GEGEVENSBESCHERMINGSBELEID

APG GROEP (APG)

INHOUDSOPGAVE

1 Strategisch

In dit hoofdstuk wordt ingegaan op de strategische uitgangspunten die APG Groep N.V. (APG) hanteert met zijn Gegevensbeschermingsbeleid.

1.1 Doel Gegevensbeschermingsbeleid

APG verzorgt als financiële dienstverlener bestuursadvisering, assetmanagement, pensioenadministratie, pensioencommunicatie en werkgeversdiensten. Daarnaast worden in de pensioenmarkt inkomensaanvullingen aangeboden aan individuen. APG voert deze werkzaamheden uit namens (pensioen)fondsen en werkgevers in de sectoren onderwijs, overheid, bouw, schoonmaak en glazenwassers, woningcorporaties, energie- en nutsbedrijven, sociale werkvoorziening, architectenbureaus en medisch specialisten.

In het kader van deze dienstverlening aan of ten behoeve van opdrachtgevers, externe partijen en klanten verwerkt APG op grote schaal persoonsgegevens. Ook van zijn medewerkers en overige voor hem werkzaam zijnde personen verwerkt APG persoonsgegevens. Tenslotte verwerkt APG persoonsgegevens van bezoekers, ook die van zijn websites.

APG hecht grote waarde aan een rechtmatige, behoorlijke, transparante en daarmee kwalitatieve verwerking van persoonsgegevens. APG wil vertrouwen bieden aan zijn opdrachtgevers, externe partijen, klanten, medewerkers en overige betrokkenen in de wijze waarop hij met hun persoonsgegevens en privacy omgaat.

Snelle technologische ontwikkelingen, innovatie en globalisering zijn nieuwe uitdagingen voor de bescherming en verwerking van persoonsgegevens. De hiermee gepaard gaande voortschrijdende digitalisering stelt nieuwe en andere eisen aan het omgaan met data in het algemeen en persoonsgegevens in het bijzonder.

Afgeleid van de generieke (compliance) doelstelling van APG van een integere en beheerste uitvoering van de bedrijfsactiviteiten, stelt APG zich een zorgvuldige en naar behoren bescherming en verwerking van persoonsgegevens ten doel.

Met dit Gegevensbeschermingsbeleid wil APG uitdrukking geven aan die bewustwording op het waarborgen van gegevensbescherming.
In dit beleid zijn de uitgangspunten opgenomen die APG hanteert bij de bescherming en verwerking van persoonsgegevens.

1.2 Scope Gegevensbeschermingsbeleid

Het Gegevensbeschermingsbeleid van APG is van toepassing op:
- de gehele APG-organisatie, d.w.z. alle interne en externe medewerkers alsmede overige personen die voor APG werkzaam zijn;
- alle processen en procedures inzake gegevensverwerking die APG voor zijn opdrachtgevers, externe partijen, klanten, medewerkers en overige betrokkenen uitvoert;

• alle bedrijfsonderdelen en 100% deelnemingen van APG; en
• alle verwerkingsactiviteiten en gegevensverzamelingen die door of namens APG worden verricht.

1.3 Privacy governance

De privacy wet- en regelgeving vormt een bijzonder onderdeel van compliance.
Privacy is als compliance thema opgenomen in het compliance risicoraamwerk dat op zijn beurt geïntegreerd is in het integrale risicomanagement van APG (AIR).

Vanuit de in paragraaf 1.1 genoemde grote waarde die APG hecht aan een zorgvuldige en adequate bescherming en verwerking van persoonsgegevens, acht APG het essentieel en randvoorwaardelijk dat er een efficiënte en effectieve privacy governancestructuur binnen APG is ingericht.

1.3.1 Centrale inrichting

De Raad van bestuur van APG is (eind)verantwoordelijk voor een zorgvuldige en juiste naleving van de privacy wet- en regelgeving.

Binnen APG is het toezicht op de bescherming van de privacy en de verwerking van persoonsgegevens toebedeeld aan de functionaris voor de gegevensbescherming.

Een functionaris voor de gegevensbescherming is een wettelijk gereguleerde functionaris die:
• informeert en adviseert over de privacyverplichtingen;
• toezicht houdt op de toepassing en naleving van de privacy wet- en regelgeving en het gegevensbeschermingsbeleid;
• advies verstrekt over de gegevensbeschermingseffectbeoordeling (zie ook par. 4.4) en toeziet op de uitvoering ervan;
• het contact onderhoudt met de toezichthoudende autoriteit, de Autoriteit Persoonsgegevens; en
• rapporteert aan de raad van bestuur van APG.

In de situaties waarin APG als verwerker (zie par. 2.5.2) optreedt, informeert of rapporteert de functionaris voor de gegevensbescherming conform de met de opdrachtgevers hierover gemaakte afspraken over de toepassing en naleving van de privacy wet- en regelgeving en dit gegevensbeschermingsbeleid door APG in relatie tot de gegevensverwerkingen die de opdrachtgever aan APG heeft uitbesteed.

APG zorgt er voor dat:
• de functionaris voor de gegevensbescherming naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens;
• de functionaris voor de gegevensbescherming wordt ondersteund met bevoegdheden en middelen om zijn taken te kunnen vervullen en zijn deskundigheid in stand te kunnen houden;

• de functionaris voor de gegevensbescherming zijn rol onafhankelijk kan vervullen;
• de functionaris voor de gegevensbescherming geen nadeel ondervindt bij de uitvoering van zijn taken;
• betrokkenen contact kunnen opnemen met de functionaris voor de gegevensbescherming over hun gegevensverwerkingen en de uitvoering van hun rechten;
• de functionaris voor de gegevensbescherming geen andere taken en plichten binnen APG vervult die leiden tot een belangenconflict.

De functionaris voor de gegevensbescherming is aangemeld bij de Autoriteit Persoonsgegevens Ingeval een functionaris voor de gegevensbescherming is benoemd, stelt de Autoriteit Persoonsgegevens zich terughoudend op in zijn toezichtrol.

1.3.2 Decentrale inrichting

Binnen de decentrale bedrijfsonderdelen van APG zijn de desbetreffende directies verantwoordelijk voor een zorgvuldige en juiste naleving van de privacy wet- en regelgeving door hun respectievelijk onderdeel.

Binnen de bedrijfsonderdelen zijn specifieke functionarissen, privacy officers, aangewezen die er op toezien dat de externe en interne privacyregels, waaronder die van de functionaris voor de gegevensbescherming, worden nageleefd binnen het bedrijfsonderdeel waaraan ze zijn toebedeeld. Zij zorgen er voor dat binnen het bedrijfsonderdeel effectieve en efficiënte processen op privacy en verwerking van persoonsgegevens zijn ingericht. Zij rapporteren hierover aan zowel het management en de directie van het desbetreffende bedrijfsonderdeel alsook aan compliance en de functionaris voor de gegevensbescherming, zodat deze laatste zijn taken zoals beschreven onder 1.3.1 zorgvuldig en naar behoren kan uitvoeren.

Het omgaan met privacy en het verwerken van persoonsgegevens maken onderdeel uit van het integrale en decentrale risicomanagement beheersproces dat binnen APG is uitgerold. Door de bedrijfsonderdelen worden in het kader van deze interne beheersing specifieke op privacy en het verwerken van persoonsgegevens afgestemde beheers- en controlemaatregelen uitgevoerd. Deze worden door compliance gereviewd.
De functionaris voor de gegevensbescherming wordt door de bedrijfsonderdelen en compliance geïnformeerd over de (controle respectievelijk review)bevindingen op privacy en de verwerking van persoonsgegevens, zodat hij zijn taken zoals beschreven onder 1.3.1 zorgvuldig en naar behoren kan uitvoeren.

De bevindingen van de bedrijfsonderdelen, compliance en de functionaris voor de gegevensbescherming worden gerapporteerd via daarvoor voorziene risk- en compliance rapportages aan directies, raad van bestuur en, indien en voor zover afgesproken, aan opdrachtgevers.

2 Wet- en regelgeving

In dit hoofdstuk wordt stilgestaan bij de wettelijke en overige regelgeving die op het Gegevensbeschermingsbeleid van APG van toepassing is. Verduidelijkt wordt welke (beleids)uitgangspunten APG hanteert zowel op beginselniveau als ten aanzien van bijzondere situaties bij de verwerking van persoonsgegevensprincipes, om te voldoen aan deze wet- en regelgeving en te waarborgen dat de hieruit voor APG voortvloeiende verplichtingen worden nageleefd.

2.1 Wettelijke kaders

De bescherming van persoonsgegevens is een grondrecht dat in het Handvest van de grondrechten van de Europese Unie en het Verdrag betreffende de werking van de Europese Unie is vastgelegd. De Algemene verordening gegevensbescherming ('Verordening' of 'AVG') is een Europese wet die de bescherming van dit grondrecht regelt (de officiële benaming is 'General Data Protection Regulation', ook wel 'GDPR').

De AVG is vanaf 25 mei 2016 in werking getreden en is vanaf 25 mei 2018 rechtstreeks toepasselijk in de gehele Europese Unie. Zij vervangt van laatstgenoemde datum de Nederlandse Wet bescherming persoonsgegevens (Wbp). De Wbp was gebaseerd op de voorloper van de AVG, de Europese Richtlijn gegevensbescherming.

Bij het invullen en uitvoeren van zijn Gegevensbeschermingsbeleid en de omgang met persoonsgegevens houdt APG rekening met:

- de AVG (regelt de rechtmatige en zorgvuldige omgang met persoonsgegevens binnen de Europese Unie);
- de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG; regelt met name de rol en positie van de Autoriteit Persoonsgegevens, het gebruik van bijzondere categorieën van persoonsgegevens zoals biometrische en genetische gegevens, en van persoonsidentificerende gegevens, zoals het Burgerservicenummer.

Daarnaast is er specifieke Europese en nationale wetgeving die op onderdelen (m.n. cookie- en spamregels) betekenis heeft of kan hebben voor APG. Indien en voor zover de daarin opgenomen regels van toepassing zijn op en betekenis hebben voor de bescherming en verwerking van persoonsgegevens door APG, houdt APG ook met deze regelgeving rekening. Het gaat daarbij om:

- De Europese richtlijn betreffende privacy en elektronische communicatie (E-privacy richtlijn);
- de Telecommunicatiewet (hoofdstuk 11: bescherming van persoonsgegevens en de persoonlijke levenssfeer).

2.2 Begripsbepalingen

APG hanteert in het kader van zijn Gegevensbeschermingsbeleid en bij zijn verwerking van persoonsgegevens dezelfde begripsbepalingen als vastgelegd in de AVG dan wel overige van toepassing zijnde wet- of regelgeving.

2.3 Verwerkingsbeginselen

Iedere verwerking van persoonsgegevens moet voldoen aan de in deze paragraaf te benoemen beginselen. Deze verwerkingsbeginselen vormen het normatieve kader van het Gegevensbeschermingsbeleid. Zij worden nader geconcretiseerd in de rechten die opdrachtgevers, externe partijen, klanten, medewerkers en overige betrokkenen ten aanzien van de verwerking van hun persoonsgegevens door APG hebben en in de verplichtingen die APG heeft om deze gegevensverwerkingen zorgvuldig en naar behoren uit te voeren om daarmee te voldoen aan de eisen en verplichtingen die de privacy wet- en regelgeving stellen.

2.3.1 Rechtmatigheid, behoorlijkheid en transparantie

APG verwerkt persoonsgegevens alleen voor gerechtvaardigde doeleinden (zie par. 2.4). APG zorgt er voor dat de verwerking correct en op verantwoorde wijze gebeurt. Ook maakt APG duidelijk voor welke doelen en op welke wijze persoonsgegevens worden verwerkt. Deze duidelijkheid verschaft APG onder meer middels de op zijn website(s) te publiceren privacyverklaring.

2.3.2 Doelbinding

APG verzamelt persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. De gegevens worden alleen voor een ander doel gebruikt als dat doel niet onverenigbaar is met de oorspronkelijke verzameldoeleinden.

2.3.3 Dataminimalisatie

APG verwerkt alleen persoonsgegevens die toereikend, ter zake dienend en noodzakelijk zijn voor de doeleinden waarvoor ze worden verwerkt. Dit betekent dat APG zich beperkt tot een minimale gegevensverwerking.

2.3.4 Juistheid

APG zorgt er voor dat de persoonsgegevens juist en actueel zijn. APG neemt alle redelijke maatregelen om er voor te zorgen dat gegevens die dat niet (meer) zijn, worden gewist of gerectificeerd.

2.3.5 Opslagbeperking

APG bewaart persoonsgegevens niet langer in een identificeerbare vorm dan noodzakelijk is voor de doeleinden waarvoor ze worden verwerkt.

2.3.6 Integriteit en vertrouwelijkheid

APG neemt passende technische en organisatorische maatregelen om te waarborgen dat de persoonsgegevens passend zijn beveiligd. De persoonsgegevens moeten worden beschermd tegen ongeoorloofde of onrechtmatige verwerking en tegen (on)opzettelijk verlies, vernietiging of beschadiging. Een belangrijke maatregel om dit te waarborgen betreft het inregelen van een procedure *melden datalekken* (zie par. 5.2).

2.4 Verwerkingsgrondslagen

Elke gegevensverwerking moet gerechtvaardigd zijn. Om gerechtvaardigd te zijn moet de verwerking te baseren zijn op tenminste een van de in de AVG vastgelegde verwerkingsgrondslagen. Voor APG zijn niet alle verwerkingsgrondslagen relevant. Of een verwerkingsgrondslag relevant is hangt onder meer af van het doel dat met de gegevensverwerking wordt beoogd.

De relevante verwerkingsgrondslagen voor APG zijn:
- de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden (zie ook par. 2.6.1);
- de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen;
- de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op APG rust[1]; of
- de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen (bv. fraudepreventie, direct marketing, bestrijden cybersecurity) van APG of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van de persoonsgegevens nopen, zwaarder wegen dan die belangen.

Bij de *noodzakelijkheidsgrondslagen* maakt APG de afweging of de verwerkingen noodzakelijk en daarmee gerechtvaardigd zijn voor de in deze grondslagen genoemde doeleinden. Hierbij wordt gekeken of de verwerking van gegevens proportioneel is en of zij voldoet aan de eis van subsidiariteit.

De vraag of de verwerking proportioneel is, beoordeelt APG aan de hand van de criteria van *effectiviteit* en *evenredigheid*.
Een verwerking is effectief als met de gegevensverwerking het gestelde doel kan worden bereikt of als dat zeer waarschijnlijk is.
Een verwerking is evenredig als het doel dat met de verwerking wordt nagestreefd in verhouding staat tot het feit dat persoonsgegevens worden verwerkt.

Bij de vraag of de verwerking subsidiair is, kijkt APG of het doel niet op een andere, minder op de privacy ingrijpende wijze kan worden bereikt.

Alleen als de gegevensverwerking niet te baseren valt op een van de *noodzakelijkheidsgrondslagen*, is toestemming van de betrokkene voor de gegevensverwerking nodig. Ook een verwerking op de grondslag *toestemming* moet voldoen aan de eisen van proportionaliteit en subsidiariteit.

[1] deze wettelijke plicht moet een grondslag hebben in het recht van de Europese Unie dan wel van een unierechtelijke lidstaat

De verwerkingsgrondslag *gerechtvaardigd belangen* dient afgewogen, zorgvuldig en onderbouwd te zijn. Dit omwille van het feit dat het hierbij gaat om een belangenafweging tussen enerzijds het belang van de gegevensverwerkende verwerkingsverantwoordelijke of derde en anderzijds dat van de betrokkene. Het belang van de betrokkene staat voorop. Beoordeeld moet worden of de gegevensverwerking al dan niet onredelijk indruist tegen de belangen, de grondrechten en de fundamentele vrijheden van de betrokkene. Anders gezegd, beoordeeld moet worden of de betrokkene redelijkerwijs die gegevensverwerking wel of niet mag verwachten.

Bij gerechtvaardigd belangen gaat het om verwerkingen die noodzakelijk zijn voor en ten dienste staan aan een adequate, zorgvuldige, behoorlijke en verantwoorde bedrijfsvoering van APG. Het moet gaan om reële, concrete en rechtstreekse belangen.

Als APG gebruik maakt van de verwerkingsgrondslag *gerechtvaardigde belangen*, worden niet alleen die belangen vastgelegd, maar ook:
- het doel van de verwerking
- het type te verwerken persoonsgegevens
- met wie de persoonsgegevens worden gedeeld
- de bewaartermijn van de gegevens

Betrokkene heeft het recht bezwaar te maken tegen een verwerking op grond van gerechtvaardigde belangen. De gegevensverwerking moet in dat geval worden stopgezet, tenzij APG kan aantonen dat zijn belangen of die van een derde zwaarder wegen dan die van betrokkene. Bij een bezwaar tegen direct marketing wordt de verwerking onmiddellijk stopgezet (zie ook par. 3.7).

2.5 Verwerkingsverantwoordelijke en verwerker

APG verwerkt persoonsgegevens als verwerkingsverantwoordelijke, maar ook als verwerker. In welke hoedanigheid APG deze gegevens verwerkt, hangt af van de aard van zijn bedrijfsvoering en dienstverlening alsook van zijn juridische bevoegdheid of positie ten opzichte van de gegevensverwerking.

De mate waarin of de wijze waarop de (wettelijke) privacyverplichtingen op APG van toepassing zijn, zijn afhankelijk van de rol, functie en verantwoordelijkheid die APG heeft ten aanzien van de verwerking van persoonsgegevens. De privacy wet- en regelgeving legt aan een verwerkingsverantwoordelijke meer omvattende, zwaardere en strakkere verplichtingen op dan aan een verwerker. Ten gronde is en blijft de verwerkingsverantwoordelijke verantwoordelijk voor de gegevensverwerking door de verwerker. Althans in zoverre de verwerker verwerkingsactiviteiten verricht in opdracht van en ten behoeve van de verwerkingsverantwoordelijke (zie ook hoofdstuk 4).

2.5.1 Verwerkingsverantwoordelijke

APG is verwerkingsverantwoordelijke voor alle verwerkingen van persoonsgegevens waarvan hij het doel van en de middelen voor de gegevensverwerking vaststelt. Dit is het geval bij alle gegevensverwerkingen waarvan APG bepaalt welke persoonsgegevens worden verwerkt, voor welk doel dit gebeurt en met welke middelen dit plaatsvindt.

APG is verwerkingsverantwoordelijke in de situaties:

- waar hij de impliciete bevoegdheid heeft om persoonsgegevens te verwerken;

Dit wordt afgeleid van de gangbare juridische regels en de maatstaven in het maatschappelijk verkeer. Deze situatie doet zich voor bij het verwerken van persoonsgegevens van medewerkers of directe klanten van APG, zoals bij inkomensaanvullingen of werkgeversdiensten.

- waar hij de feitelijke invloed heeft op de verwerking van persoonsgegevens.

Het gaat er dan om wie daadwerkelijk de beslissingen neemt en feitelijk bepaalt wat er met de gegevens gebeurt. De juridische verhoudingen tot en de contractuele afspraken met partijen voor wie persoonsgegevens worden verwerkt, zijn hier relevante aanknopingspunten.

Wanneer APG samen met anderen, zoals opdrachtgevers en externe partijen, doel van en middelen voor de gegevensverwerking bepaalt, kan er sprake zijn van gezamenlijke verwerkingsverantwoordelijkheid. Of hiervan sprake is, hangt in belangrijke mate af van de juridische verhoudingen tot en de contractuele afspraken met die opdrachtgevers en externe partijen. De facto valt deze situatie onder die van welke feitelijke invloed heeft APG op de gegevensverwerking.

2.5.2 Verwerker

APG is verwerker wanneer hij ten behoeve van een verwerkingsverantwoordelijke persoonsgegevens verwerkt, zonder dat hij aan diens rechtstreekse gezag is onderworpen of in een hiërarchische verhouding tot die verwerkingsverantwoordelijke staat.

Het gaat hier om gegevensverwerking die in opdracht aan APG is gegeven en waar de dienstverlening van APG volledig gericht is op het uitvoering geven aan die opdracht en onderliggende instructies. Van dergelijke gegevensverwerking is sprake bij het uitvoeren van werkzaamheden voor (pensioen)fondsen en werkgevers.

2.6 Bijzondere situaties

In deze paragraaf is een aantal bijzondere situaties met betrekking tot het verwerken van persoonsgegevens opgenomen waar APG in zijn bedrijfsvoering en bij zijn dienstverlening meer dan incidenteel mee te maken krijgt of kan krijgen en waarvan het essentieel en relevant is dat APG daar beleid op voert.

2.6.1 Toestemming

Een van de rechtsgrondslagen voor een gerechtvaardigde gegevensverwerking is toestemming (zie par. 2.4).

Er is sprake van rechtsgeldige toestemming als deze:
• vrij gegeven is en betrokkene de vrije keuze heeft te weigeren;
• specifiek en geïnformeerd is, zodat betrokkene voldoende informatie heeft om een afgewogen beslissing te kunnen nemen;
• ondubbelzinnig is, waardoor geen twijfel bestaat dat betrokkene toestemming heeft gegeven.

De bewijslast dat toestemming is gegeven ligt bij APG. Om die reden zorgt APG er voor dat toestemming alleen gegeven kan worden middels een ondubbelzinnige wilsuiting of ondubbelzinnige actieve handeling van betrokkene.

Bij het vragen van toestemming informeert APG gelijktijdig over de mogelijkheid dat de toestemming op ieder moment kan worden ingetrokken.

APG registreert en beheert de afgegeven of ingetrokken toestemmingen.

2.6.2 Bijzondere categorieën van persoonsgegevens

Verwerking van bijzondere categorieën van persoonsgegevens (bijv. gegevens over ras, etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, seksueel gedrag, vakbondslidmaatschap of genetische, biometrische of gezondheidsgegevens) is omwille van de gevoeligheid in beginsel verboden.

APG verwerkt bijzondere categorieën van persoonsgegevens dan ook alleen in situaties dat de privacy wet- en regelgeving hierop uitzonderingen toestaat èn de verwerking gerechtvaardigd is alsook aan de overige verwerkingseisen voldoet.

De voor APG relevante algemene uitzonderingsgronden zijn:
• betrokkene heeft zijn uitdrukkelijke toestemming gegeven;
Uitdrukkelijke toestemming gaat nog een stapje verder dan ondubbelzinnige toestemming (voor niet-bijzondere categorieën van persoonsgegevens) en houdt in dat er op geen enkele wijze ook maar enige twijfel mag bestaan of de betrokkene toestemming heeft gegeven.
• de verwerking is noodzakelijk in het kader van de uitvoering van regels op het gebied van arbeids- en sociaal zekerheidsrecht;
• de verwerking noodzakelijk is voor de instelling, uitoefening of onderbouwing van een rechtsvordering; of
• de verwerking betrekking heeft op persoonsgegeven die kennelijk door de betrokkene openbaar zijn gemaakt.

Daarnaast zijn er specifieke uitzonderingsgronden, waarin APG bijzondere categorieën van persoonsgegevens mag verwerken zoals:
• persoonsgegevens over ras en etnische afkomst mogen verwerkt worden als dit noodzakelijk is voor: – de identificatie van de betrokkene;

– het toekennen van een bevoorrechte positie aan personen van een bepaalde etnische of culturele minderheidsgroep teneinde feitelijke nadelen, verband houdende met de grond ras of etnische afkomst, op te heffen of te verminderen.

• biometrische gegevens mogen verwerkt worden als dit noodzakelijk is voor authenticatie of beveiligingsdoeleinden;
• gezondheidsgegevens mogen verwerkt worden als dit noodzakelijk is voor:
– een goede uitvoering van wettelijke voorschriften, pensioenregelingen of collectieve arbeidsovereenkomsten die voorzien in aanspraken die afhankelijk zijn van de gezondheidstoestand van de betrokkene;
– de re-integratie of begeleiding van medewerkers of uitkeringsgerechtigden in verband met hun gezondheid.

2.6.3 Strafrechtelijke persoonsgegevens

Naast de categorieën van bijzondere persoonsgegevens zijn ook persoonsgegevens van strafrechtelijke aard gevoelige persoonsgegevens die alleen onder specifieke in de privacy wet- en regelgeving genoemde voorwaarden mogen worden verwerkt. Deze voorwaarden worden met name genoemd in de Uitvoeringswet AVG (UAVG).

Onder strafrechtelijke gegevens worden verstaan:
• persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen; of
• persoonsgegevens betreffende een door de rechter opgelegd verbod naar aanleiding van onrechtmatig of hinderlijk gedrag.

Persoonsgegevens van strafrechtelijke aard mogen worden verwerkt, indien en voor zover hier voor APG van belang:
• de betrokkene uitdrukkelijke toestemming heeft gegeven voor de verwerking van die persoonsgegevens voor een of meer welbepaalde doeleinden;
• de verwerking betrekking heeft op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt;
• de verwerking noodzakelijk is voor de instelling, uitoefening of onderbouwing van een rechtsvordering;
• de verwerking gebeurt ter beoordeling van een verzoek van de betrokkene om een beslissing over hem te nemen of aan hem een prestatie te leveren;
• het gaat om strafbare feiten die zijn of op grond van feiten en omstandigheden naar verwachting zullen worden gepleegd jegens APG of jegens personen die in zijn dienst zijn;
• de regels zoals vastgesteld in de Wet op de ondernemingsraden (WOR), worden gevolgd als het gaat om medewerkers in dienst van APG.

2.6.4 Burgerservicenummer (BSN)

APG verwerkt nationale identificatienummers, waarvan het meest gangbare voorbeeld het Burgerservicenummer (BSN) is, uitsluitend als hiervoor een wettelijke grondslag bestaat. APG

gebruikt het BSN alleen als er geen gelijkwaardige minder op de privacy ingrijpende identificerende alternatieven zijn.

2.6.5 Privacy by design en by default

APG houdt bij het ontwikkelen van nieuwe producten en diensten en het ontwerp van nieuwe gegevenssystemen rekening met de eisen die de privacy en de gegevensbescherming stellen aan de omgang met persoonsgegevens.

APG zorgt er voor dat de inbreuk op de privacy of persoonlijke levenssfeer bij de gegevensverwerking tot een minimum beperkt blijft. Daartoe neemt APG passende technische en organisatorische maatregelen om de gegevensbeschermingsbeginselen, zoals het alleen verwerken van noodzakelijke gegevens, op een doeltreffende en zorgvuldige wijze uit te voeren en de bescherming van persoonsgegevens te waarborgen.

3 Rechten betrokkene

In dit hoofdstuk wordt ingegaan op de versterkte en vernieuwde rechten die door de AVG aan de betrokkene zijn toegekend.

APG houdt in dit beleid rekening met de grondgedachte achter de AVG dat de betrokkene een eerlijke en transparante verwerking van persoonsgegevens moet kunnen verwachten, waarbij hij deze rechten op een gemakkelijke en eenvoudige wijze moet kunnen uitoefenen naar de verwerkingsverantwoordelijke.

3.1 Informatie en communicatie

APG informeert de betrokkene over de gegevensverwerkingen en communiceert met hem over zijn rechten in duidelijke en eenvoudige taal. APG zorgt er voor dat deze informatie en communicatie in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm plaatsvindt. Dit kan schriftelijk, maar ook met elektronische middelen gebeuren. Als betrokkene daarom verzoekt, kan dit zelfs mondeling.

APG faciliteert de betrokkene in de uitoefening van zijn rechten. Dit kan door het beschikbaar stellen van een digitale voorziening dan wel van een standaardformulier.

Het verstrekken van de informatie, de communicatie of het treffen van de maatregelen om de rechten te kunnen uitoefenen, gebeurt kosteloos. Alleen wanneer de verzoeken van de betrokkene kennelijk ongegrond of buitensporig zijn, kan APG:

- een redelijke administratieve vergoeding aanrekenen; of
- de verzoeken zelfs weigeren.

APG informeert de betrokkene uiterlijk binnen een maand na ontvangst van het verzoek om uitvoering van zijn rechten over het gevolg dat aan het verzoek is gegeven. Afhankelijk van de complexiteit van het verzoek kan deze termijn met nog eens twee maanden worden verlengd. Van deze verlenging wordt de betrokkene binnen een maand na ontvangst van het verzoek in kennis gesteld.

Wanneer APG geen gevolg geeft aan het verzoek, deelt hij dat de betrokkene uiterlijk binnen een maand na ontvangst van het verzoek gemotiveerd mee. Ook informeert APG hem daarbij op de mogelijkheid om klacht in te dienen bij de Autoriteit Persoonsgegevens (zie ook par. 7.1) en beroep bij de rechter (zie ook par. 7.2).

Om de betrokkene te informeren over hoe APG omgaat met persoonsgegevens en gegevensverwerkingen stelt APG een privacyverklaring op. De privacyverklaring wordt indien nodig periodiek vernieuwd en geplaatst op de website(s) van APG.

3.1.1 Informatie bij persoonsgegevens van de betrokkene verkregen

Indien de persoonsgegevens van de betrokkene zelf worden verkregen, verstrekt APG op het moment van de verkrijging van die gegevens aan de betrokkene in ieder geval informatie over:

- de contactgegevens van APG
- de contactgegevens van de functionaris voor de gegevensbescherming;
- de doeleinden waarvoor de gegevens worden verwerkt;
- de rechtsgrond van de verwerking en de gerechtvaardigde belangen als deze de rechtsgrond zijn;
- in voorkomend geval, de (categorieën van) ontvangers van de persoonsgegevens;
- in voorkomend geval, bij voorgenomen doorgifte van persoonsgegevens aan een land of een internationale organisatie buiten de Europese Unie:
  - of er een adequaatheidsbesluit van de Europese Commissie is;
  - of en welke passende of geschikte waarborgen zijn getroffen en hoe en waar ze kunnen worden geraadpleegd.

Aanvullend verstrekt APG alle informatie die nodig is om tegenover de betrokkene een behoorlijke en transparante verwerking te waarborgen.

Als APG de persoonsgegevens voor een ander niet onverenigbaar doel gaat gebruiken dan waarvoor hij ze verkregen heeft, verstrekt APG de betrokkene voor die verdere verwerking informatie over dat andere doel en alle relevante verdere informatie.

Deze informatieverstrekking blijft achterwege indien en voor zover de betrokkene reeds over deze informatie beschikt.

3.1.2 Informatie bij persoonsgegevens buiten de betrokkene om verkregen

Indien de persoonsgegevens buiten de betrokkene om worden verkregen (bijv. via andere organisaties zoals UWV, SVB), verstrekt APG uiterlijk binnen een maand na de verkrijging er van aan de betrokkene in beginsel dezelfde informatie als die verstrekt wordt ingeval de persoonsgegevens van de betrokkene zelf worden verkregen.
Als extra informatie worden nog vermeld:

- de betrokken categorieën van persoonsgegevens; en
- de bron waaruit de persoonsgegevens verkregen zijn.

Ook hier verstrekt APG alle informatie die nodig is om tegenover de betrokkene een behoorlijke en transparante verwerking te waarborgen.

Indien de persoonsgegevens aan een andere ontvanger worden verstrekt, informeert APG de betrokkene uiterlijk op het tijdstip waarop de gegevens voor het eerst aan die andere ontvanger worden verstrekt.

Als APG de persoonsgegevens voor een ander niet onverenigbaar doel gaat gebruiken dan waarvoor hij ze verkregen heeft, verstrekt APG de betrokkene voor die verdere verwerking informatie over dat andere doel en alle relevante verdere informatie.

Deze informatieverstrekking blijft achterwege indien en voor zover:
- de betrokkene reeds over deze informatie beschikt;
- het informeren onmogelijk blijkt of onevenredig veel inspanning zou vergen;
- de betrokkene op grond van andere wet- of regelgeving over de informatie beschikt;
- vertrouwelijkheid is gevraagd in verband met een beroepsgeheim.

3.2 Inzage

Indien de betrokkene gebruik maakt van zijn recht om inzage te krijgen in de persoonsgegevens die APG van hem verwerkt, verleent APG hem deze inzage en geeft hem informatie over:
- de verwerkingsdoeleinden;
- de categorieën van persoonsgegevens;
- de (categorieën van) ontvangers van de persoonsgegevens;
- indien mogelijk, hoe lang de persoonsgegevens worden bewaard;
- het recht op rectificatie, wissen, beperking en bezwaar;
- het recht om klacht in te dienen bij de Autoriteit Persoonsgegevens;
- de bron van die gegevens als ze niet van betrokkene zelf afkomstig zijn;
- het bestaan van geautomatiseerde besluitvorming, waaronder profilering, en het belang en de verwachte gevolgen van die verwerking voor de betrokkene.

Wanneer APG de persoonsgegevens doorstuurt naar een land of een internationale organisatie buiten de Europese Unie, informeert APG de betrokkene over de passende waarborgen inzake deze doorgifte.

De genoemde informatie wordt middels een kopie verstrekt. Wanneer de betrokkene zijn verzoek elektronisch indient en niet om een andere regeling verzoekt, verstrekt APG de informatie in een gangbare elektronische vorm.

3.3 Rectificatie

Indien de betrokkene gebruik maakt van zijn recht op rectificatie, zorgt APG er voor dat de betrokkene zijn persoonsgegevens kan rectificeren indien deze onjuist of onvolledig zijn.

APG stelt partijen met wie de gerectificeerde persoonsgegevens gedeeld zijn op de hoogte van de wijzigingen. Dit informeren blijft achterwege wanneer:
- dit onmogelijk blijkt; of
- een onevenredige inspanning vergt.

3.4 Wissing en vergetelheid

Indien de betrokkene gebruik maakt van zijn recht op gegevenswissing en vergetelheid, zal APG de persoonsgegevens van de betrokkene zo snel mogelijk wissen in een van de volgende situaties:

• de persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor zij zijn verzameld of anderszins verwerkt;
• betrokkene trekt zijn toestemming voor het verwerken in en dit is de enige grondslag waarop de verwerking berust of kan berusten;
• betrokkene heeft gegrond bezwaar gemaakt tegen een verwerking:
- op basis van onder meer de grondslag *noodzakelijk voor de behartiging van het gerechtvaardigd belangen van de verwerkingsverantwoordelijke of van een derde;* of
- ten behoeve van direct marketing;
• de persoonsgegevens zijn onrechtmatig verwerkt;
• de persoonsgegevens moeten worden gewist om te voldoen aan een wettelijke verplichting die op APG rust.

Naast het recht op wissing heeft de betrokkene onder bepaalde omstandigheden ook het recht om *vergeten te worden* ('vergetelheid'). Het gaat hier om de situatie waarbij de verwerkingsverantwoordelijke persoonsgegevens van de betrokkene openbaar heeft gemaakt (bijv. door ze online te zetten). Het recht om vergeten te worden geldt voor iedereen, maar in het bijzonder bij de verwerking van gegevens van kinderen.

Deze situatie is feitelijk niet aan de orde bij de gegevensverwerkingen die APG verricht. APG plaatst niet publiekelijk, d.w.z. openbaar op internet persoonsgegevens van betrokkenen, anders dan van bij of voor APG werkzame personen waarbij het online zetten nodig is voor de dienstverlening door APG.

APG stelt partijen met wie de persoonsgegevens die worden gerectificeerd, gedeeld zijn op de hoogte van de wijzigingen. Dit informeren blijft achterwege wanneer:
• dit onmogelijk blijkt; of
• een onevenredige inspanning vergt.

3.5 Beperking

Indien de betrokkene gebruik maakt van zijn recht op beperking van de verwerking, stopt APG de gegevensverwerking wanneer:
• de juistheid van de persoonsgegevens wordt betwist;
• de verwerking onrechtmatig is;
• APG de persoonsgegevens niet meer nodig heeft voor de verwerkingsdoeleinden, maar de betrokkene ze nodig heeft ten behoeve van een rechtsvordering;
• de betrokkene bezwaar maakt tegen de verwerking op basis van de rechtsgrond *gerechtvaardigd belang* in afwachting van de vraag of de gerechtvaardigde belangen van APG zwaarder wegen dan die van de betrokkene.

Wanneer de verwerking is beperkt, verwerkt APG alleen nog persoonsgegevens:
- met toestemming van de betrokkene;
- in het kader van een rechtsvordering;
- ter bescherming van de rechten van andere personen; of
- gewichtige redenen van algemeen belang.

APG stelt partijen met wie de persoonsgegevens die worden beperkt, gedeeld zijn op de hoogte van de wijzigingen. Dit informeren blijft achterwege wanneer:
- dit onmogelijk blijkt; of
- een onevenredige inspanning vergt.

3.6 Overdraagbaarheid

Indien de betrokkene gebruik maakt van zijn recht op overdraagbaarheid van de persoonsgegevens die hijzelf aan APG heeft verstrekt ('dataportabiliteit'), zorgt APG er voor dat de betrokkene een kopie krijgt van deze gegevens in een gestructureerde, gangbare en machineleesbare vorm.

Het recht op overdraagbaarheid geldt alleen voor de door de betrokkene verstrekte gegevens die geautomatiseerd worden verwerkt op basis van de grondslagen:
- ondubbelzinnige dan wel uitdrukkelijke toestemming van de betrokkene;
- noodzakelijk voor de uitvoering van een overeenkomst.

3.7 Bezwaar

Indien de betrokkene gebruik maakt van zijn recht van bezwaar tegen gegevensverwerking op basis van de grondslag *gerechtvaardigd belangen*, stopt APG de verwerking, tenzij de belangen voor APG om de persoonsgegevens te verwerken zwaarder wegen dan de belangen van de betrokkene om de gegevensverwerking te staken.

Indien de betrokkene bezwaar maakt tegen de verwerking van persoonsgegevens voor direct marketing, stopt APG de verwerking onmiddellijk en onvoorwaardelijk.

Indien de betrokkene bezwaar maakt tegen de verwerking van bijzondere persoonsgegevens waaruit ras of etnische afkomst blijkt, voor het toekennen van een bevoorrechte positie teneinde feitelijke nadelen, verband houdende met de grond ras of etnische afkomst, op te heffen of te verminderen, stopt APG de verwerking onmiddellijk en onvoorwaardelijk.

APG informeert de betrokkene over dit recht bij het eerste contact bij gegevensverwerking op basis van *gerechtvaardigd belangen* en bij het eerste direct marketing-contact.

3.8 Geautomatiseerde individuele besluitvorming, waaronder profilering

De betrokkene heeft het recht om niet te worden onderworpen aan een enkel op geautomatiseerde verwerking (waaronder profilering) gebaseerd besluit, wanneer dit:

- rechtsgevolgen voor hem heeft; of
- het hem anderszins in aanzienlijke mate treft.

APG staakt een dergelijke verwerking, tenzij:

- dit noodzakelijk is voor de totstandkoming of de uitvoering van een overeenkomst tussen de betrokkene en een verwerkingsverantwoordelijke;
- de betrokkene zijn uitdrukkelijke toestemming heeft gegeven;
- dit is toegestaan bij wet.

Indien gebruik wordt gemaakt van de eerste twee uitzonderingen, neemt APG maatregelen die tenminste het volgende omvatten:

- het recht op menselijke tussenkomst;
- het recht voor de betrokkene om zijn standpunt kenbaar te maken; en
- het recht om het besluit aan te vechten.

APG baseert geautomatiseerde individuele besluiten niet op bijzondere categorieën van persoonsgegevens tenzij:

- betrokkene daarvoor uitdrukkelijke toestemming heeft gegeven;
- het gebruik noodzakelijk is met het oog op een zwaarwegend algemeen belang op grond van Unierecht of lidstatelijk recht.

4 Plichten verwerkingsverantwoordelijke en verwerker

In dit hoofdstuk worden de verplichtingen genoemd die op APG als verwerkingsverantwoordelijke en als verwerker rusten.

In paragraaf 2.5 is uiteengezet welke onderscheiden rollen, functies en verantwoordelijkheden APG heeft vanuit zijn bedrijfsvoering en dienstverlening en welke er toe leiden dat hij bij zijn gegevensverwerkingen de ene keer als verwerkingsverantwoordelijke en de andere keer als verwerker is te kwalificeren.

De privacy wet-en regelgeving legt zowel aan de verwerkingsverantwoordelijke als aan de verwerker verplichtingen op. De facto en de iure is en blijft de verwerkingsverantwoordelijke (eind)verantwoordelijk voor de naleving van de privacyverplichtingen en daarmee ook voor de gegevensverwerkingen die de verwerker ten behoeve van hem uitvoert. Tenzij de verwerkingsverantwoordelijke hiervoor niet aansprakelijk is te stellen (zie ook hoofdstuk 7).

4.1 Verantwoordingsplicht

Als verwerkingsverantwoordelijke is APG verantwoordelijk voor een rechtmatige en zorgvuldige verwerking van persoonsgegevens in overeenstemming met de verwerkingsbeginselen . Dat betekent dat APG:

- de verplichtingen uit de privacy wet- en regelgeving moet naleven; en
- deze naleving moet kunnen aantonen (‘accountability’).

Als verwerker is APG verantwoordelijk dat hij de gegevensverwerkingen die aan hem zijn uitbesteed, op een zodanig rechtmatige en zorgvuldige wijze uitvoert dat zijn opdrachtgevers de op hun als verwerkingsverantwoordelijken rustende verantwoordingsplicht kunnen nakomen.

De wijze waarop en de maatregelen waarmee APG deze verantwoordingsplicht invult, wordt beschreven in dit Gegevensbeschermingsbeleid.

4.2 Register van verwerkingsactiviteiten

Als verwerkingsverantwoordelijke houdt APG een elektronisch register van verwerkingsactiviteiten bij waarvoor APG verwerkingsverantwoordelijke is. In dit register worden de volgende gegevens opgenomen:

- naam en contactgegevens van de verwerkingsverantwoordelijke en van de functionaris voor de gegevensbescherming;
- de verwerkingsdoeleinden;
- een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens
- de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt;
- indien van toepassing, doorgifte aan een land of een internationale organisatie buiten de Europese Unie;

• indien mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van persoonsgegevens worden gewist;
• indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

Als verwerker houdt APG een elektronisch register van verwerkingsactiviteiten bij waarbij APG als verwerker optreedt. In dit register worden de volgende gegevens opgenomen:
• naam en contactgegevens van de verwerker, iedere verwerkingsverantwoordelijke waarvoor wordt gehandeld, en van de functionaris voor de gegevensbescherming;
• de categorieën van verwerkingen die voor iedere verwerkingsverantwoordelijke zijn uitgevoerd;
• indien van toepassing, doorgifte aan een land of een internationale organisatie buiten de Europese Unie;
• indien mogelijk, een algemene beschrijving van technische en organisatorische beveiligingsmaatregelen.

4.3 Verwerkersovereenkomst

Als APG als verwerkingsverantwoordelijke een verwerker inschakelt voor zijn gegevensverwerkingen, sluit hij met deze een schriftelijke, waaronder elektronische, overeenkomst waarin de volgende zaken worden geregeld:
• het onderwerp en de duur van de verwerking;
• de aard en het doel van de verwerking;
• het soort persoonsgegevens en de categorieën van betrokkenen;
• de rechten en verplichtingen van APG.

In de verwerkersovereenkomst wordt ten aanzien van de verwerker vastgelegd dat deze:
• de persoonsgegevens alleen verwerkt onder schriftelijke instructies van APG;
• waarborgt dat de toegang tot die gegevens is beperkt tot gemachtigde en aan geheimhouding gebonden personen;
• een passend beveiligingsniveau hanteert;
• APG alle mogelijke ondersteuning biedt bij het nakomen van diens verplichtingen met het oog op beantwoording van verzoeken rondom de rechten van betrokkenen;
• APG bijstaat bij het nakomen van zijn verplichtingen op het gebied van beveiliging van persoonsgegevens, de meldplicht datalekken en het uitvoeren van een gegevensbeschermingseffectbeoordeling;
• na beëindiging van de overeenkomst de verwerkte persoonsgegevens wist of aan APG teruggeeft, en bestaande kopieën verwijdert;
• APG alle informatie ter beschikking stelt die nodig is om aantoonbaar te maken dat de verplichtingen op grond van de privacy wet en regelgeving rondom het inzetten van een verwerker worden nageleefd, en die nodig is om audits mogelijk te maken;

• geen subverwerkers in dienst neemt zonder voorafgaande schriftelijke toestemming van APG en met deze subverwerkers eenzelfde verwerkersovereenkomst afsluit als hijzelf met APG heeft afgesloten.

Als APG als verwerker in opdracht van opdrachtgevers (bijv. pensioenfondsen) gegevensverwerkingen verricht, is de opdrachtgever verantwoordelijke voor het afsluiten van de verwerkersovereenkomst. APG is op grond van die overeenkomst verplicht de daarin opgenomen verplichtingen na te komen.

4.4 Gegevensbeschermingseffectbeoordeling

Wanneer een voorgenomen verwerking van persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, voert APG voorafgaand aan de verwerking een gegevensbeschermingseffectbeoordeling uit. Met deze gegevensbeschermingseffectbeoordeling, ook wel Data Protection Impact Assessment (DPIA) genoemd, beoordeelt APG de effecten van een voorgenomen verwerkingsactiviteit op de bescherming van persoonsgegevens.

De gegevensbeschermingseffectbeoordeling bevat in ieder geval:
• een beschrijving van de beoogde verwerking en de verwerkingsdoeleinden;
• een beoordeling van de noodzakelijkheid en evenredigheid van de verwerking met betrekking tot de verwerkingsdoeleinden;
• een beoordeling van de risico's voor betrokkenen;
• de beoogde maatregelen in de zin van waarborgen, veiligheidsmaatregelen en mechanismen om die risico's weg te nemen of te beperken.

Bij het uitvoeren van een gegevensbeschermingseffectbeoordeling wint APG advies in bij zijn FG.

Als het APG niet lukt om maatregelen te vinden voor het beperken van het hoge privacyrisico raadpleegt APG, voordat met de verwerking wordt gestart, eerst de AP. aan de AP verstrekt worden.

5 Persoonsgegevensbeveiliging

In dit hoofdstuk wordt stilgestaan bij de verplichting om met betrekking tot de gegevensverwerkingen een passend beveiligingsniveau te waarborgen.

5.1 Passende beveiliging

APG neemt passende technische en organisatorische maatregelen om een op het verwerkingsrisico afgestemd passend beveiligingsniveau te waarborgen. Deze maatregelen omvatten onder meer:

- pseudonimisering en versleuteling van de persoonsgegevens;
- het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
- het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
- een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

5.1.1 Informatiebeveiligingsbeleid

APG heeft zijn informatiebeveiligingsbeleid vastgelegd in zijn Beleid informatiebeveiliging, Beleid business continuity en de hieraan gekoppelde Informatiebeveiliging standaard.

Het Beleid informatiebeveiliging beschrijft de wijze waarop APG Informatiebeveiliging (IB) risico's identificeert, evalueert, beheerst en bewaakt.
Het Beleid business continuity management beschrijft de wijze waarop APG Business continuity management (BCM) de continuïteit van de bedrijfsvoering en dienstverlening van APG en daarmee de (persoons)gegevensverwerkingen garandeert.
De Informatiebeveiliging standaard (IB standaard) bevat de kaders voor IB, BCM en privacy zoals deze voor APG gelden. De IB standaard is richtinggevend en kaderstellend voor de verdere vertaling naar onderliggende procedures, richtlijnen of instructies op operationeel niveau. De IB standaard omvat kaders voor informatiebeveiliging, business continuity en privacy. Het voldoen aan de IB standaard maakt aantoonbaar dat passende technische en organisatorische maatregelen zijn genomen die waarborgen dat de privacy wet- en regelgeving wordt nageleefd (*accountability*).

5.2 Melden datalekken

Een inbreuk in verband met persoonsgegevens ('datalek') is een inbreuk op de beveiliging van persoonsgegevens die leidt tot de vernietiging, het verlies, de wijziging, de ongeoorloofde verstrekking of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens.

Voor de situatie dat zich een datalek voordoet, heeft APG een procedure *melden datalekken* ingericht dat verloopt via de APG Incidentenregeling of, ingeval van bijzondere datalekken ('foutieve correspondentie'), middels specifiek daarvoor ingerichte procedures.
Deze procedure omvat onder meer:
• een intern meldadres meldendatalekken@apg.nl waarop datalekken kunnen worden gemeld bij de functionaris voor de gegevensbescherming;
• een intern meldingsformulier datalekken;
• een handleiding *melden datalekken*.

Als APG als verwerkingsverantwoordelijke kwalificeert en voor zijn gegevensverwerking een beroep doet op een verwerker, maakt APG met deze verwerker middels de verwerkersovereenkomst (zie par. 4.3) de afspraak dat de verwerker een bij zijn gegevensverwerking geconstateerd datalek zo snel als mogelijk meldt bij APG.

Als APG als verwerker kwalificeert, zorgt APG er voor dat wanneer bij zijn in opdracht verrichte gegevensverwerkingen een datalek plaatsvindt, dit zo snel als mogelijk wordt gemeld bij de verwerkingsverantwoordelijke c.q. opdrachtgever.

5.2.1 Melden bij de toezichthouder

Een datalek meldt APG uiterlijk binnen 72 uur bij de Autoriteit Persoonsgegevens, tenzij het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de betrokkenen.

Bij de melding aan de Autoriteit Persoonsgegevens wordt ten minste het volgende omschreven of meegedeeld:
• de aard van het datalek;
• waar mogelijk de categorieën van betrokkenen en, bij benadering, het aantal betrokkenen;
• de naam en de contactgegevens van de functionaris voor de gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;
• de waarschijnlijke gevolgen van het datalek; en
• de maatregelen die APG voorgesteld of genomen heeft om het datalek aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

De melding aan de Autoriteit Persoonsgegevens wordt gedaan door de functionaris voor de gegevensbescherming of door een andere gekwalificeerde functionaris die de functionaris voor de gegevensbescherming hiervan in kennis stelt.

APG houdt een overzicht bij van alle, waaronder ook de aan de Autoriteit Persoonsgegevens gemelde, datalekken.

5.2.2 Melden bij de betrokkene

Wanneer het datalek waarschijnlijk een hoog risico voor de betrokkene inhoudt, meldt APG het datalek zo snel als mogelijk ook aan de betrokkene.

Mededeling aan betrokkenen kan achterwege blijven wanneer:
• APG passende technische en organisatorische beschermingsmaatregelen heeft genomen, met name die welke de persoonsgegevens onbegrijpelijk maken voor onbevoegden, zoals versleuteling;
• APG achteraf maatregelen heeft genomen waarmee de vastgestelde risico's voor de betrokkene zich waarschijnlijk niet meer zullen voordoen;
• de melding aan de betrokkene APG onevenredig veel inspanning zou kosten. In dat geval kan de informatie over het datalek op de website van APG worden gepubliceerd.

Bij de melding aan de betrokkene wordt ten minste het volgende omschreven of meegedeeld:
• de aard van het datalek;
• de naam en de contactgegevens van de functionaris voor de gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;
• de waarschijnlijke gevolgen van het datalek; en
• de maatregelen die APG voorgesteld of genomen heeft om het datalek aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

6 Doorgifte van persoonsgegevens

In dit hoofdstuk wordt aangegeven hoe APG omgaat indien en voor zover er bij gegevensverwerkingen persoonsgegevens worden doorgegeven aan een land of aan een internationale organisatie buiten de Europese Unie.

APG mag alleen persoonsgegevens aan een land of een internationale organisatie buiten de Europese Unie doorgegeven als daarmee het door de AVG vereiste beschermingsniveau niet wordt ondermijnd. Dat kan alleen als dat land of die organisatie een adequaat niveau van gegevensbescherming kent, als APG passende waarborgen biedt bij die doorgifte of als er afwijkingen of uitzonderingen zijn toegestaan.

APG heeft zijn Cloudbeleid en de daarop ingerichte procedures aangepast aan de in de AVG opgenomen eisen en verplichtingen aan doorgifte van persoonsgegevens.

6.1 Adequaatheidsbesluiten

Landen die een met de AVG vergelijkbaar niveau van gegevensbescherming bieden in hun nationale wetgeving worden geacht een passend niveau van gegevensbescherming te bieden. De Europese Commissie stelt vast of dit het geval is en neemt dan een 'adequaatheidsbesluit'. Alle landen met een adequaatheidsbeslissing zijn te vinden op de website van de Europese Commissie:
http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

6.2 Passende waarborgen

Doorgifte van persoonsgegevens aan een land of een internationale organisatie buiten de Europese Unie waarvoor geen adequaatheidsbesluit is afgegeven, is alleen toegestaan als dat land of die organisatie passende waarborgen bieden.

Van passende waarborgen is in ieder geval sprake ingeval van:
- bindende bedrijfsvoorschriften;
- door de Europese Commissie en de Autoriteit Persoonsgegevens vastgestelde standaardbepalingen inzake gegevensbescherming;
- een door de Autoriteit persoonsgegevens goedgekeurde gedragscode van verenigingen en andere organen die categorieën van verwerkingsverantwoordelijken of verwerkers vertegenwoordigen in combinatie met bindende en afdwingbare toezeggingen van de verwerkingsverantwoordelijke of verwerker in een niet-EU land om passende waarborgen toe te passen;
- toestemming van de Autoriteit Persoonsgegevens op contractbepalingen tussen de verwerkersverantwoordelijke of de verwerker en de verwerkersverantwoordelijke, de verwerker of de ontvanger van de persoonsgegevens in het land buiten de Europese Unie of de internationale organisatie;
- door de Europese Commissie goedgekeurde modelcontracten (zgn. Standard contractual clauses oftewel SCC's), zolang deze niet worden gewijzigd, vervangen of ingetrokken.

6.3 Afwijkingen

Als er geen adequaatheidsbesluiten of passende waarborgen zijn, zal APG als afwijking hiervan alleen persoonsgegevens doorgeven wanneer:

- betrokkene uitdrukkelijk toestemming heeft gegeven;
- dit noodzakelijk is voor de uitvoering van precontractuele maatregelen of van een overeenkomst tussen betrokkene en APG;
- dit noodzakelijk is voor de sluiting of uitvoering van een in het belang van de betrokkene tussen APG en een derde gesloten overeenkomst; of
- dit noodzakelijk is ten behoeve van een rechtsvordering.

6.4 Uitzonderingen

Als er geen adequaatheidsbesluit of passende waarborgen zijn en geen afwijkingen van toepassing zijn, zal APG als uitzondering hierop alleen persoonsgegevens doorgeven wanneer de doorgifte:

- niet repetitief is;
- een beperkt aantal betrokkenen betreft;
- noodzakelijk is voor dwingende gerechtvaardigde belangen van APG die niet ondergeschikt zijn aan de belangen van de betrokkene; en
- gewaarborgd is met passende beschermingsmaatregelen door APG.

Als doorgifte op basis van deze uitzonderingsgronden plaatsvindt, informeert APG zowel de Autoriteit Persoonsgegevens als de betrokkene over de doorgifte.

7 Beroep en aansprakelijkheid

In dit hoofdstuk wordt ingegaan op de mogelijkheden die de betrokkene heeft als hij van mening is dat APG zijn persoonsgegevens in strijd met de (verplichtingen uit de) AVG verwerkt.

7.1 Klacht

De betrokkene kan klacht indienen bij de Autoriteit Persoonsgegevens wanneer hij vindt dat APG met de verwerking van zijn persoonsgegevens inbreuk maakt op de AVG.

7.2 Voorziening in rechte

De betrokkene kan een doeltreffende voorziening in rechte instellen tegen APG wanneer hij vindt dat zijn rechten uit de AVG zijn geschonden ten gevolge van een verwerking van zijn persoonsgegevens die niet voldoet aan de (verplichtingen uit de) AVG.

7.3 Schadevergoeding

Iedereen die materiële of immateriële schade heeft geleden ten gevolge van een inbreuk op de AVG door APG, heeft het recht om van APG schadevergoeding te ontvangen voor de geleden schade.

Als APG als verwerkingsverantwoordelijke is te kwalificeren, is hij aansprakelijk voor de geleden schade. Als APG gebruik maakt van een verwerker, is deze slechts aansprakelijk voor de schade die door de gegevensverwerking is veroorzaakt wanneer hij niet heeft voldaan aan de op de verwerker rustende verplichtingen uit de AVG of buiten dan wel in strijd met de afspraken met APG heeft gehandeld.

Als APG als verwerker is te kwalificeren, is hij alleen aansprakelijk voor (dat deel van) de geleden schade die een gevolg is van het niet voldoen aan de op hem van toepassing zijnde verplichtingen van de AVG of van het buiten dan wel in strijd met de afspraken met de verwerkingsverantwoordelijke handelen.

Als APG voor de gehele schade aansprakelijk wordt gehouden, kan hij het deel van de schade(vergoeding) dat niet aan hem kan worden toegerekend, verhalen op de andere partij(en) die mee verantwoordelijk is of zijn voor de geleden schade. Deze hoofdelijke aansprakelijkheid kan zich voordoen zowel in de situatie dat APG verwerkingsverantwoordelijke is als in het geval dat APG verwerker is.

APG is niet aansprakelijk voor schade als hij kan bewijzen dat hij op geen enkele wijze verantwoordelijk is voor de geleden schade.