VERBOND VAN VERZEKERAARS

(Zelf)evaluatie Gedragscode Verwerking Persoonsgegevens Financiële Instellingen

Indien persoonsgegevens worden verwerkt, dient met name voldaan te worden aan de Wet bescherming persoonsgegevens (Wbp) en aan de Gedragscode Verwerking Persoonsgegevens Financiële Instellingen (Gedragscode) van de Nederlandse Vereniging van Banken en het Verbond van Verzekeraars. U dient periodiek te evalueren of u de Wbp en de Gedragscode naleeft. Ter ondersteuning bij deze evaluatie heeft het Verbond een *Model Zelfevaluatie* opgesteld.

Het Model Zelfevaluatie dient als een hulpmiddel bij het uitvoeren van de (zelf)evaluatie. Het overzicht is niet uitputtend en dient door de verzekeraar verder te worden aangevuld en aangepast aan de eigen situatie binnen het bedrijf.

Toelichting bij het gebruik van het Model Zelfevaluatie

Het Model bestaat uit 8 hoofdstukken waarin 8 normen, gebaseerd op de Gedragscode, zijn opgenomen. Na de norm volgt een overzicht van de algemene wettelijke voorschriften, de uitwerking van deze voorschriften gericht op de verzekeraar, een toelichting daarop en de vindplaats van relevante artikelen in wetgeving en zelfregulering van het Verbond. Hoe vaak u de evaluatie uitvoert, bepaalt u zelf. Wel dient u doorlopend aan de regelgeving te voldoen. Een jaarlijkse evaluatie is dan ook aan te raden.

Voor verwijzingen naar eerder verstrekte informatie van het Verbond van Verzekeraars kunt u terecht op www.verzekeraars.nl.

Hoofdstuk 1 Melding

Uw organisatie moet maatregelen en procedures hebben geïmplementeerd voor het melden van verwerkingen van persoonsgegevens, met stappen vanaf het voornemen om persoonsgegevens te gaan verwerken tot en met het melden van de verwerking bij het College Bescherming Persoonsgegevens (CBP). De verantwoordelijke is de rechtspersoon die formeel-juridisch aansprakelijk kan worden gesteld wanneer de verwerking van persoonsgegevens in strijd met wet- en regelgeving plaatsvindt.

Volgnr.	Voorschrift	Uitwerking bij verzekeraar	Toelichting	Vindplaats in wet, gedragscode, protocol
1	Het moet voor betrokkene duidelijk te zijn wie/welke entiteit verantwoordelijk is voor de verwerking van zijn persoonsgegevens.	In al uw privacyteksten (waaronder uw privacystatement op internet) is duidelijk opgenomen wie de verantwoordelijke is. U geeft aan onder welke naam of onder welk nummer de melding is terug te vinden.	Het is raadzaam om per organisatie een persoon aan te wijzen als privacy officer, die het register bijhoudt, de verzoeken om inzage regelt, controleert of men zich aan gestelde termijnen houdt en kan dienen als vraagbaak voor de organisatie.	Artikel 4.7, 4.8 en 5.1.3 Gedragscode Artikel 33 en 34 Wbp
2	Persoonsgegevens mogen verzameld worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen.	Het doel van de verwerking is duidelijk bepaald en nauwkeurig omschreven. Bij de melding bij het CBP worden de doelen aangegeven om welke verwerking het gaat. *Alle* verwerkingen van persoonsgegevens binnen uw organisatie zijn in kaart gebracht.	Conform de Gedragscode Verwerking Persoonsgegevens Financiële Instellingen vinden verwerkingen van persoonsgegevens plaats voor efficiënte en effectieve bedrijfsvoering, in het bijzonder in het kader van de activiteiten als weergegeven in artikel 5.1.1. Denk bij het in kaart brengen van alle verwerkingen ook aan onderdelen van het verzekeringsbedrijf die zich niet direct bezig houden met verzekeren zoals stichtingen in het kader van rechtshulpverlening of re-integratiebedrijven. Het verdient aanbeveling om deze inventarisatie van verwerkingen op te nemen als vast onderdeel in de reguliere compliance check.	Artikel 7 Wbp Artikel 5.1.1 Gvpfi
3	Alle verwerkingen van persoonsgegevens worden vooraf gemeld bij het CBP of, indien aangesteld, de Functionaris voor de Gegevensverwerking (FG). Melding van een verwerking bij het CBP is niet aangewezen als gebruik mag worden gemaakt van het Vrijstellingsbesluit.	Controleer of alle verwerkingen van persoonsgegevens binnen de organisatie gemeld zijn bij het CBP dan wel de FG. Controleer periodiek of het Vrijstellingbesluit (nog) van toepassing is.	Als gebruik wordt gemaakt van het Vrijstellingsbesluit moet duidelijk zijn om welk onderdeel het gaat. Als bij controle blijkt dat het Vrijstellingsbesluit niet (meer) van toepassing is, geldt alsnog de meldplicht bij CBP of FG. Vrijgesteld van melding zijn bijvoorbeeld de bezoekersadministratie, salarisadministratie of personeelsadministratie.	Artikel 27 e.v. Wbp Artikel 5.1.3 Gvpfi Vrijstellingsbesluit Wbp

4	Als de verwerking van persoonsgegevens verandert, moet dit bij het CBP worden gemeld.	Geef aanpassingen in de verwerking van persoonsgegevens, binnen de in de wet gestelde termijnen, aan het CBP door. Controleer periodiek of alle onderdelen van de gegevensverwerking nog in overeenstemming zijn met bij de melding aan het CBP doorgegeven informatie over bijvoorbeeld de verzameldoelen, kring van betrokkenen en ontvangers.	Denk bij een verandering van de verwerking niet alleen aan uitbreiding van de ontvangers, maar ook aan fusies, naamswijzigingen of overnames. Houdt rekening met de termijnen die voor de betreffende wijziging gelden. Zo geldt voor naam- en adreswijzigingen een termijn van een week en voor andere wijzigingen, zoals uitbreiding van de ontvangers, één jaar.	Artikel 28 lid 3 Wbp Artikel10 Gvpfi
5	In bepaalde gevallen is Voorafgaand Onderzoek door het CBP verplicht.	Geef bij de melding bij het CBP aan dat sprake is van de noodzaak tot het uitvoeren van een Voorafgaand Onderzoek als sprake is van: 1. gebruik van een nummer ter identificatie voor andere doeleinden dan waarvoor het nummer specifiek bedoeld is; 2. verzamelen van informatie door middel van eigen waarneming zonder betrokkene te informeren 3. verwerking van strafrechtelijke gegevens of gegevens van onrechtmatig of hinderlijk gedrag ten behoeve van derden.	Voorafgaand onderzoek (VO) is niet vereist als door een andere Verantwoordelijke een VO aan het CBP is gevraagd en het CBP heeft verklaard dat de verwerking rechtmatig is. Ten aanzien van de verwerking van persoonsgegevens in een Incidentenregister en EVR op grond van het PIFI is door de betrokken brancheverenigingen gezamenlijk een VO aangevraagd en heeft het CBP een rechtmatigheidverklaring afgegeven. Voor het incidentenregister is derhalve geen VO meer aangewezen en kan worden volstaan met de melding van de verwerking aan het CBP onder overlegging van een getekende toetredingsverklaring tot en een exemplaar van het PIFI.	Artikel 31 Wbp Artikel 5.3.1 Gvpfi Artikel 3.1.1. PIFI
6	Bij aanwezigheid van een Functionaris voor de Gegevensverwerking (FG) moet een register aanwezig zijn van de verwerkingen die plaats vinden.	De FG binnen uw organisatie beheert een register waarin de verwerkingen van de organisatie zijn opgenomen. Het register is bekend bij en toegankelijk (bijvoorbeeld door plaatsing op internet) voor betrokkene. Het register is kosteloos voor iedereen raadpleegbaar.	Het verdient aanbeveling om een centraal aanspreekpunt voor privacy te hebben, ook als geen FG volgens de Wbp is aangesteld. Let op: raadplegen van dit register van verwerkingen is niet hetzelfde als inzage verstrekken aan betrokkene in een verwerking van zijn persoonsgegevens. Hier betreft het een opsomming van de soorten van verwerkingen. Het CBP hanteert eveneens een publiek toegankelijk register waarin alle aangemelde verwerkingen zijn te raadplegen.	Artikel 62 en 63 Wbp Artikel 30 Wbp Artikel 8.1. Gvpfi

Hoofdstuk 2 Transparantie

Bij transparantie gaat het om de voorlichting aan de betrokkene. In uw organisatie is de verwerking van de persoonsgegevens voor de betrokkenen transparant en wordt aan de wettelijke informatieverplichting voldaan. Voor deze informatieplicht geldt een aantal uitzonderingen. Deze is niet nodig wanneer de betrokkene al op de hoogte is, wanneer het voldoen aan de verplichting onmogelijk is of een onevenredige inspanning kost, dan wel het een verwerking betreft die bij wet is voorgeschreven. Ook is het mogelijk (tijdelijk) gebruik te maken van de uitzonderingsbepalingen als aangegeven in artikel 43 Wbp.

Volgnr	Voorschrift	Uitwerking bij verzekeraar	Toelichting	Vindplaats in wet, gedragscode, protocol
7	Betrokkene moet voorafgaand aan de verwerking van zijn persoonsgegevens geïnformeerd worden over het doel van de verwerking en over de verantwoordelijke voor de verwerking.	Uw organisatie hanteert teksten ten behoeve van de informatieverplichting richting de cliënt. Hierin moet ten minste genoemd worden welke organisatie verantwoordelijk is voor de verwerking en welke doeleinden daaraan zijn verbonden. Op alle uitingen die leiden tot een verwerking van persoonsgegevens zijn teksten geplaatst die de betrokkene hierover informeren.	Het Verbond heeft voorbeeldteksten opgesteld ten behoeve van deze informatieplicht. De voorbeeldteksten kunnen gebruikt worden bij alle uitingen (denk aan informatiefolders, aanbiedingen, offertes etc.) die (kunnen) leiden tot verwerking van persoonsgegevens.	Artikel 33 en 34 Wbp Circulaire LV 2011/61 inzake voorbeeldteksten
8	Betrokkene heeft het recht verzet aan te tekenen als verwerking van zijn persoonsgegevens voor marketingdoeleinden kan plaatsvinden.	Betrokkene wordt transparant en duidelijk geïnformeerd over zijn mogelijkheid tot verzet bij verwerking van zijn persoonsgegevens ten behoeve van marketing doeleinden.	Er is een onderscheid tussen post, telefoon en elektronische berichten en het plaatsen van cookies. Zie hiervoor het Overzicht geldende wet- en regelgeving van 1 oktober 2009 inzake de Verwerking van (persoons)gegevens voor direct marketing doeleinden. Zie tevens de circulaire over de gewijzigde Telecommunicatiewet van 1 augustus 2012 over het plaatsen van cookies.	Artikel 41 Wbp Circulaires LV-2009/49 van 30 september 2009 en LV-2012/44 van 1 augustus 2012
9	Als verwerking van persoonsgegeven ten behoeve van derden plaatsvindt, wordt dit aan betrokkene meegedeeld. Informeren over deze verwerking vindt uiterlijk op het moment van eerste verstrekking plaats.	De betrokkene wordt vooraf geïnformeerd als zijn gegevens worden verstrekt of getoetst aan de CIS databank.	Het Verbond heeft voorbeeldteksten opgesteld in het kader van de informatieplicht. Hierin zijn voorbeeldteksten opgenomen voor het informeren van betrokkene over de verwerking van persoonsgegevens bij Stichting CIS. Denk ook bij elektronische (schade)formulieren aan een duidelijke verwijzing naar de verwerking bij Stichting CIS.	Artikel 33 en 34 Wbp Deelnemerovereenkomst Stichting CIS Circulaire LV 2011/61 inzake voorbeeldteksten.

10	Als het binnen de wettelijke grenzen noodzakelijk is, kan de informatieplicht over de verwerking van persoonsgegevens buiten toepassing worden gelaten.	Controleer periodiek of de gevallen waarin gebruik wordt gemaakt van een beroep op een uitzondering op de informatieplicht op grond van art. 43 Wbp of dit beroep noodzakelijk is en binnen de omschrijving uit de wet valt.	Het gaat hier vooral om de afweging van de noodzakelijkheid en het belang bij de voorkoming van strafbare feiten (onderdeel b) en het belang van de rechten en vrijheden van derden (onderdeel e). Leg de afweging om niet te informeren schriftelijk vast; de cliënt kan tegen een dergelijke afweging in beroep gaan. De uitzondering betreffende opsporing en vervolging van strafbare feiten is niet van toepassing omdat dit geen taken van een verzekeraar betreft maar is voorbehouden aan politie en Justitie.	Artikel 43 Wbp Artikel 9 Gvpfi

Hoofdstuk 3 Behoorlijke en zorgvuldige verwerking

De persoonsgegevens worden in overeenstemming met de Wet bescherming persoonsgegevens op een behoorlijke en zorgvuldige wijze verwerkt. Onder verwerking worden vele vormen van omgang met persoonsgegevens begrepen, zoals verzamelen, ordenen, doorzenden, verwijderen, vernietigen e.d. (artikel 1 onder b. Wbp).

Volgnr	Voorschrift	Uitwerking bij verzekeraar	Toelichting	Vindplaats in wet, gedragscode, protocol
11	De persoonsgegevens worden in overeenstemming met de wet en op een behoorlijke en zorgvuldige wijze verwerkt.	Controleer periodiek of verwerkte persoonsgegevens op legitieme wijze zijn verkregen en op een zorgvuldige manier binnen uw organisatie worden toegepast. Zorg dat verwerkingen alleen toegankelijk zijn voor daartoe bevoegde medewerkers ten behoeve van de uitoefening van hun functie.	Het gaat hierbij om meer wetten dan alleen de Wbp. Denk hierbij aan bijvoorbeeld de Telecommunicatiewet, de Wet op het financieel toezicht en de Wet ter voorkoming van witwassen en financiering van terrorisme. Voor een compleet overzicht dient u zelf regelmatig de wetgevingskalender te raadplegen. Bij zorgvuldige verwerking moet onder meer rekening worden gehouden met de doeleinden waarvoor de gegevens zijn verkregen.	Artikel 6 en 11 Wbp
12	Voor elke verwerking moet minimaal één rechtmatige grondslag aanwezig zijn.	Controleer per verwerking of een rechtmatige grondslag, als omschreven in de Wbp, aanwezig is.	Rechtmatige grondslagen voor verwerking zijn onder meer: • betrokkene heeft toestemming gegeven; • in het kader van de uitvoering van de overeenkomst waarbij betrokkene partij is; • in het gerechtvaardigde belang van de verantwoordelijke of derden; • ter nakoming van een wettelijke verplichting. Het is van belang om de grondslag vast te stellen in verband met het relatieve recht van verzet. Verzet is alleen van toepassing op de volgende grondslagen: • gegevensverwerking is noodzakelijk voor goede invulling van publieke taak; • voor behartiging van gerechtvaardigd belang. Recht van verzet is dus niet van toepassing bij verwerking persoonsgegevens in het kader van een overeenkomst.	Artikel 8 Wbp Artikel 4.3 Gvpfi

13	Persoonsgegevens mogen niet worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen.	Zorg dat duidelijk is welke doeleinden voor de verwerking van persoonsgegevens zijn vastgesteld en controleer periodiek of persoonsgegevens niet worden gebruikt op een manier die met die doeleinden onverenigbaar is.	Verenigbaarheid met vastgestelde doeleinden is ruimer dan verwerking conform de vastgestelde doeleinden. Uitgangspunt van deze open normering is dat het verantwoordelijke bewijs kan leveren waarom geen sprake is van onverenigbaarheid.	Artikel 9 lid 1 Wbp Artikel 4.4 Gvpfi
14	Persoonsgegevens worden, gelet op de doeleinden waarvoor ze zijn of worden verzameld, verwerkt voor zover zij toereikend, ter zake dienend en niet bovenmatig zijn. Persoonsgegevens moeten juist en nauwkeurig zijn.	Controleer periodiek of de verwerkte persoonsgegevens ook daadwerkelijk nodig zijn om de activiteiten uit te kunnen voeren. Leg niet meer vast dan strikt noodzakelijk is. Zorg dat bij vastlegging van persoonsgegevens accuraat wordt gewerkt. Voer controle uit op de ontvangen gegevens in geval van onduidelijkheid of twijfels over de juistheid.	Het doel van de verwerking is bepalend voor hoeveel en welke soort van informatie kan worden verwerkt. Als de juistheid van verwerkte persoonsgegevens twijfelachtig is, kan verwerking daarvan consequenties hebben voor een derde. De verantwoordelijkheid voor het nemen van de controle maatregelen rust op de verzekeraar.	Artikel 11 Wbp Artikel 4.5 Gvpfi
15	Persoonsgegevens mogen, niet langer bewaard blijven dan voor het doel noodzakelijk is.	Stel binnen de organisatie beleid op met betrekking tot de bewaartermijnen. Bewaartermijnen kunnen per verwerking of soort van persoonsgegeven verschillen. De feitelijke termijnen worden bepaald op basis van individueel maatschappijbeleid.	Bij de bepaling van de bewaartermijnen van verwerkingen kan bijvoorbeeld een relatie worden gelegd met de vierdeling: • cliëntadministratie • veiligheid en integriteit (Protocol Incidentenwaarschuwingssysteem) • marketing (houd rekening met snel verouderde gegevens) • gegevens omtrent de gezondheid	Artikel 10 Wbp Artikel 4.6.1 Gvpfi

16	Verwerking van persoonsgegevens door medewerkers, onder gezag van de verantwoordelijke of de bewerker, vindt alleen plaats in opdracht van de verantwoordelijke. Geheimhouding is verplicht behoudens wettelijke verplichtingen mededeling voorschrijven of voor de medewerkers uit hun taak de noodzaak tot mededeling voortvloeit.	Hanteer een geheimhoudingsplicht als onderdeel van iedere arbeidsovereenkomst of overeenkomst met een bewerker. Informeer medewerkers over de vertrouwelijkheid van de persoonsgegevens en houdt toezicht op de naleving van de geheimhoudingsverplichting.	Van belang is dat iedere medewerker zich blijft realiseren dat schending van de vertrouwelijkheid met betrekking tot de verwerking van persoonsgegevens gevolgen heeft voor de verzekeraar.	Artikel 12 Wbp Artikel 1.1 Gedragscode
17	Verwerking van het burger service nummer (BSN) is slechts toegestaan in de gevallen waarin de wet dit heeft bepaald.	Controleer of de maatschappij kwalificeert als een gebruiker op grond van de Wet algemene bepalingen burger service nummer (Wabb).	Gebruik van BSN is uitsluitend toegestaan als daar een wettelijke grondslag voor bestaat. Uitgangspunt is: als u geen persoonsgebonden gegevens, waaronder een persoonsnummer, hoeft vast te leggen voor de uit te voeren handeling of dienst mag u ook het BSN niet vastleggen of gebruiken. Als werkgever mag u BSN bijvoorbeeld toepassen in verband met het doorgeven van gegevens aan de Belastingdienst. Voor de uitvoering van commerciële diensten (uw cliëntadministratie) is gebruik van het BSN weer niet toegelaten.	Artikel 1 Wabb

Hoofdstuk 4 Rechten van betrokkene

De betrokkene van wie de persoonsgegevens worden verwerkt, heeft diverse rechten wanneer zijn persoonsgegevens worden of zijn verwerkt. Een aantal daarvan zijn in algemene zin in de voorgaande hoofdstukken al aan de orde gekomen. In dit hoofdstuk wordt verder ingegaan op een aantal specifieke rechten van betrokkene.

Volgnr	Voorschrift	Uitwerking bij verzekeraar	Toelichting	Vindplaats in wet, gedragscode, protocol
18	Betrokkene heeft recht om vrijelijk en met redelijke tussenpozen aan verantwoordelijke te verzoeken mee te delen of zijn persoonsgegevens worden verwerkt.	Iedereen waarvan de verzekeraar persoonsgegevens verwerkt, heeft recht op inzage in deze verwerking. Daartoe heeft de verantwoordelijke geregeld: • dat bekend is hoe en waar het inzageverzoek moet worden ingediend; • dat identiteitscontrole van betrokkene plaatsvindt; • dat betrokkene binnen vier weken wordt meegedeeld of over hem persoonsgegevens worden verwerkt en zo ja, welke gegevens dat zijn; • dat betrokkene een volledig en begrijpelijk overzicht krijgt van de verwerkte persoonsgegevens, een omschrijving van de doeleinden van de verwerking, de categorieën van gegevens waarop de verwerking betrekking heeft, de (categorieën van) ontvangers en de beschikbare informatie over de herkomst van de gegevens.	Iedereen heeft het recht te weten welke gegevens over hem worden verwerkt. Dit vindt slechts uitzondering in de gevallen die in de wet (artikel 43 Wbp) zijn genoemd. Per maatschappij moet zelf worden vastgesteld wat onder het recht op inzage moet worden verstrekt aan betrokkene. Het gaat volgens de wet specifiek om de persoonsgegevens van betrokkenen. Dat betekent dat veel maar niet alles onder het recht op inzage valt. Denk aan stukken voor intern overleg of documentatie betreffende eigen gedachtevorming. De identiteitscontrole is van belang om te voorkomen dat persoonsgegevens worden verstrekt aan een derde. Verstrek dan ook geen overzicht aan anderen dan betrokkene zelf. Alleen betrokkene heeft recht op inzage.	Artikel 35 Wbp Artikel 7.1 Gvpfi Artikel 9.3 PIFI
19	Betrokkene heeft het recht om te verzoeken persoonsgegevens te verbeteren, aan te vullen, te verwijderen of af te schermen indien deze feitelijk onjuist zijn,	Zorg dat betrokkenen geïnformeerd wordt over zijn recht op correctie. Zorg dat duidelijk is: • hoe en waar de verzoeken tot verbetering, aanvulling, verwijdering of afscherming moeten worden	Omdat het recht om een correctieverzoek in te dienen in de wet gekoppeld is aan een voorafgaand verzoek tot inzage kan betrokkene bij het verstrekken van het overzicht (artikel 35 Wbp) geïnformeerd worden over het correctierecht.	Artikel 36 Wbp Artikel 7.1.3 Gvpfi Artikel 9.4 PIFI

	voor de doeleinden van de verwerking onvolledig of niet ter zake dienend zijn dan wel anderszins in strijd zijn met een wettelijk voorschrift worden verwerkt.	ingediend; • dat de identiteit van de betrokkene wordt gecontroleerd; • dat de betrokkene binnen 4 weken schriftelijk wordt meegedeeld in hoeverre aan zijn verzoek wordt voldaan (indien verzoek wordt afgewezen, met bijbehorende motivatie).	Zonder voorafgaande inzage kan formeel geen correctie worden gevraagd. Dit in verband met de eis dat betrokkene moet aangeven welke wijzigingen hij verwacht.	
20	Wanneer de verwerking plaatsvindt op de grondslag van artikel 8 onder e. en f. Wbp heeft de betrokkene het recht verzet aan te tekenen tegen de verwerking van persoonsgegevens op grond van bijzondere persoonlijke omstandigheden.	Zorg dat betrokkene kennis kan nemen van het recht van verzet en informeer hem: • hoe en waar het verzoek tot verzet moet worden ingediend; • dat zijn identiteit wordt gecontroleerd; • dat binnen 4 weken schriftelijk wordt meegedeeld in hoeverre zijn verzet gerechtvaardigd is. Als het verzet gerechtvaardigd wordt gevonden, zorg dan dat de verwerking onmiddellijk beëindigd.		Artikel40 Wbp Artikel7.2.1 Gedragscode
21	De betrokkene heeft het absoluut recht van verzet bij het gebruik van zijn gegevens voor commerciële of charitatieve doeleinden.	Zorg dat, als de betrokkene rechtstreeks een boodschap wordt toegezonden, hij steeds wordt gewezen op de mogelijkheid tot het doen van verzet. Zorg dat betrokkene kennis kan nemen: • hoe en waar het verzet kan worden ingediend; • dat het verzet op deze grond kosteloos kan worden ingediend. In geval van verzet wordt: • de betreffende verwerking direct beëindigd; • betrokkene op zijn verzoek binnen vier weken geïnformeerd over de genomen maatregelen.	Het Verbond heeft een publicatie uitgebracht met hierin informatie betreffende de scheiding tussen post, elektronische berichten en telefoon. Zie hiervoor het Overzicht geldende wet- en regelgeving van 1 oktober 2009 betreffende de Verwerking van (persoons)gegevens voor het overbrengen van (ongevraagde) communicatie voor direct marketing doeleinden en circulaire over de Wijziging Telecommunicatiewet met informatie over de nieuwe Cookiebepaling van 1 augustus 2012. Zie er op toe dat maatregelen zijn getroffen om deze vorm van verwerking terstond te beëindigen zodra verzet gehonoreerd wordt en dat technische en organisatorische maatregelen zijn genomen die op grond van de Telecommunicatiewet noodzakelijk zijn.	Artikel 41 Wbp Artikel7.2.2 – 7.2.6 Gvpfi Circulaire LV-2009/49 en LV-2012/44 van 1 augustus 2012

Hoofdstuk 5 Bewerker

Het is mogelijk dat uw organisatie (delen van de) gegevensverwerking aan derden heeft uitbesteed. De bewerker is degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt zonder aan zijn rechtstreeks gezag te zijn onderworpen (artikel 1 onder e. Wbp). Een bewerker kan per organisatie verschillen. Denk bijvoorbeeld aan het uitbesteden van de salarisadministratie aan een extern bureau of het laten sturen van direct mail door een extern bureau. Om dit te kunnen doen, moeten dergelijke organisaties beschikking krijgen over de door u verwerkte persoonsgegevens.

Volgnr	Voorschrift	Uitwerking bij verzekeraar	Toelichting	Vindplaats in wet, gedragscode, protocol
22	Persoonsgegevens kunnen namens de verantwoordelijke worden verwerkt door een bewerker.	Bij uitbesteding van activiteiten waarbij persoonsgegevens ten behoeve van de organisatie worden verwerkt, is een bewerkerovereenkomst opgesteld. In de overeenkomst wordt afdoende gespecificeerd aangegeven welke verwerking mag worden uitgevoerd, welke doeleinden van toepassing zijn en hoe moet worden voorzien in geheimhouding. Neem de verplichting voor de bewerker tot het nemen van afdoende technische en organisatorische maatregelen ter beveiliging van de data moet in de overeenkomst op.	Denk bij de bewerkerovereenkomst ook aan afspraken over de omgang met gegevens in geval van eenmalig gebruik of gebruik van beperkte duur, bijvoorbeeld mailing house of callcenter.	Artikel 1 Wbp Artikel 14 Wbp Artikel 4.12 en 8.3.2 Gvpfi
23	De verantwoordelijke is verplicht toe te zien op naleving van de organisatorische en technische waarborgen ter beveiliging van de verwerking van persoonsgegevens.	Leg vast in de bewerkerovereenkomst dat de verzekeraar een audit kan uitvoeren bij de bewerker. Spreek met de bewerker af dat hij rapporteert over de genomen maatregelen en de veiligheidsincidenten en hoe vaak deze rapportage moet.	Maak bij uitbesteding van de verwerking van persoonsgegevens duidelijk afspraken over de controle die de verantwoordelijke kan (laten) uitvoeren en de rapportages die de bewerker periodiek moet overleggen.	Artikel 14 Wbp Artikel 4.12 en 8.3.2 Gvpfi

Hoofdstuk 6 Verwerking met landen buiten de Europese Unie

Uitgangspunt is dat gegevens niet buiten de Europese Unie worden doorgegeven, tenzij een van de uitzonderingen van artikel 77 Wbp van toepassing is. In dat artikel zijn aanvullende en bijzondere regels gesteld, zoals de situatie dat verstrekking noodzakelijk is in het kader van de uitvoering van een overeenkomst. Voor verzekeraars valt te denken aan gegevensuitwisseling in verband het ziek worden van verzekerde of een autoschade in een land buiten de EU.

Volgnr	Voorschrift	Uitwerking bij verzekeraar	Toelichting	Vindplaats in wet, gedragscode, protocol
24	Persoonsgegevens mogen alleen verstrekt worden aan landen buiten de Europese Unie als in dat land van een passend beschermingsniveau sprake is.	Controleer periodiek of persoonsgegevens die worden verwerkt worden doorgegeven aan landen buiten de EU.	Alle landen binnen de EER hebben een passend beschermingsniveau alsmede voor landen die door het CBP zijn aangewezen. Zie de actuele lijst met landen op de website van het CBP: www.cbpweb.nl. Houd rekening met deze voorschriften in een organisatie met vestigingen buiten de EU.	Artikel 76 Wbp
25	Wanneer geen sprake is van een passend beschermingsniveau kan het geoorloofd zijn persoonsgegevens door te geven wanneer het gaat om een van de uitzonderingen als genoemd in artikel 77 Wbp.	Draag er zorg voor dat per concreet geval waarin persoonsgegevens buiten de EU worden doorgegeven, vastgesteld wordt welke van de wettelijke uitzonderingsbepalingen van toepassing is.	Als voorbeeld voor de doorgifte van persoonsgegevens aan het buitenland kan gedacht worden aan: noodzakelijk voor de uitvoering van een (verzekerings)overeenkomst.	Artikel 77 lid 1 sub a tot en met f Wbp
26	De Minister van Justitie en Veiligheid kan, indien bovenstaande voorschrift geen uitzondering biedt, voor doorgifte van gegevens aan derde landen waar geen passend beschermingsniveau aanwezig is, een vergunning afgegeven.	Als wordt vastgesteld dat geen sprake is van een wettelijke uitzondering als bedoeld in artikel 77 lid 1 Wbp en de doorgifte van persoonsgegevens wordt door de organisatie desondanks noodzakelijk geacht, moet gezorgd worden voor een ministeriele vergunning voor doorgifte.	Voor contracten met landen buiten de EU zijn door de Europese Commissie modellen opgesteld. Indien geen gebruik wordt gemaakt van deze Europese model contracten dan is een vergunning van de Minister vereist. Een vergunning moet worden aangevraagd door tussenkomst van het CBP. Indien er wel gebruik wordt maakt van deze model contracten dan is een vergunning van de Minister niet nodig.	Artikel77 lid 2 Wbp

Hoofdstuk 7 Gegevens omtrent gezondheid

Gegevens omtrent gezondheid dienen in overeenstemming met toepasselijke wetgeving en de Gedragscode Verwerking Persoonsgegevens Financiële Instellingen op een behoorlijke en zorgvuldige wijze worden verwerkt. Bij wet moet behalve de Wet bescherming persoonsgegevens ook worden gedacht aan de Wet op de geneeskundige behandelingsovereenkomst (Wgbo; opgenomen in de artikelen 7:446 - 468 Burgerlijk Wetboek) en de Wet op de medische keuringen (WMK). Deze aanvulling is vooral van belang voor het onderscheid tussen de verwerking van persoonsgegevens omtrent iemands gezondheid door verzekeraars aan de ene kant en door de medisch adviseur en zijn staf aan de andere kant.

Volgnr.	Voorschrift	Uitwerking bij verzekeraar	Toelichting	Vindplaats in wet, gedragscode, protocol
27	Gegevens omtrent gezondheid mogen door de verzekeraar alleen verwerkt voor zover noodzakelijk: 1. voor de beoordeling van het te verzekeren risico en de betrokkene daartegen geen bezwaar maakt 2. voor de uitvoering van de verzekeringsovereenkomst.	Bedrijfsprocessen zijn zo ingericht dat medische persoonsgegevens alleen verwerkt worden voor risicobeoordeling als instemming van betrokkene is vastgesteld en bij verwerking in uitvoering van de overeenkomst dat deze gegevens door de betrokkene zelf zijn verstrekt.	Bij verwerking van medische gegevens is scheiding van verantwoordelijkheden in bedrijfsprocessen van belang. Laat een acceptant geen claimbesluit nemen over polissen waar hij de medische gegevens heeft beoordeeld.	Artikel 16 en 21 Wbp Artikel 6.1 Gvpfi
28	Betrokkene moet in de gelegenheid zijn bezwaar te maken tegen het gebruik van gegevens betreffende zijn gezondheid in het kader van de beoordeling van het te verzekeren risico.	Betrokkene wordt voor aanvang van het acceptatieproces gewezen op de mogelijkheid om bezwaar te maken inzake verstrekking van gegevens over zijn gezondheid.	Omdat deze norm (tevens) een uitvloeisel is van de voorwaarden die de WGBO stelt, kunnen voor deze bezwaarregeling afspraken met de medisch adviseur worden gemaakt over de te volgen procedure. Informeer betrokkene over noodzaak van verstrekking en consequenties van het bezwaar.	Artikel 21 Wbp
29	Verwerking van gegevens omtrent iemands gezondheid is ook toegestaan, wanneer: 1. hiertoe de uitdrukkelijke toestemming van de cliënt is verkregen; 2. de gegevens door de betrokkene duidelijk openbaar zijn gemaakt; 3. dit noodzakelijk is voor de vaststelling, uitoefening of verdediging van een recht in rechte;	Draag er zorg voor dat bij verwerking van gegevens betreffende de gezondheid op basis van de genoemde uitzonderingen: • toestemming expliciet is gegeven en vastgelegd; • van geraadpleegde openbare bron is bron, verkregen informatie, raadpleegdatum en tijdstip vastgelegd; • volkenrechtelijke verplichting waaraan moet worden voldaan is vastgelegd;	Omdat het om uitzonderingen gaat, is het van groot belang de overwegingen die tot de uitzondering hebben geleid, vast te leggen in het dossier.	Artikel 16 jo. 23 lid 1 Wbp Artikel 6.1.2 Gvpfi

	4. dit noodzakelijk is ter voldoening aan een volkenrechtelijke verplichting; 5. dit noodzakelijk is met het oog op een zwaarwegend algemeen belang, passende waarborgen worden geboden ter bescherming van de persoonlijke levenssfeer en dit bij wet wordt bepaald dan wel het CBP ontheffing heeft verleend.	• algemeen belang is vastgelegd en de zwaarwegendheid kan worden onderbouwd.		
30	Gegevens omtrent de gezondheid van een cliënt, die verkregen zijn in het kader van een bepaald product, mogen niet worden doorgegeven voor de beoordeling, de acceptatie of de uitvoering van een overeenkomst met de betrokken cliënt ten behoeve van een ander product of andere schadeclaim.	Stel passende technische en/of procedurele waarborgen ter voorkoming dat gegevens omtrent de gezondheid worden gebruikt voor andere doeleinden dan waarvoor deze zijn verkregen. Binnen de organisatie is vastgelegd wat onder 'ander product' of 'andere schadeclaim' moet worden verstaan.	Door intern vast te stellen waar uw grenzen liggen van 'andere producten en andere schadeclaims' wordt eventuele onduidelijkheid over onrechtmatig gebruik beperkt. Dergelijke beleidsregels kunnen ter toelichting of verdediging in procedures worden gebruikt.	Artikel 11 Wbp Artikel 6.1.3 Gvpfi
31	Gegevens omtrent gezondheid mogen worden verwerkt voor wetenschappelijk onderzoek of statistiek als: • het onderzoek een algemeen belang dient; • de verwerking voor het betreffende onderzoek of statistiek noodzakelijk is; • het vragen van toestemming van betrokkene onmogelijk is of een onevenredige inspanning kost; • maatregelen zijn getroffen opdat de persoonlijke levenssfeer niet onevenredig wordt geschaad.	In geval van wetenschappelijk onderzoek of statistiek zijn in het onderzoeksplan de noodzakelijkheid, het algemeen belang en de maatregelen ter waarborging van de privacy vastgelegd. Bij een beroep op onmogelijkheid of onevenredige inspanning voor het verkrijgen van toestemming per betrokkene is de argumentatie daartoe in het onderzoeksplan vastgelegd.		Artikel 23 lid 2 Wbp

32	De verwerking van gegevens omtrent de gezondheid om een advies te kunnen uitbrengen over de medische beoordeling van een (aspirant)-verzekerde mag alleen plaatsvinden door de medisch adviseur en de personen die onder zijn verantwoordelijkheid betrokken zijn bij dat advies.	Gezondheidsverklaringen worden alleen door de medisch adviseur en zijn staf verzameld en beoordeeld. Draag er zorg voor dat gezondheidsverklaringen door betrokkene rechtstreeks gericht worden aan de medisch adviseur of de medische staf.		Artikel 21 lid 2 Wbp Artikel 6.1.4 Gvpfi
33	Het opvragen van gegevens omtrent de gezondheid ter beoordeling van gezondheidssituatie van een cliënt geschiedt uitsluitend door een medisch adviseur of de medische staf.	Bij het opvragen van gegevens omtrent de gezondheid in het acceptatieproces wordt het verzoek altijd door of namens de medisch adviseur aan betrokkene voorgelegd.	Deze bepaling laat onverlet dat in bepaalde gevallen ook anderen binnen de organisatie gegevens omtrent de gezondheid mogen verwerken. Iedere verwerking moet plaatsvinden binnen de kaders van de Wbp.	Artikel 21 lid 2 Wbp
34	Verwerking van gegevens omtrent gezondheid is alleen toegestaan voor personen die tot geheimhouding verplicht zijn uit hoofde van ambt, beroep of wettelijk voorschrift of op grond van een overeenkomst tot geheimhouding.	Medewerkers van de medische staf moeten een geheimhoudingsverklaring tekenen bij indiensttreding.		Artikel 21 lid 2 Wbp Artikel 7:457 BW Artikel 6.1.9 Gvpfi
35	Een medisch adviseur mag alleen gegevens omtrent de gezondheid bij een derde opvragen met toestemming en een machtiging van de cliënt. In de machtiging moeten de aard van de opgevraagde gegevens en het doel van het verzoek vermeld zijn.	Hanteer schriftelijke verklaringen voor toestemming en machtigingen. Draag er zorg voor dat deze documenten aangeven voor welk concreet omschreven aangelegenheid gegevens benodigd zijn. Informeer cliënt bij het verzoek om de machtiging over aard van de op te vragen gegevens en het doel van de opvraging.	Uit de machtiging moet voldoende duidelijk zijn waarom en waarvoor de betrokkene zijn toestemming geeft. Daarmee is voor zowel betrokkene als de derde die de informatie moet verstrekken duidelijk waar de grenzen liggen.	Artikel 6.1.5 Gvpfi

36	De medisch adviseur richt een medisch dossier in dat onder zijn verantwoordelijkheid wordt bewaard.	De medisch adviseur en de medische staf leggen dossiers aan. De dossiers zijn zodanig opgeslagen dat deze niet voor andere medewerkers binnen de organisatie toegankelijk zijn.		Artikel 7:454 BW
37	Voor de bewaartermijnen van medische dossiers bij de medisch adviseur gelden de termijnen zoals gesteld in de Wbp en niet in de WGBO.	Stel in de organisatie een beleid vast waarin de bewaartermijn per categorie persoonsgegevens wordt bepaald.	De bewaartermijn is van gegevens die herleidbaar zijn tot een natuurlijk persoon is afhankelijk van de noodzaak om ze te bewaren in relatie tot de doeleinden voor de verwerking.	Artikel 10 Wbp Artikel 7:464 lid 2 sub a BW Artikel 4.6.1 Gvpfi Artikel 4.6.2 Gvpfi
38	Indien in het kader van acceptatie en/of schadebehandeling medewerking van een cliënt aan een medische keuring of aan een aanvullend medisch onderzoek wordt gevraagd, moet in de keuringsstukken of formulieren gewezen worden op het belang van legitimatie teneinde verwisseling van personen te voorkomen.	Draag zorg voor dat in formulieren voor medische keuringen gewezen wordt op de legitimatieplicht door betrokkene. Voor zover de keuring of het onderzoek onder verantwoordelijkheid van de eigen organisatie wordt uitgevoerd, is controle op legitimatie binnen het desbetreffende werkproces voorgeschreven.		Artikel 6.1.7 onder a. Gvpfi
39	De cliënt zal bij een medische keuring of aanvullend onderzoek worden geïnformeerd dat hij het recht heeft om schriftelijk te kennen te geven dat hij de uitslag en gevolgtrekking van het onderzoek wenst te vernemen. Tenzij het een tot stand gekomen burgerrechtelijke verzekering betreft, moet de cliënt bovendien het recht worden geboden als eerste kennis te nemen van zijn gegevens.	Richt formulieren zodanig in dat de cliënt wordt gewezen op zijn (eerste) informatierecht en zijn recht om doorgifte aan anderen te blokkeren.		Artikel 6.1.7 onder b. Gvpfi

	Cliënt moet kunnen beslissen dat geen mededeling van die uitslag en gevolgtrekking aan anderen wordt gedaan.			
40	Op persoonsgegevens over erfelijke eigenschappen is het moratorium erfelijkheidsonderzoek van toepassing.	Zorg er voor dat de medisch adviseur bekend is met de betreffende richtlijnen en controleer periodiek of naleving plaatsvindt.		Artikel 6.1.10 Gvpfi
41	Op persoonsgegevens die ontleend kunnen worden aan bloedonderzoek is de 'HIV Gedragscode' van toepassing.	Zorg er voor dat de medisch adviseur bekend is met de betreffende Gedragscode en controleer periodiek of naleving plaatsvindt.		Artikel 6.1.11 Gvpfi

Hoofdstuk 8 Gebeurtenissen, Incidenten en Strafrechtelijke (persoons)gegevens

Het begrip strafrechtelijke gegevens heeft betrekking op zowel veroordelingen als op min of meer gegronde verdenkingen. Veroordelingen betreffen gegevens waarbij de rechter strafrechtelijk gedrag bewezen heeft verklaard. Bij verdenkingen gaat het om concrete aanwijzingen ten opzichte van een bepaalde persoon. Door een verzekeraar kunnen strafrechtelijke gegevens in meerdere situaties worden verwerkt. De eerste betreft de vraag naar het strafrechtelijke verleden, de tweede de verwerking van gegevens in de Gebeurtenissenadministratie en het eventueel daaraan gekoppelde Interne Verwijzingsregister (IVR) en de derde situatie is de verwerking van gegevens in het Incidentenregister en het daaraan gekoppelde Externe Verwijzingsregister (EVR). Op de eerste twee situaties zijn de Gedragscode Verwerking Persoonsgegevens Financiële Instellingen (Gvpfi) en de Wet bescherming persoonsgegevens (WBP) van toepassing, de derde verwerking is geregeld in het Protocol Incidentenwaarschuwingssysteem Financiële Instellingen (PIFI) dat geldt als uitwerking van de Gvpfi.

Volgnr.	Voorschrift	Uitwerking bij verzekeraar	Toelichting	Vindplaats in wet, gedragscode, protocol
42	Voor het sluiten van de verzekeringsovereenkomst mag verzekeringnemer gevraagd worden naar feiten betreffende zijn strafrechtelijk verleden betrekking hebbend op een periode tot 8 jaar voorafgaand aan de aanvraag tot verzekering. Het opgegeven strafrechtelijk verleden wordt slechts gebruikt in het kader van de beoordeling van de verzekeringsaanvraag.	Hanteer op aanvragen (schriftelijk/ elektronisch) voor een verzekering heldere en gerichte vragen naar het strafrechtelijk verleden.	Bij vragen naar het strafrechtelijk verleden is van cruciaal belang dat deze concreet en duidelijk is. Een te algemeen geformuleerde vraag omtrent het verleden is niet afdoende om een beroep op niet nakomen mededelingsplicht te doen. Zie ook de voorbeeldteksten van het Verbond van Verzekeraars (LV-2011/61).	Artikel 7:928 lid 5 BW Artikel 6.2.3 Gvpfi
43	Omgang met strafrechtelijke gegevens is toegelaten conform de toegestane doeleinden en grondslagen uit de Wbp. Daarbij moet sprake zijn van passende technische en/of procedurele waarborgen om te voorkomen dat strafrechtelijke gegevens worden gebruikt voor andere doeleinden dan waarvoor zij verkregen zijn.	Toets periodiek of medewerkers afdoende bekend zijn met de wettelijke voorschriften omtrent doel en grondslag voor verwerking en of deze worden nageleefd. Draag er zorg voor dat de doeleinden en grondslagen voor verwerking van strafrechtelijke gegevens transparant en tijdig bekend worden gemaakt aan medewerkers en aan cliënten.	Zorg er voor dat in het privacystatement op websites en in polisvoorwaarden de verwerking van persoonsgegevens in het kader van veiligheid en integriteit als een van de doeleinden voor verwerking is opgenomen.	Artikel 7 en 8 Wbp Artikel 13 Wbp Artikel 6.2 Gvpfi Artikel 5.1.1. onder d. GVPFI

44	De verwerking van persoonsgegevens in een Gebeurtenisadministratie geschiedt alleen ten behoeve van de eigen organisatie.	Draag er (organisatorisch / technisch) zorg voor dat gegevens uit de Gebeurtenissenadministratie uitsluitend intern gebruikt kunnen worden en niet aan derden beschikbaar worden gesteld.	Intern wil zeggen binnen de economische eenheid. Als de gegevens bij verschillende bedrijfsonderdelen raadpleegbaar zijn, moet aan de betrokkene duidelijk worden weergegeven waar zijn gegevens terecht kunnen komen.	Artikel 33 Wbp Artikel 5.5 Gvpfi
45	Verwerking van persoonsgegevens in een Gebeurtenissenadministratie kan binnen een organisatie door Veiligheidszaken of een daartoe aangewezen afdeling worden uitgevoerd. In de Gebeurtenissenadministratie komen gegevens: • die gelet op het bijzonder karakter van de financiële sector de zorg en aandacht van de financiële instelling behoeven; • over (potentiële) vorderingen; • over het niet nakomen van contractuele verplichtingen of andere (toerekenbare) tekortkomingen; • van handelingen van de instelling waaronder onderzoeken op grond van wettelijke verplichtingen.	Leg vast welke afdeling een Gebeurtenissenadministratie hanteert en voor welke aard van gegevens deze verwerking wordt gebruikt binnen de betreffende afdeling. Stel bedrijfsbeleid vast ten aanzien van omgang met signalen uit de Gebeurtenissenadministratie en het daaraan gekoppelde Interne Verwijzingsregister (IVR) door personeel op overige afdelingen (zie ook 47).	Omdat niet iedere gegevenssoort specifiek bedoeld is om te worden verwerkt door een Veiligheidszaken kunnen bepaalde verwerkingen door andere afdelingen worden uitgevoerd. De organisatie van bijvoorbeeld de afdeling Compliance aanwijzen om een Gebeurtenissenadministratie op het terrein van CDD controles of MOT meldingen te voeren.	Artikel 5.5.1 Gvpfi Artikel 5.6.1 Gvpfi
46	De Gebeurtenissenadministratie is bij het CBP gemeld.	Zorg voor melding van deze verwerking van persoonsgegevens bij het CBP of de eigen functionaris gegevensverwerking.	Bij de melding kunnen de categorieën worden opgegeven waarvoor gebeurtenissen worden vastgelegd (zie de limitatieve opsomming van de categorieën onder 45).	Artikel 27 e.v. Wbp Artikel 5.1.3 Gvpfi Artikel 5.5.1. GVPFI

47	Binnen de Gebeurtenisadministratie kunnen gegevens worden opgenomen in het Interne Verwijzingsregister (IVR). Het IVR is toetsbaar voor daartoe aangewezen functionarissen binnen de eigen organisatie.	Formuleer voorwaarden waaronder gegevens in het IVR worden geplaatst en door welke personeelleden deze mogen worden getoetst.	Het IVR is de deelverzameling van de Gebeurtenissenadministratie die door de overige personeelsleden getoetst kan worden. Het IVR bevat slechts een beperkte set gegevens (NAWG is afdoende). Het IVR is bedoeld als (systeem)oplossing om eigen personeel te kunnen attenderen op het feit dat persoonsgegevens in een Gebeurtenissenadministratie van een verzekeraar zijn opgenomen. Met een IVR kan technisch worden geregeld dat niet ieder personeelslid de volledige inhoud van een dossier in de Gebeurtenissenadministratie kan inzien.	Artikel 5.5.1 Gvpfi Zie ook de toelichting op de Gvpfi, pagina 28
48	Het Incidentenregister is ondergebracht bij Veiligheidszaken als bedoeld in het Protocol Incidentenwaarschuwingssysteem Financiële instellingen (PIFI).	Zorg dat de verwerking (organisatorisch en technisch) alleen door Veiligheidszaken wordt uitgevoerd en andere medewerkers geen toegang hebben tot het Incidentenregister.	Veiligheidzaken is de afdeling of persoon die verantwoordelijk is voor de verwerking van persoonsgegevens op het gebied van veiligheid en integriteit.	Artikel 5.5.2 Gvpfi
49	Het Incidentenregister is gemeld bij het CBP.	Stel vast of aanmelding van deze verwerking bij het CBP op de juiste wijze heeft plaatsgevonden en de organisatie is vermeld op de lijst van PIFI deelnemers.	Op grond van artikel 31 lid 3 Wbp is geen Voorafgaand Onderzoek nodig. Het PIFI is bij het CBP beoordeeld en voorzien van een rechtmatigheidverklaring. Bij de melding van deze verwerking aan het CBP moet een getekende toetredingsverklaring tot en een exemplaar van het PFI worden meegezonden. Een toetredingsverklaring kan worden opgevraagd bij het Verbond van Verzekeraars/Centrum Bestrijding Verzekeringscriminaliteit.	Artikel 27 e.v. Wbp Artikel 31 Wbp Artikel 3.1.1 PIFI Artikel 5.1.3 jo. artikel 5.5.2 Gvpfi
50	Bij de melding aan het CBP is het doel omschreven als vastgelegd in artikel 4.1.1 van het PIFI.	Controleer of de doelomschrijving in de melding bij het CBP identiek is aan het PIFI.		Artikel 3.1.1. PIFI Artikel 4.1.1. PIFI Artikel 5.5.2 Gvpfi

51	De gegevens in het Incidentenregister zijn alleen toegankelijk voor Veiligheidszaken.	Zorg dat autorisaties voor toegang, organisatorisch en technisch, duidelijk zijn vastgelegd en gewaarborgd.	Gezien de gevoeligheid van de gegevens is een hoge mate van beveiliging en afscherming noodzakelijk.	Artikel 13 Wbp Artikel 3.5 PIFI Artikel 8.3.1 Gvpfi
52	Bij toetsing van het Extern Verwijzingsregister (EVR) wordt bij een 'hit' door Veiligheidszaken contact opgenomen met de primaire bron van de EVR.	Zorg voor naleving van het toetsingsproces conform het PIFI. Informeer personeelsleden met toetsingsbevoegdheid periodiek over de verplichte stappen bij het aantreffen van een EVR.	Het PIFI stelt het contactleggen na het aantreffen van een EVR verplicht. Omdat de informatie-uitwisseling is voorbehouden aan Veiligheidszaken moet het eigen personeel bij het treffen op een EVR in het landelijk waarschuwingssysteem altijd in contact treden met de eigen veiligheidsafdeling.	Artikel 3.2.1 e.v. PIFI
53	Invoer van gegevens in het incidentenregister en in het EVR vindt plaats volgens de voorschriften van het PIFI. De persoonsgegevens moeten legaal zijn verkregen en tot de bron gedocumenteerd herleidbaar zijn.	Controleer of medewerkers Veiligheidzaken bekend zijn met de werking van het Incidentenregister en de regels uit het PIFI voor invoer van gegevens in het Incidentenregister en EVR. Zorg dat herkomst van de gegevens en besluitvorming tot verwerking daarvan is vastgelegd in het betreffende dossier.	In het PIFI is nauwkeurig voorgeschreven waaraan moet worden voldaan om een gebeurtenis ook als incident te kunnen kwalificeren. Plaatsing van gegevens in het EVR is verplicht voor de deelnemers aan het PIFI zodra is vastgesteld dat aan de criteria voor registratie is voldaan.	Artikel 3.3.1 PIFI Artikel 4.1.1 PIFI Artikel 5.2.1 PIFI Artikel 5.5.2 Gvpfi
54	De gegevens die conform PIFI worden verwerkt moeten strikt vertrouwelijk worden behandeld en de organisatie moet voorzieningen treffen die waarborgen dat de aangewezen medewerker onder een geheimhoudingsplicht valt.	Medewerkers Veiligheidzaken moeten een geheimhoudingsverklaring tekenen bij indiensttreding.		Artikel 3.4 PIFI
55	De verwerking is beschermd tegen verlies of enige vorm van onrechtmatige verwerking.	Zorg voor optimale technische en organisatorische maatregelen ter beveiliging van de gegevens.	Hoewel deze gegevensbeveiliging deel kan uitmaken van het gehele beveiligingsbeleid, vraagt verwerking van bijzondere persoonsgegevens extra waarborgen gezien de aard van de gegevens.	Artikel 13 Wbp Artikel 3.5 PIFI

	Rekening houdend met de stand van de techniek en de kosten voor tenuitvoerlegging moeten de maatregelen een passend beveiligingsniveau hebben.	Controleer periodiek of (nog) sprake is van afdoende beveiliging van de gegevens in het Incidentenregister. Leg de overwegingen voor de gekozen aard en omvang van de beveiligingsmaatregelen vast.		
56	De gegevens uit het Incidentenregister mogen slechts worden uitgewisseld met de personen en instanties als genoemd in het PIFI.	Controleer periodiek of uitwisseling binnen de PIFI kaders plaatsvindt door na te gaan aan welke personen informatie uit het Incidentenregister is verstrekt.	Gegevens van incidenten mogen alleen op het niveau van Veiligheidszaken worden uitgewisseld. Om de eigen organisatie te kunnen informeren kan het, aan de Gebeurtenissenadministratie gekoppelde IVR, gebruikt worden.	Artikel 4.2 en 5.4 PIFI
57	Gegevens worden verwijderd uit het Incidentenregister uiterlijk 8 jaar na opname, tenzij zich een nieuwe aanleiding voor opname heeft voorgedaan	Zorg dat gegevens na acht jaar worden verwijderd uit het Incidentenregister. Zorg in voorkomende gevallen dat op dossierniveau wordt vastgelegd waarom de bewaartermijn is verlengd.	Als waarborg voor tijdige verwijdering kan dit deel uitmaken van een geautomatiseerd proces binnen de administratie van Veiligheidszaken.	Artikel 4.3 PIFI
58	Opname in het EVR vindt plaats indien: a. de gedraging(en) van de (rechts)persoon een bedreiging vormden, vormen of kunnen vormen voor de (financiële) belangen van cliënten en/of medewerkers van een financiële instelling, alsmede de (organisatie van de) financiële instelling zelf of de continuïteit en/of integriteit van de financiële sector; b. in voldoende mate vaststaat dat de (rechts) persoon betrokken is bij die gedraging(en) als bedoeld onder a;	Zorg dat EVR registraties voldoen aan de criteria uit het PIFI en controleer of de besluitvorming wordt gedocumenteerd in het Incidentenregister. Als aan de criteria voor een EVR registratie wordt voldaan, wordt deze in het landelijk waarschuwingssysteem geplaatst. Zorg dat een EVR alleen geplaatst kan worden als een tweede beoordelaar het incident/dossier ook onderzocht heeft.	Deze voorwaarden vormen de kern van het waarschuwingssysteem. De criteria geven de grenzen wanneer gegevens over (rechts)personen met andere deelnemers aan het PIFI mogen worden uitgewisseld.	Artikel 5.2.1 PIFI

	c. het proportionaliteitsbeginsel in acht is genomen.			
59	EVR meldingen worden verwijderd uiterlijk 8 jaar na opname, tenzij zich een nieuwe aanleiding voor opname heeft voorgedaan.	Controleer of EVR meldingen gelijktijdig met de verwijdering van de gegevens uit het Incidentenregister plaatsvindt (zie onder 59). Zorg in voorkomende gevallen dat op dossierniveau wordt vastgelegd waarom de bewaartermijn is verlengd.		Artikel 5.3 PIFI
60	Deelname aan het EVR is alleen toegestaan indien de organisatie deelnemer is conform het PIFI en een toetredingsverklaring heeft ondertekend.	Controleer of wordt voldaan aan de voorwaarden voor deelname en een afschrift van de ondertekende toetredingsverklaring, zoals die aan het CBP bij de melding van de verwerking is verstrekt, aanwezig is.	Deelname staat open voor leden van de bij PIFI aangesloten brancheverenigingen die een Incidentenregister hebben aangemeld bij het CBP en de toetredingsverklaring hebben ondertekend.	Artikel 2 PIFI (begrip ‘deelnemer’) Artikel 3.1.1 PIFI Artikel 7 PIFI
61	Werkwijze voor toepassing van het Incidentenregister en de toetsing van het EVR, zoals neergelegd in het PIFI, zijn geconcretiseerd in werkprocessen.	Zorg voor procesbeschrijvingen conform het PIFI voor Veiligheidzaken en overige betrokken organisatieonderdelen. Controleer periodiek of de processen (nog) in lijn met het PIFI beschreven zijn en worden toegepast.		Artikel 8.4.1 PIFI
62	Betrokkenen hebben recht op informatie over de registratie in het Incidentenregister en het EVR, recht op inzage en correctie en recht van verzet.	Zorg dat betrokkenen afdoende, duidelijk en tijdig worden geïnformeerd over verwerking van hun gegevens.	.	Artikel 33-36 Wbp Artikel 41 Wbp Artikel 9.1, 9.3, 9.4 en 9.5 PIFI

		Wijs betrokkenen op hun rechten ten aanzien van inzage, correctie en verzet. In geval van verzet wordt: • de betreffende verwerking direct beëindigd; • betrokkene op zijn verzoek binnen vier weken geïnformeerd over de genomen maatregelen. Zorg dat de motivering voor afwijking van de informatieplicht of het recht op inzage in voorkomende gevallen in het dossier wordt vastgelegd.		
63	Bij geschillen kan betrokkene binnen de organisatie terecht bij bestuur/directie als voorportaal van de beroepsmogelijkheden.	Draag zorg voor een klachtenprocedure en zie erop toe dat de klachtenfunctionarissen afdoende kennis hebben van het PIFI. Bij beantwoording van klachten wordt betrokkene gewezen op de beroepsmogelijkheden bij Kifid en SKGZ, CBP en bevoegde rechter.		Artikel 10 PIFI