Rabobank

Gedragscode Verwerking Persoonsgegevens

Financiële Instellingen

rapportnummer: 2010/bl/13170/mblom d.d. 16 maart 2010

1. Overwegingen

1.1 Banken en verzekeraars (hierna: Financiële instellingen) verwerken in het kader van hun bedrijfsvoering Persoonsgegevens en vinden het belangrijk dat met deze Persoonsgegevens zorgvuldig wordt omgegaan en dat deze vertrouwelijk worden behandeld.

1.2 De Wet bescherming persoonsgegevens (hierna: WBP) biedt waarborgen voor de bescherming van de persoonlijke levenssfeer van natuurlijke personen met betrekking tot het verwerken van Persoonsgegevens.

1.3 De Nederlandse Vereniging van Banken (hierna: de NVB) en het Verbond van Verzekeraars (hierna: het Verbond) hebben in lijn met het bepaalde in de WBP, de Gedragscode Verwerking Persoonsgegevens Financiële Instellingen (hierna: Gedragscode) opgesteld, waarvoor het College bescherming persoonsgegevens (hierna: CBP) op 13 april 2010 een goedkeurende verklaring heeft afgegeven. Deze verklaring is op 26 april 2010 gepubliceerd in de Staatscourant [no. 6360]. Het CBP heeft verklaard dat de Gedragscode, gelet op de bijzondere kenmerken van de sector, een juiste uitwerking vormt van de WBP en andere wettelijke bepalingen betreffende de Verwerking van Persoonsgegevens. De goedkeuring geldt voor een periode van vijf jaar. Deze Gedragscode vervangt de voorgaande Gedragscode Verwerking Persoonsgegevens Financiële Instellingen.

1.4 De Gedragscode heeft tot doel:
a. regels te stellen aan Financiële instellingen voor het Verwerken van Persoonsgegevens;
b. informatie te verschaffen aan personen van wie Persoonsgegevens door Financiële instellingen verwerkt (zullen) worden; en
c. bij te dragen aan de transparantie van de regels die de door de Financiële instellingen worden gehanteerd met betrekking tot het Verwerken van Persoonsgegevens.

2. Begripsbepaling

In deze Gedragscode wordt verstaan onder:

a. Bestand: elk gestructureerd geheel van Persoonsgegevens dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen.
b. Betrokkene: degene op wie een Persoonsgegeven betrekking heeft.
c. Bewerker: degene die ten behoeve van de Verantwoordelijke Persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen.
d. Bijzondere persoonsgegevens: Persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging, evenals strafrechtelijke Persoonsgegevens en Persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.
e. CBP: het College bescherming persoonsgegevens als bedoeld in artikel 51 WBP.
f. Cliënt: de Betrokkene met wie een Financiële instelling; (i) in een rechtsverhouding staat; of (ii) in een rechtsverhouding heeft gestaan, (iii) overweegt een rechtsverhouding aan te gaan; of (iv) die te kennen heeft gegeven te overwegen een rechtsverhouding met een Financiële instelling aan te gaan of (v) personen van wie een Financiële instelling krachtens wettelijk voorschrift of met het oog op geldende verjaringstermijnen Persoonsgegevens dient te verwerken dan wel (vi) personen van wie een Financiële instelling Persoonsgegevens dient te verwerken in verband met contractuele of wettelijke verplichtingen jegens een Cliënt, Verzekerde of

derde.
g. Derde: eenieder, niet zijnde de Betrokkene, de Verantwoordelijke, de Bewerker, of enig persoon, die onder rechtstreeks gezag van de Verantwoordelijke of de Bewerker gemachtigd is om Persoonsgegevens te verwerken.
h. Direct Marketing: het overbrengen van informatie door een Financiële instelling aan een Betrokkene ter bevordering van de totstandkoming van een overeenkomst.
i. Financiële instelling: een bank en/of verzekeraar.
j. Functionaris: de functionaris voor de gegevensbescherming (FG) als bedoeld in artikel 62 WBP.
k. Gebeurtenissenadministratie: Verwerking van Persoonsgegevens die van belang kunnen zijn voor de veiligheid en integriteit van de Financiële instelling en om die reden speciale aandacht behoeven.
l. Gedragscode: de Gedragscode Verwerking Persoonsgegevens Financiële instellingen.
m. Groep: de economische eenheid waarin rechtspersonen en vennootschappen organisatorisch zijn verbonden en waartoe een Financiële instelling behoort.
n. Medisch adviseur: de arts die als verantwoordelijke optreedt voor de Verwerking van Persoonsgegevens omtrent iemands gezondheid, die noodzakelijk is om een onafhankelijk deskundig advies te kunnen geven, terzake de beoordeling van de gezondheidstoestand (i) van de Verzekerde, (ii) van personen die een claim hebben ingediend bij een Verzekerde of (iii) van de te verzekeren persoon dan wel (iv) terzake de beoordeling van het medisch handelen van een Verzekerde, aan de afdelingen van het verzekeringsbedrijf die tot taak hebben omtrent een aanvraag of claim de beslissing te nemen.
o. Persoonsgegeven: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.
p. Protocol: het Protocol Incidentenwaarschuwingssysteem Financiële Instellingen.
q. Veiligheidszaken: de afdeling(en) of de persoon die binnen een Financiële instelling verantwoordelijk is (zijn) voor de Verwerking van Persoonsgegevens in het kader van het waarborgen van de veiligheid en integriteit.
r. Verantwoordelijke: de rechtspersoon die, alleen of tezamen met anderen, het doel en de middelen voor de Verwerking van Persoonsgegevens vaststelt of de rechtspersoon die binnen een Groep hiertoe is aangewezen.
s. Verzekerde: een natuurlijke of rechtspersoon die met een Financiële instelling een verzekering heeft gesloten en andere personen die overeenkomstig de polisvoorwaarden als rechthebbende op schadevergoeding en/of uitkering zijn aan te merken.
t. Verwerking van Persoonsgegevens: elke handeling of elk geheel van handelingen met betrekking tot Persoonsgegevens, waaronder verzamelen, vastleggen, ordenen, bewaren, wijzigen, raadplegen, gebruiken, verstrekken en vernietigen.
u. WBP: Wet bescherming persoonsgegevens.

3. De reikwijdte van de Gedragscode

3.1 De sector

3.1 .1 De Gedragscode is van toepassing op Financiële instellingen die; (i) lid zijn van de NVB; (ii) aangesloten zijn bij Rabobank Nederland; of (iii) lid zijn van het Verbond.

3.2 Toepassing

3.2 .1 De Gedragscode is in de eerste plaats van toepassing op de (gedeeltelijk) geautomatiseerde Verwerking van Persoonsgegevens door een Financiële instelling in het kader van de bedrijfsvoering. De Gedragscode is ook van toepassing op de handmatige Verwerking van Persoonsgegevens door een Financiële instelling in het kader van de bedrijfsvoering, op voorwaarde dat de Persoonsgegevens zijn opgenomen in een Bestand of bestemd zijn om

daarin te worden opgenomen.

3.2.2 Verwerkingen van Persoonsgegevens in verband met: (i) incidentenregisters door Veiligheidszaken; (ii) het Externe Verwijzingsregister (hierna: EVR); of (iii) in de hoedanigheid van de Financiële instelling als werkgever vallen buiten de reikwijdte van deze Gedragscode.

3.2.3 Indien de Gedragscode Verwerking Persoonsgegevens Zorgverzekeraars is goedgekeurd, heeft voor zorgverzekeraars, die tevens lid zijn van Zorgverzekeraars Nederland, bij discrepantie de Gedragscode Verwerking Persoonsgegevens Zorgverzekeraars voorrang.

4. Beginselen van Verwerking van Persoonsgegevens

4.1 Persoonsgegevens worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt.

4.2 Persoonsgegevens worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden verkregen. In artikel 5 Gedragscode wordt dit nader bepaald.

4.3 Persoonsgegevens worden slechts verwerkt indien en voor zover is voldaan aan minimaal één van de volgende rechtmatige grondslagen:

a. de Betrokkene heeft voor de Verwerking van Persoonsgegevens zijn ondubbelzinnige toestemming verleend;
b. de Verwerking van Persoonsgegevens is noodzakelijk voor de uitvoering van een overeenkomst waarbij de Cliënt partij is, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de Cliënt en die noodzakelijk zijn voor het sluiten van een overeenkomst;
c. de Verwerking van Persoonsgegevens is noodzakelijk om een wettelijke verplichting na te komen waaraan de Financiële instelling onderworpen is;
d. de Verwerking van Persoonsgegevens is noodzakelijk ter vrijwaring van een vitaal belang van de Betrokkene;
e. de Verwerking van Persoonsgegevens is noodzakelijk voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt; of
f. de Verwerking van Persoonsgegevens is noodzakelijk voor de behartiging van het gerechtvaardigde belang van de Financiële instelling of van een Derde aan wie de Persoonsgegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de Betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert.

4.4 Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen.

4.5 Een Financiële instelling neemt maatregelen zodat Persoonsgegevens, gelet op de doeleinden waarvoor zij door de Financiële instelling worden verwerkt, accuraat, toereikend, ter zake dienend en niet bovenmatig zijn.

4.6.1 Persoonsgegevens worden verwijderd nadat de door de Financiële instelling vastgestelde bewaartermijnen zijn verstreken en kunnen worden overgebracht naar een archiefbestemming ten behoeve van het archiefbeheer, het behandelen van geschillen en het verrichten van (wetenschappelijk, statistisch of historisch) onderzoek.

4.6.2 Persoonsgegevens mogen langer worden bewaard dan bepaald in artikel 4.6.1 Gedragscode voor zover

ze voor historische, statistische of wetenschappelijke doeleinden worden bewaard, en de verantwoordelijke de nodige voorzieningen heeft getroffen ten einde te verzekeren dat de desbetreffende gegevens uitsluitend voor deze specifieke doeleinden worden gebruikt.

4.7 Indien Persoonsgegevens worden verzameld bij de Betrokkene, informeert de Verantwoordelijke de Betrokkene over zijn identiteit en de doeleinden van de Verwerking van Persoonsgegevens, tenzij de Verantwoordelijke op goede gronden mag aannemen dat de Betrokkene daarvan reeds op de hoogte is. Aan deze informatieplicht wordt voldaan vóór het moment van verkrijging.

4.8 Indien de Persoonsgegevens op een andere manier worden verkregen, informeert de Verantwoordelijke de Betrokkene over zijn identiteit en de doeleinden van de Verwerking van Persoonsgegevens op het moment van vastlegging of, wanneer de Persoonsgegevens bestemd zijn om te worden verstrekt aan een Derde, op het moment van eerste verstrekking. De verplichting geldt niet wanneer de Betrokkene reeds op de hoogte is, dan wel wanneer de mededeling aan Betrokkene onmogelijk blijkt of een onevenredige inspanning kost. In dat geval wordt de herkomst van de Persoonsgegevens vastgelegd. De verplichting geldt evenmin wanneer de vastlegging of de verstrekking bij of krachtens de wet is voorgeschreven.

4.9 Indien het, gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, nodig is uit oogpunt van het waarborgen van een behoorlijke en zorgvuldige Verwerking van Persoonsgegevens, zal in aanvulling op de informatie als aangegeven in 4.7 en 4.8 Gedragscode nadere informatie worden verstrekt aan de Betrokkene.

4.10 Een Financiële instelling kan in het kader van de bedrijfsvoering via het internet Persoonsgegevens van een Betrokkene, die een Financiële instelling via dit medium benadert, vastleggen en verder verwerken. Financiële instellingen zullen via een privacy statement op de betreffende website informatie beschikbaar stellen over het beleid met betrekking tot de door middel van het internet verkregen Persoonsgegevens. Het privacy statement bevat minimaal de informatie als bedoeld in artikel 4.7 Gedragscode.

4.11 Het doelbindingsbeginsel (artikel 4.4 Gedragscode) en de plicht tot het verstrekken van informatie (artikel 4.7, 4.8 en 4.9 Gedragscode) kan tevens door een Financiële instelling (in aanvulling op de uitzonderingen genoemd in artikel 4.7 en 4.8 Gedragscode) buiten toepassing worden gelaten als wordt voldaan aan het bepaalde in artikel 9 Gedragscode.

4.12 Financiële instellingen kunnen bij de Verwerking van Persoonsgegevens gebruik maken van een Bewerker. Indien gebruik wordt gemaakt van de diensten van een Bewerker zal met deze Bewerker een overeenkomst worden gesloten, waarin schriftelijk of in een andere, gelijkwaardige vorm onder meer wordt vastgelegd dat technische en organisatorische maatregelen ter beveiliging van die gegevens moeten worden genomen.

5. Doeleinden voor de Verwerking van Persoonsgegevens

5.1 Algemeen

5.1.1 Verwerking van Persoonsgegevens door Financiële instellingen vindt plaats, met inachtneming van de beginselen voor Verwerking van Persoonsgegevens ten behoeve van een efficiënte en effectieve bedrijfsvoering, in het bijzonder in het kader van het uitvoeren van de volgende activiteiten:

a. het beoordelen en accepteren van een Cliënt, het aangaan en uitvoeren van overeenkomsten met een Cliënt en het afwikkelen van het betalingsverkeer;
b. het verrichten van analyses van Persoonsgegevens ten behoeve van statistische en wetenschappelijke doeleinden;
c. het uitvoeren van (gerichte) marketingactiviteiten teneinde een relatie met een Betrokkene tot stand te brengen en/of met een Cliënt in stand te houden dan wel uit te breiden;
d. het waarborgen van de veiligheid en integriteit van de financiële sector, daaronder mede begrepen het onderkennen, voorkomen, onderzoeken en bestrijden van (pogingen tot) (strafbare of laakbare) gedragingen gericht tegen de branche waar een Financiële instelling deel van uitmaakt, de Groep waartoe een Financiële instelling behoort, de Financiële instelling zelf, haar Cliënten en medewerkers, alsmede het gebruik van en de deelname aan waarschuwingssystemen;
e. het voldoen aan wettelijke verplichtingen;
f. het beheren van de relatie met de Cliënt.

5.1.2 Een Financiële instelling verwerkt niet meer Persoonsgegevens dan strikt noodzakelijk is. Financiële instellingen stellen deze Persoonsgegevens binnen de Groep slechts beschikbaar aan medewerkers die daartoe bevoegd zijn.

5.1.3 Financiële instellingen zullen waar nodig hun specifieke activiteiten melden bij het CBP of, voor zover van toepassing, bij de eigen Functionaris.

5.2 Verwerking van Persoonsgegevens in het kader van het beoordelen en accepteren van Cliënten, het aangaan en uitvoeren van overeenkomsten met een Cliënt en het afwikkelen van het betalingsverkeer

5.2.1 In het kader van het beoordelen en accepteren van een Cliënt en het aangaan en uitvoeren van een overeenkomst met een Cliënt worden Persoonsgegevens (verzameld en) verwerkt. Voor zover het gaat om Persoonsgegevens betreffende iemands gezondheid en strafrechtelijke Persoonsgegevens zijn de bepalingen van artikel 6 Gedragscode van toepassing.

5.2.2 Financiële instellingen kunnen voor het beoordelen en accepteren van een Cliënt en het aangaan en uitvoeren van een overeenkomst met een Cliënt Persoonsgegevens verstrekken en onttrekken aan waarschuwingssystemen als bedoeld in artikel 5.5.2 Gedragscode.

5.2.3 Door een Financiële instelling worden in het kader van de normale afwikkeling van het betalingsverkeer Persoonsgegevens doorgegeven aan de wederpartij. Tevens worden, tenzij vooraf anders is overeengekomen, aanvullende Persoonsgegevens verstrekt aan de bij de verdere Verwerking van Persoonsgegevens betrokken partijen, voor zover deze redelijkerwijs noodzakelijk zijn voor verificatiedoeleinden of reconstructiedoeleinden.

5.3 Verwerking van Persoonsgegevens in het kader van analyses ten behoeve van historische, statistische en wetenschappelijke doeleinden

5.3.1 Verwerking van Persoonsgegevens voor historische, statistische of wetenschappelijke doeleinden wordt niet beschouwd als onverenigbaar met de doeleinden waarvoor de Persoonsgegevens eerder zijn verzameld.

De Financiële instelling treft de nodige voorzieningen om te verzekeren dat de verdere Verwerking van de Persoonsgegevens uitsluitend plaats heeft ten behoeve van deze specifieke doeleinden.

5.3.2 Analyses van Persoonsgegevens om groepsprofielen op te stellen worden beschouwd als Verwerkingen voor statistische of wetenschappelijke doeleinden.

5.4 Verwerking van Persoonsgegevens in het kader van marketingactiviteiten

5.4.1 Indien het aan een Cliënt voldoende duidelijk is gemaakt dat de Financiële instelling waar deze contact mee heeft deel uitmaakt van een Groep kan de Cliënt worden benaderd door alle entiteiten van de Groep ten behoeve van marketingactiviteiten, mits aan de overige bepalingen van de WBP is voldaan.

5.4.2 Bij marketingactiviteiten wordt primair gebruik gemaakt van Persoonsgegevens die van de Betrokkene zelf afkomstig zijn. In geval er gebruik wordt gemaakt van Persoonsgegevens die niet van de Betrokkene zelf verkregen worden, is artikel 4.8 Gedragscode van toepassing en zal de Financiële instelling zich er van overtuigen dat in overeenstemming met de WBP wordt gehandeld.

5.4.3 Ten behoeve van marketingactiviteiten kunnen Financiële instellingen hiertoe gespecialiseerde bedrijven inschakelen. Financiële instellingen zullen er voor zorg dragen dat met deze bedrijven een bewerkersovereenkomst wordt gesloten, waarin schriftelijk of in een andere, vergelijkbare vorm, verplichtingen zijn vastgelegd waaraan een Bewerker zich in het kader van de WBP dient te houden. Financiële instellingen zullen toezien op correcte naleving van de tussen partijen gemaakte afspraken.

5.4.4 Het is een Financiële instelling toegestaan, onverminderd het bepaalde in artikel 6.3.1 Gedragscode, Persoonsgegevens opgenomen in betaalopdrachten te gebruiken om financiële producten van de Groep, waartoe de Financiële instelling behoort, onder de aandacht van de Cliënt te brengen. De Financiële instelling zal deze attenderingen achterwege laten indien de Cliënt daarom verzoekt.

5.4.5 Bij marketingactiviteiten zal steeds worden nagegaan of een Betrokkene gebruik heeft gemaakt van het recht van verzet, als bedoeld in artikel 7.2 Gedragscode, in relatie tot de Verwerking van Persoonsgegevens voor dit doeleinde. Tevens zal steeds gecontroleerd worden of de Betrokkene zich heeft laten opnemen in het in artikel 11.7 lid 6,Telecommunicatiewet bedoelde register.

5.4.6 Bijzondere Persoonsgegevens zullen alleen voor marketingdoeleinden worden gebruikt met de uitdrukkelijke toestemming van de Betrokkene.

5.5 Verwerking van Persoonsgegevens in het kader van de veiligheid en integriteit van de Financiële sector alsmede het gebruik van waarschuwingssystemen

5.5.1 Ten behoeve van de veiligheid en integriteit van de Financiële sector kunnen gegevens, waaronder Persoonsgegevens, die betrekking hebben op: (i) gebeurtenissen die gelet op het bijzondere karakter van de Financiële sector de zorg en aandacht behoeven van de Financiële instelling; (ii) (potentiële) vorderingen onder meer ten aanzien van een met de Financiële instelling gesloten overeenkomst; (iii) het niet nakomen van contractuele verplichtingen of andere (toerekenbare) tekortkomingen; of (iv) handelingen van Financiële instellingen, waaronder onderzoek als bedoeld in artikel 5.6.1 Gedragscode, worden opgenomen in een

Gebeurtenissenadministratie gehouden door Veiligheidszaken of een daartoe aangewezen afdeling van de betreffende Financiële instelling. Op deze Gebeurtenissenadministratie is de Gedragscode van toepassing.

5.5.2 Indien een in het eerste lid bedoelde gebeurtenis voldoet aan de criteria als opgenomen in het Protocol worden de met deze gebeurtenis verband houdende gegevens opgenomen in het incidentenregister en is opname in het EVR mogelijk (Bijlage I: Document B).

5.6 Verwerking van Persoonsgegevens in verband met wettelijke voorschriften

5.6.1 Financiële instellingen dienen op grond van onder meer onderstaande wettelijke voorschriften in bepaalde gevallen Persoonsgegevens van een Betrokkene te verzamelen, te verwerken en aan bepaalde instellingen (waaronder overheidsinstellingen en toezichthouders) te verstrekken. Een aantal van die wettelijke verplichtingen wordt, niet uitputtend, hieronder vermeld.

a. Op grond van de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) dient, indien er sprake is van een zakelijke relatie, ter voorkoming van witwassen en financieren van terrorisme, een cliëntenonderzoek te worden uitgevoerd.
b. Wet op het financieel toezicht (Wft): op grond van de Wft dienen Financiële instellingen die zich bezig houden met het verstrekken van kredieten aan natuurlijke personen die onder de werking van de Wft vallen, te zijn aangesloten bij een 'stelsel van kredietregistraties'. Het Bureau Krediet Registratie te Tiel (BKR) beheert een dergelijk stelsel van kredietregistraties. Financiële instellingen verstrekken Persoonsgegevens over het ontstaan en afwikkelen van financieringen aan het BKR en kunnen tevens beschikken over de door andere Financiële instellingen aangeleverde Persoonsgegevens. De aard van de vastgelegde Persoonsgegevens, de voorwaarden voor vastlegging, gebruik en verstrekking en de regels voor verwijdering van de Persoonsgegevens zijn neergelegd in het reglement van het BKR, dat ook voorziet in een specifieke geschillenregeling.
c. De Wft legt verder een aanbieder van een overeenkomst inzake een financiële dienst de verplichting op informatie in te winnen over de financiële positie van de Cliënt. Daarnaast geeft het Besluit prudentiële regels aan dat Financiële instellingen zorg dienen te dragen voor een systematische analyse van integriteitsrisico's en voor het voeren van beleid met betrekking tot maatregelen en procedures met betrekking tot een integere uitoefening van het bedrijf.
d. Wet inkomstenbelasting 2001 en Invoeringswet inkomstenbelasting 2001: op grond van deze wetten is voorgeschreven dat door Financiële instellingen het burgerservicenummer (hierna: BSN) als verplicht identificerend gegeven op de renseigneringen wordt vermeld.
e. Wet algemene bepalingen burgerservicenummer (Wabb): op grond van deze wet moeten verzekeraars als bedoeld in artikel 23, eerste lid, onder c Pensioenwet het burgerservicenummer gebruiken ter uitvoering van pensioenregelingen.
f. Algemene wet inzake rijksbelastingen (AWR): op grond van deze wet zijn - administratieplichtige - Financiële instellingen gehouden het BSN van het identiteitsbewijs in hun administratie te bewaren.
g. Verschillende wetten, waaronder het Wetboek van Strafvordering, verplichten Financiële instellingen om, indien dat gevorderd wordt, gegevens over transacties van Cliënten ter beschikking te stellen aan opsporingsambtenaren en toezichthouders.

6. Verwerking van Bijzondere Persoonsgegevens

6.1 Persoonsgegevens betreffende iemands gezondheid

6.1.1 Het is een Financiële instelling toegestaan Persoonsgegevens betreffende iemands gezondheid te verwerken voor zover dat noodzakelijk is voor: de beoordeling van een Cliënt, de acceptatie van een Cliënt, het uitvoeren van een overeenkomst met een Cliënt en het afwikkelen van het betalingsverkeer.

6.1.2 Onverminderd het bepaalde in artikel 6.1.1 Gedragscode is het een Financiële instelling toegestaan Persoonsgegevens betreffende iemands gezondheid te verwerken indien: (i) hiertoe de uitdrukkelijke toestemming van de Cliënt is verkregen; (ii) de gegevens door de Betrokkene duidelijk openbaar zijn gemaakt; (iii) dit noodzakelijk is voor de vaststelling, de uitoefening of de verdediging van een recht in rechte; (iv) dit noodzakelijk is ter voldoening aan een volkenrechtelijke verplichting; (v) dit noodzakelijk is met het oog op een zwaarwegend algemeen belang, passende waarborgen worden geboden ter bescherming van de persoonlijke levenssfeer en dit bij wet wordt bepaald dan wel het CBP ontheffing heeft verleend.

6.1.3 Persoonsgegevens betreffende iemands gezondheid die zijn verwerkt met het oog op de beoordeling van een Cliënt, de acceptatie van een Cliënt, het uitvoeren van een overeenkomst met een Cliënt gericht op een specifiek product of de afhandeling van een schadeclaim van een Cliënt zullen zonder uitdrukkelijke toestemming van de Cliënt niet worden gebruikt in het kader van de beoordeling van een Cliënt, de acceptatie van een Cliënt, het uitvoeren van een overeenkomst met een Cliënt ten behoeve van een ander product of de afhandeling van een andere schadeclaim.

6.1.4 Het verwerken van Persoonsgegevens betreffende iemands gezondheid door een Financiële instelling om een advies te kunnen uitbrengen over de medische beoordeling van een Cliënt alsmede van het medisch handelen van een Verzekerde is voorbehouden aan een Medisch adviseur en de personen die onder zijn verantwoordelijkheid betrokken zijn bij dat advies. Het opvragen van aanvullende gegevens omtrent de gezondheid van en bij een Cliënt gebeurt uitsluitend door een Medisch adviseur of mensen uit zijn medische dienst of staf.

6.1.5 Het verzamelen van Persoonsgegevens betreffende iemands gezondheid door een Medisch adviseur van een Financiële instelling bij anderen dan de Cliënt zal alleen plaatsvinden nadat de Cliënt daarvoor toestemming heeft verleend en daartoe een machtiging heeft verstrekt. Deze machtiging dient niet algemeen van aard te zijn, maar dient zich te richten op de Verwerking ten behoeve van een concrete aangelegenheid. De Cliënt dient te worden geïnformeerd over de aard van de op te vragen gegevens, alsmede over het doel daarvan. Dit dient uit de machtiging te blijken.

6.1.6 Rapporten van een geneeskundige, de Arbodienst, alsmede informatie van de behandelend sector dienen te worden opgenomen in een medisch dossier dat onder de verantwoordelijkheid van de Medisch adviseur wordt bewaard. De Cliënt heeft het recht - bij voorkeur via een door hem of haar benoemde vertrouwensarts - een op de Cliënt betrekking hebbend medisch dossier volledig, met uitzondering van werkaantekeningen van de Medisch adviseur, in te zien en daarvan kopieën te ontvangen, tenzij de privacy van de in het rapport besproken Derden zich daartegen verzet.

6.1.7 a. Indien in het kader van acceptatie en/of schadebehandeling medewerking van een Cliënt aan

een medische keuring of aan een aanvullend onderzoek wordt gevraagd, zal de Financiële instelling in de keuringsstukken en formulieren wijzen op het belang van legitimatie teneinde verwisseling van personen te voorkomen.

b. De Cliënt zal daarbij worden geïnformeerd dat hij het recht heeft om schriftelijk te kennen te geven dat hij de uitslag en gevolgtrekking van het onderzoek wenst vernemen. Tenzij het betreft een tot stand gekomen burgerrechtelijke verzekering heeft de Cliënt het recht mede te delen om als eerste kennis te nemen van deze gegevens teneinde te kunnen beslissen dat geen mededeling van die uitslag en gevolgtrekking aan anderen wordt gedaan

6.1.8 Niet onder de verantwoordelijkheid van de Medisch adviseur vallen Verwerkingen van Persoonsgegevens omtrent iemands gezondheid voor zover dat noodzakelijk is voor:

a. het nemen van een beslissing inzake het door de verzekeraar te verzekeren risico;
b. de schadeafhandeling om de omvang van de gemelde claim of de schade te kunnen vaststellen, teneinde te kunnen beslissen of aanvullende informatie nodig is of dat direct tot uitkering kan worden overgegaan. Dit alles onverminderd het bepaalde in artikel 6.1.4 dat de aanvullende informatie wordt opgevraagd en beoordeeld door de Medisch adviseur en dat bij de directe schadeafhandeling alleen daartoe noodzakelijke persoonsgegevens omtrent gezondheid worden verwerkt;
c. de uitvoering van de verzekerings- of financieringsovereenkomst, waaronder mede begrepen de Verwerking van Persoonsgegevens in het kader van het ontvangen en verwerken van declaraties en financieringsovereenkomsten dan wel indien daarom door of namens de Cliënt is verzocht in verband met diens gezondheidstoestand.

6.1.9 De gegevens omtrent iemands gezondheid worden slechts verwerkt door personen die uit hoofde van ambt, beroep of wettelijk voorschrift dan wel krachtens een overeenkomst tot geheimhouding zijn verplicht, behoudens voor zover de wet hen tot mededeling verplicht of uit hun taak de noodzaak voortvloeit dat de gegevens worden medegedeeld aan anderen die krachtens artikel 6.1 Gedragscode bevoegd zijn tot Verwerking daarvan.

6.1.10 Op de Verwerking van Persoonsgegevens betreffende erfelijke eigenschappen is het moratorium erfelijkheidsonderzoek van toepassing. (Bijlage I: Document D).

6.1.11 Op de Verwerking van Persoonsgegevens betreffende iemands gezondheid die ontleend kunnen worden aan bloedonderzoek is de 'HIV- gedragscode' van toepassing. (Bijlage I: Document E).

6.2 Persoonsgegevens van strafrechtelijke aard

6.2.1 Het is Financiële instellingen toegestaan strafrechtelijke Persoonsgegevens te verwerken voor zover dat noodzakelijk is voor: (i) de beoordeling van een Cliënt, de acceptatie van een Cliënt, het uitvoeren van een overeenkomst met een Cliënt en het afwikkelen van het betalingsverkeer; (ii) het waarborgen van de veiligheid en integriteit van de financiële sector, daaronder mede begrepen onderkennen, voorkomen, onderzoeken en bestrijden van (pogingen tot) (strafbare of laakbare) gedragingen gericht tegen de branche waar een Financiële instelling deel van uitmaakt, de Groep waartoe een Financiële instelling behoort, de Financiële instelling zelf, haar Cliënten en medewerkers, alsmede het gebruik van en de deelname aan waarschuwingssystemen; of (iii) het voldoen aan wettelijke verplichtingen.

6.2.2 Onverminderd het bepaalde in artikel 6.2.1 is het Financiële instellingen toegestaan Persoonsgegevens van strafrechtelijke aard te verwerken indien: (i) hiertoe de uitdrukkelijke toestemming van de Cliënt is verkregen; (ii) de gegevens door de Betrokkene duidelijk openbaar zijn gemaakt; (iii) dit noodzakelijk is voor de vaststelling, de uitoefening of de verdediging van een recht in rechte; (iv) dit noodzakelijk is ter voldoening aan een volkenrechtelijke verplichting; (v) dit noodzakelijk is met het oog op een zwaarwegend algemeen belang, passende waarborgen worden geboden ter bescherming van de persoonlijke levenssfeer en dit bij wet wordt bepaald dan wel het CBP ontheffing heeft verleend; (v) indien passende en specifieke waarborgen zijn getroffen en de procedure is gevolgd ingevolge artikel 31 WBP.

6.2.3 Financiële instellingen kunnen met het oog op een verantwoord acceptatiebeleid vragen naar feiten omtrent een eventueel strafrechtelijk verleden van te verzekeren personen en anderen wiens belangen op de aangevraagde verzekering worden (mee)verzekerd (bestuurders en aandeelhouders van rechtspersonen daaronder begrepen), voor zover die feiten betrekking hebben op een periode van 8 jaar voorafgaand aan de aanvraag tot verzekering. Daarbij geldt dat het opgegeven strafrechtelijk verleden slechts gebruikt zal worden voor de beoordeling van de verzekeringsaanvraag en dat langs rechtmatige weg verkregen gegevens omtrent een strafrechtelijk verleden kunnen worden gebruikt in het kader van een beroep op niet nakomen van de mededelingsplicht.

6.2.4 Het verbod om andere Bijzondere gegevens te verwerken is niet van toepassing voor zover dit noodzakelijk is in aanvulling op de verwerking van strafrechtelijke gegevens voor de doeleinden waarvoor deze gegevens worden verwerkt.

6.2.5 Persoonsgegevens die:(i) betrekking hebben op strafbare feiten die zijn, of op grond van feiten en omstandigheden naar verwachting zullen worden, begaan jegens één van de in een Groep verbonden Financiële instellingen; of (ii) dienen ter vaststelling van mogelijk strafbaar gedrag jegens één van de in een Groep verbonden Financiële instellingen, kunnen door de Financiële instelling worden verstrekt binnen de Groep, mits de gegevens uitsluitend worden verstrekt aan functionarissen die de gegevens voor de uitoefening van hun functie nodig hebben alsmede aan politie en Justitie.

6.3 Andere Bijzondere Persoonsgegevens

6.3.1 Het mededelingenveld van een betalingsopdracht kan Bijzondere Persoonsgegevens bevatten. De uitvoering van de betalingsopdrachten brengt met zich mee dat Verwerking van dergelijke Persoonsgegevens plaatsvindt. De Verwerking van Persoonsgegevens vindt onder meer plaats door het archiveren van de originele bescheiden of van de al dan niet elektronische afschriften daarvan.

6.3.2 Het is een Financiële instelling toegestaan (andere) Bijzondere Persoonsgegevens te verwerken indien: (i) hiertoe de uitdrukkelijke toestemming van de Cliënt is verkregen; (ii) de gegevens door de Betrokkene duidelijk openbaar zijn gemaakt; (iii) dit noodzakelijk is voor de vaststelling, de uitoefening of de verdediging van een recht in rechte; (iv) dit noodzakelijk is ter voldoening aan een volkenrechtelijke verplichting; (v) dit noodzakelijk is met het oog op een zwaarwegend algemeen belang, passende waarborgen worden geboden ter bescherming van de persoonlijke levenssfeer en dit bij wet wordt bepaald dan wel het CBP ontheffing heeft verleend.

7. Rechten van Betrokkene

7.1 Kennisneming en correctie

7.1.1 Een Betrokkene is gerechtigd - met redelijke tussenpozen - een Financiële instelling schriftelijk een overzicht te vragen van de Persoonsgegevens van de Betrokkene die door die Financiële instelling worden verwerkt. De Financiële instelling zal, behoudens de in artikel 9 Gedragscode genoemde uitzonderingsgevallen, de Betrokkene binnen vier weken na ontvangst van het verzoek een volledig overzicht van de Persoonsgegevens doen toekomen. Indien door de Financiële instelling geen Persoonsgegevens van de Betrokkene worden verwerkt, zal de Financiële instelling dit tevens binnen vier weken na ontvangst van het verzoek aan de Betrokkene laten weten.

7.1.2 Het overzicht als genoemd in artikel 7.1.1 Gedragscode omvat in begrijpelijke vorm: (i) een omschrijving van het doel of de doeleinden van de Verwerking; (ii) de categorieën van Persoonsgegevens waarop de Verwerking betrekking heeft; (iii) de ontvangers of categorieën van ontvangers, alsmede; (iv) de beschikbare informatie over de herkomst van de Persoonsgegevens.

7.1.3 Indien uit het verstrekte overzicht blijkt dat Persoonsgegevens feitelijk onjuist zijn, voor het doel van de Verwerking onvolledig of niet ter zake dienend dan wel anderszins in strijd met deze Gedragscode of wettelijk voorschrift worden verwerkt, kan de Betrokkene schriftelijk om verbetering, aanvulling, verwijdering of afscherming van de betreffende Persoonsgegevens verzoeken. Een Financiële instelling zal de Betrokkene binnen vier weken na ontvangst van genoemd verzoek, schriftelijk laten weten of dan wel in hoeverre aan het verzoek wordt voldaan. Indien niet of niet volledig aan het verzoek van de Betrokkene wordt voldaan wordt dit met redenen omkleed.

7.1.4 Het in artikel 7.1.1 Gedragscode genoemde verzoek dient te worden gedaan bij de Financiële instelling die verantwoordelijk is voor de betreffende Verwerking van Persoonsgegevens. Het verzoek om correctie dient een specificatie te bevatten van de Persoonsgegevens die gecorrigeerd dienen te worden. De Financiële instelling draagt zorg voor een deugdelijke vaststelling van de identiteit van de verzoeker.

7.1.5 Indien het voor de Betrokkene onduidelijk is wie als Verantwoordelijke voor de Verwerking van de betreffende Persoonsgegevens dient te worden aangemerkt, bijvoorbeeld omdat de Financiële instelling deel uitmaakt van een Groep, kan de Betrokkene zijn verzoek richten tot de directie van de Financiële instelling waarvan hij vermoedt dat deze zijn Persoonsgegevens verwerkt. De directie van de betreffende Financiële instelling dient er voor zorg te dragen dat het verzoek op de juiste wijze wordt afgehandeld.

7.2 Verzet en toestemming

7.2.1 Indien de grondslag van de Verwerking van Persoonsgegevens is gelegen in het gerechtvaardigde belang van de Verantwoordelijke of van een Derde aan wie de Persoonsgegevens worden verstrekt heeft de Betrokkene het recht verzet aan te tekenen tegen de Verwerking van Persoonsgegevens in verband met zijn bijzondere persoonlijke omstandigheden. Binnen vier weken na ontvangst van het verzet beoordeelt de Verantwoordelijke of het verzet gerechtvaardigd is. Is dat het geval dan wordt de Verwerking van Persoonsgegevens van die Betrokkene onmiddellijk beëindigd.

7.2.2 Indien een Financiële instelling Persoonsgegevens verwerkt met het oog op werving voor commerciële of

charitatieve doelen kan de Betrokkene daartegen altijd kosteloos verzet aantekenen. In geval van verzet treft de Financiële instelling maatregelen om deze vorm van Verwerking van Persoonsgegevens onmiddellijk te beëindigen. De Verantwoordelijke zal zorg dragen dat, indien voor de hiervoor genoemde doelen rechtstreeks een boodschap aan Betrokkene wordt gezonden, deze daarbij telkens wordt gewezen op de mogelijkheid tot het doen van verzet.

7.2.3 Het gebruik van automatische oproepsystemen zonder menselijke tussenkomst, faxen of elektronische berichten voor Direct Marketing is uitsluitend toegestaan indien de verzender kan aantonen dat de Betrokkene daarvoor voorafgaand toestemming heeft verleend ("opt-in"). Er zijn voor de Betrokkene geen kosten verbonden aan het verlenen van deze toestemming.

7.2.4 Het gebruik van andere dan de in artikel 7.2.3 Gedragscode genoemde technieken waaronder telefoon en 'gewone' post voor Direct Marketing is toegestaan, tenzij de betreffende Betrokkene te kennen heeft gegeven informatie of mededelingen waarbij van deze technieken gebruik wordt gemaakt, niet te willen ontvangen ("opt-out"). Er zijn voor de Betrokkene geen kosten verbonden aan voorzieningen waarmee wordt voorkomen dat aan een Betrokkene ongevraagde informatie wordt overgebracht.

7.2.5 Een Financiële instelling die elektronische contactgegevens voor elektronische berichten (zoals e-mail, sms-berichten, mms-berichten) heeft verkregen in het kader van de verkoop van een financieel product of het verlenen van een financiële dienst mag deze gegevens gebruiken voor Direct Marketing ten behoeve van eigen gelijksoortige financiële producten of financiële diensten ("soft opt-in"). Dit op voorwaarde dat: (i) bij de verkrijging van de contactgegevens aan de Betrokkene uitdrukkelijk de gelegenheid is geboden om kosteloos verzet aan te tekenen tegen het gebruik van die elektronische contactgegevens; en, (ii) indien de Betrokkene hiervan geen gebruik heeft gemaakt, hem bij elke tot stand gebrachte communicatie nadrukkelijk de mogelijkheid wordt geboden om kosteloos verzet aan te tekenen tegen het verdere gebruik van zijn elektronische contactgegevens. Artikel 41 lid 2 WBP is van overeenkomstige toepassing.

7.2.6 Bij het gebruik van elektronische berichten voor Direct Marketing dient de Financiële instelling te voldoen aan de informatieplicht ingevolge artikel 3:15 e Burgerlijk Wetboek.

7.2.7 Een Financiële instelling zal zich slechts door middel van een elektronisch communicatiemiddel toegang verschaffen tot Persoonsgegevens die zijn opgeslagen in apparatuur van een gebruiker van een openbaar communicatienetwerk indien dat noodzakelijk is om de verzending van communicatie over een openbaar netwerk uit te voeren of te vergemakkelijken dan wel om de door de gebruiker gevraagde dienst te leveren en de opslag of toegang tot gegevens daarvoor strikt noodzakelijk is.

7.2.8 In alle andere gevallen zal een Financiële instelling zich een dergelijke toegang slechts verschaffen indien de gebruiker op een duidelijke en nauwkeurige wijze is geïnformeerd over de doeleinden waarvoor toegang tot apparatuur of Persoonsgegevens gewenst is en op voldoende kenbare wijze de gelegenheid is geboden om deze handeling te weigeren.

7.3 Vergoeding van kosten

7.3.1 Een Financiële instelling kan voor een verzoek van een Betrokkene als bedoeld in de artikelen 7.1.1 en 7.2.1 Gedragscode een vergoeding van kosten verlangen die niet hoger is dan het bij algemene maatregel van bestuur

vastgestelde bedrag.

7.3.2 Indien tot aanpassing, wijziging of verwijdering van de Persoonsgegevens wordt overgegaan als bedoeld in artikel 7.1.3 Gedragscode of indien het verzet als bedoeld in artikel 7.2.1 Gedragscode gegrond wordt bevonden wordt de vergoeding als bedoeld in artikel 7.3.1 Gedragscode gerestitueerd.

7.4 Besluit op grond van geautomatiseerde Verwerking van Persoonsgegevens

7.4.1 Het nemen van een besluit door een Financiële instelling uitsluitend op grond van geautomatiseerde Verwerking van Persoonsgegevens bestemd om een beeld van bepaalde aspecten van iemands persoonlijkheid te krijgen is slechts toegestaan indien: (i) dit wordt genomen in het kader van het sluiten of uitvoeren van een overeenkomst, of (ii) dit besluit zijn grondslag vindt in een wet waarin maatregelen zijn vastgelegd die strekken tot bescherming van het gerechtvaardigde belang van de Betrokkene.

7.4.2 Indien bij het besluit niet is voldaan aan het verzoek van de Betrokkene zal deze in de gelegenheid worden gesteld zijn zienswijze naar voren te brengen. De Financiële instelling deelt in dat geval de logica mede die aan de geautomatiseerde Verwerking van Persoonsgegevens ten grondslag heeft gelegen.

8. Speciale onderwerpen

8.1 Functionaris

8.1.1 Een Financiële instelling kan een Functionaris benoemen. Als Functionaris kan slechts worden benoemd een natuurlijke persoon die voor de vervulling van zijn taak over toereikende kennis beschikt en voldoende betrouwbaar kan worden geacht. De Functionaris is voor zijn taakuitoefening onafhankelijk van de Financiële instelling die hem heeft benoemd en kan daarvan geen aanwijzingen met betrekking tot de uitoefening van zijn taak ontvangen. De Financiële instelling die hem benoemt dient de Functionaris in de gelegenheid te stellen zijn taak naar behoren te vervullen, en draagt er zorg voor dat deze geen nadeel ondervindt van de uitoefening van zijn taak. In dat verband geniet de Functionaris ontslagbescherming.

8.1.2 De Functionaris ziet toe op de naleving door de Financiële instelling van de voorschriften met betrekking tot het verwerken van Persoonsgegevens gesteld bij of krachtens enige wet, alsmede op de naleving van de voorschriften van deze Gedragscode. Hij stelt jaarlijks een verslag op van zijn werkzaamheden en bevindingen. De Functionaris heeft de bevoegdheden die hem op grond van artikel 63 en 64 WBP zijn toegekend. De Algemene wet bestuursrecht wordt analoog toegepast.

8.2 Gegevensverkeer met landen buiten de Europese Economische Ruimte (EER)

8.2.1 Financiële instellingen wisselen in het kader van hun dienstverlening Persoonsgegevens uit binnen de Groep met door Financiële instellingen ingeschakelde Bewerkers en met Derden. Dit kan met zich mee brengen dat Persoonsgegevens aan landen worden doorgegeven die zich buiten de EER bevinden, nu entiteiten die deel uitmaken van de Groep, Bewerkers en Derden zich kunnen bevinden in landen buiten de EER.

8.2.2 Doorgifte van Persoonsgegevens naar landen buiten de EER door een Financiële instelling is toegestaan, met inachtneming van de beginselen van Verwerking van Persoonsgegevens, indien het betreffende land een

passend beschermingsniveau ten aanzien van de doorgegeven Persoonsgegevens waarborgt. Van een passend beschermingsniveau wordt onder meer gesproken indien de Europese Commissie heeft besloten dat een betreffend land een passend beschermingsniveau heeft. Tevens kan door implementatie van goedgekeurde Binding Corporate Rules binnen een Groep wereldwijd een passend beschermingsniveau worden gecreëerd.

8.2.3 Doorgifte van Persoonsgegevens door een Financiële instelling is altijd toegestaan indien:

a. de Betrokkene daarvoor zijn ondubbelzinnige toestemming heeft gegeven; of
b. de doorgifte noodzakelijk is voor de uitvoering van een overeenkomst tussen Cliënt en de Verantwoordelijke, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van Cliënt en die noodzakelijk zijn voor het sluiten van een overeenkomst; of
c. de doorgifte noodzakelijk is voor de sluiting of uitvoering van een in het belang van de Cliënt tussen de Verantwoordelijke en een Derde gesloten of te sluiten overeenkomst; of
d. de doorgifte noodzakelijk is vanwege een zwaarwegend algemeen belang of voor de vaststelling, de uitvoering of de verdediging in rechte van enig recht; of
e. de doorgifte noodzakelijk is ter vrijwaring van vitale belangen van de Betrokkene; of
f. de minister van Justitie een vergunning heeft gegeven voor doorgifte of categorieën van doorgiften.

8.3 Beveiliging van Persoonsgegevens

8.3.1 De Financiële instelling die Persoonsgegevens verwerkt treft, rekening houdend met: (i) de stand van de techniek; (ii) de kosten van de tenuitvoerlegging; (iii) de risico's die de Verwerking met zich meebrengt; (iv) en de aard van de Persoonsgegevens, passende technische en organisatorische maatregelen om Persoonsgegevens te beveiligen tegen onder meer (opzettelijke) vernietiging, verlies, vervalsing, ongewenste verspreiding of toegang, dan wel tegen enige andere vorm van onrechtmatige Verwerking van Persoonsgegevens.

8.3.2 Indien de Verwerking van Persoonsgegevens wordt gedaan door een Bewerker draagt de Verantwoordelijke er zorg voor dat met de betreffende Bewerker in een overeenkomst schriftelijk of in een andere, gelijkwaardige vorm wordt vastgelegd, dat de Bewerker zorg draagt voor voldoende waarborgen ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten Verwerking van Persoonsgegevens.

8.4 Cameratoezicht

8.4.1 Het is een Financiële instelling toegestaan onder bepaalde voorwaarden toezicht te houden door gebruik van camera's. Cameratoezicht, de daarvoor verkregen beelden en verwerking daarvan hebben als doel:

a. gebouwen en terreinen die de Financiële instelling gebruikt/eigendom van de Financiële instelling is te beveiligen;
b. goederen in die gebouwen te bewaken;
c. belangen van de Financiële instelling en de veiligheid en belangen van de medewerkers, Cliënten of Derden te beschermen;
d. strafbare feiten of overtredingen van (bedrijfs)regels van de Financiële instelling te voorkomen, vast te stellen of te onderzoeken;
e. juridische procedures te ondersteunen.

8.4.2 Camera toezicht door Financiële instellingen is slechts toegestaan, indien:

a. cameratoezicht op selectieve wijze wordt uitgeoefend, dat wil zeggen dat niet meer plaatsen en personen mogen worden vastgelegd dan voor de genoemde doeleinden noodzakelijk is. Verzekeraars dienen hierbij tevens het bepaalde in de Gedragscode Persoonlijk Onderzoek (Bijlage I: Document C) te volgen;
b. de door cameratoezicht verkregen Persoonsgegevens niet langer worden bewaard dan nodig is voor de in artikel 8.4.1 Gedragscode omschreven doeleinden. De bewaarduur kan per cameratoepassing verschillen;
c. de door cameratoezicht verkregen beelden zodanig bewaard en beveiligd worden dat deze niet toegankelijk zijn voor onbevoegden, terwijl zodanige maatregelen worden getroffen dat manipulatie wordt voorkomen en beelden traceerbaar zijn en gereconstrueerd kunnen worden;
d. cameratoezicht duidelijk kenbaar is gemaakt. In voorkomende gevallen kan gebruik worden gemaakt van een verborgen camera om strafbare feiten of overtredingen van bedrijfsregels vast te stellen of te onderzoeken, of om juridische procedures te ondersteunen.

8.4.3 Voor zover bij cameratoezicht Persoonsgegevens omtrent ras worden verwerkt dan geschiedt dat uitsluitend met het oog op de identificatie van de Betrokkene en slechts voor zover dat voor het doel onvermijdelijk is.

8.4.4 De door camera's verkregen beelden kunnen door Financiële instellingen worden verstrekt aan politie en Justitie, Veiligheidszaken en binnen de Groep aan functionarissen die handhaving van de bedrijfsregels tot taak hebben.

8.4.5 Een Betrokkene heeft het recht de cameraopname te bekijken en/of een kopie van de cameraopname te verkrijgen. Dit op voorwaarde dat de Betrokkene de Financiële instelling voldoende informeert om zodoende de Financiële instelling in staat te stellen de betreffende cameraopname te traceren. De Betrokkene dient de Financiële instelling ten minste te informeren over de plaats, datum en tijdstip van de opname, dan wel een andere indicatie om het zoeken te vergemakkelijken. De Financiële instelling behoeft geen inzage te verlenen indien wordt voldaan aan de voorwaarden van artikel 9 Gedragscode.

8.5 Vastlegging telefoongesprekken

8.5.1 Het opnemen van telefoongesprekken door een Financiële instelling, de daardoor verkregen bandopnames en Verwerking daarvan hebben als doel: (i) het kunnen leveren van bewijs onder andere ten aanzien van interpretatieverschillen of onenigheid met betrekking tot de inhoud van het telefoongesprek; (ii) (fraude) onderzoek en opsporing; (iii) evalueren van de kwaliteit van de dienstverlening; (iv) trainings-, coachings- en beoordelingsdoeleinden.

8.5.2 De bandopnames worden zodanig bewaard en beveiligd dat deze niet toegankelijk zijn voor onbevoegden, terwijl zodanige maatregelen worden getroffen dat manipulatie wordt voorkomen.

8.5.3 De bandopname wordt door de Financiële instelling niet langer bewaard dan noodzakelijk voor de in artikel 8.5.1 Gedragscode genoemde doeleinden.

8.5.4 Een Betrokkene heeft het recht de bandopname te beluisteren, een kopie van de band te krijgen of een transcriptie van het opgenomen telefoongesprek te verkrijgen, zulks afhankelijk van de inhoud van de band. Dit op

voorwaarde dat de Betrokkene de Financiële instelling voldoende informeert om zodoende de Financiële instelling in staat te stellen de betreffende bandopname te traceren. De Betrokkene dient de Financiële instelling ten minste te informeren over de datum en tijdstip van het gesprek, het door de Betrokkene gebruikte telefoonnummer en een aanduiding omtrent het door de Betrokkene gebelde telefoonnummer dan wel een andere indicatie om het zoeken te vergemakkelijken. De Financiële instelling behoeft geen inzage te verlenen indien wordt voldaan aan de voorwaarden genoemd in artikel 9 Gedragscode.

8.5.5 De bandopnames kunnen door Financiële instellingen worden verstrekt aan politie en Justitie, Veiligheidszaken en binnen de Groep aan functionarissen die handhaving van de bedrijfsregels tot taak hebben.

8.6 Vastlegging elektronische communicatie

8.6.1 Bij het vastleggen van Persoonsgegevens verkregen via elektronische communicatie met een Betrokkene wordt artikel 8.5 Gedragscode zo veel als mogelijk analoog toegepast.

9. Dringende redenen

9.1 Het doelbindingsbeginsel, transparantiebeginsel en de rechten van de Betrokkenen als genoemd in de artikelen 4.4, 4.7, 4.8, 4.9, 7.1.1, 8.4.5 en 8.5.4 Gedragscode kunnen in bijzondere omstandigheden, waarbij alle feiten en omstandigheden van belang zijn, opzij worden gezet als hiertoe een dringende noodzaak bestaat, welke noodzaak zwaarder weegt dan de rechten en vrijheden van de Betrokkene,een en ander in het kader van:

a. het voorkomen, opsporen, onderzoeken en vervolgen (waaronder de samenwerking met (toezichthoudende) autoriteiten) van overtreding van wetgeving, regelgeving of bedrijfsregels van de Financiële instelling;
b. het beschermen en verdedigen van de rechten en vrijheiden van de Financiële instelling/Financiële sector, het personeel of andere personen (waaronder de Betrokkene of een Derde) waaronder: (i) de veiligheid (van werknemers en Cliënten) van de Financiële instelling/Financiële sector; (ii) bedrijfsgeheimen en reputatie van de Financiële instelling; (iii) de continuïteit van de Financiële instelling/Financiële sector; (iv) geheimhouding in het kader van bijvoorbeeld een (voorgenomen) fusie of overname; (v) betrokkenheid van adviseurs op onder meer het gebied van recht, fiscaliteit en verzekeringen.

10. Naleving van de Gedragscode

10.1 Financiële instellingen hechten belang aan een correcte naleving van de regels van de WBP en Gedragscode. In dat kader hebben Financiële instellingen een stelsel van zelfevaluaties geïmplementeerd door middel waarvan periodiek risicoanalyses worden gemaakt met betrekking tot de naleving van de WBP en deze Gedragscode. Onderdeel hiervan is dat door een Financiële instelling wordt vastgesteld op welke wijze en hoe frequent de diverse onderdelen van de Financiële Instelling worden gecontroleerd op correcte naleving van de WBP en de Gedragscode, alsmede het opstellen van rapportages.

10.2 Ter bevordering van de naleving van de regels van de WBP en Gedragscode is een Financiële instelling gehouden interne instructies op te stellen en te geven waarin nader wordt aangegeven op welke wijze Persoonsgegevens door de Financiële instelling worden verwerkt. De interne instructies betreffen in ieder geval die onderwerpen waarvan de Financiële instelling van oordeel is dat nadere uitleg wenselijk is.

11. Geschillen

11.1 Een Betrokkene die van mening is dat een Financiële instelling in strijd handelt met de Gedragscode dan wel de WBP, kan zich wenden tot de Stichting Klachteninstituut Financiële Dienstverlening (KiFiD), Postbus 93257, 2509 AG Den Haag. Voorwaarde is dat eerst de interne klachtenprocedure van de Financiële instelling is doorlopen. Afhankelijk van de inhoud van de klacht kan de Betrokkene zich ook rechtstreeks tot het CBP dan wel de bevoegde rechter wenden. In alle gevallen dient hij acht te slaan op de termijnen van artikel 46 en 47 WBP.

Toelichting bij de Gedragscode Verwerking Persoonsgegevens Financiële instellingen

1. Overwegingen

Toelichting

Vrijwel iedereen in Nederland heeft een relatie met een Financiële instelling. Zo heeft men bijvoorbeeld een betaalrekening, een hypothecaire financiering, een persoonlijke lening of een verzekering. Onder meer in het kader van de relatie die een Financiële instelling heeft of wenst aan te gaan met een Cliënt zal de Financiële instelling Persoonsgegevens verwerken. Bij het verwerken van Persoonsgegevens spelen verschillende belangen een rol. De Betrokkene heeft er belang bij dat zijn persoonlijke levenssfeer zo goed mogelijk wordt beschermd, terwijl de Financiële instelling zijn gerechtvaardigde belangen zo goed mogelijk wenst te behartigen.

Om mogelijk conflicterende belangen in verband met het verwerken van Persoonsgegevens op een goede wijze met elkaar te verenigen zijn regels opgesteld in de vorm van de Wet bescherming persoonsgegevens (hierna: WBP)1. De WBP legt een Financiële instelling die Persoonsgegevens verwerkt, de Verantwoordelijke, een aantal verplichtingen op. De mensen van wie Persoonsgegevens worden verwerkt, de Betrokkenen, hebben op grond van de WBP een aantal rechten toegekend gekregen, zoals het recht op inzage, correctie en verzet. Er wordt ook (onafhankelijk) toezicht gehouden op naleving van de WBP door: (i) het College bescherming persoonsgegevens (hierna: CBP) (ii) de functionaris voor de gegevensbescherming (hierna: Functionaris), indien deze door een Financiële instelling is aangesteld of (iii) door speciale privacyfunctionarissen of -managers die door een Financiële instelling daartoe zijn aangesteld.

1 Stb, 2001, 337. De WBP is gebaseerd op de EU Richtlijn betreffende de bescherming van natuurlijke personen in verband met de Verwerking van Persoonsgegevens en betreffende het vrije verkeer van die gegevens.

De WBP biedt aan een organisatie, branche en sector de mogelijkheid om nadere regels te stellen, die bijvoorbeeld meer toegesneden zijn op een bepaalde bedrijfsvoering. Gelet op de verwevenheid tussen banken en verzekeraars hebben de Nederlandse Vereniging van Banken (hierna: NVB) en het Verbond van Verzekeraars (hierna: Verbond) er voor gekozen één Gedragscode op te stellen: de Gedragscode Verwerking Persoonsgegevens Financiële instellingen (hierna: Gedragscode). Ten aanzien van de eerste Gedragscode Verwerking Persoonsgegevens Financiële Instellingen van 25 januari 2003 heeft het CBP een goedkeurende verklaring voor een periode van 5 jaar verstrekt. Deze Gedragscode is vervolgens geactualiseerd en het CBP heeft verklaard dat de Gedragscode een juiste uitwerking vormt van de WBP . De verklaring geldt voor een periode van vijf jaar.

2. Begripsbepaling

Toelichting

De meeste begrippen die in de Gedragscode zijn gedefinieerd sluiten (om consistent te blijven) aan bij de begrippen die in de WBP zijn opgenomen. Vier begrippen die min of meer specifiek zijn voor een Financiële instelling en die niet in de WBP voorkomen zijn Cliënt, Medisch adviseur, Veiligheidzaken en Verzekerde. De begrippen Cliënt en Verzekerde zullen nader worden uitgelegd bij het begrip Betrokkene. De andere begrippen zullen bij de desbetreffende artikelen (resp. 6.1 en 5.5 Gedragscode) nader worden toegelicht.

Voor een goed begrip van de Gedragscode dient men de betekenis van drie definities te onthouden, te weten die van de Verantwoordelijke, de Betrokkene en de Bewerker. De WBP legt verplichtingen op aan de zogenaamde Verantwoordelijke voor de Verwerking van Persoonsgegevens en kent rechten toe aan de zogenaamde Betrokkene. Daarnaast is het van belang onderscheid te maken tussen een Verantwoordelijke en een Bewerker.

De Verantwoordelijke is degene die het doel en de middelen van de Verwerking vaststelt. Het gaat om de rechtspersoon die formeel bevoegd is om beslissingen te nemen over de Verwerking van Persoonsgegevens. In beginsel zal de Financiële instelling met wie de Betrokkene bijvoorbeeld een overeenkomst sluit optreden als Verantwoordelijke. De WBP staat er niet aan in de weg dat in de praktijk regelingen worden getroffen waardoor de verantwoordelijkheid binnen een Groep wordt toegerekend aan een andere partij (bijvoorbeeld aan de moedermaatschappij) dan de partij onder wiens bevoegdheid de operationele Verwerking van Persoonsgegevens plaatsvindt (bijvoorbeeld een dochtervennootschap). In het geval een Financiële instelling onderdeel uitmaakt van een Groep kan dus een andere rechtspersoon binnen de Groep als Verantwoordelijke zijn aangewezen. Door de statuten of door middel van een overeenkomst worden in dat geval aan een bepaalde rechtspersoon binnen de Groep de bevoegdheid toegekend om doel en middelen van de Verwerking van Persoonsgegevens binnen de Groep te bepalen. De moedermaatschappij kan aldus als Verantwoordelijke optreden voor alle Verwerkingen van Persoonsgegevens die binnen de Groep plaatsvinden, omdat de juridische zeggenschap krachtens de getroffen regelingen bij de rechtspersoon berust. Als niet is vast te stellen wie formeel bevoegd is om te beslissen over de Verwerking van Persoonsgegevens, is degene aan wie naar de in het maatschappelijk verkeer geldende maatstaven de Verwerking van Persoonsgegevens moet worden toegerekend verantwoordelijk. In algemene termen is het moeilijk om hier een nadere invulling aan te geven: wat in het maatschappelijk verkeer geldende maatstaven zijn, zal afhangen van de feitelijke situatie.

De Betrokkene is degene op wie een Persoonsgegeven betrekking heeft. Tot de groep van Betrokkenen behoren in elk geval de personen die voorkomen in enige vorm van Cliëntregistratiesysteem. In dit systeem worden gegevens opgenomen van personen met wie de Financiële instelling om diverse redenen een relatie heeft. Deze personen worden generiek aangeduid met de term Cliënt. Het gaat dan om de volgende groepen van personen:

(i) personen met wie een overeenkomst is afgesloten;
(ii) personen met wie in het verleden een overeenkomst was afgesloten en van wie om diverse redenen de persoonsgegevens nog steeds moeten worden verwerkt;
(iii) personen die door een Financiële instellingen benaderd worden om een overeenkomst aan te gaan;
(iv) personen die zelf een Financiële instelling benaderen door het opvragen van informatie of het aanvragen van een offerte;
(v) personen van wie een Financiële instelling krachtens wettelijk voorschrift (bijvoorbeeld de

toestemming van de echtgenoot ex artikel 88 boek 1 BW) dan wel met het oog op geldende verjaringstermijnen, Persoonsgegevens dient te verwerken; en

(vi) personen van wie een Financiële instelling in verband met contractuele of wettelijke verplichtingen jegens een Cliënt, Verzekerde of derde Persoonsgegevens dient te verwerken.

Bij deze laatste groep betreft bijvoorbeeld het personen die een Verzekerde aansprakelijk stellen voor de door hen geleden schade als gevolg van een gebeurtenis waarvoor de Verzekerde in hun ogen aansprakelijk is. Dit laatste speelt bijvoorbeeld bij de medische aansprakelijkheid, waarbij een zorgverlener, bijvoorbeeld een ziekenhuis, aansprakelijk kan worden gesteld voor een verkeerde diagnose of behandeling. Aangezien het bij deze Verzekerde kan gaan zowel om een natuurlijke persoon als een rechtspersoon is dat uitdrukkelijk in de begripsbepaling tot uitdrukking gebracht. Anderzijds kan het ook gaan om zakelijke Betrokkenen, zoals tussenpersonen en hypothecaire adviseurs. Tot slot: ook een eenmansbedrijf zonder rechtspersoonlijkheid wordt als Betrokkene beschouwd, omdat gegevens over het bedrijf informatie bevatten over de persoon van de directeur of eigenaar, waarmee deze gegevens beschouwd moeten worden als Persoonsgegevens.

De Bewerker verwerkt Persoonsgegevens ten behoeve van de opdrachtgever, de Verantwoordelijke. De Bewerker heeft geen zeggenschap over de Verwerking, maar handelt slechts in overeenstemming met de instructies van de Verantwoordelijke. Als voorbeeld van de verhouding tussen Bewerker en Verantwoordelijke het volgende. Financiële instellingen hebben de afwikkeling van het betalingsverkeer in belangrijke mate uitbesteed aan Equens. Daarbij is het uitgangspunt dat de rol van Equens bestaat uit het uitvoering geven aan de opdrachten van de Financiële instellingen. Equens heeft geen zelfstandige bevoegdheid om de aan haar in het kader van het betalingsverkeer toevertrouwde Persoonsgegevens voor andere doeleinden te gebruiken. Equens is in die situatie Bewerker. Dat is anders voor zover er sprake is van zelfstandige diensten die door Equens worden aangeboden. In dat geval is Equens te beschouwen als Verantwoordelijke. In dat verlengde het volgende voorbeeld. Financiële instellingen maken gebruik van creditcardmaatschappijen om zodoende via Equens creditcardfaciliteiten aan te bieden aan Cliënten. Deze creditcardmaatschappijen dienen als Verantwoordelijken te worden beschouwd, omdat zij zelfstandig diensten aanbieden en in dat kader zelfstandig beslissen over de wijze waarop Persoonsgegevens, die door de Financiële instellingen aan de creditcardmaatschappij worden verstrekt, worden verwerkt. Financiële instellingen maken in de praktijk veelvuldig gebruik van IT-dienstverleners, aan wie Financiële instellingen bijvoorbeeld onderhoud en supportfuncties uitbesteden. Deze IT-dienstverleners dienen te worden beschouwd als Bewerker, omdat zij geen zelfstandige zeggenschap hebben over de Persoonsgegevens die in het kader van de dienstverlening aan de IT-dienstverlener ter beschikking worden gesteld, terwijl tevens ten behoeve van de Financiële instelling diensten worden verleend. Tot slot een laatste voorbeeld. Tussenpersonen, die bemiddelen ten behoeve van Financiële instellingen, dienen te worden beschouwd als Verantwoordelijken, omdat zij zelfstandige diensten aanbieden en zelfstandig beslissen over de Verwerking van Persoonsgegevens.

3. De reikwijdte

Toelichting

Voor toepasselijkheid van de Gedragscode op Financiële instellingen geldt de strikte eis dat: (i) banken lid dienen te zijn van de NVB; of (ii) banken dienen te zijn aangesloten bij Rabobank Nederland; of (iii) verzekeraars lid dienen te zijn van het Verbond. Dit betekent bijvoorbeeld dat wanneer een bank als assurantietussenpersoon optreedt ten behoeve van een verzekeraar de Gedragscode van toepassing is. De Gedragscode geldt bijvoorbeeld niet wanneer het een onafhankelijk tussenpersoon betreft of die bank niet is aangesloten bij de NVB of Rabobank Nederland. Het uitgangspunt dat de Gedragscode van toepassing is op Financiële instellingen, impliceert tevens dat

onderdelen van Financiële instellingen, die niet als bank of verzekeraar optreden, niet onder deze Gedragscode vallen, hoewel de Gedragscode wel op de Financiële instelling van toepassing is. Dat is bijvoorbeeld het geval bij een Financiële instelling, waarvan een afdeling bestaat uit rechtsbijstandverleners die rechtshulp verlenen aan personen die een rechtsbijstandsverzekering hebben afgesloten. Op de verzekeraar is in dat geval de Gedragscode wel van toepassing, echter niet op de rechtsbijstandsverlener, die in dezen vergelijkbaar is met een advocaat die een persoon in soortgelijke zaken bijstaat. Bovenstaande reikwijdte laat onverlet dat ook andere natuurlijke en rechtspersonen die niet vallen onder de definitie van Financiële instelling, zoals onafhankelijke tussenpersonen, rechtsbijstandverleners en schaderegelingskantoren, bevoegd zijn om (onderdelen van) de Gedragscode te onderschrijven.

Onder de reikwijdte van de Gedragscode valt niet de Verwerking van Persoonsgegevens van het personeel van een Financiële instelling. Evenmin valt de Verwerking van Persoonsgegevens van personen die: (i) in het Incidentenregister; of (ii) het Externe Verwijzingregister (hierna: EVR) zijn opgenomen, onder de reikwijdte van de Gedragscode. Op deze Verwerkingen is het Protocol Incidentenwaarschuwingssysteem Financiële Instellingen (hierna: Protocol) van toepassing (Bijlage I: Document B).

Voor zorgverzekeraars die lid zijn van het Verbond èn Zorgverzekeraars Nederland (ZN) geldt, zodra de Gedragscode Verwerking Persoonsgegevens Zorgverzekeraars is goedgekeurd door het CBP, tevens de Gedragscode Verwerking Persoonsgegevens Zorgverzekeraars. Hoewel beide codes op belangrijke onderdelen op elkaar zijn afgestemd valt een samenloop niet te vermijden. In het bijzonder kan daarbij gedacht worden aan de Verwerking van Persoonsgegevens omtrent iemands gezondheid. In dat geval heeft voor zorgverzekeraars de Gedragscode Verwerking Persoonsgegevens Zorgverzekeraars voorrang.

4. Beginselen van Verwerking van Persoonsgegevens

Toelichting

Onder Verwerking van Persoonsgegevens worden alle handelingen begrepen die met Persoonsgegevens worden verricht. Het betreft het verzamelen tot en met het vernietigen van de Persoonsgegevens, inclusief alle tussenliggende handelingen. De belangrijkste voorwaarden voor een rechtmatige Verwerking van Persoonsgegevens zijn: (i) het vaststellen van de doeleinden van de Verwerking; (ii) het vaststellen van een grondslag voor de Verwerking; en (iii) de informatieplicht die op de Verantwoordelijke rust. Hierna zullen deze voorwaarden worden toegelicht. Daarbij zal in verband met het vaststellen van de doeleinden uitvoerig worden ingegaan op het zogenaamd "verenigbaar gebruik", aangezien dit bepalend is voor de verdere Verwerking van Persoonsgegevens, zoals bijvoorbeeld de verstrekking.

Doeleinden van Verwerking van Persoonsgegevens (artikel 4.1 en artikel 4.2)

Persoonsgegevens mogen slechts voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld. Deze doeleinden moeten zijn vastgesteld of aangepast alvorens met de (aangepaste) Verwerking mag worden begonnen. Welbepaald houdt in dat de doelomschrijving duidelijk moet zijn. In artikel 5 Gedragscode worden de doeleinden voor de Verwerking van Persoonsgegevens door Financiële instellingen bepaald. Het doel waarvoor de Persoonsgegevens worden verzameld geldt als toetsingscriterium voor tal van andere bepalingen, zoals het verenigbaar gebruik, de bewaartermijnen en de voorwaarde dat niet meer Persoonsgegevens mogen worden verzameld dan voor het doel noodzakelijk is. Zie voor een uitvoerige

toelichting ten aanzien van de doeleinden, de toelichting bij artikel 5 Gedragscode.

Rechtmatige grondslag (artikel 4.3)

De Verwerking van Persoonsgegevens moet gebaseerd zijn op één van de in de WBP genoemde grondslagen. Deze zijn dan ook opgenomen in de Gedragscode. Indien geen van de grondslagen van toepassing is, is de Verwerking van Persoonsgegevens niet toegestaan. Er kunnen ook meerdere grondslagen worden vastgesteld. Dat zal vooral het geval zijn bij gebruik van Persoonsgegevens voor meerdere activiteiten. Financiële instellingen baseren de Verwerking van Persoonsgegevens met name op de grond dat de Verwerking noodzakelijk is voor het sluiten en uitvoeren van een overeenkomst met de Betrokkene, om te voldoen aan wettelijke verplichtingen of omdat de Verwerking noodzakelijk is voor het gerechtvaardigde belang van de Financiële instelling. Hieronder volgt een toelichting op deze door de Financiële instellingen veel gebruikte grondslagen.

De Persoonsgegevens zijn noodzakelijk voor de uitvoering van de overeenkomst waarbij de Betrokkene partij is of voor het nemen van precontractuele maatregelen
De eerste door Financiële instellingen veel gebruikte grondslag op basis waarvan het verwerken van Persoonsgegevens geoorloofd is betreft het verwerken van Persoonsgegevens indien dit noodzakelijk is voor de uitvoering van een overeenkomst waarbij de Betrokkene partij is. Dit is bijvoorbeeld het geval als iemand zijn bank opdracht geeft een bepaalde geldsom over te maken naar de rekening van een derde. De daarvoor noodzakelijke Verwerking door de bank van de Persoonsgegevens van de Betrokkene is een uitvloeisel van de rekeningcourantovereenkomst die deze persoon heeft met zijn bank. Het is overigens niet noodzakelijk dat de Verantwoordelijke zelf partij is bij de overeenkomst. Van belang is dat de Betrokkene partij is bij de overeenkomst. De Persoonsgegevens mogen ook worden verwerkt in de fase vóór het sluiten van de overeenkomst. Een voorbeeld hiervan is de Betrokkene die aan een bank verzoekt een rekening te openen of een offerte vraagt voor het aangaan van een hypothecaire lening of verzekering.

De Persoonsgegevens zijn noodzakelijk om een wettelijke verplichting na te komen waaraan de Verantwoordelijke is onderworpen
Financiële instellingen dienen in toenemende mate Persoonsgegevens te verwerken om te voldoen aan wettelijke verplichtingen. In dat verband kunnen met name de Wet op het financieel toezicht (hierna: Wft) en de Wet ter voorkoming van witwassen en financieren van terrorisme worden genoemd (hierna: Wwft). Zie de toelichting bij artikel 5 Gedragscode voor meer gedetailleerde informatie over de wettelijke verplichtingen waaraan Financiële instellingen zijn onderworpen.

De Persoonsgegevens zijn noodzakelijk voor het gerechtvaardigde belang van de Verantwoordelijke (of van een Derde aan wie de Persoonsgegevens worden verstrekt), tenzij het belang of de fundamentele rechten en vrijheden van de Betrokkene prevaleert
Om dit te beoordelen zal bij deze grondslag steeds een belangenafweging moeten plaatsvinden tussen beide in het geding zijnde belangen. Deze laatste grondslag geldt onder meer wanneer Persoonsgegevens worden verwerkt in het kader van marketingactiviteiten, het verrichten van het betalingsverkeer (waarbij bijvoorbeeld Persoonsgegevens van een begunstigde, niet zijnde de contractspartij, worden verwerkt), bij het risicobeheer en fraudebestrijding. Ook de verstrekking door een Financiële instelling aan een Derde kan op deze grondslag worden gebaseerd. Te denken valt onder meer aan het verstrekken van Persoonsgegevens aan een toezichthouder, (juridisch) adviseur of andere Financiële instelling in het kader van een onderzoek of een (mogelijke) juridische procedure.

Voor de goede orde: naast de hierboven uitgewerkte grondslagen verwerken Financiële instellingen ook Persoonsgegevens op grond van de overige in artikel 4.3 Gedragscode genoemde grondslagen, waaronder bijvoorbeeld ondubbelzinnige toestemming van de Betrokkene. Deze toestemming behoeft niet schriftelijk te worden verkregen. Toestemming kan ook blijken uit bepaalde gedragingen van de Betrokkene. Financiële instellingen kunnen de Betrokkene onder meer om toestemming vragen via het laten aankruisen van een vakje op een papieren of elektronisch document, waarbij de Financiële instelling de Betrokkene uiteraard zal informeren over de doeleinden van de Verwerking.

Verenigbaar gebruik (artikel 4.4)

Financiële instellingen hebben het doel voor het verwerken van Persoonsgegevens geconcretiseerd in meerdere activiteiten. Voor het verenigbaar gebruik betekent dit dat of, en in hoeverre, Persoonsgegevens die in het kader van de onder de doeleinden genoemde activiteiten zijn verkregen ook mogen worden verwerkt in het kader van andere activiteiten, afhankelijk is van de vraag of het doel van de aan de orde zijnde activiteit verenigbaar is met de desbetreffende activiteit of activiteiten waarvoor de Persoonsgegevens oorspronkelijk zijn verkregen.

Alvorens Persoonsgegevens verder te verwerken geeft de Financiële instelling zich er dan ook rekenschap van dat dit niet onverenigbaar is met de activiteit of activiteiten waarvoor de Persoonsgegevens zijn verkregen. Bij de beantwoording van de vraag of er sprake is van verenigbaar gebruik spelen diverse factoren een rol. Een aantal daarvan wordt - niet limitatief - opgesomd in artikel 9, lid 2 WBP, zoals verwantschap met het doel of de producten waarvoor de Persoonsgegevens werden verzameld, 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. Zo kunnen Persoonsgegevens gevoelig zijn door de context waarin zij worden gebruikt, bijvoorbeeld gegevens over iemands kredietwaardigheid of welstand. Hoe "gevoeliger" het Persoonsgegeven is, hoe minder snel mag worden aangenomen dat er sprake is van verenigbaar gebruik als bij de Verwerking wordt afgeweken van het oorspronkelijke doel. De factoren moeten in onderling verband worden beoordeeld en gewogen. 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 kunnen door het gebruik in een bepaalde context gevoelig van aard worden, terwijl de gevolgen voor de Betrokkenen ingrijpend zijn, zal er niet snel sprake zijn van verenigbaar gebruik. In geval de Betrokkene toestemming heeft gegeven voor de verdere Verwerking, wordt in ieder geval voldaan aan het vereiste van verenigbaar gebruik.

Het gaat bij verenigbaar gebruik dus om open normen die van geval tot geval moeten worden beoordeeld en gewogen om te kunnen vaststellen of een bepaalde gegevensuitwisseling geoorloofd is. Ter toelichting een aantal voorbeelden.

* In het kader van betaalopdrachten kunnen opdrachtgevers en begunstigden de beschikking krijgen over naam-, adres-, en woonplaatsgegeven (NAW-gegevens) die behoren bij een tegenrekening-nummer. Die informatie wordt met de betaling meegeleverd. Opdrachtgevers en begunstigden kunnen ook ten aanzien van specifieke betalingen navraag doen naar de gegevens van de tegenrekening. Dergelijke verzoeken worden bij de eigen bank ingediend. De bank behandelt de verzoeken met bancaire zorgvuldigheid. Indien de navraag duidelijk een doel heeft dat is gelegen buiten het betalingsverkeer wordt het verzoek geweigerd. Voorafgaand aan betaalopdrachten worden geen adres- en woonplaatsgegevens behorend bij een rekeningnummer verstrekt. Wel kunnen partijen in het kader van het betalingsverkeer vooraf verifiëren of naam en nummercombinaties correct zijn. Doel is om de

kans op fouten te minimaliseren.

* Indien zich bij de uitvoering van een overeenkomst onregelmatigheden voordoen mogen de medewerkers van de Financiële instelling Persoonsgegevens over de overeenkomst en de geconstateerde onregelmatigheden doorgeven aan Veiligheidszaken die kan bestaan uit een aparte afdeling of een daartoe geautoriseerde functionaris. Die mag deze Persoonsgegevens verder verwerken in het kader van het bestrijden van fraude en de gegevens, onder de voorwaarden genoemd in het Protocol (laten) opnemen in het Incidentenregister en het EVR.

* Uit betaalopdrachtgegevens kan door een bank informatie worden afgeleid met betrekking tot de mogelijke belangstelling van een Cliënt voor bepaalde financiële diensten uit het assortiment van de bank. Indien de bank deze informatie gebruikt voor het aanbieden van die diensten is sprake van verenigbaar gebruik. Zo kan een Cliënt die student is blijkens het feit dat de Cliënt studiefinanciering op zijn bankrekening ontvangt, door de bank worden benaderd voor een studentenrekening. Betaalopdrachtgegevens bestaan slechts uit identificerende gegevens van de opdrachtgever en de begunstigde en de informatie die daaruit kan worden afgeleid. Deze gegevens moeten worden onderscheiden van de gegevens die de opdrachtgever in het mededelingenveld bij de betaling vermeldt. Informatie opgenomen in het mededelingenveld mag niet worden gebruikt voor marketingactiviteiten.

* Binnen een Groep kan het bestaan van een vordering op een Betrokkene ertoe leiden dat informatie wordt uitgewisseld om na te gaan of bij een ander onderdeel van de Groep nog een uitkering onder een schadeverzekering verschuldigd is. Op die wijze kunnen de vordering en schuld met elkaar worden verrekend of, als dat niet mogelijk is, kan er derdenbeslag op de verschuldigde schadevergoeding worden gelegd.

* Een voorbeeld van verenigbaar gebruik is de bank die naar aanleiding van een afgesloten hypothecaire lening een schadeverzekeraar binnen de Groep wijst op de mogelijkheid om een mailing met betrekking tot een opstalverzekering aan de betreffende Cliënt te verzenden.

* Het is ook toelaatbaar als een ziektekostenverzekeraar NAW-gegevens en geboortedatum van zijn verzekerden verstrekt aan een tot dezelfde Groep behorende pensioenverzekeraar, om die in de gelegenheid te stellen de Betrokkenen door middel van een mailing te wijzen op het nut van het sluiten van een aanvullende pensioenverzekering. Dit kan niet worden aangemerkt als onverenigbaar met het doel waarvoor de Persoonsgegevens door de ziektekostenverzekeraar zijn verkregen. Bovendien heeft de ziektekostenverzekeraar binnen de Groep een gerechtvaardigd belang om haar Verwerking van Persoonsgegevens met betrekking tot de verzekerden op deze wijze te gebruiken ten dienste van de belangen van de andere entiteiten binnen de Groep, terwijl de privacybelangen van de verzekerden door deze handelwijze niet onevenredig worden geschaad. Dat is anders als de ziektekostenverzekeraar op basis van het "claimgedrag" van de verzekerden een selectie toepast en de resultaten van die selectie doorgeeft aan de eveneens tot de Groep behorende arbeidsongeschiktheidsverzekeraar. Een dergelijk gebruik is in de Gedragscode uitgesloten.

Kwaliteit van de Persoonsgegevens (artikel 4.5)

De kwaliteit van Persoonsgegevens omvat twee aspecten. Allereerst mogen niet meer Persoonsgegevens worden verwerkt dan noodzakelijk. Het doel van de Verwerking is bepalend voor de hoeveelheid en de soort Persoonsgegevens die mogen worden verwerkt. Dit volgt uit de woorden "toereikend, terzake dienend en niet bovenmatig". Daarnaast dienen Persoonsgegevens accuraat te zijn. Deze laatste voorwaarde gaat uit van een

inspanningsverplichting van de Verantwoordelijke. De Verantwoordelijke moet die maatregelen treffen die redelijkerwijs nodig zijn om er voor te zorgen dat de Persoonsgegevens juist en nauwkeurig zijn. Deze verplichting is dus niet absoluut.

Bewaartermijn (artikel 4.6)

Ten aanzien van het bewaren van Persoonsgegevens door een Financiële instelling het navolgende. De Verantwoordelijke dient zich af te vragen of er redenen zijn op grond waarvan de Persoonsgegevens vastgelegd kunnen blijven. Zijn daarvoor voldoende redenen dan kan de Verantwoordelijke bepalen welke termijnen gelden voor het bewaren van deze Persoonsgegevens. Daarbij is artikel 10, eerste lid WBP het uitgangspunt: Persoonsgegevens worden niet langer bewaard dan noodzakelijk is voor de verwerkelijking van de doeleinden waarvoor de gegevens zijn verzameld of vervolgens verwerkt. Een Financiële instelling 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.

Informatieplicht (artikel 4.7 tot en met artikel 4.9)

De ratio achter de informatieplicht is dat de Verantwoordelijke aanspreekbaar is voor de Betrokkene. 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. Bij het aangaan van een relatie met een Financiële instelling zal doorgaans uitdrukkelijk op het openings- c.q. aanvraagformulier worden aangegeven wat de doeleinden zijn waarvoor de Persoonsgegevens worden verzameld. Financiële instellingen kunnen de Betrokkene verder onder meer informeren over de Verwerking van Persoonsgegevens via klantvoorwaarden, deze Gedragscode, relevante websites en via een algemene melding bij het CBP. De informatieplicht geldt ook wanneer de Financiële instelling via internet met een Betrokkene communiceert en Persoonsgegevens verwerkt. In dat geval kan aan die plicht worden voldaan door het plaatsen van een privacy statement. Worden de Persoonsgegevens verzameld buiten de Betrokkene om, dan zal de informatieplicht gelden, tenzij de verstrekker de Betrokkene reeds op de hoogte heeft gesteld.

Als het informeren van de Betrokkene onmogelijk is of onevenredige inspanning kost vervalt de informatieplicht mits de herkomst van de Persoonsgegevens wordt vastgelegd. Indien het op een later tijdstip informeren van de Betrokkene zonder onevenredige inspanning kan plaatsvinden kan in een later stadium aan de informatieplicht worden voldaan, bijvoorbeeld op het moment dat met de Betrokkene schriftelijk contact wordt opgenomen. Het is algemeen geaccepteerd dat het ondoenlijk is om voorafgaand aan de werkelijke mailing een brief te moeten uitsturen waarin wordt aangegeven dat de Persoonsgegevens van de Betrokkene worden vastgelegd met als doel hen binnenkort een mailing te sturen. Het is daarom verdedigbaar dat de informatieplicht de ruimte biedt om deze te combineren met de werkelijke mailing.

Het doelbindingsbeginsel en de informatieplicht die rust op Financiële instellingen is niet absoluut. Naast de uitzonderingen genoemd in artikel 4.7 en artikel 4.8 Gedragscode vervalt de informatieplicht en het doelbindingsbeginsel indien wordt voldaan aan de uitzonderingen genoemd in artikel 9 Gedragscode.

Bewerker (artikel 4.12)

Financiële instellingen zijn vrij een Bewerker in te schakelen ten behoeve van de Verwerking van Persoonsgegevens. Deze Bewerker kan zich zowel binnen als buiten de Groep evenals in landen binnen de Europese Economische Ruimte (EER) als buiten de EER bevinden. Tussen de Bewerker en de Verantwoordelijke moet een overeenkomst worden gesloten, waarin schriftelijk of in een andere, gelijkwaardige vorm onder meer de technische en organisatorische beveiliging van de Verwerking van Persoonsgegevens wordt geregeld. Zie voor een uitleg over wanneer sprake is van een Bewerker de toelichting bij artikel 2 Gedragscode. Voor de regels die gelden wanneer sprake is van een Bewerker die zich in landen buiten de EER bevindt wordt verwezen naar de toelichting bij artikel 8 Gedragscode.

5. Doelen voor de Verwerking van Persoonsgegevens

Toelichting

Algemeen (artikel 5.1)

De doeleinden waarvoor een Financiële instelling Persoonsgegevens verwerkt hebben betrekking op het geheel aan activiteiten welke een Financiële instelling verricht in het kader van een efficiënte en effectieve bedrijfsvoering. De doeleinden zijn door de Financiële instellingen geconcretiseerd in meerdere activiteiten. In de eerste plaats betreft dat het beoordelen en accepteren van Cliënten en de mogelijk daaruit voortvloeiende activiteiten als het aangaan en uitvoeren van overeenkomsten en het afwikkelen van het betalingsverkeer. In de tweede plaats worden de Persoonsgegevens gebruikt om gerichte marketingactiviteiten te kunnen ontplooien, om de relatie met de Cliënt in stand te houden of uit te breiden, dan wel om nieuwe Cliënten te werven. Een derde activiteit betreft in algemene zin het risicobeheer: het bestrijden, voorkomen en opsporen van gedragingen die gericht zijn tegen de Financiële instelling of de sector in het algemeen. Daarnaast dienen Financiële instellingen in toenemende mate Persoonsgegevens te verwerken om te voldoen aan wettelijke verplichtingen. Bij deze activiteiten wordt het beheren van de relatie met de Cliënt steeds belangrijker, niet in het minst door de verplichtingen die op grond van wet- en regelgeving worden opgelegd zoals de uitvoering van het risicobeheer als de Customer Due Diligence (CDD). In dat verband kunnen met name de Wft en de Wwft worden genoemd.

Meer in het algemeen gaat het om activiteiten die van belang zijn voor een Financiële instelling als geheel om de relatie met de Cliënt te kunnen beheren en onderhouden. De activiteiten vormen een samenhangend geheel. Het gaat daarbij om de totale relatie met de Cliënt, waaronder mede wordt begrepen het Cliëntonderzoek, zoals dat op grond van de Wwft verplicht is. Alleen wanneer de activiteiten in samenhang worden uitgevoerd is het mogelijk dat de bedrijfsvoering op een effectieve en efficiënte manier verloopt. Samenhangend wil echter niet zeggen dat alle activiteiten ook zonder meer met elkaar verenigbaar zijn. Zo is het niet toegestaan om Bijzondere gegevens te gebruiken als selectiecriterium voor marketingactiviteiten, tenzij Betrokkene daarvoor zijn uitdrukkelijke toestemming heeft verleend. Dat kan bijvoorbeeld het geval zijn bij etnomarketing, waarbij allochtone bevolkingsgroepen worden benaderd voor (voor hen) specifieke producten. Gebruik van de Persoonsgegevens in het kader van de diverse activiteiten moet steeds getoetst worden aan de beginselen van de Verwerking van Persoonsgegevens.

Aangaan en uitvoeren van een overeenkomst (artikel 5.2)

Binnen de Financiële instellingen wordt in toenemende mate in het kader van efficiënte en effectieve bedrijfsvoering gewerkt met geïntegreerde cliëntinformatiesystemen. Deze systemen mogen alleen gebruikt worden door die medewerkers binnen de Financiële instelling die de Persoonsgegevens voor de vervulling van hun taak nodig hebben. Deze taakvervulling zal per medewerker verschillen en daarmee ook de toegang tot de Persoonsgegevens. De toegang tot de geïntegreerde cliëntsystemen beperkt zich niet tot de afzonderlijke rechtspersonen, maar kan gelden voor alle entiteiten binnen de Groep. Zie tevens artikel 5.4 Gedragscode.

Door een Financiële instelling worden in het kader van de normale afwikkeling van het betalingsverkeer Persoonsgegevens doorgegeven aan de wederpartij. Tevens worden, tenzij vooraf anders is overeengekomen, aanvullende Persoonsgegevens verstrekt aan de bij de verdere Verwerking van Persoonsgegevens betrokken partijen, voor zover deze redelijkerwijs noodzakelijk zijn voor verificatieen/ of reconstructiedoeleinden. Hierbij kan bijvoorbeeld gedacht worden aan het verstrekken van NAWgegevens van een (ten onrechte) begunstigde partij aan de opdrachtgever in verband met een foutieve betaalopdracht.

In het kader van de uitvoering van het betalingsverkeer worden door een Financiële instelling ook andere partijen zoals tussenpersonen en verwerkingscentra op diverse wereldwijde locaties ingeschakeld. Dit brengt met zich mee dat een Financiële instelling Persoonsgegevens kan doorgeven aan landen buiten de EER. Opdrachtgevers kunnen zowel tijdens als na de Verwerking voorwerp zijn van onderzoek door bevoegde nationale autoriteiten en bevoegde toezichthoudende organen van de landen waar degelijke gegevens zich vanwege het verwerkingsproces bevinden.

Statistische analyses (artikel 5.3)

Statistische analyses, waaronder begrepen creditscoring en datamining, waarbij Persoonsgegevens - niet zijnde Bijzondere Persoonsgegevens - worden verwerkt, zijn niet onverenigbaar met het doel waarvoor de Persoonsgegevens zijn verzameld. Creditscoring is een methode om het toekomstige betalingsgedrag van personen te voorspellen aan de hand van een aantal indicatoren. Datamining kan op vele gebieden worden toegepast bijvoorbeeld voor het analyseren van productieprocessen. Datamining kan worden gebruikt om al bestaande informatie uit een database te analyseren, met als doel verbanden bloot te leggen om zodoende bedrijfsprocessen te sturen. De bestaande informatie wordt daartoe in een datawarehouse opgenomen. Informatie binnen een datawarehouse is gerangschikt op de verschillende onderwerpen die voor een organisatie van belang kunnen zijn. Vervolgens wordt deze informatie geanalyseerd.

Bij deze analyse dient onderscheid te worden gemaakt tussen de fase waarbij profielen worden opgesteld en de fase waarbij op basis van dat profiel een score of kenmerk aan een persoon wordt toegerekend. Bij het opstellen van groepsprofielen mogen aan de invoerkant Persoonsgegevens worden verwerkt, mits maatregelen worden getroffen die bewerkstelligen dat bij de analyse de gegevens uitsluitend voor statistische doeleinden worden gebruikt. Deze maatregelen kunnen daaruit bestaan dat schriftelijk wordt vastgelegd dat de gegevens niet zullen worden gebruikt voor het nemen van maatregelen of besluiten gericht op een bepaald persoon. Het betreft een Verwerking die gelijk te stellen is met Verwerkingen voor statistische doeleinden, omdat het resultaat een profiel is dat niet aan een individuele persoon te relateren is.

Indien omgekeerd een persoon aan dat profiel of creditscore wordt gekoppeld is er wel sprake van Verwerking van Persoonsgegevens. In dat geval worden de Persoonsgegevens van een individuele Betrokkene vergeleken met

een profiel of score en gelden de ruimere bepalingen van het verenigbaar gebruik niet. Indien de toerekening aan een persoon geschiedt om deze te benaderen voor marketingactiviteiten dan is dat een Verwerking in het kader van marketing en zal getoetst moeten worden of een dergelijk gebruik verenigbaar is met het doel waarvoor de Persoonsgegevens zijn verkregen. De Betrokkene kan in dat geval gebruik maken van zijn recht van verzet.

Indien voor de statistische analyse wel Bijzondere Persoonsgegevens noodzakelijk zijn, dan is de uitdrukkelijke toestemming van de Betrokkene nodig, tenzij het vragen van toestemming onmogelijk is dan wel een onevenredige inspanning kost. Wel zal in dat geval getoetst moeten worden of ook voldaan is aan de aanvullende voorwaarden, namelijk dat de analyse een algemeen belang moet dienen, dat de Verwerking voor de betreffende analyse noodzakelijk is en dat er bij de uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de Betrokkene niet onevenredig wordt geschaad.

Marketingactiviteiten (artikel 5.4)

Met betrekking tot het gebruik van Persoonsgegevens voor marketingactiviteiten geldt het algemene beginsel dat de Verwerking behoorlijk en zorgvuldig moet zijn. Een uitwerking hiervan is dat bij voorkeur gebruik wordt gemaakt 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 artikel 4.8 Gedragscode. Dit betekent bijvoorbeeld dat, in het geval van externe inkoop van Persoonsgegevens met het oogmerk door middel van bijvoorbeeld verrijking of mailing de Betrokkene beter te benaderen, de Betrokkene van de marketingdoeleinden op de hoogte zal worden gesteld of indien dit onevenredig veel inspanning kost dat de herkomst van de Persoonsgegevens zal worden vastgelegd. Verder dient met bedrijven die als Bewerker optreden, zoals mailingbureaus, een bewerkersovereenkomst gesloten te worden. Ook dient steeds te worden gecontroleerd of de Betrokkene gebruik heeft gemaakt van zijn recht om van deze vorm van Verwerking verschoond te blijven.

Bij het verrichten van marketingactiviteiten kunnen verschillende middelen worden ingezet, zoals post, telefoon en elektronische middelen. Voor elk van deze middelen gelden aparte regels en voorwaarden. Aangezien deze vooral betrekking hebben op de daarbij aan een Betrokkene toegekende rechten, zijn deze regels en voorwaarden nader uitgewerkt bij het betreffende onderdeel (artikel 7.2 Gedragscode).

Cliënten die producten afnemen bij één onderdeel van een Groep kunnen door dat onderdeel, maar ook door andere onderdelen van die Groep worden benaderd in het kader van de marketing van producten. In beide gevallen blijven uiteraard alle voorwaarden als vermeld in de Gedragscode van toepassing. Indien de activiteit niet voortvloeit uit het doel van de activiteit waarvoor de Persoonsgegevens zijn verzameld, dient te worden nagegaan of de voorgenomen Verwerking daarmee niet onverenigbaar is. Bij deze afweging speelt onder meer de mate waarin de Cliënt is geïnformeerd over de samenstelling van de Groep een rol. Dat kan bijvoorbeeld gebeuren door middel van reclamespots of vermelding van de samenstelling van de Groep in communicatieuitingen richting de Cliënt. Indien een Cliënt op de een of andere wijze voldoende duidelijk is gemaakt dat de Financiële instelling deel uitmaakt van een Groep, kan de Cliënt door alle entiteiten van de Groep ten behoeve van marketingactiviteiten worden benaderd. Marketing van producten of diensten die door eenzelfde Groep op de markt worden aangeboden kunnen om die reden als verwant worden beschouwd. De Cliënt heeft altijd het recht verzet aan te tekenen.

In het kader van het betalingsverkeer kan onderscheid worden gemaakt tussen gegevens die worden verwerkt met het oog op de uitvoering van de betalingsopdracht, de zogenaamde opdrachtgegevens, en de gegevens

die door een Cliënt worden meegegeven in het mededelingenveld. De opdrachtgegevens mogen voor marketingdoeleinden worden gebruikt, mededelingen in het mededelingenveld niet.

Indien een Financiële instelling gebruik maakt van telemarketing zal de Financiële instelling voorafgaand aan dit gebruik in het zogeheten 'Bel me niet' register controleren of de Betrokkene heeft aangegeven van een dergelijke benadering verschoond te blijven.

Veiligheid en integriteit (artikel 5.5)

Binnen een Financiële instelling vormt Veiligheidszaken, die zich bezig houdt met de bestrijding van fraude en criminaliteit, vaak een afgezonderde eenheid. Deze afdeling legt onder meer gebeurtenissen vast die van belang zijn voor de veiligheid en integriteit van de Financiële sector en om die reden speciale aandacht behoeven. Het kan daarbij gaan om uiteenlopende gebeurtenissen als de melding van een gestolen laptop tot het vermoeden dat een bepaald persoon betrokken is bij een vorm van fraude of criminaliteit. Deze Persoonsgegevens worden vastgelegd in een zogeheten Gebeurtenissenadministratie. De Persoonsgegevens opgenomen in de Gebeurtenissenadministratie mogen in beginsel alleen gebruikt worden binnen de Financiële instelling of de Groep waartoe de Financiële instelling behoort. Om een oncontroleerbaar gebruik van deze Persoonsgegevens te voorkomen wordt een beperkte set aan gegevens (naam, adres, woonplaats en geboortedatum) opgenomen in een Intern Verwijzingsregister (IVR) dat in het kader van onder meer acceptatie en schadeafhandeling door de betreffende afdelingen geraadpleegd mag worden. Indien blijkt dat een Betrokkene in dit IVR voorkomt moet contact worden opgenomen met Veiligheidszaken, die vervolgens adviseert over de beslissing die moet worden genomen. Op deze Verwerking van Persoonsgegevens is de Gedragscode van toepassing en is een separate melding gedaan bij het CBP.

Het is onvermijdelijk dat ook medewerkers uit het cliëntbedrijf van de Financiële instelling een rol spelen bij de bestrijding van fraude en criminaliteit. Medewerkers uit het cliëntbedrijf van de Financiële instelling kunnen in dat kader bijvoorbeeld aan Veiligheidszaken melding doen van relevante gebeurtenissen, of indien nodig advies vragen over hoe met betrekking tot een bepaalde Cliënt te handelen. De Gedragscode is ook in die gevallen van toepassing.

Indien, na nader onderzoek, blijkt dat de gebeurtenis van zodanige aard is dat deze voldoet aan de voorwaarden genoemd in het Protocol worden de gegevens opgenomen in het Incidentenregister en, wanneer aan aanvullende voorwaarden is voldaan, in het EVR. Op deze Verwerkingen is niet de Gedragscode, maar het Protocol van toepassing.

In bepaalde gevallen worden Persoonsgegevens in verband met kredietaanvragen, vorderingen en gebeurtenissen mede vastgelegd in registers die worden gehouden door een van de Financiële instelling onafhankelijke rechtspersoon. Voorbeelden zijn Stichting BKR en Stichting CIS die respectievelijk optreden als Verantwoordelijke voor het Centrale Krediet Informatiesysteem (hierna: CKI) en voor de Speciale Meldingen en het Systeem Vertrouwelijke Mededelingen (SVM). Op het verstrekken aan en het onttrekken van Persoonsgegevens aan deze systemen is deze Gedragscode van toepassing. De Verwerking van de Persoonsgegevens in de systemen zelf vallen buiten de Gedragscode.

Een bijzondere 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. 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 (Bijlage I: Document C).

Verwerking van Persoonsgegevens in verband met wettelijke voorschriften (artikel 5.6)

De afgelopen jaren kenmerken zich door een toename in het aantal verplichtingen om Persoonsgegevens op grond van wettelijke voorschriften te verzamelen en beschikbaar te stellen. Naast voorschriften die min of meer logisch uit de wetgeving rond Financiële instellingen voortvloeien, zoals de verzekeringswetgeving, is daarbij in het bijzonder de verplichting bijgekomen van het Cliëntenonderzoek, ook wel de Customer Due Diligence (CDD) genoemd. Zo is ter uitvoering van de richtlijnen 2005/60/EG en 2006/70/EG de Wet ter voorkoming van witwassen en financieren terrorisme (Wwft) geïmplementeerd. Deze wet is een samenvoeging van de Wet ter identificatie bij dienstverlening (Wid) en Wet Melding ongebruikelijke transacties (MOT).

De Wwft eist dat de gegevens van het document waarmee de identiteit is vastgesteld moeten worden vastgelegd. De vastlegging van de gegevens is in lijn met de verplichting tot uitvoeren van het Cliëntenonderzoek uit de Wwft. Aangezien de Wwft riskbased is, betekent dit dat de Financiële instelling de mogelijkheid heeft om het Cliëntenonderzoek af te stemmen op de risicogevoeligheid voor witwassen of financiering van terrorisme van het type Cliënt, 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. Net als bij de Wid en de Wet MOT is in de Wwft een belangrijke rol weggelegd voor toezichthouders. Als bewijsmateriaal voor identificatie en verificatie - twee eisen uit de Wwft - mogen Financiële instellingen - net als onder de WID - het 'kopietje paspoort' opnemen in hun administratie. De Wwft schrijft (samengevat) twee activiteiten voor op het gebied van Cliëntenonderzoek en de Melding van ongebruikelijke transacties. Voor de goede orde wordt opgemerkt dat er daarnaast nog vele wettelijke voorschriften bestaan op grond waarvan een Financiële instelling verplicht is bepaalde Persoonsgegevens te verwerken.

In veel gevallen moeten Financiële instellingen het burgerservicenummer in hun administratie opnemen. Daarnaast dienen ook achtergrondgegevens van Cliënten te worden verzameld en gecontroleerd. Een voorbeeld hiervan is de Wet op het financieel toezicht (Wft) die voorschrijft dat bij het verlenen van krediet altijd getoetst moet worden aan een stelsel van kredietregistraties, zoals bijvoorbeeld het Centraal Krediet Informatiesysteem (CKI) dat door de Stichting BKR wordt bijgehouden. Ook schrijft deze wet voor dat steeds informatie moet worden ingewonnen over de financiële positie van de kredietnemer. De uitwerking in het Besluit prudentiële regels gaat nog een stap verder en stelt dat de Financiële instelling moet zorgen voor een systematische analyse van integriteitsriscico's. Onderdeel hiervan is dat dit beleid zijn weerslag vindt in procedures en maatregelen die op een onafhankelijke wijze getoetst moeten worden. 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 deze adviseren over complexe producten (o.a. bepaalde levensverzekeringen).

Van geheel andere orde is de plicht om op vordering van opsporingsambtenaren of toezichthouders gegevens ter beschikking te stellen. Bij een bevel tot het beschikbaar stellen van informatie gaat het soms alleen om identificerende gegevens als naam, adres, woonplaats of geboortedatum behorend bij een bankrekening of verzekeringspolisnummer. In andere gevallen kan bijvoorbeeld de officier van justitie om meer gegevens vragen zoals de duur, de aard van de dienstverlening, informatie over rekeningen en betalingsverkeer. Het komt ook voor

dat om Bijzondere Persoonsgegevens wordt gevraagd.

6. Verwerking van Bijzondere Persoonsgegevens

Toelichting

Persoonsgegevens omtrent iemands gezondheid (artikel 6.1)

Voor de Verwerking van Persoonsgegevens door een Financiële instelling omtrent iemands gezondheid geldt een aantal aanvullende voorschriften.

Het is een Financiële instelling onder voorwaarden toegestaan Persoonsgegevens omtrent iemands gezondheid te verwerken. De voorwaarden waaronder dat kan zijn verwoord in artikel 6.1 Gedragscode. Een Financiële instelling kan bijvoorbeeld Persoonsgegevens omtrent iemands gezondheid verwerken indien dat noodzakelijk is voor de beoordeling van een Cliënt, de acceptatie van een Cliënt of het uitvoeren van een overeenkomst met een Cliënt. Dit is onder meer het geval indien een Cliënt met een Financiële instelling een overeenkomst ten aanzien van een hypotheek of levensverzekering wenst aan te gaan.

Bij de beoordeling van de gezondheidstoestand en de daaraan verbonden risico's in verband met acceptatie of een aanspraak op verzekering van een (aspirant)verzekerde speelt de Medisch adviseur een centrale rol. Hij stelt een medisch onderzoek in, waarbij onder strikte voorwaarden tevens een keuringsarts kan worden ingeschakeld, en deelt de uitslag en gevolgtrekking als onderdeel van zijn gemotiveerd advies mede aan de verzekeraar. De Medisch adviseur is verantwoordelijk voor alle Verwerkingen van Persoonsgegevens omtrent iemands gezondheid die door hem, en de personen die onder zijn verantwoordelijkheid aan het onderzoek werken, plaatsvinden. De kring van personen die onder zijn verantwoordelijkheid werken wordt aangeduid met medische staf of medische dienst. Bij het aangaan van een verzekering heeft de Betrokkene het recht om als eerste kennis te nemen van de uitslag en gevolgtrekking van het onderzoek als bedoeld in artikel 7:464, tweede lid, onder b WGBO en mag op grond daarvan beslissen of de uitslag en gevolgtrekking aan anderen mogen worden medegedeeld. Teneinde gebruik te kunnen maken van deze rechten dient de Betrokkene de verzekeraar schriftelijk om deze gegevens te verzoeken.

De verzekeraar neemt op basis van het advies van de Medisch adviseur een beslissing over de acceptatie of schadeafhandeling. Gezondheidsverklaringen moeten worden gezonden naar de Medisch adviseur of zijn medische dienst of staf. Het is onvermijdelijk dat Persoonsgegevens omtrent iemands gezondheid, anders dan de Gezondheidsverklaring, ter kennis komen van personen die met de besluitvorming over acceptatie of schadeafhandeling zijn belast. Zij kunnen deze Persoonsgegevens rechtstreeks krijgen van een (potentiële) verzekerde, maar ook van de Medisch adviseur. Zo wordt bij het indienen van een claim in het geval van bijvoorbeeld letselschade vaak ongevraagd door gelaedeerde aangegeven wat de aard van het letsel is. Het is ter beoordeling en verantwoordelijkheid van deze Medisch adviseur om vast te stellen welke gegevens omtrent iemands gezondheid ten behoeve van het nemen van een beslissing strikt noodzakelijk zijn en mogen worden verstrekt. De acceptant en schadebehandelaar mogen deze gegevens uitsluitend gebruiken in het kader van die acceptatie of schadeafhandeling. Op deze wijze wordt een scheiding aangebracht tussen de beoordeling van de gezondheidstoestand in de vorm van een advies van de Medisch adviseur en de beslissing die mede op grond daarvan wordt genomen door de verzekeraar. De acceptant en schadebehandelaar hebben in dat kader op grond van artikel 21, tweede lid WBP een geheimhoudingsplicht uit hoofde van ambt, beroep of wettelijk voorschrift, dan

wel krachtens overeenkomst. Het is eveneens ter beoordeling en verantwoordelijkheid van de Medisch adviseur om vast te stellen welke gegevens omtrent iemands gezondheid ten behoeve van het geven van een advies mogen worden verstrekt aan diegenen die werkzaam zijn binnen de medische dienst/medische staf.

Ook in het kader van het afwikkelen van het betalingsverkeer verwerkt een Financiële instelling gegevens omtrent iemands gezondheid. Dit is onder meer het geval indien het mededelingenveld in het kader van een betaalopdracht gegevens omtrent iemands gezondheid bevat.

Het is een Financiële instelling toegestaan Persoonsgegevens omtrent iemands gezondheid (verder) te verwerken indien de Financiële instelling daartoe de uitdrukkelijke toestemming van de Betrokkene heeft verkregen.

Persoonsgegevens omtrent iemands gezondheid die zijn verwerkt met het oog op de beoordeling van een Cliënt, de acceptatie van een Cliënt en het uitvoeren van een overeenkomst met een Cliënt gericht op een specifiek product zullen zonder toestemming van de Betrokkene niet worden gebruikt in het kader van de beoordeling van een Cliënt, de acceptatie van een Cliënt of het uitvoeren van een overeenkomst met een Cliënt ten behoeve van een ander product. Indien bijvoorbeeld gegevens omtrent iemands gezondheid door een Financiële instelling worden verwerkt in het kader van een levensverzekering die de Betrokkene met de Financiële instelling wenst aan te gaan, mogen deze gegevens door de Financiële instelling niet worden gebruikt in het kader van een arbeidsongeschiktheidsverzekering. Dit is wel toegestaan indien de Betrokkene daarvoor uitdrukkelijk toestemming geeft.

Niet onder de verantwoordelijkheid van de Medisch adviseur valt de Verwerking van Persoonsgegevens noodzakelijk in het kader van de uitvoering van de overeenkomst. Zo valt niet onder de verantwoordelijkheid van de Medisch adviseur de Verwerking van Persoonsgegevens omtrent iemands gezondheid in het kader van het opstellen van declaraties of in het kader van juridische procedures of de behandeling van klachten. Evenmin vallen daaronder de Verwerkingen waarbij bepaalde gegevens omtrent de gezondheid, die zijn medegedeeld door of namens de Betrokkene in verband met het beheer van de relatie met de Cliënt, opgeslagen worden in de administratie. Het kan gaan om specifieke situaties, waarbij op grond van gegevens omtrent gezondheid vanuit een zorgplicht maatregelen moeten worden genomen met betrekking tot beleggingen of vermogensbeheer. Te denken valt aan vormen van ernstige ziekte of dementie.

Als aanvullend onderzoek plaatsvindt of als Persoonsgegevens bij anderen dan de Betrokkene worden verzameld wordt de uitdrukkelijke toestemming van de Betrokkene gevraagd.

Voor zeer specifieke verwerkingen van Persoonsgegevens betreffende iemands gezondheid, zoals Persoonsgegevens omtrent erfelijkheid en HIV, zijn aparte gedragsregels opgesteld. Deze regels zijn vastgelegd in respectievelijk het "Moratorium erfelijkheidsonderzoek" en de "HIV-gedragscode".

Persoonsgegevens van strafrechtelijke aard (artikel 6.2)

Voor de Verwerking van Persoonsgegevens van strafrechtelijke aard door een Financiële instelling geldt een aantal aanvullende voorschriften.

Het is een Financiële instelling onder voorwaarden toegestaan Persoonsgegevens van strafrechtelijke aard te verwerken. De voorwaarden waaronder dat kan zijn verwoord in artikel 6.2 Gedragscode. Een Financiële instelling

kan bijvoorbeeld Persoonsgegevens van strafrechtelijke aard verwerken indien dat noodzakelijk is voor de beoordeling van een Cliënt, de acceptatie van een Cliënt of het uitvoeren van een overeenkomst met een Cliënt. Zo wordt bijvoorbeeld bij de aanvraag van een verzekering gevraagd naar het strafrechtelijk verleden van de aanvrager en anderen voor zover dat voor het afsluiten van een verzekering noodzakelijk is. Het gaat hierbij om feiten uit de laatste acht jaar. Ook kan een Financiële instelling gegevens van strafrechtelijke aard verwerken als dat noodzakelijk is in het kader van de veiligheid en integriteit van onder meer de Financiële sector. Zo kunnen door een Financiële instellingPersoonsgegevens van strafrechtelijke aard met betrekking tot fraude en criminaliteit door Veiligheidszaken worden verwerkt. Indien dat noodzakelijk is voor de bevordering van veiligheid en integriteit mogen in aanvulling op de strafrechtelijke gegevens ook andere Bijzondere Persoonsgegevens worden verwerkt. Gegevens van strafrechtelijk aard mogen door een Financiële instelling altijd worden verwerkt indien de Financiële instelling daartoe de toestemming van de Betrokkene heeft verkregen.

Persoonsgegevens die betrekking hebben op strafbare feiten die zijn of op grond van feiten en omstandigheden naar verwachting zullen worden begaan jegens een van de in een Groep verbonden Financiële instellingen kunnen door de Financiële instelling worden verstrekt binnen de Groep. Dit geldt ook voor Persoonsgegevens die dienen ter vaststelling van mogelijk strafbaar gedrag jegens een van de in de Groep verbonden Financiële instellingen. Dit op voorwaarde dat de gegevens uitsluitend worden verstrekt aan functionarissen die de gegevens voor de uitoefening van hun taaknodig hebben, alsmede aan politie en Justitie.

Aan functionarissen buiten de Groep mogen deze Persoonsgegevens slechts worden verstrekt indien het Protocol wordt onderschreven en nageleefd.

Andere Bijzondere Persoonsgegevens (artikel 6.3)

Naast Persoonsgegevens omtrent gezondheid en strafrechtelijke gegevens kunnen onder meer in de volgende situaties nog andere Bijzondere Persoonsgegevens door Financiële instellingen worden verwerkt. In de eerste plaats gaat het om gegevens die worden meegeleverd, bijvoorbeeld in het mededelingenveld van een betaalopdracht. Het kan dan gaan om de vermelding dat het de betaling van het lidmaatschap van een politieke partij of kerkgenootschap betreft. De Verwerking van Persoonsgegevens vindt onder meer plaats door het archiveren van de originele bescheiden of van de al dan niet elektronische afschriften daarvan. Verder wordt in sommige gevallen het burgerservicenummer (BSN) in de administratie van een Financiële instelling opgenomen. Als aangegeven in artikel 5.6 Gedragscode gebeurt dat alleen wanneer daarvoor een wettelijke grondslag aanwezig is. De Persoonsgegevens mogen in dat geval alleen gebruikt worden voor het aangegeven doel. Het kan tevens gaan om Persoonsgegevens betreffende etniciteit, die alleen met de uitdrukkelijke toestemming van een Betrokkene, gebruikt mogen worden voor marketingactiviteiten.

7. Rechten van Betrokkenen

7.1 Kennisneming en correctie

Toelichting

In de WBP zijn rechten toegekend aan de Betrokkene: het recht kennis te nemen van de eigen Persoonsgegevens en het recht om deze Persoonsgegevens te verbeteren, aan te vullen, te verwijderen of af te schermen. Daarnaast heeft Betrokkene het recht van verzet en het recht verschoond te blijven van een besluit genomen op basis van

uitsluitend een geautomatiseerde Verwerking van Persoonsgegevens.

Recht om van de gegevens kennis te nemen en deze eventueel te corrigeren (artikel 7.1)

Een Betrokkene is gerechtigd - met redelijke tussenpozen - een Financiële instelling schriftelijk een overzicht te vragen van de Persoonsgegevens van de Betrokkene die door die Financiële instelling worden verwerkt. 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. De Verantwoordelijke dient dit overzicht binnen vier weken na de datum van ontvangst van het verzoek aan de Betrokkene te verstrekken.

Een Financiële instelling hoeft geen gehoor te geven aan een verzoek tot inzage indien wordt voldaan aan het bepaalde in artikel 9 Gedragscode. Zo kan inzage worden geweigerd als het om zaken gaat zoals de veiligheid van de Financiële instelling en voorkoming, opsporing en vervolging van strafbare feiten. Een ander voorbeeld is de situatie dat naast de Persoonsgegevens van de Betrokkene ook Persoonsgegevens verwerkt worden van een Derde die bedenkingen kan hebben tegen het verlenen van inzage in ook zijn of haar Persoonsgegevens. In dat geval moet beoordeeld worden of in het geheel niets verstrekt kan worden of dat het mogelijk is de gegevens waartegen bedenkingen zijn geuit weg te laten of weg te lakken.

Afhankelijk van de omstandigheden kan het nodig zijn dat kopieën worden verstrekt van documenten of kopieën of uittreksels van de gegevensdragers waarop de Persoonsgegevens zijn vastgelegd. Hiervan kunnen zijn uitgezonderd: (i) documenten waarover de Betrokkene reeds beschikt (omdat bijvoorbeeld reeds een kopie is verstrekt) en hij zich een oordeel heeft kunnen vormen en (ii) de vastlegging van persoonlijke gedachten van medewerkers die onder meer bedoeld zijn voor intern overleg en beraad. Het verzoek om kopieën mag in aanvulling op het bepaalde in artikel 9 Gedragscode bovendien worden geweigerd indien sprake is van misbruik door de Betrokkene of het verzoek leidt tot een disproportionele belasting van de Financiële instelling en tot aantasting van de rechten of belangen van derden.

Bij de uitleg van het inzagerecht wordt rekening gehouden met jurisprudentie, zoals bijvoorbeeld de Dexia uitspraak.

Als onderdeel van het inzagerecht heeft de Betrokkene het recht informatie te krijgen over de logica die ten grondslag ligt aan de geautomatiseerde Verwerking indien gebruik wordt gemaakt van bijzondere computerprogrammatuur. Gedacht kan worden aan dataminingsprogramma's en het opstellen van creditscores. De bekendmaking van de logica mag geen afbreuk doen aan het zakengeheim of aan het intellectuele eigendom en met name aan het auteursrecht dat de software beschermt. Dit mag er echter niet toe leiden dat alle informatie wordt geweigerd.

Met betrekking tot het inzagerecht geldt nog een aanvullende bepaling. De Verantwoordelijke moet zorg dragen 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 kan in voorkomende gevallen de Verantwoordelijke verzoeken de Persoonsgegevens te verbeteren,

aan te vullen, te verwijderen of af te schermen indien deze feitelijk onjuist zijn, voor het doel of de doeleinden van de Verwerking onvolledig of niet ter zake dienend dan wel anderszins in strijd met een wettelijk voorschrift worden verwerkt. Bij het afschermen betreft het situaties waarbij de Persoonsgegevens niet verwijderd kunnen worden omdat ze bijvoorbeeld mogelijk in een procedure gebruikt moeten worden. In dat geval dienen technische of organisatorische maatregelen te worden genomen om ander gebruik te voorkomen.

Indien een Verantwoordelijke voldaan heeft aan een verzoek om gegevens te verbeteren, aan te vullen, te verwijderen of af te schermen, dan is hij verplicht aan Derden aan wie de betreffende Persoonsgegevens zijn verstrekt kennis te geven van de aangebrachte wijzigingen, tenzij dit onmogelijk is of een onevenredige inspanning kost.

Recht van verzet en toestemming (artikel 7.2)

In de WBP is het stelsel van verzet gespecificeerd en wordt onderscheid gemaakt tussen relatieve en absolute verzoeken om verzet. Relatieve verzoeken kunnen worden ingediend indien de rechtsgrond van de Verwerking gelegen is in de behartiging van het gerechtvaardigde belang van de Verantwoordelijke. De Betrokkene kan dan op grond van zijn bijzondere persoonlijke omstandigheden verzoeken om de Verwerking van zijn Persoonsgegevens te beëindigen. De Verantwoordelijke dient in dat concrete geval de Verwerking te heroverwegen en zijn belang af te wegen tegen het (bijzondere) belang van de Betrokkene.

Dit relatieve verzet moet nadrukkelijk onderscheiden worden van het verzet dat mogelijk is bij het gebruik van Persoonsgegevens voor commerciële, charitatieve of ideële doeleinden. In dat geval geldt een geschakeerde regeling, afhankelijk van het medium dat wordt gebruikt.

Het gebruik van automatische oproepsystemen zonder menselijke tussenkomst of faxen voor Direct marketing is uitsluitend toegestaan indien de Betrokkene daarvoor voorafgaand toestemming heeft verleend (“opt-in”).

Voor het gebruik van contactgegevens voor het aanbieden van producten en diensten per telefoon of per post geldt het minder zware regime van “opt-out”. Gebruik is toegestaan zolang de Betrokkene niet te kennen heeft gegeven dit gebruik te willen laten blokkeren. Wel moet de Betrokkene bij elk gebruik van zijn Persoonsgegevens voor marketingdoeleinden gewezen worden op de mogelijkheid van”opt-out”. In dat geval dient het gebruik terstond te worden beëindigd.

Bij het gebruik van de telefoon dient de Betrokkene te worden gewezen op het bestaan van het ‘bel-meniet’ register waarin alle verzoeken om een blokkade worden opgenomen. Tevens dient een Financiële instelling voor het benaderen van een Betrokkene via de telefoon voor Direct Marketing met betrekking tot beleggingsproducten, voorafgaand toestemming te hebben verkregen van de Betrokkene (“opt-in”).

Een Financiële instelling die elektronische contactgegevens voor elektronische berichten (zoals e-mail, sms-berichten, mms-berichten) heeft verkregen in het kader van de verkoop van een financieel product of het verlenen van een financiële dienst mag deze gegevens gebruiken voor Direct Marketing ten behoeve van eigen gelijksoortige financiële producten of financiële diensten (“soft opt-in”). In dat geval moet de Betrokkene wel steeds gewezen worden op zijn absolute recht van verzet om dit gebruik terstond te laten beëindigen (“opt-out”).

Het onttrekken en gebruiken van Persoonsgegevens uit de apparatuur van een Betrokkene (cookies) is slechts

toegestaan wanneer de Persoonsgegevens noodzakelijk zijn om de werking van het systeem te beoordelen of om te kunnen voldoen aan een verzoek van de Betrokkene. Elk ander gebruik is slechts geoorloofd indien de Betrokkene over dat gebruik in alle openheid is geïnformeerd en hij niet te kennen heeft gegeven met een dergelijk gebruik niet akkoord te gaan.

Vergoeding van kosten (artikel 7.3)

Voor een verzoek om inzage in de eigen gegevens of gebruik van het relatieve verzet kan de Verantwoordelijke een vergoeding in de kosten verlangen, die niet hoger mag zijn dan een bij algemene maatregel van bestuur vastgesteld bedrag. Dat bedrag is vastgesteld op € 0,23 per pagina tot een maximum van € 4,50. Dat maximum of zelfs meer tot een maximum van € 22,50 mag ook gevraagd worden wanneer het gaat om vanwege hun aard moeilijk toegankelijke verwerkingen of wanneer het om veel afschriften gaat.2

2 Besluit kostenvergoeding rechten betrokkenen WBP (Stb. 2001, 305). Zie ook uitspraak CBP, z2006- 00052.

Besluit gebaseerd op geautomatiseerde verwerking (artikel 7.4)

De Verantwoordelijke dient er zorg voor te dragen dat de Betrokkene niet wordt onderworpen aan een besluit uitsluitend gebaseerd op een geautomatiseerde verwerking, indien aan dat besluit rechtsgevolgen zijn verbonden of indien dat besluit de Betrokkene in aanmerkelijke mate treft. Het betreft met name besluiten die worden genomen op basis van geautomatiseerde Verwerkingen die bedoeld zijn om een beeld te krijgen van bepaalde aspecten van iemands persoonlijkheid.

De bepaling is niet absoluut en geeft aan dat er situaties zijn waarin een dergelijk besluit is geoorloofd, zoals wanneer een besluit wordt genomen in het kader van het sluiten of het uitvoeren van een overeenkomst en passende maatregelen zijn genomen, dan wel wanneer het besluit zijn grondslag vindt in een wet, waarin maatregelen zijn vastgesteld die strekken tot bescherming van het gerechtvaardigde belang van de Betrokkene. In dat verband kan gedacht worden aan het sluiten van een verzekerings- of financieringsovereenkomst en aan artikelen 4:32 en 4:34 Wft. De passende maatregelen bestaan uit de gelegenheid die wordt geboden aan de Betrokkene om zijn zienswijze kenbaar te maken. Bij een negatief besluit moet de Betrokkene de logica medegedeeld worden die ten grondslag ligt aan de geautomatiseerde Verwerking van Persoonsgegevens.

8. Speciale onderwerpen

Toelichting

Functionaris voor de Gegevensbescherming (artikel 8.1)

De WBP biedt de mogelijkheid om een Functionaris voor de Gegevensbescherming aan te stellen. De Functionaris kan optreden als (interne) toezichthouder. De aanstelling van een dergelijke Functionaris is facultatief.
Alleen indien de Functionaris is aangemeld bij het CBP is het toegestaan de melding van de Verwerking van Persoonsgegevens bij deze door de Verantwoordelijke aangestelde Functionaris te doen plaatsvinden. Aanvragen voor een voorafgaand onderzoek mogen alleen worden gemeld bij het CBP. Om zijn toezicht daadwerkelijk te kunnen uitvoeren, is het noodzakelijk dat de Functionaris toegang heeft tot alle systemen waar mogelijk Persoonsgegevens worden verwerkt.

Gegevensverkeer met landen buiten de EER (artikel 8.2)

Internationaal gegevensverkeer is van belang voor Financiële instellingen. Voor een Financiële instelling is dat veelal een voortvloeisel van de taken die moeten worden uitgeoefend als het doen van betalingsverkeer en het uitvoeren van verzekeringsovereenkomsten. Bij de uitvoering van dergelijke opdrachten worden noodzakelijkerwijs ook andere partijen zoals tussenpersonen en/of verwerkingscentra op diverse wereldwijde locaties ingeschakeld. Opdrachtgevers kunnen daardoor zowel tijdens als na de verwerking voorwerp zijn van onderzoek door bevoegde nationale autoriteiten van landen waar dergelijke Persoonsgegevens zich vanwege het verwerkingsproces bevinden.

Doorgifte van Persoonsgegevens naar landen binnen de EER is altijd geoorloofd. De gelaagdheid van de regelgeving op het gebied van doorgifte van Persoonsgegevens naar landen buiten de EER ligt voor Financiële instellingen anders dan voor andere Verantwoordelijken, omdat primair de nadruk ligt op het bepaalde in artikel 8.2.3 Gedragscode. Dat artikellid geeft uitdrukkelijk aan dat uitwisseling en doorgifte van Persoonsgegevens geoorloofd is wanneer dat noodzakelijk is voor onder meer de uitvoering van een overeenkomst tussen een Betrokkene en de Verantwoordelijke of wanneer dat noodzakelijk is voor de sluiting of uitvoering van een in het belang van de Betrokkene te sluiten overeenkomst. Het kan daarbij bijvoorbeeld gaan om internationaal betalingsverkeer in opdracht van Betrokkenen, herverzekering of om gegevens uitwisseling in verband met schade of ongeluk in het buitenland. Ook kan doorgifte plaatsvinden indien daartoe ondubbelzinnige toestemming is verkregen van de Betrokkene bijvoorbeeld via klantvoorwaarden of wanneer het noodzakelijk is in verband met een zwaarwegend algemeen belang. Dit belang kan de omstandigheid omvatten dat een Financiële instelling onderworpen is aan (buitenlandse) wetgeving en/of regelgeving van (buitenlandse) toezichthouders waardoor Persoonsgegevens onder meer op grond van (buitenlandse) exploten dienen te worden doorgegeven. Indien de Financiële instelling in dit specifieke geval gehouden is Persoonsgegevens door te geven zal de Financiële instelling aanvullende passende maatregelen nemen teneinde de belangen van de Betrokkene te beschermen en zo nodig met het CBP in overleg treden.

In het geval geen beroep kan worden gedaan op een van de bepalingen van artikel 8.2.3 Gedragscode geldt dat doorgifte naar landen buiten de EER is toegestaan indien sprake is van een passend beschermingsniveau. Van een passend beschermingsniveau wordt onder meer gesproken indien de Europese Commissie heeft besloten dat een betreffend land passende waarborgen biedt ter bescherming van de persoonsgegevens. Ook kunnen bijvoorbeeld door implementatie van goedgekeurde Binding Corporate Rules binnen een Groep wereldwijd passende waarborgen worden geboden. Binding Corporate Rules zijn regels die binnen een Groep wereldwijd bindend voorschrijven hoe men Persoonsgegevens dient te verwerken. Indien Binding Corporate Rules binnen de Groep zijn geïmplementeerd kunnen de Persoonsgegevens binnen de Groep worden uitgewisseld conform het bepaalde in de Binding Corporate Rules. In het geval van doorgifte van Persoonsgegevens aan een Bewerker of Verantwoordelijke in de Verenigde Staten kan gebruik worden gemaakt van de regeling als vastgelegd in de Safe Harbor Principles, indien de ontvangende partij zich hieraan heeft gecommitteerd. Doorgifte door een Financiële instelling is altijd toegestaan indien daartoe een vergunning op grond van artikel 77 lid 2 WBP is afgegeven.

Beveiliging van Persoonsgegevens (artikel 8.3)

Financiële instellingen vinden beveiliging van groot belang en treffen in verband met de elektronische uitwisseling van Persoonsgegevens dan ook passende maatregelen. Bijna steeds is een beveiligingsbeleid ontwikkeld, waarin

concreet wordt aangegeven welke organisatorische en technische maatregelen genomen moeten worden om Persoonsgegevens te beschermen tegen diefstal en 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.

Cameratoezicht (artikel 8.4)

Het is een Financiële instelling toegestaan onder de in artikel 8.4 Gedragscode genoemde voorwaarden gebruik te maken van camera's. Zo geldt dat cameratoezicht geoorloofd is wanneer dat noodzakelijk is voor de beveiliging van een Financiële instelling of haar Cliënten 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 Cliënt 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.

Opnemen van telefoongesprekken (artikel 8.5)

Het is een Financiële instelling toegestaan onder de in artikel 8.5 Gedragscode genoemde voorwaarden telefoongesprekken op te nemen. Zo geldt dat het opnemen van telefoongesprekken geoorloofd is wanneer wordt voldaan aan een wettelijke verplichting, voor het leveren van bewijs, voor (fraude) onderzoek en opsporing, voor het evalueren van de kwaliteit van de dienstverlening en voor training, coaching en beoordelingsdoeleinden. Verder geldt 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. De reden voor het opnemen van telefoongesprekken is onder meer dat achteraf de inhoud van de opdracht kan worden vastgesteld, indien dit in het kader van bijvoorbeeld een geschil met een Cliënt noodzakelijk is. Te denken valt in dat verband aan een opdracht tot aan- of verkoop van effecten. Een andere reden om een telefoongesprek vast te leggen is bijvoorbeeld de vaststelling van het exacte tijdstip waarop het verlies of de diefstal van een bankpas is gemeld of indien het bedreigingen betreft gericht tegen de Financiële instelling of haar personeelsleden. Financiële instellingen zullen hun Cliënten in algemene zin informeren over het vastleggen van deze communicatie, bijvoorbeeld via hun productvoorwaarden en deze Gedragscode. Ook zal de Financiële instelling het personeel terzake instrueren. Indien de Cliënt 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 communicatie. Wel kan in dat geval van een verzoeker worden verlangd dat hij dag en tijdstip van het gesprek of het contact aangeeft.

Vastlegging communicatie (artikel 8.6)

Binnen Financiële instellingen worden communicatiegegevens bij diverse gelegenheden vastgelegd. Dit gebeurt veelal omdat opdrachten in toenemende mate via andere dan de traditionele schriftelijke en mondelinge middelen worden verstrekt. Elektronische middelen spelen een steeds grotere rol. Op het vastleggen van Persoonsgegevens verkregen via elektronische communicatie met een Betrokkene wordt artikel 8.5 Gedragscode zoveel mogelijk analoog toegepast.

9. Dringende redenen

Toelichting

Het doelbindingsbeginsel, transparantiebeginsel en de rechten van de Betrokkenen als genoemd in de artikelen 4.4, 4.7, 4.8, 4.9. 7.1.1, 8.4.5 en 8.5.4 Gedragscode kunnen in bijzondere omstandigheden, opzij worden gezet als hiertoe een dringende noodzaak bestaat, welke noodzaak zwaarder weegt dan de rechten en vrijheden van de Betrokkene. Dit kan bijvoorbeeld het geval zijn indien een Financiële instelling onderworpen is aan onderzoek dat uitgevoerd wordt door een toezichthouder of de fiscus. Ook in het geval van fraudeonderzoek dat wordt uitgevoerd door de Financiële instelling zelf of in verband met een eventuele juridische procedure kan het onder meer van belang zijn Betrokkenen daarover niet te informeren, nu dit het onderzoek zou kunnen schaden.

10. Naleving van de Gedragscode

Toelichting

Financiële instellingen hechten belang aan een correcte naleving van de regels van de WBP en Gedragscode. Het beginsel van verantwoordelijkheid voor de Verwerking van Persoonsgegevens impliceert dat de Financiële instelling voldoende overzicht heeft van de diverse Verwerkingen van Persoonsgegevens. In dat kader hebben Financiële instellingen een stelsel van zelfevaluatie geïmplementeerd door middel waarvan er onder meer wordt toegezien op de naleving van de WBP en de Gedragscode. De door een Financiële instelling ingestelde (i) auditafdeling, draagt bij aan de controle door periodiek, bij voorkeur jaarlijks, via een vorm van zelfevaluatie na te gaan op welke wijze met de Verwerking van Persoonsgegevens wordt omgegaan. Binnen de Financiële instelling is tevens het (ii) management van de instelling verantwoordelijk voor de naleving van wet- en regelgeving. Daarnaast dient (iii) Compliance of een andere met toezicht belaste afdeling er zorg voor te dragen dat binnen de wettelijke kaders wordt gehandeld.

Bovengenoemde onderdelen van Financiële instellingen kunnen ook rapportages opstellen over de naleving van de WBP. Afhankelijk van de uitkomsten hiervan en de aard en omvang van de afzonderlijke Verwerkingen van Persoonsgegevens wordt aangegeven bij welke onderdelen aanvullend onderzoek dient plaats te vinden. Ter bevordering van de naleving van de regels van de WBP en Gedragscode is een Financiële instelling tevens gehouden interne instructies op te stellen en te implementeren waarin nader wordt aangegeven op welke wijze binnen de Financiële instelling Persoonsgegevens dienen te worden verwerkt. De instructies betreffen in ieder geval die onderwerpen waarvan de Financiële instelling van oordeel is dat nadere uitleg wenselijk is. Het betreft hier tal van onderwerpen zoals bijvoorbeeld security manuals en documenten waarin uiteengezet wordt welke technische en organisatorische maatregelen genomen dienen te worden. Tevens kan worden gedacht aan een reglement opnemen telefoongesprekken.

11. Geschillen

Toelichting

De Nederlandse Vereniging van Banken (NVB) en het Verbond van Verzekeraars (Verbond) zijn beide 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.

De procedures die mogelijk zijn, zijn de volgende. Iedere Financiële instelling kent een interne procedure voor klachtenafhandeling. Indien de klacht niet of niet naar tevredenheid wordt afgehandeld kan de Betrokkene binnen 3 maanden na deze afhandeling het geschil voorleggen aan KiFiD. De beslissing op basis van de interne geschillenprocedure van de Financiële instelling geldt als een beslissing in de zin van artikel 46 WBP. Indien het geschil betrekking heeft op het recht op inzage/correctie en binnen 6 weken na de beslissing van de interne geschillenprocedure van de Financiële instelling wordt ingediend bij KIFID, wordt derhalve op grond van artikel 47 WBP de periode van 6 weken waarbinnen de Betrokkene het recht heeft om de zaak aan het CBP 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, is het uiteraard niet meer mogelijk gebruik te maken van de procedure van artikel 46/47 WBP.

Betrokkene is ter eigen keuze eveneens gerechtigd om met voorbijgaan aan de interne geschillenprocedure van betreffende Financiële instelling een geschil voor te leggen aan het CBP of de rechtbank. Daarmee vervalt zijn recht om alsnog de interne geschillenprocedure van de Financiële instelling, alsmede daaropvolgend KIFID in te schakelen.

Voor meer informatie over KIFID verwijzen wij naar de volgende website: www.kifid.nl of Klachteninstituut Financiële Dienstverlening (Kifid), Postbus 93257, 2509 AG Den Haag, telefoon 0900-klacht of 0900- 35552248 (€ 0,10 per minuut).

Bij vragen over de Gedragscode kan tevens contact worden opgenomen met de NVB, Postbus 3543, 1001 AH Amsterdam, telefoon 020 55 02 888 of per email info@nvb.nl of met het Verbond van Verzekeraars, Postbus 93450, 2509 AL Den Haag, telefoon 070 333 8500 of per email: Gedragscode_Privacy@verzekeraars.nl.

Bijlage I: Informatie

Ter informatie bij deze Gedragscode zijn de volgende documenten opgenomen:
A. Voorschrift Informatie Fiscus/Banken
B. Protocol Incidentenwaarschuwingssysteem Financiële instellingen
C. Gedragscode Persoonlijk Onderzoek
D. Moratorium erfelijkheidsonderzoek Verbond van Verzekeraars
E. HIV-gedragscode
F. Protocol Verzekeringskeuringen