

### **Preamble Protocol “Incidentenwaarschuwingssysteem financiële instellingen”**

Financiële instellingen worden regelmatig geconfronteerd met frauduleuze bedreigingen. Om te voorkomen dat deze bedreigingen een gevaar vormen voor de continuïteit en de integriteit van de financiële sector, de belangen van de cliënten en/of de financiële belangen van de instellingen zelf, worden risicobeheersende maatregelen genomen. Eén van deze maatregelen is het vastleggen van gedragingen van (rechts)personen die hebben geleid of kunnen leiden tot benadeling van financiële instellingen. Door het vastleggen van relevante gegevens over deze (rechts)personen en door het creëren van mogelijkheden om deze gegevens te raadplegen, kunnen de betreffende risico's tijdig worden onderkend en kunnen eventuele negatieve gevolgen worden beperkt.

Gedragingen van (rechts)personen die hebben geleid of kunnen leiden tot benadeling van financiële instellingen, worden door deze instellingen vastgelegd in incidentenregisters. Aan het incidentenregister zijn twee verwijzingsregisters gekoppeld. Het interne verwijzingsregister (IVR) bevat verwijzingsgegevens van (rechts)personen die uitsluitend raadpleegbaar zijn door de organisatie van de desbetreffende financiële instelling. Adequate risicobeheersing vergt dat de verwijzingsgegevens uit de incidentenregisters via een waarschuwingssysteem beschikbaar zijn voor andere financiële instellingen. Daarom kunnen de financiële instellingen die de bepalingen van het protocol “incidentenwaarschuwingssysteem financiële instellingen” onderschrijven, deze gegevens via een extern verwijzingsregister (EVR) raadplegen. Het protocol bevat de voorwaarden voor opname in het incidentenregister en de verwijzingsregisters. Het protocol voorziet tevens in waarborgen tegen ongeautoriseerd gebruik van het stelsel van gegevensuitwisseling. Het protocol is geen gedragscode ex artikel 25 van de Wet bescherming persoonsgegevens, maar een toelichting op de aanmelding van het incidentenregister ex artikel 27 van de Wet bescherming persoonsgegevens door aan het incidentenwaarschuwingssysteem deelnemende financiële instellingen.

In het kader van het gebruik van het incidentenregister en de daaraan gekoppelde verwijzingsregisters zijn door de financiële instellingen diverse technische voorzieningen getroffen. De banken die nu lid zijn van de Nederlandse Vereniging van Banken (NVB), alsmede de financieringsinstellingen, die lid zijn van de Vereniging van Financieringsinstellingen in Nederland (VFN), hebben de mogelijkheid om via de zogenaamde Externe Verwijzingsapplicatie (EVA) te toetsen of een (rechts)persoon in het extern verwijzingsregister van de banken voorkomt. Verzekeraars kennen een vergelijkbaar waarschuwingssysteem, het Fraude en Informatiesysteem Holland (FISH). Een deelmodule van FISH biedt deelnemende verzekeraars de mogelijkheid om door middel van toetsing vast te stellen of een (rechts)persoon is opgenomen in de externe verwijzingsindex van de verzekeraars (EVI). In het kader van de praktische uitvoering van het “Protocol Incidentenwaarschuwingssysteem financiële instellingen”, zal een technische voorziening worden getroffen om de externe verwijzingsindices voor de aan het incidentenwaarschuwingssysteem deelnemende banken, verzekeraars en financieringsinstellingen toegankelijk te maken.

# PROTOCOL INCIDENTENWAARSCHUWINGSSYSTEEM FINANCIËLE INSTELLINGEN

## 1. Overwegingen inzake het gerechtvaardigd belang

- 1.1 Financiële instellingen zoals banken, verzekeringsmaatschappijen en/of financieringsmaatschappijen worden voortdurend geconfronteerd met activiteiten van (rechts)personen, die op enigerlei wijze schade toebrengen of dreigen toe te brengen aan die financiële instellingen, hun medewerkers of hun cliënten, of voor onoorbare doeleinden gebruik maken van hun diensten (waaronder het witwassen van criminele gelden).
- 1.2 Deze activiteiten kunnen een bedreiging vormen voor de continuïteit en de integriteit van de financiële instellingen, de financiële belangen van de cliënten en/of de financiële belangen van de instellingen zelf. Door het vastleggen van relevante gegevens over deze (rechts)personen en door het creëren van mogelijkheden om deze gegevens te raadplegen, kunnen de betreffende risico's tijdig worden onderkend en verkleind en kunnen eventuele negatieve gevolgen worden beperkt.
- 1.3 Criminaliteitsbeheersing- en risicomanagement vergen dat financiële instellingen samenwerken, ondermeer door op basis van reciprociteit informatie met betrekking tot (rechts)personen uit te wisselen.
- 1.4 Niet alleen de "eigen" belangen van de financiële instellingen dwingen tot samenwerking. Ook van overheidswege wordt in toenemende mate een beroep gedaan op de financiële instellingen om samen te werken op het gebied van criminaliteitsbestrijding. Tegen de achtergrond van de Nota Integriteit Financiële Sector (TK vergaderjaar 1997-1998, 25830) en als uitvloeisel van het project Financieel Rechercheren is in handhavingsarrangementen met het Openbaar Ministerie vastgelegd dat financiële instellingen de horizontale fraude zowel van binnenuit als van buitenaf gecoördineerd aanpakken ter ondersteuning van opsporing en vervolging, en de noodzakelijke maatregelen nemen om deze fraude te voorkomen.
- 1.5 De noodzaak tot samenwerking en gegevensuitwisseling vloeit ook voort uit de intensivering van het beleid van de financiële toezichthouders (DNB, PVK en AuFM) om de integriteit van de financiële sector te versterken. Voor cliëntacceptatie en vacaturevervulling impliceert deze beleidsintensivering, dat bij het aangaan van een relatie voldoende aandacht dient te worden gegeven aan het risico van onoorbare activiteiten en aan het (afbreuk)risico voor de financiële instelling(en).
- 1.6 De overwegingen 1.1 tot en met 1.5 vormen de rechtmatige grondslag voor het aanleggen en gebruiken van het incidentenwaarschuwingssysteem financiële instellingen.
- 1.7 Financiële instellingen onderkennen dat de vastlegging van gegevens leidt tot het ontstaan van verzamelingen van gegevens, op basis waarvan voor de betrokken (rechts)personen belangrijke beslissingen kunnen worden genomen. Het verzamelen en verder verwerken van dergelijke gegevens dient daarom met waarborgen te worden omkleed. Dit protocol bevat regels ten aanzien van de gegevensuitwisseling tussen de financiële instellingen en voorziet in waarborgen tegen het ongeautoriseerd gebruik van het stelsel van gegevensuitwisseling.
- 1.8 Aangezien op basis van dit protocol ook strafrechtelijke gegevens worden verwerkt ten behoeve van derden, anders dan krachtens een vergunning op grond van de Wet particuliere beveiligingsorganisaties en recherchebureaus (artikel 31 lid 1 onder c juncto artikel 22 lid 4 en lid 5 WBP), is de gegevensverwerking in het kader van het incidentenregister van de aan het incidentenwaarschuwingssysteem deelnemende financiële instellingen onderworpen aan voorafgaand onderzoek door het College Bescherming Persoonsgegevens.

## 2. Begripsbepalingen

In dit protocol wordt verstaan onder:

- Incidentenregister:** de gegevensverzameling(en) van de deelnemer, waarin incidentgegevens zijn vastgelegd;
- Intern Verwijzingsregister (IVR):** de deelverzameling van het incidentenregister van de deelnemer die slechts verwijzingsgegevens bevat met betrekking tot (rechts)personen en die uitsluitend bestemd is voor gebruik door (de eigen organisatie van) de deelnemer;
- Extern Verwijzingsregister (EVR):** de deelverzameling van het incidentenregister van de deelnemer die slechts verwijzingsgegevens bevat met betrekking tot (rechts)personen en die bestemd is voor gebruik door (de organisaties van) alle deelnemers.
- Externe Verwijzings-Applicatie (EVA)** de voorziening die door de deelnemers wordt gebruikt teneinde de externe en interne verwijzingsregisters toegankelijk te maken; een (tweetal) daartoe door de brancheorganisaties aangewezen organisatie(s) onderhoud(t)(en) deze voorziening;
- Deelnemer:** het volgens de procedure van artikel 8.1 tot het incidentenwaarschuwingssysteem financiële instellingen toegelaten lid van de Nederlandse Vereniging van Banken, het Verbond van Verzekeraars dan wel de Vereniging van Financieringsondernemingen in Nederland dat beschikt over een incidentenregister;
- Organisatie van de deelnemer** de deelnemer zelf, de dochtermaatschappijen van de deelnemer (als bedoeld in artikel 2:24a BW) dan wel de groepsmaatschappijen waarmee een deelnemer in een economische eenheid is verbonden (artikel 2:24b BW), als ook de bij de Rabobank Nederland aangesloten banken. Voorts worden de door de deelnemer geautoriseerde gevolmachtigde tussenpersonen tot de organisatie van de deelnemer gerekend, mits zij functioneren als financiële dienstverlener;
- (Primaire) bron:** de deelnemer die (als eerste) gegevens met betrekking tot (rechts)personen in het extern verwijzingsregister heeft opgenomen;

### **3. Algemeen**

#### **3.1 Incidentenregister en verwijzingsindices**

Iedere deelnemer heeft een incidentenregister dat als zodanig aangemeld is bij het College Bescherming Persoonsgegevens. Onder verantwoordelijkheid van de deelnemer treedt een veiligheidsafdeling of daartoe geautoriseerd personeel op als (sub)beheerder van het incidentenregister.

Aan het incidentenregister zijn twee verwijzingsindices gekoppeld. Enerzijds is er een index van verwijzingsgegevens van (rechts)personen die uitsluitend raadpleegbaar is door de deelnemer zelf, alsmede door de organisatie van de deelnemer (IVR). Anderzijds is er een index van verwijzingsgegevens van (rechts)personen die ook door andere deelnemers, alsmede de organisaties van die deelnemers kan worden geraadpleegd (EVR). Het incidentenregister van de deelnemer vormt tezamen met de daarvan afgeleide (interne en externe) verwijzingsregisters één geheel. De Externe Verwijzingsapplicatie (EVA) is de voorziening die door de deelnemers wordt gebruikt, teneinde de interne verwijzingsregisters en het externe verwijzingsregister register toegankelijk te maken.

#### **3.2 Toetsingsproces**

Bij toetsing door een deelnemer wordt op basis van de ingevoerde verwijzingsgegevens in de eerste plaats het IVR geraadpleegd. Indien dit geen positief resultaat oplevert, wordt, indien de bevrager daartoe geautoriseerd is, automatisch het EVR benaderd. In geval van een 'hit' dient de bevrager te allen tijde de eigen veiligheidsafdeling respectievelijk de geautoriseerde functionaris te raadplegen; deze raadpleegt vervolgens de veiligheidsafdeling respectievelijk de geautoriseerde functionaris van de (primaire) bron.

Met het oog op het traceren van misbruik van het systeem wordt iedere bevraging vastgelegd. Daarbij wordt vastgelegd wie heeft getoetst, waar vandaan is getoetst, wanneer is getoetst en of de toetsing al dan niet een 'hit' opleverde. Tevens controleert de veiligheidsafdeling of daartoe geautoriseerde functionaris of inderdaad het betreffende referentietelefoonnummer is geraadpleegd. De eigen veiligheidsafdeling of daartoe geautoriseerde functionaris van de bevrager en de veiligheidsdienst van de (primaire) bron worden namelijk van een 'hit' op de hoogte gesteld door een automatisch door het systeem aangemaakt bericht. Dit om te voorkomen dat alleen wordt gekeken of iemand ergens voorkomt, zonder bij de veiligheidsafdeling of daartoe geautoriseerde functionaris te verifiëren wat de reden voor opname is.

#### **3.3 Invoervalidatie**

De persoonsgegevens van de in het incidentenregister opgenomen personen dienen in overeenstemming met de wet te zijn verkregen en dienen bij de (primaire) bron gedocumenteerd herleidbaar te zijn.

Daarvoor in aanmerking komende functionarissen worden geïnformeerd omtrent de werking van het systeem. Zij worden er nadrukkelijk op gewezen dat het gebruik van het systeem uitsluitend is toegestaan binnen de regels van het protocol en de binnen de organisatie van de deelnemer geldende interne procedures en voorschriften.

De deelnemers dienen zorg te dragen voor een zorgvuldige invoervalidatie en instructies aan de veiligheidsafdeling teneinde zeker te stellen dat uitsluitend in overeenstemming met de regels van het protocol gegevens worden ingevoerd in het incidentenregister c.q. in de verwijzingsregisters.

Indien een deelnemer twijfelt of invoer van gegevens kan plaatsvinden conform de regels van het protocol, dient hij van invoer af te zien.

### **3.4 Geheimhouding**

Alle in de onder dit protocol begrepen registers opgenomen gegevens zullen als "strikt vertrouwelijk" worden behandeld. De deelnemers treffen voorzieningen die waarborgen dat geautoriseerde functionarissen onder een geheimhoudingsplicht vallen die zich zowel tijdens de duur van de dienstbetrekking als na afloop daarvan uitstrekt.

### **3.5 Beveiliging**

Iedere deelnemer dient maatregelen te treffen om te waarborgen dat uitsluitend deelnemers en/of daartoe geautoriseerde functionarissen toegang hebben tot IVR, EVR respectievelijk het incidentenregister. Verder neemt iedere deelnemer passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging dienen deze maatregelen te voorzien in een passend beveiligingsniveau, gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen.

## **4. Incidentenregister**

### **4.1 Doel incidentenregister**

Met het oog op het kunnen deelnemen aan het incidentenwaarschuwingssysteem financiële instellingen is iedere deelnemer gehouden de volgende doelstelling voor het incidentenregister te hanteren:

“Het geheel aan verwerkingen 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 financiële instellingen;
- 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, haar cliënten en medewerkers;
- het gebruik van en de deelname aan waarschuwingssystemen.”

### **4.2 Vastlegging**

In het incidentenregister worden slechts gegevens opgenomen van (rechts)personen, indien er naar het oordeel van de deelnemer sprake is van een gerede aanleiding, een en ander met inachtneming van de in 4.1 genoemde doelstelling.

### **4.3 Toegang incidentenregister**

Toegang tot de in het incidentenregister opgenomen gegevens door alle functionarissen uit de organisatie van de deelnemer is niet noodzakelijk noch wenselijk. Om redenen van vertrouwelijkheid zijn de gegevens uit het incidentenregister daarom slechts toegankelijk voor daartoe uitdrukkelijk aangewezen medewerkers van de veiligheidsafdeling(en) of de geautoriseerde functionaris van de deelnemer. De gegevens van het incidentenregister van de deelnemers zijn -voorzover relevant- op basis van reciprociteit beschikbaar voor de veiligheidsafdelingen van de andere deelnemers.

#### **4.4 Verwijdering van gegevens**

Indien er geen reden meer is voor het vastleggen van persoonsgegevens, bijvoorbeeld naar aanleiding van een verzoek ex artikel 10.4, draagt de deelnemer zorg voor verwijdering van gegevens en is verplicht zodanige maatregelen te treffen dat deze gegevens niet langer toegankelijk zijn. Verwijdering moet voorts plaatsvinden binnen een periode van maximaal 8 jaar, indien zich ten aanzien van betrokkene geen nieuwe aanleiding als bedoeld in artikel 4.2 van dit protocol heeft voorgedaan.

### **5. Intern verwijzingsregister (IVR)**

#### **5.1 Functie**

De functie van IVR is het vaststellen of een (rechts)persoon is opgenomen in het intern verwijzingsregister opdat gegevens uit het incidentenregister beschikbaar worden gesteld aan (de organisatie van) de deelnemer.

#### **5.2 Vastlegging**

In het intern verwijzingsregister kunnen uitsluitend verwijzingsgegevens worden opgenomen van (rechts)personen waarvan gegevens zijn vastgelegd in het incidentenregister en die een risico vormen voor (de organisatie van) de deelnemer. Daarbij kunnen de navolgende criteria als richtsnoer gelden:

- (redelijk vermoeden van) opzettelijke benadeling van de deelnemer, oneigenlijk gebruik van producten, diensten en voorzieningen en/of poging daartoe;
- (redelijk vermoeden van) het plegen van strafbare of laakbare gedragingen en/of overtreding van (wettelijke) voorschriften dan wel pogingen daartoe, gericht tegen de deelnemer, de organisatie van de deelnemer, haar cliënten en medewerkers.

#### **5.3 Toegang**

Aangezien volledige en ongecontroleerde toegang tot de incidentenregisters door alle functionarissen (uit de organisatie) van de deelnemers ongewenst is, is gekozen voor de opzet om slechts verwijzingsgegevens op te nemen in het IVR.

Het IVR is langs geautomatiseerde weg uitsluitend toegankelijk voor door (de organisatie van) de deelnemer aangewezen personen.

De toetsing resulteert in de vaststelling, dat de getoetste (rechts)persoon wel of niet is opgenomen in het incidentenregister. Toetsing in het IVR geeft derhalve uitsluitend een signalering en geen nadere gegevens omtrent de aanleiding van opname.

Bij een 'hit' wordt het telefoonnummer van de eigen veiligheidsafdeling of daartoe geautoriseerde functionaris van de deelnemer getoond waar nadere informatie dient te worden opgevraagd. In dat geval moet de toetsende persoon contact opnemen met de eigen veiligheidsafdeling of geautoriseerde functionaris van de deelnemer. Deze afdeling of functionaris stelt een nader onderzoek in naar de in het incidentenregister opgenomen gegevens. Op grond van dit nader onderzoek adviseert de veiligheidsafdeling respectievelijk de geautoriseerde functionaris degene die heeft getoetst, bijvoorbeeld over het al of niet aangaan van een relatie.

#### **5.4 Informatie-uitwisseling**

Informatie-uitwisseling uit de incidentenregisters naar aanleiding van een hit is beperkt tot de (organisatie van de) deelnemer en vindt uitsluitend plaats voor zover dit niet onverenigbaar is met het doel waarvoor de gegevens zijn verzameld.

## **6. Extern verwijzingsregister (EVR)**

### **6.1 Functie**

De functie van het EVR is het vaststellen of een (rechts)persoon is opgenomen in het extern verwijzingsregister opdat gegevens uit het incidentenregister van de deelnemers beschikbaar zijn voor (de organisatie van) de andere deelnemers.

### **6.2 Vastlegging**

Deelnemers dragen er voor zorg dat verwijzingsgegevens van (rechts)personen die aan de hierna vermelde criteria voldoen worden opgenomen in het extern verwijzingsregister. Opname geschiedt in beginsel door de financiële instelling die benadeeld is. Andere bij het incident betrokken deelnemers kunnen echter ook tot opname van gegevens overgaan, indien het nadeel de financiële sector in zijn algemeenheid treft.

De beslissing tot vastlegging wordt genomen door daartoe aangewezen medewerkers van de veiligheidsafdeling of daartoe geautoriseerde functionaris van de deelnemer. Voor opname in het extern verwijzingsregister gelden de volgende opnamecriteria:

1. De activiteiten van de (rechts)persoon kunnen een bedreiging vormen voor de continuïteit en de integriteit van financiële instellingen, de financiële belangen van cliënten en/of de financiële belangen van de (organisatie van de) deelnemer.
2. Er dient een proportionaliteitsafweging plaats te vinden, waarbij de betreffende functionaris vaststelt, dat het belang van de opname in het verwijzingsregister prevaleert boven de mogelijk nadelige gevolgen voor betrokkene als gevolg van de opname van zijn gegevens.
3. De betreffende (rechts)persoon moet betrokken zijn bij een benadeling van enige financiële instelling (of poging daartoe) of bij onoorbaar gebruik (of poging daartoe) van het financieel stelsel van zodanige aard
  - dat aangifte bij een opsporingsinstantie is gedaan of kan worden gedaan of
  - de relatie of overeenkomst is opgezegd of het besluit daartoe is genomen of
  - is geweigerd om een relatie of overeenkomst aan te gaan.

### **6.3 Uitzondering op vastlegging**

Indien er sprake is van opsporingsbelangen of andere gewichtige belangen kan opname achterwege blijven.

### **6.4 Toegang**

Aangezien volledige en ongecontroleerde toegang tot de incidentenregisters ongewenst is, is gekozen voor de opzet om slechts verwijzingsgegevens op te nemen in het EVR.

Het EVR is langs geautomatiseerde weg uitsluitend toegankelijk voor (de organisatie van) de deelnemers.

De toetsing resulteert in de vaststelling, dat de getoetste (rechts)persoon wel of niet is opgenomen in het incidentenregister.

Toetsing in het externe verwijzingsregister geeft geen nadere gegevens omtrent de aanleiding van opname.

Bij een 'hit' wordt het telefoonnummer van de eigen veiligheidsafdeling of geautoriseerde - functionaris van de deelnemer getoond waar nadere informatie dient op te worden opgevraagd. In dat geval dient de toetsende persoon contact op te nemen met de eigen veiligheidsafdeling of geautoriseerde functionaris van de deelnemer. Deze afdeling of functionaris stelt een nader onderzoek in en neemt onverwijld contact op met de veiligheidsafdeling of geautoriseerde functionaris van de (primaire) bron. Op grond van dit nader onderzoek en de verkregen informatie adviseert de veiligheidsdienst of geautoriseerde

functionaris degene die getoetst heeft omtrent bijvoorbeeld het al of niet aangaan van een relatie of het doen van een transactie.

### **6.5 Informatie-uitwisseling**

Informatie-uitwisseling uit de incidentenregisters naar aanleiding van een hit is beperkt tot de deelnemers en vindt uitsluitend plaats voor zover dit niet onverenigbaar is met het doel waarvoor de gegevens zijn verkregen.

## **7. Begeleidingscommissie**

Teneinde de uniformiteit inzake de uitleg en de toepassing van de regels van dit protocol te waarborgen is een begeleidingscommissie ingesteld. De begeleidingscommissie bestaat uit de door betreffende brancheverenigingen aangewezen personen. Indien daartoe aanleiding bestaat adviseert de begeleidingscommissie de deelnemers over de toepassing van de vastleggingscriteria. De deelnemers verbinden zich over de door hen gevolgde uitleg en toepassing van de vastleggingscriteria alle gevraagde informatie aan de begeleidingscommissie te verstrekken. De begeleidingscommissie brengt van haar bevindingen in ieder geval één keer per jaar verslag uit aan het bestuur van de betreffende brancheverenigingen.

## **8. Deelname**

### **8.1 Aanmelding en toetreding**

Deelnemers hebben het recht om toe te treden tot het incidentenwaarschuwingssysteem financiële instellingen, indien de begeleidingscommissie van oordeel is dat de toetreders aan daaraan door de begeleidingscommissie te stellen eisen voor toetreding voldoet. Nieuwe toetreders ondertekenen een toetredingsverklaring, waarin zij verklaren dat zij dit protocol zullen naleven.

### **8.2 Uittreding**

Een deelnemer heeft het recht uit te treden uit het incidentenwaarschuwingssysteem financiële instellingen. Hij dient zijn wens tot uittreding schriftelijk bij zijn branche-organisatie neer te leggen onder vermelding van de datum van uittreding. Na uittreding zal de deelnemer noch de organisatie van de deelnemer nog langer toegang hebben tot het EVR. De uitgetreden deelnemer zal direct ervoor zorgdragen dat de deelnemers geen toegang meer hebben tot de door hem of zijn organisatie ingebrachte gegevens.

### **8.3 Uitsluiting**

Indien en voorzover een deelnemer de in dit protocol neergelegde bepalingen niet naleeft, is het bestuur van de betreffende branchevereniging op advies van de begeleidingscommissie gerechtigd de deelnemer uit te sluiten van deelname.

Na uitsluiting is de deelnemer gehouden onverwijld de toegang tot de door hem ingebrachte gegevens te blokkeren.

### **8.4 Kosten**

De deelnamekosten worden aan de deelnemers in rekening gebracht op basis van een nader vast te stellen verrekeningsmethodiek.



## **9. Rechten en plichten deelnemers**

### **9.1 Reciprociteit**

De deelnemers zijn jegens elkaar gehouden tot naleving van het protocol.

### **9.2 Processuele bijstand**

De deelnemers verlenen elkaar desgevraagd processuele bijstand in geval van claims in verband met de verstrekking en het gebruik van gegevens zoals geregeld in dit protocol.

### **9.3 Aansprakelijkheid**

De deelnemer die gegevens verstrekt is aansprakelijk voor schade die ontstaat doordat de gegevens door deze deelnemer niet conform de vereisten van het protocol zijn opgenomen in het EVR, tenzij deze tekortkoming in de nakoming deze deelnemer niet kan worden toegerekend.

De deelnemer die gegevens gebruikt welke hij middels het EVR heeft verkregen is aansprakelijk voor schade die ontstaat doordat hij van deze gegevens onjuist of disproportioneel gebruik heeft gemaakt, tenzij deze tekortkoming in de nakoming deze deelnemer niet kan worden toegerekend.

## **10 Rechten betrokkene**

### **10.1 Mededeling van opname**

Degene wiens gegevens in een incidentenregister respectievelijk de interne verwijzingsregisters en het extern verwijzingsregister zijn opgenomen, heeft recht op mededeling van opname op of omstreeks het moment dat vastlegging van diens gegevens heeft plaatsgevonden, tenzij deze daarvan al op de hoogte is of tenzij een dergelijke mededeling achterwege blijft vanwege opsporings- respectievelijk onderzoeksbelangen, het belang van bronbescherming of het risico van het in verkeerde handen komen van de opnamemededeling.

Indien betrokkene niet overeenkomstig het voorgaande op de hoogte is gesteld wordt hij/zij op de hoogte gesteld zodra een toets geresulteerd heeft in een "hit".

Wanneer er sprake is van een hit in het intern verwijzingsregister (IVR), wordt deze mededeling schriftelijk gedaan door de veiligheidsafdeling c.q. –functionaris van de organisatie waartoe de toetsende functionaris behoort.

Wanneer de hit betrekking heeft op gegevens uit het incidentenregister van een andere of andere deelnemers (EVR-hit), verneemt betrokkene dit van de veiligheidsafdeling c.q. –functionaris van de primaire bron (art. 34 lid 1 onder b WBP).

De mededeling blijft echter - ook na een hit - achterwege, indien opsporings- respectievelijk onderzoeksbelangen, het belang van bronbescherming of het risico van het in verkeerde handen komen van de opnamemededeling het noodzakelijk maken dat een dergelijke mededeling achterwege blijft (art. 43 WBP).

### **10.2 Protocol**

Een ieder die daartoe een aanvraag indient kan bij de betreffende brancheorganisatie of bij de deelnemer dit protocol opvragen.

### **10.3 Mededelingen uit het incidentenregister**

Een ieder heeft het recht zich tot een deelnemer te wenden met het verzoek hem mede te delen of hem betreffende persoonsgegevens in het incidentenregister en/of het intern verwijzingsregister en/of het extern verwijzingsregister zijn opgenomen.

Dit verzoek dient schriftelijk te geschieden. Voordat op het verzoek wordt ingegaan dient betrokkene zich te legitimeren. Binnen vier weken wordt betrokkene schriftelijk medegedeeld of, en zo ja welke hem betreffende gegevens worden verwerkt.

Indien zodanige gegevens worden verwerkt, bevat de mededeling een volledig overzicht daarvan in begrijpelijke vorm, een omschrijving van het doel of de doeleinden van de verwerking, de categorieën van gegevens waarop de verwerking betrekking heeft en de ontvangers of categorieën van ontvangers, alsmede de beschikbare informatie over de herkomst van de gegevens.

De mededeling blijft achterwege, indien opsporings- respectievelijk onderzoeksbelangen, het belang van bronbescherming of het risico van het in verkeerde handen komen van gegevens het noodzakelijk maken dat een dergelijke mededeling achterwege blijft (art. 43 WBP).

#### **10.4 Correctie**

Degene aan wie overeenkomstig de artikelen 10.1 of 10.3 kennis is gegeven dat hem betreffende persoonsgegevens zijn opgenomen in het incidentenregister en/of in het interne en/of het externe verwijzingsregister, kan de verantwoordelijke verzoeken deze te verbeteren, aan te vullen, te verwijderen, of af te schermen indien deze feitelijk onjuist zijn, voor het doel of de doeleinden van de verwerking onvolledig of niet ter zake dienend zijn, dan wel anderszins in strijd met een wettelijke voorschrift worden verwerkt. Het verzoek bevat de aan te brengen wijzigingen.

De verantwoordelijke bericht de verzoeker binnen vier weken na ontvangst van het verzoek schriftelijk of dan wel in hoeverre hij daaraan voldoet. Een weigering is met redenen omkleed.

De verantwoordelijke draagt zorg dat een beslissing tot verbetering, aanvulling, verwijdering of afscherming zo spoedig mogelijk wordt uitgevoerd.

#### **10.5 Kettingbepaling**

De WBP verplicht de verantwoordelijke niet om een lijst bij te houden van deelnemers aan wie gegevens uit het incidentenregister zijn verstrekt (protocolverplichting).

De WBP verplicht de verantwoordelijke echter wel om, in het geval dat persoonsgegevens zijn verbeterd, aangevuld, verwijderd of afgeschermd naar aanleiding van een verzoek ex artikel 10.4, de deelnemers aan wie gegevens daaraan voorafgaand zijn verstrekt daarvan in kennis te stellen, tenzij dit onmogelijk is of een onevenredige inspanning kost.

Een dergelijke verplichting is alleen uitvoerbaar indien na te gaan is aan welke deelnemer(s) gegevens zijn verstrekt. Om die reden onderhoudt de verantwoordelijke een overzicht van verrichte verstrekkingen voor de duur van 1 jaar na de datum waarop de gegevens aan de andere deelnemer verstrekt is.

### **11 Overige regels**

#### **11.1 Geschillen**

Bij geschillen over de rechtmatigheid en juistheid van de individuele vastleggingen kan men zich wenden tot het bestuur/de directie van de betreffende deelnemer.

Indien deze stap niet leidt tot een oplossing van het geschil kan men zich wenden tot:

- de Geschillencommissie Bankzaken, indien het een geschil betreft met een lid van de Nederlandse Vereniging van Banken;
- de Stichting Klachteninstituut Verzekeringen indien het een geschil betreft met een lid van het Verbond van Verzekeraars of
- de Klachtencommissie van de Vereniging van Financieringsondernemingen in Nederland

indien het een geschil betreft met een lid van de Vereniging van Financieringsondernemingen in Nederland.

### **11.2 Toezicht**

De interne accountantsdienst of de externe accountant van de deelnemer zal de naleving van de bepalingen in dit protocol jaarlijks controleren. Van haar bevindingen naar aanleiding van deze jaarlijkse controle brengt de accountant(sdienst) verslag uit aan het bestuur van de deelnemer.

Ingeval van onregelmatigheden van EVR of een vermoeden van niet naleving van het protocol, kan het bestuur van de Nederlandse Vereniging van Banken, het Verbond van Verzekeraars of de Vereniging van Financieringsondernemingen in Nederland uit eigen beweging of op verzoek aan een deelnemer een afschrift van een accountantsrapport verzoeken dat wordt opgemaakt over de naleving van het protocol dan wel is opgemaakt naar aanleiding van de onregelmatigheden. De deelnemers zijn verplicht een accountantsrapport op te laten maken ingeval van vermoeden van niet naleving van protocol. De accountant brengt vertrouwelijk verslag uit aan het bestuur van de deelnemer.

De hiervoor genoemde besturen zijn gerechtigd een deelnemer van verdere deelname aan EVR uit te sluiten ingevolge het in artikel 8.3 van dit protocol bepaalde, alsmede indien een deelnemer weigert een afschrift van het rapport aan de genoemde besturen te verstrekken dan wel anderszins aanleiding geeft tot het nemen van deze beslissing.

### **12 Wijzigingen protocol**

Het bestuur van de Nederlandse Vereniging van Banken, het Verbond van Verzekeraars en de Vereniging van financieringsondernemingen kunnen gezamenlijk besluiten tot aanpassing of wijziging van het protocol. Een dergelijk besluit wordt genomen nadat de aanpassingen of wijzigingen niet op bezwaren zijn gestuit bij het College Bescherming Persoonsgegevens.