Gemeente Wassenaar

Privacybeleid

Gemeente Wassenaar

Inhoudsopgave

1. Inleiding

De gemeente Wassenaar heeft persoonsgegevens nodig om haar taken uit te kunnen voeren. Zonder de verwerking van persoonsgegevens is het onmogelijk om bijvoorbeeld aan een burger een uitkering te verstrekken of een vergunning te verlenen. De burger moet er hierbij op kunnen vertrouwen dat de gemeente zorgvuldig en veilig met zijn persoonsgegevens omgaat. De verwerking van persoonsgegevens kan risico's met zich meebrengen. Zo kan het voorkomen dat er meer dan noodzakelijk persoonsgegevens van de burger worden verwerkt, wat kan leiden tot een inbreuk op de persoonlijke levenssfeer. Dat risico kan nog vergroot worden naarmate er meerdere soorten persoonsgegevens worden verzameld. Dit is met name van toepassing op het verwerken van bijzondere persoonsgegevens zoals gezondheidsgegevens.
Een ander risico is dat er persoonsgegevens van burgers bij derden terecht komen. Dit kunnen andere burgers zijn of medewerkers die niet bij de verwerking betrokken zijn. Dat zou bijvoorbeeld tot identiteitsfraude kunnen leiden. Hierbij kan het voorkomen dat de burger zich in zijn of haar rechten geschonden voelt als de informatie onbedoeld bekend wordt bij anderen. Het voorkomen daarvan is een belangrijk motief voor het zorgvuldig omgaan met persoonsgegevens van burgers.

2. Principes AVG

Persoonsgegevens worden steeds meer in digitale vorm vastgelegd. Dat stelt nieuwe eisen aan de manier waarop door gemeenten met persoonsgegevens moet worden omgegaan. Pas als sprake is van een gerechtvaardigd, duidelijk omschreven, doel mogen persoonsgegevens worden verzameld. Er mogen niet meer persoonsgegevens worden verzameld dan nodig zijn om het vooraf omschreven doel te bereiken. De gemeente is verplicht om te zorgen voor passende (technische en organisatorische) maatregelen om de persoonsgegevens te beveiligen tegen verlies en onrechtmatige verwerking. De gemeente moet ervoor zorgen dat deze digitale persoonsgegevens afdoende worden beveiligd tegen verlies en onrechtmatige toegang (hacks) zodat de privacy zo optimaal mogelijk wordt beschermd. Het zogenaamde lekken van data moet door de gemeente worden voorkomen. Daarvoor neemt de gemeente maatregelen op het gebied van informatieveiligheid en dataminimalisatie. In het kader van de informatieveiligheid zorgt de gemeente voor bewustzijn bij haar medewerkers als het gaat om de goede omgang met persoonsgegevens en zorgt zij voor technische middelen ter bescherming van persoonsgegevens . Dataminimalisatie houdt in dat alleen die persoonsgegevens worden verzameld die noodzakelijk zijn om het doel te realiseren waarvoor de persoonsgegevens worden verzameld.

Aanleiding voor dit privacy-beleid is de inwerkingtreding van de Algemene Verordening Gegevensbescherming (AVG) per 25 mei 2018. Met de AVG is sprake van een versterking en uitbreiding van privacy-rechten van burgers en ontstaan er meer verantwoordelijkheden voor organisaties. De bevoegdheden van de Europese toezichthouders, voor Nederland de Autoriteit Persoonsgegevens, worden uitgebreid.

Feitelijk is de verantwoordingsplicht (‘accountability’) het centrale begrip binnen de AVG. Het is opgenomen in artikel 5 AVG. De essentie van de verantwoordingsplicht is dat de verwerkingsverantwoordelijke (bij gemeenten in de meeste gevallen het college van burgemeester en wethouders) verantwoordelijk is voor het naleven van deze beginselen, en dat ook kan aantonen. Dus niet de burger hoeft aan te tonen of de gemeente een fout heeft gemaakt, maar de gemeente moet aantonen geen fout te hebben gemaakt.

<u>De 6 principes zijn:</u>

1. Rechtmatigheid, behoorlijkheid, transparantie: De gemeente mag niet in strijd met de wet handelen, moet behoorlijk handelen en voor betrokkenen duidelijk maken en zijn in hoeverre en op welke manier er persoonsgegevens worden verwerkt. Alle communicatie richting betrokkenen moet begrijpelijk zijn, ook met betrekking tot de rechten van betrokkenen.
2. Doelbinding: Persoonsgegevens mogen enkel voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld, en vervolgens alleen verder verwerkt worden wanneer er sprake is van een verenigbaar doel.
3. Minimale gegevensverwerking (‘ dataminimalisatie’): Er mogen niet meer persoonsgegevens worden verwerkt dan strikt noodzakelijk is voor het doel. Verder moet steeds worden gekeken of het doel niet op een minder ingrijpende wijze kan worden bereikt (dit zijn de principes van proportionaliteit en subsidiariteit).
4. Juistheid: Het is van belang dat voortdurend moet worden nagegaan of de persoonsgegevens die de gemeente van betrokkenen verwerkt juist en actueel zijn. Als blijkt dat de gegevens niet meer correct zijn moeten ze door de gemeente gewijzigd of verwijderd worden.
5. Opslagbeperking: Persoonsgegevens mogen niet langer worden bewaard dan nodig is voor het doel van de verwerking.
6. Integriteit en vertrouwelijkheid: De gemeente dient te zorgen voor een goede beveiliging van persoonsgegevens, door het nemen van passende technische of organisatorische maatregelen. De gemeente moet er voor zorgen dat ongeoorloofde toegang tot- en gebruik van persoonsgegevens voorkomen wordt.

In dit beleid wordt richting gegeven hoe de gemeente om gaat met privacy. Zij laat zien dat zij de privacy waarborgt, beschermt en handhaaft. Dit beleid is van toepassing op de gehele organisatie en op alle processen, onderdelen, objecten en gegevensverzamelingen van de gemeente (inclusief WODV) waarin persoonsgegevens worden verwerkt.

2.1 Bijzondere en gevoelige persoonsgegevens

Bijzondere persoonsgegevens en gevoelige persoonsgegevens spelen een belangrijke rol. Bijzondere persoonsgegevens worden in de AVG geregeld, in de praktijk speelt ook het ruimere begrip 'gevoelige gegevens' een rol.

Er worden in de AVG een aantal categorieën van bijzondere persoonsgegevens gehanteerd, die extra privacygevoelig zijn. Het betreft: ras of etniciteit, politieke opvattingen, religie/levensbeschouwing, vakbondslidmaatschap, genetische gegevens, biometrische gegevens, gegevens over gezondheid, gegevens betreffende seksualiteit.

In principe is het verboden om deze gegevens te verwerken, tenzij. De AVG en de Uitvoeringswet AVG bepalen in welke gevallen bijzondere of gevoelige gegevens verwerkt mogen worden. Er zijn uitzonderingen op dat verbod , bijvoorbeeld in het geval betrokkene uitdrukkelijke toestemming heeft gegeven, of in het geval de gemeente de gegevens moet verwerken voor het uitvoeren van een wettelijke taak, zoals bijvoorbeeld de WMO 2015. De gemeente zal met deze bijzondere persoonsgegevens uiterst zorgvuldig omgaan.

Genetische en biometrische gegevens behoren tot de bijzondere persoonsgegevens. Bij biometrische gegevens moet gedacht worden aan een pasfoto op een rijbewijs of paspoort of een vingerafdruk. Deze gegevens worden enkel gebruikt om iemand te identificeren. Ook hier geldt dus: verwerking is verboden, tenzij. De gemeente verwerkt biometrische gegevens enkel als dit nodig is voor het uitvoeren van een wettelijke taak (bijvoorbeeld bij de uitgifte van een paspoort op grond van de Paspoortwet) en niet langer dan nodig is.

Strafrechtelijke gegevens behoren tot de bijzondere persoonsgegevens. Er wordt onder de AVG hiervoor een apart artikel 10 aan gewijd. De gemeente mag o.a. strafrechtelijke gegevens verwerken in het kader van het Veiligheidshuis. Uiteraard mag dat alleen wanneer het strikt noodzakelijk is.

Ook al wordt het onder de AVG geen bijzonder persoonsgegeven genoemd, voor het burger-servicenummer (BSN) blijft gelden dat het enkel gebruikt mag worden wanneer het door de wet is voorgeschreven, en enkel voor de doeleinden gebruikt mag worden die de wet bepaalt. Nederland gaat hier dus verder dan de AVG, en heeft op dit punt gebruik gemaakt van de beleidsvrijheid die de AVG biedt.

Gezien het risico van het verwerken van bijzondere persoonsgegevens voor betrokkenen, zal de gemeente deze alleen door derden niet zijnde een overheidsorganisatie laten verwerken, indien er zwaarwegende belangen zijn. Indien desondanks bijzondere persoonsgegevens niet 'in house' worden verwerkt (maar bij een verwerker), dient het beschermingsniveau gegarandeerd te zijn. Dit betekent ook dat bijzondere persoonsgegevens in beginsel binnen de Europese Economische Ruimte (EER) gehost dienen te worden.

Onder gevoelige persoonsgegevens worden dus ten eerste de bijzondere persoonsgegevens gerekend. Daarnaast behoren financiële persoonsgegevens tot de gevoelige gegevens (bijvoorbeeld gegevens over schulden, salarisstroken, enz.). Verder vallen persoonsgegevens op grond waarvan mensen kunnen worden 'nagewezen' (stigmatisering), zoals bijvoorbeeld gegevens over een goksverslaving, ook onder gevoelige persoonsgegevens. Tenslotte worden wachtwoorden, inloggegevens, Burgerservicenummers, kopieën van identiteitsbewijzen, en bankrekeningnummers tot de gevoelige gegevens gerekend. Indien iemand ten onrechte toegang krijgt tot deze gegevens, kan daarmee (identiteits)fraude gepleegd worden. Dat is een groot risico.

Van belang is dat ook al zou iemand vinden dat het niet erg is als een gevoelig persoonsgegeven bekend wordt ('ze mogen alles van me weten') niet relevant is bij de beoordeling of een persoonsgegeven gevoelig is.

Of een persoonsgegeven gevoelig van aard is speelt ook een rol bij de bepaling of de gemeente persoonsgegevens die voor een bepaald doel zijn verzameld ook mag verwerken voor een ander doel. Hoe gevoeliger het persoonsgegeven, hoe minder snel de gemeente mag en zal aannemen dat er sprake is van een verenigbaar doel.

3. Verantwoordelijkheden binnen de AVG

3.1 Verwerkingsverantwoordelijke

In de AVG wordt derhalve de nadruk gelegd op de verantwoordelijkheid van organisaties en instanties (in de AVG aangeduid als 'verwerkingsverantwoordelijken') om te kunnen aantonen dat zij zich aan de wet houden (accountability). De verwerkingsverantwoordelijke is degene die alleen of samen met anderen het doel van en de middelen voor de verwerking vaststelt.

Het college van B&W respectievelijk de burgemeester respectievelijk bestuur WODV zijn de verantwoordelijke bestuursorganen die, ieder voor zover het hun taakuitoefening betreft, invulling geven aan de taken en verantwoordelijkheid die krachtens de AVG zijn toebedeeld aan de verwerkingsverantwoordelijke. Formeel is het college van B&W respectievelijk de burgemeester respectievelijk het Bestuur van de WODV dan ook verantwoordelijk voor alle verwerkingen die onder de reikwijdte van de AVG vallen.

De verwerkingsverantwoordelijken zijn verantwoordelijk voor:

- De naleving van de beginselen voor de verwerking van persoonsgegevens.
- De maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met dit beleidskader verordening wordt uitgevoerd.

Voor het overgrote deel van de processen, lees persoonsgegevens, zijn de Colleges van B&W respectievelijk de Burgemeesters de verwerkingsverantwoordelijke, terwijl (een groot deel van) het proces zich binnen de WODV afspeelt. Het Bestuur van de WODV is privacy-verwerkingsverantwoordelijke voor een aantal bedrijfsvoeringsprocessen. In het verwerkingsregister wordt vastgelegd wie voor welk proces verantwoordelijk is.

3.2 Lijnmanagement en Privacy-Officer

De dagelijkse verantwoordelijkheid voor de zorgvuldige omgang met persoonsgegevens ligt (logischerwijze) bij de afdelingshoofden. Dat betekent dat de lijn zelf wordt aangesproken op het nakomen van de uit het privacy-beleid voortvloeiende eisen. Privacy is immers niet een op zichzelf staand iets, maar is onlosmakelijk verbonden met de gemeentelijke dienstverlening. Het eigenaarschap van bepaalde processen en systemen waarmee wordt gewerkt, is belegd bij afdelingsmanagers. In die rol zijn zij verantwoordelijk voor het zorgvuldig beheer van alle gegevens in deze systemen, in het bijzonder voor persoonsgegevens, voor deugdelijke classificatie van gegevens en bijbehorende bescherming en voor het toekennen van rechten in deze systemen. Zij zijn verantwoordelijk voor het zodanig uitvoeren van het beleid dat privacy-risico's tot een minimum worden beperkt. De Privacy Officer (PO) biedt ondersteuning op het gebied van advisering bij het handelen conform het privacy-beleid en de privacy-administratie.

3.3 Functionaris voor de gegevensbescherming (FG)

De AVG stelt het aanstellen van een FG verplicht voor overheidsinstanties en publieke organisaties. De FG ziet er op toe dat de organisatie voldoet aan de wettelijke verplichtingen bij het verwerken van persoonsgegevens. Hij is een interne toezichthouder en toetst onder andere de naleving van de wettelijke eisen, gemeentelijke richtlijnen op het gebied van privacy, het privacy-beleid en informatiebeveiligingsbeleid. De FG is een onafhankelijke functionaris die de verwerkingsverantwoordelijke, B&W, Burgemeester en Bestuur WODV rechtstreeks kan adviseren. De functie kent een beperkte overlap met de CISO, die zorg moet dragen voor een samenhangend pakket aan maatregelen om de vertrouwelijkheid, integriteit en beschikbaarheid van de informatie binnen een gemeente te waarborgen. De FG werkt samen met de CISO en de PO.

3.4 CISO

De Concern Informatie Security Officer (CISO) is verantwoordelijk voor het informatiebeveiligingsproces binnen het concern. De CISO stelt kaders op voor informatiebeveiliging en adviseert het bestuur (B&W, Burgemeester, Bestuur WODV) en lijnmanagement hierover. De CISO houdt toezicht op de informatiebeveiligingsmaatregelen, waaronder persoonsgegevens, te beveiligen. De CISO werkt hierbij samen met de FG en PO.

3.5 Verantwoordingsplicht

De verantwoordingsplicht van de gemeente, ook wel accountability genoemd, brengt met zich mee dat de gemeente niet alleen de regels moet naleven, maar ook moet kunnen aantonen deze regels nageleefd te hebben.

In dit kader worden in ieder geval de volgende maatregelen getroffen:

1. Een actueel en volledig register van verwerkingen en het publiceren van een abstract van het register.
2. Opname in het verwerkingenregister van (een verwijzing) naar alle relevante documenten die betrekking hebben op de naleving van de verplichtingen uit de AVG, zoals informatieplicht en de afspraken met verwerkers.
3. Openbaarmaking van het onderhavige privacy-beleid.
4. Zorgen voor de aantoonbaarheid van de juiste behandeling van informatie. Tevens houdt de verantwoordingsplicht in dat de gemeenten en de WODV een register van datalekken die zijn opgetreden, bijhoudt en, waar passend, een gegevensbeschermingseffect-beoordeling (DPIA) uitvoert.

NB. Bij een datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens zonder dat dit de bedoeling is of toegestaan is.

4. Governance

Het college van B&W, Burgemeester c.q. bestuur WODV is integraal verantwoordelijk voor de bescherming van persoonsgegevens en de uitvoering van de AVG binnen de werkprocessen van de gemeente en voor de gemeente door de WODV. De specifieke rol van het college is het vaststellen van kaders en normen voor privacybescherming en het voldoen aan wet- en regelgeving (compliance) op dit gebied. Het College c.q. Bestuur WODV legt verantwoording af over uitvoering en handhaving van deze kaders en normen.

4.1 Overzicht en inzicht

De gemeente moet overzicht en inzicht hebben voor wie de gemeente aansprakelijk is. Hoe groot is de “corporate familie” en verbonden partijen (verwerkers), alsmede de achterliggende partijen (sub-verwerkers). Voor gemeenten is het verkrijgen van het gewenste overzicht een lastige opgave omdat een gemeente met veel organisaties samenwerkt en het niet altijd duidelijk is op basis van welke titel de samenwerking is ingericht.

En natuurlijk is het verkrijgen van overzicht over welke persoonsgegevens er binnen de gemeente zelf allemaal verwerkt worden essentieel. Het hebben van een betrouwbare inventarisatie en vervolgens deze actueel houden (verwerkingenregister), is een belangrijke basis om verdere maatregelen te kunnen treffen.

4.2 Privacy-administratie

Het systematisch vastleggen van verwerkingen van persoonsgegevens, het bewijs van effectieve werking van de getroffen beheers- en beveiligingsmaatregelen, en incidenten en datalekken dienen te worden opgenomen in een administratie. De leiding, het College of Bestuur, gebruikt de administratie voor het afleggen van verantwoording gegevensbescherming aan het maatschappelijk verkeer. Er is dus een privacy administratie nodig op basis waarvan de gemeente de naleving van “de wet” kan aantonen (artikel 5.2 AVG, de verantwoordingsplicht/accountability).

4.3 Accountable

De gemeente is accountable en verantwoord zich aan het maatschappelijk verkeer. Hierbij zijn 2 soorten te onderscheiden:

a. De betrokkenen (burgers en medewerkers) kunnen hun passieve en actieve rechten uitoefenen. Passieve rechten hebben voornamelijk betrekking op het door de gemeente accountable zijn en dat aan de betrokkene informeren. Dus: de juiste informatie verstrekken, ook wel transparant zijn over de wijze van verwerken van persoonsgegevens. De betrokkene kan zijn / haar actieve rechten uitoefenen door vragen

te stellen aan de gemeente. Voor de betrokkene (burgers en medewerkers) is de FG met assistentie van de PO het eerste aanspreekpunt om mee te communiceren. Als die er niet is dan kan de betrokkene zich wenden tot de AP.

b. De gemeente verantwoordt zich over hoe zij omgaat met privacy, wat haar beleid in deze is en verantwoordt zich achteraf over hoe dat is uitgevoerd.

4.4 Hoe zou de governance en compliance van de privacy georganiseerd moeten worden?

De gemeentelijke planning en control cyclus is in essentie zo opgebouwd dat in het jaar t-1 (het jaar voor het begrotingsjaar) de voornemens worden opgesteld en de daarbij behorende middelen worden bepaald in de vorm van een kadernota of Perspectiefnota en vervolgens worden vastgesteld in de begroting. Met de vaststelling van de begroting wordt daarmee het ambitieniveau van een onderwerp voor het volgende jaar vastgelegd.

Na afloop van een jaar, in het voorjaar t+1, worden vervolgens een jaarverslag en jaarrekening opgesteld, waarmee door B&W/Bestuur WODV verantwoording over het afgelopen jaar wordt afgelegd.

4.5 De voornemens

Het governance- en compliance-model van privacy volgt dit stramien van de gemeentelijke Planning en Control. Het start met het opstellen en vaststellen van Privacy-beleid, de voornemens worden in de begroting meegenomen en uiteindelijk is het dan onderdeel van het jaarverslag en jaarrekening als onderdeel van de algehele maatschappelijke verantwoording. In de loop van het jaar en na afloop van het jaar vindt evaluatie van het beleid plaats, die zo nodig tot aanpassing van het beleid kan leiden.
Het privacy-beleid, de voornemens, zal opgebouwd gaan worden aan de hand van een normenkader en een indeling in volwassenheidsniveau. Door het hanteren van volwassenheidsniveaus kan het privacy-beleid een groeimodel worden.

4.6 De vastlegging

Een belangrijke voorwaarde is dat de Privacy Organisatie gebruik maakt van een adequate administratie met overzicht en inzicht in het verantwoordelijkheids- en aansprakelijkheidsdomein van de gemeente, actuele verwerkingen, een aan wet- en regelgeving gerelateerde normenset, bewijs van effectieve werking beheers- en beveiligingsmaatregelen, incidenten / datalekken en overzicht van besluiten van de feitelijk leidinggevenden alsmede uitkomsten van beheer. Een verwerkingenregister en een register van incidenten is reeds aanwezig. Het register van verwerkingen wordt geactualiseerd en zal ook daarna regelmatig een actualisatie behoeven. De andere administraties worden komende periode opgebouwd.

In situaties waarin het niet direct rechtstreeks duidelijk is of in een bepaalde situatie persoonsgegevens gebruikt mogen worden of gedeeld mogen worden, zal, indien het de bedoeling is een betere kwaliteit na te streven van het desbetreffende beleid, de afweging om de persoonsgegevens toch te gebruiken navolgbaar worden vastgelegd.

4.7 De verantwoording

Artikel 5.2 AVG: de verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van “de wet” en kan dit aantonen (“verantwoordingsplicht”). In artikel 24 AVG wordt het duidelijk dat het gaat om het kunnen overleggen van het bewijs van effectieve werking van getroffen beheers- en beveiligingsmaatregelen die naleving van de AVG borgen. Een samenvattende verantwoording wordt opgenomen in het jaarverslag en is daarmee een onderdeel van de maatschappelijke verantwoording.
In het bovenstaande governance & compliance model kunnen wij vier actoren met een wettelijke status onderkennen. B&W (en bestuur WODV) verantwoordt zich voor de gang van zaken van de gemeente c.q. werkorganisatie met behulp van jaarrekening plus jaarverslag / bestuurdersverslag aan het maatschappelijk verkeer. Hier past ook in een (maatschappelijke) verantwoording over het gevoerde privacy-beleid.

Op termijn zal deze verantwoording worden gecombineerd met de in control verklaring (rechtmatigheidsverklaring), die voor gemeenten verplicht wordt. Dat kan dan in de vorm van een zogenaamde DOA (Declaration of Accountability).

4.8 Uitvoering
Indien daar aanleiding toe is, kan in de voortgangsrapportages gedurende het jaar worden gerapporteerd over de lopende uitvoering van het privacybeleid.

4.9 Plaats in de P&C-producten
De voornemens en verantwoording van privacy zouden voor de gemeenten het beste passen in het programma 0: Bestuur en ondersteuning. Bij de WODV ligt het meest voor de hand om ze in het hoofdstuk Beleidsbegroting op de nemen.

5.0 Rol FG in governance
De FG heeft, conform zijn wettelijke taken, in dit kader een tweetal taken:

1. Hij ziet er op toe dat privacy-administratie inderdaad gedegen wordt uitgevoerd.
2. Voordat B&W/bestuur WODV een besluit neemt over de privacy-verantwoording of voornemens brengt de FG hierover een advies uit.

5. WODV en de gemeenten Wassenaar en Voorschoten
WODV kan je beschouwen als ware het een afdeling binnen de gemeente. Het staat daarbij dichter bij de gemeenten dan andere samenwerkingspartners. De 2 gemeenten en de WODV passen de AVG toe en zijn daarvoor accountable naar elkaar en naar het maatschappelijk verkeer. Met als doel de accountability effectief en kostenefficiënt te regelen is het verstandig dat WODV met de gemeenten een overeenkomst afsluit c.q. afspraken over privacy vastlegt.

De WODV heeft zelf als verantwoordelijke slechts een beperkt aantal eigen processen, waarvoor zij in privacy-termen zelf verantwoordelijke is, namelijk op het terrein van bedrijfsvoering. Voor alle overige processen zijn de beide gemeenten (B&W en Burgemeester) in privacy-termen de verantwoordelijke.

6. Rechten van betrokkenen
Binnen het beleid worden de volgende rechten van betrokkenen geborgd:

Recht op informatie
De gemeente verzamelt gegevens om haar taken te kunnen uitvoeren. Indien dit persoonsgegevens betreffen, heeft de gemeente de plicht om betrokkenen, voor zover deze daar niet reeds van op de hoogte zijn, te informeren over verwerkingen van hun persoonsgegevens. De gemeente verstrekt dan aan betrokkenen informatie over de verwerking, zoals het doel daarvan, welke persoonsgegevens worden verwerkt en of de gegevens aan anderen worden verstrekt. Dit met inachtneming van de beperkingen zoals die neergelegd zijn in wet- en regelgeving.

Daartoe zal een relevant deel van het register van verwerkingen ook worden gepubliceerd op de website van respectievelijk gemeente Voorschoten, gemeente Wassenaar en de WODV.

Recht op inzage
Betrokkenen hebben de mogelijkheid om te controleren of en op welke manier hun gegevens worden verzameld en verwerkt. Dit wordt uitgevoerd met inachtneming van de beperkingen zoals neergelegd in wet- en regelgeving. Voor de verwerking van deze verzoeken is een procedure opgesteld.

Recht op correctie
Als de gemeente persoonsgegevens van betrokkenen verwerkt die naar hun oordeel onjuist zijn, kunnen zij een verzoek indienen bij de gemeente om dit te verbeteren. Dit met inachtneming van de beperkingen zoals neergelegd in wet- en regelgeving.

Recht om vergeten te worden
Betrokkenen hebben het recht persoonsgegevens te laten verwijderen indien de gemeente niet langer een goede grond heeft voor het gebruik hiervan, bijvoorbeeld indien betrokkenen een gegeven toestemming intrekken, indien de gegevens onjuist zijn of de gegevens niet langer nodig zijn.

Recht op bezwaar tegen verwerking
Betrokkenen hebben het recht aan de gemeente te vragen hun persoonsgegevens niet meer te gebruiken en bezwaar te maken tegen de verwerking van hun persoonsgegevens. De gemeente moet hieraan voldoen, tenzij er gerechtvaardigde gronden zijn voor de verwerking.

Recht op beperking van de verwerking
Het recht op beperking houdt in dat de gemeente de persoonsgegevens (tijdelijk en onder voorwaarden) niet mag verwerken en niet mag wijzigen, bijvoorbeeld wanneer betrokkenen de juistheid van de gegevens ter discussie stellen.

Recht op overdraagbaarheid van gegevens (dataportabiliteit)
De gemeente is vanuit de AVG niet verplicht invulling te geven aan overdraagbaarheid van gegevens voor zover het werkzaamheden betreft in het kader van algemeen belang, de uitoefening van een openbaar gezag, wanneer deze zijn openbare taken uitoefent of aan een wettelijke verplichting voldoet. Desondanks zal de gemeente in voorkomende gevallen voorzieningen treffen in het kader van dataportabiliteit.

Recht niet te worden onderworpen aan geautomatiseerde individuele besluitvorming/profiling
Uitgangspunt in de AVG is dat er geen geautomatiseerde besluitvorming op basis van profilering mag plaatsvinden, als daaraan rechtsgevolgen voor de betrokkene (degene wiens persoonsgegevens het betreft) zijn verbonden of het besluit hem in aanmerkelijke mate treft. Daarbij kan gedacht worden aan bijvoorbeeld de kredietwaardigheid van een persoon. Een ander voorbeeld is het verwerken van sollicitaties via internet zonder menselijke tussenkomst.

6.1 Uitoefening van rechten
Om gebruik te maken van de bovenstaande rechten kunnen de betrokkenen een verzoek indienen. Dit verzoek kan zowel schriftelijk als via de website van de gemeente ingediend worden. Binnen vier weken beoordeelt de gemeente of het verzoek gerechtvaardigd is. De gemeente c.q. WODV laat binnen die termijn weten wat er met het verzoek gaat gebeuren, waaronder of de gemeente de behandeling van het verzoek met twee maanden verlengt. De gemeente c.q. de WODV behandelt het verzoek volgens de daarvoor door haar vastgestelde en bekendgemaakte procedure.

Als het verzoek niet op tijd wordt opgevolgd, deelt de gemeente c.q. WODV uiterlijk binnen vier weken mee waarom het verzoek zonder gevolg is gebleven. De betrokkene heeft dan de mogelijkheid om bezwaar te maken bij de gemeente of een klacht in te dienen bij de Autoriteit Persoonsgegevens (AP).

6.2 Bewustwording
Er wordt gezorgd voor voldoende bewustwording bij de medewerkers op het gebied van privacy. Hierbij dienen zij minimaal op de hoogte te zijn van de privacyregels en de voor hun werkzaamheden relevante bepalingen zodat zij deze in hun dagelijkse werk kunnen toepassen.

7. Interne regelingen afspraken

7.1 Meldplicht datalekken

Indien zich een datalek voordoet, waarbij bijvoorbeeld gegevens van personen in verkeerde handen kunnen komen of zijn gekomen, handelt de gemeente in overeenstemming met de vastgestelde werkwijze in het Protocol Meldplicht en afhandeling van (vermoedelijke) datalekken. Dit protocol bevat een vastgesteld proces van te doorlopen stappen om de eventuele schade of de kans hierop, bij een datalek te beperken en de getroffen perso(o)n(en) te beschermen. In ieder geval wordt een datalek intern gemeld aan de FG.

Het gaat bij een datalek om situaties waarbij een onrechtmatige verwerking van persoonsgegevens heeft plaatsgevonden of kan plaatsvinden, waarbij beveiligingsmaatregelen (on)bewust zijn omzeild of doorbroken of dat geen of onvoldoende beveiligingsmaatregelen zijn genomen. Het gaat ook om situaties waarbij persoonsgegevens verloren zijn gegaan, waardoor ze niet meer beschikbaar zijn, en om situaties waarin gegevens in handen kunnen komen of zijn gekomen van derden die geen toegang tot die gegevens mogen hebben.

De plicht tot het melden aan de Autoriteit Persoonsgegevens van een (vermoeden van een) datalek geldt als er sprake is van een aanzienlijke kans op ernstige nadelige gevolgen voor betrokkene(n), dan wel ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. Het betreft situaties van het (mogelijk) lekken van persoonsgegevens uit gemeentelijke bestanden en/of gegevens waarvoor de gemeente verantwoordelijkheid draagt. Wanneer er een dergelijk datalek heeft plaatsgevonden, wordt dit zonder onredelijke vertraging, uiterlijk 72 uur nadat er kennis van de inbreuk is vernomen, gemeld aan de Autoriteit Persoonsgegevens. 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 wordt dit datalek ook aan de betrokkenen gemeld, in eenvoudige en duidelijke taal.

7.2 Het register van verwerkingsactiviteiten

De functionaris voor gegevensbescherming (FG) houdt namens de verantwoordelijke er toezicht op dat er een register van verwerkingen van persoonsgegevens wordt bijgehouden. De PO draagt zorg voor de inschrijving van de verwerkingen van persoonsgegevens in dit register. Afdelingsmanagers dienen (nieuwe) verwerkingen of wijzigingen direct aan de PO te melden.

<u>Bij de inschrijving worden in ieder geval de volgende gegevens vermeld:</u>

a. de naam van de verwerking;

b. wie de verantwoordelijke is voor de verwerking;

c. het doel van de verwerking;

d. de groep van personen van wie persoonsgegevens worden verwerkt (betrokkenen);

e. de categorie persoonsgegevens die bij de verwerking worden gebruikt;

f. de ontvangers van de gegevens;

g. de rechtmatige grondslag voor de verwerking van de persoonsgegevens;

h. eventuele verstrekkingen aan andere landen buiten de Europese Economische Ruimte;

i. de verwijderingstermijnen die in acht genomen worden;

De FG houdt toezicht op de volledigheid en rechtmatigheid van de in het register ingeschreven verwerkingen van persoonsgegevens en de daarbij behorende documenten (eventuele verwerkersovereenkomst, model Gegevensbeschermingseffectbeoordeling, privacy-protocol, informatieverplichting), de registratie van incidenten.

7.3 Gegevensbeschermingseffectbeoordeling (DPIA)

Een Gegevensbeschermingseffectbeoordeling (DPIA) is een instrument waarmee het effect van beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens op een gestructureerde en heldere manier in beeld in kaart wordt gebracht om vervolgens maatregelen te kunnen nemen om de risico's te verkleinen. Een Gegevensbeschermingseffectbeoordeling wordt doorgaans uitgevoerd met ondersteuning van de PO, voorafgaand aan de verwerking en maar ook bij bestaande verwerkingen waarvoor hij nog niet eerder was uitgevoerd en waar sprake is van een gegevensverwerking die een hoog privacy-risico oplevert voor de betrokkenen.

Tevens heeft de AP nog een lijst samen gesteld voor verwerkingen waarbij een Gegevensbeschermingseffectbeoordeling altijd verplicht is.

Of er sprake is van een hoog privacy-risico, toetst de gemeente aan de hand van een Risk Impact Assessment (RIA). De RIA wordt uitgevoerd op het moment dat een van de BIV-classificaties 2 of hoger scoort. Dus naast de Vertrouwelijkheid, waar privacy geraakt wordt, ook op Beschikbaarheid en Integriteit.

Op grond van de AVG is verder in ieder geval sprake van een hoog privacy-risico indien de gemeente:

- Systematisch en uitvoerig persoonlijke aspecten evalueert, waaronder profiling;
- Op grote schaal bijzondere persoonsgegevens verwerkt of op grote schaal en systematisch mensen volgt in een publiek toegankelijk gebied; Hierbij wordt gelet op het aantal betrokkenen, het volume van gegevens en/of het bereik van verschillende gegevens/items die worden verwerkt, de duur of het permanente karakter van de gegevensverwerkingsactiviteit en de geografische omvang van de verwerkingsactiviteit;
- Indien wordt voldaan aan twee of meer criteria van de in bijlage 1 opgenomen criteria van de werkgroep van Europese privacy-toezichthouders (WP29).

Voor de Gegegevensbeschermingseffectbeoordeling gelden de volgende kaders:

1. Een Gegevensbeschermingseffectbeoordeling vindt plaats voordat met de betreffende verwerking wordt gestart.

2. Een Gegevensbeschermingseffectbeoordeling wordt herhaald bij wijzigingen waardoor de risico's van de verwerking toenemen.

3. Bij het uitvoeren van een Gegevensbeschermingseffectbeoordeling wordt de FG altijd geïnformeerd.

4. Het afdelingshoofd ziet toe op het nemen van maatregelen die blijkens de Gegevensbeschermingseffectbeoordeling nodig zijn om de risico's te verkleinen.

5. Het resultaat van de Gegevensbeschermingseffectbeoordeling en de genomen maatregelen om het risico te beperken worden aan de FG voorgelegd ter toetsing en opneming in het registerverwerkingen.

6. Gegevensbeschermingseffectbeoordelingen die binnen de gemeente worden uitgevoerd vinden plaats volgens een gemeentelijke standaard.

7.4 Overgangsregeling

Voor verwerkingen met een hoog privacy-risico die voor 25 mei 2018 al bestonden is een Gegevensbeschermingseffectbeoordeling (DPIA) na deze datum verplicht indien:

1. De verwerking verandert, bijvoorbeeld door nieuwe technologie of wijziging van doel;

2. Het risico verandert;

3. De omgeving verandert, bijvoorbeeld door maatschappelijke veranderingen.

Deze overgangstermijn eindigt op 25 mei 2021. Dan dient derhalve voor iedere verwerking met een hoog risico een DPIA te zijn uitgevoerd.

7.5 Inschakeling verwerkers, verwerkersovereenkomst

Wanneer de gemeente een partij inschakelt om ten behoeve van de gemeente persoonsgegevens te verwerken en het verwerken van de persoonsgegevens de primaire taak is van deze partij, kan deze partij worden beschouwd als verwerker. De gemeente schakelt enkel verwerkers in die afdoende garanties bieden met betrekking tot het toepassen van passende technische, procesmatige, communicatieve en organisatorische maatregelen. De afspraken omtrent de verwerking door de verwerker worden schriftelijk vastgelegd in een verwerkersovereenkomst. Deze worden vastgelegd voordat de dienstverlening aanvangt. Daarna worden deze afspraken periodiek of steekproefsgewijs getoetst.

Inmiddels is door de VNG een standaardverwerkingsovereenkomst vastgesteld, die alle gemeenten dienen te gebruiken.

In sommige gevallen treedt de gemeente op als verwerker voor derden. Hierbij zijn deze derden de Verwerkingsverantwoordelijke. De gemeente streeft er in deze gevallen naar voor deze verwerkingen heldere en eenduidige voorwaarden op te stellen voor gelijksoortige verwerkingen. De gemeente biedt daarbij aan de Verwerkingsverantwoordelijke voldoende garanties voor het zorgvuldig verwerken van gegevens door het toepassen van passende technische en organisatorische maatregelen. De afspraken omtrent de verwerking worden schriftelijk vastgelegd in een verwerkersovereenkomst, voordat de dienstverlening door de gemeente aanvangt.

Voor de gemeenten Voorschoten en Wassenaar is het gewenst afspraken met de WODV op dit punt vast te leggen.

Verder kan het voorkomen dat de gemeente een andere partij inschakelt, die geen verwerker is, maar waarmee wel persoonsgegevens worden uitgewisseld. Ook dan maakt de gemeente passende afspraken. In dat geval zal de gemeente een overeenkomst sluiten omtrent de verwerking van persoonsgegevens, of samen met de andere partij een regeling vaststellen, waarin de respectieve verantwoordelijkheden worden vastgelegd.

De gemeente laat regelmatig taken door anderen uitvoeren of geeft subsidie voor het doen van activiteiten. Daarbij zullen de organisaties die deze taken uitvoeren of subsidie voor ontvangen ook meestal persoonsgegevens verwerken. Voor deze verwerkingen zal de gemeente in de meeste gevallen niet de privacy-verantwoordelijke zijn, maar de gemeente heeft wel een zekere kwaliteitsverantwoordelijkheid. In dat kader zal de gemeente er op toezien dat deze organisaties veilig met persoonsgegevens omgaan. Dit kan bijvoorbeeld voor de WMO door middel van het Toezicht WMO worden uitgevoerd.

7.6 Camerabeelden

De gemeente past op verschillende plekken binnen haar organisatie registratie van bewegende beelden toe. Voorbeelden hiervan zijn beelden van bewakingscamera’s, burgerloketten en wachtkamers. Voor elke registratie van camerabeelden bepaalt de gemeente of en hoe lang deze worden bewaard.
Er worden videotulen gemaakt van raads- en commissievergaderingen. Eventuele insprekers worden daarover ingelicht en toestemming gevraagd.

7.7 Toegang medewerkers

Medewerkers mogen alleen toegang tot die persoonsgegevens hebben die zij voor hun werk nodig hebben. Het is gewenst dit zorgvuldig vast te leggen en hierop regelmatig een controle op te houden. Hiertoe worden zo veel als mogelijk in de systemen harde toegangsgrenzen ingericht. Hiertoe moeten alle systemen van logging zijn voorzien en dient er op gezette tijd een controle te worden uitgevoerd op basis van die logging-gegevens. De uitkomsten hiervan worden gedurende een bepaalde tijd bewaard.

8. Actieve publicatie van persoonsgegevens

Gemeenten publiceren regelmatig persoonsgegevens. Het kan zijn door openbaarmaking van besluitenlijsten, door raads- en collegestukken, door bezwaarschriften, vergunningen enz.

Om persoonsgegevens te mogen publiceren is een wettelijke grondslag nodig om dat in dat specifieke geval te mogen doen en soms kan het ook op grond van toestemming van betrokkene. Dit is een noodzakelijkheidsvereiste!

8.1 Artikel 8 WOB

1. Het bestuursorgaan dat het rechtstreeks aangaat, verschaft uit eigen beweging informatie over het beleid, de voorbereiding en de uitvoering daaronder begrepen, zodra dat in het belang is van een goede en democratische bestuursvoering.

2. Het bestuursorgaan draagt er zorg voor dat de informatie wordt verschaft in begrijpelijke vorm, op zodanige wijze, dat belanghebbende en belangstellende burgers zoveel mogelijk worden bereikt en op zodanige tijdstippen, dat deze hun inzichten tijdig ter kennis van het bestuursorgaan kunnen brengen.

Het verstrekken van overheidsinformatie uit eigen beweging is een verplichting voor ieder overheidsorgaan, die ontstaat zodra het verstrekken in het belang is van een goede en democratische bestuursvoering.

De plicht om informatie openbaar te maken kan – wanneer deze overheidsinformatie persoonsgegevens bevat – stuiten op het belang van eerbiediging van de persoonlijke levenssfeer. Welk belang in welke mate prevaleert, is afhankelijk van welke soort persoonsgegevens het betreft en mogelijk van een te maken belangenafweging van enerzijds het algemeen belang om bepaalde informatie openbaar te maken en anderzijds het belang van de betrokkene van bescherming van de persoonlijke levenssfeer te veel wordt aangetast. Indien de openbaarmaking het belang van bescherming van de persoonlijke levenssfeer teveel aantast, dan dient openbaarmaking achterwege te blijven.

8.2 Uitwerking van de vereisten

Ingevolge de AVG mogen persoonsgegevens alleen worden verwerkt als daar een grondslag voor bestaat. Een van die grondslagen is: "de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen." Artikel 8 eerste lid van de WOB is een voorbeeld van een dergelijke verplichting. (artikel 8, lid 1, WOB: Het bestuursorgaan dat het rechtstreeks aangaat, verschaft uit eigen beweging informatie over het beleid, de voorbereiding en de uitvoering daaronder begrepen, zodra dat in het belang is van een goede en democratische bestuursvoering.)

De AVG maakt gebruik van het woord 'noodzakelijk'. Dit noodzakelijkheidsbegrip moet breed worden opgevat, dus betekent **indien** en **voor zover**. Dat houdt in dat er twee afwegingen gemaakt moeten worden:

1. de vraag **of** een verwerking van persoonsgegevens moet plaatsvinden, maar eveneens;
2. de vraag in **welke mate** persoonsgegevens verwerkt moeten worden.

Een dergelijke verwerking behoeft ingevolge de artikelen 5 en 6 van de AVG de afweging of dat dit noodzakelijk is, rekening houdend met het doel waardoor de verwerking geschiedt. Een dergelijke afweging dient **navolgbaar** te gebeuren, dat wil zeggen hij dient vastgelegd te worden opdat eventueel later er op kan worden teruggegrepen en kan worden bewezen dat er een zorgvuldige afweging heeft plaatsgevonden. De beoordeling van de noodzakelijkheid heeft daarna ook invloed op de wijze waarop de gemeente voornemens is de gegevens openbaar te maken. Artikel 8 verplicht immers niet tot een bepaalde vorm van openbaarmaking. De vorm van openbaarmaking is een aan de openbaarmaking gelieerde verwerking maar dient wel een eigen doel. Openbaarmaking op het internet kan in dat kader qua noodzakelijkheid een andere uitkomst hebben, dan ter inzage legging of losse verstrekking.

Als gevolg van het spanningsveld tussen de plicht tot openbaarheid en het recht op eerbiediging van de persoonlijke levenssfeer rust op het bestuursorgaan de plicht om bij actieve openbaarmaking een inbreuk op het recht op de eerbiediging van de persoonlijke levenssfeer te vermijden dan wel zo beperkt mogelijk te houden. Anders gezegd: het bestuursorgaan moet openbaarmaking van persoonsgegevens in overheidsinformatie achterwege laten als het doel daarvan, namelijk openbaarmaking, ook langs andere weg en met minder ingrijpende middelen kan worden bereikt.

Bij publicatie moet het bestuursorgaan derhalve alle mogelijkheden beoordelen om die inbreuk te beperken, bijvoorbeeld door wel het besluit te publiceren maar de persoonsgegevens weg te laten, er moet voldaan zijn aan het noodzakelijkheidsvereiste. **Het is niet tenzij…..**

In geval van openbaarmaking van overheidsinformatie moet het doel van de publicatie/kennisgeving /bekendmaking voor ogen worden gehouden. Bijvoorbeeld: in het geval van het kennisgeven van een besluit op de aanvraag van een omgevingsvergunning, is het relevant om te weten op welk adres de omgevingsvergunning is aangevraagd. Belanghebbenden moeten zichzelf immers als zodanig kunnen herkennen. Daarbij is het echter niet nodig dat degene aan wie de vergunning is verleend, met naam en toenaam wordt genoemd. Ergo: als er al vanwege het onderwerp toch persoonsgegevens gepubliceerd moeten worden: dan zo min mogelijk, gelet op het doel van de publicatie.

Op het openbaar maken van bijzondere persoonsgegevens, maar ook het BSN-nummer, rust in beginsel een verbod. De WOB en de AVG voorzien theoretisch in uitzonderingsgronden maar dat zal slechts in zeer uitzonderlijke gevallen gebruikt kunnen worden. **Hier geldt in principe nooit….**

Overigens geldt ook beeld- en geluidsmateriaal, waarop personen herkenbaar zijn, als een persoonsgegeven.

Een voorbeeld: bij de publicatie van aanvragen voor omgevingsvergunningen kan worden volstaan met de adresgegevens van de aanvrager. E-mailadres, BSN-nummer of handtekening doen hier niet ter zake voor publicatie en mogen dan ook niet gepubliceerd worden.

8.3 B&W besluitenlijsten

Artikel 60 lid 3 van de gemeentewet bepaalt dat Colleges hun besluitenlijsten moeten publiceren: Het college maakt de besluitenlijst van zijn vergaderingen op de in de gemeente gebruikelijke wijze openbaar. Het college laat de openbaarmaking achterwege voor zover het aangelegenheden betreft ten aanzien waarvan op grond van artikel 55 geheimhouding is opgelegd of ten aanzien waarvan openbaarmaking in strijd is met het openbaar belang.

Dit artikel betekent dat besluitenlijsten openbaar gemaakt moeten worden. Het betekent niet dat achterliggende stukken openbaar moeten worden. En het verplicht niet tot openbaarmaking noch publicatie van persoonsgegevens. Het al dan niet openbaar maken en publiceren van namen of andere persoonsgegevens is dus afhankelijk van de beoordeling van de noodzakelijkheid. Over het algemeen zal het in beginsel niet noodzakelijk zijn persoonsgegevens openbaar te maken.

Soms kan het noemen van namen van functionarissen echter bijdragen aan een goede informatievoorziening van de gemeente. Dat is bijvoorbeeld bij de benoeming in een functie het geval. Maar ook dan zal afgewogen moeten worden welke persoonsgegevens dienstig zijn om te vermelden in dat geval.

Bij een besluit op bezwaar, op een aanvraag, zouden ook persoonsgegevens van burgers openbaar kunnen worden. Hier komt een belangenafweging tussen openbaarheid en transparantie en de behoefte aan privacy aan te pas. De afdeling Bestuursrechtspraak van de Raad van State neemt als vertrekpunt dat openbaarmaking achterwege moet blijven als dit in strijd is met het openbaar belang, waarbij onder openbaar belang mede begrepen moet worden de bescherming van de persoonlijke levenssfeer.

Anders gezegd anonimisering is aan de orde als het belang van de eerbiediging van de persoonlijke levenssfeer zwaarder weegt dan het belang van publicatie van persoonsgegevens in de besluitenlijst. Daarbij dient rekening te worden gehouden met de aard van het besluit waarmee de betrokkene in verband wordt gebracht en anderzijds de risico’s verbonden aan het openbaar maken van bepaalde persoonlijke gegevens. Daarbij dient nadrukkelijk te worden bedacht dat

alleen die persoonsgegevens dienen te worden vermeld die van uitdrukkelijk belang zijn voor de aard van het besluit. Het is aan de gemeente om deze belangenafweging te maken. Afgewogen moet dus worden of het, gezien de aard van het besluit, of er, en zo ja welke, meerwaarde er uitgaat van publicatie van persoonsgegevens als adresgegevens en/of van namen.

9. Deelnemingen

Vaak hebben gemeenten taken uitbesteed aan Gemeenschappelijke Regelingen (GR'en; op basis van juridische titel) en samenwerkingsverbanden (zonder juridische titel). Meestal is er dan sprake van uitbesteding van en of meerdere verwerkingen. Maar soms is een GR zelfstandig verwerkingsverantwoordelijke en voeren zij een resultaatsverplichting uit (Bijvoorbeeld in de uitvoering van de participatiewet of gemeentelijke belastingwetten).

De gemeenten Wassenaar en Voorschoten hebben verschillende soorten deelnemingen. Bij de meeste deelnemingen heeft de gemeente wel invloed, maar is niet alleen bepalend voor het uitzetten van de koers.

Voor het beantwoorden van de vraag of deze deelnemingen een eigen privacy-beleid behoeven en of ze zelf verwerkingsverantwoordelijke zijn, zijn de volgende criteria van belang:

1. Verwerkt de deelneming veel persoonsgegevens?
2. Bepaalt de deelneming zelf doel en middelen van de persoonsgegevens?

De deelnemingen betreffen voor Voorschoten en Wassenaar veelal gemeenschappelijke regelingen. Deelnemingen en samenwerkingen moeten door de komst van de AVG in zoverre in een ander daglicht worden beschouwd dat in veel gevallen het gemeentebestuur toch verantwoordelijk en aansprakelijk is en blijft voor de uitvoeringsprocessen door de GR'en en samenwerkingen voor wat betreft privacy.

Het is een kwestie van de juiste balans vinden tussen de inspanningen die gedaan moeten worden en de middelen die beschikbaar zijn voor de uitvoering. Gevolgen voor de gemeenten, GR'en en samenwerkingsverbanden zijn:

· Er is ketenaansprakelijkheid door gebruik te maken van GR'en en samenwerkingsverbanden, leveranciers, etc.;

· Aandacht voor privacy-overeenkomsten door de ketenaansprakelijkheid is belangrijk teneinde heldere onderlinge afspraken te hebben.