Protocol Waarschuwingsregister Hotel Security Management

Preambule

Hotels worden met enige regelmaat geconfronteerd met personen die op enigerlei wijze schade toebrengen aan die hotels, hun medewerkers of hun hotelgasten of voor onbedoelde doeleinden gebruik maken van de faciliteit van een hotel. Te denken valt dan aan misdragingen, geweld, bedreigingen, uitlokking, onaangepast gedrag, handelen in drugs, fraude, oplichting, diefstal en discriminerend gedrag. Deze activiteiten vormen een bedreiging voor de veiligheid van hotels, hun personeel en hotelgasten. Eisen van goed gastheerschap, die eigen zijn aan het beheren van een hotel, verplichten hotels om zich tot het uiterste in te spannen om de veiligheid van personeel en hotelgasten zo goed mogelijk te waarborgen.

Om aan deze verplichting nader invulling te geven hebben hotels, aangesloten bij het Hotel Security Management (in het vervolg HSM) besloten om te komen tot een Waarschuwingsregister HSM (in het vervolg: Waarschuwingsregister of register). Door het vastleggen van relevante gegevens over de personen die zich misdragen hebben en door het creëren van mogelijkheden om deze gegevens te raadplegen, kan de betreffende problematiek tijdig worden onderkend en kunnen eventuele negatieve gevolgen worden beperkt.

Gegevens van individuele personen die zich zodanig hebben misdragen dat zij een bedreiging vormen voor de veiligheid van de hotels, hun personeel en hun hotelgasten, worden door de deelnemers vastgelegd in het Waarschuwingsregister. Adequate risicobeheersing vergt dat de gegevens uit het Waarschuwingsregister beschikbaar zijn voor andere deelnemers. Daarom kunnen deelnemers die zijn aangesloten bij het onderhavige Protocol Waarschuwingsregister HSM (in het vervolg: Protocol), deze gegevens invoeren, raadplegen of verstrekt krijgen. Het Protocol bevat de voorwaarden voor opname in en raadpleging van het Waarschuwingsregister. Het Protocol voorziet in waarborgen tegen ongeautoriseerd gebruik van het stelsel van gegevensuitwisseling.

In het kader van het gebruik van het Waarschuwingsregister is door de verantwoordelijke een technische voorziening getroffen om de gegevens in het Waarschuwingsregister voor de deelnemers toegankelijk te maken.

1. Overwegingen inzake het gerechtvaardigd belang

1.1 Misdragingen van personeelsleden, bezoekers en hotelgasten vormen een toenemend probleem waarmee het personeel van hotels en hun hotelgasten en bezoekers worden geconfronteerd.

1.2 Deze problematiek heeft gevolgen voor het personeel, de hotelgasten, bezoekers en het maatschappelijk aanzien van hotels. Door het vastleggen van noodzakelijke gegevens over deze individuele personen en door het creëren van mogelijkheden om deze gegevens te raadplegen, kan de betreffende problematiek eerder worden voorkomen en kunnen eventuele negatieve gevolgen worden beperkt.

1.3 De ernst van de problematiek vergt dat deelnemende hotels samenwerken, onder meer door op basis van reciprociteit informatie met betrekking tot individuele personen uit te wisselen. Deze verplichting vloeit voort uit de eisen van goed gastheerschap, die de hotels zich hebben opgelegd en die kenmerkend zijn voor het wezen van hotels.

1.4 De deelnemers aan het Waarschuwingsregister hebben hun maatschappelijke verantwoordelijkheid willen nemen door met het instellen van dit Waarschuwingsregister een bijdragen te leveren aan het voorkomen en bestrijden van overlast in de hotelbranche.

1.5 De overwegingen 1.1 tot en met 1.4 vormen de rechtmatige grondslag voor het aanleggen en gebruiken van het Waarschuwingsregister. De verwerking is noodzakelijk voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke en van derden aan wie de gegevens

worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert.

1.6 Verantwoordelijke en deelnemers onderkennen 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 deelnemers en voorziet in waarborgen tegen het ongeautoriseerde gebruik van het stelsel van gegevensuitwisseling.

1.7 Opname van persoonsgegevens in het Waarschuwingsregister van de HSM betekent niet automatisch dat een bij de HSM aangesloten hotel geen hotelkamer aan de betreffende persoon zal verhuren of geen bezoekers toelaat. In geval van een “hit” in het Waarschuwingsregister zal het bij de HSM aangesloten hotel op basis van de in de database vermelde reden van registratie een afweging maken of tot verhuur van een hotelkamer zal worden overgegaan of dat een bezoeker zal worden toegelaten. Eenzelfde afweging zal worden gemaakt bij aanname van personeel.

2. Begripsbepalingen

In dit Protocol wordt verstaan onder:

HSM	De afkorting HSM staat voor Hotel Security Management.
Het bestuur:	Het bestuur van de Vereniging Hotel Security Management die optreedt als verantwoordelijke in de zin van de Wbp voor het Waarschuwingsregister.
Overlast:	Misdragingen jegens (goederen van) een deelnemer, zijn personeel of zijn hotelgasten, die maatschappelijk onbetamelijk zijn en van een zodanige omvang of duur dat opname in het Waarschuwingsregister proportioneel is ten opzichte van de gevolgen voor de betrokkene.
Incidentenregister:	Het verwerken van persoonsgegevens die van belang kunnen zijn voor de veiligheid en integriteit van het hotelbedrijf en om die reden speciale aandacht behoeven.
Waarschuwingsregister:	De verwerking van persoonsgegevens die onder verantwoordelijkheid van de Vereniging HSM deelnemers in staat stelt om na te gaan of een sollicitant, potentiële bezoeker of potentiële hotelgast bij een deelnemer overlast van een zodanige omvang heeft veroorzaakt dat opname in het Waarschuwingsregister heeft plaatsgevonden.
Deelnemer:	Het volgens de procedure van artikel 7.1 toegelaten lid van HSM tot het Waarschuwingsregister, dat verplicht is om gegevens in te voeren in het register en gerechtigd is om gegevens in het Waarschuwingsregister te raadplegen.
Betrokkene:	Een natuurlijke persoon die overlast van een zodanige omvang heeft veroorzaakt dat zijn persoonsgegevens zijn opgenomen in het Waarschuwingsregister. Het kan daarbij gaan om personeelsleden, bezoekers en hotelgasten.

Verantwoordelijke:	de rechtspersoon, die alleen of tezamen met anderen het doel en de middelen voor de verwerking van persoonsgegevens vaststelt, i.c. de Vereniging HSM.
Primaire bron:	de deelnemer die als eerste gegevens met betrekking tot individuele personen in het Waarschuwingsregister heeft opgenomen.
Bezwaar:	Voordat personen worden opgenomen in het Waarschuwingsregister wordt dit, indien mogelijk, aan hen kenbaar gemaakt. Wanneer de betreffende persoon van mening is dat dit onterecht is, kan zij/hij binnen 6 weken bij de deelnemer bezwaar maken tegen opname in het Waarschuwingsregister. Indien na 6 weken geen bezwaar is ontvangen worden de gegevens opgenomen
Oplossing van het geschil:	Om opname in het Waarschuwingsregister van HSM te voorkomen kan de betrokkene binnen de bezwaartermijn van 6 weken tot schikking van het geschil overgaan. Dit houdt in dat de betrokkene met de deelnemer overeenkomt dat opname in het Waarschuwingsregister niet geschiedt omdat bijvoorbeeld veroorzaakte schade wordt vergoed of rekeningen worden betaald. Indien de betrokkene na 6 weken niet tot herstel over is gegaan worden de gegevens opgenomen.

3. Algemeen

3.1 Incidentenregister en verwijzingsapplicatie

Iedere deelnemer heeft een incidentenregister dat als zodanig aangemeld is bij het College bescherming persoonsgegevens (CBP). Onder verantwoordelijkheid van de deelnemer treedt een veiligheidsafdeling of een daartoe geautoriseerde functionaris op als beheerder van het incidentenregister.

Uit het incidentenregister worden onder voorwaarden gegevens beschikbaar gesteld aan het Waarschuwingsregister.

3.2 Toetsingsproces

Bij toetsing 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 van het register 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 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 register 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 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 register. Zij worden er nadrukkelijk op gewezen dat

het gebruik van het register 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 in de onder dit protocol begrepen registers opgenomen gegevens zullen als strikt vertrouwelijk worden behandeld. De verantwoordelijke 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.

3.5 Beveiliging en waarborgen

De verantwoordelijke en iedere deelnemer dienen maatregelen te treffen om te waarborgen dat uitsluitend de verantwoordelijke of daartoe geautoriseerde functionarissen van een deelnemer toegang hebben tot het Waarschuwingsregister en de daaraan ten grondslag liggende gegevens van 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 (Risicoklasse II). De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

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 verwerken van persoonsgegevens die noodzakelijk zijn voor het waarborgen van de veiligheid en integriteit van het hotelbedrijf en om die reden speciale aandacht behoeven.
- 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. In het incidentenregister worden alle gegevens (inclusief bewijsstukken) aangaande de aard, omvang en tijdstip van het incident vastgelegd, alsmede –indien bekend- de personalia van de betrokkene.

4.3 Toegang incidentenregister

Toegang tot de in het incidentenregister opgenomen gegevens door alle medewerkers 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 veiligheidsfunctionaris van de deelnemer. Alleen gegevens uit het incidentenregister van betrokkenen die zijn opgenomen in het Waarschuwingsregister zijn –voor zover relevant- op basis van reciprociteit beschikbaar voor de veiligheidsafdelingen van de andere deelnemers.

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 verplicht zodanige maatregelen te treffen dat deze gegevens niet langer toegankelijk zijn. Verwijdering moet voorts plaatsvinden binnen een periode van maximaal 3 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 Doel

Het Waarschuwingsregister heeft tot doel het ten behoeve van de bestrijding van overlast vastleggen en beschikbaar stellen van persoonsgegevens van bekende en onbekende personen teneinde, indien noodzakelijk, te kunnen beoordelen of, en zo ja onder welke voorwaarden, een persoon tot het hotel moet worden toegelaten dan wel dat met een persoon een arbeidsrelatie kan worden aangegaan.
Voor dat doel worden maximaal de volgende gegevens van de drie soorten van betrokkenen in het waarschuwingsregister opgenomen:

- (achter)naam van de man en meisjesnaam van de vrouw
- voorletters en voorvoegsels
- woonplaats en land
- geslacht
- datum opname
- primaire bron
- reden van opname

Deze gegevens zijn alleen toegankelijk voor daartoe geautoriseerde personen.

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.

De beslissing tot opname 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. De overlast die de individuele natuurlijke persoon heeft veroorzaakt moet zodanig zijn dat de persoon niet alleen de verdere toegang tot het hotel is ontzegd, maar dat naar maatschappelijke maatstaven gemeten de overlast tevens als onbetamelijk moet worden aangemerkt. Te denken valt aan handgemeen, bedreiging van het personeel, ernstige vervuiling van de kamers en geluidsoverlast na waarschuwing.
2. Indien het strafbare feiten betreft zal aangifte worden gedaan. Daarbij gaat het om incidenten als diefstal, tassenroof en het verlaten van het hotel zonder te betalen. Indien het een personeelslid of een persoon waarmee een arbeidsrelatie was aangegaan betreft, zal daarnaast ontslag worden verleend dan wel de arbeidsrelatie opgezegd..
3. Er moeten voldoende bewijsstukken zijn en worden bewaard in het onderliggende dossier.
4. Voor opname in het Waarschuwingsregister bij overlast en strafbare feiten weegt de deelnemer het belang van de deelnemer, en die van de andere deelnemers aan het Waarschuwingsregister, bij opname af tegen de gevolgen van de opname voor de betrokkene. De gevolgen van opname dienen in verhouding te staan tot het gepleegde delict en de overige omstandigheden van het geval.
5. De betrokken persoon moet van het feit van opname in het Waarschuwingsregister 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 bezwaar bij de deelnemer en beroep bij het Bestuur ex artikel 6.1.

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. Slechts wanneer het een persoon betreft die niet geïdentificeerd kon worden, kunnen andere gegevens, waaronder foto's, worden vastgelegd. Het Waarschuwingsregister is langs geautomatiseerde weg uitsluitend toegankelijk voor (de organisatie van) de deelnemers. De toetsing resulteert in de vaststelling, dat de getoetste persoon wel of niet in het Waarschuwingsregister voorkomt.

Bij een 'hit' wordt het telefoonnummer van de eigen veiligheidsafdeling of geautoriseerde functionaris van de primaire bron 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 toelaten tot het hotel of het aangaan van een arbeidsrelatie.

5.5 Informatie-uitwisseling

Informatie-uitwisseling uit het incidentenregister 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 ten gevolge van overlast of het plegen van strafbare feiten 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 van gegevens ten gevolge van het plegen van strafbare feiten moet voorts plaatsvinden binnen een periode van maximaal 3 jaar, indien zich ten aanzien van betrokkene geen nieuwe strafbare feiten als bedoeld in artikel 5.2 van dit protocol hebben voorgedaan. Bij overlast geldt in dat geval een periode van maximaal 1 jaar. Tevens bestaat de mogelijkheid dat de registratie van de betrokkene uit het Waarschuwingsregister verwijderd wordt indien het geschil met het betreffende HSM lid is opgelost. Verwijdering van persoonsgegevens is onherroepelijk en niet meer voor deelnemers te traceren.

5.7. Invoervalidatie

De persoonsgegevens dienen in overeenstemming met de Wbp te zijn verkregen en dienen bij de deelnemer gedocumenteerd herleidbaar te zijn. Daarvoor in aanmerking komende geautoriseerde medewerkers worden geïnformeerd omtrent de werking van het register. Zij worden er nadrukkelijk op gewezen dat het gebruik van het register 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 medewerkers van de deelnemer waar de overlast is veroorzaakt teneinde zeker te stellen dat uitsluitend in overeenstemming met de regels van het Protocol gegevens worden ingevoerd 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.

6. Bestuur: taken en bevoegdheden

6.1 Bestuur

Het Bestuur waarborgt de uniformiteit inzake de uitleg en de toepassing van de regels van dit Protocol. Het Bestuur stelt, op voorstel van een deelnemer, de criteria vast die ten grondslag liggen aan opname in het Waarschuwingsregister. Indien daartoe aanleiding bestaat adviseert het Bestuur de deelnemers over de toepassing van de vastleggingscriteria. De deelnemers verbinden zich over het door hen gevolgde beleid inzake uitleg en toepassing van de vastleggingscriteria alle gevraagde informatie aan het Bestuur te verstrekken. Het Bestuur brengt van haar bevindingen in ieder geval één keer per jaar verslag uit aan de deelnemers.

7. Deelname

7.1 Aanmelding en toetreding
Deelnemers, 3, 4 en 5 sterren hotels in Nederland, hebben het recht om 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 en dat het incidentenregister van de deelnemer is gemeld bij het College bescherming persoonsgegevens.

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 zorg dragen dat de ingebrachte persoonsgegeven uit het waarschuwingsregister worden verwijderd.

7.3 Uitsluiting
Indien en voor zover een deelnemer de in dit protocol neergelegde bepalingen niet naleeft, is het Bestuur 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.

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

8. Rechten en plichten deelnemers

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

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 het incidentenregister, het Waarschuwingsregister en de externe applicatie is openbaar. Degene wiens gegevens in een incidentenregister respectievelijk het Waarschuwingsregister zijn opgenomen, wordt hiervan schriftelijk op de hoogte gesteld op het moment dat diens gegevens worden vastgelegd, tenzij het opsporingsbelang zich tegen het doen van mededeling verzet of het

informeren onmogelijk is dan wel een onevenredige inspanning kost..

9.2 Protocol
Een ieder die daartoe een aanvraag indient kan bij het Bestuur of bij een deelnemer dit protocol opvragen. Het protocol is ook toegankelijk is via de website van HSM.

9.3 Mededelingen uit het incidentenregister
Een ieder heeft het recht zich tot de verantwoordelijke en een deelnemer te wenden met het verzoek hem mede te delen of hem betreffende persoonsgegevens in het incidentenregister en/of Waarschuwingsregister zijn opgenomen. 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 voor zover dat noodzakelijk is in het belang van de voorkoming, opsporing en vervolging van strafbare feiten of de bescherming van de betrokkene of de rechten en vrijheden van anderen.

9.4 Correctie
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 Waarschuwingsregister kan de deelnemer of 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 deelnemer of 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 deelnemer of verantwoordelijke draagt zorg dat een beslissing tot verbetering, aanvulling, verwijdering of afscherming zo spoedig mogelijk wordt uitgevoerd.

9.5 Kettingbepaling
De WBP verplicht de deelnemer en 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.

9.6 Recht van verzet
De betrokkene kan te allen tijde bij de deelnemer of het Bestuur verzet aantekenen tegen de verwerking van zijn persoonsgegevens in verband met zijn bijzondere persoonlijke omstandigheden. De deelnemer of het Bestuur beoordeelt binnen vier weken na ontvangst van het verzet of dit verzet gerechtvaardigd is. Indien het verzet gerechtvaardigd is beëindigt de deelnemer of het Bestuur terstond de verwerking.

9.7 Rechtsbescherming
Met betrekking tot een beslissing als bedoeld in artikel 9.3, 9.4, 9.5 en 9.6 kan een belanghebbende zich wenden tot de rechtbank met het schriftelijk verzoek de deelnemer of verantwoordelijke te bevelen alsnog het verzoek toe of af te wijzen dan wel het verzoek als bedoeld in artikel 9.6 van dit Protocol al dan niet te honoreren. Ook kan een belanghebbende zich binnen zes weken na de beslissing van een deelnemer of verantwoordelijke wenden tot het College bescherming persoonsgegevens met het verzoek te bemiddelen of te adviseren in zijn geschil met een deelnemer of de verantwoordelijke.

10. Overige regels

10.1 Geschillen

Bij geschillen over de rechtmatigheid en juistheid van de individuele vastleggingen kan een belanghebbende zich wenden tot de deelnemer. Indien dit niet naar tevredenheid tot een oplossing leidt kan een belanghebbende zich binnen zes weken wenden tot het Bestuur. De belanghebbende kan getuigen laten horen en zich door deskundigen doen bijstaan. De uitspraak van het Bestuur dient ter meerdere zekerheid van de betrokkene te leiden tot een nieuw besluit van de deelnemer, dat vatbaar is voor beroep bij de rechter.

10.2 Toezicht

De verantwoordelijke en de deelnemer zullen de naleving van de bepalingen in dit protocol periodiek (laten) controleren. Van haar bevindingen naar aanleiding van deze periodieke controle brengt de deelnemer verslag uit aan het Bestuur.

Ingeval van onregelmatigheden van het Waarschuwingsregister of een vermoeden van niet naleving van het protocol, kan de het Bestuur uit eigen beweging of op verzoek aan een deelnemer een afschrift van een onderzoeksrapport verzoeken dat wordt opgemaakt over de naleving van het protocol dan wel is opgemaakt naar aanleiding van de onregelmatigheden. De verantwoordelijke en deelnemers verklaren zich bereid een onderzoeksrapport op te zullen maken ingeval van vermoeden van niet naleving van protocol.

Het Bestuur is gerechtigd een deelnemer van verdere deelname aan het Waarschuwingsregister uit te sluiten ingevolge het in artikel 7.3 van dit protocol bepaalde, alsmede indien een deelnemer weigert een afschrift van het rapport aan het Bestuur te verstrekken dan wel anderszins aanleiding geeft tot het nemen van deze beslissing.

11. Restbepalingen

11.1 Wijzigingen protocol

Dit protocol is vastgesteld door het Bestuur en kan door het Bestuur worden gewijzigd. Elke wijziging van het protocol zal bij de AP worden gemeld en pas na toestemming van de AP worden doorgevoerd. Het besluit is bindend voor de deelnemers.

11.2 Toezicht op naleving protocol

Eens per jaar zal het Bestuur een interne controle laten uitvoeren op het protocol door een door het Bestuur aan te wijzen persoon. Hierbij worden de volgende onderdelen getoetst:

- juist gebruik van persoonsgegevens in het licht van het doel van het register;
- integere en vertrouwelijk omgang met gegevens;
- naleving inzage- en correctierecht;
- administratieve organisatie gegevensopslag en verstrekking;
- naleving van retentiebeleid en eventueel daaruit voorvloeiende vernietiging van de persoonsgegevens;

Elke vijf jaar zal het Bestuur een audit laten uitvoeren op de correcte toepassing van het protocol. De AP ontvangt een afschrift van dit auditrapport. Bij gewijzigde omstandigheden zal het Bestuur een wijziging van de melding indienen.