# GEDRAGSCODE VERWERKING PERSOONSGEGEVENS VERZEKERAARS


VERBOND VAN VERZEKERAARS

# Inhoud

# Inleiding en leeswijzer

Iedere Nederlander en ieder bedrijf is klant bij een verzekeraar, of het nu gaat om een wettelijk verplichte aansprakelijkheidsverzekering of een vrijwillige reis- of levensverzekering. Verzekeringen gaan uit van een simpel principe: door met een grote groep mensen risico's te delen, zijn we samen beter gewapend bij tegenspoed. Deze solidariteit is de pijler waarop verzekeren is gebouwd en komt tot uitdrukking in de kernwaarden van de 95% van de Nederlandse verzekeraars die zijn aangesloten bij het Verbond van Verzekeraars.

Al eeuwenlang is de analyse van informatie onmisbaar om verzekeringen effectief, eerlijk en betaalbaar te maken. Aan de hand van informatie over de klant en trends in de samenleving kunnen verzekeraars risico's beter inschatten, de premie van de verzekering bepalen, verzekeringsclaims beoordelen, schade voorkomen of beperken en de klant beter en meer op maat van dienst zijn. Verzekeraars zijn daarnaast wettelijk verplicht om de klant te kennen, de juiste informatie te geven over producten en verzekeringsfraude en witwassen te voorkomen en te bestrijden.

Vandaag de dag is de verwerking van persoonsgegevens, gegevens die herleidbaar zijn tot personen, steeds belangrijker voor verzekeraars: nieuwe technieken, zoals computergestuurde analyse van grote hoeveelheden data ('big data analyse'), stellen verzekeraars niet alleen in staat risico's in de samenleving eerder te herkennen en effectiever te opereren, maar ook om hun klanten meer op maat te bedienen. Tegelijkertijd kan de verwerking van informatie gevolgen hebben voor de privacy van de klant. Voor verzekeraars is het beschermen van privacy niet alleen wettelijk verplicht, maar ook een voorwaarde voor consumentenvertrouwen en voor een gezonde bedrijfsvoering.

De bescherming van persoonsgegevens wordt steeds belangrijker. Verzekeraars merken dat klanten steeds meer vragen stellen over privacy en dat de wereld om ons heen in rap tempo innoveert en digitaliseert. Vrijwel alles en iedereen genereert continu data, of het nu is door het rijden in een nieuwe auto of het surfen op het internet. Nieuwe technologie biedt ook kansen de klant meer controle te geven over hun persoonsgegevens of op maat gesneden aanbiedingen te doen en preventie te bevorderen.

De afgelopen jaren is de wet- en regelgeving voor de verwerking van persoonsgegevens ingrijpend veranderd. Vanuit Europa heeft de Algemene Verordening Gegevensbescherming (hierna: ‘AVG’) de spelregels voor de bescherming van persoonsgegevens verbeterd en uitgebreid. Deze spelregels zijn vanaf 25 mei 2018 van kracht in geheel Europa. In Nederland is ook de financiële wetgeving sterk in beweging en zijn verzekeraars wettelijk verplicht steeds meer te weten over hun klanten en hun klanten actief te begeleiden bij hun keuzes ten aanzien van verzekeringsproducten.

Deze Gedragscode Verwerking Persoonsgegevens Verzekeraars (hierna: ‘de Gedragscode’) vertaalt de algemene wet- en regelgeving voor Verzekeraars in concrete spelregels voor de verzekeringsbranche. Omdat deze algemene wet- en regelgeving op alle organisaties die persoonsgegevens verwerken van toepassing is, moedigt de AVG het opstellen van zulke gedragscodes aan om voor de bedrijven en klanten duidelijk te maken hoe persoonsgegevens in een bepaalde sector worden verwerkt. Ook het Kabinet juicht het initiatief van het Verbond van Verzekeraars om een Gedragscode aan te nemen toe.[1]

[1] Dit schrijft de Minister van Financiën aan de Tweede Kamer op 9 februari 2018: https://zoek.officielebekendmakingen.nl/kst-34616-3.html

Met deze Gedragscode wil het Verbond van Verzekeraars aansluiten op deze maatschappelijke, technologische en juridische ontwikkelingen.

## Leeswijzer

De Gedragscode is niet bedoeld als een samenvatting van de huidige wet- en regelgeving, maar als een uitwerking daarvan voor de verzekeringsbranche. Bepaalde onderwerpen zijn daarbij buiten beschouwing gelaten, omdat de wet- en regelgeving duidelijk beschrijft wat verzekeraars moeten doen. Een voorbeeld daarvan is het melden van datalekken. De AVG, de Beleidsregels van de Autoriteit Persoonsgegevens en financiële wetgeving beschrijven precies in welke situaties verzekeraars IT-incidenten moeten melden, en bij wie. Deze onderwerpen staan wel kort beschreven in deze Gedragscode, zodat verzekeraars, de klant en rest van de samenleving ziet dat deze onderwerpen ook moeten worden nageleefd door verzekeraars.

Andere onderwerpen in de Gedragscode komen uitgebreid aan bod, omdat zij uniek zijn voor de verzekeringssector. Twee van de belangrijkste onderwerpen zijn de analyse van informatie door verzekeraars voor het bepalen van de premie en het waarborgen van de veiligheid en integriteit van de sector, bijvoorbeeld om verzekeringsfraude te voorkomen. Deze onderwerpen komen uitgebreid aan bod in afdeling 4 van de Gedragscode. Omdat de onderwerpen ingewikkeld kunnen zijn voor klanten, bevat de Gedragscode ook grafische stappenplannen van wat verzekeraars precies doen op dit vlak. Deze 'infographics' over het aanvragen van een verzekering en de voorkoming en bestrijding van verzekeringsfraude en andere vormen van verzekeringscriminaliteit staan in de bijlage van de Gedragscode.

Aangezien de Gedragscode algemene normen en regels uit wet- en regelgeving uitwerkt, behoeven de bepalingen soms uitleg. Om die reden bevat de Gedragscode een uitgebreide toelichting, waarin de bepalingen stuk voor stuk worden toegelicht. De Gedragscode verwijst in sommige gevallen naar definities uit wet- en regelgeving, zoals Verwerkingsverantwoordelijke en Verwerker. Deze termen zijn met een hoofdletter geschreven en gedefinieerd in afdeling 10 van de Gedragscode.

Mocht u na lezing van deze Gedragscode vragen of opmerkingen hebben, dan hoort het Verbond van Verzekeraars graag van u. U kunt zich in dit geval richten tot info@verzekeraars.nl.

Ingangsdatum: 1 juli 2024

# 1 Overwegingen

1.1.1 Verzekeraars verwerken Persoonsgegevens in overeenstemming met geldende wet- en regelgeving voor de bescherming van Persoonsgegevens. Met deze Gedragscode Verwerking Persoonsgegevens Verzekeraars geven Verzekeraars uitdrukking aan het belang dat zij hechten aan een transparante, veilige en zorgvuldige Verwerking van Persoonsgegevens in de eigen sector. Verzekeraars leven de bepalingen van deze Gedragscode na in hun externe en interne privacybeleid en bedrijfsvoering.

1.1.2 De Gedragscode heeft tot doel:

(a) de geldende wet- en regelgeving voor de Verwerking van Persoonsgegevens nader uit te werken voor Verzekeraars en gegevensverwerkingen in de sector, en

(b) transparantie te bieden aan klanten en de samenleving over de verwerking van Persoonsgegevens door Verzekeraars.

1.1.3 Deze versie van de Gedragscode vervangt alle eerdere gedragscodes voor de Verwerking van Persoonsgegevens voor Verzekeraars, met inbegrip van de Gedragscode Verwerking Persoonsgegevens Financiële Instellingen uit 2010.

# 2 Reikwijdte en toepassing

## 2.1 Verzekeraars

2.1.1 De leden van het Verbond van Verzekeraars zijn gebonden aan deze Gedragscode wanneer zij het verzekeringsbedrijf uitoefenen. Verzekeraars die geen lid zijn van het Verbond, kunnen vrijwillig verklaren dat zij zich aansluiten bij deze Gedragscode. Zij zijn dan binnen de uitvoering van het verzekeringsbedrijf eveneens gebonden aan deze Gedragscode. Verzekeraars zullen bij uitbesteding van taken aan gevolmachtigden of andere dienstverleners, naleving van deze code dwingend opleggen in een onderlinge overeenkomst. Voor zorgverzekeraars die gebonden zijn aan de Gedragscode Verwerking Persoonsgegevens Zorgverzekeraars geldt bij uitoefening van het zorgverzekeringsbedrijf deze laatstgenoemde Gedragscode.

## 2.2 Toepassing

2.2.1 De Gedragscode is van toepassing op de (gedeeltelijk) geautomatiseerde Verwerkingen van Persoonsgegevens door Verzekeraars in het kader van hun bedrijfsvoering. De Gedragscode is ook van toepassing op handmatige verwerkingen van persoonsgegevens door Verzekeraars in het kader van hun bedrijfsvoering, voor zover deze gegevens zijn opgenomen in een bestand of bestemd zijn om daarin te worden opgenomen.

2.2.2 De Gedragscode is niet van toepassing op de verwerking van Persoonsgegevens:

(a) in het Incidentenregister van de Verzekeraars en het hieraan gekoppelde Externe Verwijzingsregister (EVR). Hierop is het Protocol Incidentenwaarschuwingssysteem Financiële Instellingen (PIFI) van toepassing.

(b) in de arbeidsrelatie van Verzekeraars.

# 3 Beginselen

## 3.1 Algemeen

3.1.1 Verzekeraars verwerken Persoonsgegevens in overeenstemming met geldende wet- en regelgeving. Zij respecteren de beginselen van proportionaliteit, subsidiariteit en vertrouwelijkheid en verwerken Persoonsgegevens op een transparante, behoorlijke en zorgvuldige wijze.

## 3.2 Grondslagen verwerking

3.2.1 Verzekeraars baseren iedere Verwerking van Persoonsgegevens op een in geldende wet- en regelgeving opgenomen grondslag. De Gedragscode bevat een nadere uitwerking van rechtmatige grondslagen uit wet- en regelgeving voor Verwerkingen van Persoonsgegevens door Verzekeraars.

## 3.3 Verzameling Persoonsgegevens

3.3.1 Verzekeraars verzamelen Persoonsgegevens voor welbepaalde en uitdrukkelijk omschreven doeleinden. In de Gedragscode staat een aantal van deze doeleinden verder uitgewerkt in artikel 4. Daarnaast kunnen Verzekeraars in overeenstemming met geldende wet- en regelgeving Persoonsgegevens Verwerken op grond van andere doeleinden. Verzekeraars omschrijven de doeleinden van Verwerkingen en de bronnen van Persoonsgegevens in een privacybeleid.

## 3.4 Kwaliteit Verwerking Persoonsgegevens

3.4.1 Verzekeraars beperken Verwerkingen tot Persoonsgegevens die redelijkerwijs noodzakelijk en relevant zijn voor de doeleinden van desbetreffende Verwerking. Zij voeren een beleid ten aanzien van de juistheid van Persoonsgegevens, de bewaartermijnen, het vastleggen van Verwerkingen in een daartoe bestemd verwerkingsregister en de verwijdering van Persoonsgegevens.

## 3.5 Rechten Betrokkene

3.5.1 Verzekeraars respecteren de rechten van de Betrokkene ten aanzien van de Verwerking van Persoonsgegevens. In de Gedragscode staan deze rechten nader uitgewerkt in artikel 6.

## 3.6 Dringende reden

3.6.1 Verzekeraars kunnen afwijken van deze algemene beginselen als er sprake is van een Dringende reden. In de Gedragscode staat deze Dringende reden nader uitgewerkt in artikel 8.

# 4 Doeleinden

## 4.1 Algemeen

4.1.1 Verzekeraars beschrijven de doeleinden voor de Verwerking van Persoonsgegevens in hun privacybeleid. Artikel 4 werkt veelvoorkomende doeleinden voor de Verwerking van Persoonsgegevens door Verzekeraars nader uit.

4.1.2 Verzekeraars voeren een gegevensbeschermingseffectbeoordeling (hierna DPIA) uit als bedoeld in artikel 7.4, zodra zij Persoonsgegevens verder verwerken voor andere doeleinden dan beschreven in het privacybeleid en deze verdere verwerking, gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Deze verdere Verwerking van Persoonsgegevens is alleen geoorloofd als het nieuwe doel verenigbaar is met het oorspronkelijke doel van de Verwerking. Verzekeraars informeren de Betrokkene over de nieuwe Verwerking van Persoonsgegevens in overeenstemming met afdeling 6 van de Gedragscode.

## 4.2 Aangaan en uitvoeren verzekering

4.2.1 Verzekeraars verwerken Persoonsgegevens voor het aangaan en uitvoeren van een verzekering. Voor zover redelijkerwijs noodzakelijk voor het aangaan en uitvoeren van de verzekering, kunnen Verzekeraars Persoonsgegevens verstrekken aan Derden. De Verwerking van Gezondheidsgegevens en Strafrechtelijke gegevens in het kader van het aangaan en uitvoeren van een verzekering geschiedt in overeenstemming met artikel 5.1 en artikel 5.2 van de Gedragscode.

4.2.2 Verzekeraars kunnen voor het nemen van een besluit ten aanzien van het aangaan of uitvoeren van een verzekering volledig geautomatiseerde Verwerkingen van Persoonsgegevens, zoals profilering, verrichten. Als aan het besluit voor Betrokkene rechtsgevolgen zijn verbonden of het besluit de Betrokkene anderszins in aanmerkelijke mate treft, vinden zulke Verwerkingen slechts plaats indien het besluit:

(a) noodzakelijk is voor het aangaan of uitvoeren van de verzekering; of

(b) berust op uitdrukkelijke toestemming van de Betrokkene; of

(c) uitvoering geeft aan een publiekrechtelijke taak of wettelijke verplichting.

Als in deze gevallen het besluit noodzakelijk is voor het aangaan of uitvoeren van de verzekering of berust op toestemming kan de Betrokkene zijn standpunt kenbaar maken over het besluit, het besluit aanvechten en de Verzekeraar verzoeken met menselijke tussenkomst een besluit toe te lichten en door een mens te laten heroverwegen.

In overeenstemming met afdeling 6 van de Gedragscode informeert de Verzekeraar de Betrokkene over de Verwerking. Voorafgaand aan de volledig geautomatiseerde besluitvorming met rechtsgevolg of die de betrokkene in aanmerkelijke mate treft, voert een Verzekeraar een DPIA uit in overeenstemming met artikel 7.4 van de Gedragscode. De Verzekeraar evalueert de geautomatiseerde besluitvorming periodiek om overeenstemming met de algemene beginselen van afdeling 3 van de Gedragscode te waarborgen.

## 4.3 Analyses voor historische, statistische en wetenschappelijke doeleinden

4.3.1 Verzekeraars kunnen Persoonsgegevens verwerken voor historische, statistische of wetenschappelijke doeleinden. In overeenstemming met artikel 7.4 voeren Verzekeraars een DPIA uit om de impact op de privacy van de Betrokkene in kaart te brengen en beschermende maatregelen te treffen. Verzekeraars kunnen voor dit doeleinde gearchiveerde Persoonsgegevens analyseren in overeenstemming met artikel 7.5 van de Gedragscode.

4.3.2 Verzekeraars kunnen de uitkomst van historische, statistische en wetenschappelijke analyse gebruiken om groepsprofielen op te stellen. Verzekeraars zullen de Persoonsgegevens ten grondslag aan de analyse voor het opstellen van groepsprofielen anonimiseren of pseudonimiseren in overeenstemming met artikel 7.6 van de Gedragscode.

4.3.3 Verzekeraars kunnen in het kader van wetenschappelijke, historische en statistische doeleinden Bijzondere Persoonsgegevens verwerken. De Verwerking dient noodzakelijk te zijn voor het verrichten van een specifieke analyse en te voldoen aan de overige voorwaarden van artikel 5 van de Gedragscode. De Verzekeraar voert daarnaast voorafgaand aan de Verwerking een DPIA uit in overeenstemming met artikel 7.4 van de Gedragscode. De Verzekeraar treft passende maatregelen ter bescherming van de persoonlijke levenssfeer van de Betrokkene.

## 4.4 Marketingactiviteiten en relatiemanagement

4.4.1 Verzekeraars kunnen Persoonsgegevens voor marketingactiviteiten en relatiemanagement verwerken. Bij Verwerking van Persoonsgegevens voor marketingdoeleinden die Verzekeraars niet direct bij betrokkene hebben verzameld, informeren zij de Betrokkene in overeenstemming met artikel 6.1.1 van de Gedragscode. De Verzekeraar beëindigt de Verwerking voor marketingactiviteiten als de Betrokkene kenbaar maakt dat de hem betreffende Persoonsgegevens hiervoor niet gebruikt mogen worden.

Verzekeraars kunnen Betrokkenen via diverse kanalen benaderen voor Direct Marketing. Verzekeraars doen dit in overeenstemming met de Telecommunicatiewet. Gebruik van ‘gewone’ post voor Direct Marketing is toegestaan, tenzij de Betrokkene aangeeft zulke Direct Marketing niet te willen ontvangen (‘opt-out’). De Betrokkene kan de voornoemde opt-in of opt-out op ieder moment kosteloos verlenen of intrekken.

4.4.2 Verzekeraars voeren voorafgaand aan de verdere Verwerking van Persoonsgegevens voor direct marketingactiviteiten, aan de hand van eerder opgestelde groepsprofielen in overeenstemming met artikel 4.3.2. van de Gedragscode, een DPIA uit als is voldaan aan de criteria van artikel 7.4 van de Gedragscode. Indien de uitkomst van de DPIA dit verlangt, zullen Verzekeraars de Persoonsgegevens ten grondslag aan de ontwikkeling van nieuwe producten en diensten anonimiseren of pseudonimiseren in overeenstemming met artikel 7.6 van de Gedragscode.

4.4.3 Verzekeraars verwerken Bijzondere Persoonsgegevens alleen voor direct marketingdoeleinden na de uitdrukkelijke toestemming van de Betrokkene.

## 4.5 Integriteit en veiligheid dienstverlening

4.5.1 Verzekeraars verwerken Persoonsgegevens om de integriteit en veiligheid van (de dienstverlening van) de Verzekeraar, de Groep waartoe de Verzekeraar behoort en van de verzekeringsbranche te waarborgen. Zij treffen daartoe maatregelen, waaronder het (laten) uitvoeren van een interne audit en het inrichten van een Incidentenregister en eventuele deelname aan andere waarschuwingssystemen.

4.5.2 Een audit richt zich op het handelen van Verzekeraars of ingeschakelde Derden. De Verzekeraars treffen passende waarborgen ter bescherming van Persoonsgegevens van de Betrokkene gedurende het onderzoek van de Verzekeraar of ingeschakelde Derden. Een auditverslag bevat geen Persoonsgegevens.

4.5.3 Verzekeraars houden een Gebeurtenissenadministratie bij ter waarborging van de veiligheid en integriteit van de dienstverlening en de sector. Verzekeraars informeren Betrokkenen over het bestaan en de mogelijkheid tot Verwerking van Persoonsgegevens in dit verband. De afdeling Veiligheidszaken of een andere daartoe aangewezen afdeling bij een Verzekeraar kan besluiten de Persoonsgegevens uit de Gebeurtenissen-administratie op te nemen in een Intern Verwijzingsregister (IVR). In het IVR nemen Verzekeraars uitsluitend Persoonsgegevens op van (rechts)personen die een risico vormen voor de veiligheid en/of integriteit van de Verzekeraar of de Groep waartoe de Verzekeraar behoort. Indien een gebeurtenis voldoet aan de criteria uit het Protocol Incidentenwaarschuwingssysteem Financiële Instellingen (PIFI), nemen Verzekeraars de relevante Persoonsgegevens op in een Incidentenregister en, in voorkomende gevallen, het Extern Verwijzingsregister (EVR). In overeenstemming met artikel 2.2.2 van de Gedragscode is het PIFI van toepassing op deze Verwerking.

## 4.6 Voorschriften uit wet- en regelgeving

4.6.1 Verzekeraars moeten in bepaalde gevallen Persoonsgegevens van een Betrokkene verzamelen, verwerken of delen met bevoegde autoriteiten op grond van voorschriften uit wet- en regelgeving en van sectortoezichthouders.

# 5 Bijzondere persoonsgegevens

## 5.1 Gezondheidsgegevens

5.1.1 De Verzekeraar verwerkt alleen Gezondheidsgegevens als:

(a) de Betrokkene uitdrukkelijke toestemming heeft verleend; of

(b) dit noodzakelijk is voor de beoordeling en acceptatie van een Betrokkene en het uitvoeren van een verzekering. De Verzekeraar kan vragen naar Gezondheidsgegevens, voor zover deze Gezondheidsgegevens redelijkerwijs noodzakelijk zijn voor de totstandkoming en de uitvoering van de verzekering. De Verzekeraar mag Gezondheidsgegevens die de Betrokkene aan de medisch adviseur heeft verstrekt in verband met een verzekering niet gebruiken voor een andere verzekering, tenzij de Betrokkene hiervoor uitdrukkelijke toestemming verleent; of

(c) ter waarborging van de veiligheid en integriteit van de sector in overeenstemming met artikel 4.5 van de Gedragscode; of

(d) de Verwerking betrekking heeft op Gezondheidsgegevens die de Betrokkene kennelijk zelf heeft geopenbaard; of

(e) dit noodzakelijk is met het oog op een zwaarwegend algemeen belang in overeenstemming met de wet, en de Verzekeraar passende waarborgen treft ter bescherming van de persoonlijke levenssfeer van de Betrokkene; of

(f) dit noodzakelijk is voor historische, statistische of wetenschappelijke doeleinden, in overeenstemming met artikel 4.3.3. van de Gedragscode; of

(g) dit noodzakelijk is voor de vaststelling, uitoefening of de verdediging van de belangen van de Verzekeraar bij geschillenbeslechting; of

(h) naleving van wet- en regelgeving dit expliciet toestaat.

5.1.2 Voorafgaand aan een categorie nieuwe Verwerkingen van Gezondheidsgegevens en belangrijke aanpassingen van een bestaande categorie Verwerkingen van Gezondheidsgegevens bepaalt de Verzekeraar of een DPIA uitgevoerd dient te worden, in overeenstemming met de criteria van artikel 7.4 van de Gedragscode.

5.1.3 Alleen de Medisch Adviseur mag Gezondheidsgegevens verwerken voor het opstellen van een medisch advies. De Medisch Adviseur kan daartoe aanvullende Gezondheidsgegevens opvragen bij de Betrokkene. De Medisch Adviseur mag na uitdrukkelijke toestemming en indien noodzakelijk met machtiging van de Betrokkene Gezondheidsgegevens verzamelen uit andere bronnen. De machtiging is niet algemeen van aard, maar richt zich op een concrete Verwerking voor een specifiek geval. De machtiging bevat ook informatie over de aard van de op te vragen gegevens, het doel van de Verwerking en de rechten van de Betrokkene in overeenstemming met de bepalingen uit artikel 6 van de Gedragscode. De Medisch Adviseur is verantwoordelijk voor het bewaren van het medisch dossier van de Betrokkene. De verzekeraar zal voor het bewaren van het medisch dossier van de Betrokkene instructies van de Medisch Adviseur opvragen en volgen. Het medisch dossier kan onder andere de volgende informatie bevatten:

(a) de machtiging ten aanzien van de Verwerking van Gezondheidsgegevens;

(b) informatie verstrekt door de Betrokkene, zoals de gezondheidsverklaring van de Betrokkene;

(c) informatie verkregen van de behandelend artsen en andere behandelaars;

(d) rapporten die een keurend arts heeft opgesteld in verband met het aangaan of uitvoeren van de verzekering of de gegevens van de arbodienst/bedrijfsarts;

De Medisch Adviseur en personen die onder zijn of haar verantwoordelijkheid vallen, zijn niet verantwoordelijk voor de Verwerking van Gezondheidsgegevens door de (i) Technisch Acceptant en claimbehandelaar; (ii) personen binnen de Verzekeraar die rechtstreeks van de Betrokkene Gezondheidsgegevens hebben verkregen, al dan niet gelijktijdig met het melden van een claim of schade, als deze Gezondheidsgegevens noodzakelijk zijn voor verdere beoordeling daarvan, en (iii) de Betrokkene die vanwege zijn gezondheidstoestand om de Verwerking heeft verzocht.

5.1.4 De Betrokkene heeft in overeenstemming met artikel 6.2 van de Gedragscode recht op inzage in de Verwerking van Persoonsgegevens in het medisch dossier. De Medisch Adviseur kan passages uit het medisch dossier onleesbaar maken om de belangen van anderen te beschermen bij voldoening aan het inzageverzoek van de Betrokkene.

5.1.5 De personen die voor of namens Verzekeraars Gezondheidsgegevens verwerken zijn vanwege ambt, beroep, wettelijk voorschrift of door een overeenkomst tot geheimhouding verplicht.

## 5.2 Strafrechtelijke gegevens

5.2.1 De Verzekeraar verwerkt alleen Strafrechtelijke gegevens als:

(a) de Betrokkene uitdrukkelijke toestemming heeft verleend; of

(b) deze noodzakelijk zijn voor de beoordeling en acceptatie van een Betrokkene als Verzekerde en het uitvoeren van een verzekering. De Verzekeraar kan de Betrokkene vragen naar het bestaan van strafrechtelijke feiten en een strafrechtelijk verleden van de aanstaande Verzekerde en meeverzekerden (waaronder bestuurders en aandeelhouders van rechtspersonen); of

(c) ter waarborging van de veiligheid en integriteit van de sector in overeenstemming met artikel 4.5 van de Gedragscode; of

(d) de Verwerking betrekking heeft op Strafrechtelijke gegevens die de Betrokkene kennelijk zelf heeft geopenbaard; of

(e) de Autoriteit Persoonsgegevens een vergunning heeft verleend voor de Verwerking; of

(f) dit noodzakelijk is voor historische, statistische of wetenschappelijke doeleinden, in overeenstemming met artikel 4.3.3. van de Gedragscode; of

(g) dit noodzakelijk is voor de vaststelling, uitoefening of de verdediging van de belangen van de Verzekeraar bij geschillenbeslechting; of

(h) naleving van wet- en regelgeving dit vereist.

5.2.2 Voorafgaand aan een categorie nieuwe Verwerkingen van Strafrechtelijke gegevens en belangrijke aanpassingen van een bestaande categorie Verwerkingen van Strafrechtelijke gegevens, bepaalt de Verzekeraar of een DPIA uitgevoerd dient te worden, in overeenstemming met de criteria van artikel 7.4 van de Gedragscode.

5.2.3 Verzekeraars kunnen strafrechtelijke gegevens uitsluitend verstrekken aan medewerkers van Groepsmaatschappijen indien toegang tot deze gegevens noodzakelijk is voor de uitoefening van hun functie of om de gegevens vervolgens te verstrekken aan opsporingsdiensten. Deze verstrekking binnen Groepsmaatschappijen is beperkt tot:

(a) persoonsgegevens die betrekking hebben op strafbare feiten die zijn, of op grond van feiten en omstandigheden naar verwachting worden, begaan tegen de Groep; of

(b) persoonsgegevens die onrechtmatig gedrag tegen de Groep kunnen bewijzen.

## 5.3 Andere Bijzondere Persoonsgegevens

5.3.1 Verzekeraars mogen andere Bijzondere Persoonsgegevens dan Gezondheidsgegevens en Strafrechtelijke gegevens alleen verwerken als:

(a) de Betrokkene uitdrukkelijke toestemming heeft verleend; of

(b) de verwerking noodzakelijk is voor de vaststelling, uitoefening of de verdediging van de belangen van de Verzekeraar in rechte; of

(c) ter waarborging van de veiligheid en integriteit van de sector in overeenstemming met artikel 4.5 van de Gedragscode; of

(d) de Verwerking betrekking heeft op Persoonsgegevens die de Betrokkene kennelijk zelf heeft geopenbaard; of

(e) dit noodzakelijk is voor historische, statistische of wetenschappelijke doeleinden, in overeenstemming met artikel 4.3.3. van de Gedragscode; of

(f) de verwerking noodzakelijk is met het oog op een zwaarwegend algemeen belang in overeenstemming met de wet, en de Verzekeraar passende waarborgen treft ter bescherming van de persoonlijke levenssfeer van de Betrokkene; of

(g) naleving van wet- en regelgeving dit expliciet toestaat.

5.3.2 Voorafgaand aan een categorie nieuwe Verwerkingen van andere Bijzondere Persoonsgegevens en belangrijke aanpassingen van een bestaande categorie Verwerkingen van Bijzondere Persoonsgegevens, bepaalt de Verzekeraar of een DPIA uitgevoerd dient te worden, in overeenstemming met de criteria van artikel 7.4 van de Gedragscode.

# 6 Rechten betrokkene

## 6.1 Informatie over Verwerkingen Persoonsgegevens

6.1.1 Verzekeraars informeren de Betrokkene over de Verwerking van Persoonsgegevens, zodat de Betrokkene de Verwerking kan beoordelen en kan opkomen voor de in dit hoofdstuk benoemde rechten. Als Verzekeraars Persoonsgegevens verzamelen bij de Betrokkene, informeren zij de Betrokkene volledig en voorafgaand aan de verzameling van Persoonsgegevens. Bij het verzamelen van Persoonsgegevens via andere kanalen of uit andere bronnen dan direct van de Betrokkene, informeren Verzekeraars de Betrokkene binnen een maand na de verzameling ervan of voorafgaand in hun externe privacystatement.

6.1.2 De Verzekeraar kan deze informatieplicht alleen achterwege laten als dit in de praktijk onmogelijk is, onevenredige inspanning vergt of de Betrokkene al op de hoogte is van de Verwerking. Daarnaast kan de Verzekeraar een redelijk belang hebben de Betrokkene nog niet op de hoogte te stellen of kan er sprake zijn van een Dringende reden in overeenstemming met artikel 8 van de Gedragscode. Verzekeraars beoordelen dan op basis van de algemene beginselen van artikel 3.1 Gedragscode of zij de Betrokkene alsnog naderhand informeren.

6.1.3 Verzekeraars informeren Betrokkenen op transparante wijze en in begrijpelijke taal over Verwerking van Persoonsgegevens. Verzekeraars verwijzen in hun externe privacystatement naar deze Gedragscode. Het externe privacystatement is te raadplegen op de website van de Verzekeraars.

6.1.4 Voorafgaand aan een Verwerking voor een ander doeleinde dan waarvoor de Persoonsgegevens verzameld zijn, informeren Verzekeraars de Betrokkene over het andere doeleinde en de betrokken Persoonsgegevens.

6.1.5 Als Verzekeraars een besluit aangaande een Betrokkene nemen dat is gebaseerd op geautomatiseerde verwerkingen van Persoonsgegevens en dat de Betrokkene in aanmerkelijke mate kan treffen verschaffen zij de Betrokkene informatie over het bestaan, het belang, de logica en de te verwachten gevolgen van deze Verwerking. De verschafte informatie is zo concreet en praktisch mogelijk, zodat de Betrokkene een overzichtelijk beeld kan ontwikkelen over de mogelijke gevolgen van het besluit.

## 6.2 Inzage Verwerking Persoonsgegevens

6.2.1 Betrokkenen hebben het recht Verzekeraars schriftelijk te vragen om een overzicht van de verwerkte Persoonsgegevens. Daarnaast verschaffen Verzekeraars de Betrokkene informatie over wettelijk vereiste categorieën, zoals de verwerkingsdoeleinden, de eventuele ontvangers en bronnen van de Persoonsgegevens, getroffen waarborgen voor de bescherming van de Persoonsgegevens, het bestaan van volledig geautomatiseerde verwerkingen en, indien mogelijk, de bewaartermijnen van de Persoonsgegevens. Als Persoonsgegevens buiten de Europese Unie worden verwerkt, bieden Verzekeraars informatie over de getroffen waarborgen voor de bescherming van Persoonsgegevens. Het overzicht bevat ook informatie over de andere rechten die de Betrokkenen op basis van dit hoofdstuk van de Gedragscode geniet.

6.2.2 Verzekeraars beantwoorden het inzageverzoek van de Betrokkene gemotiveerd en binnen een maand. Als de Verzekeraar geen Persoonsgegevens van de Betrokkene verwerkt, stelt de Verzekeraar de Betrokkene daarvan ook binnen een maand na ontvangst van het

verzoek op de hoogte. Als de Betrokkene via elektronische weg om het overzicht verzoekt, zal de Verzekeraar het overzicht in elektronische vorm aan de Betrokkene toesturen, tenzij de Betrokkene expliciet om een andere vorm vraagt of de beveiliging van de Persoonsgegevens niet kan worden gewaarborgd. Verzekeraars mogen een redelijke vergoeding vragen indien de Betrokkene extra kopieën van het overzicht verzoekt.

6.2.3 De Verzekeraar mag het inzageverzoek van een Betrokkene weigeren, als daartoe een Dringende Reden bestaat, als de bescherming van de Persoonsgegevens van Derden dat rechtvaardigt of als intellectuele eigendomsrechten of bedrijfsgeheimen van de Verzekeraars onevenredig getroffen worden door het verschaffen van de Persoonsgegevens.

6.2.4 Als de Verzekeraar verantwoordelijk is voor de vaststelling van de identiteit van de Betrokkene, verzoekt de Verzekeraar de Betrokkene zich te legitimeren voorafgaand aan het voldoen aan het inzageverzoek, tenzij identificatie reeds heeft plaatsgevonden.

## 6.3 Correctie, bezwaar, beperking en verwijdering Persoonsgegevens

6.3.1 Als de Verzekeraar onjuiste of onvolledige Persoonsgegevens verwerkt, heeft de Betrokkene het recht op verbetering of aanvulling van de betreffende Persoonsgegevens. Als de Persoonsgegevens in strijd met deze Gedragscode of wettelijk voorschrift worden verwerkt, heeft de Betrokkene recht op beperking of verwijdering van de betreffende Persoonsgegevens, tenzij de belangen van een Verzekerde of een Derde hierdoor onevenredig worden geschaad. Verzekeraars beantwoorden een schriftelijk verzoek van de Betrokkene tot correctie, bezwaar, beperking of verwijdering gemotiveerd en in beginsel binnen een maand. De Verzekeraar kan de Betrokkene vragen om een motivering van zijn verzoek.

6.3.2 De Betrokkene heeft het recht schriftelijk bezwaar te maken tegen de Verwerking van Persoonsgegevens door de Verzekeraar of een Derde aan wie de Persoonsgegevens worden verstrekt. Het recht op bezwaar geldt alleen als de Verzekeraar Persoonsgegevens verwerkt op grond van het gerechtvaardigde belang van de Verzekeraar. Verzekeraars beantwoorden het bezwaar van de Betrokkene gemotiveerd en binnen een maand. Bij gerechtvaardigd bezwaar van de Betrokkene beëindigt de Verzekeraar de Verwerking van Persoonsgegevens onmiddellijk. Zo lang niet duidelijk is of de Betrokkene een gerechtvaardigd verzoek heeft ingediend bij de Verzekeraar, beperkt de Verzekeraar de Verwerking van desbetreffende Persoonsgegevens. Als de Betrokkene bezwaar aantekent tegen een Verwerking voor direct marketing door een Verzekeraar, onthoudt de Verzekeraar zich van deze Verwerking. Daartoe documenteert de Verzekeraar het bezwaar van de Betrokkene in een intern register.

6.3.3 Als de Verzekeraar verantwoordelijk is voor de vaststelling van de identiteit van de Betrokkene, verzoekt de Verzekeraar de Betrokkene zich te legitimeren voorafgaand aan het voldoen aan een verzoek op grond van deze paragraaf, tenzij identificatie reeds heeft plaatsgevonden.

## 6.4 Dataportabiliteit

6.4.1 Verzekeraars helpen een Betrokkene op diens verzoek met het verhuizen van Persoonsgegevens naar een andere Verzekeraar of Verwerkingsverantwoordelijke. Het verzoek van de Betrokkene kan zich richten tot de Persoonsgegevens die door de Betrokkene aan de Verzekeraar zijn verstrekt en die de Verzekeraar verwerkt op basis van de uitdrukkelijke toestemming van de Betrokkene of ter uitvoering van de verzekering. Verzekeraars beschermen de rechten van Derden bij het voldoen aan een verzoek om het verhuizen van Persoonsgegevens van de Betrokkene.

6.4.2 Verzekeraars verstrekken de Persoonsgegevens in een voor de Betrokkene en ontvangende Verwerkingsverantwoordelijke begrijpelijke vorm. De versturende Verzekeraar verstuurt geen Persoonsgegevens waaruit ontvangende Verwerkings-verantwoordelijke profielen van de betrokkene of bedrijfsgeheimen kan herleiden. De ontvangende Verwerkingsverantwoordelijke is verantwoordelijk voor de ontvangen Persoonsgegevens en is verplicht de bescherming van de rechten van de betrokkene te waarborgen.

6.4.3 Als de Verzekeraar verantwoordelijk is voor de vaststelling van de identiteit van de Betrokkene, verzoekt de Verzekeraar de Betrokkene zich te legitimeren voorafgaand aan het voldoen aan een verzoek op grond van deze paragraaf, tenzij identificatie reeds heeft plaatsgevonden.

# 7 Speciale onderwerpen

## 7.1 Verzamelen gegevens via apparatuur Betrokkene

7.1.1 Verzekeraars plaatsen gegevens, waaronder cookies, op de apparatuur van de Betrokkene om zo gegevens van de Betrokkene te verzamelen voor het leveren van een gevraagde dienst. In alle andere gevallen zal een Verzekeraar zulke gegevens pas verzamelen, nadat de Betrokkene op een transparante wijze en in begrijpelijke taal is geïnformeerd in overeenstemming met artikel 6.1.1 van de Gedragscode. Als een Verzekeraar via zulke gegevens Persoonsgegevens van Betrokkene verzamelt voor marketingactiviteiten, krijgt de Betrokkene de gelegenheid de Verwerking te weigeren. Verzekeraars mogen de verzamelde Persoonsgegevens alleen voor marketingactiviteiten gebruiken in overeenstemming met artikel 4.4 van de Gedragscode. Verzekeraars stellen een beleid op voor het verzamelen van Persoonsgegevens en andere gegevens op de randapparatuur van de Betrokkene.

## 7.2 Beveiliging

7.2.1 Verzekeraars zijn zich bewust van het cruciale belang van de beveiliging van Persoonsgegevens voor de Betrokkene. Persoonsgegevens van de Betrokkene zijn beveiligd met passende technische en organisatorische middelen die zijn vastgelegd in een beveiligingsbeleid. Verzekeraars voldoen niet alleen aan de eisen uit geldende wet- en regelgeving ten aanzien van de bescherming van Persoonsgegevens, maar ook aan de eisen uit het Toetsingskader Informatiebeveiliging van De Nederlandsche Bank, dat specifieke en strenge beveiligingsnormen bevat voor de financiële sector.

## 7.3 Datalekken

7.3.1 Verzekeraars melden een meldingsplichtig datalek zonder onredelijke vertraging en, indien mogelijk, binnen 72 uur na kennisname aan de Autoriteit Persoonsgegevens. Verzekeraars kunnen indien noodzakelijk of wenselijk een datalek aan de Betrokkene melden op grond van de zorgplicht uit de Wft.

## 7.4 Gegevensbeschermingseffectbeoordeling (DPIA)

7.4.1 Voorafgaand aan een categorie nieuwe Verwerkingen en belangrijke aanpassingen van een bestaande categorie Verwerkingen, bepalen Verzekeraars of zij een gegevensbeschermingseffectbeoordeling (DPIA) uitvoeren. Verzekeraars maken een DPIA als de Verwerking gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van de Betrokkene.

7.4.2 Een DPIA bevat een analyse van de beoogde Verwerking, de doeleinden, de noodzaak en de evenredigheid met betrekking tot de doeleinden, de grondslagen, mogelijke risico's voor de Betrokkene en waarborgen die de Verzekeraar treft om eventuele risico's te mitigeren. Indien de verzekeraar een FG heeft aangewezen wint de Verzekeraar diens advies in bij het uitvoeren van een DPIA.

## 7.5 Beleid bewaren Persoonsgegevens

7.5.1 Verzekeraars voeren een beleid ten aanzien van het bewaren van Persoonsgegevens. Zij bewaren Persoonsgegevens voor specifieke doeleinden en totdat de in het bewaarbeleid vastgestelde bewaartermijnen zijn verstreken. Na het verstrijken van de bewaartermijn zullen Verzekeraars de Persoonsgegevens vernietigen, anonimiseren, pseudonimiseren of

overbrengen naar een bestemming ten behoeve van archiefbeheer en ter waarborging van geschillenbeslechting. Verzekeraars kunnen gearchiveerde Persoonsgegevens analyseren voor het verrichten van historische, statistische of wetenschappelijke analyse. Verzekeraars verwerken deze Persoonsgegevens overeenkomstig artikel 4.3 van de Gedragscode.

## 7.6 Pseudonimisering

7.6.1 Na pseudonimisering van Persoonsgegevens treffen Verzekeraars maatregelen om ongeoorloofde re-identificatie van Betrokkenen te voorkomen. Verzekeraars bewaren de Persoonsgegevens die de Betrokkene kunnen koppelen aan informatie in de pseudonieme dataset apart, wijzen de voor de pseudonimisering verantwoordelijke werknemers aan en leggen deze maatregelen vast in een beleidsplan. Als Verzekeraars overgaan tot re-identificatie van de in de pseudonieme dataset opgenomen Betrokkenen voor commerciële doeleinden, is er sprake van een Verwerking waarvoor een nieuwe grondslag is vereist. De Gedragscode is integraal van toepassing op deze nieuwe Verwerking.

## 7.7 Cameratoezicht

7.7.1 Verzekeraars kunnen cameratoezicht inzetten als dat voor de volgende doeleinden noodzakelijk is:

(a) beveiliging van gebouwen, terreinen, medewerkers, goederen, informatie en andere significante belangen van de Verzekeraar, de Betrokkene en Derden; of

(b) voorkomen, vaststellen en onderzoeken van strafbare feiten en overtredingen van bedrijfsregels; of

(c) ondersteuning van (mogelijke) juridische procedures.

7.7.2 De inzet van cameratoezicht door Verzekeraars dient aan de volgende criteria te voldoen:

(a) Selectiviteit. Verzekeraars selecteren locaties met het oog op de in artikel 7.7.1. van de Gedragscode omschreven doeleinden;

(b) Bewaartermijn. Verzekeraars bewaren de verkregen Persoonsgegevens en camerabeelden niet langer dan noodzakelijk voor de in artikel 7.7.1.van de Gedragscode omschreven doeleinden. De bewaartermijn kan per doeleinde verschillen. In overeenstemming met artikel 7.5 van de Gedragscode leggen Verzekeraars de bewaartermijn vast in een beleid.

(c) Passende Beveiliging. Verzekeraars waarborgen dat de informatie is opgenomen in beveiligde informatiesystemen.

(d) Kenbaarheid. Verzekeraars zorgen ervoor dat de inzet van cameratoezicht duidelijk kenbaar is gemaakt. Met inachtneming van de criteria neergelegd in artikel 7.4 van deze Gedragscode, kan met passende waarborgen hiervan worden afgeweken als de inzet bedoeld is voor de in artikel 7.7.1 sub b en c genoemde doeleinden.

7.7.3 De Verzekeraar kan de Betrokkene naar aanleiding van een inzageverzoek vragen plaats, datum en tijd van de opname nader te specificeren. De Verzekeraar honoreert het inzageverzoek, tenzij er sprake is van een Dringende reden in overeenstemming met artikel 8 van de Gedragscode.

## 7.8 Verwerkersovereenkomst

7.8.1 Als Verzekeraars Verwerkers inschakelen die op instructie van de Verzekeraar Persoonsgegevens verwerken, waarborgen Verzekeraars dat deze externe organisaties de beginselen uit deze Gedragscode en de geldende wet- en regelgeving naleven. Verzekeraars sluiten hiertoe een verwerkersovereenkomst. In deze verwerkersovereenkomst zijn alle verplichtingen vastgelegd waaraan een Verwerker op grond van geldende wet- en regelgeving moet voldoen.

## 7.9 Doorgifte van Persoonsgegevens buiten de Europese Economische Ruimte

7.9.1 Als Verzekeraars Persoonsgegevens buiten de Europese Economische Ruimte verwerken, bijvoorbeeld bij Verwerkingen door een Verwerker of een Groepsmaatschappij, waarborgt de Verzekeraar dat de Persoonsgegevens van de Betrokkene adequate bescherming genieten in overeenstemming met geldende wet- en regelgeving en de Gedragscode.

## 7.10 Groepsmaatschappijen

7.10.1 Verzekeraars kunnen Persoonsgegevens binnen de Groep verwerken, mits aan de overige bepalingen van de Gedragscode, de AVG en overige toepasselijke wet- en regelgeving is voldaan. De Betrokkene dient in het bijzonder in overeenstemming met artikel 6.1.1 van de Gedragscode voldoende informatie te hebben ontvangen dat de Verzekeraar en de Groepsmaatschappij deel uitmaken van dezelfde Groep.

# 8 Dringende reden

8.1.1 De Verzekeraar kan afwijken van de bepalingen uit de Gedragscode indien er sprake is van een Dringende Reden. Aan de hand van de specifieke feiten en omstandigheden van het geval beoordeelt de Verzekeraar of de Dringende reden zwaarder weegt dan het beschermen van de rechten en vrijheden van de Betrokkene. Verzekeraars passen deze uitzonderingsmogelijkheid op de Gedragscode strikt toe in het kader van:

(a) het voorkomen, opsporen, onderzoeken en vervolgen van overtredingen van wetgeving, regelgeving of bedrijfsregels van Verzekeraars (daaronder inbegrepen de samenwerking met relevante autoriteiten); of

(b) het beschermen en verdedigen van de rechten en vrijheden van de Verzekeraar, het personeel of andere personen (waaronder de Betrokkene of een derde), zoals:

(i) de veiligheid van personen, Verzekeraars en de sector; of

(ii) bedrijfsgeheimen en de reputatie Verzekeraars; of

(iii) de continuïteit en integriteit van de dienstverlening van Verzekeraars en van de sector; of

(iv) de betrokkenheid van adviseurs op onder meer het gebied van recht, fiscaliteit en verzekeringen.

# 9 Naleving Gedragscode

## 9.1 Functionaris Gegevensbescherming

9.1.1 Verzekeraars stellen in beginsel een Functionaris Gegevensbescherming aan. De Functionaris Gegevensbescherming is een deskundige, onafhankelijke professional die de Verzekeraar van binnenuit adviseert over de bescherming van Persoonsgegevens en toeziet op de naleving van de Gedragscode en geschilbeslechting in overeenstemming met artikel 9.3.1. van de Gedragscode. Verzekeraars stellen de Functionaris Gegevensbescherming in de gelegenheid zijn taak naar behoren te vervullen. Verzekeraars kunnen van het aanstellen van een FG afzien, indien de aard van de dienstverlening en/of producten daartoe aanleiding geven.

## 9.2 Interne onderzoeken

9.2.1 Verzekeraars geven invulling aan het belang van correcte naleving van de Gedragscode door periodiek interne onderzoeken te gelasten. Deze interne onderzoeken zien op de naleving van de Gedragscode en geldende wet- en regelgeving ten aanzien van de bescherming van Persoonsgegevens en controleren ook de rechtmatigheid van gegevensverwerkingen. De Functionaris Gegevensbescherming adviseert de Verzekeraar over de opzet en de inhoud van interne onderzoeken.

## 9.3 Geschillen

9.3.1 Verzekeraars richten een interne klachtenprocedure in, zodat een Betrokkene een klacht kan indienen over het handelen van een Verzekeraar bij mogelijke strijd met de Gedragscode of geldende wet- en regelgeving.

9.3.2 Als een Betrokkene de interne klachtenprocedure heeft doorlopen en zich op het standpunt stelt dat de Verzekeraar de klacht ontoereikend heeft behandeld, kan de Betrokkene een klacht indienen tegen de Verzekeraar bij de Stichting Klachteninstituut Financiële Dienstverlening (Kifid), postbus 93257, 2509 AG Den Haag. De Betrokkene kan zich ook rechtstreeks wenden tot de Autoriteit Persoonsgegevens of de bevoegde rechter.

# 10 Definities

In deze Gedragscode geldt het volgende:

**ACM** is de Autoriteit Consument & Markt;

**AP** is de Autoriteit Persoonsgegevens;

**AVG** is de Algemene Verordening Gegevensbescherming (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016;

**Bestand** is elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn, ongeacht of dit geheel gecentraliseerd of gedecentraliseerd is dan wel op functionele of geografische gronden is verspreid;

**Betrokkene** is degene op wie een Persoonsgegeven betrekking heeft;

**Bijzondere Persoonsgegevens** zijn Persoonsgegevens waaruit ras of etnische afkomst, politieke opvatting, religieuze of levensbeschouwelijke overtuiging, het lidmaatschap van een vakbond, genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, gegevens over gezondheid of seksueel gedrag of seksuele gerichtheid blijkt;

**BSN** is het Burgerservicenummer;

**Derde** is ieder persoon, behalve de Betrokkene, de Verwerkingsverantwoordelijke, de Verwerker, de Verzekeraar of enig ander persoon die onder rechtstreeks gezag van de Verwerkingsverantwoordelijke of de Verwerker gemachtigd is om Persoonsgegevens te verwerken;

**Direct Marketing** is het gericht overbrengen van informatie door een Verzekeraar aan een Betrokkene ter bevordering van de totstandkoming van een overeenkomst;

**DNB** is De Nederlandsche Bank;

**DPIA** is Data Protection Impact Assessment, oftewel een gegevensbeschermingseffectbeoordeling, in overeenstemming met artikel 35 AVG;

**Dringende Reden** is gedefinieerd in artikel 8.1.1;

**Extern Verwijzingsregister** (**EVR**) is de deelverzameling van het Incidentenregister van een deelnemer aan het PIFI, die uitsluitend verwijzingsgegevens bevat over (rechts)personen en is bestemd voor gebruik door (de organisaties van) deelnemers aan dat protocol;

**Functionaris Gegevensbescherming** (**FG**) is de functionaris voor de gegevensbescherming als bedoeld in afdeling 4, artikel 37 e.v. van de AVG;

**Gebeurtenis** is een voorval dat de aandacht verlangt van een Verzekeraar vanwege een (mogelijk) effect op de veiligheid en integriteit van de bedrijfsvoering, werknemers, klanten, overige relaties en de verzekeringsbranche. Hieronder valt bijvoorbeeld mogelijke fraude of ander laakbaar of onrechtmatig gedrag, potentiële en daadwerkelijke vorderingen, onder meer ten aanzien van een met een Verzekeraar gesloten overeenkomst en het niet nakomen van contractuele verplichtingen of andere (toerekenbare) tekortkomingen;

**Gebeurtenissenadministratie** is de Verwerking van Persoonsgegevens in verband met een Gebeurtenis;

**Gedragscode** is deze Gedragscode Verwerking Persoonsgegevens Verzekeraars;

**Gezondheidsgegevens of gegevens over gezondheid** zijn Persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven;

**Groep** is de economische eenheid van rechtspersonen en vennootschappen waartoe een Verzekeraar behoort;

**Groepsmaatschappij** is een organisatie waarmee de Verzekeraar een economische eenheid van rechtspersonen en vennootschappen vormt;

**Incident** is een gebeurtenis die als gevolg heeft, zou kunnen hebben of heeft gehad dat de belangen, integriteit of veiligheid van een Verzekeraar, cliënten of medewerkers van een Verzekeraar, zelf of de sector als geheel in het geding zijn of kunnen zijn. Bijvoorbeeld het falsificeren van nota's, identiteitsfraude, verduistering in dienstbetrekking en opzettelijke misleiding;

**Incidentenregister** is een gegevensverzameling van de Verzekeraar die tevens deelneemt aan het PIFI, waarin gegevens worden vastgelegd naar aanleiding van of betrekking hebbend op een (mogelijk) Incident;

**Intern Verwijzingsregister (IVR)** is de deelverzameling van de Gebeurtenissenadministratie van de Verzekeraar, die uitsluitend verwijzingsgegevens bevat met betrekking tot (rechts)personen en bestemd is voor intern gebruik binnen de maatschappij of Groep, in overeenstemming met artikel 7.10.1. van de Gedragscode;

**Kifid** is het Klachteninstituut Financiële Dienstverlening;

**Medisch Adviseur** is de arts en de medische dienst of staf die onder diens verantwoordelijkheid valt en binnen de door de arts bepaalde richtlijnen handelt, die Gezondheidsgegevens verwerkt om een onafhankelijk deskundig advies te kunnen geven over de gezondheidstoestand van de volgende Betrokkenen: (i) de verzekeringnemer; (ii) personen die een claim

hebben ingediend bij een verzekeringnemer of diens verzekeraar; (iii) de te verzekeren persoon;

**Persoonsgegevens** is alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (de Betrokkene); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;

**PIFI** is het Protocol Incidentenwaarschuwingssysteem Financiële Instellingen;

**Pseudonimisering** is het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke Betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de Persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld;

**Strafrechtelijke gegevens** zijn Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen als bedoeld in artikel 10 van de AVG, alsmede Persoonsgegevens betreffende een door de rechter opgelegd verbod naar aanleiding van onrechtmatig of hinderlijk gedrag;

**Tw** is de Telecommunicatiewet;

**UAVG** is de Uitvoeringswet Algemene Verordening Gegevensbescherming;

**Veiligheidszaken** is de afdeling of de persoon die binnen Verzekeraar verantwoordelijk is voor de Verwerking van Persoonsgegevens in het kader van het waarborgen van de veiligheid en integriteit van de Verzekeraar of de sector en het voorkomen van fraude;

**Verbond** is het Verbond van Verzekeraars;

**Verwerker** is een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de Verwerkingsverantwoordelijke Persoonsgegevens verwerkt;

**Verwerking** is een bewerking of een geheel van bewerkingen met betrekking tot Persoonsgegevens of een geheel van Persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending,

verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;

**Verwerkingsverantwoordelijke** is een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van Persoonsgegevens vaststelt;

**Verzekeraar** is gedefinieerd in artikel 2.1;

**Verzekerde** is de natuurlijke- of rechtspersoon die overeenkomstig de polisvoorwaarden als rechthebbende op schadevergoeding of uitkering is aan te merken, dan wel degene wiens leven of gezondheid de verzekering betreft;

**Wft** is de Wet op het financieel toezicht;

**Wwft** is de Wet ter voorkoming van witwassen en financieren van terrorisme.

# 11 Artikelsgewijze Toelichting

## 11.1 Afdeling 1

*Artikel 1.1.1.*

De inleidende overwegingen beschrijven de bestaansreden van deze Gedragscode en de achterliggende reden dat het Verbond van Verzekeraars de Gedragscode heeft ontwikkeld. De Verwerking van Persoonsgegevens door Verzekeraars wordt gereguleerd door een lange reeks van wetten en lagere regelgeving. In aanvulling op de Europese Algemene Verordening Gegevensbescherming (AVG) en de Nederlandse Uitvoeringswet AVG (UAVG), zijn vele andere wetten van belang voor de Verwerking van Persoonsgegevens door Verzekeraars, zoals de Wet op het financieel toezicht (Wft), de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) en de Telecommunicatiewet (Tw). Daarnaast bevatten de beleidsregels, besluiten, richtsnoeren en andere richtlijnen van (sector)toezichthouders als de EDPB, Autoriteit Persoonsgegevens, De Nederlandsche Bank en de Autoriteit Financiële Markten regels op allerlei onderwerpen om de transparante, veilige en zorgvuldige Verwerking van Persoonsgegevens door Verzekeraars te waarborgen.

Bij Verzekeraars bestaat de behoefte deze vaak algemene regels concreet uit te werken voor de eigen sector. Voor Verzekerden, Betrokkenen en de samenleving bestaat tegelijkertijd de behoefte te weten hoe Verzekeraars omgaan met Persoonsgegevens. De Gedragscode wil deze twee belangen samenbrengen en kan op brede steun rekenen binnen de sector. Verzekeraars leven de bepalingen van deze Gedragscode na in hun eigen bedrijfsvoering en hun privacybeleid. De Gedragscode geldt niet zonder meer voor gevolmachtigd agenten. Dit zijn financiële dienstverleners die namens Verzekeraars optreden richting de klant. Verzekeraars die onder deze Gedragscode vallen, verplichten Gevolmachtigd agenten om de Gedragscode na te leven indien en voor zover zij deze inschakelen.

*Artikel 1.1.2.*

Het Verbond beoogt met deze Gedragscode de algemene wet- en regelgeving voor de Verwerking van Persoonsgegevens uit te leggen voor Verzekeraars en zo de naleving ervan te bevorderen. De Gedragscode is geen volledige kopie van alle wet- en regelgeving die van toepassing is op de Verwerking van Persoonsgegevens, maar heeft juist als doel deze wet- en regelgeving verder uit te werken in specifieke bepalingen. De Gedragscode strekt tot zelfregulering van de sector. De Gedragscode is daarmee geen formele gedragscode in de zin van de AVG. De voorwaarden die de Europese privacytoezichthouders in hun richtlijnen voor formele gedragscodes hebben gesteld, zijn zodanig dat daaraan nog niet kan worden voldaan. Het gaat dan vooral om het inrichten van een onafhankelijk orgaan dat toezicht moet houden op de gedragscode.

De bepalingen van de Gedragscode worden in deze toelichting geconcretiseerd aan de hand van praktijkvoorbeelden. Zo schept de Gedragscode duidelijke kaders waarbinnen Verzekeraars Persoonsgegevens kunnen verwerken en biedt de Gedragscode op dit vlak inzicht aan Verzekerden en de bredere samenleving.

## 11.2 Afdeling 2

*Artikel 2.1.1.*

De Gedragscode wordt breed gedragen binnen de verzekeringsbranche. Dit artikel regelt welke verzekeraars zijn gebonden door de Gedragscode. Alle leden van het Verbond van Verzekeraars zijn automatisch gebonden aan de bepalingen van de Gedragscode ten aanzien van hun verzekeringsactiviteiten. Onderdelen van verzekeraars die niet optreden als verzekeraar, vallen niet onder de Gedragscode.

Natuurlijke en rechtspersonen die niet vallen onder de definitie van Verzekeraars, zoals onafhankelijke tussenpersonen, gevolmachtigd agenten, rechtsbijstandverleners en schaderegelingskantoren kunnen (onderdelen van) de Gedragscode onderschrijven in hun interne en externe privacybeleid. Het Verbond van Verzekeraars moedigt een zo breed mogelijke onderschrijving van de Gedragscode aan. Wanneer verzekeraars taken uitbesteden aan Gevolmachtigd agenten, zijn zij verplicht naleving van de code af te dwingen in de volmachtovereenkomst.

Voor leden van Zorgverzekeraars Nederland geldt de Gedragscode Verwerking Persoonsgegevens Zorgverzekeraars.

*Artikel 2.2.1.*

Paragraaf 2.2. van de Gedragscode regelt wanneer de Gedragscode wel en niet van toepassing is. De strekking van deze bepaling is dat een Verzekeraar ten aanzien van vrijwel alle Verwerkingen met Persoonsgegevens de regels uit de Gedragscode dient op te volgen. Vanaf het verzamelen tot het vernietigen van Persoonsgegevens, inclusief alle tussenliggende handelingen, is de Gedragscode van toepassing.

*Artikel 2.2.2.*

De Verwerking van Persoonsgegevens van het personeel van een Verzekeraar in zijn hoedanigheid als werkgever valt buiten de reikwijdte van de Gedragscode. Op zulke Verwerkingen, bijvoorbeeld in het kader van salarisadministratie en sollicitatieprocedures, is de algemene wet- en regelgeving voor de Verwerking van Persoonsgegevens uiteraard gewoon van toepassing. Als een werknemer van een Verzekeraar tevens Verzekerde, meeverzekerde of Betrokkene is ten opzichte van de Verzekeraar, bijvoorbeeld bij personeelsverzekeringen, geldt de Gedragscode onverkort in die klantrelatie. De Gedragscode is evenmin van toepassing op de Verwerking van Persoonsgegevens die (i) in het Incidentenregister, of (ii) het Externe Verwijzingsregister zijn opgenomen. Op deze Verwerkingen is het Protocol Incidentenwaarschuwingssysteem Financiële Instellingen (PIFI) van toepassing.

In aanvulling op de Gedragscode hebben het Verbond en de verzekeraars voor specifieke gevallen aanvullende gedragscodes, protocollen en convenanten ontwikkeld. Deze specifieke instrumenten scheppen gedetailleerde kaders voor Verzekeraars voor de Verwerking van Persoonsgegevens in concrete gevallen en zijn niet in strijd met de Gedragscode. Alle zelfregulering van de sector is raadpleegbaar via de website van het Verbond: https://www.verzekeraars.nl/branche/zelfregulering.

## 11.3 Afdeling 3

*Artikel 3.1.1.*

In deze bepaling staan de overkoepelende beginselen voor de Verwerking van Persoonsgegevens door Verzekeraars opgenomen. In alle Verwerkingen geven Verzekeraars zich rekenschap van de privacybelangen van de Betrokkene. In gevallen waarin wet- en regelgeving en de specifieke bepalingen van de Gedragscode niet voorzien, beoordelen Verzekeraars de Verwerking van Persoonsgegevens aan de hand van deze algemene beginselen. Het is van belang deze beginselen een centrale plek te geven in de Gedragscode. Zo kan het voorkomen dat bestaande regels geen goed antwoord hebben op nieuwe technologische omwentelingen. Het is bijvoorbeeld denkbaar dat technologische omwentelingen, zoals kunstmatige intelligentie, de aard en de omvang van Verwerkingen van Persoonsgegevens in verregaande mate veranderen. Verzekeraars zullen aan de hand van de overkoepelende beginselen altijd beoordelen of een handeling die impact heeft op de privacybelangen van Betrokkenen. Zijn de gevolgen voor de privacy van de Betrokkenen in verhouding met de belangen van de Verzekeraar (beginsel 'proportionaliteit')? Zijn er minder ingrijpende manieren voor de Verzekeraar om dezelfde doeleinden te bereiken (beginsel 'subsidiariteit')? Verzekeraars zullen deze beginselen en die van vertrouwelijkheid, transparantie en zorgvuldigheid in al hun handelen hoog in het vaandel houden, ook als wet- en regelgeving, richtlijnen van relevante toezichthouders en de Gedragscode (nog) geen duidelijke juridische kaders bieden.

*Artikel 3.2.1.*

Verzekeraars baseren iedere Verwerking van Persoonsgegevens op één van de in de geldende wet- en regelgeving genoemde grondslagen. Indien geen van de grondslagen van toepassing is, is de Verwerking van Persoonsgegevens niet toegestaan. In afdeling 4 en afdeling 5 koppelt de Gedragscode deze wettelijke grondslagen - zoals de uitdrukkelijke toestemming van de Betrokkene of het voldoen aan een wettelijke zorgplicht uit financiële regelgeving - aan veelvoorkomende doeleinden voor de Verwerking van Persoonsgegevens in de sector.

*Artikel 3.3.1.*

Verzekeraars verzamelen Persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. De Verzekeraar stelt deze doeleinden vast voorafgaand aan de Verwerking. Welbepaald houdt in dat de doelomschrijving duidelijk moet zijn. In artikel 4 bepaalt de Gedragscode de doeleinden voor de Verwerking van Persoonsgegevens door Verzekeraars. Het betreffende doeleinde bepaalt in belangrijke mate de toepasselijkheid van andere bepalingen in de Gedragscode, zoals de toegestane grondslag voor de Verwerking, het beveiligingsniveau en de bewaartermijn van de Persoonsgegevens.

Verzekeraars verzamelen Persoonsgegevens bij de Betrokkene zelf, bijvoorbeeld via een aanvraagformulier of een gezondheidsverklaring om een verzekering af te sluiten. Daarnaast verzamelen Verzekeraars Persoonsgegevens via technologische kanalen, zoals cookies op een website, direct vanaf de smartphone bij het gebruik van een app, de 'Mijnomgeving' van de verzekeraar en social media. De verzameling van Persoonsgegevens via technische kanalen is in belangrijke mate gereguleerd door de Telecommunicatiewet en wordt verder uitgewerkt in afdeling 7.1 van de Gedragscode. Verzekeraars verzamelen ook Persoonsgegevens via externe organisaties. Zo hebben Verzekeraars onder financiële wetgeving (zoals de Wft en het Besluit Gedragstoezicht Financiële Instellingen Wft) de plicht om Customer Due Diligence (CDD), oftewel klantonderzoek, uit te voeren en klantenbestanden up-to-date te houden. Ook kunnen zij

researchbureaus inschakelen die de Verzekeraar helpen bij marketingactiviteiten. Verzekeraars zullen Verwerking altijd afwegen in het licht van de doeleinden en de grondslag van de Verwerking, de Betrokkene altijd informeren hoe Persoonsgegevens zijn verzameld (zie artikel 6.1 van de Gedragscode) en passende waarborgen treffen voor de bescherming en beveiliging van Persoonsgegevens, zoals het afsluiten van een Verwerkersovereenkomst (zie artikel 7.8 van de Gedragscode).

*Artikel 3.4.1.*

De kwaliteit van Persoonsgegevens omvat twee aspecten. Uit de woorden 'ter zake dienend' volgt dat Verzekeraars niet meer Persoonsgegevens mogen verwerken dan redelijkerwijs noodzakelijk voor de bedrijfsvoering. Hiermee geven Verzekeraars uitvoering aan het wettelijke beginsel van 'dataminimalisatie' en de beperking van de opslag van Persoonsgegevens. Het doel van de Verwerking is in belangrijke mate bepalend voor de aard en de omvang van de Persoonsgegevens die Verzekeraars mogen verwerken, en hoe lang zij deze Persoonsgegevens mogen verwerken. Deze beginselen worden in deze Gedragscode concreet uitgewerkt, bijvoorbeeld in de bepalingen over de doeleinden voor de Verwerking van Persoonsgegevens (afdeling 4) en het bewaarbeleid (artikel 7.5). Verzekeraars houden een overzicht bij van Verwerkingen van Persoonsgegevens in een daartoe bestemd verwerkingsregister.

Daarnaast dienen Persoonsgegevens 'juist' te zijn. De Verantwoordelijke moet die maatregelen treffen die redelijkerwijs nodig zijn om ervoor te zorgen dat de Persoonsgegevens accuraat zijn. Deze verplichting, die ook op grond van financiële wetgeving op Verzekeraars rust, is niet absoluut. Verzekeraars zijn namelijk vaak afhankelijk van de Persoonsgegevens die de Betrokkene verstrekt. Verzekeraars zullen klanten en andere Betrokkenen dan ook wijzen op het belang van het verstrekken van de juiste Persoonsgegevens en het tijdig doorgeven van wijzigingen.

*Artikel 3.5.1.*

Privacywetgeving bevat een aantal belangrijke rechten die de Betrokkene in staat stellen een oordeel te vormen over de Verwerking van de hun betreffende Persoonsgegevens door Verzekeraars, zoals het recht op inzage en het recht op bezwaar. De AVG bevat ook een recht op dataportabiliteit. Artikel 6 van de Gedragscode werkt deze rechten in detail uit.

*Artikel 3.6.1.*

In uitzonderlijke gevallen kunnen Verzekeraars afwijken van de basisbeginselen voor de Verwerking van Persoonsgegevens en de bepalingen uit de Gedragscode. Verzekeraars leggen deze Dringende redenen, zoals de bescherming van de veiligheid van personen, restrictief uit. De Dringende redenen staan opgesomd in artikel 8.

## 11.4 Afdeling 4

*Artikel 4.1.1.*

In deze afdeling staan de belangrijkste doelen voor de Verwerking van Persoonsgegevens door Verzekeraars. In beginsel zullen Verzekeraars Persoonsgegevens niet verwerken voor andere doeleinden, dan waarvoor zij de Persoonsgegevens verzameld hebben (het beginsel van doelbinding).

*Artikel 4.1.2.*

Geldende wet- en regelgeving (bijvoorbeeld artikel 6 lid 4 van de AVG) geeft Verzekeraars de mogelijkheid Persoonsgegevens voor andere doeleinden te verwerken. Deze verdere Verwerking is aan aanvullende voorwaarden gebonden. Het doel van de nieuwe Verwerking dient verenigbaar te zijn met het doel waarvoor de Persoonsgegevens oorspronkelijk zijn verkregen. Naast deze verwantschap van de doeleinden spelen de aard van de gegevens, de gevolgen van de Verwerking voor de Betrokkene en de mate waarin ten aanzien van de Betrokkene is voorzien in passende waarborgen een belangrijke rol. Bijvoorbeeld, hoe gevoeliger het Persoonsgegeven is, hoe terughoudender de Verzekeraar mag aannemen dat er sprake is van een geoorloofde verdere Verwerking.

De Verzekeraar moet de hiervoor genoemde factoren in onderling verband beoordelen en afwegen. Geen van de factoren is op zichzelf van doorslaggevende betekenis. Als er bijvoorbeeld een zekere verwantschap bestaat met het doel van verkrijging, maar de Persoonsgegevens door het gebruik in een bepaalde context gevoeliger van aard worden en de gevolgen voor de Betrokkenen ingrijpend zijn, zal er niet snel sprake zijn van verenigbaar gebruik. Als de verdere Verwerking van Persoonsgegevens alleen ziet op analyses voor historische, statistische en wetenschappelijke doeleinden in overeenstemming met artikel 4.3 van de Gedragscode, is er eerder sprake van geoorloofd verenigbaar gebruik. Verzekeraars kunnen technieken als pseudonimisering toepassen, in overeenstemming met artikel 7.6 van de Gedragscode, om de Persoonsgegevens in een dataset minder gevoelig te maken en de gevolgen voor de privacy van de Betrokkene te beperken. Bij de beoordeling van verenigbaar gebruik dient de Verzekeraar dus de open normen van geval tot geval te beoordelen om te kunnen vaststellen of een bepaalde gegevensuitwisseling geoorloofd is. Daarom dienen Verzekeraars bij de beoordeling van zulke verdere Verwerkingen van Persoonsgegevens een DPIA uit te voeren, in overeenstemming met de criteria van artikel 7.4 van de Gedragscode.

*Artikel 4.2.1.*

Een van de belangrijkste doelen voor de Verwerking van Persoonsgegevens door Verzekeraars is het aangaan en uitvoeren van de verzekering. Verzekeraars verwerken Persoonsgegevens voor dit doeleinde in tal van praktijksituaties, zoals de afwikkeling van de premiebetalingen, het verifiëren van de identiteit van de Betrokkene, de administratie van de verzekering, de afhandeling van schadeclaims of het vaststellen van de hoogte van de premie. Verzekeraars kunnen bijvoorbeeld binnen een Groep verifiëren of bij een ander onderdeel van de Groep nog een uitkering onder een schadeverzekering verschuldigd is en om het klantenbestand accuraat te houden. Verzekeraars verwerken Persoonsgegevens ook in de precontractuele fase, oftewel voorafgaand aan het sluiten van de verzekering. Dat betekent dat zij bij het aangaan van een verzekering een risico-inschatting maken van de Betrokkene en op basis daarvan de premie vaststellen voor een verzekering of herverzekering. Verzekeraars laten zich daarbij leiden door wet- en regelgeving, richtlijnen van relevante toezichthouders en door hun speciale rol in het maatschappelijke verkeer, waarin zij solidariteit en gemeenschappelijk dragen van risico's mogelijk maken. Het aanvraagproces is grafisch weergegeven in de infographic 'Aanvragen verzekering' in de bijlage bij de Gedragscode.

Verzekeraars kunnen Persoonsgegevens verstrekken aan de bij verdere Verwerking van Persoonsgegevens betrokken partijen, voor zover deze redelijkerwijs noodzakelijk zijn voor verificatie- en/of reconstructiedoeleinden. Dit komt in de praktijk bijvoorbeeld vaak voor bij de afhandeling van schadeclaims. Voordat Verzekeraars een verzekering afsluiten, en als er tijdens de uitvoering van de verzekering concrete aanleiding toe is, kunnen Verzekeraars controleren of bepaalde Persoonsgegevens in daartoe opgerichte waarschuwingssystemen zijn opgenomen om de

veiligheid en integriteit van de dienstverlening en de sector te waarborgen. Dit doeleinde wordt nader uitgewerkt in artikel 4.5 van de Gedragscode. Verzekeraars zoeken daarbij aansluiting bij de aanbevelingen die zijn gedaan door de Europese privacytoezichthouders, zoals algorithmic auditing om discriminatie te voorkomen.[2]

*Artikel 4.2.2.*

Geautomatiseerde besluitvorming speelt een belangrijke rol in de verzekeringsbranche. De beoordeling en analyse van grote hoeveelheden data is namelijk noodzakelijk voor het aangaan en uitvoeren van een verzekering. Verzekeraars passen hiertoe technologieën, waaronder geautomatiseerde verwerkingen en profilering, toe. Deze technologieën stellen Verzekeraars namelijk in staat om risico's van miljoenen Nederlanders te beoordelen en te verzekeren.

Het toepassen van die technologieën omvat niet altijd het nemen van een besluit over een aanvraag voor een verzekering van een Betrokkene. Verzekeraars kunnen zulke technologieën namelijk ook inzetten voor andere doeleinden, zoals naleving van wettelijke taken, bijvoorbeeld ter voorkoming van witwassen en terrorismefinanciering. Daarnaast moeten Verzekeraars op basis van financiële wetgeving hun klanten kennen (Customer Due Diligence, oftewel klantonderzoek), voordat zij bepaalde producten of diensten kunnen afnemen. Geautomatiseerde besluitvorming is essentieel bij het voldoen aan deze verplichting. Verzekeraars passen zulke technologieën alleen toe in overeenstemming met de AVG. De AVG schept speciale waarborgen ten aanzien van volledig geautomatiseerde besluitvorming waaraan voor de Betrokkene rechtsgevolgen zijn verbonden of die hem in aanmerkelijke mate treft, zoals de beëindiging van een verzekering.

Verzekeraars treffen passende maatregelen om de transparantie van zulke Verwerkingen te waarborgen. Zo geven zij invulling aan de rechten van Betrokkenen en beperken zij de impact op hun persoonlijke levenssfeer. Verzekeraars dragen ook zorg voor periodieke evaluatie van de geautomatiseerde besluitvorming, zodat de algemene beginselen van afdeling 3 van de Gedragscode niet alleen zijn gewaarborgd op het moment van het optuigen van het systeem, maar ook gedurende het gebruik ervan.

Verzekeraars beoordelen een schriftelijk verzoek van de Betrokkene naar aanleiding van volledig geautomatiseerde besluitvorming waaraan voor de Betrokkene rechtsgevolgen zijn verbonden of die hem in aanmerkelijke mate treft, met behulp van menselijk beoordelingsvermogen. De Betrokkene hoeft niet expliciet te hebben verzocht om deze menselijke controle.

*Artikel 4.3.1.*

Verzekeringen bestaan om met elkaar risico's te delen. Verzekeraars moeten voor hun bedrijfsvoering, en vaak ook op grond van financiële wetgeving, historische, statistische en wetenschappelijke analyses uitvoeren om effectieve, eerlijke en betaalbare verzekeringen aan te kunnen bieden. Hierbij maken Verzekeraars gebruik van nieuwe technologieën, zoals datamining, big data analytics en kunstmatige intelligentie. Zo kunnen Verzekeraars bestaande informatie in een database (zoals een klantenbestand) analyseren om nieuwe verbanden te ontdekken die iets zeggen over ontwikkelingen in bijvoorbeeld verzekeringsrisico's, bedrijfsprocessen of de prijs van een product. Verzekeraars kunnen voor dit doeleinde onder meer gearchiveerde informatie en gegevens uit externe bronnen gebruiken. Denk aan gegevens uit openbare registers (zoals het Handelsregister van de Kamer van Koophandel en het kadaster), openbare bronnen (zoals kranten) of gegevens afkomstig van onderzoeksbureaus. Dit soort onderzoek resulteert onder meer in

[2] Zie Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251, p. 30.

bedrijfseconomische indicatoren en gegevens over het gebruik van producten en diensten. Een voorbeeld hiervan is onderzoek naar claimoorzaken rondom smartphones. In dit domein is er sprake van een relatief groot aantal claims. Verzekeringsdata worden dan verwerkt om een claimtrend te signaleren, een oorzaak te benoemen en vervolgens aanpassingen in het product of het aanvraagproces te maken. Met zulke historische en statistische inzichten voorkomen Verzekeraars oneigenlijk gebruik van verzekeringsproducten en blijft de schadelast voor andere verzekerden beperkt.

Verzekeraars nemen passende maatregelen om de impact op de persoonlijke levenssfeer van Betrokkenen te beperken (het principe van 'privacy by design'). In overeenstemming met artikel 7.4 van de Gedragscode voeren Verzekeraars waar nodig een DPIA uit om deze impact in kaart te brengen. De beschermende maatregelen hangen samen met het doel van de analyse en de impact van de analyse. Verzekeraars kunnen de te gebruiken informatie bijvoorbeeld zorgvuldig selecteren en isoleren in een aparte dataset, zodat alleen de informatie wordt verwerkt die voor de analyse van belang is (dataminimalisatie). Daarnaast kunnen Verzekeraars waarborgen dat alleen de medewerkers die noodzakelijkerwijs toegang moeten hebben tot de dataset om de analyse uit te voeren toegang hebben tot de dataset, in plaats van alle medewerkers van de Verzekeraar (functionele scheiding van toegang). Ook kunnen Verzekeraars de dataset anonimiseren, zodat de dataset niet langer Persoonsgegevens bevat, of Pseudonimisering toepassen. Pseudonimisering en andere passende technische en organisatorische maatregelen worden nader uitgewerkt in de volgende bepalingen.

*Artikel 4.3.2.*

Verzekeraars maken onderscheid tussen het opstellen van groepsprofielen voor historische, statistische of wetenschappelijke doeleinden en het toekennen van een score of kenmerk aan een persoon op basis van een groepsprofiel. Bij het opstellen van groepsprofielen mogen aan de invoerkant Persoonsgegevens worden verwerkt, mits passende waarborgen zijn getroffen om de impact op de persoonlijke levenssfeer te minimaliseren. Een DPIA dient uit te wijzen welke maatregelen passend zijn en die waarborgen dat de bij de analyse betrokken gegevens uitsluitend voor historische, statistische of wetenschappelijke doeleinden worden gebruikt. Deze maatregelen kunnen bestaan uit het pseudonimiseren van de dataset in overeenstemming met paragraaf 7.6 van de Gedragscode. Als Verzekeraars vervolgens een persoon aan dat profiel willen koppelen, kan er sprake zijn van een verdere Verwerking of een nieuwe Verwerking van Persoonsgegevens. Een verdere Verwerking is een Verwerking die verenigbaar is met de doelen waarvoor de gegevens oorspronkelijk zijn verzameld. De Verzekeraar toetst hiertoe of bijvoorbeeld marketingactiviteiten verenigbaar zijn met het doel waarvoor de Persoonsgegevens zijn verkregen (zie artikel 4.4.3. van de Gedragscode) en of de Betrokkene op het moment van verkrijging adequaat over deze Verwerking is geïnformeerd (zie paragraaf 6.1 van de Gedragscode). Verwerkingen voor andere doeleinden kunnen een andere grondslag vereisen dan de grondslag van de oorspronkelijke Verwerking. Een praktijkvoorbeeld van dat laatste is het onderzoek van Gebeurtenissen ten aanzien van een Betrokkene. Dit is veelal gericht op één of slechts enkele Betrokkenen en is in dat geval niet snel te kwalificeren als een Verwerking voor het opstellen van een groepsprofielen, maar als een Verwerking ter waarborging van de integriteit en veiligheid van de bedrijfsvoering of de sector (zie paragraaf 4.5 van de Gedragscode). Hetzelfde geldt voor zulke analyses in het kader van financiering, boekhouding, investeringen, belastingen, implementeren van bedrijfs-beheersmaatregelen, risicomanagement en audits, herverzekeringsactiviteiten, IT-onderhoud en bedrijfsstrategieën. Daarnaast zijn Verzekeraars in bepaalde gevallen op grond van financiële wetgeving verplicht om soortgelijke analyses te verrichten, zoals het berekenen van de kostprijs van producten op grond van historische data (op grond van Solvency II-wetgeving).

*Artikel 4.3.3.*

Verzekeraars beperken het gebruik van Bijzondere Persoonsgegevens voor het verrichten van historische, statistische en wetenschappelijke analyses. Soms zal het gebruik van Bijzondere Persoonsgegevens toch nodig zijn om zulke analyses uit te voeren, bijvoorbeeld de Verwerking van Gezondheidsgegevens bij het ontdekken van trends in arbeidsongeschiktheidsverzekeringen. Zulke Verwerkingen zullen Verzekeraars met extra waarborgen omkleden om de privacybelangen van de Betrokkene te waarborgen.[3]

*Artikel 4.4.1.*

Marketingactiviteiten en relatiemanagement zijn nauw verwant, omdat beide betrekking hebben op communicatie met (potentiële) klanten. Om die reden zijn beide doeleinden in deze bepaling genoemd. Bij marketing gaat het om een zuiver commercieel doeleinde; bij relatiemanagement staat service centraal. Voor relatiemanagement geldt dan ook een lichter regime binnen deze Gedragscode. De Verzekeraar verwerkt deze Persoonsgegevens ter uitvoering van de verzekering met de Betrokkene of op grond van gerechtvaardigd belang om de service te kunnen verlenen. Daarnaast hebben Verzekeraars een gerechtvaardigd belang voor de Verwerking van Persoonsgegevens voor marketingdoeleinden.[4] Zij treffen aanvullende waarborgen bij marketingactiviteiten om de privacybelangen van de Betrokkene tegemoet te komen en te voldoen aan de algemene beginselen van behoorlijke en zorgvuldige Verwerking. Daarom maken Verzekeraars bij voorkeur gebruik van Persoonsgegevens die afkomstig zijn van de Betrokkene zelf. Indien de Persoonsgegevens niet van de Betrokkene afkomstig zijn, geldt met betrekking tot de informatieplicht het bepaalde in paragraaf 6.1 van de Gedragscode. In geval van externe inkoop van Persoonsgegevens om de Betrokkene per brief te benaderen, zal de Betrokkene hiervan voorafgaand aan de verzameling van de Persoonsgegevens op de hoogte worden gesteld. Als dit onevenredig veel inspanning kost, bijvoorbeeld omdat de Verzekeraar niet beschikt over een e-mailadres, kan de Verzekeraar de Betrokkene achteraf hierover informeren en de herkomst van de Persoonsgegevens vastleggen.

Marketing- en serviceberichten kunnen nauw samenhangen met het verrichten van historisch, statistisch en wetenschappelijk onderzoek door een Verzekeraar. Een Verzekeraar kan bijvoorbeeld een online tool ontwikkelen, waarmee de Betrokkene inzicht krijgt in de afgesloten pensioenverzekering en of deze verzekering de meest gunstige is. Ook kan de Verzekeraar geaggregeerd onderzoek verrichten naar pensioentrends. Op basis van kenmerken van grote groepen personen wordt dan bekeken hoe verzekerden in algemene zin beter geïnformeerd kunnen worden over hun pensioen. Zulke onderzoeksgegevens worden gepseudonimiseerd gebruikt. Als de Betrokkene hiervoor expliciete toestemming heeft verleend, kan de Verzekeraar de Betrokkene na de analyse benaderen voor gepersonaliseerde informatie over andere pensioenverzekeringen. Verzekeraars kunnen daarnaast in het kader van het bestendigen van de klantrelatie samenwerken met Derden. Dit kan de Betrokkene voordeel bieden, bijvoorbeeld in de vorm van korting op een entreebewijs voor een pretpark of musical. Voor deze samenwerking is geen uitdrukkelijke toestemming van de Betrokkene vereist. Voor servicedoeleinden kan de Verzekeraar de door de Betrokkene ingevulde gegevens binnen de tool 'onthouden', zodat de Betrokkene zijn gegevens niet elke keer opnieuw hoeft in te vullen.

[3] Zie artikel 24 sub d UAVG.
[4] Zie overweging 47, AVG.

*Artikel 4.4.2.*

Direct Marketing is in de definities omschreven als het overbrengen van informatie door een Verzekeraar aan een Betrokkene ter bevordering van de totstandkoming van een overeenkomst. Deze bepaling maakt onderscheid tussen de verschillende kanalen voor Direct Marketing in overeenstemming met geldende wet- en regelgeving. Zo vloeien uit de Telecommunicatiewet diverse verplichtingen voort die van toepassing zijn op commerciële communicatie met een Betrokkene via telefoon, smartphone, e-mail of internet. De Telecommunicatiewet is per 1 juli 2021 gewijzigd, resulterend in een aanscherping van de regels. Daarbij is het uitgangspunt nu dat net als marketing via elektronische berichten (zoals e-mail, sms, mms), telemarketing aan natuurlijke personen niet mag plaatsvinden, tenzij hiervoor uitdrukkelijk toestemming is gegeven of het om een bestaande relatie gaat. Na afloop van ieder telemarketinggesprek moet de Betrokkene worden gewezen op de mogelijkheid van opt-out. De bel-me-niet register is niet langer nodig en dus vervallen.

Voor bestaande relaties geldt naast de mogelijkheid van opt-in het volgende. Heeft een Verzekeraar elektronische contactgegevens verkregen in het kader van de verkoop van een product of het verlenen van een dienst, dan mag de Verzekeraar deze Persoonsgegevens gebruiken voor Direct Marketing ten behoeve van gelijksoortige producten of diensten, mits de Verzekeraar de Betrokkene bij het verkrijgen van deze contactgegevens en vervolgens bij iedere Direct Marketing boodschap wijst op zijn recht deze Verwerking te beëindigen (‘opt-out’), mede in overeenstemming met artikel 6.3 van de Gedragscode.

De Telecommunicatiewet geeft daarnaast nog extra mogelijkheden voor de benadering van een Betrokkene die handelt in de uitoefening van een beroep of bedrijf, zoals wanneer die Betrokkene elektronische contactgegevens speciaal bekendmaakt om daarop marketingboodschappen te ontvangen.

*Artikel 4.4.3.*

Deze bepaling is de spiegelbepaling van artikel 4.3.2. van de Gedragscode en een nadere invulling van de algemene bepaling over verdere Verwerkingen van artikel 4.1.2. van de Gedragscode. Als een Verzekeraar een groepsprofiel heeft ontwikkeld op basis van een historische, statistische of wetenschappelijke analyse, kan de Verzekeraar eerder gepseudonimiseerde data alleen gebruiken om daarin opgenomen Betrokkenen te benaderen voor marketingdoeleinden na het uitvoeren van een DPIA. Afhankelijk van de gevolgen voor de persoonlijke levenssfeer van de Betrokkene, die moet blijken uit de uitgevoerde DPIA, dienen Verzekeraars te beoordelen of er sprake is van een nieuwe Verwerking en of Verzekeraars deze nieuw Verwerking moeten baseren op de uitdrukkelijke toestemming van de Betrokkene of op het gerechtvaardigd belang van de Verzekeraar. Het antwoord op deze vraag hangt nauw samen met het doeleinde waarvoor de Persoonsgegevens oorspronkelijk zijn verzameld, de verwantschap van dit doeleinde met het doel van de verdere Verwerking en de tijd die is verstreken tussen de verzameling en deze verdere Verwerking. De andere bepalingen van de Gedragscode gelden ook onverkort voor deze verdere Verwerking, zoals de informatieplicht en andere rechten van Betrokkenen (afdeling 6).

*Artikel 4.4.4.*

Verzekeraars beperken het gebruik van Bijzondere Persoonsgegevens voor marketingactiviteiten en relatiemanagement. Zulke Verwerkingen zullen Verzekeraars met extra waarborgen omgeven in overeenstemming met het zwaardere regime voor Bijzondere Persoonsgegevens uit artikel 5 van de Gedragscode.

*Artikel 4.5.1*

Veiligheid en integriteit zijn essentieel voor Verzekeraars. Daarnaast zijn Verzekeraars wettelijk verplicht een beheerste en integere bedrijfsvoering te hebben. Daarom moeten Verzekeraars beschermende maatregelen nemen. Zo kunnen verzekeringsfraude en overige criminaliteit worden voorkomen en bestreden. En kunnen Verzekeraars veiligheid, integriteit en kwaliteit waarborgen. De Verwerking van Persoonsgegevens in het kader hiervan is grafisch weergegeven in de infographic 'Voorkomen en bestrijden van verzekeringsfraude en -criminaliteit' in de bijlage bij de Gedragscode.

De afdeling Veiligheidszaken houdt zich binnen een Verzekeraar bezig met zaken rondom veiligheid en integriteit. Gelet op de gevoeligheid van de werkzaamheden en verwerkte informatie, is de afdeling Veiligheidszaken vaak een binnen de onderneming afgezonderde eenheid. Indien zich bij de aanvraag of uitvoering van een overeenkomst onregelmatigheden voordoen, mogen de medewerkers van de Verzekeraar Persoonsgegevens over de overeenkomst in relatie tot de geconstateerde onregelmatigheden doorgeven aan de afdeling Veiligheidszaken. Deze afdeling kan Persoonsgegevens verder verwerken in het kader van het bestrijden van verzekeringscriminaliteit, zoals verzekeringsfraude, en de gegevens, onder de voorwaarden genoemd in het PIFI, (laten) opnemen in het Incidentenregister en het EVR. Dit wordt nader uitgewerkt onder artikel 4.5.3. Verzekeraars die geen lid zijn van het Verbond kunnen de Gedragscode in overeenstemming met artikel 2.1 onderschrijven, maar krijgen niet automatisch toegang tot deze systemen. Voor de toegang tot deze systemen gelden de aanvullende voorwaarden van het PIFI.

Een aparte Verwerking van Persoonsgegevens betreft het Persoonlijk onderzoek door Verzekeraars. Het Persoonlijk onderzoek kan bijvoorbeeld noodzakelijk zijn om te voorkomen dat ten onrechte tot uitkering van een gevorderde schadevergoeding wordt overgegaan, of om de juistheid van de toedracht van een schade te onderzoeken. De legitimiteit van een claim wordt dan bijvoorbeeld gecontroleerd door het verrichten van buurtonderzoek of cameraregistratie. Op deze vormen van onderzoek is tevens de gedragscode ‘Persoonlijk onderzoek’ van toepassing.

*Artikel 4.5.2.*

Een van de maatregelen ter waarborging van de kwaliteit, veiligheid en integriteit van de onderneming en de sector is het doen van een audit. Om de correcte werking van processen aantoonbaar te maken is het onvermijdelijk dat bij deze audits Persoonsgegevens en in sommige gevallen zelfs Bijzondere Persoonsgegevens inzichtelijk zijn. Deze Persoonsgegevens worden dan niet gebruikt om een oordeel te geven over de Betrokkene, maar alleen om aan te kunnen tonen dat de Verzekeraar een zorgvuldige bedrijfsvoering heeft. Waar mogelijk worden geen Persoonsgegevens opgenomen in een audit- of onderzoeksverslag.

De audits hoeven niet noodzakelijkerwijs door een auditafdeling van een Verzekeraar uitgevoerd te worden. Een audit kan ook uitbesteed worden aan externe organisaties. Een voorbeeld hiervan is de Stichting toetsing verzekeraars. Deze organisatie voert een onafhankelijke toets uit op de naleving van zelfregulering door de leden van het Verbond van Verzekeraars.

*Artikel 4.5.3.*

Eén van de veiligheidsmaatregelen die Verzekeraars nemen is het vastleggen van Gebeurtenissen die van belang kunnen zijn voor de veiligheid en integriteit van de onderneming en de sector. Deze Gebeurtenissen worden door Verzekeraars vastgelegd in een administratie. Dit deel van de administratie wordt de Gebeurtenissenadministratie genoemd. In deze administratie worden gegevens bijgehouden die naar het oordeel van de Verzekeraar van belang kunnen zijn voor de

kwaliteit, veiligheid en integriteit van de Verzekeraar, de Groep waartoe de Verzekeraar behoort en de verzekeringsbranche. Het kan daarbij gaan om uiteenlopende gebeurtenissen. Denk aan uitkomsten van screeningsverzoeken, klachten van klanten, (mogelijke) verzekeringsfraude of het niet naleven van afspraken waaronder structureel wanbetalingsgedrag of faillissementen. De Gebeurtenissenadministratie is een verzameling van gegevens en vormt het geheugen van de Verzekeraar. Verzekeraars hebben geen inzage in elkaars Gebeurtenissenadministraties, tenzij ze deel uitmaken van dezelfde Groep. Ondernemingen die behoren tot een Groep kunnen ook een gezamenlijke Gebeurtenissenadministratie voeren.

De afdeling Veiligheidszaken of een daartoe aangewezen afdeling van de Verzekeraar kan besluiten de verwijzingsgegevens van personen waarvan gegevens zijn vastgelegd in de Gebeurtenissenadministratie op te nemen in een Intern Verwijzingsregister (IVR). Een klein deel van de informatie uit de Gebeurtenissenadministratie wordt zo toetsbaar. Het IVR bestaat ter voorkoming van toegang tot Persoonsgegevens van een brede groep medewerkers en om veilig gebruik binnen de Groep waartoe de Verzekeraar behoort te faciliteren. Dit register kan dus, net zoals de Gebeurtenissenadministratie, niet door andere verzekeraars worden geraadpleegd.

Een IVR bevat verwijzingsgegevens. Dit zijn identificerende gegevens (NAW-gegevens en geboortedatum) van personen die een zeker risico vormen. Het IVR bevat dus geen aanvullende informatie over de persoon of de Gebeurtenis. De Verzekeraar maakt steeds een zorgvuldige afweging voordat verwijzingsgegevens worden opgenomen, waarbij het gewicht van de Gebeurtenis een belangrijke rol speelt (direct of voor de toekomst). Om een Gebeurtenis op deze wijze binnen maatschappij of Groep te delen, kan onder meer een rol spelen of een redelijk vermoeden bestaat van opzettelijke benadeling door de Betrokkene. Het kan bijvoorbeeld gaan om oneigenlijk gebruik van producten, diensten en voorzieningen van een Verzekeraar of pogingen daartoe. Denk ook aan het intern signaleren van een redelijk vermoeden van het plegen van strafbare of laakbare gedragingen of (een poging tot) overtredingen van (wettelijke) voorschriften gericht tegen de Verzekeraar, haar klanten of medewerkers.

Voor zover relevant voor zijn werkzaamheden kan een medewerker van de Verzekeraar het IVR raadplegen. Bijvoorbeeld als een persoon klant wil worden of bij sollicitatieprocedures. Er vindt een toets plaats aan de hand van de NAW-gegevens en geboortedatum van de betreffende persoon. Het systeem van de toetsing werkt op basis van hit-no hit. De medewerker die de toets uitvoert ziet bij een hit niet waarom, maar wel dat een (rechts)persoon is opgenomen. In het geval van een hit moet de medewerker altijd de afdeling Veiligheidszaken of een daartoe aangewezen afdeling van de Verzekeraar inschakelen die de medewerker vervolgens adviseert. Het advies kan bijvoorbeeld zijn om wel of geen contract met de sollicitant aan te gaan. Met betrekking tot een klant kunnen bijvoorbeeld speciale voorwaarden worden afgesproken, zoals aanvullende polisvoorwaarden of dekkingsbeperkingen. Relevante afdelingen of medewerkers kunnen zo op de hoogte worden gesteld dat bepaalde personen of zaken extra aandacht nodig hebben.

Naast het hebben van een Gebeurtenissenadministratie en een IVR dient een Verzekeraar ook een branchewaarschuwingssysteem te voeren. Dit is een systeem dat het mogelijk maakt voor Verzekeraars om elkaar te waarschuwen. Omdat Persoonsgegevens in dit geval buiten de Groep worden gedeeld, gelden hiervoor bijzondere aanvullende regels. De regels met betrekking tot het branchewaarschuwingssysteem zijn vastgelegd in het Protocol Incidentenwaarschuwingssysteem Financiële Instellingen (PIFI).

In bepaalde gevallen kunnen Verzekeraars Persoonsgegevens in verband met royementen, vorderingen, het indienen van een claim en andere Gebeurtenissen mede vastleggen in registers die worden onderhouden door een onafhankelijke rechtspersoon, bijvoorbeeld de Stichting Centraal Informatiesysteem die optreedt als Verantwoordelijke voor het Centraal Informatie Systeem in de verzekeringsbranche. Op het verstrekken en raadplegen van Persoonsgegevens in deze systemen is deze Gedragscode van toepassing. De Verwerking van de Persoonsgegevens in de systemen zelf valt buiten de Gedragscode. De Stichting Centraal Informatie Systeem hanteert daarvoor een eigen privacy- en gebruikersreglement, dat is te raadplegen via de website: https://www.stichtingcis.nl/nl-nl/regelgeving.aspx.

*Artikel 4.6.1.*

De afgelopen jaren kenmerken zich door een toename van het aantal verplichtingen om Persoonsgegevens op grond van wettelijke voorschriften te verzamelen en beschikbaar te stellen. Hieronder volgen enkele voorbeelden. Daarnaast bestaan er nog vele andere wettelijke voorschriften op grond waarvan een Verzekeraar verplicht is bepaalde Persoonsgegevens te verwerken.

Financiële wetgeving verplicht Verzekeraars in toenemende mate Persoonsgegevens te Verwerken. Naast voorschriften uit algemene verzekeringswetgeving nemen bijvoorbeeld verplichtingen uit de Wft ten aanzien van klantonderzoek, ook wel Customer Due Diligence genoemd, toe. Verzekeraars hebben een zorgplicht hun klanten te kennen en volledig te informeren over bestaande risico's en betalingsverplichtingen. Ook nemen de verplichtingen op het terrein van fraudebestrijding en terrorismefinanciering toe, die bijvoorbeeld volgen uit de Europese Richtlijnen 2005/60/EU en 2006/70/EU van de Wet ter voorkoming van witwassen en financieren terrorisme (Wwft). De Wwft vereist dat de gegevens uit het document, waarmee de identiteit is vastgesteld, moeten worden vastgelegd. De Wwft is zogeheten risico-gebaseerde wetgeving. Dit houdt in dat de Verzekeraar het klantonderzoek moet afstemmen op de risicogevoeligheid voor witwassen of financiering van terrorisme van het type klant, de zakelijke relatie, het product of de transactie. Dit geeft de instelling de vrijheid om eigen keuzes te maken, rekening houdend met risico's en reeds bestaande beheersmaatregelen. In de Wwft is een belangrijke rol weggelegd voor toezichthouders. Verzekeraars zullen samenwerking aangaan met relevante toezichthouders en autoriteiten bij de verdere invulling van deze taak.

Voor verzekeraars geldt eveneens dat de Wft voorschrijft dat in sommige gevallen informatie ingewonnen moet worden over de financiële positie, kennis, ervaring, doelstellingen en risicobereidheid van een klant, bijvoorbeeld wanneer Verzekeraars adviseren over complexe producten (zoals levensverzekeringen). Ook dienen achtergrondgegevens van (aspirant-)klanten te worden verzameld en gecontroleerd. In het kader van fiscale wetgeving dient het Burgerservicenummer uitgewisseld te worden met de Belastingdienst. In aanvulling daarop wisselen Verzekeraars Persoonsgegevens uit met de Belastingdienst in het kader van renseignering (de wettelijke verplichting voor Verzekeraars om bepaalde voorgeschreven gegevens en inlichtingen aan de Belastingdienst te verstrekken). Het BSN wordt ook uitgewisseld met het UWV in het kader van de beoordeling van mogelijke arbeidsongeschiktheid.

De Sanctiewet verplicht Verzekeraars de Persoonsgegevens van Verzekeringnemers en Verzekerden bij het aangaan van de verzekering, gedurende de looptijd van de verzekering en bij het verstrekken van een uitkering te toetsen aan de nationale en internationale sanctielijsten. Opsporingsautoriteiten kunnen gegevensvorderingen indienen bij Verzekeraars op grond van het Wetboek van Strafvordering. Voldoet een vordering aan de vereiste wettelijke criteria, dan moet een Verzekeraar medewerking verlenen aan een vorderingen.

## 11.5 Afdeling 5

*Artikel 5.1.1.*

Het algemene toetsingskader voor de Verwerking van Persoonsgegevens is geregeld in afdeling 4 van de Gedragscode. Verzekeraars verwerken in voorkomende gevallen ook Gezondheidsgegevens. Deze afdeling van de Gedragscode bevat specifieke regels omtrent de Verwerking van Gezondheidsgegevens. Voor Gezondheidsgegevens geldt een zwaarder regime in aanvulling op het algemene toetsingskader. Tegelijkertijd geeft geldende wet- en regelgeving ruimere bevoegdheden aan Verzekeraars om Gezondheidsgegevens (verder) te verwerken dan bedrijven in andere sectoren.[5]

Dit hangt samen met het maatschappelijke belang van verzekeringen. De Verzekeraar kan zoals volgt uit artikel 5.1.1 Gezondheidsgegevens verwerken als dat noodzakelijk is voor de beoordeling van het door de Verzekeraar te verzekeren risico dan wel het uitvoeren van een (first of third party) verzekeringsovereenkomst. Daaronder valt bijvoorbeeld de beoordeling van het risico op arbeidsongeschiktheid tijdens de looptijd van de verzekering en of dat risico genormaliseerd moet worden met bijvoorbeeld dekkingsbeperkende clausules of een verhoogde premie.

Bij de acceptatie kan de Verzekeraar de Betrokkene vragen om een gezondheidsverklaring (GV) in te vullen. In de GV stelt de Verzekeraar onder andere vragen over klachten, ziekte of aandoeningen. De GV kan vragen bevatten over medicijngebruik, artsenbezoek, of men wel of niet rookt, het gebruik van alcohol en of de Betrokkene een bril of contactlenzen draagt. De Verzekeraar kan de Betrokkene ook vragen om een medische machtiging te verstrekken, voor het geval de Medisch Adviseur aanvullende informatie wenst op te vragen bij andere artsen/instanties (bijvoorbeeld de huisarts van de Betrokkene). Door de machtiging weet de geraadpleegde arts of andere zorgverlener/ behandelaar dat het medisch beroepsgeheim doorbroken mag worden (informatie aan de Medisch Adviseur verstrekt mag worden). Is de verzekering eenmaal tot stand gekomen, dan kan de verzekeraar ook nog om (aanvullende) Gezondheidsgegevens vragen om de aanspraak op een uitkering of een gewijzigd risico te kunnen (her)beoordelen. Bij een wijziging van het te verzekeren risico, kan dit met zich mee brengen dat om een gezondheidsverklaring of het ondergaan van een medische keuring wordt gevraagd.

Bij het beoordelen van de gezondheidstoestand zoals omschreven in voornoemde situaties speelt de Medisch Adviseur een centrale rol. Deze rol wordt nader uitgewerkt vanaf artikel 5.1.3 van de Gedragscode. De Verzekeraar kan de Betrokkene vragen een medische keuring te ondergaan. Deze keuring wordt vaak verricht door een huisarts, niet zijnde de huisarts van de Betrokkene, en kan bestaan uit medisch onderzoek en bloedonderzoek.

De Medisch Adviseur kan voor het aangaan en uitvoeren van een verzekering Gezondheidsgegevens delen met de Medisch Adviseur van een herverzekeraar. De herverzekeraar implementeert net als Verzekeraars een strikt onderscheid tussen advies en beslissing over acceptatie en claimafhandeling, heeft een Medisch Adviseur in dienst en verwerkt alleen de Gezondheidsgegevens die noodzakelijk zijn voor het aangaan en uitvoeren van de verzekering in overeenstemming met artikel 4.2 van de Gedragscode.

In sommige situaties kunnen Verzekeraars Bijzondere Persoonsgegevens opnieuw verwerken in het kader van de uitvoering van de verzekering. Een voorbeeld is de afhandeling van een tweede schadeclaim op grond van dezelfde verzekering. Voor deze Verwerking is geen uitdrukkelijke toestemming vereist als de Verzekeraar de op grond van een eerste schadeclaim door de klant

[5] Zie artikel 30 lid 3 sub b onder 1 UAVG.

verstrekte Gezondheidsgegevens wederom verwerkt. Heeft een Betrokkene bijvoorbeeld een claim ingediend op grond van een arbeidsongeschiktheidsverzekering en wordt er een orthopedische expertise verricht, dan kan de Verzekeraar deze expertise gebruiken bij de afhandeling van een tweede claim, als de Betrokkene een half jaar na beëindiging van de eerste claim een tweede claim indient vanwege dezelfde rugklachten. Betreft de tweede claim echter een andere verzekering, dan kan de Verzekeraar de Gezondheidsgegevens alleen verwerken na uitdrukkelijke toestemming van de Betrokkene. Voor de afhandeling van meerdere verzekeringsclaims op grond van dezelfde verzekering is dus geen uitdrukkelijke toestemming van de Betrokkene vereist, maar bij de afhandeling van meerdere claims uit verschillende verzekeringen is de uitdrukkelijke toestemming van de Betrokkene wél vereist, tenzij de verzekeringen hetzelfde risico dekken (bijvoorbeeld bij een WIA-verzekering gevolgd door een WIA-excedentverzekering).

Verzekeraars zijn wettelijk verplicht de veiligheid en integriteit van de bedrijfsvoering en de sector te garanderen met inachtneming van het bepaalde in paragraaf 4.5. van de Gedragscode. Een concreet voorbeeld dat in het kader van Gezondheidsgegevens vaak voorkomt, is de niet nagekomen wettelijke mededelingsplicht, ook wel bekend als 'verzwijging'. Als de Verzekeraar een redelijk vermoeden heeft dat een Betrokkene een medische situatie heeft verzwegen, heeft de Verzekeraar de plicht Gezondheidsgegevens en claimhistorie te analyseren om te evalueren of er toch eerder al aanwijzingen waren voor een verzwijging door de Betrokkene.

Dit artikel 5.1.1 somt tot slot de overige doeleinden voor de Verwerking van Gezondheidsgegevens op. Verzekeraars zijn terughoudend met de Verwerking van Gezondheidsgegevens op basis van deze overige doeleinden.

*Artikel 5.1.2.*

Dit artikel verheldert dat Verzekeraars bij de Verwerking van Gezondheidsgegevens de privacybelangen van de Betrokkene goed in kaart moeten brengen en daartoe een DPIA uitvoeren. Op basis daarvan beoordelen Verzekeraars onder meer welke beschermende maatregelen zij treffen en of verdere Verwerking geoorloofd is.

*Artikel 5.1.3.*

De Medisch Adviseur neemt een bijzondere plaats in bij de Verwerking van Gezondheidsgegevens. De Verzekeraar neemt immers op basis van het advies van de Medisch Adviseur een beslissing over de acceptatie of claimafhandeling. Om die reden brengt de Gedragscode een scheiding aan tussen enerzijds de beoordeling van de gezondheidstoestand in de vorm van een advies van de Medisch Adviseur, anderzijds de beslissing door de Technisch Acceptant of claimbehandelaar van de Verzekeraar. Gezondheidsverklaringen of medische gegevens uit de behandelend sector evenals andere medische gegevens zoals genoemd in artikel 5.1.3 moeten worden gezonden naar de Medisch Adviseur. Het is ook de taak van de Medisch Adviseur te beoordelen welke aanvullende Gezondheidsgegevens nodig zijn voor een adequate beoordeling en via welke kanalen deze Gezondheidsgegevens verzameld kunnen worden. Deze aanvullende Gezondheidsgegevens kunnen alleen verzameld worden op basis van de uitdrukkelijke toestemming van de Betrokkene. Als er informatie bij een huisarts of medisch specialist of andere hulpverlener wordt opgevraagd, gebeurt dit met medische machtiging van Betrokkene.

Voor de acceptant en claimbehandelaar kan het noodzakelijk zijn om ook bepaalde Gezondheidsgegevens te ontvangen van de Medisch Adviseur. De claimbehandelaar en de acceptant kunnen zo gemotiveerd beslissen of zij het advies van de Medisch Adviseur overnemen.

De Medisch Adviseur stelt vast welke relevante Gezondheidsgegevens hij aan de acceptant of claimbehandelaar van de Verzekeraar verstrekt. De acceptant en claimbehandelaar mogen deze gegevens uitsluitend gebruiken in het kader van die acceptatie of claimafhandeling. Bij verzuimverzekeringen toetst de Medisch Adviseur de medische oordeelsvorming en het nakomen van voorgesteld beleid door het UWV. In het kader van de uitvoering van de overeenkomst adviseert de Medisch Adviseur de verzuimverzekeraar uitsluitend in diens hoedanigheid van reïntegratiebedrijf/-afdeling, dus ten behoeve van de re-integratie. Op een arbeidsdeskundige, de persoon die binnen een verzekeringsbedrijf vaststelt in hoeverre iemand arbeid kan verrichten, is de Gedragscode volledig van toepassing. De arbeidsdeskundige stelt alleen de vragen aan de Betrokkene die nodig zijn voor een behoorlijke taakuitoefening.

De Medisch Adviseur is verantwoordelijk voor het beheer van het medisch dossier. In deze bepaling staat een niet-limitatieve opsomming van de gegevens die in het medische dossier terecht kunnen komen. Bij de (her)beoordeling van een claim of verzekeringsaanvraag geeft de Medisch Adviseur samen met zijn medisch advies de relevante Gezondheidsgegevens door aan de claimbehandelaar[6] of de acceptant. De claimbehandelaar en de acceptant kunnen zo gemotiveerd beslissen of zij het advies van de Medisch Adviseur overnemen. Verzekeraars leggen de verdeling van rollen en interne verantwoordelijkheden vast in het verwerkingsregister in overeenstemming met artikel 3.4 van de Gedragscode.

De Medisch Adviseur is niet verantwoordelijk voor de Verwerking van de Gezondheidsgegevens door de claimbehandelaar en acceptant. Evenmin valt onder de verantwoordelijkheid van de Medisch Adviseur de Verwerkingen omtrent iemands gezondheid indien noodzakelijk in het kader van het opstellen van declaraties of in het kader van juridische procedures of de behandeling van klachten. Gezondheidsgegevens die door of namens de Betrokkene zijn verstrekt in verband met het beheer van de relatie van de Verzekeraar met de Betrokkene vallen evenmin onder de verantwoordelijkheid van de Medisch Adviseur. De Verzekeraar mag Gezondheidsgegevens die een Betrokkene telefonisch verstrekt niet zonder meer vastleggen in de administratie en past in deze situatie de voorwaarden voor de Verwerking van Gezondheidsgegevens uit artikel 5.1.1 van de Gedragscode strikt toe. Als de arbeidsdeskundige spontaan Gezondheidsgegevens ontvangt van de Betrokkene, verstrekt hij deze niet aan de acceptant of de claimbehandelaar, maar vertrouwt hij deze Gezondheidsgegevens toe aan de Medisch Adviseur en informeert hij de Betrokkene hierover. Als de claimbehandelaar spontaan gezondheidsgegevens ontvangt van Betrokkene zelf mag hij deze gegevens niet vastleggen, maar geeft hij deze Gezondheidsgegevens door aan de Medisch Adviseur en informeert hij de Betrokkene hierover tenzij er geen medisch beoordelingstraject nodig is (bijvoorbeeld bij licht letsel). In dat geval legt de claimbehandelaar de Gezondheidsgegevens vast in het ‘technisch’ dossier. Wel is de Medische paragraaf van de Gedragscode Behandeling Letselschade (GBL) duidelijk over de situatie waarin er wel een medisch beoordelingstraject is gestart: in dat geval is altijd uitdrukkelijke toestemming nodig van Betrokkene (benadeelde[7]).

*Artikel 5.1.4.*

Deze bepaling is een specifieke uitwerking van het algemene inzagerecht in Verwerkingen van Persoonsgegevens, dat verder wordt uitgewerkt in paragraaf 6.2 van de Gedragscode. Voor wat betreft Gezondheidsgegevens geldt dat Betrokkene recht heeft op inzage in het medisch dossier. Het inzagerecht ziet op de Persoonsgegevens zelf en heeft als doel de Betrokkene in staat te stellen de Verwerkingen van de Verzekeraar en de Medisch Adviseur te controleren. Het inzagerecht strekt

[6] Onder claimbehandelaar kunt u ook verstaan schadebehandelaar of case manager: alle personen binnen de verzekeraar die zich bezighouden met behandeling en/of afwikkeling van de aanspraak onder een verzekering.
[7] Het kan gaan om een verzekerde, maar ook om derde partijen die een schade onder een aansprakelijkheidsverzekering claimen.

niet tot beoordeling van de totstandkoming van het medisch advies, en omvat bijvoorbeeld niet de interne notities of de werkaantekeningen van de Medisch Adviseur. De Betrokkene kan ook via een vertrouwensarts verzoeken om inzage in zijn medisch dossier. Een Verzekeraar dient ook de bescherming van de rechten en vrijheden van anderen te respecteren bij de beoordeling van een inzageverzoek. De Medisch Adviseur kan, om aan een inzageverzoek te voldoen, passende maatregelen treffen (zoals het zwartmaken van passages in een medisch dossier).

*Artikel 5.1.5.*

De Verzekeraar dient op grond van geldende wet- en regelgeving er voor te zorgen dat met de acceptant en de claimbehandelaar een geheimhoudingsverplichting overeen is gekomen.

*Artikel 5.2.1.*

Een Verzekeraar kan Persoonsgegevens van strafrechtelijke aard verwerken. Het onderliggende doeleinde van zulke Verwerkingen is meestal de acceptatie of uitvoering van een verzekering of de waarborging van de integriteit en veiligheid van de bedrijfsvoering en de sector. Deze en andere doeleinden worden hier opgesomd.

Bij een aanvraag van een verzekering vraagt de Verzekeraar naar het strafrechtelijk verleden van de aanvrager en anderen, voor zover dat voor het afsluiten van een verzekering noodzakelijk is. De verzochte feiten hebben betrekking op een periode van acht jaar voorafgaand aan de aanvraag voor een verzekering, op grond van art. 7:928 Burgerlijk Wetboek. De Betrokkene is verplicht de vraag naar waarheid te beantwoorden. Verzekeraars mogen het opgegeven strafrechtelijk verleden alleen gebruiken voor de beoordeling van de verzekeringsaanvraag en voor een beroep op onvolledige nakoming van de mededelingsplicht van de aanvrager.

Indien een gebeurtenis voldoet aan de criteria uit het Protocol Incidentenwaarschuwingssysteem Financiële Instellingen (PIFI), nemen Verzekeraars de relevante Persoonsgegevens op in een Incidentenregister en, in voorkomende gevallen, het Extern Verwijzingsregister (EVR). Dit wordt beschreven in artikel 4.5.3. In overeenstemming met artikel 2.2.2 is het PIFI van toepassing op deze Verwerking.

*Artikel 5.2.2.*

Dit artikel verheldert dat Verzekeraars bij de Verwerking van strafrechtelijke gegevens de privacybelangen van de Betrokkene goed in kaart moeten brengen en daartoe een DPIA uitvoeren. Op basis daarvan beoordelen Verzekeraars onder meer welke beschermende maatregelen zij treffen en of verdere Verwerking geoorloofd is. Verzekeraars verwerken Strafrechtelijke Gegevens daarnaast altijd in overeenstemming met het algemene toetsingskader van paragraaf 4.1. van de Gedragscode.

*Artikel 5.2.3.*

Persoonsgegevens die betrekking hebben op strafbare feiten (zoals fraude) die zijn of op grond van feiten en omstandigheden naar verwachting zullen worden begaan jegens een Groepsmaatschappij, kunnen door de Verzekeraar worden verstrekt binnen de Groep. Dit geldt ook voor Persoonsgegevens die dienen ter vaststelling van mogelijk strafbaar gedrag jegens een Groepsmaatschappij, op voorwaarde dat de gegevens uitsluitend worden verstrekt aan functionarissen die de gegevens voor de uitoefening van hun taak nodig hebben, zoals

Veiligheidszaken, alsmede aan politie en Justitie. Aan organisaties buiten de Groep mogen deze Persoonsgegevens slechts worden verstrekt indien het PIFI wordt onderschreven en nageleefd.

*Artikel 5.3.1.*

Naast Gezondheidsgegevens en Strafrechtelijke Gegevens kunnen Verzekeraars voor de doeleinden genoemd in deze bepaling andere Bijzondere Persoonsgegevens verwerken. De categorieën Bijzondere Persoonsgegevens staan opgesomd in hoofdstuk 3 van de UAVG. In de verzekeringssector vindt de Verwerking van Bijzondere Persoonsgegevens onder meer plaats voor het archiveren van de originele documenten of elektronische afschriften daarvan. Ook kan het gebruik van biometrische gegevens ten behoeve van identificatie/authenticatie met zich meebrengen dat Bijzondere persoonsgegevens worden verwerkt. Verder neemt de Verzekeraar in bepaalde gevallen het Burgerservicenummer (BSN) in de administratie op. Dat gebeurt alleen als de Verzekeraar daarvoor een wettelijke grondslag heeft, zoals bijvoorbeeld om te renseigneren aan de Belastingdienst.

*Artikel 5.3.2.*

Dit artikel verheldert dat Verzekeraars bij de Verwerking van andere Bijzondere persoonsgegevens de privacybelangen van de Betrokkene goed in kaart moeten brengen en daartoe een DPIA uitvoeren. Op basis daarvan beoordelen Verzekeraars onder meer welke beschermende maatregelen zij treffen en of verdere Verwerking geoorloofd is.

## 11.6 Afdeling 6

*Artikel 6.1.1.*

Deze paragraaf beschrijft de rechten van de Betrokkene bij de Verwerking van Persoonsgegevens door een Verzekeraar. De informatieplicht geldt ongeacht het doel of de middelen van de Verwerking, ongeacht de onderliggende reden en de gebruikte technologie. In de AVG zijn deze rechten verbeterd en uitgebreid opgesomd. Voor wat betreft de informatieplicht, die is vervat van artikel 12 tot en met 14 van de AVG, biedt de wetgeving een uitgebreide opsomming van informatie die de Verzekeraar dient mede te delen aan de Betrokkene bij de Verwerking van Persoonsgegevens. Deze verplichtingen zijn in paragraaf 6.1. niet volledig gekopieerd, maar nader uitgewerkt in het kader van voor verzekeraars en Betrokkenen relevante onderwerpen.

De onderliggende gedachte van de informatieplicht is dat de Betrokkene weet welke Persoonsgegevens voor welke doeleinden worden verwerkt, en zo de Verwerkingsverantwoordelijke kan aanspreken op deze Verwerkingen. Verzekeraars geven continu uitdrukking aan deze informatieplicht, bijvoorbeeld door een extern privacybeleid (zoals een privacy statement) op de website op te nemen en gezamenlijk deze Gedragscode te ontwikkelen. Ook als de Verzekeraar de Persoonsgegevens niet direct bij de Betrokkene verzamelt, geldt de informatieplicht, tenzij de Verzekeraar de Betrokkene reeds op de hoogte heeft gesteld, bijvoorbeeld via een privacystatement op de website. In deze Gedragscode zijn al enkele voorbeelden ter sprake gekomen van verzamelen van Persoonsgegevens bij Derden, zoals klantonderzoek en het verifiëren van klantgegevens bij Derden (Customer Due Diligence) in het kader van de wettelijke zorgplicht van Verzekeraars op grond van de Wft, Wwft en andere financiële wetgeving.

*Artikel 6.1.2.*

De norm is dat de informatieverplichting geldt, tenzij de Betrokkene 'reeds op de hoogte is'. Afhankelijk van de omstandigheden mag de Verantwoordelijke het ‘op de hoogte zijn’ aannemen, bijvoorbeeld omdat aan de Betrokkene de relevante informatie is overhandigd of is toegezonden of omdat uit de gedragingen van de Betrokkene blijkt dat hij op de hoogte is. Het informeren van de Betrokkene kan ook achterwege blijven als niet redelijkerwijs kan worden verwacht van de Verzekeraar dat hij de Betrokkene informeert. Hiervan kan bijvoorbeeld sprake zijn bij een vermoeden van verzekeringsfraude. Verzekeraars passen uitzonderingen op de hoofdregel van de informatieplicht restrictief toe. Verzekeraars zullen zich in zulke uitzonderlijke situaties bovendien inspannen de Betrokkene alsnog naderhand te informeren, bijvoorbeeld nadat een Persoonlijk onderzoek in het kader van mogelijke verzekeringsfraude is afgerond.

*Artikel 6.1.3.*

In aanvulling op de vereisten uit geldende wet- en regelgeving onderkennen Verzekeraars het belang van een transparante, open en eerlijke informatieverschaffing aan Betrokkenen. Dit komt de betrouwbaarheid van de onderneming en de sector als geheel ten goede. Daarnaast kunnen Verzekeraars meerdere informatielagen bieden aan Betrokkenen, zodat in de eerste laag informatie overzichtelijk en kernachtig per onderwerp wordt aangeboden en in de onderliggende lagen meer gedetailleerdere informatie te vinden. Verzekeraars hechten aan een innovatieve informatievoorziening aan Betrokkenen, bijvoorbeeld via internetportals zoals 'Mijn omgeving'.

*Artikel 6.1.4.*

Deze bepaling onderschrijft het belang van de informatieplicht bij de verdere Verwerking van Persoonsgegevens van de Gedragscode. Een veelvoorkomend voorbeeld in de praktijk is het verwerken van persoonsgegevens voor statistische doeleinden. Als daarvan sprake is, stelt de Verzekeraar de Betrokkene hiervan op de hoogte, over het algemeen via het privacy statement.

*Artikel 6.1.5.*

De Betrokkene heeft het recht informatie te krijgen over alle in dit artikel genoemde elementen van Verwerkingen die zijn gebaseerd op volledig geautomatiseerde besluitvorming. Als Verzekeraars bijvoorbeeld gebruikmaken van kredietscores die zijn opgesteld door externe onderzoeksbureaus, informeren zij de Betrokkene hierover en over de categorieën Persoonsgegevens die aan het besluit ten grondslag liggen. Zij informeren de Betrokkene ook over hun recht op bezwaar, heroverweging van het besluit door een mens en de factoren die ten grondslag liggen aan geautomatiseerde besluitvorming. De bekendmaking van deze 'logica' van de geautomatiseerde besluitvorming mag geen afbreuk doen aan bedrijfsgevoelige informatie of aan het intellectuele eigendom van de onderliggende software en algoritmes. Verzekeraars gebruiken deze uitzonderingsgronden echter niet om alle informatieverstrekking aan de Betrokkenen te beperken en streven hierin een redelijke balans na. Uitgangspunt blijft de verstrekking van begrijpelijke en relevante informatie over de geautomatiseerde besluitvorming, die de Betrokkene in staat stelt om de besluitvorming te beoordelen en de door afdeling 6 van de Gedragscode toegekende rechten uit te oefenen.

*Artikel 6.2.1.*

Een Betrokkene is gerechtigd een Verzekeraar schriftelijk een overzicht te vragen van de Verwerkingen van Persoonsgegevens. Dit overzicht dient een omschrijving van het doel van de Verwerking, de categorieën van Persoonsgegevens waarop de Verwerking betrekking heeft, de

ontvangers of categorieën van ontvangers en de beschikbare informatie over de herkomst van de Persoonsgegevens te bevatten.

Deze bepaling beschrijft de informatie die een Verzekeraar dient te leveren in antwoord op een geldig inzageverzoek. Zoals beschreven onder artikel 5.1.5 van de Gedragscode ziet het inzagerecht op de Persoonsgegevens zelf.[8] Het inzagerecht strekt niet tot dossiers van de Betrokkene, gehele documenten, verslagen van intern beraad, interne notities of werkaantekeningen. Het overzicht bevat evenmin de elektronische communicatie tussen Verzekeraar en de Betrokkene.

*Artikel 6.2.2.*

De Verwerkingsverantwoordelijke dient dit overzicht binnen een maand na de datum van ontvangst van het verzoek aan de Betrokkene te verstrekken. Bij complexe inzageverzoeken kan de Verzekeraar de beantwoording van het verzoek met twee maanden uitstellen. Deze termijnen worden opgeschort zo lang de Betrokkene de Verzekeraar niet in staat stelt aan het inzageverzoek te voldoen, bijvoorbeeld als de Verzekeraar de Betrokkene nog dient te identificeren maar geen legitimatiebewijs ontvangt. Voor een inzageverzoek kan de Verantwoordelijke een vergoeding in de kosten verlangen, als het verzoek kennelijk ongegrond of buitensporig is, bijvoorbeeld vanwege het herhaaldelijke karakter. Dat bedrag is vooralsnog vastgesteld op € 0,23 per pagina tot een maximum van € 5,00 per verzekering. Dat bedrag mag oplopen tot een maximum van € 22,50 wanneer het gaat om vanwege hun aard moeilijk toegankelijke verwerkingen of wanneer het meerdere verzekeringen betreft.

*Artikel 6.2.3.*

Een Verzekeraar hoeft geen gehoor te geven aan een verzoek tot inzage als verzoeken kennelijk ongegrond of buitensporig zijn of als er sprake is van een Dringende Reden. Een Verzekeraar kan inzage bijvoorbeeld weigeren als de voorkoming, opsporing en vervolging van strafbare feiten in het geding zijn. Het inzageverzoek mag in aanvulling op het bepaalde in afdeling 8 van de Gedragscode worden geweigerd indien sprake is van misbruik door de Betrokkene, leidt tot een disproportionele belasting van de Verzekeraar of tot aantasting van de rechten of belangen van Derden, die bedenkingen kunnen hebben tegen het verlenen van inzage. In dat geval mag een Verzekeraar besluiten die Persoonsgegevens niet te verstrekken of onleesbaar te maken.

*Artikel 6.2.4.*

De Verwerkingsverantwoordelijke moet op grond van geldende wet- en regelgeving zorgdragen voor een deugdelijke vaststelling van de identiteit om te verzekeren dat de juiste persoon toegang krijgt tot de eigen Persoonsgegevens. Bij schriftelijke verzoeken om inzage moeten daarom aangepaste maatregelen worden genomen, zoals de verplichting een kopie bij te sluiten van paspoort of rijbewijs om de handtekeningen te kunnen vergelijken, eventueel met reeds aanwezige handtekeningen. De Betrokkene mag het Burgerservicenummer en de foto afschermen. Verzekeraars kunnen ook algemeen geaccepteerde identificatiemethoden gebruiken ter vaststelling van de identiteit van een Betrokkene, zoals het IDIN.

[8] Zie Rb. Gelderland, 1 nov. 2016, r.o.v. 2.11, ECLI:NL:RBGEL:2016:6508.

*Artikel 6.3.1.*

De Betrokkene kan de Verzekeraar verzoeken de Persoonsgegevens te verbeteren, aan te vullen, te verwijderen of de Verwerking te beperken indien deze feitelijk onjuist zijn, voor het doel of de doeleinden van de Verwerking onvolledig zijn of niet ter zake dienend dan wel anderszins in strijd met een wettelijk voorschrift worden verwerkt. Bij het beperken betreft het situaties waarbij de Persoonsgegevens niet verwijderd kunnen worden omdat ze bijvoorbeeld mogelijk in een procedure gebruikt moeten worden. In dat geval dienen passende maatregelen te worden genomen om ander gebruik te voorkomen. Indien een Verzekeraar heeft voldaan aan een verzoek om gegevens te verbeteren, aan te vullen, te verwijderen of de Verwerking te beperken, dan is hij verplicht Derden die eerder kennis hebben genomen van de betreffende Persoonsgegevens eveneens op de hoogte te brengen van de aangebrachte wijzigingen, tenzij dit onmogelijk is of een onevenredige inspanning kost.

*Artikel 6.3.2.*

De Betrokkene heeft het recht om bezwaar aan te tekenen tegen Verwerkingen van Persoonsgegevens indien de rechtsgrond van de Verwerking gelegen is in de behartiging van het gerechtvaardigde belang van de Verwerkingsverantwoordelijke. De Betrokkene kan dan op grond van zijn specifieke omstandigheden verzoeken om de Verwerking van zijn Persoonsgegevens te beëindigen. De Verwerkingsverantwoordelijke dient in dat concrete geval de Verwerking te heroverwegen en zijn belang af te wegen tegen het (bijzondere) belang van de Betrokkene. Ook als Persoonsgegevens vanwege wetenschappelijke, historische of statistische doeleinden worden verwerkt, heeft de Betrokkene het recht om met zijn specifieke situatie verband houdende redenen bezwaar te maken tegen de verwerking van hem betreffende persoonsgegevens.

Als een Betrokkene bezwaar aantekent tegen Verwerkingen voor marketingdoeleinden, beëindigen Verzekeraars de Verwerking onmiddellijk.

*Artikel 6.3.3.*

De Verwerkingsverantwoordelijke moet op grond van geldende wet- en regelgeving zorgdragen voor een deugdelijke vaststelling van de identiteit om te verzekeren dat de juiste persoon toegang krijgt tot de eigen Persoonsgegevens. De Verzekeraar kan vragen een kopie bij te sluiten van paspoort of rijbewijs om de handtekeningen te kunnen vergelijken, eventueel met reeds aanwezige handtekeningen. De Betrokkene mag het Burgerservicenummer en de foto afschermen. Verzekeraars kunnen ook algemeen geaccepteerde identificatiemethoden gebruiken ter vaststelling van de identiteit van een Betrokkene, zoals het IDIN.

*Artikel 6.4.1.*

Dit artikel geeft uitdrukking aan het recht op dataportabiliteit uit de AVG. In de verzekeringsbranche zal dit recht op het verhuizen van Persoonsgegevens primair gericht zijn op het afsluiten van een verzekering bij een andere Verzekeraar. Daarnaast vereist de AVG dat Persoonsgegevens ook kunnen verhuizen naar andere dienstverleners of de Betrokkene. Dit zijn namelijk Persoonsgegevens die door de Betrokkene worden gegenereerd gedurende het afnemen van de verzekering. Dataportabiliteit ziet niet op profielen, kredietscores en informatie die tot stand komt door analyses van de Verzekeraar. Persoonsgegevens die op andere basis dan toestemming en het aangaan of uitvoeren van de verzekering worden verwerkt, bijvoorbeeld voor het waarborgen van de integriteit en veiligheid van de sector en ter voorkoming van mogelijke fraude, vallen buiten de reikwijdte van deze bepaling.

*Artikel 6.4.2.*

De ontvangende Verwerkingsverantwoordelijke zal moeten beoordelen of de versturende Verzekeraar de juiste Persoonsgegevens heeft verzonden en of het ontvangen gegevensbestand niet bovenmatig is.

*Artikel 6.4.3.*

De Verwerkingsverantwoordelijke moet op grond van geldende wet- en regelgeving zorgdragen voor een deugdelijke vaststelling van de identiteit om te verzekeren dat de juiste persoon toegang krijgt tot de eigen Persoonsgegevens. De Verzekeraar kan vragen een kopie bij te sluiten van paspoort of rijbewijs om de handtekeningen te kunnen vergelijken, eventueel met reeds aanwezige handtekeningen. De Betrokkene mag het Burgerservicenummer en de foto afschermen. Verzekeraars kunnen ook algemeen geaccepteerde identificatiemethoden gebruiken ter vaststelling van de identiteit van een Betrokkene, zoals het IDIN.

## 11.7 Afdeling 7

*Artikel 7.1.1.*

Het opslaan op of toegang krijgen tot informatie in de randapparatuur van de Betrokkene is aan wettelijke regels onderworpen. Met Betrokkene wordt hier bedoeld de gebruiker (natuurlijke of rechtspersoon) die in de zin van de Telecommunicatiewet gebruikmaakt van of verzoekt om een openbare elektronische communicatiedienst. Uitgangspunt van de Telecommunicatiewet is dat het niet is toegestaan zonder medeweten en geïnformeerde toestemming van de Betrokkene persoonlijke informatie van bijvoorbeeld een computer of smartphone van de Betrokkene te lezen of te kopiëren. Uitzonderingen op deze regel zijn er ook. Zo is het toegestaan om technisch noodzakelijke cookies en cookies die nauwelijks gevolgen hebben voor de privacy van de Betrokkene te plaatsen of te lezen. Worden bij het opslaan op of toegang krijgen tot informatie in de randapparatuur van de gebruiker Persoonsgegevens verwerkt, dan gelden naast het bepaalde in de Telecommunicatiewet onverkort de regels van de geldende privacywetgeving.

Technologie op het gebied van het gebruik van cookies wijzigt snel. Niet uitgesloten is dat gedurende de looptijd van deze Gedragscode (technische) ontwikkelingen zorgen voor aanpassingen in de regelgeving over cookies. Verzekeraars dragen er zorg voor dat zij op de hoogte blijven van en zich conformeren aan deze wijzigingen.

Verzekeraars verstrekken op transparante wijze en in begrijpelijke taal informatie over de doeleinden van de verzameling van de gegevens op de randapparatuur van de Betrokkene. Voor ieder doeleinde specificeren Verzekeraars de categorieën gegevens, de bewaartermijn, de grondslag voor de Verwerking van Persoonsgegevens en de rechten van de Betrokkene in overeenstemming met artikel 6 van de Gedragscode. De Betrokkene ontvangt een heldere notificatie over het verzamelen van gegevens via randapparatuur met een directe link naar het in deze bepaling genoemde beleid.

*Artikel 7.2.1.*

Verzekeraars hechten aan een zorgvuldige beveiliging van Persoonsgegevens. Iedere Verzekeraar ontwikkelt een beveiligingsbeleid, waarin concreet wordt aangegeven welke organisatorische en technische maatregelen zijn genomen om Persoonsgegevens te beschermen tegen ongeautoriseerde toegang. Bij het vaststellen van het passend beveiligingsniveau wordt rekening gehouden met de stand van de techniek, de kosten van de tenuitvoerlegging, de risico's die de Verwerking met zich meebrengt en de aard van de te beschermen Persoonsgegevens. Daarbij

volgen Verzekeraars de Richtsnoeren Beveiliging van Persoonsgegevens van de AP en het Toetsingskader Informatiebeveiliging van DNB. Periodieke audits en kwaliteitscontroles vormen ook een onderdeel van het beveiligingsbeleid. Verzekeraars dragen zorg voor de naleving van dit beleid, volgens de methodiek Plan-do-check-act van de Richtsnoeren Beveiliging van Persoonsgegevens van de AP. Het Verbond heeft daarnaast een Handreiking Responsible Disclosure opgesteld om de beveiliging van Persoonsgegevens in de sector te stimuleren.

*Artikel 7.3.1.*

In overeenstemming met geldende wet- en regelgeving en de Beleidsregels Meldplicht Datalekken van de AP, melden Verzekeraars meldingsplichtige datalekken bij de AP. Verzekeraars zijn in privacywetgeving uitgesloten van de plicht datalekken direct aan Betrokkenen te melden, maar kunnen hiertoe wel verplicht zijn op grond van de Wft en regelgeving omtrent financieel toezicht. De relevante toezichthouder op de zorgplicht uit de Wft is DNB. Verzekeraars voeren regelmatig overleg met DNB in het kader van het financiële toezicht. Deze bepaling is kort, omdat de wetgeving en de Beleidsregels meldplicht datalekken van de AP de wettelijke vereisten duidelijk beschrijven.

*Artikel 7.4.1.*

Het woord 'gegevensbeschermingseffectbeoordeling' is de Nederlandse vertaling in geldende wet- en regelgeving voor de bekendere vakterm data protection impact assessment. De Europese toezichthouders hebben de wettelijke verplichtingen voor het uitvoeren van een DPIA nader uitgewerkt. Kort gezegd dienen Verzekeraars de effecten van een Verwerking te beoordelen als de Verwerking mogelijk een hoog risico inhoudt voor de persoonlijke levenssfeer van Betrokkenen. Dit kan het geval zijn bij systematische profilering (zoals de risicobeoordeling van aspirant-Verzekerden), grootschalige verwerkingen van Bijzondere Persoonsgegevens en bij verdere Verwerkingen van Persoonsgegevens, bijvoorbeeld voor marketingdoeleinden, als deze Persoonsgegevens oorspronkelijk zijn verzameld voor het aangaan van een verzekering (en niet na geldige uitdrukkelijke toestemming van een Betrokkene voor dit doeleinde). De Europese toezichthouders hebben in hun uitleg negen factoren opgesomd, die Verzekeraars zullen wegen in hun beslissing een DPIA uit te voeren.[9] De Autoriteit Persoonsgegevens heeft daarnaast een lijst opgesteld van soorten verwerkingen waarvoor het uitvoeren van een DPIA verplicht is.[10]

*Artikel 7.4.2.*

Zodra Verzekeraars een DPIA uitvoeren, winnen zij advies in van de FG als zij die hebben aangewezen. In de analyse nemen zij ten minste de aspecten mee, die in deze bepaling zijn opgesomd.

*Artikel 7.5.1.*

Verzekeraars stellen een nauwkeurig beleid op ten aanzien van het bewaren en archiveren van Persoonsgegevens. Gelet op het karakter van verzekeren en het belang van historische en statistische gegevens voor risico-inschatting en voor het afwikkelen van claims, zijn Verzekeraars vaak verplicht Persoonsgegevens langer te bewaren dan ondernemingen in andere sectoren. Steeds dienen Verzekeraars zich af te vragen of er redenen zijn op grond waarvan de Persoonsgegevens vastgelegd moeten blijven. Persoonsgegevens worden niet langer bewaard dan noodzakelijk is voor de verwerkelijking van de doeleinden waarvoor de gegevens zijn verzameld of vervolgens verwerkt.

[9] Deze negen factoren zijn te vinden op: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/data-protection-impact-assessment-dpia#in-welke-gevallen-moet-ik-een-dpia-uitvoeren-5879
[10] Staatscourant van 27 november 2019, nr. 64418: https://zoek.officielebekendmakingen.nl/stcrt-2019-64418.pdf

Voorbeelden van bewaardoelstellingen zijn het voldoen aan wettelijke bewaarverplichtingen, het kunnen leveren van bewijs in geval van geschillen en het kunnen beschikken over gegevens voor het verrichten van onderzoek. Een Verzekeraar stelt beleid op met betrekking tot de bewaartermijnen van de Persoonsgegevens, de verwijdering van de Persoonsgegevens en het eventueel overbrengen van deze Persoonsgegevens naar een archiefbestemming. In het laatste geval zullen de Persoonsgegevens slechts worden gebruikt voor het archiefbeheer, het behandelen van geschillen en het doen van wetenschappelijk, statistisch of historisch onderzoek.

*Artikel 7.6.1.*

Met pseudonimisering vervangen Verzekeraars direct identificerende gegevens van een Betrokkene door andere identificatiemiddelen, zoals een IP-adres, gebruikersnaam of een klantnummer. Door bijvoorbeeld een naam van een Betrokkene te vervangen voor een nietszeggend klantnummer, bemoeilijken Verzekeraars re-identificatie van de Betrokkene door het personeel van de Verzekeraar, of cybercriminelen na een cyberaanval. Gepseudonimiseerde data zijn nog altijd persoonsgegevens, omdat een pseudoniem een natuurlijke persoon indirect kan identificeren. Door pseudonimisering beschermen Verzekeraars de privacy van de Betrokkene en om die reden mogen Verzekeraars een adequaat gepseudonimiseerde dataset bijvoorbeeld gebruiken voor het maken van historische, statistische of wetenschappelijke analyses, in overeenstemming met artikel 4.3 van de Gedragscode. Pseudonimisering is ook een belangrijk instrument voor de beveiliging van gegevensbestanden. De Verzekeraar dient de originele dataset apart te bewaren van de gepseudonimiseerde dataset, de toegang tot de originele dataset zowel technisch (via bijvoorbeeld versleuteling) als organisatorisch (alleen een beperkt aantal personeelsleden) te beperken.

*Artikel 7.7.*

Verzekeraars kunnen voor de in deze bepaling genoemde doeleinden gebruikmaken van cameratoezicht. Zo geldt dat cameratoezicht geoorloofd is wanneer dat noodzakelijk is voor de beveiliging van een Verzekeraar of haar relaties en medewerkers, voor de opsporing van strafbare feiten of vaststellen van overtreding van (bedrijfs)regels en ter ondersteuning van juridische procedures. Verder geldt dat opnamen selectief moeten plaatsvinden, dat de gegevens niet langer bewaard worden dan noodzakelijk en dienen de noodzakelijke organisatorische en technische maatregelen te worden genomen ter bescherming van de Persoonsgegevens. Indien de Betrokkene daarom vraagt, zal te allen tijde nadere informatie worden verschaft. Onder inzage kan in voorkomende gevallen ook worden verstaan het verzoeken om inzage in hier bedoelde beelden. Wel kan in dat geval van een verzoeker worden verlangd dat hij dag en tijdstip van het contact aangeeft. Indien de beelden ook informatie over andere natuurlijke personen bevatten worden die beelden niet aan de Betrokkene verstrekt.

*Artikel 7.8.1.*

Verzekeraars kunnen de Verwerking van Persoonsgegevens uitbesteden aan Verwerkers. Verzekeraars maken bijvoorbeeld veelvuldig gebruik van IT-dienstverleners voor onderhoud en supportfuncties. Deze IT-dienstverleners dienen te worden beschouwd als Verwerker, zodra zij geen zelfstandige zeggenschap hebben over de Persoonsgegevens die in het kader van de dienstverlening aan de IT-dienstverlener ter beschikking worden gesteld. De Verzekeraar moet in dat geval afspraken maken met de Verwerker, die enerzijds voortvloeien uit geldende privacywet- en regelgeving, anderzijds uit wetgeving op het gebied van het financieel toezicht. Een belangrijk onderdeel van de afspraken betreft de beveiliging van de Verwerking van de Persoonsgegevens. Ook bij uitbesteding blijft de Verzekeraar in de regel de Verwerkingsverantwoordelijke. Toch zijn er

ook situaties denkbaar waarin beide partijen Verwerkingsverantwoordelijke blijven. Bij pensioenovereenkomsten die werkgever aangaan ten behoeve van hun werknemers, zijn de werkgever en de Verzekeraar (en in voorkomende gevallen de tussenpersoon) zelfstandig Verwerkingsverantwoordelijke.

Regelgeving op het gebied van het financieel toezicht stelt eveneens eisen aan de kwaliteit van de gegevensverwerking. Financieel toezichthouders zoals DNB houden toezicht op de kwaliteit van de uitbesteding. Als de Verwerker buiten de Europese Economische Ruimte (EER) is gevestigd, moet de uitbestedende Verzekeraar bovendien voldoen aan de aanvullende eisen voor de doorgifte van Persoonsgegevens in overeenstemming met artikel 7.9 van de Gedragscode. Als de Verwerker gebruikmaakt van cloud-technologie zal de Verzekeraar in kaart brengen waar de Persoonsgegevens uiteindelijk worden verwerkt. Hij zal dan ook met de Verwerker afspraken maken die hem zekerheid geven met betrekking tot de naleving van de contracten en het overeengekomen niveau van beveiliging. Die verplichting geldt ook naar eventuele sub-verwerkers, oftewel de leveranciers aan wie de Verwerker onderdelen van de dienstverlening uitbesteedt. Deze afspraken legt de Verzekeraar vast in een Verwerkersovereenkomst, in aanvulling op de categorieën die zijn genoemd in artikel 28 AVG.

*Artikel 7.9.1.*

In de regel verwerken Verzekeraars Persoonsgegevens binnen de Europese Economische Ruimte (EER) en is op die verwerkingen de AVG integraal van toepassing. Soms verwerken Verzekeraars Persoonsgegevens van de Betrokkene buiten de EER, bijvoorbeeld omdat een Verwerker of een Groepsmaatschappij buiten de Europese Economische Ruimte van de Persoonsgegevens gevestigd is. In zulke gevallen treffen Verzekeraars de volgens de wet vereiste waarborgen om een adequaat niveau van bescherming te garanderen. De gelaagdheid van de regelgeving op het gebied van doorgifte van Persoonsgegevens naar landen buiten de EER ligt voor Verzekeraars anders dan voor andere Verwerkingsverantwoordelijken. Vaak is de Verwerking buiten de EER noodzakelijk voor onder meer de uitvoering van een overeenkomst tussen een Betrokkene en de Verantwoordelijke of noodzakelijk voor de sluiting of uitvoering van een in het belang van de Betrokkene te sluiten overeenkomst. Het kan daarbij bijvoorbeeld gaan om herverzekering of om gegevensuitwisseling in verband met schade of ongeluk in het buitenland. Ook kan doorgifte plaatsvinden indien daartoe ondubbelzinnige toestemming is verkregen van de Betrokkene of wanneer het noodzakelijk is in verband met een zwaarwegend algemeen belang. Als vuistregel hanteren de Verzekeraars dat de Persoonsgegevens van de Betrokkene buiten Europa eenzelfde niveau van bescherming genieten als bij Verwering door de Verantwoordelijke zelf, binnen Europa.

*Artikel 7.10.1.*

Verwerking van persoonsgegevens binnen een Groep is toegestaan wanneer aan de voorwaarden van de Gedragscode wordt voldaan. Voor de Betrokkene moet steeds duidelijk zijn welke maatschappijen tot de Groep behoren.

## 11.8 Afdeling 8

De beginselen en bepalingen uit de Gedragscode, zoals het doelbindingsbeginsel, transparantiebeginsel en de rechten van de Betrokkenen, moeten in bijzondere gevallen wijken als hiertoe een dringende noodzaak bestaat mits de AVG zich hier niet tegen verzet. Deze Dringende redenen staan opgesomd in artikel 8.1.1. Hiervan is bijvoorbeeld sprake als een Verzekeraar onderworpen is aan onderzoek van een bevoegde toezichthouder of de fiscus. Ook bij incidentonderzoek door de Verzekeraar van een Betrokkene kan het belang van het onderzoek

zwaarder wegen dan de privacybelangen van de Betrokkene, nu het vroeg informeren van de Betrokkene een incidentonderzoek kan frustreren. Verzekeraars passen de uitzonderingsgrond van de Dringende Reden restrictief toe. Steeds geldt dat de noodzaak af te wijken van de algemene bepalingen uit de Gedragscode evident zwaarder weegt dan de rechten en vrijheden van de Betrokkene en de afwijking past binnen het kader van de AVG.

## 11.9 Afdeling 9

*Artikel 9.1.1.*

Verzekeraars stellen in beginsel binnen hun organisatie een Functionaris Gegevensbescherming (FG) aan. De FG adviseert de Verzekeraar over de opzet en de inhoud van het privacybeleid en de Verwerking van Persoonsgegevens in de bedrijfsvoering. De Functionaris Gegevensbescherming kan in dienst zijn bij de Verzekeraar of extern worden ingehuurd, zo lang de FG onafhankelijk opereert en geen aanwijzingen krijgt van de Verzekeraar in verband met de uitoefening van zijn taak. De FG ondervindt geen nadeel van de uitoefening van zijn taak en geniet bescherming tegen ontslag of einde van de overeenkomst tot opdracht wegens verschil van inzicht. De FG beschikt over de vereiste kennis en capaciteiten om zijn taak naar behoren te vervullen, in het bijzonder relevante werkervaring op het gebied van de bescherming van Persoonsgegevens. De FG heeft toegang tot alle systemen waar mogelijk Persoonsgegevens worden verwerkt. De FG kan ook het eerste aanspreekpunt zijn voor de Betrokkene bij klachten over de naleving van de Gedragscode, die in overeenstemming met artikel 9.3.1. van de Gedragscode kunnen worden ingediend.

Een verzekeraar kan afzien van het aanstellen van een FG indien dienstverlening of productaanbod daar aanleiding toe geeft. Hierbij geldt het principe ‘pas toe of leg uit’. Het afwijken van de verplichting vergt een zorgvuldige belangenafweging, een en ander in overeenstemming met de AVG en de relevante opinies van de (nationale) privacytoezichthouder. Het is van belang in de afweging rekening te houden met het feit dat een verzekeraar die medische gegevens verwerkt al snel onder de verplichting valt om een FG aan te stellen.

*Artikel 9.2.1.*

Verzekeraars dragen zorg voor de naleving van deze Gedragscode en geldende wet- en regelgeving. Verzekeraars nemen de volgende concrete maatregelen om de naleving te waarborgen:

(a) De Verzekeraar toetst periodiek, bij voorkeur jaarlijks, via zelfevaluatie de naleving.

(b) Het management van de Verzekeraar neemt verantwoordelijkheid voor de naleving.

(c) De met toezicht belaste afdeling (bijvoorbeeld de compliance-afdeling of de FG) draagt zorg voor de naleving.

Waar de DPIA de Verwerking van Persoonsgegevens toetst voor specifieke Verwerkingen, kunnen Verzekeraars ook interne onderzoeken (zoals audits) uitvoeren die de naleving in kaart brengen. Afhankelijk van de uitkomsten hiervan en de aard en omvang van de afzonderlijke Verwerkingen van Persoonsgegevens stellen zulke interne onderzoeken vast bij welke onderdelen aanvullend onderzoek dient plaats te vinden.

Ter bevordering van de naleving is een Verzekeraar daarnaast gehouden een intern privacybeleid op te stellen en te implementeren. In dit beleid wordt aangegeven op welke wijze Persoonsgegevens dienen te worden verwerkt. De instructies betreffen in ieder geval die onderwerpen waarvan het interne onderzoek vaststelt dat nader beleid wenselijk is. In de praktijk betreft het documentaties als

security manuals waarin de technische en organisatorische maatregelen ter beveiliging van Persoonsgegevens staan beschreven.

*Artikel 9.3.1.*

Iedere Verzekeraar kent een interne procedure voor klachtenafhandeling. Voor de beantwoording van klachten geldt de termijn in geldende wet- en regelgeving. De gehele procedure wordt hieronder verder toegelicht.

*Artikel 9.3.2.*

Het Verbond van Verzekeraars is aangesloten bij het Klachteninstituut Financiële Dienstverlening (Kifid). Dit onafhankelijke instituut is bedoeld om één loket te bieden voor beslechting van conflicten met financiële instellingen. De binnen Kifid werkzame Ombudsman en Geschillencommissie bieden een alternatief voor de gang naar de rechter. In een relatief kort tijdsbestek wordt in overleg met de betrokken dienstverlener getracht een oplossing te vinden of wordt geoordeeld over de kwestie.

Indien de Betrokkene een klacht heeft ingediend bij de Verzekeraar en de klacht niet of niet naar tevredenheid wordt afgehandeld, kan de Betrokkene binnen drie maanden na deze afhandeling het geschil voorleggen aan Kifid. Als het geschil betrekking heeft op het recht op inzage/correctie en binnen zes weken na de beslissing van de interne geschillenprocedure van de Verzekeraar wordt ingediend bij Kifid, wordt op grond van geldende wet- en regelgeving de periode van zes weken, waarbinnen de Betrokkene het recht heeft de zaak aan de AP of – via een verzoekschriftprocedure – de rechtbank voor te leggen, opgeschort (te rekenen vanaf het moment van indienen tot de beëindiging van de procedure bij Kifid). Indien de Betrokkene een geschil pas na het verstrijken van de periode van zes weken voorlegt aan Kifid, kan de Betrokkene niet langer gebruikmaken van de procedure uit geldende privacywet- en regelgeving.

Een Betrokkene kan ook kiezen voorbij te gaan aan de interne geschillenbeslechting van de Verzekeraar. De Betrokkene kan een geschil dus direct voorleggen aan de AP of aan de bevoegde rechter. Daarmee vervalt zijn recht om alsnog de interne geschillenprocedure van de Verzekeraar, en daaropvolgend Kifid in te schakelen.

Voor meer informatie over het Kifid verwijzen wij naar de volgende website: www.kifid.nl of Klachteninstituut Financiële Dienstverlening, Postbus 93257, 2509 AG Den Haag. Bij vragen over de Gedragscode kan tevens contact worden opgenomen met het Verbond van Verzekeraars, postbus 93450, 2509 AL Den Haag, telefoon 070 - 333 8500 of per e-mail: Gedragscode_Privacy@verzekeraars.nl.

## 11.10 Afdeling 10

De begrippen in deze Gedragscode sluiten aan bij de begrippen uit geldende wet- en regelgeving. In aanvulling op de in de Gedragscode opgenomen definities, zijn de definities uit geldende wet- en regelgeving onverminderd van toepassing bij de uitleg van de Gedragscode. Sommige begrippen zijn specifiek aan het verzekeringsbedrijf en zijn niet gedefinieerd in de wet, zoals Medisch Adviseur, Veiligheidszaken en Verzekerde. Voor een goed begrip van deze Gedragscode zijn enkele centrale begrippen uit afdeling 10 hieronder verder uitgewerkt.

*Betrokkene*

De Betrokkene is degene op wie een Persoonsgegeven betrekking heeft. Vaak is de Betrokkene dezelfde persoon als de verzekeringnemer, met wie de Verzekeraar een verzekering heeft gesloten. Toch zijn er ook veel situaties te bedenken waarin dit niet het geval is. Het alleen opnemen van het begrip Verzekerde in deze Gedragscode zou dan ook niet goed uitpakken. Denk aan de situatie waarin de werkgever namens alle werknemers een werkgeversverzekering afsluit. De werkgever is dan de klant van de Verzekeraar, maar de Persoonsgegevens van werknemers dienen ook te worden beschermd. Daarnaast treft de Verwerking van Persoonsgegevens in het kader van een verzekering vaak meerdere personen. Denk aan (aspirant-)Verzekerden, begunstigden, meeverzekerden (bijvoorbeeld gezinsleden) en personen die een Verzekerde aansprakelijk stellen. Door het bredere begrip Betrokkene te hanteren, brengt deze Gedragscode tot uitdrukking dat Verzekeraars ook de Persoonsgegevens van deze bredere kring beschermen. De Betrokkene is dus een flexibel begrip en kan, afhankelijk van de feiten en omstandigheden van het geval, omvatten:

(a) personen met wie een verzekering is afgesloten (de verzekeringnemer) of degenen die onder de overeenkomst verzekerd zijn (Verzekerden);

(b) personen met wie in het verleden een verzekering is afgesloten (inclusief Verzekerden) en van wie de Persoonsgegevens nog steeds moeten worden verwerkt;

(c) personen die worden benaderd om een verzekering aan te gaan;

(d) personen die zelf een Verzekeraar benaderen door het opvragen van informatie of het aanvragen van een offerte;

(e) personen van wie een Verzekeraar op basis van een wettelijk voorschrift (bijvoorbeeld de toestemming van de echtgenoot ex artikel 88 boek 1 BW) of vanwege geldende verjaringstermijnen Persoonsgegevens dient te verwerken;

(f) personen die betrokken zijn bij een Gebeurtenis (bijvoorbeeld de benadeelde ingeval van schade);

(g) personen van wie een Verzekeraar in verband met contractuele of wettelijke verplichtingen Persoonsgegevens dient te verwerken;

(h) een bezoeker van het bedrijfspand.

*Verwerker*

De Verwerker verwerkt Persoonsgegevens ten behoeve van de opdrachtgever, de Verwerkingsverantwoordelijke. De Verwerker heeft geen zeggenschap over de Verwerking, maar volgt slechts de instructies op van de Verwerkingsverantwoordelijke. Verzekeraars hebben de opslag van Persoonsgegevens bijvoorbeeld in belangrijke mate belegd bij cloudproviders. Deze aanbieders van cloud computing diensten hebben meestal geen zelfstandige bevoegdheid om de aan hun toevertrouwde Persoonsgegevens voor andere doeleinden te gebruiken. Cloud providers zijn dan ook meestal Verwerker.

*Verwerkingsverantwoordelijke*

De Verwerkingsverantwoordelijke is de rechtspersoon die het doel en de middelen van de Verwerking vaststelt en formeel bevoegd is om beslissingen te nemen over de Verwerking van Persoonsgegevens. De Verwerkingsverantwoordelijke is ook de rechtspersoon die aansprakelijk is als geldende wet- en regelgeving niet of onjuist wordt nageleefd. In beginsel treedt de Verzekeraar, met wie de Betrokkene een verzekering sluit, op als Verwerkingsverantwoordelijke.

# 12 Het Verbond van Verzekeraars

Het Verbond van Verzekeraars is de belangenvereniging van schade- en levensverzekeraars in Nederland. Ook bedrijven die zich toeleggen op banksparen voor de oude dag en premiepensioeninstellingen zijn lid. De leden van het Verbond vertegenwoordigen samen meer dan 95 procent van de verzekeringsmarkt. Het Verbond treedt namens de aangesloten verzekeraars op als gesprekspartner voor de politiek, media en andere relevante partijen over onderwerpen die verzekeraars raken.

Het Verbond heeft als brancheorganisatie de volgende vier hoofddoelstellingen:

1. Vertegenwoordigen van de leden

Het Verbond is in de eerste plaats vertegenwoordiger van particuliere verzekeraars en bedrijven die zich toeleggen op banksparen en premiepensioeninstellingen. Namens de leden treedt het Verbond op als gesprekspartner voor de politiek, overheid en andere organisaties (nationaal en internationaal). Samen met die andere partijen zoekt het Verbond naar raakvlakken om oplossingen voor vraagstukken te vinden.

2. Bevorderen van het imago van de verzekeringstak

Bij de bevordering en de instandhouding van de goede naam van het verzekeringsbedrijf in Nederland, speelt communicatie een belangrijke rol. Het Verbond coördineert de pr van de gehele bedrijfstak, verwoordt het beleid naar de media en speelt in op ontwikkelingen.

3. Bieden van een platform

Om de rol als vertegenwoordiger van de sector te kunnen uitvoeren, is uiteraard draagvlak nodig. Het Verbond creëert dat draagvlak onder meer door bijeenkomsten voor representanten van de bedrijfstak te organiseren. De vereniging houdt regelmatig themadagen voor de leden over actuele onderwerpen die de aandacht van verzekeraars vragen. Tijdens de ledenvergaderingen wordt het algemene beleid besproken. Al deze bijeenkomsten hebben ook een sociale functie: leden kunnen elkaar ontmoeten.

4. Dienstverlening

Belangenbehartiging betekent ook dat je er moet zijn voor je leden. Door de vertegenwoordigende rol is het Verbond op de hoogte van relevante ontwikkelingen en fungeert daarom als kenniscentrum voor zijn leden. De leden worden via diverse kanalen op de hoogte gehouden. Omdat het Verbond de collectieve belangen die de gehele bedrijfstak aangaan coördineert, vervult het daarmee een adviserende functie voor het te voeren beleid. Meer weten over de vormen van dienstverlening die we voor leden te bieden hebben? Bezoek onze website: www.verzekeraars.nl.