

# Protocol Incidenten waarschuwingssysteem Financiële Instellingen

2013



Stichting **Fraudebestrijding  
Hypotheek**

 Nederlandse  
Vereniging van Banken

 **vfn**  
vereniging van  
financieringsinstellingen  
in Nederland

 **FOV**



VERBOND VAN VERZEKERAARS

Zorgverzekeraars Nederland



## Protocol Incidentenwaarschuwingssysteem Financiële Instellingen

**Nederlandse Vereniging van Banken (NVB)**

**Verbond van Verzekeraars (Verbond)**

**Vereniging van Financieringsondernemingen in Nederland (VFN)**

**Stichting Fraudebestrijding Hypotheken (SFH)**

**Zorgverzekeraars Nederland (ZN)**

**Federatie van Onderlinge Verzekeringsmaatschappijen (FOV)**

### **Preambule Protocol 'Incidentenwaarschuwingssysteem Financiële Instellingen'**

Financiële instellingen worden voortdurend geconfronteerd met (rechts)personen die een Financiële instelling willen schaden of op oneigenlijke gronden gebruik maken van diensten van de Financiële instelling. Dit vormt een gevaar voor de continuïteit en de integriteit van de financiële sector. Ook kunnen de belangen van een Financiële instelling en van cliënten en medewerkers van Financiële instellingen hierdoor worden geschaad.

Financiële instellingen hebben daarom ter bescherming maatregelen genomen. Daartoe zijn zij ook gehouden op grond van wetgeving zoals de Wet op het financieel toezicht (Wft) of de Wet ter voorkoming van witwassen en financieren terrorisme (Wwft). Ook de overheid, waaronder het Openbaar Ministerie, roept Financiële instellingen op om samen te werken op het gebied van criminaliteitsbestrijding. Een van de door Financiële instellingen genomen maatregelen is het vastleggen van gedragingen van (rechts)personen die hebben geleid of kunnen leiden tot benadeling van Financiële instellingen.

Deze gegevens worden door de Financiële instellingen vastgelegd in een Incidentenregister.

Aan het Incidentenregister is een Extern Verwijzingsregister gekoppeld. Dit Extern Verwijzingsregister bevat uitsluitend Verwijzingsgegevens (bijvoorbeeld een naam en geboortedatum of KvK-nummer) die onder strikte voorwaarden mogen worden opgenomen. Iedere Deelnemer heeft afhankelijk van het lidmaatschap van de betreffende Branchevereniging toegang tot een deel of meerdere delen van het Externe Verwijzingsregister. De banken die lid zijn van de Nederlandse Vereniging van Banken (NVB), alsmede de financieringsinstellingen, die lid zijn van de Vereniging van Financieringsinstellingen in Nederland (VFN), hebben de mogelijkheid om via een Verwijzingsapplicatie te toetsen of een (rechts)persoon in het extern verwijzingsregister (EVR) van de banken voorkomt.

De hypothecair financiers, aangesloten bij de Stichting Fraudebestrijding Hypotheken (SFH), hebben in 2004 het SFH-systeem ontwikkeld, dat deelnemers op vergelijkbare wijze in staat stelt om na te gaan of (rechts)personen in een extern verwijzingsregister voorkomen. Voor hypothecair financiers die geen lid zijn van NVB, Verbond of VFN is deze uitwisseling echter beperkt tot gegevens ingebracht door hypothecair financiers.

Verzekeraars kennen een Waarschuwingssysteem via de Stichting CIS. De Stichting CIS biedt de deelnemers de mogelijkheid om door middel van toetsing vast te stellen of een (rechts)persoon is opgenomen in het Externe verwijzingsregister van de verzekeraars.

Met de inwerkingtreding van dit Protocol in 2011 kunnen ook alle zorgverzekeraars, aangesloten bij Zorgverzekeraars Nederland, toetreden tot het Incidentenwaarschuwingssysteem. Voorwaarde is wel dat de individuele zorgverzekeraars hun incidentenregister hebben gemeld bij het CBP en het voorafgaand onderzoek is afgerond. Voor deze zorgverzekeraars geldt een soortgelijke constructie als bij de hypothecair financiers, waardoor voor leden van ZN, die geen lid zijn van het Verbond, de toegang is beperkt tot gegevens ingebracht door verzekeraars. Vanaf 2013 kunnen ook leden van de Federatie van Onderlinge Verzekeringmaatschappijen (FOV) toetreden tot het incidentenwaarschuwingssysteem.

Om er voor zorg te dragen dat de belangen van de Betrokkene op goede wijze worden beschermd, is opname in en raadpleging van het Incidentenregister en Extern Verwijzingsregister alleen toegestaan onder de voorwaarden van dit Protocol met de daarbij horende Annex.

Het CBP heeft vastgesteld dat de Verwerking van Persoonsgegevens zoals omschreven in het Protocol rechtmatig is. Het CBP heeft daartoe een voorafgaand en een nader onderzoek uitgevoerd. Het Protocol is geen Gedragscode zoals omschreven in artikel 25 WBP.

## **1 Overwegingen inzake het gerechtvaardigd belang van het Incidentenwaarschuwingssysteem voor Financiële instellingen**

- 1.1 Financiële instellingen worden voortdurend geconfronteerd met activiteiten van (rechts)personen die een Financiële instelling, haar medewerkers of cliënten op enigerlei wijze (dreigen te) schaden of voor onoorbare doeleinden gebruik maken van diensten van de Financiële instelling. Deze activiteiten kunnen een bedreiging vormen voor (I) de continuïteit en de integriteit van de financiële sector en/of de betreffende Financiële instelling(en), alsmede voor (II) de (financiële) belangen van cliënten en/of medewerkers van Financiële instellingen en/of de Financiële instellingen zelf. Door het vastleggen van relevante gegevens over deze (rechts)personen en door het creëren van mogelijkheden om deze gegevens te raadplegen, kunnen de betreffende risico's tijdig worden onderkend en verkleind en kunnen eventuele negatieve gevolgen worden beperkt.
- 1.2 Criminaliteitsbeheersing en risicomanagement vergen dat Financiële instellingen samenwerken, ondermeer door op basis van reciprociteit gegevens met betrekking tot (rechts)personen uit te wisselen.
- 1.3 Niet alleen de belangen van de Financiële instellingen, hun cliënten en medewerkers dwingen tot samenwerking. Ook van overheidswege wordt in toenemende mate een beroep gedaan op de Financiële instellingen om samen te werken op het gebied van criminaliteitsbestrijding. Het Openbaar Ministerie en andere (overheids)instanties verwachten dat Financiële instellingen de horizontale fraude zowel van binnenuit als van buitenaf gecoördineerd aanpakken ter ondersteuning van opsporing en vervolging. Zij dienen de noodzakelijke maatregelen te nemen om deze fraude te voorkomen. De noodzaak tot samenwerking en gegevensuitwisseling vloeit ook voort uit de intensivering van wet- en regelgeving en het beleid van de financiële toezichthouders (waaronder De Nederlandsche Bank (DNB)) om de integriteit van de financiële sector te versterken. Voor onder meer cliëntbeoordeling en de beoordeling van de integriteit van (potentiële) medewerkers impliceert deze beleidsintensivering, dat voldoende aandacht dient te worden besteed aan het risico van onoorbare handelingen en aan het (afbreuk)risico voor de Financiële Instelling.
- 1.4 De overwegingen 1.1 tot en met 1.3 Protocol vormen de rechtmatige grondslag voor het aanleggen en gebruiken van het Incidentenwaarschuwingssysteem Financiële Instellingen.
- 1.5 Financiële instellingen onderkennen dat de vastlegging van gegevens leidt tot het ontstaan van verzamelingen van Persoonsgegevens, op basis waarvan voor de betrokken (rechts)personen belangrijke beslissingen kunnen worden genomen. Het Verwerken van dergelijke gegevens dient daarom met waarborgen te worden omkleed. Dit Protocol bevat regels ten aanzien van de gegevensuitwisseling tussen de Financiële instellingen en voorziet in waarborgen tegen het ongeautoriseerd gebruik van het stelsel van gegevensuitwisseling.
- 1.6 Aangezien op basis van dit Protocol strafrechtelijke gegevens worden verwerkt ten behoeve van derden, anders dan krachtens een vergunning op grond van de Wet particuliere beveiligingsorganisaties en recherchebureaus (artikel 31 lid 1 onder c

juncto artikel 22 lid 4 en lid 5 WBP), is de gegevensverwerking in het kader van het Incidentenregister van de aan het waarschuwingssysteem deelnemende Financiële instellingen onderworpen aan het voorafgaand onderzoek door het College bescherming persoonsgegevens (CBP).

## 2 Begripsbepalingen

In dit Protocol wordt verstaan onder:

<b>Betrokkene</b>	degene op wie een Persoonsgegeven betrekking heeft;
<b>Branchevereniging</b>	Nederlandse Vereniging van Banken (NVB) of Verbond van Verzekeraars (Verbond) of Vereniging van Financieringsondernemingen in Nederland (VFN) of Zorgverzekeraars Nederland (ZN) of Stichting Fraudebestrijding Hypotheken (SFH) of de Federatie van Onderlinge Verzekeringmaatschappijen (FOV);
<b>CBP</b>	het College bescherming persoonsgegevens als bedoeld in artikel 51 WBP;
<b>Deelnemer</b>	het volgens artikel 7.1 Protocol toegelaten lid van de NVB, het Verbond, de VFN, ZN, FOV, dan wel aangesloten bij de SFH, welke beschikt over een Incidentenregister;
<b>Derde-organisatie</b>	een niet bij het Protocol aangesloten organisatie met wie, indien aan de voorwaarden als aangegeven in artikel 4.2.7 is voldaan, persoonsgegevens mogen worden uitgewisseld;
<b>Extern Verwijzingsregister (EVR)</b>	de deelverzameling van het Incidentenregister van de betreffende Deelnemers, welke uitsluitend Verwijzingsgegevens bevat met betrekking tot (rechts)personen en welke bestemd is voor gebruik door (de Organisaties van) alle Deelnemers;
<b>Geautoriseerde functionaris</b>	de persoon die binnen de Organisatie van de Deelnemer in het kader van zijn taakuitoefening gerechtigd is om gegevens aan het Extern Verwijzingsregister te toetsen;
<b>Incident</b>	een gebeurtenis die als gevolg heeft, zou kunnen hebben of heeft gehad dat de belangen, integriteit of veiligheid van de cliënten of medewerkers van een Financiële Instelling, de Financiële Instelling zelf of de financiële sector als geheel in het geding

zijn of kunnen zijn, zoals het falsificeren van nota's, identiteitsfraude, skimming, verduistering in dienstbetrekking, phishing en opzettelijke misleiding.

**Incidentenregister**

de gegevensverzameling(en) van de Deelnemer, waarin gegevens zijn vastgelegd voor het in artikel 4.1.1 Protocol genoemde doel, naar aanleiding van of betrekking hebbend op een (mogelijk) Incident;

**Waarschuwingssysteem**

het Incidentenwaarschuwingssysteem Financiële Instellingen dat bestaat uit de Incidentenregisters van de Deelnemers en de Brancheverenigingen en een Extern Verwijzingsregister;

**Financiële instelling**

een bank en/of verzekeraar en/of hypothecaire instelling en/of financieringsonderneming;

**Fraudeloket**

Veiligheidszaken van een Branchevereniging waar gegevens naar aanleiding van of betrekking hebbend op een (mogelijk) incident bij een Deelnemer worden vastgelegd conform het in artikel 4.1.1. Protocol genoemde doel ten behoeve van de coördinatiefunctie als bedoeld in artikel 4.2.3 Protocol;

**Organisatie van de Deelnemer**

de Deelnemer zelf, de dochtermaatschappijen van de Deelnemer (als bedoeld in artikel 2:24a BW) dan wel de groepsmaatschappijen waarmee een Deelnemer in een economische eenheid is verbonden (artikel 2:24b BW), als ook de bij de Rabobank Nederland aangesloten banken. Voorts worden de door de Deelnemer geautoriseerde gevolmachtigde tussenpersonen tot de organisatie van de Deelnemer gerekend, mits zij functioneren als financiële dienstverlener;

**(Primaire) Bron**

de Deelnemer die (als eerste) gegevens met betrekking tot een (rechts)persoon in het Extern Verwijzingsregister heeft opgenomen;

**Persoonsgegevens**

elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon;

**Protocol**

het Protocol Incidentenwaarschuwingssysteem Financiële Instellingen;

**Veiligheidszaken**

de afdeling of de persoon die binnen een Financiële instelling verantwoordelijk is voor de

verwerking van Persoonsgegevens in het kader van het waarborgen van de veiligheid en integriteit;

**Verwerking van Persoonsgegevens**

elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens;

**Verwijzingsapplicatie**

de technische voorziening die door een Deelnemer wordt gebruikt om toegang te verkrijgen tot het Extern Verwijzingsregister;

**Verwijzingsgegevens**

het gegeven dat van een (rechts)persoon is opgenomen in het Extern Verwijzingsregister overeenkomstig het bepaalde in artikel 5.2 Protocol, zijnde bijvoorbeeld de volledige naam van de (rechts)persoon en geboortedatum (of KvK-nummer);

**WBP**

Wet bescherming persoonsgegevens.

### 3 Algemeen

#### 3.1 Incidentenregister en Extern Verwijzingsregister

3.1.1 Iedere Deelnemer heeft een Incidentenregister, waarin door de betreffende Deelnemer gegevens van (rechts)personen worden vastgelegd ten behoeve van het in artikel 4.1.1 Protocol genoemde doel, naar aanleiding van of betrekking hebbend op een (mogelijk) Incident. Dit Incidentenregister is door de betreffende Deelnemer gemeld bij het CBP. Onder verantwoordelijkheid van de Deelnemer treedt Veiligheidszaken op als (sub)beheerder van het Incidentenregister.

3.1.2 Aan het Incidentenregister is het Extern Verwijzingsregister gekoppeld. Dit Extern Verwijzingsregister is raadpleegbaar door de Deelnemers, alsmede de Organisatie van de Deelnemers via een Verwijzingsapplicatie en bevat uitsluitend Verwijzingsgegevens die onder strikte voorwaarden conform artikel 5.2 Protocol door de Deelnemers mogen worden opgenomen.

#### 3.2 Toetsingsproces

3.2.1 Toetsing van persoonsgegevens op een registratie in het Extern Verwijzingsregister kan geautomatiseerd of handmatig worden uitgevoerd. De (geautoriseerde functionaris van de) deelnemer voert de hem ter beschikking staande persoonsgegevens en/of KvK nummer in het Extern Verwijzingsregister in. De (geautoriseerde functionaris van de) deelnemer wordt aangemerkt als bevrager. De bevraging van het Extern Verwijzingsregister 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 Extern Verwijzingsregister moet een geautoriseerde functionaris van de deelnemer het signaal uit het Extern Verwijzingsregister controleren op de mate van overeenstemming met de persoonsgegevens van betrokkene.

Wanneer overeenstemming afdoende is vastgesteld moet de geautoriseerde functionaris van de deelnemer Veiligheidszaken informeren. Deze afdeling benadert Veiligheidszaken van de (primaire) bron voor een toelichting op de registratie van betrokkene in het Extern Verwijzingsregister. Met inachtneming van de informatie die van de (primaire) bron is verkregen, adviseert Veiligheidszaken de bevrager. Dit advies kan onder meer het al dan niet onder voorwaarden aangaan van een overeenkomst, financiële dienst of arbeidsrelatie betreffen. Het is de deelnemer slechts toegestaan informatie over registratie in het Extern Verwijzingsregister toe te passen in zijn besluitvorming over betrokkene na kennisneming van het advies van Veiligheidszaken.

3.2.2 In overeenstemming met artikel 9.6.3 worden alle bevragingen gedurende maximaal één jaar door de deelnemer vastgelegd. Daarbij wordt geregistreerd wie bevraged heeft, waar vandaan de bevraging is uitgevoerd, wanneer de bevraging is gedaan en of het resultaat van de bevraging al dan niet een overeenstemming met de ingevoerde bevraging is geweest.



- 3.2.3 Tevens controleert Veiligheidszaken of inderdaad navraag is gedaan door de bevrager naar aanleiding van een 'hit'. Dit is mogelijk omdat Veiligheidszaken, alsmede Veiligheidszaken van de (Primaire) Bron, op de hoogte worden gesteld van een 'hit' via een door de Verwijzingsapplicatie aangemaakt automatisch bericht. Op deze wijze wordt voorkomen dat uitsluitend wordt geoordeeld aan de hand van een 'hit', zonder na te gaan wat de reden voor opname is.
- 3.2.4 Een toetsing die aanvankelijk niet in een 'hit' resulteerde kan binnen een periode van 2 maanden vanaf het moment van toetsing toch (automatisch) leiden tot een "hit". Dit wordt ook wel 'hit' achteraf" genoemd, een extra veiligheidsmaatregel om Financiële instellingen te beschermen. Dit is het geval indien het betreffende Verwijzingsgegeven dat leidt tot een 'hit' binnen de periode van 2 maanden na toetsing in het Externe Verwijzingsregister wordt opgenomen.

### **3.3 Invoervalidatie**

- 3.3.1 De Persoonsgegevens van de in het Incidentenregister opgenomen personen dienen in overeenstemming met de wet te zijn verkregen en dienen bij de (Primaire) Bron gedocumenteerd herleidbaar te zijn.
- 3.3.2 Daarvoor in aanmerking komende functionarissen worden geïnformeerd over de werking van het Waarschuwingssysteem. Zij worden er nadrukkelijk op gewezen dat het gebruik van het Waarschuwingssysteem uitsluitend is toegestaan binnen de regels van het Protocol en de binnen de Organisatie van de Deelnemer geldende interne procedures en voorschriften.
- 3.3.3 De Deelnemer dient zorg te dragen voor een zorgvuldige invoervalidatie en instructie aan Veiligheidszaken om zeker te stellen dat gegevens uitsluitend in overeenstemming met de regels van het Protocol worden ingevoerd in het Incidentenregister c.q. het Externe Verwijzingsregister.
- 3.3.4 Indien een Deelnemer twijfelt of invoer van bepaalde gegevens kan plaatsvinden volgens het Protocol, dient deze van invoer van de betreffende gegevens af te zien.

### **3.4 Geheimhouding**

De Persoonsgegevens die in het kader van dit Protocol worden verwerkt en worden opgenomen in het Incidentenregister en het Externe Verwijzingsregister dienen strikt vertrouwelijk te worden behandeld. De Deelnemer treft passende voorzieningen die waarborgen dat de Geautoriseerde functionaris onder een geheimhoudingsplicht valt.

### **3.5 Beveiliging**

De Deelnemer dient maatregelen te treffen om te waarborgen dat uitsluitend de Deelnemers toegang hebben tot het Incidentenregister en het Externe Verwijzingsregister. Verder neemt iedere Deelnemer passende technische en organisatorische maatregelen om Persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging dienen deze maatregelen te voorzien in een passend beveiligingsniveau, gelet op de risico's die de Verwerking en de aard van de te beschermen Persoonsgegevens met zich meebrengen.

## 4 Incidentenregister

### 4.1 Doel Incidentenregister

4.1.1 Met het oog op het kunnen deelnemen aan het Waarschuwingssysteem is iedere Deelnemer gehouden de volgende doelstelling voor het vastleggen van gegevens in het Incidentenregister te hanteren:

“Het geheel aan verwerkingen ten aanzien van het Incidentenregister heeft tot doel het ondersteunen van activiteiten gericht op het waarborgen van de veiligheid en de integriteit van de financiële sector, daaronder mede begrepen (het geheel van) activiteiten die gericht zijn:

- op het onderkennen, voorkomen, onderzoeken en bestrijden van gedragingen die kunnen leiden tot benadeling van de branche waar de financiële instelling deel van uitmaakt, van de economische eenheid (groep) waartoe de financiële instelling behoort, van de financiële instelling zelf, alsmede van haar cliënten en medewerkers;
- op het onderkennen, voorkomen, onderzoeken en bestrijden van oneigenlijk gebruik van producten, diensten en voorzieningen en/of (pogingen) tot strafbare of laakbare gedragingen en/of overtreding van (wettelijke) voorschriften, gericht tegen de branche waar de financiële instelling deel van uitmaakt, de economische eenheid (groep) waartoe de financiële instelling behoort, de financiële instelling zelf, alsmede haar cliënten en medewerkers;
- op het gebruik van en de deelname aan waarschuwingssystemen.”

### 4.2 Toegang tot het Incidentenregister

4.2.1 Toegang tot de in het Incidentenregister opgenomen gegevens door alle medewerkers uit de Organisatie van de Deelnemer is niet noodzakelijk noch wenselijk. De gegevens opgenomen in het Incidentenregister dienen strikt vertrouwelijk te worden behandeld. Dit brengt met zich mee dat de gegevens in het Incidentenregister alleen toegankelijk dienen te zijn voor Veiligheidszaken voor zover dit niet onverenigbaar is met het doel, als aangegeven in artikel 4.1.1. van het Protocol, waarvoor de gegevens zijn verkregen.

4.2.2 De gegevens in het Incidentenregister van de Deelnemers zijn met inachtneming van de bepalingen in de artikelen 4.2.4 tot en met 4.2.7 Protocol voor zover relevant op basis van reciprociteit beschikbaar voor Veiligheidszaken van de andere (Organisaties van de) Deelnemers

4.2.3 De gegevens uit het Incidentenregister van de Deelnemer mogen tevens worden uitgewisseld met functionarissen werkzaam bij de daartoe ingerichte, coördinatiefuncties van de NVB, Verbond, VFN, ZN, FOV en SFH (de fraudeloketten).

4.2.4 De (Organisaties van de) Deelnemers die lid zijn van het Verbond, FOV of ZN mogen gegevens uit het Incidentenregister uitwisselen met Veiligheidszaken van de Stichting Waarborgfonds Motorverkeer. De Stichting Waarborgfonds Motorverkeer onderschrijft het Protocol, is gehouden zorg te dragen voor strikte naleving van het

Protocol en verleent medewerking aan toezichtmaatregelen en –activiteiten op grond van het Protocol.

- 4.2.5 Deelnemers aan SFH, die geen lid zijn van de NVB, VFN, FOV of het Verbond, kunnen gegevens uitwisselen met Incidentenregisters van Veiligheidszaken van andere Deelnemers aan SFH voor zover die gegevens betrekking hebben op fraude met hypothecaire financieringen.
- 4.2.6 Zorgverzekeraars die geen lid zijn van het Verbond of FOV kunnen alleen gegevens uitwisselen met Incidentenregisters van Veiligheidszaken van Deelnemers die lid zijn van het Verbond, ZN of FOV.
- 4.2.7 De gegevens uit het Incidentenregister mogen slechts worden uitgewisseld met Veiligheidszaken van derde-organisaties als wordt voldaan aan ieder van de volgende criteria:
  - a. de derde-organisatie beschikt over een wettelijke grondslag;
  - b. de taakuitoefening van de derde-organisatie staat in direct verband met de werkzaamheden van de financiële instellingen;
  - c. de derde-organisatie heeft een gerechtvaardigd belang bij de uitwisseling van de gegevens;
  - d. de derde-organisatie onderschrijft het Protocol, draagt zorg voor strikte naleving van het Protocol en verleent medewerking aan toezichtmaatregelen en –activiteiten op grond van het Protocol; en
  - e. de gegevensuitwisseling met de derde-organisatie maakt uitdrukkelijk deel uit van de informatieplicht van de verantwoordelijke.

### **4.3 Verwijdering van gegevens uit het Incidentenregister**

- 4.3.1 Indien niet langer aan de voorwaarden van artikel 3.1.1 Protocol wordt voldaan draagt de Deelnemer zorg voor verwijdering van dit gegeven uit het Incidentenregister. De Deelnemer doet dit ook op basis van een gehonoreerd verzoek tot verwijdering van gegevens conform artikel 9.4 Protocol.
- 4.3.2 Verwijdering van gegevens uit het Incidentenregister moet plaatsvinden uiterlijk 8 jaar na opname van het betreffende gegeven in het Incidentenregister, tenzij zich ten aanzien van de betreffende (rechts)persoon een nieuwe aanleiding heeft voorgedaan die de opname in het Incidentenregister rechtvaardigt.

## **5 Extern Verwijzingsregister**

### **5.1 Functie van het Extern Verwijzingsregister**

- 5.1.1 Volledige en ongecontroleerde toegang tot het Incidentenregister van een Deelnemer door de overige Deelnemers is niet wenselijk. Daarom is er voor gekozen aan het Incidentenregister een Extern Verwijzingsregister te koppelen. In het Extern Verwijzingsregister zijn uitsluitend Verwijzingsgegevens opgenomen. Het Extern Verwijzingsregister is raadpleegbaar door de (Organisaties van de) Deelnemers. Nadat door een Deelnemer wordt vastgesteld dat een (rechts)persoon is opgenomen in het Externe Verwijzingsregister, zijn volgens het bepaalde in artikel 4.2 Protocol gegevens uit het Incidentenregister voor de Deelnemer beschikbaar. Op deze wijze

worden gegevens uit het Incidentenregister op een zorgvuldige en gecontroleerde wijze beschikbaar voor de (Organisaties van de) Deelnemers.

## **5.2 Vastlegging van gegevens in het Extern Verwijzingsregister**

5.2.1 De Deelnemer dient de Verwijzingsgegevens van (rechts)personen die aan de hierna onder a en b vermelde criteria voldoen en na toepassing van het onder c genoemde proportionaliteitsbeginsel op te nemen in het Extern Verwijzingsregister.

- a) De gedraging(en) van de (rechts)persoon vormen, vormen of kunnen een bedreiging vormen voor (I) de (financiële) belangen van cliënten en/of medewerkers van een Financiële instelling, alsmede de (Organisatie van de) Financiële instelling(en) zelf of (II) de continuïteit en/of de integriteit van de financiële sector.
- b) In voldoende mate staat vast dat de betreffende (rechts)persoon betrokken is bij de onder a bedoelde gedraging(en). Deze vaststelling betekent dat van strafbare feiten in principe aangifte of klachten wordt gedaan bij een opsporingsambtenaar.
- c) Het proportionaliteitsbeginsel wordt in acht genomen. Dit houdt in dat Veiligheidszaken vaststelt, dat het belang van opname in het Externe Verwijzingsregister prevaleert boven de mogelijk nadelige gevolgen voor de Betrokkene als gevolg van opname van zijn Persoonsgegevens in het Extern Verwijzingsregister.

5.2.2 Een Deelnemer is niet gehouden tot opname van Verwijzingsgegevens in het Extern Verwijzingsregister indien opsporingsbelangen of andere gewichtige belangen hiertoe aanleiding geven.

5.2.3 In geval sprake is van strafbare feiten zal de directie van de Deelnemer, op advies van Veiligheidszaken, daarvan aangifte of klachten doen behoudens in de gevallen waarin opsporingsbelangen of andere belangen aan het doen van aangifte of klachten in de weg staan. In die gevallen is de Deelnemer verplicht tot vastlegging van de redenen op grond waarvan de Deelnemer, al dan niet tijdelijk, heeft afgezien van het doen van aangifte of klachten.

5.2.4 De beslissing tot vastlegging van Verwijzingsgegevens in het Extern Verwijzingsregister wordt genomen door Veiligheidszaken.

5.2.5 Opname gebeurt in beginsel door de Deelnemer wiens belang in het geding is. De overige bij het Incident betrokken Deelnemers kunnen echter ook tot opname van de Verwijzingsgegevens overgaan, indien het belang van de financiële sector in het geding is.

## **5.3 Verwijdering van gegevens uit het Extern Verwijzingsregister**

5.3.1 Indien niet langer aan de voorwaarden van artikel 5.2.1 Protocol wordt voldaan draagt de Deelnemer zorg voor verwijdering van de door de Deelnemer opgenomen Verwijzingsgegevens uit het Extern Verwijzingsregister. De Deelnemer doet dit ook

naar aanleiding van een gehonoreerd verzoek tot verwijdering conform artikel 9.4 Protocol.

- 5.3.2 Verwijdering van Verwijzingsgegevens uit het Extern Verwijzingsregister moet plaatsvinden uiterlijk 8 jaar na opname van het betreffende gegeven in het Incidentenregister, tenzij zich ten aanzien van de betreffende (rechts)persoon een nieuwe aanleiding heeft voorgedaan en opname in het Extern Verwijzingsregister conform artikel 5.2.1 Protocol heeft plaatsgevonden.

#### **5.4 Toegang**

- 5.4.1 Het Extern Verwijzingsregister is voor (de Organisatie van) de Deelnemer uitsluitend toegankelijk langs geautomatiseerde weg.
- 5.4.2 Toetsing vindt plaats volgens het proces als omschreven in artikel 3.2 Protocol.

### **6 Begeleidingscommissie**

- 6.1 Om de uniformiteit met betrekking tot de uitleg en de toepassing van het Protocol te waarborgen is per Branchevereniging of voor meerdere Brancheverenigingen samen een begeleidingscommissie ingesteld. De begeleidingscommissie bestaat uit door de betreffende Branchevereniging(en) aangewezen personen.
- 6.2 Indien daartoe aanleiding bestaat adviseert de begeleidingscommissie de Deelnemers over de toepassing van de onder artikel 5.2.1 Protocol genoemde vastleggingcriteria. De Deelnemer dient op verzoek van de begeleidingscommissie alle relevante informatie over de uitleg en toepassing van de vastleggingcriteria aan de begeleidingscommissie te verstrekken. De Deelnemer is gebonden aan de door de begeleidingscommissie gevolgde uitleg. De begeleidingscommissie brengt van haar bevindingen in ieder geval één keer per jaar verslag uit aan het bestuur van de betreffende Branchevereniging.

### **7 Deelname aan het Waarschuwingssysteem**

#### **7.1 Toetreding**

- 7.1.1 Een Financiële instelling heeft het recht om toe te treden tot het Waarschuwingssysteem, indien de begeleidingscommissie van oordeel is dat de Financiële instelling aan de daaraan te stellen eisen als opgenomen in het Protocol voldoet.
- 7.1.2 Bij toetreding dient door de Financiële instelling een toetredingsverklaring te worden getekend, waarin de Financiële instelling verklaart het Protocol te zullen naleven en over een vergunning te beschikken op grond van de financiële toezichtwetgeving.

#### **7.2 Uittreding**

- 7.2.1 Een Deelnemer heeft het recht uit het Waarschuwingssysteem te treden. De Deelnemer dient zijn wens tot uittreding schriftelijk bij de betreffende

Branchevereniging kenbaar te maken onder vermelding van de gewenste datum van uittreding.

7.2.2 Na uittreding zal de ex-Deelnemer noch de Organisatie van de ex-Deelnemer nog langer toegang hebben tot het Extern Verwijzingsregister.

7.2.3 De ex-Deelnemer dient er voor zorg te dragen dat de door haar aangebrachte Verwijzingsgegevens direct na datum van uittreding uit het Extern Verwijzingsregister zijn verwijderd.

### **7.3 Uitsluiting**

7.3.1 Indien een Deelnemer het Protocol niet naleeft, is het bestuur van de betreffende Branchevereniging op advies van de begeleidingscommissie gerechtigd de Deelnemer uit te sluiten van deelname aan het Waarschuwingssysteem.

7.3.2 Na uitsluiting zal de ex-Deelnemer noch de Organisatie van de ex-Deelnemer nog langer toegang hebben tot het Externe Verwijzingsregister.

7.3.3 Na uitsluiting dient de ex-Deelnemer er direct voor zorg te dragen dat de door haar aangebrachte gegevens uit het Extern Verwijzingsregister worden verwijderd.

### **7.4 Kosten**

7.4.1 Aan deelname aan het Waarschuwingssysteem zijn kosten verbonden die bij iedere Deelnemer in rekening worden gebracht op basis van een nader vast te stellen verrekeningsmethodiek.

## **8 Rechten en plichten van de Deelnemer**

### **8.1 Reciprociteit**

8.1.1 Deelnemers zijn met inachtneming van hetgeen is bepaald in artikel 7.1.2 Protocol ook ten aanzien van elkaar gehouden tot naleving van het Protocol.

### **8.2 Bijstand**

8.2.1 Deelnemers verlenen elkaar desgevraagd bijstand in het geval van vorderingen of verzoeken in verband met de Verwerking van Persoonsgegevens zoals bepaald in het Protocol.

### **8.3 Aansprakelijkheid**

8.3.1 De Deelnemer die gegevens verwerkt in het Extern Verwijzingsregister is aansprakelijk voor schade die ontstaat doordat de gegevens door deze Deelnemer niet conform het Protocol zijn verwerkt in het Extern Verwijzingsregister, tenzij deze tekortkoming in de nakoming deze Deelnemer niet kan worden toegerekend.

8.3.2 De Deelnemer die gegevens verwerkt welke de Deelnemer via het Extern

Verwijzingsregister heeft verkregen is aansprakelijk voor schade die ontstaat doordat de Deelnemer onjuist of disproportioneel gebruik van deze gegevens heeft gemaakt, tenzij deze tekortkoming in de nakoming de Deelnemer niet kan worden toegerekend.

#### **8.4 Werkinstructies**

8.4.1 Deelnemers zijn gehouden om de werkwijze zoals neergelegd in het Protocol te concretiseren in werkprocessen. Deelnemers kunnen daarbij gebruik maken van voorbeeldwerkinstructies en/of handreikingen van de onderscheidene brancheverenigingen.

### **9 Rechten van de Betrokkene**

#### **9.1 Mededeling van opname**

9.1.1 De Betrokkene wiens Persoonsgegevens in het Incidentenregister respectievelijk het Extern Verwijzingsregister zijn opgenomen, heeft recht op mededeling van opname uiterlijk op het moment van de eerste verstrekking. Daarbij wordt nadere informatie verstrekt voor zover dat gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen.

9.1.2 Indien de Betrokkene niet overeenkomstig het bepaalde in artikel 9.1.1 Protocol is geïnformeerd wordt hij op de hoogte gesteld van opname zodra een toets heeft geresulteerd in een 'hit'. Dit dient te gebeuren door Veiligheidszaken van de Deelnemer c.q. - Veiligheidszaken van de (Primaire) Bron.

9.1.3 De mededeling blijft achterwege, indien sprake is van een uitzonderingssituatie als bedoeld in artikel 34 WBP of voor zover dat noodzakelijk is in het belang van de voorkoming, opsporing en vervolging van strafbare feiten of de bescherming van de betrokkene of de rechten en vrijheden van anderen.

#### **9.2 Afschrift Protocol**

9.2.1 Bij de Branchevereniging van de Deelnemer kan een afschrift van het Protocol worden opgevraagd. Dit Protocol zal tevens kunnen worden geraadpleegd via de website van de Branchevereniging.

#### **9.3 Kennisneming**

9.3.1 Een Betrokkene heeft het recht zich – met redelijke tussenpozen - tot een Deelnemer te wenden met het verzoek hem mede te delen of hem betreffende Persoonsgegevens in het Incidentenregister en/of het Extern Verwijzingsregister zijn opgenomen.

9.3.2 Het in artikel 9.3.1 Protocol genoemde verzoek dient schriftelijk te worden gedaan. Aan het verzoek wordt eerst gehoor gegeven nadat de Betrokkene zich heeft gelegitimeerd.

- 9.3.3 De Deelnemer zal, behoudens de in artikel 9.3.5 Protocol genoemde uitzonderingsgevallen, de Betrokkene binnen vier weken na ontvangst van het verzoek schriftelijk mededelen of, en zo ja welke hem betreffende Persoonsgegevens worden verwerkt.
- 9.3.4 Indien Persoonsgegevens worden verwerkt, bevat de mededeling als bedoeld in artikel 9.3.3 Protocol een volledig overzicht daarvan 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.
- 9.3.5 De mededeling blijft achterwege, voor zover dat noodzakelijk is in het belang van de voorkoming, opsporing en vervolging van strafbare feiten of de bescherming van de betrokkene of de rechten en vrijheden van anderen.

#### **9.4 Correctie**

- 9.4.1 Indien uit het verstrekte overzicht blijkt dat Persoonsgegevens feitelijk onjuist zijn, voor het doel van de Verwerking onvolledig of niet ter zake dienend zijn, dan wel anderszins in strijd met een wettelijk voorschrift worden verwerkt, kan de Betrokkene schriftelijk verzoeken om verbetering, aanvulling, verwijdering of afscherming van de betreffende Persoonsgegevens.
- 9.4.2 De Deelnemer bericht de Betrokkene binnen vier weken na ontvangst van het verzoek schriftelijk of en in hoeverre de Deelnemer het verzoek, als bedoeld in artikel 9.4.1. Protocol, zal honoreren. Indien niet of niet volledig aan het verzoek van de Betrokkene wordt voldaan wordt dit met redenen omkleed.
- 9.4.3 De Deelnemer draagt er voor zorg dat indien door de Deelnemer wordt besloten tot verbetering, aanvulling, verwijdering of afscherming dit zo spoedig mogelijk wordt uitgevoerd.

#### **9.5 Recht van verzet**

- 9.5.1 De betrokkene kan bij de verantwoordelijke te allen tijde verzet aantekenen in verband met zijn bijzondere persoonlijke omstandigheden.
- 9.5.2 De verantwoordelijke beoordeelt binnen vier weken na ontvangst van het verzet of het verzet gerechtvaardigd is. Indien het verzet gerechtvaardigd is beëindigt hij terstond de verwerking.

#### **9.6 Kettingbepaling**

- 9.6.1 De WBP verplicht een Deelnemer niet om bij te houden aan welke Deelnemers Persoonsgegevens uit het Incidentenregister zijn verstrekt.
- 9.6.2 De WBP verplicht de Deelnemer wel om, in het geval dat Persoonsgegevens zijn verbeterd, aangevuld, verwijderd of afgeschermd naar aanleiding van een verzoek overeenkomst artikel 9.4 Protocol, de Deelnemers waaraan de Persoonsgegevens



daaraan voorafgaand zijn verstrekt daarvan in kennis te stellen, tenzij dit onmogelijk is of een onevenredige inspanning vergt.

- 9.6.3 Om die reden onderhoudt de Deelnemer een overzicht van de verstrekkingen die hebben plaatsgevonden in het kader van dit Protocol aan de andere Deelnemer, voor de duur van één jaar vanaf de datum waarop de Persoonsgegevens aan de andere Deelnemer zijn verstrekt.

## **10 Overige regels**

### **10.1 Geschillen**

- 10.1 Bij een geschil over de juistheid en rechtmatigheid van een specifieke vastlegging in het Incidentenregister en/of Externe Verwijzingsregister kan de Betrokkene zich wenden tot het bestuur/de directie van de betreffende Deelnemer.
- 10.2 Indien deze stap niet leidt tot een oplossing van het geschil kan de Betrokkene zich wenden tot: (I) de Stichting Klachteninstituut Financiële Dienstverlening (KiFiD), Postbus 93257, 2509 AG Den Haag; (II) de Stichting Klachten en Geschillen Zorgverzekeringen (SKGZ) indien het geschil betrekking heeft op de zorgverzekering dan wel ziektekostenverzekering, Postbus 291, 3700 AG te Zeist (III) het CBP; of (IV) de bevoegde rechter.

## **11 Toezicht**

- 11.1 De Deelnemer is gehouden de naleving van het Protocol periodiek te (laten) controleren en hiervan door middel van een rapport verslag te doen.
- 11.2 Indien wordt vermoed dat een Deelnemer zich niet houdt aan het bepaalde in het Protocol dient dit door de Deelnemer te worden onderzocht en dient hierover een rapport te worden opgesteld, waarvan vertrouwelijk verslag dient te worden gedaan aan het bestuur van de betreffende Deelnemer.
- 11.3 Indien een Deelnemer zich niet houdt aan het bepaalde in het Protocol of wordt vermoed dat een Deelnemer zich niet houdt aan het bepaalde in het Protocol kan het bestuur van NVB, Verbond, SFH, VFN, ZN of FOV uit eigen beweging of op verzoek van een Deelnemer verzoeken om een afschrift van de onder artikel 11.1 en 11.2 Protocol genoemde rapporten en is de Deelnemer gehouden hiervan een afschrift te verstrekken.
- 11.4 Indien een Deelnemer weigert overeenkomstig artikel 11.3 Protocol een afschrift te verstrekken kan tot uitsluiting conform artikel 7.3 Protocol worden overgegaan.

## **12 Wijzigingen protocol**

- 12.1 Het bestuur van NVB, Verbond, VFN, ZN, FOV en SFH kunnen, gehoord de verschillende begeleidingscommissies, gezamenlijk besluiten tot wijziging van het Protocol. Een dergelijk besluit wordt genomen nadat de aanpassingen of wijzigingen niet op bezwaren zijn gestuit bij het CBP.

## Annex bij het Protocol Incidentenwaarschuwingssysteem Financiële Instellingen

### Aanleiding

Financiële instellingen, waaronder verzekeraars, hypothecaire instellingen, financieringsondernemingen en banken worden verstaan, hun cliënten en medewerkers hebben er belang bij dat fraude en criminaliteit die tegen hen zijn gericht tijdig worden ontdekt en bestreden. Dat belang wordt algemeen erkend en heeft zijn weerslag gevonden in de Wet op het financieel toezicht (Wft) en de Wet ter voorkoming van witwassen en financiering van terrorisme (Wwft). Op grond van beide wetten wordt financiële instellingen uitdrukkelijk opgedragen te beschikken over procedures en maatregelen om de risico's van cliënten te bepalen voor de integere uitoefening van haar bedrijf (de zogenaamde Customer Due Diligence: 'het ken-uw-klant-principe') alsmede de betrouwbaarheid te kunnen toetsen van medewerkers op integriteitgevoelige functies. Het Incidentenwaarschuwingssysteem financiële instellingen (in het vervolg: Waarschuwingssysteem) is een van de maatregelen om aan deze wettelijke verplichtingen vorm en inhoud te geven.

Ver voor de Wft en Wwft van kracht werden hadden de meeste financiële instellingen reeds de noodzakelijke maatregelen getroffen. Vanaf het begin van de jaren negentig hebben zij een afdeling Veiligheidszaken ingericht of een fraudecoördinator aangesteld, waar alle incidenten die zich voordoen binnen de organisatie moeten worden gemeld en vastgelegd in een zogeheten Incidentenregister. Om een optimale bestrijding te bereiken werd in 1990 besloten om het gebruik van de gegevens niet te beperken tot de eigen organisatie, maar om elkaar te ondersteunen bij de aanpak van fraude en criminaliteit. Hiervoor werd een protocol geschreven en het Interbancaire Registratie en Informatie Systeem (IRIS) opgezet. Deze registratie is in 1997 vervangen door het huidige Waarschuwingssysteem dat tot doel heeft de veiligheid en integriteit van de financiële sector, degenen die daarin werkzaam zijn en degenen die van financiële diensten gebruik maken, te waarborgen. Door de verzekeraars werd in 1998 een soortgelijk systeem opgezet, waarbij de spelregels werden vastgelegd in het 'Protocol betreffende preventie en bestrijding van fraude in de Verzekeringsbranche'. In 2002 werden beide systemen geïntegreerd in het huidige Incidentenwaarschuwingssysteem.

Zowel onder het regime van de Wet persoonsregistraties als de Wet bescherming persoonsgegevens (WBP) is het aan het Waarschuwingssysteem ten grondslag liggende Protocol Incidentenwaarschuwingssysteem financiële instellingen (in het vervolg: Protocol) afgestemd met en goedgekeurd door de toezichthouder voor privacybescherming in Nederland (eerst de Registratiekamer en later het College bescherming persoonsgegevens, CBP). Vanaf 2004 nemen ook de hypothecaire instellingen daaraan deel. Met de inwerkingtreding van de herziene versie van het Protocol in 2011 zijn ook alle zorgverzekeraars die zijn aangesloten bij Zorgverzekeraars Nederland toegetreden. Sinds 2013 kunnen ook leden van de Federatie van Onderlinge Verzekeringmaatschappijen (FOV) toetreden tot het Protocol.

### Werkwijze

Alle deelnemers aan het Waarschuwingssysteem beschikken over een Incidentenregister waarin onder strikte voorwaarden incidenten worden vastgelegd. Deze voorwaarden zijn vastgelegd in het Protocol. Als incidenten kunnen bijvoorbeeld voorkomen het falsificeren van nota's, identiteitsfraude, skimming, verduistering in dienstbetrekking, phishing en

opzettelijke misleiding. In het Incidentenregister worden karakteristieken van het incident vastgelegd en van de daarbij betrokken personen, evenals handelingen die naar aanleiding van het incident hebben plaatsgevonden. De gegevens in het Incidentenregister worden door de veiligheidsafdelingen of de fraudecoördinatoren van de financiële instellingen geraadpleegd als dat noodzakelijk is voor de uitvoering van hun werkzaamheden. Daarbij kan gedacht worden aan trendanalyse, het ontwikkelen van fraudepreventiestrategieën, pre-employmentscreening en integriteittoetsing, schadeverhaal en Customer Due Diligence.

Aan het Incidentenregister is een Extern Verwijzingsregister (EVR) gekoppeld om gegevens uit Incidentenregisters voor anderen dan medewerkers van de eigen veiligheidsafdelingen toegankelijk te maken. Dit register bevat slechts identificerende gegevens. Gebruikers van de gegevens kunnen slechts vaststellen of iemand in het EVR voorkomt ('hit – no hit-systeem'). Om de gegevens uit de Incidentenregisters van de deelnemers daadwerkelijk toetsbaar te maken voor de organisatie van de deelnemer of voor andere deelnemers wordt gebruik gemaakt van een technische voorziening, een zogenaamde verwijzingsapplicatie. De toetser ziet in geval van een 'hit' niet waarom iemand in het systeem is opgenomen.

Het Protocol stelt naast de regels voor het Incidentenregister ook de voorwaarden waaraan deelnemers moeten voldoen wanneer personen in het EVR worden opgenomen en wanneer het waarschuwingssysteem mag worden geraadpleegd. Ter verduidelijking voor (potentiële) cliënten en (potentiële) medewerkers van financiële instellingen wordt het Protocol op drie onderdelen nader toegelicht. Het betreft de kenbaarheid van het systeem, het aangiftebeleid en de compenserende maatregelen die zijn getroffen wanneer om de aangegeven reden van aangifte wordt afgezien.

### **Kenbaarheid**

De hoofdregel van de zorgplicht uit de WBP is dat persoonsgegevens in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze worden verwerkt. Deze zorgvuldigheidsnorm houdt onder andere de verplichting in dat de betrokkene van het bestaan van de verwerking kennis heeft kunnen nemen en ingelicht is over de omstandigheden waaronder zijn gegevens zijn of worden verkregen. Aan dit kenbaarheidvereiste wordt voldaan doordat op de websites van de betrokken brancheorganisatie het bestaan van het Waarschuwingssysteem wordt aangegeven en dat door financiële instellingen bij andere relevante communicatie richting cliënt het bestaan en de voorwaarden bekend worden gemaakt. Als onderdeel van de informatieplicht, waaraan op grond van artikel 34 behoudens de in de WBP genoemde uitzonderingen moet zijn voldaan, wordt de betrokkene op het bestaan van het EVR gewezen.

### **Aangiftebeleid**

Voor financiële instellingen die lid zijn van de brancheorganisaties die deelnemen aan het Protocol geldt als uitgangspunt dat aangifte wordt gedaan of een klacht ingediend bij een opsporingsambtenaar indien de gedragingen van betrokkene kunnen worden aangemerkt als strafbaar feit.

Dit neemt niet weg dat zich in de praktijk situaties voordoen (vaak per branche verschillend) waarbij (nog) geen aangifte wordt gedaan maar waarbij opname in het EVR wel geboden is. Ook doen zich situaties voor waarbij opname in het EVR geboden is, maar pas later aangifte kan worden gedaan. Tenslotte zijn er situaties dat de financiële instelling zelf geen aangifte kan doen of klacht kan indienen, maar waarbij opname in het EVR wel geboden is. Ter verduidelijking wordt hierna een aantal – niet-limitatieve – voorbeelden gegeven.

- **Onnodige stigmatisering door het doen van aangifte of klacht**

Het doen van aangifte heeft voor betrokkene soms ongewenste effecten die de financiële sector in bepaalde situaties disproportioneel acht. Het doen van aangifte leidt immers tot opname van persoonsgegevens van de verdachte in gegevensverwerkingen die vallen onder de Wet politiegegevens en/of de Wet justitiële en strafvorderlijke gegevens. Voor betrokkene kan opname in deze gegevensverwerkingen belemmerend zijn bij het vinden van werk of het behouden daarvan. Hij of zij heeft dan immers een strafrechtelijk verleden. Toch blijft het geboden andere financiële instellingen te kunnen waarschuwen dat iemand zich in het verleden op een bepaalde manier heeft gedragen.

Voor kwetsbare categorieën personen kan een extra afweging bij het doen van aangifte op zijn plaats zijn. Daarbij kan worden gedacht aan jongeren die verdacht worden van medeplichtigheid bij het witwassen van crimineel geld of bij andere frauduleuze praktijken doordat zij hun bankrekening beschikbaar hebben gesteld. Het zijn vaak first-offenders die zich niet bewust zijn van de gevolgen van hun handelen. In die situaties is opname in het EVR als signaal voor andere financiële instellingen wel noodzakelijk, maar het doen van aangifte (vaak in overleg met opsporingsinstanties) niet.

- **Geen aangifte vanuit maatschappelijke overwegingen**

Van afzien van een aangifte tegen (rechts)personen die frauderen met (zorg)verzekeringen kan sprake zijn als het doen van aangifte en strafrechtelijke vervolging onevenredige nadelige gevolgen hebben voor de omgeving van de fraudeur. Zo kan een veroordeling van een zorgaanbieder leiden tot het intrekken van diens toelating c.q. het doorhalen van diens registratie op grond van de Wet op de beroepen in de individuele gezondheidszorg (Wet BIG). Hierdoor kunnen niet bij het incident betrokken personen in de werkomgeving van de zorgaanbieder getroffen worden. Zorgverzekeraars zullen in alle gevallen de afweging moeten maken of het doen van aangifte het doel niet voorbij schiet. Het doel van opname in EVR is in dit voorbeeld immers primair het afgeven van een waarschuwing aan verzekeraars. De waarschuwing via een hit in het Extern Verwijzingsregister betekent dat de fraudeur zich mag verheugen in extra aandacht van de (zorg)verzekeraar in die zin dat extra waakzaamheid is geboden bij het aangaan van een overeenkomst, het beoordelen van nota's en andere geldstromen.

- **Risico van verstoring van onderzoeken van overheidswege**

Het doen van aangifte heeft in bepaalde situaties het onwenselijke effect dat onderzoeken van overheidswege, zoals van politie, justitie, AIVD, AFM en DNB, negatief kunnen worden beïnvloed. In deze situaties is het ter bescherming van de branche wel noodzakelijk dat opname in EVR plaatsvindt maar dat pas later aangifte wordt gedaan.

Een voorbeeld hiervan zijn onderzoeken die hypothecair financiers (deelnemers SFH) verrichten wanneer zij fraude hebben geconstateerd met loonstroken. Vaak is in eerste instantie al duidelijk dat een hypotheekaanvrager heeft gefraudeerd door valse inkomstgegevens te overleggen, maar moet verder onderzoek worden gedaan naar de rol van andere betrokkenen (zoals taxateurs, tussenpersonen, makelaars en notarissen). De ervaring heeft geleerd dat een valse hypotheekaanvraag niet op zichzelf staat, maar onderdeel vormt van het handelen en nalaten van (rechts)personen die in georganiseerd verband op grote schaal misbruik maken van het stelsel van financiële dienstverlening. In overleg met het OM wordt in dit soort zaken vaak bepaald wanneer het doen van aangifte opportuun is en bij welke opsporingsinstantie dat het meest effectief is. Aangifte wordt veelal

gedaan bij bovenregionale of landelijke opsporingsteams. Daarmee wordt voorkomen dat opsporingsinstanties langs elkaar heen werken.

Omdat de aanvragers veelal gelijktijdig een offerte vragen bij meerdere hypothecair financiers, is opname van gegevens van betrokkene(n) in het EVR in een vroeg stadium essentieel. Daarmee wordt voorkomen dat tijdens het lopende (opsporings)onderzoek contractuele verhoudingen worden aangegaan die later niet meer kunnen worden teruggedraaid.

- **Financiële instelling doet zelf geen aangifte of kan zelf geen klacht indienen**

Niet in alle gevallen wordt door de financiële instelling zelf aangifte gedaan. Vooral bij fraude in het betalingsverkeer is het veelal de benadeelde cliënt van de financiële instelling zelf die aangifte doet van valsheid in geschrifte of oplichting. De rekening van de cliënt is immers frauduleus gedebiteerd en de cliënt is daarmee slachtoffer van het strafbare feit. Bij klachtdelicten (zoals schending van geheimen) kan alleen het slachtoffer aangifte doen, terwijl door de gedragingen van betrokkene wel sprake kan zijn van een situatie als bedoeld in artikel 5.2.1 aanhef en onder a van het Protocol. In deze situaties kan het ter bescherming van de branche noodzakelijk zijn dat opname in EVR plaatsvindt.

Ook wanneer afgezien wordt van het doen van aangifte of de besloten wordt de aangifte uit te stellen, blijven de criteria voor opname in het EVR onverminderd van toepassing. In die gevallen dat van strafbare feiten geen aangifte of klachte wordt gedaan blijft het uitgangspunt dat een deelnemer moet kunnen aantonen dat in voldoende mate vaststaat dat de gedraging de kwalificatie strafbaar feit kan dragen en dat voldoende bewijs van betrokkenheid tegen de betreffende (rechts)persoon voorhanden is.

### **Waarborgen voor de betrokkene**

Financiële instellingen hebben zich uitgesproken om in geval van een strafbaar feit in principe aangifte te doen. Het doen van aangifte dan wel het bewust afwijken van die norm is met de nodige waarborgen omkleed. Financiële instellingen hebben daartoe in de vorm van voorbeeldinstructies compenserende voorwaarden ingebouwd. Om uniformiteit te bevorderen, zullen al bestaande werkinstructies worden aangepast en zullen per branche voorbeeldinstructies worden opgesteld.

Bij deze compenserende waarborgen gaat het om waarborgen die betrekking hebben op de fase vóór opname in het Incidentenregister en EVR en waarborgen die gelden nadat opname heeft plaatsgevonden. In het beleid betreffende de toepassing van het Waarschuwingssysteem is aangegeven welke de onderdelen zijn waarop een dossier wordt beoordeeld en in welke mate bewijsmiddelen voorhanden moeten zijn om te kunnen vaststellen dat sprake is van een zware verdenking of bewezenverklaring. Uitgangspunt is dat in een gerechtelijke procedure moet kunnen worden aangetoond dat afdoende bewijs aanwezig is om de kwalificatie fraude of een andere onoorbare of strafbare gedraging te dragen ten opzichte van een aantoonbaar betrokken (rechts)persoon. Ontbreekt een van deze elementen dan behoort geen registratie plaats te vinden. Zij vormen de criteria als aangegeven in artikel 5.2.1, onder a en b.

In de werkinstructies is nadrukkelijk aandacht voor de proportionaliteitsafweging. Voor eventuele plaatsing in het EVR dient het belang van de deelnemer, en die van de andere deelnemers, bij opname te worden afgewogen tegen de gevolgen van de opname voor de betrokkene. De gevolgen van opname moeten in verhouding staan tot het de gewraakte

gedraging en de overige omstandigheden van het geval. Dat is de basis van hetgeen met artikel 5.2.1, onder c wordt voorgeschreven.

Een Financiële Instelling informeert betrokkene over zijn opname in het Incidentenregister en in het EVR. Daarvoor zijn per branche voorbeeldteksten voorhanden, die ook gebruikt kunnen worden als onderdeel van een Privacy Statement op websites van deelnemers. Ook zal de betrokkene worden gewezen op de wijze waarop hij gebruik kan maken van zijn inzage- en correctierecht en op de wijze waarop verzet tegen een registratie van de persoonsgegevens kan worden aangetekend.

In de voorbeeldinstructies wordt, met betrekking tot registraties naar aanleiding van strafbare feiten, ingegaan op de voorwaarde dat concrete feiten en omstandigheden zodanig moeten vast staan, dat zij een als strafbaar feit te kwalificeren bewezenverklaring kunnen dragen, ongeacht of daarvan vooraf aangifte is gedaan. Verder geldt dat de betrokkenheid van de te registeren (rechts)persoon aan de gedraging in voldoende mate aannemelijk moet worden gemaakt door de concrete feiten en omstandigheden expliciet te benoemen bij het incident.

Tenslotte wordt in de voorbeeldwerkinstructie aangegeven om, bijvoorbeeld op de consumentenwebsite of in algemene voorwaarden, een passage op te nemen over het fraudebeleid van de instelling.