Protocol Incidenten-waarschuwingssysteem Financiële Instellingen 2021

Nederlandse Vereniging van Banken

VERBOND VAN VERZEKERAARS

Stichting Fraudebestrijding Hypotheken

vfa Vereniging van Financieringsondernemingen in Nederland

ZN Zorgverzekeraars Nederland

Inhoud

Dit protocol is opgesteld door:
Nederlandse Vereniging van Banken (NVB)
Verbond van Verzekeraars (Verbond)
Vereniging van Financieringsondernemingen in Nederland (VFN)
Stichting Fraudebestrijding Hypotheken (SFH)
Zorgverzekeraars Nederland (ZN)

Preambule Protocol Incidenten-waarschuwingssysteem Financiële Instellingen

Waarom een Waarschuwingssysteem? Wat is het doel?

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.

De regels en waarborgen met betrekking tot het Waarschuwingssysteem zijn vastgelegd in het Protocol Incidentenwaarschuwingssysteem Financiële Instellingen (Protocol).

Waaruit bestaat het Waarschuwingssysteem?

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

Een Financiële Instelling legt in haar eigen Incidentenregister gedragingen vast van (rechts)personen die hebben geleid of kunnen leiden tot benadeling van Financiële Instellingen, hun klanten of medewerkers of die de integriteit van Financiële Instellingen in het geding kunnen brengen. De gegevens die zijn vastgelegd in het Incidentenregister kunnen worden uitgewisseld ten behoeve van onderzoek naar Incidenten. Daarnaast worden in het aan het eigen Incidentenregister gekoppelde Extern Verwijzingsregister door de Financiële Instelling de Verwijzingsgegevens vastgelegd die op basis van een hit – no hit raadpleegbaar zijn voor andere Financiële Instellingen.

De Verwijzingsgegevens worden ontsloten door een Verwijzingsapplicatie. De Verwijzingsapplicatie van de Verzekeraars wordt beheerd door de Stichting Centraal Informatie Systeem (CIS) en die van de overige Deelnemers door Stichting Bureau Krediet Registratie (BKR). Het BKR en Stichting CIS zijn Verwerkers. Iedere Verwerkingsverantwoordelijke afzonderlijk sluit een Verwerkersovereenkomst met de Verwerker.

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 het Protocol.

Wie zijn de Verwerkingsverantwoordelijken voor de Verwerking in het kader van het Protocol?

Het is belangrijk dat het voor de Betrokkene duidelijk is wie de Verwerkingsverantwoordelijke is. De Betrokkene moet immers weten waar hij zich kan melden bij vragen en als hij zijn rechten op grond van de Algemene Verordening Gegevensbescherming wenst uit te oefenen.

Uitgangspunt is dat alleen Financiële Instellingen die lid zijn van een bij het Protocol aangesloten Branchevereniging mogen deelnemen aan het Waarschuwingssysteem. De aangesloten Brancheverenigingen zijn: Nederlandse Vereniging van Banken (NVB); Verbond van Verzekeraars (Verbond); Vereniging van Financieringsondernemingen in Nederland (VFN); Stichting Fraudebestrijding Hypotheken (SFH) en Zorgverzekeraars Nederland (ZN). De betreffende Financiële Instelling wordt een Deelnemer genoemd.

Banken die geen lid zijn van de NVB en Verzekeraars die geen lid zijn van het Verbond of ZN kunnen onder strikte voorwaarden worden toegelaten als Deelnemer aan het Protocol. Deze Banken en Verzekeraars zijn dan ook een Deelnemer. Op de website van de NVB wordt vermeld welke Banken dit zijn en op de website van het Verbond worden de Verzekeraars vermeld. Ook deze Banken en Verzekeraars kwalificeren als Verwerkingsverantwoordelijke.

Uit het Protocol volgt dat iedere Deelnemer een Incidentenregister moet hebben. De Deelnemer is de Verwerkingsverantwoordelijke voor de Verwerking van Persoonsgegevens in het eigen Incidentenregister. Dat Incidentenregister omvat, naast de specifieke dossierinformatie, ook een Extern Verwijzingsregister met Verwijzingsgegevens van in het Incidentenregister opgenomen personen. Aan de Verwijzingsgegevens (opgenomen in het Extern Verwijzingsregister) kan onder voorwaarden via de Verwijzingsapplicatie worden getoetst door frontoffices van andere Financiële Instellingen. Deze toetsing vindt plaats op basis van hit – no hit. Het Extern Verwijzingsregister met Verwijzingsgegevens blijft deel uitmaken van het Incidentenregister van de betreffende Financiële Instelling. En daarmee van de Verwerkingsverantwoordelijkheid van de betreffende Financiële Instelling.

Naast Deelnemers kent het Protocol ook de figuur van de Derde-organisatie. Het gaat om rechtspersonen die op wettelijke grondslag werkzaamheden verrichten

die in direct verband staan met de werkzaamheden van de Financiële Instellingen. Ook deze Derde-organisatie is Verwerkingsverantwoordelijke. Op het moment van de afgifte van een vergunning ter zake het Protocol door de AP is slechts één organisatie als Derde-organisatie bij het Protocol aangesloten. Het betreft de Stichting Waarborgfonds Motorverkeer. Een Derde-organisatie dient te voldoen aan de voorwaarden als genoemd in artikel 4.2.7 Protocol.

Ten slotte kunnen Fraudeloketten van de NVB, Verbond, VFN, ZN en SFH kwalificeren als Verwerkingsverantwoordelijke voor zover zij informatie ontvangen op grond van artikel 4.2.3 Protocol. De formele verantwoordelijkheid voor deze loketten ligt bij de betreffende Brancheverenigingen of de door de Brancheverenigingen aangewezen rechtspersoon. De betreffende Brancheverenigingen is Verwerkings-verantwoordelijke voor de Verwerking van Persoonsgegevens die in zijn eigen Fraudeloket plaats heeft.

Er is geen sprake van een gezamenlijke of een centrale Verwerkingsverantwoordelijke.

Vergunning AP

De AP heeft voor de Verwerking van Strafrechtelijke Persoonsgegevens overeenkomstig het Protocol een vergunning verstrekt conform artikel 33 lid 5 UAVG.

Bepalingen Protocol Incidenten-waarschuwingssysteem Financiële Instellingen

1 Overwegingen

1.1 Grondslag en zwaarwegend belang

1.1.1 Algemeen

Misbruik van het financieel stelsel omvat alle mogelijke vormen van onrechtmatig handelen, inclusief fraude, en inbreuken op de integriteit van het financieel stelsel. Het voorkomen en bestrijden van misbruik van het financieel stelsel is maatschappelijk gezien van zwaarwegend belang. Ook voorkomt dit hogere lasten voor klanten. Zowel op het terrein van bancaire diensten als via de kosten van producten en diensten van Verzekeraars en zorgverzekeraars. Misbruik kan ook rechtstreeks leiden tot benadeling van klanten. Het voorkomen en bestrijden van misbruik van het financieel stelsel brengt mee dat gegevens over natuurlijke en rechtspersonen worden verwerkt en uitgewisseld. Dit brengt tevens mee dat ook strafrechtelijke gegevens worden verwerkt. Criminaliteitsbeheersing en risicomanagement vergen immers dat Financiële Instellingen samenwerken, onder meer door op basis van reciprociteit gegevens met betrekking tot (rechts)personen uit te wisselen.

Daarbij kunnen conflicten ontstaan tussen individuele en maatschappelijke belangen. De noodzaak van een eventuele inbreuk op individuele belangen moet worden afgewogen tegen de maatschappelijke belangen die door de inbreuk worden gediend. Personen die gebruik maken van de diensten van het financiële stelsel weten dat dit stelsel alleen kan functioneren als er ook maatregelen zijn om ongeoorloofd gebruik van dat stelsel tegen te gaan. Van dergelijke maatregelen gaat bovendien een preventieve werking uit.

De grondslag voor de Verwerking van Persoonsgegevens in het kader van het Protocol is artikel 6 lid 1 (f) AVG: 'het gerechtvaardigd belang van de Verwerkingsverantwoordelijke of een derde'.

1.1.2 Financiële Instellingen dienen misbruik en fraude zo veel mogelijk te voorkomen

Vanuit de overheid wordt in toenemende mate en op diverse plaatsen een beroep gedaan op de financiële sector tot het tegengaan van misbruik, met inbegrip van fraude. Te wijzen valt op Europese regelgeving, de Wet op het financieel toezicht, de Wet ter voorkoming van witwassen en financieren van terrorisme en in op deze

regelgeving gebaseerde uitvoeringsregels. Hierin worden Financiële Instellingen op niet vrijblijvende wijze opgeroepen misbruik en fraude te bestrijden.

Financiële Instellingen moeten in dat verband samenwerken. Dat wordt ook van overheidswege van hen gevraagd. Het Openbaar Ministerie en andere (overheids) instanties verwachten dat Financiële Instellingen fraude zowel van binnenuit als van buitenaf gecoördineerd aanpakken ter ondersteuning van de voorkoming, opsporing en vervolging daarvan. Zij moeten de noodzakelijke maatregelen nemen om 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) en de Europese Centrale Bank (ECB)) 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 moet worden besteed aan het risico van onoorbare handelingen en aan het (afbreuk)risico voor een Financiële Instelling.

Het is aldus voor Financiële Instellingen van belang in samenwerking misbruik-(pogingen) en fraude te voorkomen, te onderkennen en erop te acteren. Ook als dat onder omstandigheden het recht op privacy van de Betrokkene inperkt.

Fraude is ernstig. Fraude wordt op diverse plaatsen in het Wetboek van Strafrecht strafbaar gesteld en met aanzienlijke sancties bedreigd. Het tegengaan van fraude wordt in de AVG (overweging 47) aangemerkt als een gerechtvaardigd belang om het recht op privacy in te perken. Dit volgt ook het uit het document *WP 29 Opinion 06/2014 on the notion of legitimate interests of the data controller under article 7 of Directive 95/46EC, WP 217* waarin is opgenomen dat onder meer preventie van fraude en misbruik van diensten worden aangemerkt als een gerechtvaardigd belang. In de wetgeschiedenis van de UAVG (Kamerstukken II 2017-18, 34851, Nota naar aanleiding van het verslag, pagina 47) is dat niet anders. Hierin is opgenomen dat het tegengaan van fraude als een zwaarwegend belang voor een bedrijf of onderneming geldt.

Misbruik en fraude worden tegengegaan door een goed-functionerend systeem voor screening en waarschuwing, en voor onderzoek.

1.1.3 Waarschuwing

Financiële Instellingen maken deel uit van een sterk verweven financieel stelsel. Enerzijds is er sprake van onderlinge verwevenheid van de verwerkingen door Financiële Instellingen. Anderzijds is er sprake van verwevenheid van hun verwerkingen met die van andere onderdelen van de samenleving. De samenleving vraagt om een degelijk financieel stelsel. Misbruik van het financiële stelsel moet worden voorkomen, gedetecteerd en opgevolgd.

Dat stelt hoge eisen aan de kwaliteit van de screening van klanten en medewerkers. Financiële Instellingen moeten beschikken over de juiste middelen om oneigenlijk gebruik van het financieel stelsel te bestrijden. Onder die middelen vallen extern toepasbare waarschuwingssystemen. Dergelijke systemen zijn onbruikbaar zonder

de mogelijkheid van de verwerking en uitwisseling van strafrechtelijke gegevens. Een alternatief voor een branchewaarschuwingssysteem is niet voor handen, terwijl het kunnen waarschuwen van essentieel belang is.

Personen die misbruik maken van het financiële stelsel beperken hun activiteiten zelden tot één enkele Financiële Instelling. Bij mislukte pogingen zullen zij het opnieuw proberen bij een andere Financiële Instelling. Maar ook bij een geslaagde poging bestaat risico op herhaling bij een andere Financiële Instelling.

Geslaagd misbruik heeft bovendien als regel een instelling-overschrijdende dimensie. Zo worden buitgemaakte gelden weggesluisd naar andere Financiële Instellingen. Bij verzekeringsfraude zijn of worden vaak meerdere Financiële Instellingen geraakt. Zonder tijdige signalering, kan een aaneenschakeling van samenhangende of gelijksoortige fraudes plaatsvinden met alle nadelige gevolgen voor de slachtoffers (zowel Financiële Instellingen als hun klanten) van dien.

Financiële Instellingen respecteren gelijktijdig de grondrechten van hun klanten. Inbreuken op het recht op privacy zijn niet toegestaan tenzij daar een zwaarder wegend belang mee is gediend. De Financiële Instellingen zijn zich bewust van de belangen van de Betrokkene. Zij streven naar een evenwicht tussen de belangen van enerzijds de samenleving, de Financiële Instellingen en hun klanten en anderzijds mogelijk bij misbruik betrokken natuurlijke en rechtspersonen. Daarbij hebben Financiële Instellingen de gevolgen van registratie meegewogen. De Verwerking van Persoonsgegevens in het kader van het Incidentenwaarschuwingssysteem is van invloed op het besluit van een Financiële Instelling al dan niet producten of diensten aan de Betrokkene te verstrekken. Hierbij heeft de financiële sector maatregelen genomen die onder voorwaarden borgen dat toegang tot diensten die de eerste levensbehoeften van betrokkenen betreffen wordt gegeven. Te denken valt aan de basisbankrekening en de maatregel dat zorgverzekeraars dienen te voorzien in een basisverzekering.

Ten aanzien van de vraag of informatie mag worden uitgewisseld en zo ja welke informatie gelden daarom strikte proportionaliteitseisen. Aan de opname in het EVR zijn ook strikte voorwaarden verbonden. Er gelden dus strenge registratiecriteria. Er is gekozen voor een systematiek waarbij de uitwisseling van detailinformatie uit het Incidentenregister uitsluitend plaatsvindt tussen professionele veiligheidsafdelingen en sprake is van een hit-no hit systeem. De systematiek voorziet in aanvullende waarborgen op het gebied van documentatie, informatie, beveiliging en controle. Speciale geschillenregelingen vormen een sluitstuk op dit geheel.

Waarschuwen door de Financiële Instellingen is, kortom, een noodzakelijk gevolg van het zwaarwegend maatschappelijk belang bij een integer financieel stelsel. De checks en balances uit het Protocol dragen ertoe bij dat de inbreuk op de belangen van de individuele Betrokkenen proportioneel is.

1.1.4 Onderzoek

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 die 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 kunnen delen als dit noodzakelijk is voor onderzoek, kunnen de betreffende risico's tijdig worden onderkend en verkleind en kunnen eventuele negatieve gevolgen worden beperkt.

Financiële Instellingen lopen grote risico's en dienen de maatschappij niet optimaal als zij informatie over (pogingen tot) misbruik uitsluitend voor zichzelf houden en niet willen of kunnen meewerken aan relevant onderzoek naar Incidenten. Ook als zij informatie uitsluitend kunnen delen met opsporingsautoriteiten heeft dat weinig invloed op de voorkoming van onregelmatigheden bij andere Financiële Instellingen. Het is noodzakelijk dat Financiële Instellingen – in het kader van een efficiënt en effectief stelsel van bestrijding, detectie, onderzoek en opvolging van misbruik – elkaar actief met informatie ondersteunen. Het gaat daarbij om informatie die om voor de hand liggende redenen niet van de zelf bij misbruik betrokken natuurlijke of rechtspersonen verwacht kan worden.

Ook in dit verband houden Financiële Instellingen rekening met de grondrechten van de Betrokkene en dient rekening te worden gehouden met het privacybelang van de Betrokkene. 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. De Verwerking van dergelijke Persoonsgegevens moet daarom met waarborgen 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. Enerzijds moet sprake zijn van noodzaak van Verwerking van Persoonsgegevens in relatie tot het beschermen van de veiligheid en integriteit van de Financiële sector. Anderzijds moet de Verwerking van Persoonsgegevens evenredig zijn in relatie tot dat doel. Dit betekent dat de Verwerking van Persoonsgegevens moet voldoen aan eisen van proportionaliteit en subsidiariteit. Een waarborg is onder meer gelegen in het bestaan van diverse momenten waarop getoetst wordt op de evenredigheid van het handelen van de Financiële Instelling.

Ten aanzien van de vraag of informatie ten behoeve van onderzoek naar Incidenten mag worden uitgewisseld en zo ja welke informatie gelden daarom strikte proportionaliteitseisen. Er is gekozen voor een systematiek waarbij de uitwisseling van Persoonsgegevens uitsluitend plaatsvindt tussen professionele veiligheidsafdelingen. De uitwisseling is begrensd tot een nauw omschreven groep van onder wettelijk toezicht staande Financiële Instellingen. De systematiek voorziet in aanvullende waarborgen op het gebied van documentatie (onder meer artikel 3.2.3 en 3.2.4 Protocol), informatie, (artikel 9 Protocol) beveiliging en controle. Speciale geschillenregelingen vormen een sluitstuk op dit geheel.

Ook het onderzoek naar Incidenten door de Financiële Instellingen is, kortom, een noodzakelijk gevolg van het zwaarwegend maatschappelijk belang bij een integer financieel stelsel. Ook hier dragen de checks en balances uit het Protocol eraan bij dat de inbreuk op de belangen van de individuele Betrokkenen proportioneel is.

De onder dit kopje genoemde overwegingen vormen de rechtmatige grondslag in de zin van artikel 6 lid 1 (f) AVG voor het aanleggen en gebruiken van het Incidentenwaarschuwingssysteem Financiële Instellingen. Ook is sprake van een zwaarwegend belang van derden als bedoeld in artikel 33 lid 5 UAVG met inachtneming van de in dat artikel bedoelde waarborgen.

1.2 Nationale werking

Deelnemers zijn in Nederland werkzame Financiële Instellingen, die lid zijn van één van de bij het Protocol aangesloten Brancheverenigingen of Financiële Instellingen die conform het Protocol daarmee gelijkgesteld zijn. Ook dient een Deelnemer te beschikken over een Nederlandse vergunning op grond van de financiële toezicht-wetgeving. De scope van het Protocol is nationaal.

1.3 Vergunning

Aangezien op basis van dit Protocol Strafrechtelijke Persoonsgegevens worden verwerkt ten behoeve van derden, anders dan krachtens een vergunning op grond van de Wet particuliere beveiligingsorganisaties en recherchebureaus, is ten behoeve van de Verwerking in het kader van het Protocol een vergunning verstrekt door de AP.

2 Begripsbepalingen

In dit Protocol wordt verstaan onder:

AP: de Autoriteit Persoonsgegevens;

AVG: de Algemene Verordening Gegevens-bescherming;

Bank: conform de definitie van artikel 1:1 Wft, 'een kredietinstelling als bedoeld in artikel 4 van de verordening kapitaal-vereisten, niet zijnde een kredietunie met zetel in Nederland, met dien verstande dat, tenzij anders bepaald een Bank wordt gelijkgesteld met de houder van een vergunning als bedoeld in artikel 3:4 Wft';

Betrokkene: degene op wie een Persoonsgegeven betrekking heeft;

Brancheverenigging: de Nederlandse Vereniging van Banken (NVB), het Verbond van Verzekeraars (Verbond), de Vereniging van Financieringsondernemingen in Nederland (VFN), Zorgverzekeraars Nederland (ZN) of de Stichting Fraude-bestrijding Hypotheken (SFH);

Deelnemer: het volgens artikel 7.1 Protocol toegelaten lid van de NVB, het Verbond, de VFN, ZN, dan wel aangeslotene bij de SFH, welke beschikt over een Incidentenregister; of een niet bij de NVB, Verbond of ZN aangesloten Bank respectievelijk Verzekeraar die beschikt over een Incidentenregister en overeenkomstig artikel 7.1. Protocol is toegetreden tot het Waarschuwingssysteem;

Derde-organisatie: een niet bij het Protocol aangesloten organisatie met wie, indien aan de voorwaarden als aangegeven in artikel 4.2.7 Protocol is voldaan, Persoonsgegevens mogen worden uitgewisseld;

Extern Verwijzingsregister (EVR): de deelverzameling van het Incidentenregister van de betreffende Deelnemer, welke uitsluitend Verwijzingsgegevens bevat met betrekking tot (rechts)personen en welke bestemd is voor gebruik door (de Organisaties van) alle Deelnemers;

Financiële Instelling: een Bank en/of Verzekeraar en/of hypothecaire instelling en/of financierings-onderneming;

Fraudeloket: Veiligheidszaken van een Brancheverenigging waar gegevens naar aanleiding van of betrekking hebbend op een 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;

Geautoriseerde functionaris: de persoon die binnen de Organisatie van de Deel-nemer in het kader van zijn taakuitoefening gerechtigd is om gegevens aan het Extern Verwijzingsregister te toetsen;

Incident: 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 dienst-betrekking, phishing en opzettelijke misleiding;

Incidentenregister: de gegevens-verzameling(en) van de Deelnemer, waarin gegevens zijn vastgelegd voor het in artikel 4.1.1 Protocol genoemde doel, naar aan-leiding van of betrekking hebbend op een (mogelijk) Incident;

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); 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;

Persoonsgegeven: alle informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon;

Protocol: het Protocol Incidentenwaarschuwingssysteem Financiële Instellingen;

Strafrechtelijk Persoonsgegeven: Persoonsgegevens van strafrechtelijke aard als bedoeld artikel 1 UAVG en artikel 10 AVG;

UAVG: Uitvoeringswet Algemene Verordening Gegevensbescherming;

Verzekeraar: conform de definitie van artikel 1:1 Wft: een herverzekeraar, levensverzekeraar, (natura) uitvaartverzekeraar of schadeverzekeraar;

Veiligheidszaken: de afdeling of de persoon die binnen een Financiële Instelling, Branchevereniging of Derdeorganisatie verantwoordelijk is voor de Verwerking van Persoonsgegevens in het kader van het waarborgen van de veiligheid en integriteit;

Verwerking van Persoonsgegevens: elke bewerking of geheel van bewerkingen met betrekking tot Persoonsgegevens of een geheel van Persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of op ander wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;

Verwerkingsverantwoordelijke: een natuurlijk persoon of rechtspersoon, een dienst of een ander orgaan die / dat, alleen of samen met anderen, het doel van en de middelen voor de Verwerking van Persoonsgegevens vaststelt;

Verwerkersovereenkomst: een overeenkomst conform artikel 28 AVG;

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

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

Waarschuwingssysteem: het Incidentenwaarschuwingssysteem Financiële Instellingen dat bestaat uit de Incidentenregisters en de daarvan deel uitmakende Externe Verwijzingsregisters van de Deelnemers en de Brancheverenigingen.

3 Algemeen

3.1 Incidentenregister en Extern Verwijzingsregister

3.1.1 Iedere Deelnemer heeft een Incidentenregister. In het Incidentenregister worden door de betreffende Deelnemer gegevens van (rechts)personen vastgelegd ten behoeve van het in artikel 4.1.1 Protocol genoemde doel, naar aanleiding van of betrekking hebbend op een Incident.

3.1.2 De Verwerking van Persoonsgegevens met betrekking tot het Incidentenregister (inclusief het Extern Verwijzingsregister), is door iedere Deelnemer vastgelegd in het register van verwerkingsactiviteiten in overeenstemming met artikel 30 AVG. Onder verantwoordelijkheid van de Deelnemer treedt Veiligheidszaken op als (sub) beheerder van het Incidentenregister.

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

3.2 De uitwisseling van gegevens in het kader van onderzoek onder het Protocol

3.2.1 De gegevens in het Incidentenregister kunnen door de afdeling Veiligheidszaken voor zover noodzakelijk in het kader van het onderzoeken van een Incident, worden uitgewisseld overeenkomstig het bepaalde in artikel 4.2 Protocol.

3.2.2 De onderzoekende afdeling Veiligheidszaken bepaalt welke Persoonsgegevens overeenkomstig artikel 3.2.1 Protocol uit het Incidentenregister kunnen worden verstrekt aan de bevraagde afdeling Veiligheidszaken. Deze verstrekking dient te voldoen aan het proportionaliteits- en subsidiariteitsbeginsel. De interne afwegingen om te komen tot de verstrekking, de wijze van bevragen, de wijze waarop de Betrokkene wordt geïnformeerd en als dat niet gebeurt de redenen hiervan, de proportionaliteits- en subsidiariteitsafweging worden vastgelegd door Veiligheidszaken in haar administratie.

3.2.3 De bevraagde afdeling Veiligheidszaken kan eerst na eigen toetsing aan het proportionaliteits- en subsidiariteitsbeginsel overgaan tot verstrekking van Persoonsgegevens die door de bevraagde Financiële Instelling worden verwerkt aan de vragende afdeling Veiligheidszaken. Deze verstrekking kan gegevens

betreffen uit het Incidentenregister of uit een andere administratie van de bevraagde Financiële Instelling. De uitwisseling dient toereikend, ter zake dienend en beperkt te zijn tot wat noodzakelijk is voor de doeleinden waarvoor de Persoonsgegevens worden verwerkt. De interne afwegingen om te komen tot de verstrekking, de wijze van verstrekken, en de proportionaliteits- en subsidiariteitsafweging worden vastgelegd door Veiligheidszaken in haar administratie.

3.2.4 Persoonsgegevens die in het kader van onderzoek naar Incidenten worden uitgewisseld tussen de afdelingen Veiligheidszaken van Financiële Instellingen dienen rechtmatig te zijn verwerkt. In het Incidentenregister wordt het onderzoek, waaronder de onderzoeksmethode en onderzoeksmiddelen gedocumenteerd.

3.2.5 De rechten van de Betrokkene als omschreven in artikel 9 Protocol gelden voor de Verwerking van Persoonsgegevens die in het kader van het onderhavige artikel 3.2 Protocol plaats heeft.

3.2.6 Als uit het onderzoek naar een Incident volgt dat niet langer wordt voldaan aan het bepaalde in artikel 4.1.1 Protocol, worden de gegevens direct verwijderd uit het Incidentenregister na afloop van het onderzoek.

3.2.7 De uitkomst van een onderzoek kan leiden tot een registratie in het Extern Verwijzingsregister als aan de voorwaarden van artikel 5.2.1. Protocol voor vastlegging in het Extern Verwijzingsregister wordt voldaan.

3.3 Toetsingsproces

3.3.1 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 Extern Verwijzingsregister voorkomen (hit-no hit). 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 zijn eigen afdeling 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 opname in het Extern Verwijzingsregister toe te passen in zijn besluitvorming over Betrokkene na kennisneming van het advies van Veiligheidszaken.

3.3.2 In overeenstemming met artikel 9.6.2 van dit Protocol worden alle bevragingen vastgelegd, zolang de gegevens van Betrokkene zijn opgenomen in het Incidenten-register. Daarbij wordt geregistreerd wie bevraagd heeft, waar vandaan de bevraging is uitgevoerd, wanneer de bevraging is gedaan en het resultaat van de bevraging (hit-no hit).

3.3.3 Tevens controleert Veiligheidszaken of er 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.

3.3.4 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 achteraf' binnen de periode van 2 maanden na toetsing alsnog in een Extern Verwijzingsregister wordt opgenomen.

3.4 Invoervalidatie

3.4.1 De Persoonsgegevens van de in het Incidentenregister en in voorkomende gevallen in het Extern Verwijzingsregister opgenomen personen worden verwerkt op een wijze die ten aanzien van de Betrokkene rechtmatig, behoorlijk en transparant is.

3.4.2 De Persoonsgegevens van de in het Incidentenregister en in voorkomende gevallen in het Extern Verwijzingsregister opgenomen personen dienen bij de (Primaire) Bron gedocumenteerd herleidbaar te zijn.

3.4.3 Persoonsgegevens worden slechts verwerkt indien en voor zover is voldaan aan minimaal één van de in de AVG genoemde grondslagen. De grondslag voor de Verwerking van Persoonsgegevens in het kader van het Protocol is artikel 6 lid 1 (f) AVG: 'het gerechtvaardigd belang van de Verwerkingsverantwoordelijke of een derde afgewogen tegen de belangen van de Betrokkene'.

3.4.4 De zorgvuldigheid waarmee een onderzoek wordt uitgevoerd kan met zich brengen dat de Betrokkene in de gelegenheid wordt gesteld zijn visie op de feiten te geven. Indien bij de Deelnemer twijfel bestaat of invoer van bepaalde gegevens kan plaatsvinden overeenkomstig het Protocol, moet de Deelnemer van invoer van de betreffende gegevens af zien. De Betrokkene heeft het recht van bezwaar. Dit recht is vastgelegd in artikel 9.5 van dit Protocol.

3.4.5 Daarvoor in aanmerking komende Geautoriseerde 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.

3.4.6 De Deelnemer moet zorgdragen voor een zorgvuldige invoervalidatie en instructie aan Veiligheidszaken om zeker te stellen dat gegevens uitsluitend in overeenstemming met de regels van het Protocol worden opgenomen in het Incidentenregister c.q. het Extern Verwijzingsregister.

3.4.7 Persoonsgegevens worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden verwerkt. In artikel 4.1.1 en 5.2.1 Protocol is dit nader bepaald. Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen.

3.4.8 De Deelnemer neemt maatregelen zodat Persoonsgegevens, gelet op de doeleinden waarvoor zij door de Deelnemer worden verwerkt juist zijn en zo nodig worden geactualiseerd. De Deelnemer verbetert of verwijdert Persoonsgegevens, dan wel vult deze aan indien blijkt dat deze onjuist of onvolledig zijn. De Betrokkene heeft het recht op inzage, correctie, gegevenswissing en bezwaar. Verwezen wordt naar artikel 9.3, 9.4, en 9.5 Protocol.

3.5 Geheimhouding

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

3.6 Beveiliging

3.6.1 Iedere Deelnemer neemt passende technische en organisatorische maatregelen om een op risico afgestemd beveiligingsniveau te waarborgen. Bij de vaststelling van de maatregelen wordt rekening gehouden met de stand van de techniek, de uitvoeringskosten, alsook de aard, de omvang, de context en de verwerkingsdoeleinden en de waarschijnlijkheid en ernst van de uiteenlopende risico's voor de rechten en vrijheden van de Betrokkene. De maatregelen worden eens per twee jaar geëvalueerd en indien nodig aangepast.

3.6.2 Iedere Deelnemer voldoet aan de verplichtingen die op de Deelnemer rusten ter zake datalekken overeenkomstig artikel 33 AVG, artikel 34 AVG en artikel 42 UAVG en implementeert een procedure die hiertoe zorgdraagt.

4 Incidentenregister

4.1 Doel Incidentenregister en vastlegging van gegevens in het 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.'

4.1.2 Bij de vastlegging in het Incidentenregister moeten het proportionaliteitsbeginsel en het subsidiariteitsbeginsel in acht worden genomen.

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. Protocol, waarvoor de gegevens zijn verkregen. Er wordt vastgelegd wie toegang heeft gehad tot het Incidentenregister.

4.2.2 De gegevens in het Incidentenregister van de Deelnemer zijn met inachtneming van de bepalingen in de artikelen 4.2.3 tot en met 4.2.7 Protocol voor zover relevant op basis van reciprociteit beschikbaar voor Veiligheidszaken van de andere (Organisaties van de) Deelnemer. Dit ten behoeve van het onderzoeken van Incidenten en het verifiëren van EVR toetsingsresultaten.

4.2.3 De gegevens in het Incidentenregister van de Deelnemer mogen tevens worden uitgewisseld met functionarissen werkzaam bij de daartoe ingerichte, coördinatie-functies van de NVB, Verbond, VFN, ZN en SFH (de Fraudeloketten).

4.2.4 De (Organisaties van de) Deelnemers die lid zijn van het Verbond of ZN of daaraan gelijkgesteld zijn conform artikel 7.1.1 Protocol mogen gegevens uit het Incidenten-register uitwisselen met Veiligheidszaken van de Stichting Waarborgfonds Motor-verkeer. De Stichting Waarborgfonds Motorverkeer voldoet aan de in artikel 4.2.7 opgenomen voorwaarden.

4.2.5 Deelnemers aan SFH, die geen lid zijn van de NVB, VFN of het Verbond, kunnen gegevens uit het Incidentenregister uitwisselen met Veiligheidszaken van andere Deelnemers aan SFH voor zover die gegevens betrekking hebben op fraude met hypothecaire financieringen en /of onrechtmatig gebruik van onderpanden.

4.2.6 Zorgverzekeraars die geen lid zijn van het Verbond kunnen alleen gegevens uit het Incidentenregister uitwisselen met Veiligheidszaken van Deelnemers die lid zijn van het Verbond of ZN of daaraan gelijkgesteld zijn conform artikel 7.1.1 Protocol.

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 Incidenten-register

4.3.1 Indien niet langer aan de voorwaarden van artikel 3.1.1 en 3.4.7 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 wissing van gegevens conform artikel 9.4 Protocol.

4.3.2 Onverminderd het bepaalde in artikel 4.3.1 Protocol beoordeelt de Deelnemer na afloop van een onderzoek of opname van Persoonsgegevens in het Incidenten-register nog steeds voldoet aan de doelomschrijving van artikel 4.1.1 Protocol en de toets van artikel 4.1.2 Protocol.

4.3.3 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 opname in het Incidentenregister rechtvaardigt. Ten aanzien van de duur wordt getoetst aan het proportionaliteitsbeginsel.

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 Extern Verwijzingsregister, zijn volgens het bepaalde in artikel 4.2 Protocol gegevens uit het Incidentenregister voor Veiligheidszaken van 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 onder toepassing van het onder c genoemde proportionaliteitsbeginsel op te nemen in het Extern Verwijzingsregister.

a De gedraging(en) van de (rechts)persoon vormden, 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 klachte wordt gedaan bij een opsporingsambtenaar.

c Het proportionaliteitsbeginsel wordt in acht genomen.

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 door of op advies van Veiligheidszaken, daarvan aangifte of klachte worden gedaan, behoudens in de gevallen waarin opsporingsbelangen of andere belangen aan het doen van aangifte of klachte in de weg staan. Veiligheidszaken legt de afweging die zij maakt en de ter zake genomen beslissing om al dan niet over te gaan tot aangifte vast.

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. Ten aanzien van de duur wordt getoetst aan het proportionaliteitsbeginsel.

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 3.3 Protocol. Er vindt logging van gegevens plaats conform artikel 3.3.2 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. Een Bank die geen lid is van de NVB valt onder de begeleidingscommissie van de NVB en een Verzekeraar die geen lid is van het Verbond of ZN valt onder de begeleidings-commissie van het Verbond.

6.2

Indien daartoe aanleiding bestaat adviseert de begeleidingscommissie de Deel-nemers over de toepassing van de onder artikel 5.2.1 Protocol genoemde vast-leggingscriteria. De Deelnemer dient op verzoek van de begeleidingscommissie alle relevante informatie over de uitleg en toepassing van de vastleggingscriteria 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. Daarbij geldt dat een Bank die geen lid is van de NVB en een Verzekeraar die geen lid is van het Verbond of ZN uitsluitend als Deelnemer kan worden toegelaten indien de Bank beschikt over een Nederlandse bankvergunning respectievelijk de Verzekeraar beschikt over een Nederlandse vergunning voor verzekeringsactiviteiten afgegeven door DNB. Een Bank die geen lid is van de NVB valt onder de begeleidingscommissie van de NVB. Een Verzekeraar die geen lid is van het Verbond of ZN valt onder de begeleidingscommissie van het Verbond.

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 Nederlandse vergunning te beschikken op grond van de financiële toezichtwetgeving. Of dit juist is zal worden gecontroleerd door de begeleidingscommissie. Voor Banken en Verzekeraars zal dit gebeuren, door middel van het raadplegen van het vergunningenregister DNB, waarin Banken en Verzekeraars die beschikken over een Nederlandse bankvergunning respectievelijk een Nederlandse vergunning voor verzekeringsactiviteiten afgegeven door DNB zijn opgenomen.

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 begeleidingscommissie van de Brancheverenigingkenbaar te maken onder vermelding van de gewenste datum van uittreding. Een Bank die geen lid is van de NVB valt onder de begeleidingscommissie van de NVB en een Verzekeraar die geen lid is van het Verbond of ZN valt onder de begeleidingscommissie van het Verbond.

7.2.2 Na uittreding zal de ex-Deelnemer noch de Organisatie van de ex-Deelnemer nog langer deel uitmaken van en gebruik kunnen maken van het Waarschuwingssysteem.

7.2.3 De ex-Deelnemer moet er voor zorgen 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 Brancheverenigingop advies van de begeleidingscommissie gerechtigd de Deelnemer uit te sluiten van deelname aan het Waarschuwingssysteem. Het bestuur van de NVB is gerechtigd op advies van de begeleidingscommissie van de NVB een Bank die geen lid is van de NVB uit te sluiten. Het bestuur van het Verbond is gerechtigd op advies van de begeleidingscommissie van het Verbond een Verzekeraar die geen lid is van het Verbond of ZN uit te sluiten.

7.3.2 Na uitsluiting zal de ex-Deelnemer noch de Organisatie van de ex-Deelnemer nog langer deel uitmaken van en gebruik kunnen maken van het Waarschuwingssysteem.

7.3.3 Na uitsluiting moet de ex-Deelnemer er direct voor zorgen dat de door haar aangebrachte gegevens uit het Extern Verwijzingsregister worden verwijderd.

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 (Organisatie van de) Deelnemer die gegevens verwerkt die de (Organisatie van 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 verplicht om de werkwijze zoals neergelegd in het Protocol te concretiseren in werkprocessen. Deelnemers wordt geadviseerd daarbij gebruik te maken van voorbeeldwerkinstructies en/of handreikingen van de 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, overeenkomstig artikel 13 en 14 AVG.

9.1.2 De mededeling blijft achterwege, indien sprake is van een uitzonderingssituatie als bedoeld in artikel 14 lid 5 AVG of artikel 41 UAVG. Dit is onder meer het geval 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. De interne afweging om de mededeling achterwege te laten, moet worden vastgelegd door Veiligheidszaken.

9.1.3 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.

9.1.4 De Deelnemer draagt er zorg voor dat informatie over de Verwerking van Persoonsgegevens op basis van het Protocol vast onderdeel uitmaakt van het Privacy Statement van de Deelnemer. Hiermee wordt beoogd dat de Betrokkene zo goed mogelijk vooraf wordt geïnformeerd over het bestaan van en de mogelijke opname in het Incidentenregister en het Extern Verwijzingsregister.

9.2 Afschrift Protocol

Bij de Brancheverenigingen of de Deelnemer kan een afschrift van het Protocol worden opgevraagd. Dit Protocol kan ook worden geraadpleegd via de website van de Brancheverenigingen of de Deelnemer.

9.3 Inzage

9.3.1 Een Betrokkene heeft het recht om uitsluitsel te verkrijgen of zijn Persoonsgegevens in het Incidentenregister en/of het Extern Verwijzingsregister zijn opgenomen en wanneer dat het geval is, om inzage te verkrijgen van die Persoonsgegevens overeenkomstig artikel 15 AVG.

9.3.2 Het in artikel 9.3.1 Protocol genoemde verzoek moet 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 9.3.4 Protocol genoemde uitzonderingsgevallen, de Betrokkene onverwijld en in ieder geval binnen een maand na ontvangst van het verzoek schriftelijk mededelen of, en zo ja welke hem betreffende Persoonsgegevens worden verwerkt. De mededeling zal voldoen aan de vereisten van artikel 15 AVG. Afhankelijk van de complexiteit van het verzoek en van het aantal verzoeken kan de termijn indien nodig met nog eens twee maanden worden verlengd. De Betrokkene wordt in dit geval van deze verlenging van de reactietermijn binnen 1 maand na ontvangst van het verzoek op de hoogte gesteld.

9.3.4 Geen inzage wordt verstrekt, indien sprake is van een uitzonderingssituatie als bedoeld in artikel 41 UAVG. Dit is onder meer het geval 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. De interne afweging om geen inzage te verlenen, moet worden vastgelegd door Veiligheidszaken.

9.4 Correctie, recht op gegevenswissing en recht op beperking van de Verwerking

9.4.1 Indien uit het verstrekte overzicht blijkt dat Persoonsgegevens onjuist zijn, heeft de Betrokkene het recht op correctie en, met in achtneming van de doeleinden van de Verwerking, vervollediging van hem betreffende onjuiste Persoonsgegevens. Ook heeft de Betrokkene het recht om wissing van hem betreffende Persoonsgegevens te verkrijgen overeenkomstig artikel 17 AVG. Dit is onder meer het geval als de Verwerking van Persoonsgegevens niet langer nodig zijn voor de doeleinden waarvoor zij zijn verwerkt, dan wel anderszins onrechtmatig worden verwerkt. De Betrokkene heeft ook het recht op beperking van de Verwerking overeenkomstig artikel 18 AVG.

9.4.2 De Deelnemer bericht de Betrokkene onverwijld en in ieder geval binnen een maand na ontvangst van het verzoek schriftelijk of en in hoeverre de Deelnemer het verzoek, als bedoeld in artikel 9.4.1. Protocol, honoreert. Ook wordt de Betrokkene gewezen op de geschillenregeling als opgenomen in artikel 10 Protocol. Indien niet of niet volledig aan het verzoek van de Betrokkene wordt voldaan wordt dit met redenen omkleed meegedeeld. Afhankelijk van de complexiteit van het verzoek en van het aantal verzoeken kan de termijn indien nodig met nog eens twee maanden worden verlengd. De Betrokkene wordt in dit geval van deze verlenging van de reactietermijn binnen 1 maand na ontvangst van het verzoek op de hoogte gesteld.

9.4.3 De Deelnemer zorgt dat indien door de Deelnemer wordt besloten tot correctie of gegevenswissing over te gaan dit zo spoedig mogelijk wordt uitgevoerd.

9.5 Recht van bezwaar

9.5.1 De Betrokkene kan bij de Verwerkingsverantwoordelijke te allen tijde bezwaar maken in verband met zijn bijzondere persoonlijke omstandigheden.

9.5.2 De Verwerkingsverantwoordelijke beoordeelt onverwijld en in ieder geval binnen een maand na ontvangst van het bezwaar of het bezwaar gerechtvaardigd is en gaat over tot een belangenafweging. Indien het bezwaar gerechtvaardigd is, beëindigt hij terstond de Verwerking. Ook wordt de Betrokkene gewezen op de geschillenregeling als opgenomen in artikel 10 Protocol. Afhankelijk van de complexiteit van het verzoek en van het aantal verzoeken kan de termijn indien nodig met nog eens twee maanden worden verlengd. De Betrokkene wordt in dit geval van deze verlenging van de reactietermijn binnen 1 maand na ontvangst van het verzoek op de hoogte gesteld.

9.6 Kettingbepaling

9.6.1 De AVG verplicht de Deelnemer om, in het geval dat Persoonsgegevens zijn verbeterd, aangevuld, gewist, afgeschermd of beperkt naar aanleiding van een verzoek overeenkomstig 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. De Deelnemer verstrekt de Betrokkene informatie over deze ontvangers indien de Betrokkene hierom verzoekt.

9.6.2 Om die reden onderhoudt de Deelnemer een overzicht van de verstrekkingen die hebben plaatsgevonden in het kader van dit Protocol aan de andere Deelnemer, gedurende de duur van de registratie.

10 Geschillen

10.1 Bij een geschil over de juistheid en rechtmatigheid van de Verwerking van Persoonsgegevens onder de reikwijdte van dit Protocol 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) de AP; of (IV) de bevoegde rechter.

11 Toezicht

11.1 De Deelnemer is gehouden de naleving van het Protocol om de twee jaar 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 of ZN 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 Evaluatie en wijzigingen Protocol

12.1 De aan dit Protocol verbonden Brancheverenigingen zijn verplicht de inhoud en werking van het Protocol om de twee jaar te evalueren. Deze evaluatie omvat mede toetsing aan geldende wet- en regelgeving. Ook de bevindingen van de verschillende begeleidingscommissies en ontwikkelingen in de rechtspraak zijn van belang. Indien de uitkomst van de evaluatie daartoe aanleiding geeft wordt het Protocol aangepast.

12.2 Het bestuur van NVB, Verbond, VFN, ZN en SFH kunnen, onder meer 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 de AP. Voor de aanpassingen en wijzigingen dient opnieuw een vergunning te worden verkregen.

Annex Protocol Incidenten-waarschuwingssysteem Financiële Instellingen

Aanleiding

Financiële Instellingen, waaronder Verzekeraars, hypothecaire Instellingen, financieringsondernemingen en Banken worden verstaan, hun cliënten en mede-werkers hebben er belang bij dat fraude en criminaliteit die tegen hen zijn gericht tijdig worden ontdekt en bestreden.

Vanaf het begin van de jaren negentig hebben Financiële Instellingen 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, de Wet bescherming persoonsgegevens als de Algemene Verordening Gegevensbescherming (AVG) is het aan het Waarschuwingssysteem ten grondslag liggende Protocol Incidenten-waarschuwingssysteem Financiële Instellingen (in het vervolg: Protocol) afgestemd met en goedgekeurd door de toezichthouder voor privacybescherming in Nederland, de Autoriteit Persoonsgegevens (AP). 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. Na de aanpassing in 2020 kunnen ook de Banken die niet lid zijn van NVB en Verzekeraars die geen lid zijn van het Verbond of ZN onder voorwaarden deelnemen aan het Protocol.

Werkwijze

Incident

In het Protocol is het begrip Incident belangrijk. Dit betreft 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 of de financiële sector als geheel in het geding zijn of kunnen zijn. Incidenten hebben betrekking op dusdanig ernstige zaken dat daarvan uitwisseling met een andere afdeling Veiligheidszaken mogelijk moet zijn. Als Incidenten kunnen bijvoorbeeld voorkomen het falsificeren van nota's, identiteitsfraude, skimming, verduistering in dienstbetrekking, phishing en opzettelijke misleiding. Of een gebeurtenis als Incident dient te worden gekwalificeerd bepaalt Veiligheidszaken.

Doel Incidentenregister en voorwaarden voor opname

Een Incident mag pas in het Incidentenregister worden opgenomen als het voldoet aan de doelomschrijving die is opgenomen in artikel 4.1.1 Protocol. Het doel betreft kort weergegeven het ondersteunen van activiteiten die gericht zijn op het waarborgen van de veiligheid en integriteit van de financiële sector. Hieronder valt het onderzoeken, onderkennen, voorkomen en bestrijden van Incidenten. De Deelnemer neemt maatregelen zodat Persoonsgegevens, gelet op de doeleinden waarvoor zij door de Deelnemer worden verwerkt juist zijn en zo nodig worden geactualiseerd. Voorbeelden van deze maatregelen zijn onder meer werkinstructies voor en training aan de relevante personen. Ook dient te zijn voldaan aan het proportionaliteits- en subsidiariteitsbeginsel. Dit is vastgelegd in artikel 4.1.2 Protocol. In tegenstelling tot een registratie in het EVR is een vastlegging in het Incidentenregister niet voor andere afdelingen zichtbaar, maar alleen voor Veiligheidszaken. Voor opname in het EVR gelden separate opnamecriteria die zijn vastgelegd in artikel 5.2 Protocol.

De uitwisseling van gegevens in het kader van onderzoek onder het Protocol

Algemeen

Voorafgaand aan de aanvang van een onderzoek stelt Veiligheidszaken de vraagstelling, het doel van het onderzoek en de onderzoeksaanpak vast. Financiële Instellingen maken in het algemeen gebruik van traditionele onderzoeksmethoden (administratief onderzoek zoals de analyse van financieringsaanvragen, jaarstukken, accountantsverklaringen, KvK-gegevens). Voor zover sprake is van inzet van camera's (bijvoorbeeld bij geldautomaten of in geval van interne fraude) worden daarbij de wettelijke eisen in acht genomen. Als het om personeel gaat zal indien wettelijk vereist de OR worden betrokken. Het verzamelen van gegevens bij derden vindt plaats door middel van bevragingen. Het onderzoek dient te voldoen aan het proportionaliteits- en subsidiariteitsbeginsel.

Als een Financiële Instelling in het kader van haar eigen onderzoek naar een Incident nadere gegevens nodig heeft van een andere Financiële Instelling kan zij besluiten om die andere Financiële Instelling daarom te verzoeken. Het betreft dus een 'bevraging'. Deze bevraging is de gehanteerde onderzoeksmethode. De afdeling Veiligheidszaken van de andere Financiële Instelling maakt aan de hand van het proportionaliteits- en subsidiariteitsbeginsel een eigen afweging of zij de onder

de Financiële Instelling berustende gegevens kan verstrekken. Er is geen sprake van een gezamenlijk onderzoek. Het onderzoek wordt namelijk verricht door de vragende Financiële Instelling. Het onderzoek wordt gedocumenteerd in het Incidentenregister van de onderzoekende Financiële Instelling.

De gegevens in het Incidentenregister kunnen voor zover noodzakelijk in het kader van het onderzoeken van een Incident, worden uitgewisseld. In het kader van de veiligheid en integriteit (als omschreven in artikel 4.1.1 Protocol) kan het namelijk nodig zijn dat Veiligheidszaken ten behoeve van onderzoek naar Incidenten gegevens uitwisselen. Dit kan nodig zijn om het verloop van een Incident te reconstrueren, vast te stellen of inderdaad sprake was of is van een bedreiging van de veiligheid en integriteit, bewijsmateriaal te verzamelen en maatregelen te treffen (denk aan de EVR registratie) om herhaling te voorkomen.

Onderzoek valt nadrukkelijk onder het doel van het verwerken van Persoonsgegevens in het Incidentenregister. Dit doel wordt omschreven in artikel 4.1.1 Protocol. Het gaat om een rechtmatig doel (artikel 5 AVG). De uitwisseling is gebaseerd op de grondslag van artikel 6 lid 1 (f) AVG (gerechtvaardigd belang). Deze uitwisseling van gegevens door Veiligheidszaken ten behoeve van onderzoek is met waarborgen omkleed. De waarborgen volgen uit de bepalingen in het Protocol. Ze worden hierna beschreven.

Waarborgen op hoofdlijnen

Er is sprake van een stapsgewijze opbouw van het verwerkingsproces, waarin verschillende waarborgen zijn opgenomen.

- Betrokkenen worden in overeenstemming met het Protocol geïnformeerd. Dat is bij voorkeur op het moment van het instellen van het onderzoek. Ook wordt de Betrokkene bijvoorbeeld via privacy statements, aanvraag- en sollicitatieformulieren geïnformeerd over het feit dat er onderzoek kan worden ingesteld.

- Alleen indien Veiligheidszaken vaststelt dat sprake is van een gebeurtenis die zodanig ernstig is dat wordt voldaan aan de criteria van artikel 4.1.1 Protocol, kan Veiligheidszaken besluiten tot vastlegging van gegevens betreffende het Incident in het Incidentenregister.

- Veiligheidszaken kan besluiten om Veiligheidszaken van een andere Financiële Instelling om informatie te vragen. Dit kan Veiligheidszaken alleen doen als sprake is van vastlegging van gegevens in het Incidentenregister en is voldaan aan het proportionaliteits- en subsidiariteitsbeginsel. De interne afwegingen om te komen tot de verstrekking, de wijze van bevragen, en de proportionaliteits- en subsidiariteitsafweging worden vastgelegd door Veiligheidszaken in haar administratie. De onderzoeker van de vragende afdeling Veiligheidszaken maakt aan de bevraagde afdeling Veiligheidszaken, voorafgaand aan de bevraging, duidelijk kenbaar wie hij is en hij informeert de andere afdeling Veiligheidszaken over de reden van de bevraging.

- De bevraagde afdeling Veiligheidszaken kan eerst na eigen toetsing aan het proportionaliteits- en subsidiariteitsbeginsel overgaan tot verstrekking van

Persoonsgegevens, die door de bevraagde Financiële Instelling worden verwerkt aan de vragende afdeling Veiligheidszaken. Deze verstrekking kan gegevens betreffen uit het Incidentenregister of uit een andere administratie van de bevraagde Financiële instelling. De uitwisseling dient toereikend, ter zake dienend en beperkt te zijn tot wat noodzakelijk is voor de doeleinden waarvoor de Persoonsgegevens worden verwerkt. De interne afwegingen om te komen tot de verstrekking, de wijze van verstrekken, en de proportionaliteits- en subsidiariteitsafwegingen worden vastgelegd door Veiligheidszaken in haar administratie.

- Alleen indien aan de voorwaarden van artikel 5.2.1 Protocol wordt voldaan kan de uitkomst van een onderzoek leiden tot registratie in het EVR.

- De Betrokkene wordt overeenkomstig artikel 9.1 Protocol geïnformeerd over de Verwerking van zijn Persoonsgegevens, uiterlijk op het moment van de eerste verstrekking. De Betrokkene kan hiervan tijdens een gesprek op de hoogte worden gesteld. Ook kan dit schriftelijk worden gedaan bijvoorbeeld door middel van een brief. Veiligheidszaken documenteert de informatieverstrekking in haar administratie, bijvoorbeeld door het opnemen van de informatiebrief aan de Betrokkene of notitie van het gesprek. Hiermee legt de Financiële Instelling vast dat zij aan haar informatieverplichting heeft voldaan.

- De Betrokkene wordt over de uitkomst van een onderzoek naar een Incident geïnformeerd. Als het onderzoek naar een Incident leidt tot aangepaste dienstverlening (bijvoorbeeld wel een rekening openen, maar dan zonder kredietfaciliteit of uitsluiting opnemen in een verzekeringspolis) wordt de Betrokkene daarover geïnformeerd bij de totstandkoming, aanpassing of beëindiging van de overeenkomst.

De Verwerking moet als geheel goed worden beveiligd. Dit volgt uit de AVG en staat onder meer beschreven in artikel 3.6 Protocol. De beveiligingsvereisten conform artikel 3.6 Protocol gelden onverkort ook ten aanzien van de Verwerking van Persoonsgegevens in de onderzoeksfase.

De rechten van de Betrokkene als vastgelegd in artikel 9 Protocol gelden ook ten aanzien van de onderzoeksfase. Zie de uitwerking onder (iv) hierna.

Er is een laagdrempelige geschillenregeling ingericht. Deze staat in artikel 10.1 Protocol.

Waarborgen nader bezien

Bij het uitwisselen van Persoonsgegevens, waaronder Strafrechtelijke Persoonsgegevens, ten behoeve van onderzoek gelden meerdere waarborgen:

(i) de uitwisseling van gegevens door Veiligheidszaken moet het belang van waarborging van de integriteit van de financiële sector als omschreven in artikel 4.1.1 Protocol dienen;

Er moet worden vastgesteld of de uitwisseling van Persoonsgegevens het belang van waarborging van de integriteit van de financiële sector dient. Dit is onder meer het geval als uitwisseling van gegevens plaats heeft in het kader van onderzoek naar gedragingen die kunnen leiden tot benadeling van de branche waar de Financiële Instelling deel van uitmaakt, de Financiële Instelling zelf of de klant of werknemer van de Financiële Instelling. Denk aan onderzoek naar oneigenlijk gebruik van producten, diensten en voorzieningen of (pogingen) tot strafbare of laakbare gedragingen of overtreding van (wettelijke) voorschriften, gericht tegen de Financiële Instellingen, de klant of medewerker van de Financiële Instelling.

De uitwisseling van gegevens kan dus plaatsvinden als dit nodig is voor onderzoek naar Incidenten. Hierbij kan gedacht worden aan aanwijzingen dat sprake is van bijvoorbeeld fraude in het betalingsverkeer, zoals fraude met online bankieren, creditfraude, fraude met overschrijfformulieren of factuurfraude; fraude met bankgaranties en letters of credit; fraude met beleggingen; fraude in de consumptieve en hypothecaire dienstverlening; fraude met schadeverzekeringen door verzekerden, verzekeringnemers, tegenpartijen, begunstigden, intermediairs of herstelbedrijven; fraude met overlijdensrisicoverzekeringen of inkomensverzekeringen door verzekerden waarbij personen bij het sluiten van de verzekering niet eerlijk zijn en belangrijke gegevens verzwijgen; fraude met zorgverzekeringen door verzekerden of zorgaanbieders en fraude waarbij externe fraudeurs handelen in samenspanning met daders binnen de organisatie.

(ii) de uitwisseling van gegevens vindt alleen plaats tussen geautoriseerde medewerkers van Veiligheidszaken;

Uitsluitend Veiligheidszaken is belast met het uitvoeren van onderzoek naar Incidenten. De gegevens uit het Incidentenregister zijn alleen voor rechtstreekse raadpleging door de betreffende afdeling Veiligheidszaken zelf beschikbaar. Uitzondering op deze regel vormen bijvoorbeeld de interne accountant of de Functionaris Gegevensbescherming die kunnen controleren op de naleving van voorschriften van het Protocol. De gegevens worden adequaat en overeenkomstig de wettelijke vereisten beveiligd.

(iii) de uitwisseling van gegevens voldoet aan het proportionaliteitsbeginsel en subsidiariteitsbeginsel;

Bij het proportionaliteitsbeginsel gaat het om de vraag of er een redelijke verhouding bestaat tussen de aantasting van het privacy recht van de Betrokkene enerzijds en de legitieme doelen die worden nagestreefd met het onderzoek anderzijds. Dit beginsel strekt er in essentie toe dat niet meer Persoonsgegevens worden verwerkt dan voor het wel bepaald en gerechtvaardigd doeleinde strikt noodzakelijk is. Het beginsel van proportionaliteit noopt tot een zorgvuldige afweging tussen de diverse belangen. Het subsidiariteitsbeginsel betekent dat de Persoonsgegevens in redelijkheid niet op een andere, voor de bij de Verwerking van Persoonsgegevens Betrokkene minder inbreukmakende wijze kunnen worden verwerkt.

De bevragende afdeling Veiligheidszaken (en uitsluitend die) bepaalt of de uitwisseling van gegevens over een Incident ten behoeve van onderzoek nodig is. De afdeling Veiligheidszaken bepaalt dit tegen de achtergrond van artikel 4.1.1 Protocol. Bij het besluit wordt getoetst aan het proportionaliteit en subsidiariteitsbeginsel. Daarbij wordt rekening gehouden met de ernst van de feiten, de belangen van de Betrokkene en de belangen van de financiële sector, de Financiële Instelling of haar klanten en medewerkers. Veiligheidszaken moet het besluit om gegevens uit te wisselen, kunnen onderbouwen. De verstrekkende afdeling Veiligheidszaken kan eerst na eigen toetsing aan het proportionaliteits- en subsidiariteitsbeginsel overgaan tot verstrekking aan de vragende afdeling Veiligheidszaken.

Bij onderzoek worden primair de intern aanwezige gegevens geanalyseerd en geïnterpreteerd (denk daarbij aan het analyseren van gegevens uit de klantadministratie). Zo nodig wordt aanvullende informatie verzameld. Bijvoorbeeld bij de Betrokkene zelf. Ook kunnen openbare bronnen worden geraadpleegd. Indien het nodig is, wordt informatie ingewonnen bij een andere Financiële Instelling. Bijvoorbeeld als de Betrokkene verwijst naar stukken die berusten onder of afkomstig zijn van een andere Financiële Instelling of als de Betrokkene geen medewerking verleent of het bevragen van de Betrokkene het onderzoek kan schaden. Of als sprake is van Incidenten waar andere Financiële Instellingen een rol spelen. Denk bijvoorbeeld aan fraude in het betalingsverkeer waarbij geld is overgemaakt naar een rekening die beheerd wordt door een andere Bank. Soms zal het nodig zijn informatie te verifiëren in het kader van bewijsvoering.

(iv) de rechten van de Betrokkene als omschreven in artikel 9 Protocol zijn van toepassing;

Betrokkenen worden in overeenstemming met het Protocol geïnformeerd. Dat is bij voorkeur op het moment van het instellen van het onderzoek. Ook wordt de Betrokkene via onder meer privacy statements, aanvraag- en sollicitatieformulieren geïnformeerd over het feit dat er onderzoek kan of zal worden ingesteld.

De Betrokkene wordt geïnformeerd, tenzij dit niet mogelijk is of dit past binnen de andere wettelijke uitzonderingen. Denk bijvoorbeeld aan het geval dat het onderzoek wordt geschaad, als de Betrokkene daarvan op de hoogte zou worden gesteld. Dit kan bijvoorbeeld het geval zijn als de Betrokkene de mededeling zal aangrijpen om maatregelen te nemen om de waarheidsvinding te belemmeren. Zie ook de uitleg onder het kopje ‘kenbaarheid’ verderop in de Annex.

De Betrokkene wordt over de uitkomst van een onderzoek naar een Incident geïnformeerd. Als het onderzoek leidt tot aangepaste dienstverlening (bijvoorbeeld wel een rekening, maar dan zonder kredietfaciliteit) wordt de Betrokkene daarover geïnformeerd bij totstandkoming aanpassing of beëindiging van de overeenkomst.

De Betrokkene heeft ook recht op inzage conform het bepaalde in artikel 9 Protocol ten aanzien van de Verwerking van Persoonsgegevens die in het kader van artikel 3.2 Protocol plaats heeft. Onder het recht op inzage valt ook een mededeling over de in verslaglegging vastgelegde gegevens betreffende de toegepaste onderzoeksmethode en de middelen die ten behoeve van het onderzoek zijn ingezet. In het bijzonder de herkomst van de gegevens (bijvoorbeeld analyse van jaarrekeningen, het bevragen van de afdeling Veiligheidszaken van de andere Financiële Instelling of analyse van camerabeelden). In het kader van het Protocol betreft de gehanteerde onderzoeksmethode bij het opvragen van informatie bij een andere Financiële Instelling ten behoeve van het onderzoek naar een Incident. Buiten het Protocol gaat het om de rechten conform artikel 12 AVG e.v.

(v) bewaren van gegevens

Het onderzoek naar het Incident kan twee mogelijke uitkomsten hebben. Allereerst kan dit ertoe leiden dat in voldoende mate vast staat dat de onderzochte persoon betrokken is bij gedragingen die een bedreiging vormen of kunnen vormen voor de (financiële) belangen van cliënten en /of medewerkers van een Financiële Instelling, alsmede de (organisatie) van de Financiële Instelling zelf of de continuïteit en/of integriteit van de financiële sector. Als ook aan de overige voorwaarden van artikel 5.2 Protocol is voldaan worden de Persoonsgegevens opgenomen in het EVR voor maximaal 8 jaar. Deze datum vangt aan vanaf de datum van opname in het Incidentenregister (artikel 5.3.2 Protocol). In dat geval blijven de onderzoeksgegevens in het Incidentenregister vermeld staan. Het EVR is immers aan het Incidentenregister gekoppeld (artikel 3.1.2 Protocol). Indien bijvoorbeeld de proportionaliteitsafweging van artikel 5.2 Protocol opname in het EVR niet rechtvaardigt of voor een kortere duur, kunnen de gegevens nog steeds in het Incidentenregister blijven staan. De tweede optie is dat vaststaat dat onvoldoende kan worden aangetoond dat de onderzochte persoon betrokken is bij de betreffende gedragingen. In dat geval mag geen opname in het EVR plaatsvinden. Daarnaast dienen de Persoonsgegevens ook uit het Incidentenregister te worden verwijderd. Het in artikel 4.1.1 Protocol omschreven doel wordt dan immers niet meer met de registratie gediend.

Samenvattend

(i) De gegevensuitwisseling in het kader van het Protocol vindt uitsluitend plaats door de gespecialiseerde Veiligheidsafdelingen.
(ii) Uitsluitend Veiligheidszaken is bevoegd tot het nemen van beslissingen over de uitwisseling van gegevens over Incidenten met andere Financiële Instellingen.
(iii) Uitsluitend Veiligheidszaken kan de gegevens rechtstreeks raadplegen.
(iv) De toegang tot de gegevens wordt adequaat beveiligd.
(v) Op de verzameling en uitwisseling zijn de beginselen van proportionaliteit en subsidiariteit van toepassing.
(vi) Bij de Verwerking van gegevens wordt zoveel mogelijk transparantie naar de Betrokkene betracht.
(vii) Gegevens worden niet langer bewaard dan noodzakelijk.
(viii) Er is een laagdrempelige geschillenregeling ingericht.

Gegevens in het Incidentenregister

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. Met 'bij het Incident betrokken personen' wordt bedoeld personen die relevant zijn voor de beschrijving van het Incident. Het kan gaan om de volgende gegevens: (i) de kenmerken van het Incident; (ii) Persoonsgegevens van degene die bij het Incident betrokken zijn, zoals NAW-gegevens, geboortedatum, nationaliteit, IBAN, polisnummer en nummer KvK; (iii) identificerende gegevens over ras, etniciteit of gezondheid van de Betrokkene, alsmede Strafrechtelijke Persoonsgegevens; (iv) maatregelen die naar aanleiding van het Incident zijn opgenomen; (v) indicatie of opname in het Extern Verwijzingsregister heeft plaatsgevonden; (vi) op het Incident betrekking hebbende gegevensdragers, zoals foto's, video- en geluidsdragers; (vii) NAW-gegevens, telefoonnummer, ip-adres van personen die gerelateerd zijn aan het Incident. Het verwerken van bijzondere Persoonsgegevens vindt in overeenstemming met artikel 23 c UAVG plaats indien dit noodzakelijk is in aanvulling op de Verwerking van Strafrechtelijke Persoonsgegevens voor de doeleinden waarvoor deze gegevens worden verwerkt of voor zover dit noodzakelijk is op grond van een wettelijke verplichting of de wetgeving (waaronder de AVG en UAVG) hierin voorziet. Denk bijvoorbeeld aan het camerabeeld, waarop mogelijk ook gegevens over ras of etniciteit worden verwerkt. In phishing zaken waarbij gebruik wordt gemaakt van een money mule (persoon die zijn rekening en pas beschikbaar stelt aan een fraudeur), kan op een camerabeeld van de geldautomaat zijn vastgelegd wie het geld heeft opgenomen. Dit beeld vormt bewijs en is een belangrijk element in de vastlegging van het Incident. Het camerabeeld wordt vastgelegd in het Incidentenregister.

De gegevens in het Incidentenregister worden door de veiligheidsafdelingen of de fraudecoördinatoren van de (Organisatie van de) Deelnemers geraadpleegd als dat noodzakelijk is voor de uitvoering van hun werkzaamheden. Daarbij kan gedacht worden aan trendanalyse, het ontwikkelen van fraudepreventiestrategieën, onderzoek van Incidenten, pre-employment screening en integriteittoetsing, schadeverhaal en Customer Due Diligence.

De betreffende Brancheverenging is Verwerkingsverantwoordelijke voor de Verwerking van Persoonsgegevens die in zijn eigen Fraudeloket plaatsheeft. Zo is het Verbond Verwerkingsverantwoordelijke voor de Verwerking van Persoonsgegevens die plaats heeft binnen het Centrum Bestrijding Verzekeringscriminaliteit; dit is de afdeling die uitvoering geeft aan het Fraudeloket van het Verbond. Als de Betrokkene bijvoorbeeld vragen heeft over de Verwerking van Persoonsgegevens die binnen het Fraudeloket van het Verbond plaats heeft of zijn rechten in verband met deze Verwerking wenst uit te oefenen, dient de Betrokkene zich te richten tot het Verbond. De contactgegevens van de Brancheverenigingen alsmede de link naar de website zijn onderaan de Annex van dit Protocol opgenomen.

EVR

Aan ieder Incidentenregister is een Extern Verwijzingsregister (EVR) gekoppeld. Dit register bevat slechts identificerende gegevens. Gebruikers van de gegevens kunnen alleen maar vaststellen of iemand in het EVR voorkomt ('hit – no hit-systeem)'. Als sprake is van een hit moet de toetser zijn eigen Veiligheidszaken inschakelen. Als Veiligheidszaken van de toetsende instelling de verwijzings-gegevens in het eigen EVR heeft opgenomen dan kan deze de toetser direct adviseren wat te doen ten aanzien van de (dienstverlening aan de) betrokken (rechts)persoon. Is Veiligheidszaken van een andere Deelnemer verantwoordelijk voor opname in het EVR, dan neemt Veiligheidszaken van de toetsende (Organisatie van de) Deelnemer contact op met Veiligheidszaken van de Deelnemer die verantwoordelijk is voor opname in het EVR. Tussen beide Veiligheidszaken worden de gegevens uit het Incidentenregister uitgewisseld voor zover de gegevens relevant zijn voor de toetser: één en ander ter beoordeling van de Veiligheidszaken die de opname in het EVR heeft gedaan. Nadat de gegevens tussen beide Veiligheidszaken zijn uitgewisseld adviseert Veiligheidszaken van de toetsende Deelnemer de toetser. Het advies kan bijvoorbeeld zijn om wel of geen relatie aan te gaan of om nadere voorwaarden te stellen voordat de relatie wordt aangegaan of verleend. Op deze wijze kan door de toetsende (Organisatie van de) Deelnemer een gewogen beslissing worden genomen.

De toegang tot de Verwijzingsregisters (EVR's) voor Deelnemers is afhankelijk gesteld van het lidmaatschap van de verschillende Brancheverenigingen. (i) Leden van Verbond en ZN kunnen toetsen aan elkaars Verwijzingsgegevens. (ii) Leden van NVB, SFH en VFN kunnen afhankelijk van hun lidmaatschap toetsen aan de Verwijzingsgegevens van de leden van de Brancheverenigingen waarvan zij lid zijn. (iii) Bankverzekeraars kunnen toetsen aan de Verwijzingsgegevens van Verzekeraars en Banken. (iii) SFH-leden die tevens Verzekeraar zijn kunnen toetsen aan de Verwijzingsgegevens van Verzekeraars en Banken. (iv) Een deelnemende Bank die geen lid is van de NVB kan op eenzelfde wijze toetsen aan de Verwijzingsgegevens als een deelnemende Bank die wel lid is van de NVB. Verwezen wordt naar artikel 4.2 Protocol. Een deelnemende Verzekeraar die geen lid is van het Verbond of ZN kan op eenzelfde wijze toetsen aan de Verwijzingsgegevens als een deelnemende Verzekeraar die wel lid is van het Verbond of ZN. Verwezen wordt naar artikel 4.2 Protocol.

Kerntaak van het Fraudeloket is de coördinatiefunctie. Dit houdt in dat de Fraude-lokketten nagaan of sprake is van vergelijkbare Incidenten en dat zij de betrokken Financiële Instellingen met elkaar in contact brengen. Deze functie kan niet worden uitgevoerd met algemene informatie. Het gebruik van gegevens op persoonsniveau door de Fraudeloketten is noodzakelijk. Ten behoeve van die functie kan Veiligheidszaken het Fraudeloket van informatie voorzien. Het Fraudeloket heeft zelf geen toegang tot de Incidentenregisters van de Deelnemers. De coördinatiefunctie brengt de noodzaak met zich mee dat de Fraudeloketten zelf kunnen nagaan of betrokken personen in EVR staan gesignaleerd. Daarmee wordt voorkomen dat er persoonsverwisselingen plaats vinden. Tevens beschikt men dan ook over een indicatie van de actuele status van het dossier. De Fraudeloketten plaatsen zelf geen personen in het EVR.

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 wordt geraadpleegd. Ter verduidelijking voor (potentiële) cliënten en (potentiële) medewerkers van Financiële Instellingen wordt het Protocol op vijf onderdelen nader toegelicht. Het betreft (i) beveiliging; (ii) de kenbaarheid van het systeem; (iii) de grondslagen, proportionaliteit en subsidiariteit; (iv) het aangiftebeleid en (v) de waarborgen voor de Betrokkene.

Beveiliging

Iedere Deelnemer neemt passende technische en organisatorische maatregelen om een op risico afgestemd beveiligingsniveau te waarborgen. Bij de vaststelling van de maatregelen wordt rekening gehouden met het feit dat onder het Protocol sprake is van de Verwerking van Strafrechtelijke Persoonsgegevens.

Kenbaarheid

De hoofdregel van de zorgplicht uit de AVG is dat de Verwerking van Persoonsgegevens rechtmatig, behoorlijk en transparant is.

Bij onderzoek is het belangrijk dat een Deelnemer zorgvuldig te werk gaat. Dit kan inhouden dat de Betrokkene in de gelegenheid wordt gesteld zijn visie op de feiten te geven. Dit hoeft niet onder alle omstandigheden. Bijvoorbeeld niet als feiten afdoende vaststaan of als sprake is van een situatie als genoemd in artikel 9.1.2 Protocol.

Transparantie 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 kenbaarheidsvereiste wordt voldaan doordat op de websites van de betrokken Brancheverenigingen en Deelnemer 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. Iedere Deelnemer draagt er ook zorg voor dat informatie over de Verwerking van Persoonsgegevens op basis van het Protocol vast onderdeel uitmaakt van het Privacy Statement van de Deelnemer. De Betrokkene wordt zo vooraf geïnformeerd over het bestaan van, de mogelijke opname in het Incidentenregister en EVR en de mogelijke gevolgen hiervan.

Ten aanzien van de informatieplicht wordt het bepaalde in artikel 13 AVG en 14 AVG opgevolgd, waarbij de in de AVG en UAVG genoemde uitzonderingen van toepassing kunnen zijn. In uitzonderingssituaties kan het voorkomen dat de Betrokkene niet wordt geïnformeerd. Dit is bijvoorbeeld het geval als adressen van personen onbekend zijn. Ook kan het voorkomen dat door te informeren een lopend (opsporings)onderzoek wordt geschaad doordat bijvoorbeeld bewijsmateriaal wordt vernietigd. Of dat informeren een gevaar oplevert voor anderen. In dit soort gevallen kan een Financiële Instelling er voor kiezen om de Betrokkene niet of in latere instantie te informeren.

Grondslagen, proportionaliteit en subsidiariteit

Opname van gegevens in het Incidentenregister en het EVR betreft een Verwerking van Persoonsgegevens. Deze Verwerking moet voldoen aan de AVG en UAVG. Dit betekent onder meer dat de Verwerking gebaseerd moet zijn op één van de grondslagen van artikel 6 AVG. De grondslag voor de Verwerking van Persoonsgegevens in het kader van het Protocol is artikel 6 lid 1 (f) AVG: 'het gerechtvaardigd belang van de Verwerkingsverantwoordelijke'. Ook moet aan de beginselen van proportionaliteit en subsidiariteit worden getoetst ('evenredigheid'). Bij het proportionaliteitsbeginsel gaat het om de vraag of er een redelijke verhouding bestaat tussen de aantasting van het privacy recht van de Betrokkene, die het gevolg is van de registratie enerzijds en de legitieme doelen die worden nagestreefd met de registratie anderzijds. Dit beginsel strekt er in essentie toe dat niet meer Persoonsgegevens worden verwerkt dan voor het wel bepaald en gerechtvaardigd doeleinde strikt noodzakelijk is. Het beginsel van proportionaliteit noopt tot een zorgvuldige afweging tussen de diverse belangen. Het subsidiariteitsbeginsel betekent dat de Persoonsgegevens in redelijkheid niet op een andere, voor de bij de Verwerking van Persoonsgegevens Betrokkene minder inbreukmakende wijze kunnen worden verwerkt. Relevante belangen voor het proportionaliteits- en subsidiariteitsbeginsel in deze (kunnen) onder andere zijn: de instandhouding en werking van (de doelstellingen) van het Waarschuwingssysteem; de aard van het gewraakte gedrag in het licht van de doelstellingen van het Protocol (Arrest HR Santander); de (potentiële) impact van het gewraakte gedrag; en de persoon van de Betrokkene. Ook ten aanzien van de duur moet worden getoetst of het belang van opname prevaleert boven de mogelijke nadelige gevolgen voor de Betrokkene als gevolg van opname van zijn Persoonsgegevens. De aard van de Incidenten rechtvaardigt in beginsel een opnameduur van 8 jaar in het EVR. Van deze termijn kan worden afgeweken in bijzondere omstandigheden, die door de Deelnemer worden beoordeeld.

Aangiftebeleid

Voor de Deelnemer aan het Protocol geldt als uitgangspunt dat aangifte wordt gedaan of een klacht ingediend bij een opsporingsambtenaar als 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 Verwerkingen 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 kan bijvoorbeeld gaan om first offenders die zich niet bewust waren 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 hypotheek-aanvrager heeft gefraudeerd door valse inkomstengegevens 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 bij plaatsing in het EVR 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 voor plaatsing in het EVR als aangegeven in artikel 5.2.1, onder a en b Protocol.

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 Protocol 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 inzagerecht, correctierecht, recht op gegevenswissing, recht op beperking van de Verwerking en op de wijze waarop bezwaar tegen een Verwerking van de Persoonsgegevens kan worden aangetekend.

In de voorbeeldinstructies wordt, met betrekking tot EVR-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 registreren (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.

Contactgegevens van de Brancheverenigingen

Nederlandse Vereniging van Banken (NVB)
Gustav Mahlerplein 29-35, 1082 MS Amsterdam
Postbus 7400, 1007 JK Amsterdam
T 020 550 28 88
info@nvb.nl
www.nvb.nl

Verbond van Verzekeraars (Verbond)
Bordewijklaan 2, 2591 XR Den Haag
Postbus 93450, 2509 AL Den Haag
T 070 333 85 00
info@verzekeraars.nl
www.verzekeraars.nl

Vereniging van Financieringsondernemingen in Nederland (VFN)
Maanweg 174, 2516 AB Den Haag
T 070 314 24 42
info@vfn.nl
www.vfn.nl

Stichting Fraudebestrijding Hypotheken (SFH)
p/a Nederlandse Vereniging van Banken
Gustav Mahlerplein 29-35, 1082 MS Amsterdam
Postbus 7400, 1007 JK Amsterdam
T 020 550 28 88
SFH@nvb.nl
www.stichtingfraudebestrijdinghypotheken.nl

Zorgverzekeraars Nederland (ZN)
Sparrenheuvel 16, Gebouw B, 3708 JE Zeist
Postbus 520, 3700 AM Zeist
T 030 698 89 11
info@zn.nl
www.zn.nl