijn deze data te kunnen delen. Het gebruik van kentekens om onwenselijke verkeersstromen in kaart te brengen en weggebruikers daardoor te kunnen benaderen. Of het gebruik van afvalpassen om huishoudens gericht voor te kunnen lichten inzake hun stortgedrag. Allerhande mogelijke apps die wijkgegevens inzichtelijk maken… mogelijkheden om de inwoners tot dienst te zijn te over. Helder is wel dat samenwerking met netwerkpartners steeds verdergaande vormen aanneemt. De ontwikkelingen richting de Smart City (Amsterdam en Eindhoven bewegen zich al die kant op) vragen om grote alertheid. Om onze leefomgeving klaar te stomen voor de toekomst is een integrale aanpak nodig. Bereikbaarheid, leefbaarheid, duurzaamheid, luchtkwaliteit, geluid, energie, gezondheid en economische vitaliteit zijn onlosmakelijk met elkaar verbonden. Zo kunnen data van gemeentelijke diensten met die van derde partijen gecombineerd worden. Stadsbeheer, stedelijke planning en het bedrijfsleven kunnen dan van elkaars informatie profiteren. Stadsbeheer en infrastructuurbeheerders beschikken over een schat aan

gegevens over dagelijkse stedelijke operaties en stromen als verkeer, energie, afval, bouw. In een echt slimme stad zorgen dataoplossingen ervoor dat de stedelijk planologen gebruik maken van realtime gegevens van het stadsbeheer, terwijl beheer door de informatie-uitwisseling meer oog krijgt voor de strategie op langere termijn. Burgers en bedrijven als retail, horeca, dienstverleners of projectontwikkelaars krijgen op termijn toegang tot dezelfde data, zodat zij steeds realtime weten hoe de stad ervoor staat en daar hun plannen of dienstverlening op kunnen afstemmen. Technisch gesproken zijn er nauwelijks beperkingen. Maar hoe mooi de oplossingen ook kunnen zijn, zitten burgers wel op deze gegevensdelingen te wachten? 'Big Brother is watching you' raast naar binnen en hoe veilig zijn onze gegevens als Facebook accountgegevens eenvoudig weg verkoopt en mogelijk de beïnvloeding van verkiezingen mogelijk maakt? Voor zover we lessen mogen trekken uit een referendum leert, het Wiv- referendum ons dat inwoners tenminste koudwatervrees hebben, maar overduidelijk van hun overheid verwachten dat hun persoonsgegevens goed beveiligd worden. Nu is maar een deel van alle data te kwalificeren als persoonsgegevens, maar bij elke stap in elke ontwikkeling moet het college zich als verantwoordelijke afvragen of sprake is van tot de persoon herleidbare gegevens. De risico's zullen opnieuw in kaart gebracht moeten worden. Dit zal leiden tot het bevestigen of uitbreiden van afspraken over de verwerking van de persoonsgegevens.
Op de gemeente Alphen aan den Rijn rust de grote verantwoordelijkheid om op correcte wijze om te gaan met de persoonsgegevens van haar burgers. Deze persoonsgegevens verwerkt de gemeente uit hoofde van haar publieke taken die voortvloeien uit de wet of het algemeen belang. Dit betekent dat zij de beschikking heeft over grote hoeveelheden gegevens die naar hun aard deel uitmaken van de persoonlijke levenssfeer van het individu. Dit besef is voor de gemeente Alphen aan den Rijn het uitgangspunt bij de verwerking van de haar toevertrouwde persoonsgegevens. Data die niet tot de persoon herleidbaar zijn kunnen dan ook vrij gebruikt worden, maar elk ander en nieuw gebruik zal een check op die persoonlijke herleidbaarheid nodig maken.

2.2 Vorm
De gemeente Alphen aan den Rijn volgt hiermee de bindende regels die de Algemene Verordening Gegevensbescherming (AVG) stelt. De gemeente garandeert de verwerking van persoonsgegevens conform deze wetgeving met al de hierin opgenomen normen en waarborgen. Het algemeen privacybeleid vertaalt deze wetgeving naar praktische kaders waarbij de gehele gemeentelijke organisatie aansluiting vindt. Het algemeen privacybeleid verbindt niet alleen de afzonderlijke specialismen van de organisatie(functioneel), maar bepaalt tevens het bestuur, de directie en het management bij dezelfde afspraken(hiërarchisch).

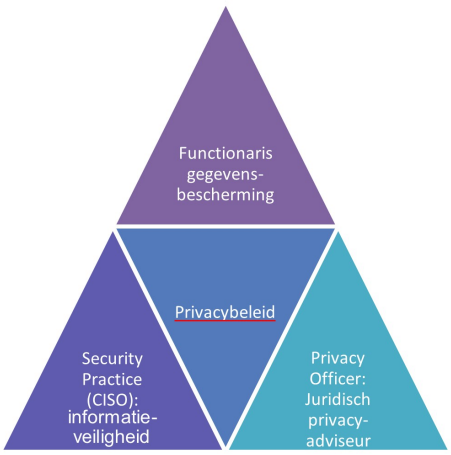
2.3 Inhoud: rechtmatig, veilig en transparant
De verantwoordelijkheid van de gemeente Alphen aan den Rijn valt uiteen in twee delen. In eerste plaats verwerkt de gemeente de verkregen persoonsgegevens te in het belang van haar inwoners. Zij streeft optimale dienstverlening na. Het verwerken van al dan niet vrijwillig verkregen persoonsgegevens is op geen andere grond gerechtvaardigd. In de tweede plaats garandeert de gemeente Alphen aan den Rijn dat wanneer zij eenmaal over de persoonsgegevens beschikt, zij deze op rechtmatige, veilige en transparante wijze verwerkt en/of deelt. Dit is het leidende principe van dit algemeen privacybeleid. Het beleid stelt het college van burgemeester en wethouders in staat de verwerking van persoonsgegevens te bewaken en te faciliteren.

3. Governance
Privacy is van onszelf en van ons allemaal. De wet belegt de verantwoordelijkheid bij het college, maar toch ligt de procesverantwoordelijkheid voor de privacyfunctie integraal bij elke afdelingsmanager en teamleider van deze organisatie voor zijn eigen taakgebied. Vanuit die gedachte zal elke manager in staat moeten worden gebracht om vanuit de integrale verantwoordelijkheid zijn processen optimaal in te richten. De integraal manager is procesverantwoordelijke en bepaalt de wijze waarop persoonsgegevens worden gebruikt in (web)applicaties, wie toegang hiertoe krijgen, welk werkproces, met welke (contract) partijen e.d.

3.1 Bestuurlijk: rapportage en verantwoording
Een evenwichtig en zorgvuldig privacybeleid behelst onder meer dat de effecten van het beleid meetbaar zijn en dat het een eigen, zelfstandige plaats verwerft binnen de planning- en controlcyclus. Beheer van (persoons)gegevens is een vorm van processturen, naast de sinds jaar en dag bekende sturing op financiële processen. Dit heeft als voordeel dat het college eenvoudiger in staat zal zijn verantwoording af te leggen over de het door haar gevoerde privacybeleid. Transparantie in beleid en maatregelen staan daarbij voorop. Een gedegen register van verwerkingen is hiervoor onontbeerlijk en monitoring van (benodigde) juridische, digitale en menselijke beheermaatregelen.

3.2 Positie FG
De AVG stelt ons verplicht om de correcte en zorgvuldige toepassing van de privacywetgeving te borgen in een controlfunctie. Dit is uitgewerkt in de verplichte aanstelling van een Functionaris Gegevensbe-

scherming (FG). Alphen aan den Rijn kiest voor een FG op wetenschappelijk opleidingsniveau, die zich in zijn functie toespitst op de controltaken. Dit is mogelijk doordat de FG in zijn functie ondersteund wordt door de Privacy Officers.
Voor de gemeente Alphen aan den Rijn is de functie van FG een nieuwe functie. Vandaar dat voorgesteld wordt om gedurende een jaar ervaring op te doen met deze nieuwe functie door een ervaren externe FG deze rol te laten vervullen. Hierdoor kan ervaring worden opgedaan met deze functie en kan een duidelijker beeld ontstaan over rol, taakinvulling en de benodigde tijdsbesteding. Na dat jaar kan beoordeeld worden of een 2e jaar ook extern wordt ingehuurd of een logisch vervolg is dat gekozen wordt voor het intern aanstellen van een FG.
De FG wordt, vanuit het pakket van strikt controltaken, functioneel voorzien onder de gemeentesecretaris, feitelijk bij de afdeling Bestuur en Concern. Voor de inhuur is samenwerking gezocht met de gemeenten Gouda, Waddinxveen, Nieuwkoop en Kaag en Braassem. Het streven is de FG per 1 mei 2018 operationeel te hebben in Alphen aan den Rijn.



3.3 Ambtelijk: beheersmaatregelen

Elke manager van elke afdeling is integraal verantwoordelijk is voor de goede uitvoering van de AVG op zijn of haar afdeling. Vanuit die gedachten zal elke manager in staat zal moeten zijn om op elke gewenst moment verantwoording af te leggen over de wijze waarop zijn of haar afdeling met persoonsgegevens om gaat. Dit vraagt bewustwording, structuur en verantwoording. Elke manager kan zijn verantwoordelijkheden mandateren aan teamleiders of aan een privacy medewerker op de afdeling. Mandaat betekent dat de manager onverkort zelf verantwoordelijk blijft. Met het vullen van het register van verwerkingen en het blijvend onderhouden van dit systeem middels plan-do- check- act.
De risicogevoeligheid van de persoonsgegevens wordt bepaald aan de hand van verschillende factoren. Worden bijzondere persoonsgegevens verwerkt of van kwetsbare doelgroepen? Wordt DigiD gebruikt? De mate van vertrouwelijkheid, wie toegang heeft tot de gegevens enzovoorts. Deze weging van risico's wordt dataclassificatie genoemd. Op basis van deze dataclassificatie wordt de omvang van de beheersmaatregelen bepaald. Beheersmaatregelen worden onderscheiden in drie categorieën : maatregelen op juridisch niveau, op technisch niveau en op menselijk niveau. Op juridisch niveau bestaan de beheersmaatregelen in de vaststelling van juridische kaders zoals de mandatering, verwerkersovereenkomsten , privacyreglementen en protocollen. Ook kan gedacht worden aan dataminimalisatie en bewaartermijnen. De maatregelen op technisch niveau komen aan de orde in het informatiebeveiligingsbeleid dat in hoofdstuk zes wordt benoemd. Te denken valt aan de aansluiting bij het informatiebeveiligingsbeleid, de wijze van verlenen autorisatie voor toegang tot een applicatie, loginregistratie van een applicatie, beveiligd e-mailen e.d. De maatregelen op menselijk niveau zijn het meest omvangrijk. Menselijke maatregelen hebben te maken met houding en gedrag, waardoor bewustzijn en training een belangrijk onderdeel hiervan is.

4. Wettelijk kader

Het algemeen privacybeleid beoogt geen juridische leidraad te zijn. Zoals reeds aangegeven ligt het primaat van het beleid bij datgene dat de AVG mogelijk maakt. Waar biedt de AVG de ruimte om diensten aan te bieden die technologisch voorop lopen, de burger efficiënt te helpen, en tegelijkertijd de persoonsgegevens zo goed mogelijk te beschermen? Hiervoor biedt dit wettelijk kader de basis. Kort en bondig komen achtereenvolgens drie onderdelen van de AVG aan bod waarin het volgende wordt behandeld: beginselen, grondslagen voor verwerking van persoonsgegevens en de, rechten van betrokkenen.

4.1 Beginselen

Elke verwerking van persoonsgegevens moet voldoen aan zes basisbeginselen. Deze beginselen zijn bedoeld als algemene borging en werken door in de interpretatie van de rechten en plichten elders uit de AVG. Bovendien kan de betrokkene wiens gegevens worden verwerkt zich rechtstreeks beroepen op deze beginselen bij de rechter of toezichthouder.
• Het beginsel van rechtmatigheid behoorlijkheid en transparantie houdt in dat het voor betrokkenen inzichtelijk moet zijn in hoeverre en op welke manier er persoonsgegevens worden verwerkt. De verwerking dient in overeenstemming te zijn met de wet en de ongeschreven regels die in het maatschappelijk verkeer gelden. Informatie en communicatie hierover dient eenvoudig, toegankelijk en begrijpelijk te zijn. Juridisch taalgebruik is dus ongewenst.
• Aansluitend op het voorgaande beginsel geldt het doelbindingsprincipe. De verwerking mag alleen gebeuren voor specifieke en gerechtvaardigde doeleinden. Deze moeten zijn vastgesteld en omschreven voordat men begint met de verwerking. De verwerking mag ook plaatsvinden voor doelen die met de eerder genoemde doelen zijn te verenigen.
• Het derde beginsel is dat van 'minimale gegevensverwerking', ofwel dataminimalisatie. Dit beginsel brengt met zich mee dat niet meer persoonsgegevens mogen worden verwerkt dan strikt noodzakelijk is voor het doel. Hieruit volgt ook dat persoonsgegevens zo snel mogelijk moeten worden gewist of onherkenbaar gemaakt.
• Juistheid. Het vierde beginsel, dat van juistheid, eist dat de gegevens actueel en juist moeten zijn. De verwerkingsverantwoordelijke heeft daarbij een verregaande inspanningsplicht om deze juistheid te borgen. Het is onjuist (en boetewaardig, artikel 83 lid 5 onder a) om passief te wachten tot betrokkenen klagen over onjuiste of achterhaalde persoonsgegevens.
• Het beginsel van opslagbeperking dient ervoor te zorgen dat persoonsgegevens niet langer worden bewaard dan noodzakelijk is voor de verwerking. Voor diverse verwerkingen geldt een wettelijke bewaarplicht. Het bewaren van deze gegevens is gerechtvaardigd onder artikel 6 AVG lid 1 onder c. (wettelijke plicht). Overige termijnen moeten een duidelijk vast te stellen einde hebben.
• Ter borging van het beginsel van integriteit en vertrouwelijkheid moet de verwerkingsverantwoordelijke technische en organisatorische beveiligingsmaatregelen nemen om ongeoorloofde toegang of het ongeoorloofd gebruik van persoonsgegevens te voorkomen. Dit beginsel word nader uitgewerkt in het verdere van dit beleidsstuk.

4.2 Grondslagen van verwerking

De grondslagen voor de verwerking van persoonsgegevens is een uitwerking van het voornoemde beginsel van rechtmatigheid. Uitsluitend de hiergenoemde grondslagen bieden een rechtvaardiging om persoonsgegevens te mogen verwerken.
• **Toestemming**. Toestemming is iedere vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene aanvaardt dat zijn persoonsgegevens worden verwerkt. Deze wilsuiting moet actief worden gedaan, stilzwijgen is nimmer voldoende. De toestemming moet duidelijk en eenvoudig zijn geformuleerd.
• **Noodzakelijk voor de uitvoering van een overeenkomst**. Slechts wanneer de overeenkomst niet goed kan worden nagekomen zonder de verwerking is sprake van een dergelijke noodzaak.
• **Wettelijke verplichting**. Wanneer de verwerkingsverantwoordelijke wettelijk verplicht is om de verwerking uit te voeren, is deze derde grondslag gegeven. Een verwerking die zijn grondslag vindt in een wettelijke plicht moet te herleiden zijn tot een specifieke wettelijke regeling in het Unierecht of nationaal recht.
• **Vitaal belang**. Ook hier geldt de noodzaak om de vitale belangen van de betrokkene (of een ander persoon, zoals diens kind) te beschermen als grondslag. De verwerking van medische gegevens bij een ongeval is het archetypisch voorbeeld.
• **Algemeen belang of bij uitoefening van het openbaar gezag**. Indien de verwerkersverantwoordelijke taken heeft te vervullen die niet specifiek bij wet zijn geregeld, maar zijn terug te voeren op het algemeen belang (bijvoorbeeld: Volksgezondheid), en deze taak niet naar behoren kan vervullen zonder het verwerken van persoonsgegevens, is deze verwerking gerechtvaardigd. Van openbaar gezag is sprake wanneer overheidsinstanties hun bij wet geregelde taak uitvoeren. In nationale of Europese wetgeving moet nader worden gespecificeerd voor welke taken en doeleinden verder verwerking als rechtmatig moet worden beschouwd.
• **Eigen gerechtvaardigd belang**. Deze grondslag moet worden beschouwd als laatste mogelijkheid wanneer de verwerkersverantwoordelijke een belang heeft bij de verwerking welke niet op de overige grondslagen is terug te voeren. Hieraan dient wel een belangenafweging ten grondslag te liggen met de grondrechten van de betrokkene. Het moge duidelijk zijn dat met de grondslagen 'wettelijke verplichting' en 'algemeen belang' het overgrote deel van de verwerkingen van de gemeente Alphen aan den Rijn is gerechtvaardigd. Niettemin dient elke verwerking langs deze maatstaf te worden gelegd.

4.3 Rechten van betrokkenen

Bescherming van privacy is een grondrecht. De betrokkene wiens persoonsgegevens worden verwerkt, heeft dan ook aantal sterke rechten ten aanzien van de verwerkingsverantwoordelijke. De belangrijkste hiervan vergen een inspanningsverplichting van de Gemeente Alphen aan den Rijn. Deze rechten worden hier kort behandeld.

• **Het recht op informatie over de verwerkingen**. Als verwerkingsverantwoordelijke heeft de Gemeente Alphen aan den Rijn de plicht om de burger te informeren over zijn gegevensverwerking. Meer specifiek hebben betrokkenen het recht om te weten wat er met hun persoonsgegevens gebeurt en waarom. Uitgangspunt is dat er altijd een informatieplicht geldt. Wanneer de gegevens bij de betrokkene zelf worden verzameld, maar ook wanneer de gegevens buitende betrokken om worden verkregen.
• **Het recht op inzage in zijn gegevens**. Iedere betrokkene heeft het recht om de persoonsgegevens die van hem verzameld zijn in te zien. De gemeente is verplicht om gehoor te geven om gehoor te geven aan verzoeken om inzage en de beschikbare informatie te verstrekken. Dit recht gaat zo ver dat de gemeente desgevraagd kosteloos een kopie van de gegevens dient te verstrekken.
• **Het recht op correctie van de gegevens als deze niet kloppen**. Alle gegevens die de Gemeente Alphen aan den Rijn verwerkt moeten accuraat zijn en blijven. Toch kan het voorkomen dat e gemeente persoonsgegevens verwerkt die niet (meer) kloppen. De betrokkene heeft dan het recht u op te dragen deze gegevens te corrigeren en/of aan te vullen.
• **Het recht op verwijdering van de gegevens**. Onder bepaalde omstandigheden hebben betrokkenen het recht om hun gegevens door de verwerkingsverantwoordelijke te laten verwijderen, bijvoorbeeld wanneer de verwerking onrechtmatig is. Daarnaast heeft de betrokkene het recht om 'vergeten te worden'. Dit recht is met name in het leven geroepen zodat mensen niet voor altijd met hun verleden worden geconfronteerd.
• **Recht om een klacht in te dienen bij de toezichthouder** . Betrokkene heeft het recht een klacht in te dienen bij de toezichthouder. De toezichthouder heeft tot taak de klacht of het verzoek te behandelen en hier een besluit over te nemen. Tegen dit besluit kan de betrokkene in bezwaar gaan bij de toezichthouder zelf. Is de betrokkene het niet eens met de beslissing op het bezwaar, dan kan deze in beroep bij de bestuursrechter.

4.4 Overig: FG en Register van Verwerkingen

De AVG kent nog twee dwingende bepalingen die genoemd moeten worden binnen het wettelijk kader. Deze bepalingen zijn reeds benoemd in een voorgaand hoofdstuk. Dit betreft de aanstelling en de rol van de Functionaris Gegevensbescherming (art. 37 AVG e.v.) en het aanleggen en accuraat houden van het register van verwerkingen (art. 30 AVG).

5. Samenwerking externe partijen

De gemeente Alphen aan den Rijn kent verschillende samenwerkingsvormen. Er zijn partijen die, in opdracht van de gemeente, een taak uitvoeren. Voorbeelden hiervan zijn Participe, TOM in de Buurt, Samenwerkingsorgaan Holland Rijnland of de Omgevingsdienst Midden Holland (ODMH). Soms voert de gemeente taken voor andere partijen uit. Van belang is dat in alle gevallen afspraken worden gemaakt over de omgang met en de beveiliging van persoonsgegevens. Waar sprake is van een verwerkingsverantwoordelijke-verwerkersrelatie zal een Verwerkingsovereenkomst gesloten moeten worden. Waar sprake is van gedeelde verantwoordelijkheid zal een wederzijdse afsprakenlijst vastgesteld en getekend worden. Primair van belang is om bij elke voorgenomen samenwerking te overdenken wat de effecten van de samenwerking op de verwerking van persoonsgegevens zijn. Het is dan ook zaak over deze overeenkomsten verantwoording af te kunnen leggen in een daarvoor opgesteld register.

6. Informatieveiligheid

Er bestaan groten raakvlakken tussen privacybeleid en informatiebeveiligingsbeleid. Zo zal er ook een intensieve samenwerking moeten bestaan tussen de Privacy Officer en de CISO. Elke organisatorische en/of technologische ontwikkeling vraagt een onderzoek op de effecten ten aanzien van de persoonsgegevens. Liefst in een zo vroeg mogelijk stadium zodat privacy by design in de praktijk gebracht kan worden. In dat opzicht hebben Privacy Officer en CISO bij de advisering beiden een onmisbare rol. Teneinde deze samenwerking een structureel karakter te geven komen de CISO, de Informatiemanager en de Privacy Officers periodiek bijeen in het P(rivacy) I (Informatiebeveiligings) Team, ook wel het PIT genoemd. Doel van deze PIT-overleggen is vroegtijdig informatie uit te wisselen

over informatietechnologische en juridische ontwikkelingen. Daarmee wordt tijdige betrokkenheid gegarandeerd en kunnen Data Protection Impact Analyses in uitgebreide of beperktere vorm, al naar gelang wat nodig is, aan de procesverantwoordelijke afdelingen worden aanbevolen. Daarmee geeft deze samenwerking weer handen en voeten aan het beginsel van Privacy by Design. Tussen de deelnemers van het PIT vindt afstemming plaats die input geeft aan enerzijds het algemeen privacybeleid en anderzijds het informatiebeveiligingsbeleid.

7. Definities/Afkortingen

AVG: Europese wetgeving op de bescherming van persoonsgegevens. Deze wet geldt in alle lidstaten.
Betrokkene: Degene over of van wie persoonsgegevens worden verwerkt.
CISO: Chief Information Security Officer is verantwoordelijk voor de databeveiliging op het terrein van informatisering en automatisering.
Functionaris Gegevensbescherming (FG): Bij wet geregelde toezichthouder ten behoeve van de naleving van wettelijke verplichtingen.
Persoonsgegevens: Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon; als identificeerbaar wordt beschouwd een natuurlijk persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, identificatienummer, locatiegegevens, een online identificator of één of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische economische culturele of sociale identiteit van die natuurlijke persoon.
DPIA: Data Protection Impact Assessment. Rapportage waarin de verwerking van persoonsgegevens wordt geanalyseerd. Dit rapport resulteert in aanbevelingen voor beheersmaatregelen op maat.
PIT: Privacy- en informatie beveiligingsteam: samenwerking tussen de Privacy Officer en de Chief Information Security Officer ter ondersteuning van de organisatie als geheel.
Verwerker: Natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.
Verwerking: Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés , zoals het 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.
Verwerkingsverantwoordelijke: Natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel en de middelen voor de verwerking van persoonsgegevens vaststelt.

Vastgesteld door het college van burgemeester en wethouders van Alphen aan den Rijn op 18 mei 2018,
De secretaris, de burgemeester.