Het nieuwe Incidentenwaarschuwingssysteem financiële instellingen

in het perspectief van de bestaande jurisprudentie inzake inzage en correctie

*prof. mr. J.M.A. Berkvens**

1. Inleiding

Op 25 mei 2011[1] heeft het College bescherming persoonsgegevens goedkeuring verleend aan het Protocol Incidentenwaarschuwingssysteem financiële instellingen (hierna: protocol IFI).[2] Financiële instellingen (banken en verzekeraars) worden door de wetgever verplicht om een beheerste en integere bedrijfsuitoefening te waarborgen. Financiële instellingen hebben in dat kader een branchewaarschuwingssysteem opgezet.[3] Hierna wordt eerst ingegaan op het algemene juridische kader dat financiële instellingen verplicht een raamwerk van beschermingsmaatregelen op te zetten. In een dergelijk raamwerk is het nagenoeg onvermijdelijk voor financiële instellingen dat zij deelnemen aan een branchewaarschuwingssysteem.[4] Vervolgens wordt het nieuwe branchewaarschuwingssysteem van de financiële instellingen belicht. Ten slotte wordt ingegaan op de privacyaspecten van het branchewaarschuwingssysteem van de financiële instellingen. Daarbij wordt ook aandacht besteed aan de betekenis van de bestaande jurisprudentie inzake inzage en correctie voor het nieuwe systeem.

2. Algemeen juridisch kader: verplichtingen van de bank

Algemeen

Niet alleen een welbegrepen eigenbelang nodigt financiële instellingen (in dit artikel worden banken en verzekeraars aangeduid als financiële instellingen) uit tot voorzichtigheid in de bedrijfsvoering. De belangen van de samenleving bij een gezonde financiële sector zijn groot. Daarom heeft de wetgever via diverse wettelijke regelingen een juridisch raamwerk opgezet dat mede is gericht op de veiligheid en integriteit van de financiële sector.[5]

De Wet op het financieel toezicht

De Wet op het financieel toezicht (hierna: Wft) verplicht financiële instellingen hun bedrijfsvoering zodanig in te richten dat een beheerste en integere uitoefening van hun bedrijf wordt gewaarborgd. Art. 3:17 Wft (naast het vergelijkbare art. 4:15 Wft) speelt daarbij een belangrijke rol.[6] Dit artikel wordt nader uitgewerkt in het Besluit prudentieel

---

* Jan Berkvens is hoogleraar Informatica en Recht aan de Radboud Universiteit Nijmegen en tevens adjunct directeur Juridische Zaken bij Rabobank Nederland.

1. *Stcrt.* 8944, 25 mei 2011. Besluit Cbp z2010-01490, 18 mei 2011.
2. In de vorm van een verklaring omtrent de rechtmatigheid conform art. 32 lid 5 Wbp.
3. A.F. Rommelse, 'Zwarte lijsten, belangen en effecten van waarschuwingssystemen', *A&V studie nr. 4*, Registratiekamer, 1995. Zie ook F.B.M. Olijslager, 'Branchewaarschuwingssystemen, zwarte lijsten en andere signaleringmethoden ter voorkoming van schade', *Vakblad Beveiliging, managementblad voor veiligheidsadviseurs en security professionals*, december 2004. Zie ook bijdrage J. Holvast en F.B.M Olijslager, 'Waarschuwingsregisters ter voorkoming van fraude en criminaliteit' in 'Wet bescherming persoonsgegevens en ICT', *Monografieën Recht en Informatietechnologie*, deel 4, Den Haag: SDU 2006.
4. Zie ook O. Klaassen en R. Veldhuijzen, 'Toezicht van banken; waar ligt de grens', *FR* 2011, nr. 3, p. 59-64.
5. Een vergelijkbaar systeem voor de overheid werd in het leven geroepen door de wet Bibob (Bevordering Integriteitsbeoordelingen door het Openbaar Bestuur). De reikwijdte van deze wet wordt thans uitgebreid: *Kamerstukken II* 2010/11, 32 676.
6. Art. 3:17 lid 1: *Een clearinginstelling, kredietinstelling of verzekeraar met zetel in Nederland richt de bedrijfsvoering zodanig in dat deze een beheerste en integere uitoefening van haar onderscheidenlijk zijn bedrijf waarborgt.*

toezicht Wft (hierna: Bpr).[7] Hoofdstuk 3 Bpr betreft de integere bedrijfsuitoefening.[8] Hoofdstuk 4 Bpr de beheerste bedrijfsuitoefening. Het Besluit gedragstoezicht financiële ondernemingen (hierna: Bgfo) bevat regels voor beleggingsinstellingen.[9] Het gaat in beide besluiten om uitwerkingen op hoofdlijnen. De hoofdlijnen zijn principle based. Dat wil zeggen dat ze geen geconcretiseerde maatregelen bevatten. Het voordeel van deze aanpak is dat financiële instellingen zelf de hoofdlijnen kunnen toesnijden op de eigen organisatie. Nadeel is dat een concrete maatregel die door financiële instellingen wordt getroffen zelf nooit berust op een concreet wettelijk voorschrift. De financiële instelling kan zich bij conflicten met klanten, personeel of derden over haar veiligheidsmaatregelen dus niet volledig beroepen op het bestaan van een wettelijke verplichting. De verplichtingen ter waarborging van de beheerste en integere bedrijfsuitoefening hebben betrekking op zowel personeel als klanten.[10]

De Wet ter voorkoming van witwassen en financieren van terrorisme

Naast de Wft is ook de Wet ter voorkoming van witwassen en financieren van terrorisme (hierna: Wwft) van belang. Art. 3 van deze wet verplicht financiële instellingen tot het doen van klantonderzoek. Daarbij wordt de identiteit van de klant vastgesteld en worden overige gegevens verzameld teneinde het doel en de beoogde aard van de zakelijke relatie vast te stellen.[11,12]

Overige opsporingsrollen van financiële instellingen

Financiële instellingen spelen daarnaast een belangrijke rol bij de opsporing en vervolging van allerlei vormen van onoorbaar gedrag. Het gaat daarbij onder meer om bepalingen in het Wetboek van Strafvordering[13] en bepalingen in sociale zekerheidswetgeving.[14] Kenmerkend voor deze regelgeving is dat financiële instellingen verplicht kunnen worden om bij hen beschikbare gegevens aan de autoriteiten over te dragen.[15]

lid 2: Bij of krachtens algemene maatregel van bestuur worden regels gesteld met betrekking tot het eerste lid. Deze regels hebben betrekking op:
a. het beheersen van bedrijfsprocessen en bedrijfsrisico's;
b. integriteit, waaronder wordt verstaan het tegengaan van:
1°. belangenverstrengeling;
2°. het begaan van strafbare feiten of andere wetsovertredingen door de financiële onderneming of haar werknemers, die het vertrouwen in de financiële onderneming of in de financiële markten kunnen schaden;
3°. relaties met cliënten die het vertrouwen in de financiële onderneming of in de financiële markten kunnen schaden; en (…….).

7. Dit besluit borduurt deels voort op de eerdere DNB Regeling organisatie en beheersing (Rob; *Stcrt*. 2001, 65).
8. Zie bijvoorbeeld de tekst van art. 14 lid 4 van het besluit: *De financiële onderneming, bedoeld in het tweede lid, onderscheidenlijk het bijkantoor, beschikt over procedures en maatregelen met betrekking tot de analyse van gegevens van cliënten, mede in relatie tot de door de cliënt afgenomen producten of diensten, en terzake van de detectie van afwijkende transactiepatronen. Aan de hand van voornoemde procedures en maatregelen bepaalt de financiële onderneming tevens de risico's van bepaalde cliënten, producten of diensten voor de integere uitoefening van haar bedrijf.*
9. De regeling voor beleggingsinstellingen is gebaseerd op art. 4:14 van de Wft en nader uitgewerkt in het Besluit Gedragstoezicht financiële ondernemingen Wft (Bgfo), *Stb.* 2006, 520.
10. Zie ook art. 3:11 en art. 4:10 Wft.
11. Zie ook de toelichting op de privacygedragscode 2010, p. 29: *De Wwft eist dat de gegevens van het document waarmee de identiteit is vastgesteld moeten worden vastgelegd. De vastlegging van de gegevens is in lijn met de verplichting tot uitvoeren van het Cliëntenonderzoek uit de Wwft. Aangezien de Wwft risk based is, betekent dit dat de Financiële instelling de mogelijkheid heeft om het Cliëntenonderzoek af te stemmen op de risicogevoeligheid voor witwassen of financiering van terrorisme van het type Cliënt, de zakelijke relatie, het product of de transactie. Dit geeft de instelling de vrijheid om eigen keuzes te maken, rekening houdend met risico's en reeds bestaande beheersmaatregelen. Net als bij de Wid en de Wet MOT is in de Wwft een belangrijke rol weggelegd voor toezichthouders. Als bewijsmateriaal voor identificatie en verificatie - twee eisen uit de Wwft – mogen Financiële instellingen - net als onder de WID - het 'kopietje paspoort' opnemen in hun administratie. De Wwft schrijft (samengevat) twee activiteiten voor op het gebied van Cliëntenonderzoek en de Melding van ongebruikelijke transacties. Voor de goede orde wordt opgemerkt dat er daarnaast nog vele wettelijke voorschriften bestaan op grond waarvan een Financiële instelling verplicht is bepaalde persoonsgegevens te verwerken.*
12. Zie ook Leidraad van het Ministerie van Financiën voor de uitvoering van wettelijke verplichtingen voor wat betreft de voorkoming van witwassen en terrorismefinanciering van 21-2-2011, gepubliceerd op http://www.rijksoverheid.nl/documenten-en-publicaties/richtlijnen/2011/02/21/algemene-leidraad-wet-ter-voorkoming-van-witwassen-en-financieren-van-terrorisme-wwft-en-sanctiewet-sw.html.
13. Bijvoorbeeld art. 126nc e.v. Sv.
14. Bijvoorbeeld titel 5.2 Awb.
15. Zie ook art. 47b Awr en art. 53 Awr in samenhang met art. 10 lid 8 van de Wet IB 2001, nader uitgewerkt in art. 22

3. Ontwikkeling van het branche-waarschuwingssysteem in de tijd

Overzicht van diverse privacygedragscodes en protocollen zoals die binnen de financiële sector in de loop van de tijd tot stand zijn gekomen

1989	Eerste Privacygedragscode banken[16] (privacy-gedragscode 1989)
1990	Vaststelling IRIS-protocol (Wpr[17])
1995	Vaststelling Privacygedragscode banken 1995 (Wpr)
1998	Vaststelling Privacygedragscode verzekeraars 1998 (Wpr)
2002	Vaststelling EVA-protocol 2002 banken en verzekeraars (Wbp)
2003	Vaststelling Gedragscode verwerking persoonsgegevens financiële instellingen(privacygedragscode 2003) (Wbp)
2004	Vaststelling EVA-protocol 2004 banken en verzekeraars (Wbp)
2006	Zorgverzekeraars treden toe tot privacygedragscode 2003 (Wbp)
2010	Vaststelling Gedragscode verwerking persoonsgegevens financiële instellingen (privacygedragscode 2010) (Wbp)
2011	Vaststelling Protocol incidentenwaarschuwingssysteem financiële instellingen (protocol IFI)[18] (Wbp)

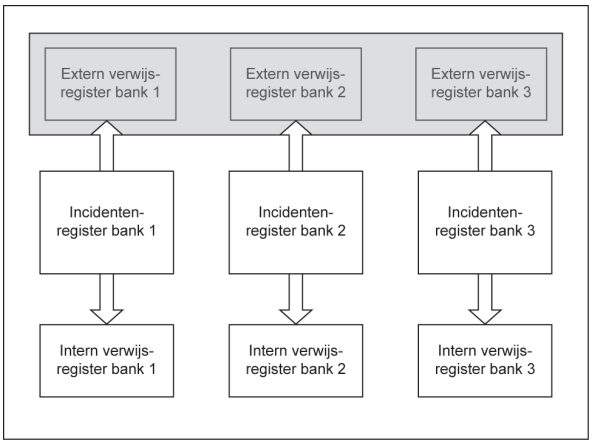
IRIS protocol

Het eerste interbancaire branchewaarschuwingssysteem dateert van omstreeks 1990.[19] Het juridisch kader van het waarschuwingssysteem werd vastgelegd in het zogenaamde IRIS protocol. De afkorting IRIS staat voor Incidenten Registratie en Informatie Systeem. De basis van dit systeem werd gevormd door de zogenaamde incidentenregisters van de afzonderlijke financiële instellingen. Die incidentenregisters werden beheerd door de veiligheidsafdelingen van de banken. De veiligheidsafdelingen beoordeelden naar aanleiding van incidenten of bij die incidenten betrokken personen een risico vormden voor de eigen organisatie. Indien dat het geval was, konden de identificerende gegevens van de betrokkenen in een intern verwijsregister worden opgenomen. De front offices van de eigen bank konden dit verwijsregister raadplegen en vervolgens overleggen met de veiligheidsafdeling of het verstandig was de betrokkene de gevraagde dienst te leveren. Van personen die naar de mening van de veiligheidsafdeling eveneens een bedreiging vormden voor andere banken, konden de identificerende gegevens worden opgenomen in een extern verwijsregister. Op die wijze konden ook de front offices van andere banken op risico-personen worden geattendeerd (zie figuur 1). De veiligheidsafdelingen zelf konden onderling gegevens uitwisselen uit hun incidentenregisters. De verwerking van persoonsgegevens in de incidentenregisters maakte geen deel uit van de privacygedragscode banken 1995.[20] De beperkingen ten aanzien van de verwerking van strafrechtelijke gegevens uit deze privacygedragscode zijn dan ook niet van toepassing op incidentenregisters. Die privacygedragscode bevatte overigens wel een antifraudedoelstelling.[21] Maar die heeft alleen betrekking op het gebruik van cliëntgegevens uit de reguliere cliëntenadministratie in het kader van fraudebestrijding.

Verzekeraars

Simultaan aan deze ontwikkeling bij de banken bouwden ook de verzekeraars aan waarschuwingssystemen. De Stichting CIS[22] onderhoudt een database met relevante meldingen van incidenten en andere gebeurtenissen zoals claimmeldingen. Het zogenaamde FISH[23] protocol beschrijft vervolgens wie voor welke doeleinden van die bestanden gebruik mag maken. In deze bijdrage wordt verder niet op deze specifieke en nog steeds actuele systemen van de verzekeraars ingegaan.

Systematiek onder IRIS-protocol en onder EVA-protocollen 2002 en 2004 (figuur 1)



van het uitvoeringsbesluit IB 2001.

16. Voor beschrijving zie Berkvens, 'De privacygedragscode voor het bankwezen', *Bank en Effectenbedrijf* 1989/4, p. 21-25.
17. Wet persoonsregistraties (hierna: Wpr), voorganger van de Wet bescherming persoonsgegevens (hierna: Wbp).
18. *Stcrt.* 8944, 25 mei 2011.
19. Brief van de NVB van 26 juni 1990 aan de Minister van Justitie.
20. Goedgekeurd door de toenmalige Registratiekamer op 16 oktober 1995.
21. Art. 9 van de privacygedragscode 1995.
22. http://www.stichtingcis.nl/.
23. Fraude Informatie Systeem Holland. Zie http://www.stichtingcis.nl/bc_upload/FISH%20protocol.pdf.

Overgang Wet persoonsregistraties (Wpr) naar Wet bescherming persoonsgegevens (Wbp)

De inwerkingtreding van de Wbp in 2001 had tot gevolg dat bij de verwerking van strafrechtelijke gegevens een onderscheid diende te worden gemaakt tussen de verwerking van strafrechtelijke gegevens voor eigen gebruik en de verwerking van deze gegevens mede ten behoeve van derden. Hoofdregel van de Wbp is het verbod op de verwerking van strafrechtelijke gegevens van art. 16 Wbp. Op grond van art. 22 lid 2 Wbp en art. 22 lid 4 sub b Wbp mogen deze gegevens toch worden verwerkt als dat nodig is in het kader van een acceptatieproces of de bescherming tegen strafbare feiten. De verwerking omvat ook gebruik en uitwisseling van gegevens binnen concerns. Indien men voornemens is, bijvoorbeeld in het kader van de deelname aan een branchewaarschuwingssysteem, om strafrechtelijke gegevens uit te wisselen met derden buiten het concern gelden de eisen van art. 22 lid 4 sub c Wbp en dient een zogenaamd voorafgaand onderzoek door het Cbp te worden aangevraagd conform de procedure van art. 31 en 32 Wbp. Het IRIS-protocol diende dan ook te worden aangepast.

EVA-protocol 2002

Geleidelijk gingen banken en verzekeraars op het gebied van veiligheid meer samenwerken. De banken, aangesloten bij de Nederlandse Vereniging van Banken (NVB) en de Vereniging van Financieringsondernemingen in Nederland (VFN) en verzekeraars, aangesloten bij het Verbond van Verzekeraars besloten hun samenwerking op het gebied van bestrijding van misbruik van financiële diensten te intensiveren. Een en ander – naast de hiervoor gesignaleerde noodzaak tot aanpassing van het IRIS-protocol aan de Wbp – leidde tot nieuwe samenwerkingsafspraken vastgelegd in het zogenaamde EVA-protocol 2002 waarin de voorwaarden voor opname en gebruik van gegevens zijn vastgelegd.[24] Op 31 juli 2002 gaf het Cbp, na het uitvoeren van een voorafgaand onderzoek, een verklaring omtrent de rechtmatigheid van het EVA-protocol 2002 af.[25] De systematiek zoals onder het IRIS-protocol bleef in grote lijnen ongewijzigd.
Evenals bij de privacygedragscode banken 1995 viel het gebruik van de incidentenregisters buiten de scope van de inmiddels vernieuwde privacygedragscode 2003.[26] Een privacygedragscode waartoe overigens in 2006 ook de leden van de brancheorganisatie Zorgverzekeraars Nederland toetraden met een Addendum Zorgverzekeraars.[27]

Uitbreiding EVA-protocol 2004

Omdat het fenomeen hypotheekfraude sterk in opkomst was ontstond al snel de behoefte aan een aanpassing van het EVA-protocol 2002. Omdat een aantal institutionele beleggers geen deel uitmaakte van de NVB en het Verbond van verzekeraars was namelijk sprake van een hiaat in het systeem. Daarom werd besloten om over te gaan tot een wijziging van het EVA-protocol 2002.[28] Daarbij werden ook de institutionele beleggers toegelaten tot een deel van het systeem. Het Cbp stemde in met de wijziging van het protocol.[29] Ook in het EVA-protocol 2004 bleef de systematiek ongewijzigd: vanuit de incidentenregisters worden per bank de interne verwijsregisters gevuld (IVR). Deze verwijsindices zijn alleen vanuit de front offices van de eigen organisatie benaderbaar.[30] Vanuit de incidentenregisters van de individuele banken wordt tevens het gezamenlijke externe verwijsregister (EVR) gevuld. Dat is benaderbaar voor de front offices van alle financiële instellingen.

Protocol IFI

Omstreeks 2008 besloten banken en verzekeraars een duidelijker scheiding aan te gaan brengen tussen verwerkingen van veiligheidsafdelingen, die op de interne bedrijfsvoering waren gericht, en verwerkingen die gericht waren op samenwerking met andere veiligheidsafdelingen.[31] Daarnaast nam men voor ook de zorgverzekeraars toegang te geven tot het branchewaarschuwingssysteem. In de privacygedragscode 2010 werden de contouren van het vernieuwde Protocol incidentenwaarschuwingssysteem financiële instellingen 2011 (hierna: protocol IFI) al zichtbaar.[32] Evenals onder de eerdere gedragcodes vallen de verwerkingen van persoonsgegevens in de incidentenregisters zelf niet onder de scope van de privacygedragscode 2010.[33] In het protocol IFI zijn de procedures en voorwaarden opgenomen die van toepassing zijn op het vastleggen, gebruiken en uitwisselen van persoonsgegevens in een incidentenregister en in een extern verwijsregister.

4. Protocol IFI

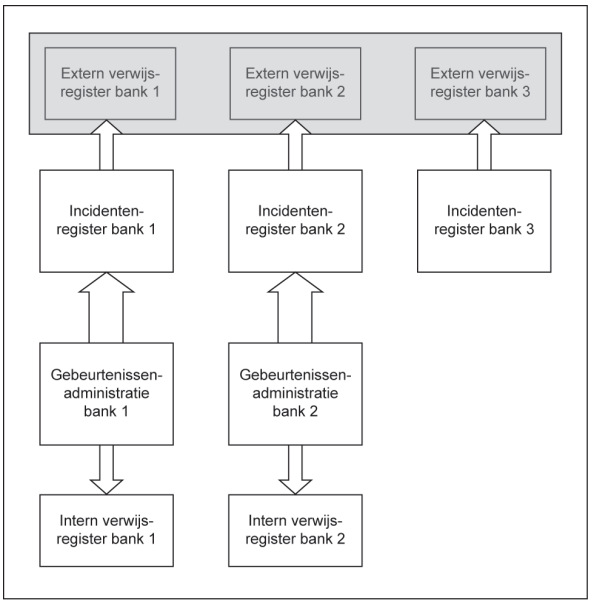
4.1 Het incidentenregister

De kern van het nieuwe incidentenwaarschuwingssysteem financiële instellingen bestaat (nog steeds) uit de incidentenregisters van individuele financiële instellingen. Het incidentenregister valt onder de verantwoordelijkheid van een veiligheidsafdeling. De gegevens die in het incidentenregister worden opgenomen kunnen uit diverse bronnen afkomstig zijn. Ze kunnen afkomstig zijn uit een gebeurtenissenadministratie (zie hierna), de personeelsadministratie of uit de cliëntenregistratie. Ook kunnen ze afkomstig zijn uit externe bronnen zoals internet, kranten of overheidsbronnen. Ten aanzien van opname in het incidentenregister geldt dat bij opname moet worden getoetst aan de doelomschrij-

24. EVA staat voor Externe Verwijs Applicatie. Niet te verwarren met EVR: het aan het incidentenregister gekoppelde Externe Verwijs-Register.
25. Cbp z2002-0945 van 31 juli 2002.
26. Goedgekeurd door het Cbp op 27 januari 2003. Het betreft een geïntegreerde privacygedragscode waar zowel banken als verzekeraars onder vallen.
27. *Stcrt.* 2 mei 2006, nr. 85.
28. Voor tekst zie onder meer de website van NVB: www.nvb.nl.
29. Cbp z2004-0134.
30. Vergelijk advies Cbp 17 juli 2003, z2002-1123 inzake fraudebestrijding binnen conglomeraten.
31. Deze scheiding loopt parallel aan de scheiding in art. 22 Wbp, waar de regels voor intern gebruik minder streng zijn dan die bij de samenwerking met derden.
32. Art. 5 lid 5 van de privacygedragscode 2010.
33. Zie ook mijn bijdrage 'Privacygedragscode financiële instellingen 2010' in *FR* 2010, nr. 5, p. 140.

ving van art. 4.1.1 van het protocol IFI.[34] In het incidentenregister worden door de deelnemende financiële instellingen gegevens opgeslagen die betrekking hebben op dusdanig ernstige zaken dat naar de mening van de betreffende instelling uitwisseling met de veiligheidsafdelingen van andere financiële instellingen mogelijk moet zijn. In verreweg het grootste aantal gevallen zal het daarbij gaan om gegevens die betrekking hebben op strafbare feiten. Ieder individueel incidentenregister is voorzien van een extern verwijsregister. Daar zijn de identificerende NAW-gegevens opgenomen van natuurlijke en rechtspersonen die op een dusdanige wijze zijn betrokken bij ernstige incidenten dat ze naar de mening van de registrerende instelling ook een risico vormen voor andere financiële instellingen. Bij opname in het externe verwijsregister moet worden getoetst aan de eisen van art. 5 lid 2 protocol IFI. Dat betekent dat het moet gaan om ernstige feiten die in voldoende mate vast staan. Bovendien moet voorafgaand aan plaatsing een proportionaliteitsafweging hebben plaats gevonden.
De registrerende financiële instelling heeft ten aanzien van het eigen incidentenregister dus twee beslismomenten. Het moment waarop wordt besloten om incidentgegevens in het incidentenregister op te nemen en het moment waarop wordt besloten om de identificerende gegevens van betrokken natuurlijke of rechtspersonen in het externe verwijsregister op te nemen.

Systematiek onder protocol IFI (figuur 2)



4.2 De gebeurtenissenadministratie

Bij veel financiële instellingen wordt een gebeurtenissenadministratie aangehouden (zie figuur 2). Daarin worden alle gegevens bijgehouden die de aandacht van de betreffende financiële instelling behoeven. Daaronder vallen bijvoorbeeld meldingen van verloren laptops, OFAC-lijsten[35], uitkomsten van screeningsonderzoeken, klachten van klanten over fraude met internetbankieren, ernstige vormen van niet naleven van afspraken of faillissementen. De gebeurtenissenadministratie is een vergaarbak van gegevens en vormt het 'geheugen' van de financiële instelling. De gebeurtenissenadministratie zal bij sommige financiële instellingen vallen onder de verantwoordelijkheid van de veiligheidsafdeling. Bij sommige financiële instellingen zal de gebeurtenissenadministratie verdeeld zijn over meerdere afdelingen. Ook kan het zijn dat categorieën gebeurtenissen zijn ondergebracht in de reguliere cliëntenregistratie of personeelsregistratie. Sommige financiële instellingen onderhouden geen gebeurtenissenadministratie. De financiële instellingen die een gebeurtenissenadministratie aanhouden hebben er bewust voor gekozen deze administratie een intern karakter te geven. Derhalve hoeft voor een dergelijke gebeurtenissenadministratie geen voorafgaand onderzoek te worden aangevraagd.
De gebeurtenissenadministratie kan gegevens omtrent strafbare feiten bevatten. Die gegevens mogen als hiervoor in onderdeel 3 gesteld op grond van art. 22 Wbp niet worden gedeeld met de veiligheidsafdelingen van andere financiële instellingen. Daarvoor is het immers vanwege art. 22 lid 4 sub Wbp vereist dat een voorafgaand onderzoek heeft plaatsgevonden. De gebeurtenissenadministratie valt vanwege haar interne karakter niet onder dit verplichte voorafgaand onderzoek.
Indien strafrechtelijke gegevens worden vastgelegd in de gebeurtenissenadministratie, gelden de regels van art. 5 lid 5 en 6 lid 2 van de privacygedragscode 2010. De vastlegging moet vallen binnen de eisen die art. 22 Wbp stelt. Uitwisseling met groepsonderdelen is dan toegestaan onder art. 22 lid 4 sub b Wbp.

4.3 Het externe verwijsregister (EVR)

Het protocol IFI besteedt de nodige aandacht aan de opname van personen in het externe verwijsregister wegens betrokkenheid bij strafbare feiten. Art. 5 lid 2 sub 1(b) van het protocol IFI bepaalt dat ingeval van strafbare feiten in principe aangifte wordt gedaan of een klacht wordt ingediend. In het annex bij het protocol worden enkele voorbeelden genoemd van gevallen waarin van deze hoofdregel mag worden afgeweken.
Zodra de identificerende (NAW) gegevens van een natuurlijke of rechtspersoon zijn opgenomen in het externe verwijsregister kunnen die gegevens worden geraadpleegd door toetsende front office medewerkers van zowel de registrerende instelling als van andere aan het protocol IFI deelnemende financiële instellingen.

4.4 Het interne verwijsregister (IVR)

Per financiële instelling kan een intern verwijsregister worden aangehouden. Dat bevat identificerende (NAW) gegevens van natuurlijke of rechtspersonen die een zeker risico vormen voor de betreffende financiële instelling. Bij financiële instellingen met een onder een veiligheidsafdeling ressorterende gebeurtenissenregistratie zal het veelal de

34. De doelomschrijving zelf is in het kader van het voorafgaand onderzoek door het Cbp al als rechtmatig beoordeeld.
35. Office of foreign assets control: een Amerikaanse sanctielijst met (rechts)personen waarvoor wettelijke beperkingen ten aanzien van het financiële verkeer gelden.

veiligheidsafdeling zijn die aan de hand van vooraf bepaalde criteria kan besluiten om de identificerende gegevens van natuurlijke of rechtspersonen op te nemen in het interne verwijsregister. Anders dan het externe verwijsregister kunnen de gegevens uit het interne verwijsregister uitsluitend worden geraadpleegd door de front office medewerkers van de registrerende financiële instelling. Het interne verwijsregister valt evenals de gebeurtenissenadministratie onder de privacygedragscode 2010. Zie daarover de toelichting op de gedragscode 2010.[36] Dat betekent dat de verwijsgegevens alleen mogen worden gebruikt ter bestrijding van (mogelijke) fraude tegen de eigen financiële instelling.

4.5 Verwijdering uit het incidentenregister of externe verwijsregister

Als een persoon niet meer voldoet aan de eisen van art. 5 lid 2 protocol IFI, dienen zijn gegevens te worden verwijderd uit het externe verwijsregister. De gegevens mogen dan nog wel in het incidentenregister blijven en kunnen ook worden uitgewisseld met veiligheidsafdelingen van andere financiële instellingen. Zodra betrokkene niet meer valt onder de doelomschrijving van het incidentenregister, dienen zijn gegevens ook daar te worden verwijderd. De gegevens kunnen dan nog wel worden vastgehouden in de gebeurtenissenadministratie van de bank. Maar de gegevens mogen dan - indien sprake is van gegevens omtrent strafbare feiten - niet meer met veiligheidsafdelingen van andere financiële afdelingen worden uitgewisseld. De gebeurtenissenadministratie voldoet immers niet aan de eisen van art. 22 lid 4 sub c van de Wbp.

4.6 Positie van geregistreerde personen

Het protocol IFI bevat een aantal voorschriften ten aanzien van de rechten van geregistreerde personen. Het gaat daarbij vooral om het recht op mededeling van opname, het recht op inzage en het recht op correctie. Hoofdregel is dat de betrokkene uiterlijk op het moment van eerste verstrekking wordt ingelicht over de opname in het incidentenregister respectievelijk EVR en de relevante achtergronden van die opname. Tenzij sprake is van toepasselijkheid van uitzonderingssituaties zoals voorzien in art. 43 Wbp[37], de Wwft[38] of het Wetboek van Strafrecht/Strafvordering.[39] De rechten op inzage en correctie worden eveneens conform de Wbp geregeld. Ten aanzien van het inzagerecht gelden evenals bij de mededelingsplicht de beperkingen bij uitzonderingssituaties zoals voorzien in art. 43 Wbp, de Wwft of het Wetboek van Strafrecht/Strafvordering.

5. De wet bescherming persoonsgegevens en waarschuwingssystemen

5.1 Algemeen

Hierna wordt eerst ingegaan op de algemene eisen die de Wbp stelt aan een waarschuwingssysteem. Vervolgens wordt in onderdeel 6 nader ingegaan op het uitoefenen van inzage- en correctierecht. Onder de Wbp moeten waarschuwingssystemen als IFI voldoen aan diverse eisen. Op de eerste plaats moeten worden bezien of de verwerking zelf voldoet aan de eisen van de Wbp. Het gaat daarbij om de grondslag voor de verwerking en de onderbouwing van de verwerking van strafrechtelijke gegevens. Op grond van art. 6 en 7 Wbp moet sprake zijn van verwerking op behoorlijke en zorgvuldige wijze van gegevens die voor een gerechtvaardigd doel worden verzameld.

5.2 Verwerkingsgrondslag

Art. 8 Wbp vereist dat sprake is van aanwezigheid van één of meer van de zes in dat artikel genoemde verwerkingsgrondslagen. Er komen er drie in aanmerking. De eerste belangrijke grondslag vormt de behartiging van het gerechtvaardigde belang van de bank (en andere financiële instellingen) dat moet worden afgewogen tegen de belangen en fundamentele vrijheden van de betrokken personen van wie gegevens worden verwerkt.[40] Op de tweede plaats kan worden gewezen op de grondslag van het bestaan van een wettelijke verplichting (met name de hiervoor genoemde bepalingen uit Wft en Wwft).[41] Op de derde plaats kan ook een grondslag worden gevonden in het feit dat verwerking plaats vindt in het kader van het afsluiten van een overeenkomst.[42] De bank moet immers als onderdeel van de acceptatieprocedure nagaan of er geen blokkerende indicaties bestaan. Naast de grondslagen van art. 8 Wbp kan ook rechtstreeks worden verwezen naar art. 22 Wbp, dat meebrengt dat banken strafrechtelijke gegevens mogen verwerken indien sprake is van acceptatie van klanten of de bescherming van de bank[43] of van derden.[44]

5.3 Verenigbaarheidstoets

Voor zover in het kader van het waarschuwingssysteem sprake is van hergebruik van bijvoorbeeld cliëntgegevens voor een ander dan het verzameldoel (niet doelconform gebruik) moet bovendien op grond van art. 9 Wbp worden afgewogen of het nieuwe verwerkingsdoel verenigbaar is met het oorspronkelijke verzameldoel.[45] In de Privacy gedragscode 2010 wordt echter al uitgegaan van een ruim verzameldoel dat ook gebruik van gegevens in het kader van waarschuwingssystemen omvat.[46] Ook de Algemene bankvoorwaarden voorzien in een vergelijkbare bepaling.[47] Derhalve mag veelal worden aangenomen dat sprake zal zijn van doelconform gebruik en kan de afweging van art. 9 achterwege blijven.[48]

---

36. Toelichting bij art. 6 lid 2 van de privacygedragscode 2010.
37. Het bestaan van opsporingsbelangen of andere zwaarwegende belangen die zich tegen mededeling verzetten.
38. Bijvoorbeeld art. 23 Wwft in geval van MOT-meldingen.
39. Art. 184 Sr. (hinderen van strafrechtelijk onderzoek) en 126bb lid 5 Sv.
40. Art. 8f Wbp.
41. Art. 8c Wbp.
42. Art. 8b Wbp.
43. Art. 22 lid 2 sub a en b. Wbp en (ten aanzien van groepsonderdelen) art. 22 lid 4 sub b Wbp.
44. Art. 22 lid 4 sub c. Wbp.
45. Art. 9 Wbp.
46. Art. 5 lid 5 van de privacygedragscode 2010.
47. Art. 10 van de ABV 2010.
48. Als toch sprake zou zijn van niet doelconform gebruik en dus de afweging van art. 9 Wbp toch gemaakt zou moeten

5.4 Voorafgaand onderzoek

Als hiervoor al aangegeven: op grond van art. 16 van de Wbp is de verwerking van strafrechtelijke gegevens verboden. Echter: op grond van art. 22 lid 1 en 2 is verwerking van strafrechtelijke gegevens voor interne beveiligingsdoeleinden toegestaan. Daaronder vallen ook verwerkingen voor groepsonderdelen.[49] Verwerking ten behoeve van derden is in het geval van banken en verzekeraars slechts toegestaan onder voorwaarde van waarborgen en een verklaring omtrent de rechtmatigheid, afgegeven door het College bescherming persoonsgegevens.[50] Dat houdt in dat de financiële instellingen die deelnemen aan het waarschuwingssysteem, ieder afzonderlijk eenmalig[51] een zogenaamd voorafgaand onderzoek dienen aan te vragen ten aanzien van hun incidentenregister.[52]
De Nederlandse Vereniging van Banken en het Verbond van Verzekeraars kwamen in 2002 met het Cbp een vereenvoudigde procedure voor het voorafgaand onderzoek overeen.[53] Door één van de deelnemers werd een voorafgaand onderzoek aangevraagd. Het Cbp stelde naar aanleiding van het voorafgaand onderzoek een nader onderzoek in waarbij de waarborgen van het EVA protocol 2002 grondig onder de loep werden genomen. Dit leidde voor die deelnemer tot een verklaring omtrent de rechtmatigheid omtrent de uitwisseling van gegevens op basis van het EVA-protocol 2002.[54] Voor de andere financiële instellingen kon vervolgens een verkorte procedure worden gevolgd: na aanvraag van een voorafgaand onderzoek voor het gebruik van het incidentenregister in samenhang met het EVA-protocol 2002 was een nader onderzoek niet meer nodig. Inmiddels heeft ook de rechter zich uitgesproken over het EVA-protocol als toetsingskader. Het Hof Amsterdam overwoog als volgt:

> 3.6 Gelet op het onder 3.5 overwogene deelt het hof de visie van SNS dat het Protocol valt te beschouwen als een regeling die voldoende waarborgen biedt voor een verwerking van persoonsgegevens zoals de WBP die voorschrijft. De grief slaagt mitsdien.[55]

5.5 Voorafgaand onderzoek en gebeurtenissenadministratie

Onder het nieuwe protocol IFI valt de gebeurtenissenadministratie buiten de procedure van het voorafgaand onderzoek nu de eventuele verwerking van gegevens betreffende strafbare feiten valt onder het regime van art. 22 lid 4 sub b Wbp. Het voorafgaand onderzoek geldt alleen het incidentenregister (althans voor zover al niet eerder aangemeld) omdat de daarin opgenomen gegevens ook uitgewisseld kunnen worden met andere financiële instellingen.

6. De rechten van de betrokkene

6.1 Het inzagerecht

Algemeen

Personen van wie gegevens worden verwerkt, moeten daarvan actief op de hoogte worden gesteld.[56] Zij hebben daarnaast een recht op inzage in hen betreffende gegevens.[57] Het recht op inzage heeft een absoluut karakter (grondrecht). Dat betekent onder meer dat de betrokkene niet verplicht is om een verzoek om inzage te motiveren.[58] Het recht op inzage wordt in de Wbp op een aantal manieren begrensd. Bij de incidentenregisters kan het gaan om gegevens waarvan de vrijgave ernstige negatieve gevolgen kan hebben voor banken of voor andere personen. Hierna wordt daarom kort ingegaan op enkele gevallen waarin het van belang kan zijn (en ook mogelijk is) de reikwijdte van het inzagerecht te beperken.[59]

Wbp van toepassing?

De eerste vraag is of de Wbp van toepassing is. Het verzoek om inzage moet betrekking hebben op de verwerking van persoonsgegevens. De Wbp is immers alleen van toepassing op persoonsgegevens. Ten aanzien van de verwerking van gegevens omtrent rechtspersonen geldt de Wbp niet.[60] Een andere begrenzing heeft betrekking op enkelvoudige dossiers.[61] Als sprake is van een niet geautomatiseerd dossier dat geen deel uitmaakt van een systematische verzameling van dossiers, dan is de Wbp niet van toepassing.[62] Hiervan zal bij incidentenregisters overigens niet snel sprake zijn omdat er sprake is van geautomatiseerde en gestructureerde verwerkingen.

---

worden brengt art. 43 Wbp (onderdelen b en e) met zich mee dat in geval van zwaarwegende opsporingsbelangen of zwaarwegende belangen van banken of derden de afweging van art. 9 achterwege kan blijven.

49. Art. 22 lid 4 sub b Wbp spreekt over rechtspersonen die in dezelfde groep in de zin van art. 2:24b BW zijn verbonden.
50. Art. 22 lid 4 sub c Wbp.
51. Eenmalig: nadat voor een incidentenregister een voorafgaand onderzoek is aangevraagd hoeft niet steeds bij protocol-aanpassingen opnieuw een voorafgaand onderzoek te worden aangevraagd.
52. Art. 31 Wbp.
53. Vgl. *Kamerstukken II* 2008/09, 31 841, nr. 2, onderdeel E (Actalwetje).
54. Cbp z2002-0495, 31 juli 2002.
55. Hof Amsterdam 18 januari 2007, *LJN* BA5933, R.O. 3.5 en 3.6. Zie bijvoorbeeld ook Rb. Alkmaar 4 november 2010, *LJN* BP5613.
56. Art. 33 en 34 Wbp.
57. Art. 35 Wbp.
58. *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 157-158.
59. Voor een uitgebreide behandeling verwijs ik naar mijn bijdrage 'De beperkingen van het inzagerecht' in het *FR* van oktober 2009.
60. Zie definitie van persoonsgegeven in art. 1 sub a Wbp.
61. Art. 2 lid 1 Wbp.
62. Bijvoorbeeld in Rb. Utrecht, 17 december 2010, *LJN* BO5230 wordt ten aanzien van een klachtdossier bepaald dat de Wbp niet van toepassing is (RO 5.4). Besproken door N. Wolters Ruckert in 'De begrenzing van het privacyrechtelijk inzagerecht; enkele recente uitspraken', *Juridisch up to date* 2011, nr. 5. Zie ook bespreking door M. Jansen, 'De grenzen van het privacyrechtelijk inzagerecht', *P&I* 2011/2, p. 83-85.
63. HR 29 juni 2007 *LJN* AZ4663 (Dexia-1); HR 29 juni 2007

Persoonlijke aantekeningen

Bij verwerkingen van persoonsgegevens die wèl onder de Wbp vallen, zijn enkele uitzonderingen op het inzagerecht mogelijk. Dat geldt bijvoorbeeld voor persoonlijke werkaantekeningen. Zowel op zichzelf staande aantekeningen als aantekeningen die op documenten zijn aangebracht.[63] Bij het voldoen aan verzoek om inzage zou schoning van documenten een optie kunnen zijn.[64] In de medische sector spelen regelmatig zaken over dit onderwerp. De uitkomsten zijn niet altijd consistent.[65]

Opsporingsbelangen

Op grond van art. 43 sub b Wbp kan het recht op inzage worden geweigerd als sprake is van een noodzaak van weigering in het belang van de opsporing, voorkoming en vervolging van strafbare feiten. Hoewel banken geen onderdeel uitmaken van het openbaar ministerie of de politie wordt toch van hen verwacht dat zij zich inzetten op het gebied van opsporing van strafbare feiten. Dat vloeit onder meer voort uit de Wwft en de Wft. Ook art. 22 Wbp impliceert dat banken strafrechtelijke gegevens moeten kunnen verwerken ter voorkoming van tegen hen gerichte criminaliteit. Zowel het doen van mededeling van opname in een verwerking als het geven van inzage kan strategische informatie opleveren aan criminelen en daardoor het onderzoek hinderen.[66]

Belangen van derden

Art. 43 sub e Wbp biedt de mogelijkheid van weigering van inzage voor zover noodzakelijk voor de behartiging van de belangen van derden. Die derden kunnen zowel personen of rechtspersonen buiten de organisatie van de bank zijn als ook de bank zelf. Bij partijen buiten de bank kan bijvoorbeeld gedacht worden aan bronnen die gevaar lopen op het moment dat hun gegevens in handen van criminelen komen.

Belangen van de bank zelf

Ook de bank zelf komt een weigeringsgrond toe op basis van art. 43 sub e Wbp. Tot de rechten van financiële instellingen hoort een zeker recht op 'privacy'. Zowel art. 10 van de Grondwet[67] als art. 8 EVRM[68] strekken zich uit over rechtspersonen. Het gaat onder meer om de vrijheid van ongestoorde gedachtewisseling en het recht om zich verdedigen tegen derden. In enkele uitspraken heeft de rechter zich op het standpunt gesteld dat personen binnen organisaties het recht hebben in vrijheid hun gedachten en opvattingen te kunnen uiten. Dat geldt ook voor derden die in vertrouwen mededelingen doen.[69]

Vorm inzage

Een laatste vraag betreft de wijze waarop aan het inzagerecht moet worden voldaan. De Wbp verplicht tot het verschaffen van een volledig overzicht van de persoonsgegevens die worden verwerkt. De wet spreekt niet over een recht op afschrift. In de Dexia-uitspraken oordeelt de Hoge Raad echter in het verlengde van een gelijkluidend advies van het Cbp[70] dat het soms onvermijdelijk is om inzage te verschaffen in de vorm van een kopie.[71]

6.2 Correctierecht algemeen

Algemeen

Personen waarvan gegevens worden verwerkt in het kader van het tegengaan van onoorbaar gebruik van het financiële stelsel, kunnen hinder ondervinden van die situatie. Zij kunnen met een beroep op de Wbp proberen hun gegevens te laten corrigeren, aanvullen, verwijderen of afschermen.
Het correctierecht wordt geregeld in art. 36 van de Wbp. Evenals onder de Wpr kan het correctierecht pas worden uitgeoefend na een voorafgaande inzage in de betreffende gegevens.[72] De situatie kan zich voordoen dat een voorafgaand verzoek om inzage is geweigerd. Bijvoorbeeld op grond van art. 43 Wbp. Verdedigbaar is dat een dergelijke weigering doorwerkt in de ontvankelijkheid van een correctieverzoek. Om voor correctie in aanmerking te komen zal moeten vast staan dat het gaat om gegevens die 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.[73]
Als het door de manier van opslag onmogelijk is de gegevens te wijzigen, dienen maatregelen te worden getroffen om de gebruiker van de gegevens daarover te informeren.[74] Ten slotte dient de bank eventuele eerdere ontvangers van gewijzigde gegevens daarover te informeren tenzij dat onmogelijk blijkt of een onevenredige inspanning kost.[75] Verantwoordelijke informeert desgevraagd betrokkene over deze eerdere ontvangers.

LJN AZ4664 (Dexia-2). Zie R.O 3:14.

64. Zie laatste 2 zinnen in R.O. 3:6 van Dexia-1 en Dexia-2.
65. Zie A. Wilken, 'Artikel 35 Wbp: Wel of geen inzage in de dossiers van de medisch adviseur van de verzekeraar', *Tijdschrift voor gezondheidsrecht* 2011, nr. 3.
66. Ook de mededeling van art. 33 en 34 Wbp kan met een beroep op art. 43 Wbp in deze gevallen achterwege blijven.
67. *Kamerstukken II* 1976/77, 13 872, nr. 7, p. 35.
68. Arrest Colas Est, EHRM, 16 april 2002.
69. Zie bijvoorbeeld Rb. 's-Gravenhage, 27 december 2005, gepubliceerd in *Uitsprakenbundel Wet bescherming persoonsgegevens*, van Dijk e.a. (red.), Den Haag, 2009 onder nr. 43.2; zie ook Rb Utrecht 17 november 2010, *LJN* BO5222 ,besproken door A. Wilken, 'Artikel 35 Wbp: Wel of geen inzage in de dossiers van de medisch adviseur van de verzekeraar', *Tijdschrift voor gezondheidsrecht* 2011, nr. 3; zie ook, Rb Utrecht 17 oktober 2010, *LJN* BO5227 (meldingssysteem ziekenhuis).
70. Cbp, z2003-1617, 3 september 2004.
71. HR 29 juni 06-2007 *LJN* AZ4663 (Dexia-1); HR 29 juni 2007 *LJN* AZ4664 (Dexia-2). Zie R.O 3:14; zie R.O. 6. Anders: Afdeling bestuursrechtspraak, Raad van State 29 november 2006 *LJN* AZ3237 (onderscheid gegevens en gegevensdrager).
72. Art. 36 lid 1 Wbp.
73. Art. 36 lid 1 Wbp.
74. Art. 36 lid 4 Wbp.
75. Art. 38 Wbp.
76. Voor een meer gedetailleerde beschrijving zie onderdeel 11

Reikwijdte correctieverzoek

Een verzoek tot correctie kan betrekking hebben op de gebeurtenissenadministratie, het incidentenregister, het aan de gebeurtenissenadministratie gekoppelde interne verwijsregister IVR en het aan het incidentenregister gekoppelde externe verwijsregister EVR. Als eerder aangegeven vormt het incidentenregister de verzameling van gegevens die wordt beheerd door de veiligheidsafdeling van de financiële instelling. De inrichting van de gebeurtenissenadministratie kan sterk verschillen per financiële instelling. Een verzoek om verwijdering van gegevens uit alle vier genoemde componenten hoeft niet voor iedere component op dezelfde wijze uit te pakken.

Corrigeren, verwijderen of vernietigen

Verzoeken om correctie kunnen gericht zijn op aanpassing van vastgelegde gegevens, verwijdering van gegevens of vernietiging van gegevens. Verwijdering van gegevens uit de EVR hoeft niet te betekenen dat ook de gegevens uit het onderliggende incidentenregister moeten worden verwijderd. Ze kunnen immers nog steeds van belang zijn voor onderzoek naar strafbare feiten. Ook verwijdering uit het incidentenregister hoeft niet te leiden tot verwijdering uit bijvoorbeeld de onderliggende gebeurtenissenadministratie. Gevolg van verwijdering uit het incidentenregister is echter wel dat de gegevens niet meer mogen worden uitgewisseld met andere financiële instellingen. Ook verwijdering uit een IVR betekent niet automatisch dat ook verwijdering uit de gebeurtenissenadministratie noodzakelijk is. Die bestaat immers voor een groot deel uit gegevens die onder een wettelijke bewaarplicht vallen of noodzakelijk zijn voor het kunnen leveren van bewijs en het afleggen van verantwoording.

6.3 Klachtenafhandeling inzake inzage en correctie

Niet altijd zal een verzoek om inzage of correctie door de bank worden gehonoreerd. De betrokkene die daar geen genoegen mee neemt kan op verschillende manieren tegen een voor hem negatieve beslissing in het geweer komen.[76] Hij kan bij het klachtenloket van de betreffende bank een klacht indienen. Indien die niet tot zijn tevredenheid wordt afgehandeld, kan hij zich vervolgens wenden tot het KIFID. Het reglement van het KIFID geldt in beginsel slechts voor klachten van klanten die consument zijn. Het reglement van het KIFID voorziet echter in de mogelijkheid voor niet-klanten en ondernemers om een privacygeschil aanhangig te maken. Het KIFID geldt als een erkende geschillenprocedure in de zin van de Wbp.[77]

Daarnaast kan de betrokkene het Cbp verzoeken te bemiddelen. Hij loopt dan wel de kans dat het College uit opportuniteitsoverwegingen eerst zal verwijzen naar de bestaande geschillenprocedure van de betreffende bank.

Op de derde plaats kan de betrokkene een beroep doen op de verzoekschriftprocedure van art. 46 Wbp. Hij dient dan een verzoekschrift in bij de rechtbank strekkende tot inzage in of correctie van zijn gegevens.

6.4 Rechtspraak inzake correctieverzoeken onder EVA-protocol 2002 en 2004

Gedurende de afgelopen jaren hebben diverse rechters zich gebogen over correctieverzoeken. Daarbij was steeds het EVA-protocol aan de orde. Over het protocol IFI bestaat nog geen jurisprudentie. Toch kan de EVA-jurisprudentie van betekenis zijn voor de toepassing van het recht op inzage en correctie met betrekking tot de gebeurtenissenadministratie, de incidentenregisters en het interne en externe verwijsregister na de invoering van het protocol IFI. Hierna wordt naast enkele meer algemene uitspraken aandacht besteed aan jurisprudentie betreffende de incidentenregisters. De jurisprudentie heeft vooral betrekking op het EVA-protocol 2004.

Een eerste meer algemene vraag is of een correctieverzoek zich leent voor behandeling in de procedure van art. 46 Wbp. Daarbij kan de vraag aan de orde komen of de feiten waarop het verzoek is gebaseerd in voldoende mate vast staan. Indien dat niet het geval is, kan de rechtbank besluiten om de verzoeker te verwijzen naar een bodemprocedure. In dat verband zij verwezen naar een tweetal uitspraken. Het Gerechtshof 's-Hertogenbosch oordeelde (bij een verzoek tot correctie van gegevens in een medisch dossier) dat 'volgens de letterlijke tekst van art. 36 Wbp de mogelijkheid bestaat om onjuiste persoonsgegevens te doen verwijderen, maar daarbij gaat het alleen om gegevens waarvan op eenvoudige en objectieve wijze de onjuistheid valt vast te stellen (bijvoorbeeld niet betwiste feiten)'.[78] In een beschikking (met betrekking tot correctie van gegevens in een incidentenregister) van de rechtbank Breda valt te lezen 'dat een verzoekschriftprocedure geen ruimte laat voor een rechtmatigheidsbeoordeling, maar dat slechts sprake kan zijn van een beoordeling op grond van de in art. 35 Wbp en art. 10 van het Protocol genoemde criteria'.[79]

Opname onder het EVA-protocol 2002 of 2004 in een incidentenregister betekende niet automatisch opname in het IVR of het EVR. Opname in het IVR was pas toegestaan als aan de eisen van art. 5 lid 2 van het EVA-protocol 2002 of 2004 werd voldaan. Opname in het EVR was alleen toegestaan als aan zwaardere eisen van art. 6 lid 2 van het EVA-protocol 2002 of 2004 werd voldaan. Dat hield verband met de grotere impact van opname van gegevens in het EVR. Bij verzoeken om correctie werd daar door rechters ook rekening mee gehouden. Zo oordeelde de rechtbank Utrecht dat een opname in het EVR onterecht was maar dat de opname in het IVR toelaatbaar was.[80] In een recente zaak oordeelde de Rechtbank Alkmaar dat de vastgestelde feiten voldoende aanleiding vormden om opname in het IVR te rechtvaardigen. Opname werd bovendien proportioneel geoordeeld gezien het feit dat alleen sprake was van opname in het IVR

van de toelichting op de privacygedragscode 2010. Zie ook art. 10 van het protocol IFI.

77. Art. 47 lid 1 Wbp.
78. Hof 's-Hertogenbosch, 27 mei 2009, *LJN* BI6357. Zie R.O. 3.2.4.
79. Rb. Breda 17-november 2008, zaaknummer / rekestnummer 187083 /HA RK 08-43. Zie R.O. 3.4.
80. Rb. Utrecht 9-december 2009, *LJN* BK5979.
81. Rb. Alkmaar 4 november 2010, *LJN* BP5613.

en betrokkene nog elders terecht kon voor financiële diensten.[81,82]

Opname in het EVR vereiste enerzijds dat sprake moest zijn van voldoende ernstige feiten. Anderzijds moest, ook in geval van ernstige feiten, een proportionaliteitsafweging plaats vinden. Ten aanzien van de proportionaliteitseis oordeelde de rechtbank Utrecht dat in de betreffende zaak geen juiste proportionaliteitsafweging had plaats gevonden (er was in onvoldoende mate vastgesteld dat sprake was van fraude). Reden om opname in het EVR ongedaan te laten maken.[83]

In een andere zaak overwoog de rechter in het kader van de proportionaliteit dat opname in een incidentenregister niet automatisch betekent dat men geen betaalrekening kan krijgen.[84] Daarbij zij aangetekend dat niet alle financiële instellingen zijn aangesloten bij het EVA-protocol (en thans het protocol IFI). Bij niet aangesloten instellingen heeft een opname in EVR dus niet tot gevolg dat de betrokkene wordt gesignaleerd en het risico loopt afgewezen te worden.

Recent overwoog de Rechtbank Alkmaar dat opname in het EVR terecht was en dat de proportionaliteitsafweging op correcte wijze had plaats gevonden.[85] Daarbij werd de mogelijkheid van het openen van een rekening onder het Convenant basisbankdiensten meegewogen.[86] Veelal zal opname in het EVR verband houden met strafbare feiten.[87] In een zaak in 2007 oordeelde het Hof Amsterdam dat opname van gegevens in het incidentenregister, IVR en EVR ongedaan moest worden gemaakt. Daarbij speelde een rol dat na aangifte geen vervolging had plaats gevonden.[88] Het enkele doen van aangifte was naar de mening van het Hof Amsterdam niet voldoende reden om een registratie te rechtvaardigen.[89] De Hoge Raad oordeelde in 2009 echter dat voor het opnemen van strafrechtelijke persoonsgegevens het niet noodzakelijk is dat er sprake is van een veroordeling door de strafrechter. Naar de mening van de Hoge Raad heeft het Hof terecht onder strafrechtelijke persoonsgegevens verstaan ‘zodanige concrete feiten en omstandigheden dat zij een als strafbaar feit te kwalificeren bewezenverklaring - in de zin van art. 350 Sv - kunnen dragen’. Als maatstaf geldt ‘of de gedragingen een zwaardere verdenking dan een redelijk vermoeden van schuld opleveren, in die zin dat de te verwerken strafrechtelijke persoonsgegevens in voldoende mate moeten vaststaan.’[90] In een vonnis van de rechtbank Rotterdam wordt deze afweging letterlijk en onder verwijzing naar de uitspraak van de Hoge Raad overgenomen. Daarbij wordt nog opgemerkt: ‘Het feit dat (tot op heden) geen strafrechtelijke veroordeling uit de door gedaagde gedane aangifte van oplichting en valsheid in geschrifte is voortgekomen, doet hier niet aan af.’[91] In een andere recentere zaak oordeelde het Hof Amsterdam dat bij de vastlegging van gegevens was voldaan aan de eisen van de art. 5.2 en 6.2 van het protocol. Daar deed niet aan af dat betrokkene uiteindelijk niet strafrechtelijk vervolgd werd.[92]

Een vraag is of verwijdering van gegevens uit een verwijsregister ook zou moeten inhouden dat de gegevens verwijderd moeten worden uit het onderliggende incidentenregister. In een geval oordeelde de rechter dat bij afwezigheid van een onderbouwd belang de gegevens ook dienden te worden verwijderd uit het incidentenregister.[93] De bank had hier nagelaten uit te leggen wat het resterende belang nog was nu de gegevens uit het IVR en het EVR waren verwijderd.

Een verzoek om verwijdering van gegevens betekent niet automatisch dat de betreffende gegevens ook moeten worden vernietigd. Verwijderen van gegevens kan met zich meebrengen dat de gegevens worden overgebracht naar een verwerking met een andere doelomschrijving. Dat kan bijvoorbeeld een archiefbestemming zijn die tot doel heeft om naderhand nog verantwoording af te kunnen leggen of in een geschil bewijs te kunnen leveren.[94,95]

7. Conclusie

Het protocol IFI zal gefaseerd worden ingevoerd. De overgang van EVA naar IFI zal voor de uitoefening van het inzage- en correctierecht met betrekking tot het incidentenregister en het EVR vermoedelijk geen grote gevolgen hebben. Uitspraken van de rechter onder het EVA-protocol 2002 en 2004 behouden naar mijn mening hun bruikbaarheid. Dat geldt ook ten aanzien van de vraag of financiële instellingen maatregelen mogen treffen die het mogelijk maken om risico-personen te signaleren via een interne verwijsindex.

---

82. Zie ook Rb. ’s Gravenhage 28 april 2011, *LJN* BQ6061.
83. Rb. Utrecht 9 december 2009, *LJN* BK5979, zie RO 4.34. Zie ook Rb. Utrecht 25 maart 2011, *LJN* BP9270, RO 4.7 (kort geding vastgoed fraudezaak) [over deze uitspraak zijn Kamervragen gesteld: KVR 2010/2011 II nr. 2011Z08779].
84. Rb. Amsterdam, 3 april 2008, zaaknummer/rolnummer: 391613 / KG ZA 08-324.
85. Rb. Alkmaar 25 november 2010, *LJN* BP5621.
86. Vindplaats: http://www.nvb.nl/index.php?p=20815.
87. Onder dat begrip vallen geen bestuursrechtelijke overtredingen die bestuursrechtelijk worden gehandhaafd. Vergelijk de discussie in het kader van de aanpassing van de Wet BIBOB. Zie *Kamerstukken II* 2010/11, 32 676, nr. 3 p. 12.
88. Hof Amsterdam 18 januari 2007, *LJN* BA5933.
89. Hof Amsterdam 12 januari 2006, *LJN* AV8245.
90. HR 29 mei 2009, *LJN* BH4720 (met conclusie Verkade). Zie R.O. 4.4.
91. Rb. Rotterdam 18 mei 2010, *LJN* BM8653. R.O. 4.4.1.
92. Hof Amsterdam 12 oktober 2010, *LJN* BO0073.
93. Hof Amsterdam 18 januari 2007, *LJN* BA5933. Zie R.O. 3.12.
94. Hof ‘s-Hertogenbosch, 27 mei 2009, *LJN* BI6357. Zie R.O. 3.2.5.
95. Vgl. Rb. ‘s Gravenhage 4 mei 2011, *LJN* BQ6062: bewaren van gegevens die nog een functie vervullen in niet verjaarde rechtsvorderingen (medische kwestie).