VERBOND VAN VERZEKERAARS

nvga

SPOORBOEKJE FRAUDEBEHEERSING VOLMACHTEN

Een handreiking bij fraudebeheersing door gevolmachtigde agenten

JULI 2023

De inhoud van het Spoorboekje Fraudebeheersing Volmacht is niet bindend en slechts indicatief van aard. Het staat partijen altijd vrij daarvan, in onderling overleg, af te wijken.

INHOUD

1. INLEIDING

Het bestrijden van verzekeringsfraude is een verantwoordelijkheid van iedereen. Verzekeringsfraude verhoogt ongewenst de premiedruk en is maatschappelijk onaanvaardbaar. Het past niet binnen het imago dat we als verzekeringstak in het geheel nastreven. Een adequaat risicobeheersingsbeleid is daarom van groot belang. De normen uit het Protocol Verzekeraars en Criminaliteit en de operationele en beleidsmatige activiteiten van het Centrum Bestrijding Verzekeringscriminaliteit van het Verbond van Verzekeraars zijn daarbij belangrijke pijlers.
Er zijn in de markt diverse geautomatiseerde oplossingen voor de aanpak van verzekeringsfraude beschikbaar welke kunnen worden gekoppeld aan de eigen Front- en BackOffice. Helaas is dit niet voor elke Gevolmachtigde haalbaar. De werkgroep Fraudebeheersing Volmachten wil met dit Spoorboekje zorgen voor een praktische uitwerking van de uitgangspunten en maatregelen, zoals vastgelegd in het Protocol Verzekeraars en Criminaliteit van het Verbond van Verzekeraars.
Dit Spoorboekje is een document dat kan bijdragen aan de inrichting van het risicobeheersingstraject binnen het volmachtkanaal met een focus op aanpak van verzekeringsfraude. Dit document heeft betrekking op de schadebranches en de collectieve inkomensverzekeringen.

- In hoofdstuk 2 zijn de relevante overlegorganen beschreven, welke rol zij uitoefenen en hoe zij bereikbaar zijn.
- Hoofdstuk 3 is gewijd aan risicobeheersing binnen de standaardprocessen. In bestaande processchema's hebben wij aangegeven op welke momenten er aandacht moet zijn voor risicobeheersing in het acceptatie- en schadeproces.
- In hoofdstuk 4 zijn de voor fraudebeheersing geldende protocollen en gedragscodes benoemd.
- In hoofdstuk 5 is de checklist inrichting risicobeheersing opgenomen. U kunt hiermee vaststellen of risicobeheersing binnen uw organisatie voldoende aandacht krijgt.
- In hoofdstuk 6 is een overzicht weergegeven van de relevante aanwezige en gewenste managementinformatie.
- In hoofdstuk 7 worden de onderlinge verwachtingen van partijen toegelicht.
- In hoofdstuk 8 is benoemd wat CIS voor u kan betekenen.
- Hoofdstuk 9 gaat over de directe aansprakelijkstelling aan verzekeringsfraudeurs.

Met dit Spoorboekje willen we Gevolmachtigden een praktische ondersteuning bieden bij het beheersen van verzekeringsfraude. De in deze handreiking gebruikte informatie zoals processchema's en scorelijsten zijn indicatief. Het staat partijen vrij om hier aanvullende / afwijkende afspraken over te maken. Uiteraard zal het beleid van de verzekeraar voor de individuele Gevolmachtigde leidend zijn.

2. OVERLEGORGANEN

Onderstaand een overzicht van relevante partijen in het kader van risicobeheersing:

	Doelstelling organisatie	**Rol in Risicobeheersing**	**Bereikbaarheid**
Verbond van Verzekeraars	Vereniging van in Nederland opererende verzekeraars, gericht op: 1.Vertegenwoordiging & belangenbehartiging 2.Verbetering & instandhouding van de reputatie van de sector 3.Het bieden van een platform 4.Dienstverlening aan leden	Lobby (nationaal en internationaal) Beleidsbepaler; Initiator nieuwe ontwikkelingen; Overleg overheid/justitie	www.verzekeraars.nl
NVGA	Vereniging van Gevolmachtigde Assuradeurenbedrijven: 1. Belangenbehartiging Gevolmachtigde Agenten 2. Professionalisering volmachtkanaal	Bewaking kwaliteit binnen het volmachtkanaal	www.nvga.org
CBV	Centrum Bestrijding Verzekeringscriminaliteit, onderdeel van de afdeling Dienstverlening van het Verbond van Verzekeraars; is binnen het Verbond de afdeling die zich specifiek richt op fraude-/ criminaliteitsbestrijding.	Centrale coördinatie en beleidsontwikkeling met betrekking tot verzekeringscriminaliteit. Aanspreekpunt voor verzekeraars en stakeholders.	www.verzekeraars.nl
Bestuurlijk Overleg (BO)	Hoogste overlegorgaan tussen NVGA en (Verbond van) Verzekeraars op het gebied van volmachtaangelegenheden	Heeft risicobeheersing binnen Gevolmachtigde Agenten als één van de 5 hoofdthema's benoemd.	
Platform Volmachten (Verbond)	Zorgt dat beleidspunten vanuit het BO uitgevoerd worden, bijv. via de installatie van werkgroepen. Zorgt voor opdrachtbeschrijving-en, budgetten en bewaakt het proces.	Opdrachtgever van de werkgroep Fraudebeheersing Volmachten.	

	Doelstelling organisatie	Rol in Risicobeheersing	Bereikbaarheid
Werkgroep Fraudebeheersing Volmachten	Verzorgt de vertaling van het Protocol Verzekeraars en Criminaliteit in concrete acties ten behoeve van Gevolmachtigde agenten voor de schadebranches en inkomen	Uniforme aanpak fraudebeleid; optimalisatie gebruik beschikbare tools en ontwikkelingen nieuwe tools evenals vergroting awareness binnen het volmachtkanaal	
CIS	Het doel van CIS is het behartigen van de gemeenschappelijke belangen van haar deelnemers door bij te dragen aan en toe te zien op informatie-uitwisseling tussen deelnemers onderling, tussen deelnemers en politie en justitie en met andere door het bestuur erkende instellingen zodat deelnemers misbruik van financiële producten en diensten kunnen ontdekken, voorkomen en bestrijden en risico's kunnen beheersen in de ruimste zin des woords.	Platform voor informatie-uitwisseling op het gebied van risicobeheersing door verzekeraars en Gevolmachtigde Agenten.	www.stichtingcis.nl
Overige betrokken partijen: a) Systeemhuizen (ANVA / CCS / Dias) b) Experts c) Marktpartijen op het gebied van softwarelevering voor risicobeheersing d) Arbodiensten/casemanagers			

3. PROCESSEN

3.1. ALGEMEEN

Algemene beleidsuitgangspunten op het gebied van risicobeheersing liggen op verschillende plaatsen vast:

- De volmachtovereenkomst;
- Beleid van verzekeraars;
- In wet- en regelgeving;
- In beleid en adviezen van overkoepelende organisaties (Verbond van Verzekeraars / NVGA).

Bestrijding van verzekeringsfraude maakt onderdeel uit van risicobeheersing.
Het is van groot belang dat zowel verzekeraars als Gevolmachtigde Agenten blijvend aandacht aan risicobeheersing besteden.

Op de volgende pagina's hebben wij in voorbeeld processchema's in het groen aangegeven op welke momenten u extra aandacht dient te hebben voor verzekeringsfraude in het acceptatie- en schadeproces.

Toolkit Indicatorenlijst
De fraude indicatoren en scorelijst zijn uit het Spoorboekje gehaald. De indicatoren zijn terug te vinden in de Toolkit Indicatorenlijst. De indicatoren zijn uitgebreid met de indicatoren van het CBV. Daarnaast heeft er een controle plaatsgevonden op discriminatoire indicatoren. Aan de indicatoren zijn risicopunten gegeven die de zwaarte aangeven van de indicator. In onderstaande tabel is een advies terug te vinden per risicopuntencategorie.

<9 punten	Beoordeling door acceptant of schadebehandelaar
<10 punten	Intern overleg met fraude coördinator
< 15 punten	Overleg met verzekeraar

De indicatoren en puntentelling zijn indicatief en geen verplichting vanuit verzekeraars.

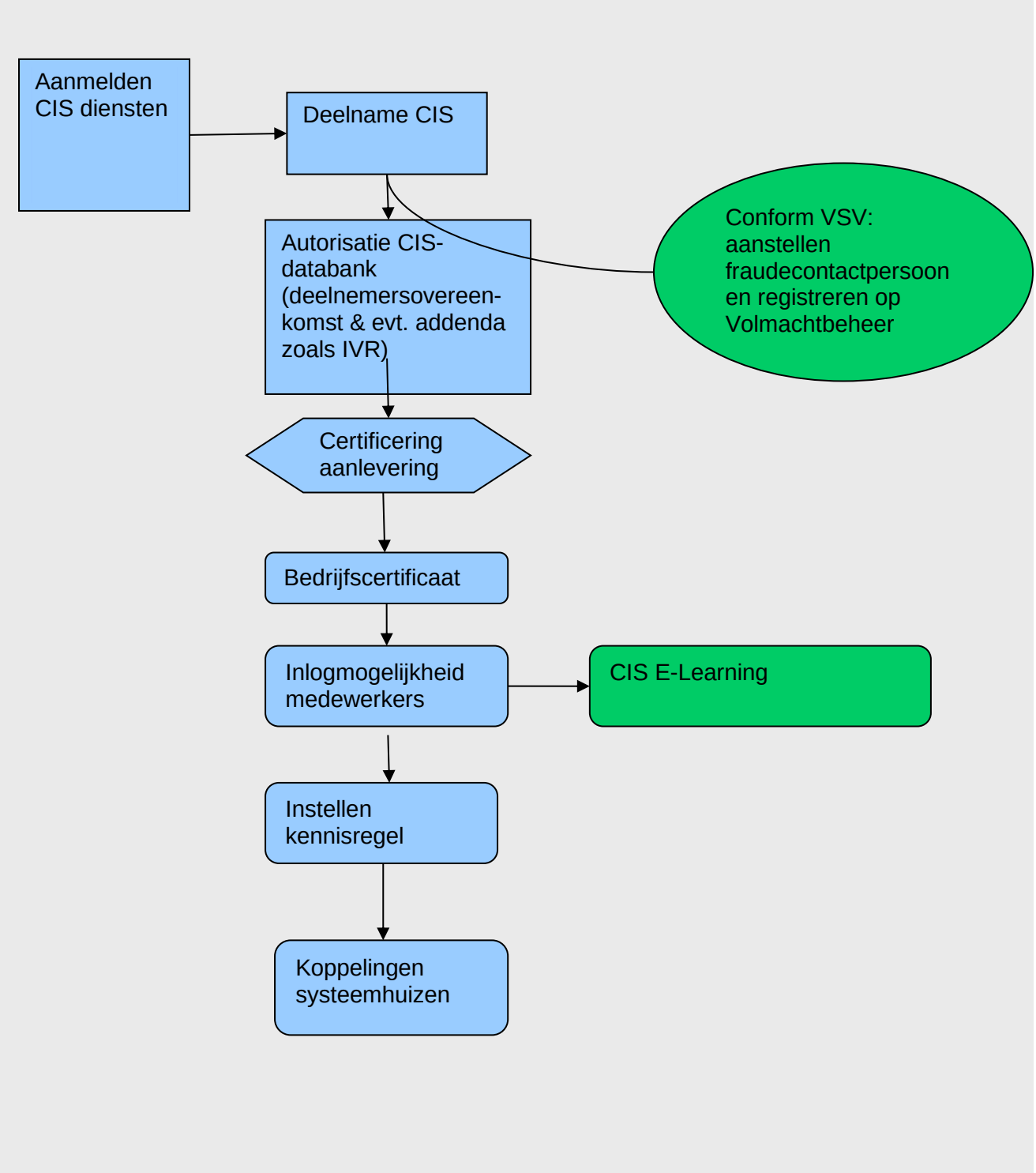
Hoe werkt de toolkit Indicatorenlijst?
Er zijn twee toolkit documenten beschikbaar. De indicatorenlijst EXCEL bevat een lijst met alle indicatoren en de risicopunten. De Indicatorenlijst Macro XLSM bevat een tool waarmee selecties makkelijker gemaakt kunnen worden. Het is mogelijk voor een acceptant om een selectie toe te passen met bijvoorbeeld alleen motor indicatoren. Daarnaast kunnen deze indicatoren worden aangevinkt en wordt er een advies gepresenteerd of dit besproken moet worden met de fraude coördinator of verzekeraar. Het document kan worden afgedrukt en gebruikt voor onderbouwing van het mogelijke fraudedossier.

De Indicatoren Macro XLSM is een macro bestand, hierdoor is het mogelijk om een melding te ontvangen waarin bevestigd moet worden dat het een veilig bestand is. Daarna moet de inhoud worden ingeschakeld om de macro werkend te krijgen. Nadat is bevestigd dat het een veilig bestand is en de inhoud is ingeschakeld kun je de tool gebruiken.

In verband met het veiligheidsrisico wordt de toolkit Indicatorenlijst alleen beschikbaar gesteld achter beschermde omgevingen zoals Volmacht Beheer/ Volmachtplein en NVGA.

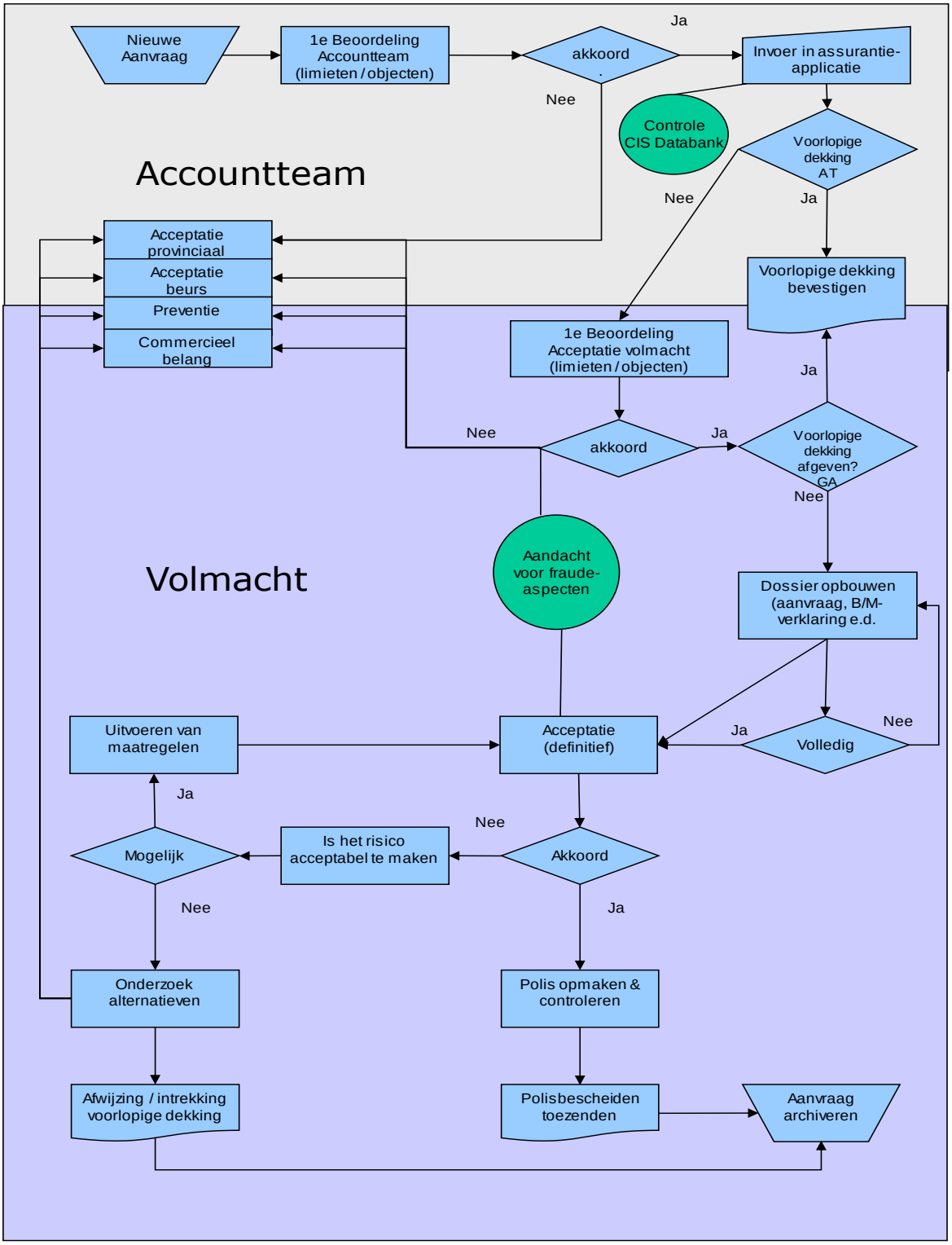
Deze processchema's en scorelijsten zijn indicatief en dienen slechts als voorbeeld. Het staat verzekeraar en zijn Gevolmachtigde vrij om hier aanvullende / afwijkende afspraken over te maken. Het beleid van de verzekeraar is leidend.

3.2 STROOMSCHEMA START GEBRUIK CIS-DATABANK

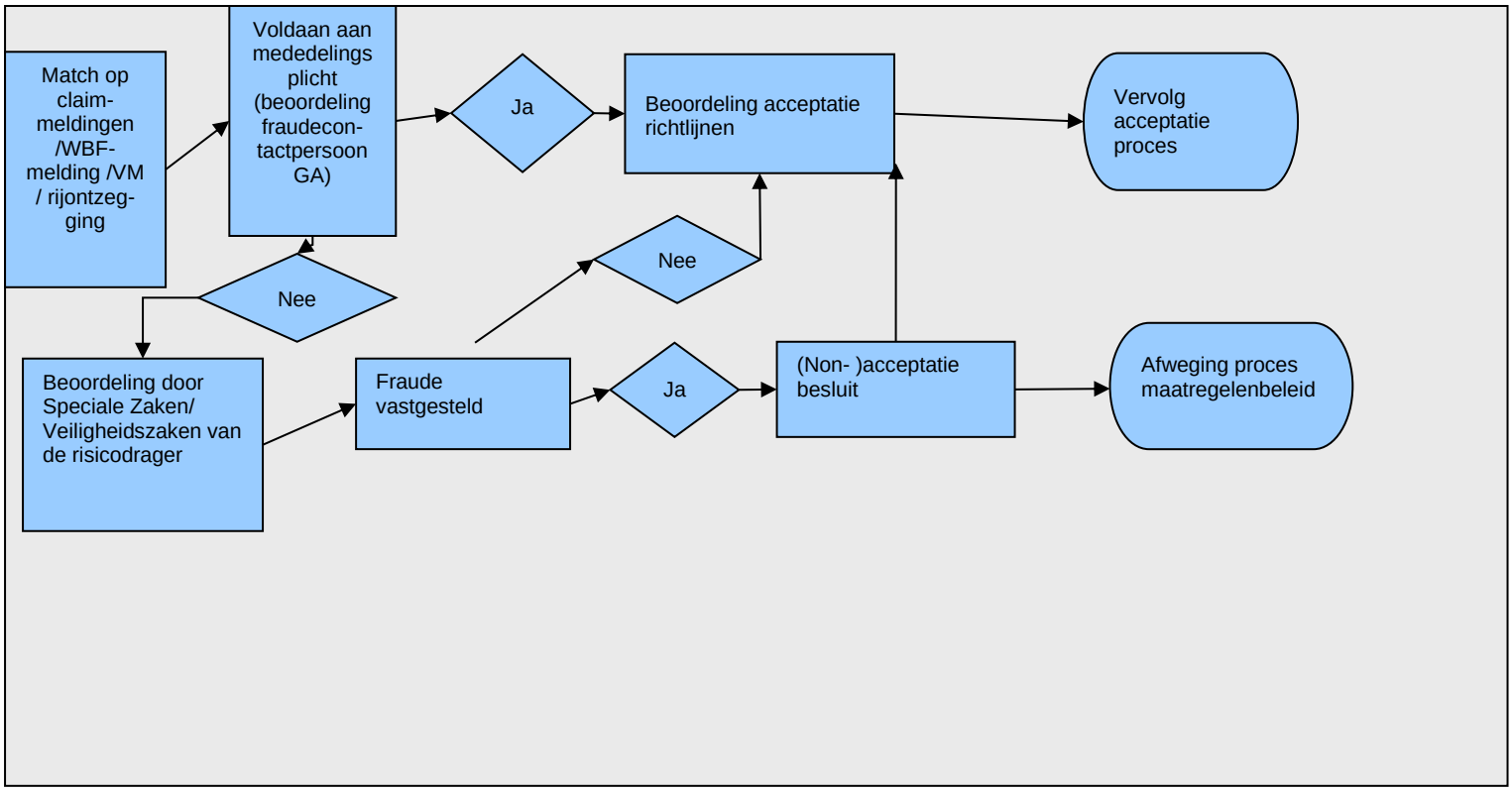


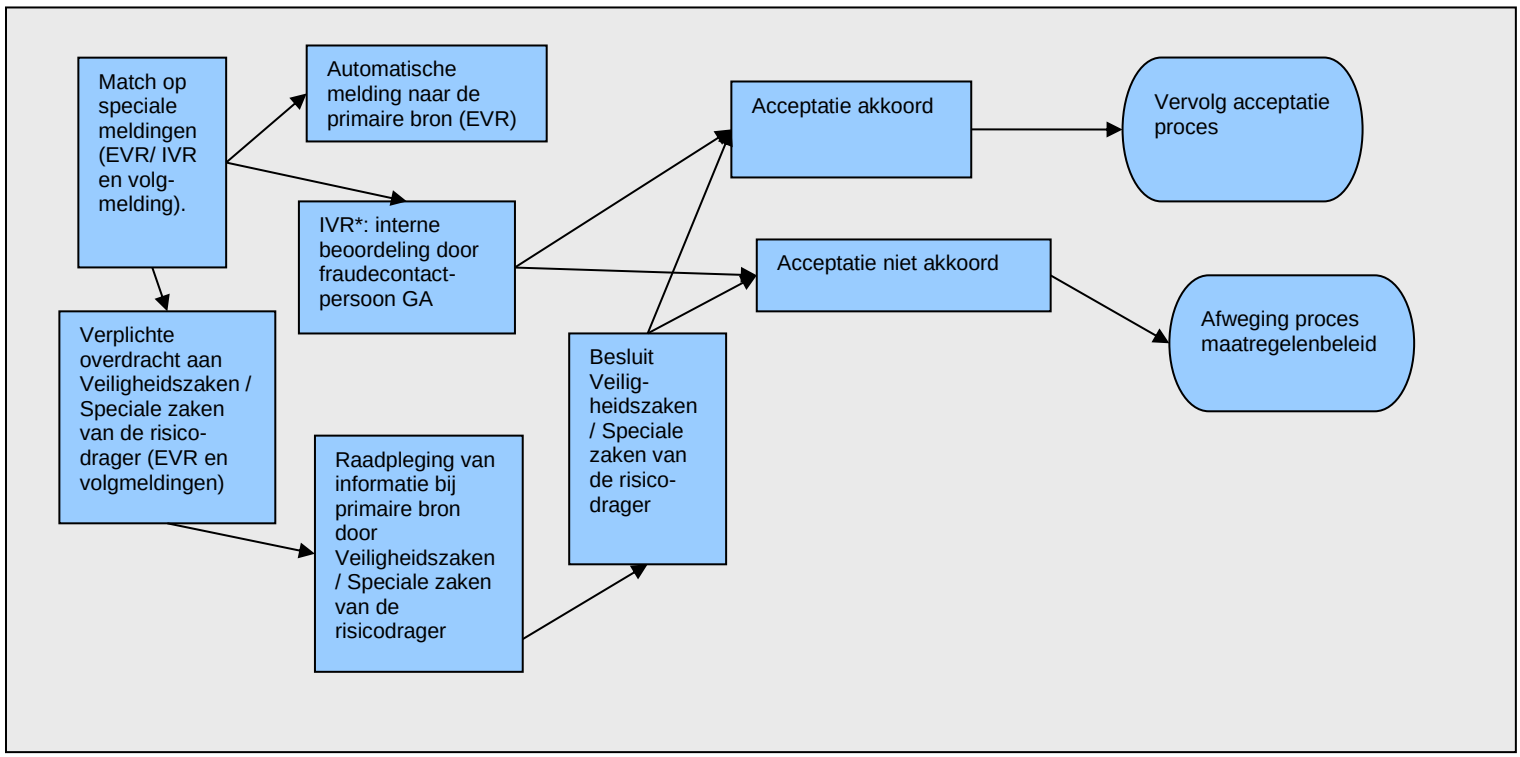
3.3 ACCEPTATIE

3.3.1 PROCESSCHEMA



3.3.2 CONTROLE CIS-DATABANK BIJ ACCEPTATIE





3.3.3 CONTROLEMOMENTEN (GEAUTOMATISEERD/HANDMATIG)

In het acceptatie/mutatieproces zijn een aantal processtappen noodzakelijk;

Aanvraag of bijsluiten verzekering in pakket*:
- Controle onderzoeksindicatoren Volmachten Acceptatie;
- Controle CIS-databank: verplicht conform overeenkomst;
- Compliancy Check: verplicht conform overeenkomst;
- Hercontrole CIS-databank: volgens Werkprogramma Risicobeheersing binnen 30-50 dagen na oorspronkelijke bevraging.

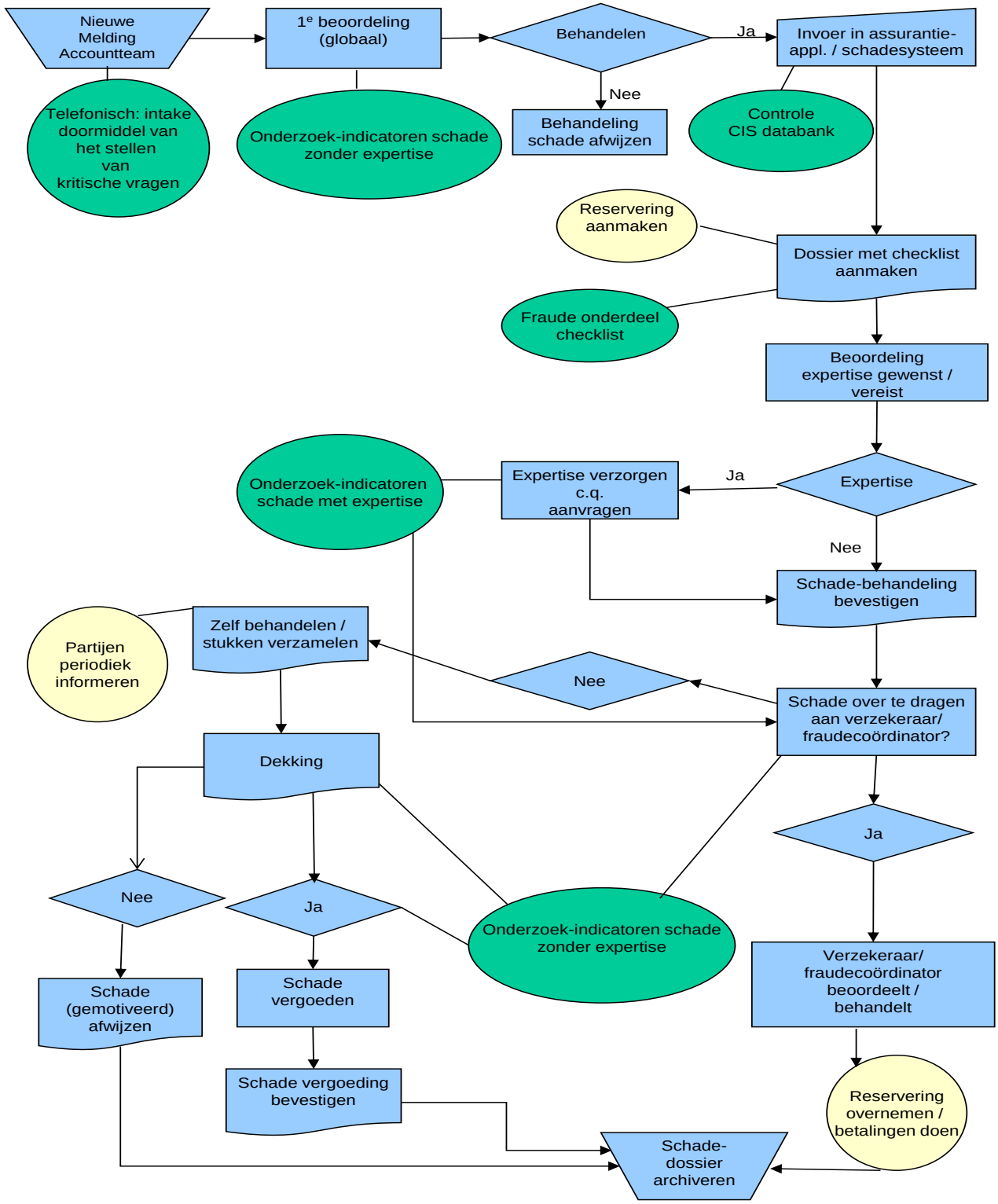
Wijziging*:
- Controle onderzoeksindicatoren Volmachten acceptatie;
- Controle CIS-databank: indien sprake is van een nieuwe (naam) verzekerde en/ of risico.

*Aanvullende controles:
- *Naast de bovengenoemde controles moeten op grond van de Sanctiewet en de Wet ter voorkoming van witwassen en financiering van terrorisme nog aanvullende controles plaatsvinden, gebaseerd op het Customer Due Diligence (CDD) beleid van de verzekeraar(s). Het CDD-beleid (waaronder het UBO-beleid) van de verzekeraar(s) is hierbij leidend.*

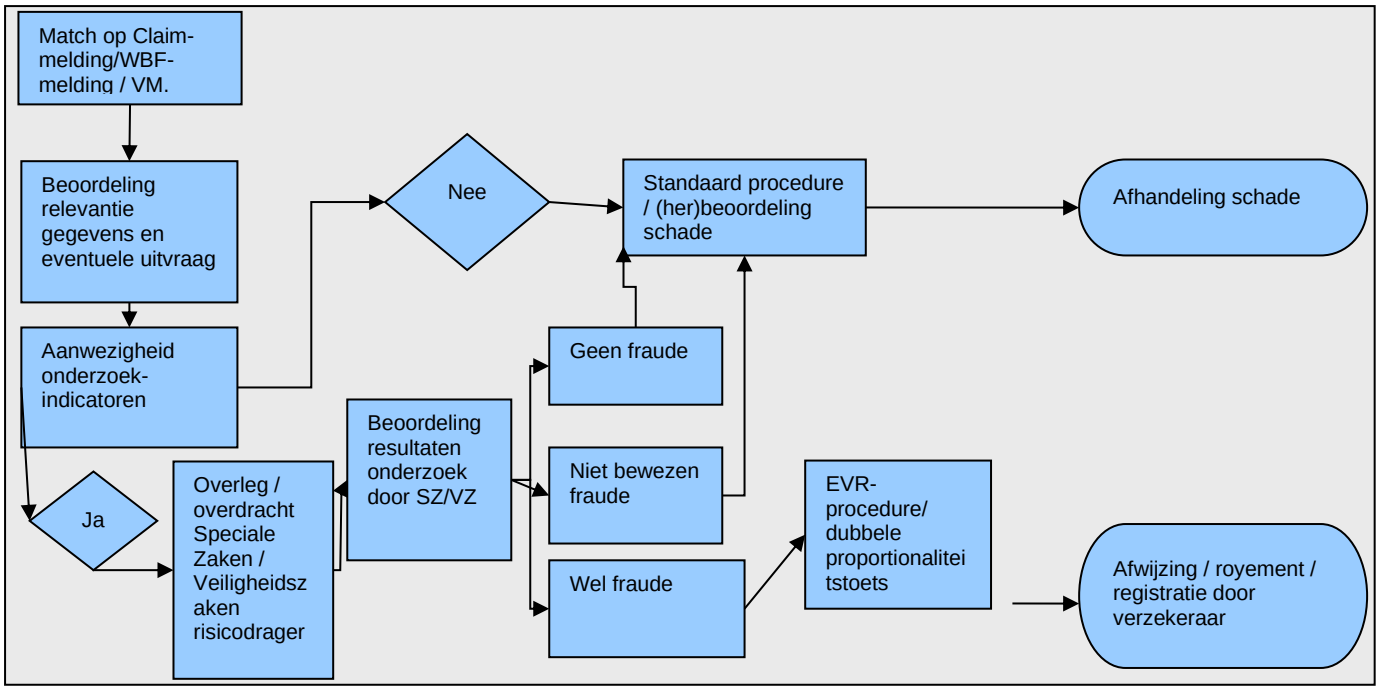
Geautomatiseerde besluitvorming
Gevolmachtigde Agenten kunnen aan de hand van het vastgestelde acceptatiebeleid van de verzekeraar volledig geautomatiseerd persoonsgegevens verwerken (bijvoorbeeld controles in CIS-databank uitvoeren). Voor het acceptatiebeleid kunnen door geautomatiseerde besluitvorming besluiten worden genomen voor het aangaan of uitvoeren van een verzekering. Het automatisch afwijzen en/of beperkt accepteren is niet toegestaan. De betrokkene moet hierover vooraf geïnformeerd worden en moet de Gevolmachtigde kunnen benaderen om een toelichting op het besluit en acceptatiebeleid te kunnen vragen. Ook moet het mogelijk zijn om een menselijke beoordeling te krijgen en een klacht te kunnen indienen.

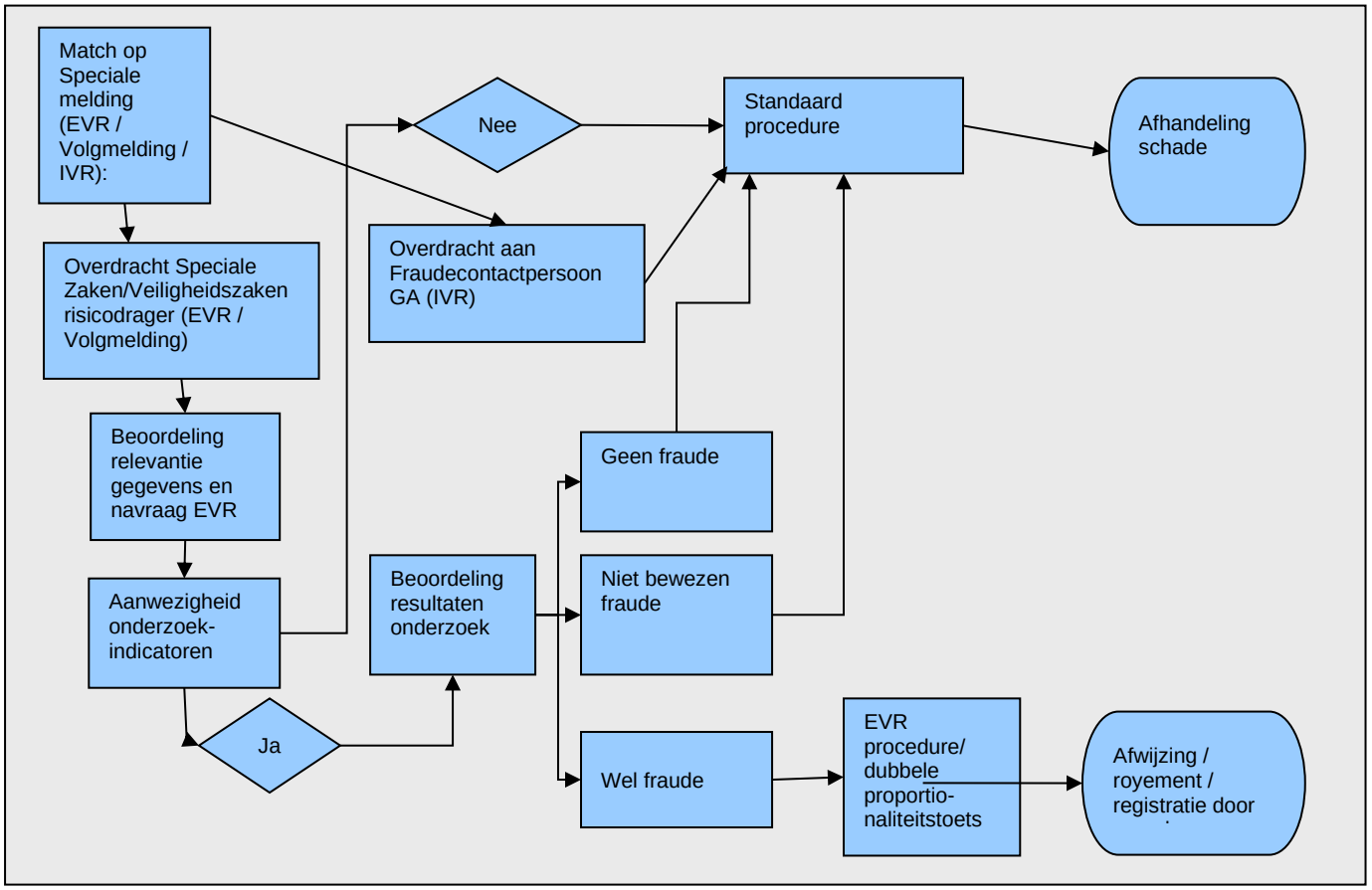
3.4 SCHADEBEHANDELING

3.4.1 PROCESSCHEMA



3.4.2 CONTROLE CIS-DATABANK BIJ SCHADE





3.4.5 CONTROLEMOMENTEN (GEAUTOMATISEERD / HANDMATIG)

Schademelding*:

- Controle op onderzoeksindicatoren Volmachten schade zonder expertise.
- Controle CIS-databank: verplicht cf. samenwerkingsovereenkomst .

Expertise*:

- Controle door onderzoeksindicatoren Volmachten schade met expertise.

** Naast de bovengenoemde controles moeten op grond van de Sanctiewet en de Wet ter voorkoming van witwassen en financiering van terrorisme nog aanvullende controles plaatsvinden, gebaseerd op het Customer Due Diligence (CDD) beleid van de verzekeraar(s). Het CDD-beleid (waaronder het UBO-beleid) van de verzekeraar(s) is hierbij leidend.*

4 PROTOCOLLEN EN GEDRAGSCODES

Protocollen en Gedragscodes worden regelmatig aangepast. De meest recente versies zijn terug te vinden op de website van het Verbond van Verzekeraars
https://www.verzekeraars.nl/branche/zelfreguleringsoverzicht-digiwijzer

4.1 GEDRAGSCODE VERZEKERAARS

De Gedragscode Verzekeraars brengt tot uitdrukking dat verzekeraars (die lid zijn van het Verbond van Verzekeraars) continu werken aan een balans tussen bedrijfseconomische groei en maatschappelijke vooruitgang. Hierbij staat het klantbelang voorop. De basis van de gedragscode wordt gevormd door de volgende kernwaarden: ‘zekerheid bieden’, ‘mogelijk maken’ en ‘maatschappelijk betrokken zijn’.

Ook in het kader van fraude- en risicobeheersing is het van belang dat alle betrokken partijen zich houden aan de in deze gedragscode genoemde kernwaarden en gedragsregels. De kernwaarden zijn in de gedragscode vertaald naar duidelijke gedragsregels. Verzekeraars, en daarmee ook Gevolmachtigde Agenten, bieden zekerheid naar hun klanten. De gedragsregels hierbij zijn:

Eenvoud & duidelijkheid

1. Wij behandelen klanten zorgvuldig en verankeren dit in onze cultuur. Wij communiceren helder en open met klanten.
2. Wij zorgen voor begrijpelijke producten en goede informatie hierover.
3. Wij investeren in educatie en voorlichting zodat klanten weten wat verzekeringen voor hen kunnen betekenen.
4. Wij zijn duidelijk over de zekerheid die wij bieden en dus ook over wat wij uitsluiten.
5. Wij zijn duidelijk over de werking en kosten van producten.
6. Wij hebben een product goedkeuringsproces, met een zorgvuldige afweging van de risico’s en zorgvuldige toetsing van andere relevante aspecten, waaronder de zorgplicht jegens de klant.
7. Wij zorgen ervoor dat het acceptatie- en het schadebehandelingsproces inzichtelijk zijn voor de klant.
8. Wij motiveren het besluit een klant niet te accepteren schriftelijk en in begrijpelijke bewoordingen. Wij wijzen de klant daarbij op eventuele andere (beroeps)-mogelijkheden.

Betrouwbaarheid

9. Wij onthouden ons van oneigenlijke verkoopmotieven, -methoden en -uitingen.
10. Wij zorgen ervoor dat een verschil van inzicht tussen verzekeraars over een schadegeval, waarbij het recht op uitkering niet ter discussie staat, geen nadelige gevolgen heeft voor de dienstverlening aan de klant.
11. Wij dragen in het schadebehandelingsproces zorg voor een voortvarende en zorgvuldige afhandeling met oog voor alle betrokkenen.
12. Wij doen geen zaken met personen, instellingen of bedrijven waarvan wij weten of kunnen weten dat zij activiteiten ontplooien die wettelijk verboden zijn.
13. Wij doen in geval van verzekeringsfraude aangifte volgens onze afspraken met het Openbaar Ministerie.
14. Wij registreren onrechtmatig handelen jegens ons, ons personeel of onze klanten.

Kwaliteit & deskundigheid

15. Wij beheren de ons toevertrouwde premies zorgvuldig en verantwoord.
16. Wij beleggen ontvangen gelden solide en rendementsbewust.
17. Wij dragen zorg voor een zorgvuldig, beheerst en duurzaam ondernemingsbestuur.
18. Wij zorgen dat er adequaat intern toezicht wordt gehouden op relevante bedrijfsprocessen. Wij bevorderen de deskundigheid van onze bestuurders en interne toezichthouders via een programma van permanente educatie. De educatie heeft in ieder geval betrekking op de zorgplicht jegens de klant.
19. Wij hebben een klantgerichte interne klachtenregeling. Wij brengen de klanten hiervan op de hoogte en wijzen hen, voor zover van toepassing, op het Klachteninstituut Financiële Dienstverlening (Kifid).
20. Wij werken onvoorwaardelijk mee aan bemiddeling door de Ombudsman Financiële Dienstverlening en volgen, afgezien van hoger beroep, de bindende adviezen op van de Geschillencommissie Financiële Dienstverlening. Daarnaast onderwerpen wij ons aan de toepasselijke rechtsgang bij de Tuchtraad Assurantiën (Tuchtraad) en de burgerlijke rechter.

Mogelijk maken

21. Wij maken het mogelijk dat zoveel mogelijk (potentiële) klanten risico's financieel af kunnen dekken en zullen ons inspannen te voorkomen dat mensen tegen hun wil onverzekerd zijn.
22. Wij spelen in op de doelen van klanten en de uitdagingen van het moment met vernieuwende oplossingen.
23. Wij stellen het klantbelang voorop, ook als spanning ontstaat tussen politieke keuzes en klantwensen.
24. Wij zetten ons in voor kwaliteitsverbetering op aan verzekeren gerelateerde maatschappelijke terreinen.
25. Wij werken samen met de overheid en andere strategische partners als verzekeraars oplossingen niet alleen kunnen realiseren.
26. Wij zijn duidelijk over de grenzen van onze mogelijkheden.

Maatschappelijk betrokken zijn:

27. Wij spelen in op maatschappelijke ontwikkelingen.
28. Wij gaan in het maatschappelijk debat de dialoog aan met belanghebbenden.
29. Wij betrekken niet alleen bedrijfseconomische, maar ook maatschappelijke, sociale en ecologische belangen bij onze bedrijfsvoering en ons beleggingsbeleid en leggen hierover verantwoording af.

4.2 PROTOCOL VERZEKERAARS & CRIMINALITEIT

Dit Protocol (juni 2018) beoogt het niveau van fraude- en criminaliteitsbeheersing bij in Nederland werkzame verzekeraars op het hoogste niveau te brengen en te houden. Doel is schade en risico's, die voortkomen uit fraude en andere vormen van criminaliteit, voor de sector, consumenten en de samenleving zoveel mogelijk te beperken.

Om dit te bereiken, legt dit Protocol regels en normen op ten aanzien van o.a. bewustwording, organisatorische aspecten van en samenwerking bij fraude- en criminaliteitsbeheersing, preventie, data-analyse, detectie, onderzoek en afdoening van zaken.

Uitgangspunten

- Op basis van dit Protocol hanteren verzekeraars bij fraude- en criminaliteitsbeheersing als uitgangspunten: een adequate inbedding van fraude- en criminaliteitsbeheersing in de eigen organisatie;
- optimale samenwerking en informatie-uitwisseling met partijen binnen en buiten de sector;
- een stevige en effectieve inzet op bewustwording en preventie;
- effectieve detectie, onderzoek, bewijsvoering en data-analyse;
- een krachtige en efficiënte afdoening van zaken;
- een systematische monitoring en naleving van (de implementatie van) het bovenstaande.

4.3 VASTLEGGING EN VERWERKING VAN PERSOONSGEGEVENS

De verwerking en gebruik van de persoonsgegevens moeten onder meer in overeenstemming zijn met:

- Algemene Verordening Gegevensbescherming en de Uitvoeringswet Algemene Verordening Gegevensbescherming (AVG en UAVG).
- De Gedragscode Verwerking Persoonsgegevens Verzekeraars.
- CIS Gebruikersprotocol.
- CIS Privacyreglement.
- Protocol Incidenten waarschuwingssysteem Financiële Instellingen.

Het is van belang dat de Gevolmachtigde Agent een eigen privacybeleid vastlegt binnen zijn onderneming waarbij de voorschriften uit de AVG en UAVG en de geldende brancheregelgeving worden nageleefd. Over het algemeen zal dit ook rekening houden met het beleid van de verzekeraar(s).

Het privacybeleid specificeert de kaders waarbinnen (persoons)gegevens verwerkt, bewaard en verstrekt mogen worden. Het privacybeleid beschrijft:

- Op welke wijze persoonsgegevens worden vastgelegd in de volmachtadministratie en in de CIS-databank en op welke wijze betrokkenen hierover geïnformeerd worden.
- Hoe lang (persoons)gegevens bewaard worden.
- Hoe omgegaan wordt met bijzondere persoonsgegevens.
- Welke beheersmaatregelen genomen worden bij bepaalde groepen klanten (bijv. veelclaimers).
- Hoe invulling wordt gegeven aan het recht op inzage, verzet of correctie door betrokkene.
- Welke informatie aan derden wordt verstrekt.
- Welke controles uitgevoerd worden op de naleving van het beleid.

Het is van belang (persoons)gegevens volgens de geldende wet- en regelgeving te verwerken en te bewaren, omdat:

- Klanten recht hebben op een zorgvuldige omgang met hun persoonsgegevens.
- Bepaalde gegevens essentieel zijn voor een integere en beheerste bedrijfsvoering.
- Hiermee uitvoering wordt gegeven aan rechten en verplichtingen.
- De gegevens noodzakelijk kunnen zijn voor een goede bewijspositie.
- Hiermee voldaan wordt aan wettelijke verplichtingen t.a.v. toezichthouders, overheidsinstanties, accountants e.d.

Hiernaast is het belangrijk om te voldoen aan de informatieplicht die u heeft als persoonsgegevens van klanten of derden verwerkt worden voordat deze verwerking plaatsvindt. Door middel van een duidelijke privacyverklaring die op de website vindbaar is, kan voldaan worden aan deze informatieplicht als u de betrokkenen hiernaar verwijst.

Voor het uitwisselen van informatie van persoonsgegevens is voor de volmachtmarkt de matrix "Gegevensverstrekking door Gevolmachtigde Agent aan derden" opgesteld (zie bijlage 4).

4.4 GEDRAGSCODE VERWERKING PERSOONSGEGEVENS VERZEKERAARS

De gedragscode Verwerking Persoonsgegevens Verzekeraars bepaalt welke gegevens verzekeraars die lid zijn van het Verbond van Verzekeraars mogen verwerken en op welke wijze dit moet worden gedaan. In de gedragscode zijn de algemene verplichtingen uit de AVG en UAVG specifiek voor verzekeraars nader uitgewerkt.

Persoonsgegevens mogen slechts verwerkt worden indien en voor zover is voldaan aan minimaal één van de volgende rechtmatige grondslagen zoals bepaald in artikel 6 van de AVG:

- Toestemming van de betrokken persoon.
- De gegevensverwerking is noodzakelijk voor de uitvoering van een overeenkomst.
- De gegevensverwerking is noodzakelijk voor het nakomen van een wettelijke verplichting.
- De gegevensverwerking is noodzakelijk ter bescherming van de vitale belangen.
- De gegevensverwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of uitoefening van openbaar gezag.
- De gegevensverwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen.

U bent zelf verantwoordelijk om te beoordelen of u zich voor een verwerking van persoonsgegevens kunt baseren op één van de 6 grondslagen.

4.5 PROTOCOL INCIDENTEN WAARSCHUWINGSSYSTEEM FINANCIËLE INSTELLINGEN

De waarborging van de veiligheid en integriteit van de financiële sector en de aanpak van sector gerelateerde criminaliteit (waaronder fraude) zijn erg belangrijk voor Financiële Instellingen. Voor Financiële Instellingen zoals Banken en Verzekeraars is een beheerste en integere bedrijfsvoering van cruciaal belang. Daarom moeten Financiële Instellingen beschermende maatregelen nemen. Op deze wijze kan fraude en criminaliteit worden bestreden. En kan veiligheid en integriteit worden gewaarborgd. Dit wordt ook van Financiële Instellingen verwacht door onder meer klanten, toezichthouders en de wetgever. Hiermee wordt ook het maatschappelijk belang gediend. De overheid roept Financiële Instellingen op om samen te werken op het gebied van criminaliteitsbestrijding.

Eén beschermende maatregel is het Incidenten Waarschuwingssysteem Financiële Instellingen (Waarschuwingssysteem). Dit is een systeem dat het mogelijk maakt voor Financiële Instellingen om (i) te onderzoeken en (ii) om na te gaan of iemand (bijvoorbeeld een klant of sollicitant) een dreiging voor de (klanten of medewerkers van de) Financiële Instelling vormt of kan vormen. Bijvoorbeeld als deze al eerder bij een Financiële Instelling heeft gefraudeerd. Op deze manier kan worden voorkomen dat die persoon dit nog een keer probeert bij een andere Financiële Instelling

Het Waarschuwingssysteem bestaat uit (i) de Incidentenregisters van individuele Financiële Instellingen en Brancheverenigingen en (ii) een aan ieder Incidentenregister gekoppeld Extern Verwijzingsregister waarin alleen Verwijzingsgegevens afkomstig van de betreffende Financiële Instelling zijn opgenomen.

Dit Extern Verwijzingsregister bevat uitsluitend Verwijzingsgegevens (bijvoorbeeld een naam en geboortedatum of KvK-nummer) die onder strikte voorwaarden daarin mogen worden opgenomen. De Gevolmachtigde Agent heeft de mogelijkheid om via de CIS-databank te toetsen of een (rechts)persoon in het Extern Verwijzingsregister (EVR) voorkomt. Hiervoor geldt als eis dat hierop alleen getoetst mag worden via de vergunning van de verzekeraar. Hiervoor is een apart (Pifi) machtigingsformulier beschikbaar, dat ondertekend dient te worden.

Toetsingsproces

Toetsing van persoonsgegevens op een registratie in het Extern Verwijzingsregister kan geautomatiseerd of handmatig worden uitgevoerd. De bevraging van het EVR resulteert in een terugkoppeling naar de bevrager dat de ingevoerde gegevens al dan niet overeenstemmen met gegevens die in het register voorkomen.

Wanneer een bevraging resulteert in terugkoppeling over een overeenstemming met een registratie in het EVR moet de fraudecontactpersoon van de Gevolmachtigde Agent het signaal uit het EVR controleren op de mate van overeenstemming met de persoonsgegevens van betrokkene. Hierbij zijn twee mogelijkheden.

- Wanneer overeenstemming afdoende is vastgesteld moet de zaak overgedragen worden aan de afdeling Veiligheidszaken van de verzekeraar. Bij diverse verzekeraars is deze rol gedelegeerd aan een team Speciale Zaken of een fraudecoördinator.

  De afdeling Veiligheidszaken van de verzekeraar legt vervolgens contact met de afdeling Veiligheidszaken van de primaire bron (de melder). Dit is een verplichting vanuit het protocol. De informatie die onderling wordt uitgewisseld is vertrouwelijk.

  De verzekeraar adviseert / besluit vervolgens over de acceptatie van het risico en/of verdere behandeling van de schade. En communiceert hierover met de Gevolmachtigde Agent.

- Wanneer geen afdoende overeenstemming is vastgesteld door de GA tussen de gegevens van de EVR-registratie en de (persoons)gegevens van de aanvrager hoeft deze de hit niet overgedragen te worden aan de verzekeraar. De hit dient echter wel door de Gevolmachtigde Agent afgemeld te worden bij de registrerende verzekeraar.

Opmerking: Het Intern Verwijzings Register (IVR), valt niet onder het protocol Incidenten waarschuwingssysteem Financiële Instellingen, maar onder de Gedragscode Verwerking Persoonsgegevens Verzekeraars. Zie hiervoor meer bij hoofdstuk 8 “Wat CIS voor u kan betekenen” In hoofdstuk 8 vindt u tevens informatie over het CIS gebruikersprotocol en het CIS privacyreglement.

4.6 GEDRAGSCODE PERSOONLIJK ONDERZOEK

De Gedragscode Persoonlijk Onderzoek geeft de beginselen aan die een verzekeraar in acht moet nemen bij het uitvoeren van een persoonlijk onderzoek. Een persoonlijk onderzoek is een onderzoek waarbij bijzondere onderzoeksmethoden of -middelen worden gebruikt, die inbreuk (kunnen) maken op de persoonlijke levenssfeer van een betrokkene.

Het instellen van een persoonlijk onderzoek kan alleen gebeuren door de afdeling Veiligheidszaken / Speciale Zaken van de Verzekeraar.

4.7 PRIVACY GEDRAGSCODE SECTOR PARTICULIERE ONDERZOEKBUREAUS

De Privacy Gedragscode Sector Particuliere Onderzoekbureaus:

- Is bindend voor advies-, recherche- en schadeonderzoekbureaus die lid zijn van de Nederlandse Veiligheidsbranche. De gedragscode bevat richtlijnen hoe in juridische zin moet worden omgegaan met persoonsgegevens die in het kader van de dienstverlening aan opdrachtgevers verwerkt worden;
- Draagt bij aan de doorzichtigheid van door de sector particuliere onderzoekbureaus gehanteerde onderzoeksmethoden en in te zetten onderzoeksmiddelen;
- Geeft aan wanneer de onderzochte persoon op de hoogte gesteld wordt van het feit dat tegen hem/haar een onderzoek is/wordt ingesteld en wat aan de onderzochte persoon wordt medegedeeld;
- Biedt aanknopingspunten voor de Autoriteit Persoonsgegevens om te beoordelen of de verwerking van de persoonsgegevens door de sector particuliere onderzoekbureaus volgens de geldende wet- en regelgeving geschiedt.

5 CHECKLIST INRICHTING FRAUDEBEHEERSING

Om u behulpzaam te zijn bij het implementeren van fraudebeleid binnen uw organisatie hebben wij een checklist ontwikkeld.

In deze checklist worden een aantal concrete ja/nee-vragen gesteld. Indien u een vraag met nee moet beantwoorden, kunt u op de site van VolmachtBeheer (onder het kopje Verbond van Verzekeraars – Fraude - Documentatie) diverse toelichtingen en voorbeelddocumenten vinden, die u kunt gebruiken.

Door het invullen van deze checklist kunt u eenvoudig vaststellen of fraudeaanpak binnen uw organisatie voldoende aandacht krijgen.

De fraudechecklist inclusief bijlagen vindt u achterin dit Spoorboekje (bijlage 1).

6 MANAGEMENTINFORMATIE

Om goed inzicht te krijgen in de inspanningen van fraudebeheersing in het volmachtkanaal is het belangrijk om managementinformatie samen te stellen. Wanneer bij een Gevolmachtigde Agent geen gebruik wordt gemaakt van geautomatiseerde fraude- en risicodetectie zal deze handmatig moeten worden samengesteld.

Fraudebestrijding wordt namelijk in de breedte aangepakt. Hierin worden onder andere ervaringen opgedaan, resultaten geboekt en trends ontdekt. Het is van belang dat de markt deze resultaten met elkaar kan delen om fraude nu en in de toekomst beter onder controle te krijgen. Het Centrum Bestrijding Verzekeringscriminaliteit speelt hierin een centrale rol.

Ook dient een Gevolmachtigd Agent in het Werkprogramma Risicobeheersing Volmachten periodiek de resultaten van zijn inspanningen te rapporteren.

Bijlage 2 bevat een rapportage van de wijze waarop deze managementinformatie verzameld en gerapporteerd kan worden.

7 ONDERLINGE VERWACHTINGEN VAN PARTIJEN

Wat wordt verwacht van partijen die betrokken zijn bij fraudeaanpak in het volmachtkanaal:
Gevolmachtigde Agenten

- Stel – al dan niet met de betrokken verzekeraar – uw eigen fraudebeleid op, op basis van de hier aangeboden informatie. Toets vanuit de fraudeoptiek het privacybeleid.
- Communiceer dit beleid met verzekerden, bemiddelaars en tegenpartijen, bijvoorbeeld via folders, dienstverleningsdocumenten, polisvoorwaarden en websites.
- Stel een fraudecontactpersoon aan en meld deze aan bij VolmachtBeheer.
- Vertaal procedures en scores uit deze handreiking naar de eigen processen.
- Zorg dat betrokken medewerkers het fraudebeleid en de bijbehorende processen kennen en op de hoogte zijn van de inhoud van alle documenten, zoals genoemd in dit Spoorboekje.
- Gebruik scorelijsten en onderzoeksindicatoren bij acceptatie en schaderegeling, liefst in ieder dossier als onderdeel van een checklist, maar zeker bij elk geval waarin u een vermoeden van fraude hebt.
- Zorg voor de opstelling van managementinformatie (zie bijlage 2).
- Meld eventuele fraudezaken met behulp van het dossier en de ingevulde scorelijst bij de u bekende fraudecoördinatoren van uw verzekeraar(s).
- Zorg voor het onderhouden van kennis en de persoonlijke contacten op het gebied van fraudebeheersing door het bezoek van door verzekeraars en andere partijen aangeboden workshops en bijeenkomsten.

Wat mag u verwachten van de verzekeraar(s)?
Zij zorgen ervoor dat de informatie uit dit Spoorboekje bekend is bij de coördinator fraudebeheersing en/of geautoriseerde functionarissen.

- Ondersteuning Gevolmachtigde Agenten in fraudebeheersing
- Melden fraudecontactpersonen voor Gevolmachtigde Agenten aan bij VolmachtBeheer.
- Zorgen in voorkomende gevallen voor een goede communicatie met de Gevolmachtigde Agenten (terugkoppeling / voortgang / inzichten).
- Stellen samen met de Gevolmachtigde Agent managementinformatie op.

8 WAT KAN CIS VOOR U BETEKENEN?

Stichting Centraal Informatie Systeem (CIS) is een stichting van en voor in Nederland werkzame verzekeraars en Gevolmachtigde Agenten. CIS beheert gegevens die voor haar deelnemende verzekeraars en Gevolmachtigde Agenten van belang kunnen zijn. Deze gegevens kunnen afkomstig zijn van verschillende partijen die betrokken zijn bij een verzekeringsclaim of bij zaken die voor de verzekeringsmarkt belangrijk zijn om te delen.

Doel van CIS is het behartigen van de gemeenschappelijke belangen van haar deelnemers door bij te dragen aan en toe te zien op informatie-uitwisseling tussen deelnemers onderling, tussen deelnemers en politie en justitie en met andere door het bestuur erkende instellingen.

Door deze informatie-uitwisseling kunnen deelnemers misbruik van financiële producten en diensten ontdekken, voorkomen en bestrijden en risico's beheersen in de ruimste zin van het woord.

Daarmee kunnen de deelnemers een beter inzicht krijgen in de aard en omvang van de aangeboden risico's (is alle gevraagde informatie op een verzekeringsaanvraag naar waarheid meegedeeld) en de verplichting om schadevergoeding of uitkering te doen.

De in de CIS-databank vastgelegde gegevens kunnen ook worden gebruikt voor wetenschappelijk onderzoek en statistische analyses in het belang van fraude- en criminaliteitsbestrijding en risicoanalyses.

CIS ziet erop toe dat haar deelnemers alle toepasselijke wet- en regelgeving volgen bij het verwerken van gegevens in de CIS-databank. Zo mogen persoonsgegevens alleen worden verwerkt volgens de regels van de AVG en UAVG.

8.1 WANNEER MAG CIS GERAADPLEEGD WORDEN?

De CIS databank raadpleegt u bij het accepteren, het wijzigen en het behandelen van een schade van een (mogelijke) klant. U moet een betrokkene (ook als deze persoon – nog – geen klant is) altijd inlichten dat diens persoonsgegevens in de CIS databank worden vastgelegd.

De CIS databank mag niet worden geraadpleegd tijdens het offertetraject
Het raadplegen van de CIS databank voor de controle van het schade-/verzekeringsverleden mag pas als de slotvragen zijn beantwoord. Hierbij moet u rekening houden met de volgende uitgangspunten:

- U mag CIS in het acceptatieproces gebruiken om te controleren of een klant een juiste opgave heeft gegeven van diens relevante verzekerings- en schadeverleden. Maar pas nadat deze vragen eerst gesteld zijn aan de klant;
- U mag CIS informatie inzetten als hulpmiddel bij de controle van informatie die de klant zelf vooraf heeft verstrekt;
- U mag de CIS data niet raadplegen als de klant niet in de gelegenheid is geweest de informatie zelf te verstrekken (wat het geval is als de slotvragen niet worden gesteld);
- De CIS databank is geen voorselectiesysteem. U mag klanten dus niet op voorhand weigeren bij een 'rood bolletje'.

Volgt er een uitval?
Dan volgt u het beleid van de betreffende verzekeraar. Zie ook de informatie onder Toetsing (pag. 17)

Informatiedeling
Er is nog veel onduidelijkheid over of en zo ja welke informatie uit de CIS databank mag worden gedeeld. Vaak wordt gedacht dat dit niet mag of alleen door medewerkers van de afdelingen Veiligheidszaken. Er mag meer dan wordt gedacht en hiervoor is dan ook de matrix gegevensuitwisseling ontwikkeld om dit te verduidelijken. Deze matrix is als bijlage 4 van dit Spoorboekje toegevoegd.

8.2 CIS-DATABANK

De CIS-databank is als volgt onderverdeeld:

- ***Claimmeldingen (SM):***

Ongekleurde claimmelding op enig verzekeringsproduct. De registratie geldt als feitelijke weergave van een claim zonder informatie over schuld of aansprakelijkheid van betrokkene. Mede op basis van deze gegevens kan de verzekeraar of Gevolmachtigde Agent controleren of er voldaan is aan de mededelingsplicht / de gestelde vragen naar waarheid zijn beantwoord.

De definitie van een claimmelding in de CIS databank is "aanspraak maken op verzekeringsdekking".

Een telefonisch verzoek om informatie over de polisvoorwaarden of de dekking, zonder dat een voorval heeft plaatsgevonden, betekent geen registratie in de CIS databank.

Er moet door de registrerende verzekeraar of gevolmachtigde gecommuniceerd worden dat de claimmelding geregistreerd wordt in de CIS databank.

Vertrouwelijke Mededelingen (VM)
Van bepaalde soorten royementen kunnen registraties in de CIS databank worden ingevoerd. Deze meldingen worden van oudsher ook wel Vertrouwelijke Mededelingen genoemd.
De Vertrouwelijke Mededeling is de registratie van (persoons)gegevens in verband met het niet nakomen van een contractuele (code 2) of financiële verplichting (code 2a) door een verzekeringnemer of verzekerde, die om die reden heeft geleid tot opzegging van de verzekering door de deelnemer.

De regels voor Vertrouwelijke Mededelingen zijn vastgelegd in de Werkinstructie en voorschriften Vertrouwelijke Mededelingen.
De meest recente versie is te vinden op www.cissystems.nl, onder “Documentatie CIS databank”.

Het is niet toegestaan een VM-melding te plaatsen als iemand niet is geaccepteerd of als er sprake is van het niet nakomen van de mededelingsplicht. Als de verzekeringnemer zelf de verzekering opzegt, wordt de beëindiging ook **niet** geregistreerd in de CIS databank.

Een CIS deelnemer moet zijn geautoriseerd om batchmatig VM code 2a registraties aan te leveren. Deze autorisatie wordt verstrekt wanneer het beleidsdocument omtrent de procedure is goedgekeurd door CIS. In dit proces wordt gekeken of de verplichte stappen onderdeel zijn van de procesbeschrijving.

Redenen Vertrouwelijke Mededeling
Ten aanzien van registratie van royementen die door de deelnemer worden geïnitieerd wegens tekortkoming in de nakoming van de afspraken uit de verzekeringsovereenkomst, kent CIS één soort Vertrouwelijke Mededeling; onderverdeeld in een hoofdcategorie 2 en een subcategorie 2a.

Registratie van polis beëindiging op initiatief van een deelnemer kan als sprake is van een:
- Royement wegens niet nakomen algemene contractuele verplichtingen (Code 2);
- Royement wegens niet nakomen financiële contractuele verplichtingen (Code 2a).

Omdat aan verwerking van deze meldingen verschillende voorwaarden worden gesteld, geldt deze splitsing. De Code 2a is een speciale variant van een Code 2 melding omdat daaraan aanvullende waarborgen voor de betrokkene zijn gesteld door CIS.

Het is van belang dat hierbij alle stappen worden gezet zoals omschreven in de Werkinstructie en voorschriften vertrouwelijke mededelingen van CIS. De meest recente versie is te vinden op de website van Stichting CIS (in de deelnemersomgeving).

- ***Extern Verwijzings Register (EVR***)
  Registratie van verwijzingsgegevens van (rechts)personen die zijn opgenomen in het Extern Verwijzingsregister conform de vereisten van het Protocol Incidentenwaarschuwingssysteem Financiële Instellingen vanwege een laakbare of onrechtmatige gedraging die een bedreiging vormde, vormt of kan vormen voor de (financiële) belangen van financiële instellingen of de continuïteit en/of integriteit van de financiële sector. Zie hiervoor hoofdstuk 4.5.

- ***Waarborgfondsmeldingen (WBF)***
  Registratie van gegevens van bestuurders, bezitters en (kenteken)houders van onverzekerde motorvoertuigen als Stichting Waarborgfonds Motorverkeer een veroorzaakte schade in behandeling neemt.

- ***Ontzeggingen van de rijbevoegdheid (OBM)***
  Registratie van ontzeggingen van de bevoegdheid tot het besturen van motorrijtuigen zoals, op grond van artikel 156 onder a. van het Reglement Rijbewijzen, door de officier van justitie verwerkt in het rijbewijzenregister. Een registratie Ontzegging van de rijbevoegdheid is gebaseerd op een gerechtelijke uitspraak en wordt, namens het Openbaar Ministerie, in de CIS databank geplaatst. Deze registratie vindt pas plaats als de termijn om in hoger beroep te gaan is verlopen. Dat wil zeggen dat de uitspraak van de rechter niet meer kan worden aangevochten en er sprake is van een definitieve veroordeling.
  Informatie uit de CIS databank over deze rijontzeggingen mogen **uitsluitend** gebruikt worden voor de beoordeling van een **verkeersrisico**, dus alleen bij aanvragen en bij de uitvoering van verkeersproducten. Deze gegevens mogen buiten de verkeersproducten niet gebruikt worden als signaal voor een eventueel strafrechtelijk verleden (niet iedere rijontzegging is bovendien opgelegd in het kader van een *misdrijf* en is dan ook geen strafrechtelijk verleden waarnaar gevraagd wordt door verzekeraars).

- ***Interne meldingen van deelnemers (IVR)***
  Als service naar de CIS-deelnemers biedt CIS de mogelijkheid om ook interne meldingen van deelnemers te presenteren via het CIS platform. Deze registraties vormen geen onderdeel van de CIS-databank en zijn uitsluitend te raadplegen door de deelnemer zelf.
  Om hier gebruik van te mogen maken is het nodig dat de deelnemer een IVR Addendum op de CIS deelnemersovereenkomst heeft getekend. Het Intern Verwijzingsregister (dat toegankelijk is via de CIS databank) bevat uitsluitend verwijzingen naar (rechts)personen waar uw eigen organisatie extra aandacht voor vraagt. Deze verwijzingsgegevens en de achtergrondgegevens zijn toegankelijk voor alle personen van de eigen organisatie die daarvoor geautoriseerd zijn. Het IVR heeft dus het karakter van een bedrijfswaarschuwingslijst en de informatie daarin is alleen voor eigen gebruik. De medewerkers kunnen de waarschuwingslijst raadplegen als dat noodzakelijk is voor de uitvoering

van hun werkzaamheden, bijvoorbeeld om de integriteit van een persoon te verifiëren voor het sluiten van een verzekering of het behandelen van een claimmelding.

8.3 OVERIGE CIS DIENSTEN

8.3.1 COMPLIANCY CHECK

Een instrument om de verplichte controles van sanctielijsten (Wwft/Sanctiewet) uit te voeren bij:

- Het aangaan van een overeenkomst met een kandidaat-verzekeringnemer.
- De aanspraak op verzekeringsdekking door een relatie.
- Periodieke bestandcontroles Compliancy Check is in combinatie met de CIS-databank te raadplegen, zowel geautomatiseerd als handmatig.
- Compliancy Check bevat een aantal standaard sanctielijsten. Daarnaast is het mogelijk voor CIS deelnemers om als keuzelijst de PEP (Political Exposed Persons) lijst af te nemen.

8.3.2 UBO-CHECK

Voortvloeiend uit de wetgeving legt de DNB, naast de verplichting om natuurlijke en rechtspersonen te controleren, de branche een extra controle op. Die controle is het vaststellen van UBO's (Ultimate Benificial Owner), oftewel wie zijn de belanghebbenden achter de rechtspersonen met wie de verzekeraar zaken doet. De dienst UBO Check stelt CIS deelnemers in staat deze controle uit te voeren en de betreffende personen vervolgens desgewenst verder te toetsen in Compliancy Check en de CIS-databank.

8.3.3 CIS REFERENTIE TOOL (CRT)

Bij de deelnemers van CIS bestaat de behoefte aan een verwijsinstrument of -tool waarmee op eenvoudige en privacy vriendelijke wijze kan worden achterhaald bij welke verzekeraar(s) en Gevolmachtigde Agent(en) een specifieke (rechts)persoon of specifiek object (zijnde: een bedrijf, voertuig, vaartuig of opstal c.q. risicoadres) is of was verzekerd.

Een dergelijk verwijsinstrument kan bijvoorbeeld nodig zijn om ten behoeve van de nabestaanden van de slachtoffers van een vliegramp erachter te komen bij welke verzekeraar een overlijdensrisicoverzekering is gesloten. Of om, ten behoeve van de opsporing en vervolging in strafzaken, erachter te komen bij welke verzekeraar (de vermogensbestanddelen van) bepaalde verdachten zijn verzekerd.
Met de komst van de CIS Referentie Tool (CRT) kan in deze behoefte worden voorzien. Het Verbond van Verzekeraars en CIS hebben de inzet van de CRT in een samenwerkingsverband vormgeven. De CRT is eigendom van CIS en zij verzorgt de techniek. Het gebruik van de toepassing zal ter hand genomen worden door het Verbond van Verzekeraars waarbij uitsluitend medewerkers van het Centrum Bestrijding Verzekeringscriminaliteit de CRT kunnen raadplegen.

CIS deelnemers kunnen het CRT toegangspakket aanvragen bij CIS.

8.4 CIS DEELNEMERSOVEREENKOMST

Om gebruik te maken van de CIS-databank moet de Gevolmachtigde Agent een deelnemersovereenkomst aangaan met CIS.

Het gebruik van de informatie uit de CIS-databank is beperkt tot uw rol als Gevolmachtigde Agent van een verzekeraar die ook deelnemer is van CIS. De informatie uit de CIS-databank mag u dus niet toepassen op uw provinciale portefeuille of delen met uw adviseur.

8.5 CIS GEBRUIKERSPROTOCOL EN CIS PRIVACYREGLEMENT

Het CIS gebruikersprotocol en het CIS privacyreglement zijn van toepassing op alle verwerkingen die samenhangen met de CIS-databank die wordt beheerd onder de verantwoordelijkheid van CIS. In het protocol en het reglement zijn de regels en de voorschriften opgenomen voor de registratie van (persoons)gegevens, het correct gebruik van de CIS-databank door de deelnemers van Stichting CIS en de toepassing van de door CIS beheerde data. Het gebruikersprotocol is vooral gericht op de gebruikers van de CIS-databank en de data. Dat zijn de deelnemers van CIS. In het protocol is onder meer vastgelegd:

- Wat het doel is van de centrale dataopslag;
- Wie mag deelnemen aan de CIS-databank;
- Welke medewerkers toegang hebben tot de CIS-databank;
- Welke informatieverplichting de deelnemer heeft;
- Hoe registraties moeten worden aangeleverd;
- Hoe registraties mogen worden gebruikt;
- Wat er gebeurt als de deelnemer niet goed met de CIS-data omgaat.

Het privacyreglement is gericht op de (rechts)persoon van wie gegevens in de CIS-databank zijn vastgelegd. Het reglement geeft onder meer aan:

* Wie geregistreerd wordt;
* Welke persoonsgegevens geregistreerd worden;
* Hoe lang de persoonsgegevens bewaard worden;
* Waarvoor persoonsgegevens gebruikt worden;
* Met wie de persoonsgegevens worden gedeeld;
* Hoe de persoonsgegevens worden beveiligd;
* Hoe betrokkene persoonsgegevens kan inzien of aanpassen.

9. DIRECTE AANSPRAKELIJKSTELLING AAN VERZEKERINGSFRAUDEURS

Verzekeraars willen in woord en daad duidelijk maken dat fraude – óók in 'lichte' gevallen – onacceptabel is en nooit zonder gevolgen blijft.

Om hier beter invulling aan te geven, hebben fraudebestrijders behoefte aan een collectief in te zetten instrument dat:

- Een krachtig fraudepreventief signaal afgeeft aan (potentiële) fraudeurs; en
- Een snellere en efficiëntere afhandeling van met name lichte fraudezaken mogelijk maakt.

Een belangrijke reden voor de vraag naar een dergelijk instrument, is dat het in de praktijk niet in alle geconstateerde gevallen komt tot een daadkrachtige aanpak. Fraudebestrijders krijgen talrijke zaken op hun bureau. In een omgeving, waarin kostenbeheersing een groeiende rol speelt, moeten zij prioriteiten stellen en keuzes maken. Hierdoor gebeurt het bijvoorbeeld dat zaken met een kleiner financieel belang, of fraudes die vóór het uitkeren van de claim worden ontdekt, 'slechts' met een royement van de polis worden afgedaan. Dit terwijl verzekeraars in zulke gevallen wel aanmerkelijke kosten hebben gemaakt door activiteiten rond de dossierbehandeling. Ofwel: arbeidsuren die ook ingezet hadden kunnen worden ten behoeve van reguliere dienstverlening aan bonafide klanten.

Een nieuwe afdoening

Als oplossing is in de zomer van 2016 de directe aansprakelijkstelling via de Service Organisatie Directe Aansprakelijkstelling (SODA) geïntroduceerd. Deze afdoeningsmethode beoogt een sterke fraudepreventieve werking en stelt de verzekeraars in alle gevallen waarbij sprake is van bewezen fraude in staat om de schade, bijvoorbeeld door ingezette arbeid, op fraudeurs te verhalen. Voor toepassing op claimfraudezaken is hiervoor op bedrijfstakniveau een herkenbaar standaardbedrag van €191,- of € 532,- per geconstateerd geval vastgesteld. Voor acceptatie wordt een standaardbedrag van €101,- in rekening gebracht.

Hierdoor geven verzekeraars een duidelijke boodschap af: fraudeurs krijgen in alle gevallen de rekening van hun onrechtmatige daad gepresenteerd.
Wij adviseren u deze regeling op te nemen in het fraudebeleid op uw website. En in de polisvoorwaarden op te nemen dat u de door u geleden schade op de 'fraudeur' kan verhalen. Mocht u zaken hebben die voor deze regeling in aanmerking komen, neemt u dan contact op met de fraudecoördinator van de verzekeraar.

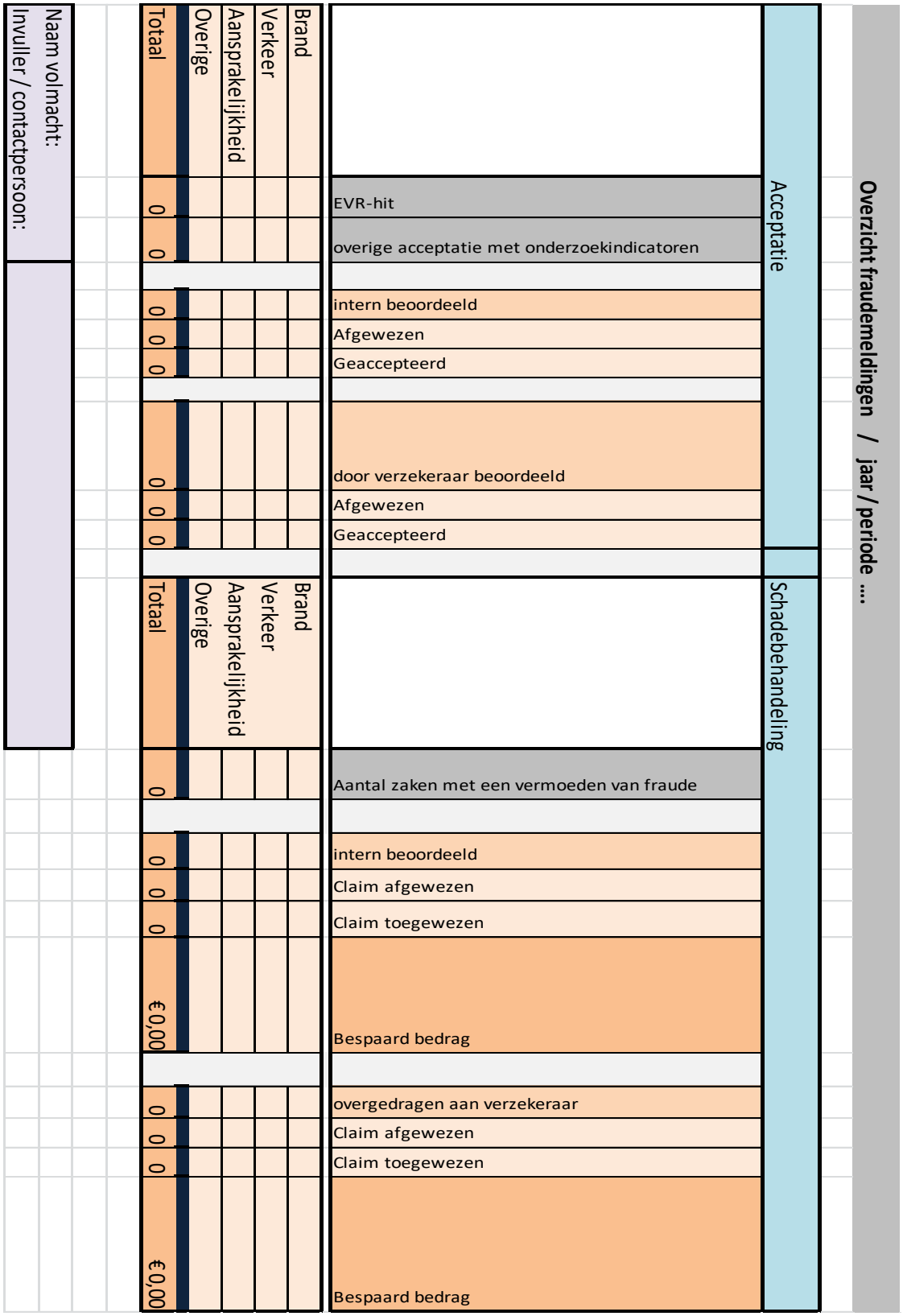
BIJLAGE 1 CHECKLIST FRAUDEBEHEERSING

Ga binnen uw organisatie na of de volgende zaken op het gebied van fraude zijn geregeld:

ORGANISATORISCHE MAATREGELEN		
1.1. Is er een verantwoordelijke benoemd voor het opstellen en het beheren van een fraudebeleid?	O JA	O NEE
1.2. Is er een fraudecontactpersoon benoemd?	O JA	O NEE
1.3. Heeft de fraudecontactpersoon voldoende autoriteit binnen het bedrijf om fraudebeleid daadwerkelijk te implementeren?	O JA	O NEE
1.4. Is deze fraudecontactpersoon in deze hoedanigheid binnen de Gevolmachtigd Agent bekend bij alle medewerkers?	O JA	O NEE
1.5. Heeft de fraudecontactpersoon een rol in de procedure conflicterende situaties?	O JA	O NEE
1.6. Worden door de fraudecontactpersoon (of andere medewerkers) jaarlijks controles uitgevoerd op het gebied van risicobeheersing?	O JA	O NEE
1.7. Is de fraudecontactpersoon aangemeld op VolmachtBeheer?	O JA	O NEE
1.8. Is fraude een vast punt op de agenda bij het werkoverleg?	O JA	O NEE
1.9. Is binnen functiebeschrijvingen en beoordelingscriteria van medewerkers aandacht besteed aan risicobeheersing?	O JA	O NEE
1.10. Is specifieke (actuele) fraudedocumentatie belegd in een (aparte) database en beschikbaar voor alle betrokken medewerkers?	O JA	O NEE
1.11. Is er een opleidingsprogramma?	O JA	O NEE
1.12 Is er een frauderegister en worden fraude en vermoedens van fraude geregistreerd en tijdig (binnen 3 werkdagen) gemeld bij de volmachtgever?	O JA	O NEE
FRAUDEBELEID		
2.1. Is er een fraudebeleid geformuleerd (is beschreven hoe de organisatie omgaat Met (vermoedelijke) fraude)?	O JA	O NEE
2.2. Is het fraudebeleid (incl. een definitie van het begrip “fraude”) opgenomen in het handboek?	O JA	O NEE
2.3. Komt uw fraudebeleid ter sprake in de communicatie met uw klant? Denk aan: dienstenwijzer / aanvraagformulieren / schade aangifteformulieren / website etc.	O JA	O NEE
FRAUDEPROCEDURES & -CONTROLES		
3.1. Zijn er procedures beschreven op het gebied van fraude, waarbij specifiek aandacht is besteed aan de (werk)gebieden: Commercie / Productontwikkeling / Acceptatie / Polisopmaak / Schadebehandeling / Financieel / Automatisering?	O JA	O NEE
3.2. Hebt u een controlebeleid op fraudebeheersing?	O JA	O NEE
3.3. Controleert u in CIS cf. de eisen van de volmachtovereenkomst?	O JA	O NEE
3.4. Voert u de controle conform de Sanctiewetgeving uit?	O JA	O NEE
3.5. Worden onderzoeksindicatoren (bijv. uit het Spoorboekje) gebruikt?	O JA	O NEE
3.6. Worden bij (vermoedelijke) fraudezaken de scorelijsten uit deze handreiking gebruikt?	O JA	O NEE
3.7. Hanteren door u gebruikte experts bij (vermoedelijke) fraudezaken scorelijsten?	O JA	O NEE

3.8. Worden alle (vermoedelijke) fraudezaken overgedragen aan de verzekeraar?	O	JA	O	NEE
AUTOMATISERING				
4.1. Indien u werkt met automatische acceptatie: Zijn onderzoeksindicatoren ingeregeld?	O	JA	O	NEE
4.2. Zijn er beheersingsmaatregelen genomen ter voorkoming van misbruik door derden?	O	JA	O	NEE
MANAGEMENTINFORMATIE				
5.1. Wordt van de onder 1.6, 3.3 en 3.4 genoemde controles management-rapportage opgesteld?	O	JA	O	NEE
5.2. Wordt de managementinformatie periodiek geanalyseerd?	O	JA	O	NEE

BIJLAGE 2 MANAGEMENTINFORMATIE



BIJLAGE 3 MEEST RELEVANTE WETSARTIKELEN VANUIT HET BW (BOEK 7)

ARTIKEL 928

- 1 De verzekeringnemer is verplicht vóór het sluiten van de overeenkomst aan de verzekeraar alle feiten mede te delen die hij kent of behoort te kennen, en waarvan, naar hij weet of behoort te begrijpen, de beslissing van de verzekeraar of, en zo ja, op welke voorwaarden, hij de verzekering zal willen sluiten, afhangt of kan afhangen.

- 2 Indien de belangen van een bij het aangaan van de verzekering bekende derde worden gedekt, omvat de in lid 1 bedoelde verplichting mede de hem betreffende feiten die deze kent of behoort te kennen, en waarvan naar deze weet of behoort te begrijpen, de beslissing van de verzekeraar afhangt of kan afhangen. De vorige zin mist toepassing bij persoonsverzekering.

- 3 Betreft een persoonsverzekering het risico van een bekende derde die de leeftijd van zestien jaren heeft bereikt, dan omvat de mededelingsplicht mede de hem betreffende feiten die deze kent of behoort te kennen en waarvan, naar hij weet of behoort te begrijpen, de beslissing van de verzekeraar afhangt of kan afhangen.

- 4 De mededelingsplicht betreft niet feiten die de verzekeraar reeds kent of behoort te kennen, en evenmin feiten, die niet tot een voor de verzekeringnemer ongunstiger beslissing zouden hebben geleid. De verzekeringnemer of de derde, bedoeld in lid 2 of lid 3, kan zich er echter niet op beroepen dat de verzekeraar bepaalde feiten reeds kent of behoort te kennen indien op een daarop gerichte vraag een onjuist of onvolledig antwoord is gegeven. De mededelingsplicht betreft voorts geen feiten waarnaar ingevolge de artikelen 4 tot en met 6 van de Wet op de medische keuringen in de daar bedoelde gevallen geen medisch onderzoek mag worden verricht en geen vragen mogen worden gesteld.

- 5 De verzekeringnemer is slechts verplicht feiten mede te delen omtrent zijn strafrechtelijk verleden of omtrent dat van derden, voor zover zij zijn voorgevallen binnen de acht jaren die aan het sluiten van de verzekering vooraf zijn gegaan en voor zover de verzekeraar omtrent dat verleden uitdrukkelijk een vraag heeft gesteld in niet voor misverstand vatbare termen.

- 6 Indien de verzekering is gesloten op de grondslag van een door de verzekeraar opgestelde vragenlijst, kan deze zich er niet op beroepen dat vragen niet zijn beantwoord, of feiten waarnaar niet was gevraagd, niet zijn medegedeeld, en evenmin dat een in algemene termen vervatte vraag onvolledig is beantwoord, tenzij is gehandeld met het opzet de verzekeraar te misleiden.

ARTIKEL 929

- 1 De verzekeraar die ontdekt dat aan de in artikel 928 omschreven mededelingsplicht niet is voldaan, kan de gevolgen daarvan slechts inroepen indien hij de verzekeringnemer binnen twee maanden na de ontdekking op de niet-nakoming wijst onder vermelding van de mogelijke gevolgen.

- 2 De verzekeraar die ontdekt dat de verzekeringnemer heeft gehandeld met het opzet hem te misleiden of die bij kennis van de ware stand van zaken geen verzekering zou hebben gesloten, kan de overeenkomst binnen twee maanden na ontdekking met dadelijke ingang opzeggen.

- 3 De verzekeringnemer kan de overeenkomst met dadelijke ingang opzeggen binnen twee maanden nadat de verzekeraar overeenkomstig lid 1 heeft gehandeld of zich bij de verwezenlijking van het risico op de niet-nakoming van de mededelingsplicht beroept. Bij persoonsverzekering kan de verzekeringnemer de beëindiging beperken tot de persoon, wiens risico het beroep op de niet-nakoming betreft.

ARTIKEL 930

- 1 Indien aan de in artikel 928 omschreven mededelingsplicht niet is voldaan, bestaat alleen recht op uitkering overeenkomstig de leden 2 en 3.

- 2 De bedongen uitkering geschiedt onverkort, indien de niet of onjuist meegedeelde feiten van geen belang zijn voor de beoordeling van het risico, zoals dit zich heeft verwezenlijkt.

- 3 Indien aan lid 2 niet is voldaan, maar de verzekeraar bij kennis van de ware stand van zaken een hogere premie zou hebben bedongen, of de verzekering tot een lager bedrag zou hebben gesloten, wordt de uitkering verminderd naar evenredigheid van hetgeen de premie meer of de verzekerde som minder zou hebben bedragen. Zou de verzekeraar bij kennis van de ware stand van zaken andere voorwaarden hebben gesteld, dan is slechts een uitkering verschuldigd als waren deze voorwaarden in de overeenkomst opgenomen.

- 4 In afwijking van de leden 2 en 3 is geen uitkering verschuldigd indien de verzekeraar bij kennis van de ware stand van zaken geen verzekering zou hebben gesloten.

- 5 In afwijking van de leden 2 en 3 is geen uitkering verschuldigd aan de verzekeringnemer of de derde, bedoeld in artikel 928 lid 2 of lid 3, die heeft gehandeld met het opzet de verzekeraar te misleiden. Evenmin is een uitkering verschuldigd aan de derde indien de verzekeringnemer, met het opzet de verzekeraar te misleiden, niet heeft voldaan aan de mededelingsplicht betreffende de derde.

ARTIKEL 941

- 1 Zodra de verzekeringnemer of de tot uitkering gerechtigde van de verwezenlijking van het risico op de hoogte is, of behoort te zijn, is hij verplicht aan de verzekeraar de verwezenlijking te melden. Dit geschiedt zo spoedig als redelijkerwijs mogelijk is.

- 2 De verzekeringnemer en de tot uitkering gerechtigde zijn verplicht binnen redelijke termijn de verzekeraar alle inlichtingen en bescheiden te verschaffen welke voor deze van belang zijn om zijn uitkeringsplicht te beoordelen.

- 3 Indien door de tot uitkering gerechtigde een verplichting als bedoeld in de leden 1 of 2 niet is nagekomen, kan de verzekeraar de uitkering verminderen met de schade die hij daardoor lijdt.

- 4 De verzekeraar kan het vervallen van het recht op uitkering wegens niet-nakoming van een verplichting als bedoeld in de leden 1 en 2 slechts bedingen voor het geval hij daardoor in een redelijk belang is geschaad.

- 5 Het recht op uitkering vervalt indien de verzekeringnemer of de tot uitkering gerechtigde een verplichting als bedoeld in de leden 1 en 2 niet is nagekomen met het opzet de verzekeraar te misleiden, behoudens voor zover deze misleiding het verval van het recht op uitkering niet rechtvaardigt.

ARTIKEL 962

- 1 Indien de verzekerde terzake van door hem geleden schade anders dan uit verzekering vorderingen tot schadevergoeding op derden heeft, gaan die vorderingen bij wijze van subrogatie op de verzekeraar over voor zover deze, al dan niet verplicht, die schade vergoedt. De verzekerde moet zich, nadat het risico zich heeft verwezenlijkt, onthouden van elke gedraging welke aan het recht van de verzekeraar tegen die derden afbreuk doet.

- 2 De verzekeraar kan de vordering waarin hij is gesubrogeerd, of die hij door overdracht heeft verkregen, niet ten nadele van het recht op schadevergoeding van de verzekerde uitoefenen.

- 3 De verzekeraar krijgt geen vordering op de verzekeringnemer, een medeverzekerde, de niet van tafel en bed gescheiden echtgenoot of de geregistreerde partner van een verzekerde, de andere levensgezel van een verzekerde, noch op de bloedverwanten in de rechte lijn van een verzekerde, op een werknemer of de werkgever van de verzekerde, of op degene die in dienst staat tot dezelfde werkgever als de verzekerde. Deze regel geldt niet voor zover zulk een persoon jegens de verzekerde aansprakelijk is wegens een omstandigheid die afbreuk zou hebben gedaan aan de uitkering, indien die omstandigheid aan de verzekerde zou zijn toe te rekenen.

BIJLAGE 4 GEGEVENSVERSTREKKING DOOR GEVOLMACHTIGDE AGENTEN AAN DERDEN

Zie toolkit 2022 Matrix informatie-uitwisseling

BIJLAGE 5 TOOLKIT INDICATORENLIJST

De toolkit Indicatorenlijst is terug te op afgesloten omgevingen zoals Volmachtbeheer/ Volmachtplein en NVGA.