PROTOCOL

Stichting Fraude Aanpak Detailhandel

Het College bescherming persoonsgegevens heeft een verklaring van rechtmatigheid afgegeven, zoals dat vereist is op grond van de artikel 22, aanhef en vierde lid, onder c, jº artikel 31, aanhef en eerste lid, onder c, van de Wet bescherming persoonsgegevens (Wbp).

- Eerste verklaring van rechtmatigheid verleend op: 24 juni 2004
- Tweede verklaring van rechtmatigheid verleend op: 10 juli 2008
- Derde verklaring van rechtmatigheid ……

Versie 0.3

Preambule

De detailhandel, die thans zowel fysieke winkels als – in toenemende mate – webwinkels omvat, wordt regelmatig geconfronteerd met frauduleuze bedreigingen. Om te voorkomen dat deze bedreigingen een gevaar vormen voor de continuïteit en de integriteit van de detailhandel, de belangen van andere personeelsleden, leveranciers en cliënten en/of de financiële belangen van de detailhandelsonderneming zelf, worden risicobeheersende maatregelen genomen. Eén van deze maatregelen is het vastleggen van gedragingen van individuele personen die hebben geleid of kunnen leiden tot benadeling van de detailhandel. Door het vastleggen van relevante gegevens over deze 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.

Gegevens van individuele personen die handelingen hebben verricht ter benadeling van detailhandelsondernemingen of derden, worden door deze ondernemingen vastgelegd in incidentenregisters. Adequate risicobeheersing vergt dat de verwijzingsgegevens uit de incidentenregisters via een Waarschuwingsregister beschikbaar zijn voor andere detailhandelsondernemingen[1]. In het kader van het gebruik van het incidentenregister en het daarvan afgeleide Waarschuwingsregister is door de detailhandel een technische voorziening getroffen om de gegevens in het Waarschuwingsregister voor de aan dit register deelnemende ondernemingen in de detailhandel toegankelijk te maken. Dit protocol bevat de voorwaarden voor opname in het incidentenregister en het Waarschuwingsregister. Het protocol voorziet in waarborgen tegen ongeautoriseerd gebruik van het stelsel van gegevensuitwisseling.

1. Overwegingen inzake het gerechtvaardigd belang

1.1. De detailhandel wordt voortdurend geconfronteerd met activiteiten van individuele personen, die op enigerlei wijze schade toebrengen aan die detailhandel, haar medewerkers, haar leveranciers of haar klanten, of voor onoorbare doeleinden gebruik maken van hun diensten.

1.2. Deze activiteiten kunnen een bedreiging vormen voor de continuïteit en de integriteit van de detailhandel, de financiële belangen van derden en/of de financiële belangen van de ondernemingen zelf. Door het vastleggen van noodzakelijke gegevens over deze individuele 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 de ondernemingen in de detailhandel samenwerken, onder meer door op basis van wederkerigheid informatie met betrekking tot individuele personen uit te wisselen.

1.4. De overwegingen 1.1 tot en met 1.3 vormen de rechtmatige grondslag voor het aanleggen en gebruiken van het incidentenregister en het Waarschuwingsregister Detailhandel, te weten de verwerking is noodzakelijk voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke en van deelnemers aan wie de gegevens worden verstrekt.

Bij deze verwerking zal het belang van de deelnemer, en dat van andere deelnemers aan het Waarschuwingsregister, bij opname in het register worden afgewogen tegen de gevolgen van

[1] Voor begripsbepaling zie hoofdstuk 2

opname voor de betrokkene. De gevolgen van de opname dienen in verhouding te staan tot de ernst, omvang en gevolgen van het gepleegde delict en de overige omstandigheden van het geval.

1.5. De detailhandel onderkent dat de vastlegging van gegevens leidt tot het ontstaan van verzamelingen van gegevens, op basis waarvan voor de betrokken individuele 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 ondernemingen in de detailhandel en voorziet in waarborgen tegen het ongeautoriseerd gebruik van het stelsel van gegevensuitwisseling.

1.6. Aangezien op basis van dit protocol strafrechtelijke gegevens worden verwerkt ten behoeve van derden, anders dan krachtens een vergunning op grond van de Wet particuliere beveiligingsorganisaties en recherchebureaus (artikel 31, aanhef en eerste lid, onder c juncto artikel 22, aanhef en vierde en vijfde lid, Wbp), heeft het College bescherming persoonsgegevens een verklaring omtrent de rechtmatigheid van de gegevensverwerking afgegeven ex artikel 32, vijfde lid, Wbp.

2. Begripsbepalingen

In dit protocol wordt verstaan onder:

Bestuur:	het Bestuur van de Stichting Fraude Aanpak Detailhandel dat optreedt als verantwoordelijke in de zin van de Wbp voor het Waarschuwingsregister;
Bewerker:	degene die persoonsgegevens verwerkt ten behoeve van het Bestuur of een deelnemer, zonder aan het rechtstreekse gezag van het Bestuur of een deelnemer te zijn onderworpen; in die gevallen waarin kleine ondernemingen gezamenlijk leveren en toetsen aan het Waarschuwingsregister, door tussenkomst van een intermediair (brancheloket), treedt deze intermediair op als bewerker;
Incidentenregister:	een gegevensverzameling betreffende natuurlijke personen die gekoppeld is aan het Waarschuwingsregister en aangemeld is bij het College bescherming persoonsgegevens. De gegevensverzameling bevat alle interne fraudegevallen. Het incidentenregister dient als bron voor het Waarschuwingsregister. Termijn van plaatsing in het incidentenregister is maximaal acht jaar;
Waarschuwingsregister:	de gegevensverzameling die onder verantwoordelijkheid van het Bestuur deelnemers in staat stelt om in het kader van *pre-employment screening* na te gaan of een sollicitant bij een deelnemer frauduleuze handelingen heeft verricht die –na zorgvuldig onderzoek- hebben geleid tot ontslag of beëindiging van de arbeidsrelatie én aangifte bij de politie. Termijn van plaatsing in het Waarschuwingsregister is: twee of vier jaar;

Deelnemer:	de rechtspersoon die door het bestuur als deelnemer aan het Waarschuwingsregister is geaccepteerd en uit dien hoofde rechtstreeks toegang heeft tot het Waarschuwingsregister;
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 organisatorisch is verbonden (artikel 2:24b BW);
Concernrelatie:	een zodanige organisatie van de deelnemer dat de incidentenregisters van dochtermaatschappijen van de deelnemer dan wel groepsmaatschappijen aan elkaar gekoppeld worden zodat het incidentenregister voor elk van de maatschappijen toegankelijk is;
(Primaire) bron:	de deelnemer die (als eerste) gegevens met betrekking tot een individuele persoon in het Waarschuwingsregister heeft opgenomen;
Geregistreerde:	een ieder die een formele overeenkomst met de deelnemer of een andere formele werkgever heeft afgesloten voor het verrichten van arbeid of het vervullen van een stage bij de deelnemer en is opgenomen in het Waarschuwingsregister. Hieronder is in ieder geval begrepen: personeel in tijdelijk en vast dienstverband bij de deelnemer, stagiairs, zzp'ers, personeel op uitzendovereenkomst en overeenkomst tot het verrichten van bepaalde werkzaamheden of diensten (externe inhuur), personeel dat op detacheringsbasis werkzaam is, personeel in dienst van een payroll-organisatie, werkzaam onder leiding en toezicht van de deelnemer, alsmede personeel, werkzaam in dienst of ten behoeve van een concessionair;
Concessionair:	aanbieder van goederen of diensten die in een vestiging van een deelnemer verkoopruimte heeft gehuurd voor de verkoop van zogeheten A-merken of aldaar tijdelijk ruimte inneemt voor het promoten en/of demonstreren van goederen of diensten;
Interne fraude:	iedere vorm van onrechtmatig handelen, gepleegd jegens een deelnemer, een personeelslid of een derde, al dan niet in samenspanning met derden, gericht op het behalen van financieel voordeel voor zichzelf of voor derden door het wegnemen en toe-eigenen van geld en/of goederen (bedrijfsinformatie daaronder begrepen) welke in eigendom toebehoren aan de deelnemer, een personeelslid of een derde. Diefstal, verduistering (in dienstbetrekking), valsheid in geschrift en oplichting zijn de meest voorkomende vormen van fraude door medewerkers in de detailhandel.

3. Algemeen

3.1 Incidentenregister en verwijzingsapplicatie

Iedere deelnemer heeft een Incidentenregister dat als zodanig aangemeld is bij het College bescherming persoonsgegevens. Onder verantwoordelijkheid van de deelnemer treedt een veiligheidsafdeling of een daartoe geautoriseerde functionaris op als (sub)beheerder van het incidentenregister. Uit het incidentenregister worden gegevens beschikbaar gesteld aan het Waarschuwingsregister.
De brancheloketten treden op als bewerker van het incidentenregister ten behoeve van aangesloten kleine detailhandelsondernemingen.

3.2 Toetsingsproces

Bij toetsing door de deelnemer wordt op basis van de ingevoerde gegevens het Waarschuwingsregister geraadpleegd. 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 en oneigenlijk gebruik[2] 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 referentie-telefoonnummer is geraadpleegd. De eigen veiligheidsafdeling of de 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 de daartoe geautoriseerde functionaris te verifiëren wat de reden voor opname is.

3.3 Invoervalidatie

De persoonsgegevens 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 bestaande 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 het Waarschuwingsregister. 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 gegevens, opgenomen in een onder dit protocol begrepen register, zullen als "strikt vertrouwelijk" worden behandeld. De verantwoordelijke, de bewerker en de deelnemers treffen voorzieningen die waarborgen dat het geautoriseerde personeel onder een geheimhoudingsplicht valt die zich zowel tijdens de duur van de dienstbetrekking als na afloop daarvan uitstrekt.

[2] Stichting FAD ziet alle bevragingen buiten het kader van *pre-employment screening* in beginsel als oneigenlijk gebruik, tenzij er sprake is van een ander gerechtvaardigd belang van de deelnemer(s).

3.5 Beveiliging

De verantwoordelijke, de bewerker en iedere deelnemer treffen maatregelen om te waarborgen dat uitsluitend deelnemers of daartoe geautoriseerde functionarissen toegang hebben tot het Waarschuwingsregister en de daaraan ten grondslag liggende gegevens van het incidentenregister. Verder nemen de verantwoordelijke, de bewerker en 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 Waarschuwingsregister is iedere deelnemer gehouden de volgende doelstelling voor het incidentenregister op te nemen:
Het ondersteunen van activiteiten gericht op het waarborgen van de veiligheid en de integriteit van de detailhandel, 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 detailhandel;
- 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 detailhandel deel van uitmaakt, de economische eenheid (groep) waartoe de detailhandel behoort, de detailhandel zelf, haar cliënten en medewerkers;
- op het gebruik van en de deelname aan het Waarschuwingsregister.

4.2 Vastlegging

In het incidentenregister worden slechts gegevens opgenomen van individuele natuurlijke personen, indien er 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 en ook niet 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 veiligheidsfunctionaris van de deelnemer, dan wel de afdeling P&O/HRM.

4.4 Verwijdering van gegevens

Indien vastlegging van persoonsgegevens niet langer gewenst is, bijvoorbeeld naar aanleiding van een verzoek ex artikel 9.4, draagt de deelnemer zorg voor verwijdering van gegevens en is hij 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. Het Waarschuwingsregister

5.1 Functie

De functie van het Waarschuwingsregister is het vaststellen of een individuele persoon is opgenomen in het Waarschuwingsregister waarna de brongegevens uit het incidentenregister van de leverende deelnemers beschikbaar zijn voor (de organisatie van) de andere deelnemers.

5.2 Vastlegging

Deelnemers dragen er voor zorg dat verwijzingsgegevens van individuele natuurlijke personen die aan de criteria voldoen worden opgenomen in het Waarschuwingsregister. Opname geschiedt in beginsel door de deelnemer die benadeeld is, tenzij de opname wordt verzorgd door een intermediair (brancheloket) waarbij de deelnemer is aangesloten.
De beslissing wordt genomen door daartoe aangewezen medewerkers van de veiligheidsafdeling of daartoe geautoriseerde functionaris van de deelnemer. Voor opname in het Waarschuwingsregister gelden de volgende opnamecriteria:

1. Er moet sprake zijn van fraude, die is vastgesteld op basis van een deugdelijk onderzoek.
   - Wanneer de fraude intern wordt afgehandeld, door bijvoorbeeld een functionaris/afdeling 'Security', zal dit op basis van deugdelijk intern fraudebeleid moeten geschieden. Wanneer geen sprake is van een dergelijke afdeling/functionaris, zal aangesloten moeten worden bij de 'Aanbevelingen fraudebeleid', opgenomen in het instructie- en feitenboekje 'Hoe en wat over het Waarschuwingsregister' van stichting FAD.
   - Als de deelnemer voor het fraudeonderzoek een externe partij (die een vergunning heeft op basis van de Wet particuliere beveiligingsorganisaties) inschakelt, en/of het fraudeonderzoek wordt verricht door een register-onderzoeker (RON), opgenomen in het door de Stichting N'Lloyd daartoe gehouden register, voldoet het onderzoek aan de kwaliteitseisen die in de beveiligingsbranche gelden.
2. De frauduleuze activiteiten van de individuele natuurlijke persoon moeten geleid hebben tot ontslag (eigen personeel) of beëindiging van de arbeidsrelatie(extern personeel. Steeds moet vaststaan dat de betrokkene niet langer binnen de organisatie van de deelnemer werkzaam zal zijn. Een ontslag wegens dringende redenen ('op staande voet') is niet vereist, al zal deze ontslaggrond in de praktijk wel vaak worden gebruikt.
3. Er moet aangifte terzake zijn gedaan bij de politie, waarvan proces-verbaal is opgemaakt.
4. Er moeten voldoende bewijsstukken zijn en worden bewaard in het onderliggende dossier.
5. De betrokken persoon moet van het feit van opname op de hoogte zijn gesteld. Bij die gelegenheid wordt hij geïnformeerd over de mogelijkheid van inzage en correctie als verwoord in de artikelen 9.3 en 9.4 en over de mogelijkheid van een klacht ex artikel 10.2 bij de Klachtencommissie.
6. Voor opname in het Waarschuwingsregister weegt de deelnemer het eigen belang, en die van de andere deelnemers aan het Waarschuwingsregister, af tegen de gevolgen van de opname voor de betrokkene (proportionaliteitstoets). De gevolgen van opname dienen in verhouding te staan tot de ernst, aard en omvang van het gepleegde delict en de overige omstandigheden van het geval. De deelnemer zal in ieder geval rekening houden met de gevolgen van opname aan de hand van de volgende factoren:
   - duur dienstverband;
   - leeftijd natuurlijke persoon;
   - functie natuurlijke persoon;
   - aard en omvang van de fraude en de gevolgen daarvan;
   - vraag of er sprake is van verzachtende of verzwarende omstandigheden (recidive);

7. Indien bij de deelnemer een zogeheten *zero tolerance*-beleid van kracht is, hetgeen altijd de instemming van de (Centrale) Ondernemingsraad moet hebben én aan de betrokken medewerkers bekend moet zijn gemaakt, vindt evengoed de proportionaliteitstoets plaats. Het belang van de deelnemer zal in dat geval zeer zwaar wegen.

5.3 Uitzondering op vastlegging

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

5.4 Toegang

Aangezien volledige en ongecontroleerde toegang tot het Waarschuwingsregister ongewenst is, is gekozen voor de opzet om slechts verwijzingsgegevens op te nemen in het Waarschuwingsregister. Het Waarschuwingsregister is langs geautomatiseerde weg uitsluitend toegankelijk voor het Bestuur, (de organisatie van) de deelnemers alsmede voor de bewerkers.

De toetsing resulteert in de vaststelling dat de getoetste persoon wel of niet is opgenomen in het incidentenregister. Toetsing aan het Waarschuwingsregister geeft geen nadere gegevens omtrent de aanleiding tot de opname. Bij een 'hit' wordt het telefoonnummer van de eigen veiligheidsafdeling of geautoriseerde functionaris van de deelnemer getoond waar nadere informatie dient 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 arbeidsovereenkomst, het bieden van een stageplaats of de inzet van een externe medewerker.

5.5 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.

5.6 Verwijdering van gegevens

Indien vastlegging van persoonsgegevens niet langer gewenst is, bijvoorbeeld naar aanleiding van een verzoek ex artikel 9.4, draagt de verantwoordelijke zorg voor verwijdering van gegevens en is hij verplicht zodanige maatregelen te treffen dat deze gegevens niet langer toegankelijk zijn. Verwijdering moet voorts plaatsvinden binnen een periode van maximaal 4 jaar, indien zich ten aanzien van betrokkene geen nieuwe aanleiding als bedoeld in artikel 5.2 van dit protocol heeft voorgedaan.

6. Auditcommissie

6.1 Taak

De Auditcommissie heeft als taak het (doen) uitvoeren van controlewerkzaamheden (audits) terzake van het gebruik van het Waarschuwingsregister door de verantwoordelijke, de bewerker of de deelnemer en de verplichtingen die dienaangaande voortvloeien uit het protocol, de Wet bescherming persoonsgegevens of andere toepasselijke wet- en regelgeving. De Auditcommissie is vanwege haar specifieke taak als enige bevoegd in opdracht van het Bestuur voor stichting FAD audits uit te voeren bij de deelnemers.

6.2 Samenstelling

De Auditcommissie bestaat uit drie onafhankelijke personen, die worden benoemd door het Bestuur.

6.3 Bevoegdheden

Indien daartoe aanleiding bestaat adviseert de Auditcommissie 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 Auditcommissie te verstrekken. De Auditcommissie brengt van haar bevindingen in ieder geval één keer per jaar verslag uit aan het Bestuur.

6.4 Inrichting werkzaamheden

De Auditcommissie is bevoegd de inrichting van haar werkzaamheden in een reglement nader te regelen.

7. Deelname

7.1 Aanmelding en toetreding

Nieuwe toetreders hebben het recht om als deelnemer toe te treden, indien het Bestuur van oordeel is dat de toetreder aan daaraan door het Bestuur te stellen eisen voor toetreding voldoet. Nieuwe toetreders ondertekenen een toetredingsverklaring, waarin zij verklaren dat zij dit protocol zullen naleven.

7.2 Uittreding

Een deelnemer heeft het recht uit te treden. Hij dient zijn wens tot uittreding schriftelijk bij het Bestuur 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 Waarschuwingsregister. De uitgetreden deelnemer zal direct ervoor zorgdragen dat de deelnemers geen toegang meer hebben tot de door hem of zijn organisatie ingebrachte gegevens.

7.3 Uitsluiting

Indien en voor zover een deelnemer de in dit protocol neergelegde bepalingen niet naleeft, is de verantwoordelijke voor het Waarschuwingsregister (het Bestuur) op advies van de Auditcommissie gerechtigd de deelnemer uit te sluiten van deelname. Na uitsluiting is de deelnemer gehouden onverwijld de toegang tot de door hem of zijn organisatie ingebrachte gegevens te blokkeren.

7.4 Kosten

De deelnamekosten worden aan de deelnemers in rekening gebracht op basis van een nader vast te stellen verrekeningsmethodiek. Daarnaast worden kosten in rekening gebracht voor het afnemen van een audit.

8. Rechten en plichten deelnemers

8.1 Wederkerigheid

De deelnemers zijn jegens elkaar gehouden tot naleving van het protocol. Dit houdt onder meer in dat zij zich bereid verklaren het Waarschuwingsregister conform artikel 5.2 actief te vullen door in geval van interne fraude, bijzondere gevallen uitgezonderd, altijd aangifte te doen. Het is ongewenst dat de wens tot aansluiting (vooral) wordt ingegeven door de mogelijkheid tot raadpleging ten eigen behoeve.

8.2 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.

8.3 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 Waarschuwingsregister, tenzij deze tekortkoming in de nakoming deze deelnemer niet kan worden toegerekend.

De deelnemer die gegevens gebruikt welke hij middels het Waarschuwingsregister 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.

De deelnemers vrijwaren het Bestuur voor alle claims en aansprakelijkheden die het gevolg zijn van het niet conform het Protocol aanleveren, ontvangen en gebruiken van gegevens uit het Waarschuwingsregister.

9. Rechten betrokkene

9.1 Openbaarheid en mededeling van opname

Het bestaan van de incidentenregisters en het Waarschuwingsregister is openbaar. Degene wiens gegevens in een incidentenregister respectievelijk het Waarschuwingsregister zijn opgenomen, wordt hiervan op de hoogte gesteld voor het moment dat diens gegevens worden vastgelegd.

9.2 Protocol

Een ieder die daartoe een aanvraag indient kan bij de stichting Fraude Aanpak Detailhandel (FAD) en bij de deelnemer dit protocol verkrijgen.

9.3 Mededelingen uit het Waarschuwingsregister

Een ieder heeft het recht zich tot een deelnemer of de verantwoordelijke te wenden met het verzoek hem mede te delen of hem betreffende persoonsgegevens in het Waarschuwingsregister zijn opgenomen. Dit verzoek dient schriftelijk te geschieden, vergezeld van een kopie van een geldig paspoort, ID-bewijs of rijbewijs van de aanvrager. 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.

9.4 Correctie

Degene aan wie overeenkomstig de artikelen 9.1 of 9.3 kennis is gegeven dat hem betreffende persoonsgegevens zijn opgenomen in het Incidentenregister en/of het Waarschuwingsregister, 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 wettelijk 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.

9.5 Kettingbepaling

De Wbp verplicht de verantwoordelijke om, in het geval dat persoonsgegevens zijn verbeterd, aangevuld, verwijderd of afgeschermd naar aanleiding van een verzoek ex artikel 9.4, 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 zijn.

10. Overige regels

10.1 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 dit niet naar tevredenheid tot een oplossing leidt, kan een belanghebbende zich wenden tot:

- de bevoegde rechter;
- de Klachtencommissie van stichting FAD (na indiening en afhandeling van een verzoek aan de betrokken deelnemer om een oplossing; adres: Postbus 182, 2260 AD, Leidschendam; klachtformulier: www.stichtingfad.nl)
- het College bescherming persoonsgegevens (na de ontvangst van het bericht als bedoeld in artikel 46, tweede lid, Wbp).

10.2 Klachten

1. Er is een onafhankelijke Klachtencommissie met als taak het doen van uitspraken in het geval van een geschil tussen een belanghebbende en een verantwoordelijke over de wijze waarop uitvoering wordt gegeven aan dit protocol en de wet; het verrichte onderzoek leidt tot een bindend oordeel van de Klachtencommissie;
2. Na ontvangst van de uitspraak van de Klachtencommissie zal het Bestuur de betrokkenen berichten over de afdoening van de klacht, als bedoeld in artikel 46, tweede lid, Wbp;
3. De Klachtencommissie is gebonden aan een reglement. Zij is bevoegd de inrichting van haar werkzaamheden, in aanvulling op dat reglement, zelf nader te regelen.

10.3 Toezicht

De deelnemer zal de naleving van de bepalingen in dit protocol periodiek laten controleren door de Auditcommissie. Van haar bevindingen naar aanleiding van deze periodieke controle brengt de Auditcommissie verslag uit aan de deelnemer.

De deelnemer wordt minimaal één keer in de drie jaar gecontroleerd of vaker, indien er sprake is van onregelmatigheden in het Waarschuwingsregister of een vermoeden bestaat van niet naleving van het protocol.

11. Wijzigingen protocol

Het bestuur van de stichting Fraude Aanpak Detailhandel (FAD) kan besluiten tot aanpassing of wijziging van het protocol. Een dergelijk besluit wordt slechts genomen nadat de aanpassing of wijziging is goedgekeurd door het College bescherming persoonsgegevens. Het besluit is bindend voor de deelnemers.

Namens: ....., ondertekend op: .....

.....

Naam en functie[3] Handtekening

[3] Ondertekening uitsluitend door statutair directeur