

Matrix informatie-uitwisseling								
Hoofregel: Je mag gegevens verstrekken aan derden indien je dit op grond van wetgeving, regelgeving, reglementen of protocollen bevoegd/verplicht bent.								
Om welke informatie gaat het?	Wie (van je eigen bedrijf) mag informatie verstrekken?	Wie (extern) mag informatie bij je opvragen?	Informatie verstrekken?	Toestemming nodig?	Welke informatie mag je geven?	Wat mag de derde-ontvanger met deze gegevens doen?	Wat is dit?	Toelichting
Claimmeldingen uit eigen bestanden of eigen claimmeldingen uit de CIS databank	Iedereen die geautoriseerd is tot het schadedossier	* Een acceptatiemedewerker in het kader van de behandeling van een verzekeringsaanvraag * Een schadebehandelaar in het kader van de behandeling van een schadeclaim * Een medewerker Veiligheidszaken (1) in het kader van onderzoeksactiviteiten	Nee, tenzij deze als claimmelding is opgenomen in de CIS databank of als de betrokkene toestemming heeft gegeven.	Indien de claimmelding in de CIS databank is opgenomen is er geen toestemming nodig.	Uitsluitend relevante verzekeringsgegevens die nodig zijn om de vraag te kunnen beantwoorden. De vrager moet aangeven waarom hij over de informatie wil beschikken. Informatie beperken tot relevante gegevens. Je mag alleen detailinformatie verstrekken over de registraties in de CIS databank die door jouw eigen organisatie daarin zijn vastgelegd. Het is niet toegestaan om bijzondere persoonsgegevens te verstrekken.	De gegevens uit de CIS databank mogen uitsluitend worden ingezet als hulpmiddel bij controle van de informatie die betrokkene zelf aan de verzekeraar of gevolmachtigde heeft verstrekt. Daarbij gaat het in het bijzonder om: - inschatting van het moreel risico bij beoordeling van een nieuwe klant of opgegeven wijziging door een klant (heeft betrokkene bijvoorbeeld zijn verzekeringsverleden naar waarheid vermeld op zijn aanvraag voor een nieuwe of aangepaste verzekering); - het tegengaan van verzekeringsfraude door controle op claim(gedrag); - waarschuwingen over eerder onrechtmatig handelen tegen een financiële instelling.	Alle claimmeldingen die door verzekeraars en gevolmachtigden worden ontvangen. Het maakt daarbij niet uit wie er schuld heeft aan een schade of dat een schade niet gedekt is volgens de polisvoorwaarden. Het gaat alleen maar om de registratie van het feit dat iemand aanspraak maakt op verzekeringsdekking. Van iedere claim worden alleen de feitelijke gegevens en de persoonsgegevens van de betrokkenen vastgelegd. Zie voor nadere informatie het document "definitie 'claimmelding' in de CIS databank". Daarnaast kan een organisatie claimmeldingen in eigen bestanden geregistreerd hebben zonder deze op te nemen in de CIS databank.	Gegevens uit de CIS databank mogen worden gebruikt bij acceptatie en/of schade, als de registrerende weet dat voor dit doel zijn gegevens in de CIS databank zijn vastgelegd. Tijdens het aanvraagproces mogen de gegevens uit de CIS databank pas gebruikt worden als er naar het schadeverleden is gevraagd. Elke betrokkene moet worden ingelicht dat zijn (persoons)gegevens in de CIS databank worden vastgelegd. Ook bijvoorbeeld een tegenpartij of een bestuurder van een auto, die niet verzekeringnemer is, dient geïnformeerd te worden. Doel: - bij acceptatie: toetsen of de vragen op de aanvraag juist zijn beantwoord (moraliteitstoets); - bij schade: controle op eerdere of dubbele claims of ter controle van het feit of bij de aanvraag aan de mededelingsplicht is voldaan (rekening houdend met artikel 7:928 lid4 BW).
Polisgegevens uit eigen bestanden	Iedereen die geautoriseerd is tot de eigen polisadministratie	* Een acceptatiemedewerker in het kader van de behandeling van een verzekeringsaanvraag * Een schadebehandelaar in het kader van de behandeling van een schadeclaim * Een medewerker Veiligheidszaken (1) in het kader van onderzoeksactiviteiten	Nee, tenzij de betrokkene toestemming heeft verleend. Op grond van de samenwerkings- dan wel uitbestedingsovereenkomst mag informatie uitgewisseld worden tussen gevolmachtigde en verzekeraar zonder toestemming van de betrokkene.	Ja Toestemming is niet vereist indien de informatieverstrekking voldoet aan de bepalingen van artikel 3.2 van het PIFI, en in het bijzonder artikel 3.2.3.	Uitsluitend relevante verzekeringsgegevens die nodig zijn om de vraag te kunnen beantwoorden. De vrager moet aangeven waarom hij over de informatie wil beschikken en de toestemming van de betrokkene kunnen overleggen. Informatie beperken tot relevante gegevens. Het is niet toegestaan om bijzondere persoonsgegevens te verstrekken.	De ontvangen informatie mag uitsluitend gebruikt worden voor het doel waarvoor deze is opgevraagd.	Alle polisgegevens die door verzekeraars en gevolmachtigden zijn vastgelegd van een bepaald persoon of object.	
Vertrouwelijke Mededelingen algemeen (code 2)	Medewerkers die op grond van hun taak en werkzaamheden rechtstreeks toegang hebben tot de Vertrouwelijke Mededelingen in de CIS databank.	* Een acceptatiemedewerker in het kader van de behandeling van een verzekeringsaanvraag * Een schadebehandelaar in het kader van de behandeling van een schadeclaim * Een medewerker Veiligheidszaken (1) in het kader van onderzoeksactiviteiten	Ja	Nee	Uitsluitend relevante verzekeringsgegevens die nodig zijn om de vraag te kunnen beantwoorden. De vrager moet aangeven waarom hij over de info wil beschikken. Je mag alleen detailinformatie verstrekken over de registraties in de CIS databank die door jouw eigen organisatie daarin zijn vastgelegd. Niet verstrekken: bijzondere persoonsgegevens.	Controle op nakomen van de mededelingsplicht en toetsen eigen acceptatiebeleid. Het feit dat een aspirant-verzekerde een registratie heeft wegens het niet nakomen van zijn contractuele verplichtingen (Code 2) mag als een op zichzelf staand feit niet als aanleiding worden gebruikt om de aanvraag van de betrokkene af te wijzen. De registratie kan bijvoorbeeld wel aanleiding vormen nadere informatie bij de betrokkene in te winnen of kan leiden tot het stellen van nadere voorwaarden met betrekking tot de onderliggende verzekering.	Opzegging van een verzekering door een verzekeraar of gevolmachtigde omdat een verzekerde zijn contractuele verplichtingen niet is nagekomen. Het betreft geen non-premiebetaling. Deze registratie mag pas geplaatst worden als is voldaan aan de voorwaarden opgenomen in het document Vertrouwelijke Mededeling van CIS (te vinden op de website van CIS of www.CISSystems.nl).	De Vertrouwelijke Mededeling Code 2 is niet toe te passen in geval een aspirant-verzekerde zijn wettelijke mededelingsplicht schendt (artikel 7:928 BW) gedurende het acceptatietraject. Omdat de Vertrouwelijke Mededeling betrekking heeft op een roeyment op initiatief van de verzekeraar moet een verzekeringsovereenkomst eerst tot stand zijn gekomen. Niet gebruiken als enige reden voor non-acceptatie. De informatie in de CIS databank kan slechts in combinatie met andere beschikbare informatie van of over betrokkene, en met inachtneming van het acceptatiebeleid van de deelnemer, worden toegepast.
Vertrouwelijke Mededelingen financieel (code 2a)	Medewerkers die op grond van hun taak en werkzaamheden rechtstreeks toegang hebben tot de Vertrouwelijke Mededelingen in de CIS databank.	* Een acceptatiemedewerker in het kader van de behandeling van een verzekeringsaanvraag * Een schadebehandelaar in het kader van de behandeling van een schadeclaim * Een medewerker Veiligheidszaken (1) in het kader van onderzoeksactiviteiten	Ja	Nee	Uitsluitend relevante verzekeringsgegevens die nodig zijn om de vraag te kunnen beantwoorden. De vrager moet aangeven waarom hij over de info wil beschikken. Je mag alleen detailinformatie verstrekken over de registraties in de CIS databank die door jouw eigen organisatie daarin zijn vastgelegd. Niet verstrekken: bijzondere persoonsgegevens.	Controle op nakomen van de mededelingsplicht en toetsen eigen acceptatiebeleid. Het feit dat een aspirant-verzekerde een registratie heeft wegens het niet nakomen van zijn financiële contractuele verplichtingen (VM code 2a) mag als een op zichzelf staand feit niet als aanleiding worden gebruikt om de aanvraag van de betrokkene af te wijzen. De registratie kan bijvoorbeeld wel aanleiding vormen voor een betere debiteurbewaking op de bewuste relatie of het stellen van nadere voorwaarden met betrekking tot automatische incasso e.d.	Opzegging van een verzekering door een verzekeraar omdat een verzekeringnemer zijn contractuele financiële verplichtingen niet is nagekomen. Deze registratie mag pas geplaatst worden als is voldaan aan de voorwaarden opgenomen in het document Werkinstructie en voorschriften Vertrouwelijke Mededeling van CIS (te vinden op de website van CIS of www.CISSystems.nl).	Niet gebruiken als enige reden voor non-acceptatie. De informatie in de CIS databank kan slechts in combinatie met andere beschikbare informatie van of over betrokkene, en met inachtneming van het acceptatiebeleid van de deelnemer, worden toegepast. Code 2a wordt alleen extern getoond na een tweede registratie binnen drie jaar na eerste registratie. Zie voor meer informatie de Werkinstructie en Voorschriften VM van CIS.

Gebeurtenisadministratie (GA)	De afdeling Veiligheidszaken (1) of een daartoe aangewezen afdeling. Valt onder de Gedragscode Verwerking Persoonsgegevens Verzekeraars.	Intern binnen de eigen organisatie: alle medewerkers voor zover noodzakelijk voor de uitvoering van hun werkzaamheden. Extern: niemand.	Intern: Ja Extern: Nee	N.v.t.	De afdeling Veiligheidszaken (1) of een andere daartoe aangewezen afdeling adviseert de behandelaar. Inhoudelijke informatie mag niet worden gedeeld.	N.v.t.	De verwerking van persoonsgegevens in verband met een voorval dat de aandacht verlangt van een verzekeraar of een gevolmachtigde vanwege een mogelijk effect op de veiligheid en integriteit van de bedrijfsvoering, werknemers, klanten, overige relaties en de verzekeringsbranche. Hieronder valt bijvoorbeeld mogelijke fraude of ander laakbaar of onrechtmatig gedrag, potentiële en daadwerkelijke vorderingen, onder meer ten aanzien van een met een verzekeraar gesloten overeenkomst en het niet nakomen van contractuele verplichtingen of andere (toerekenbare) tekortkomingen.	
Interne verwijzingsregister (IVR)	De afdeling Veiligheidszaken (1) of een daartoe aangewezen afdeling. Valt onder de Gedragscode Verwerking Persoonsgegevens Verzekeraars.	Intern binnen de eigen organisatie: alle medewerkers voor zover noodzakelijk voor de uitvoering van hun werkzaamheden. Extern: niemand.	Intern: Ja Extern: Nee	N.v.t.	Voor zover relevant kan een medewerker voor zover noodzakelijk voor zijn werkzaamheden zelf het IVR raadplegen. Voor wat betreft inhoudelijke informatie, zie Gebeurtenisadministratie	N.v.t.	De deelverzameling van de Gebeurtenisadministratie van de verzekeraar of de gevolmachtigde, die uitsluitend verwijzingsgegevens bevat met betrekking tot (rechts)personen en bestemd is voor intern gebruik binnen de maatschappij of Groep, in overeenstemming met artikel 7.11.1. van de Gedragscode Verwerking Persoonsgegevens Verzekeraars. Belangrijk: Gevolmachtigden maken geen onderdeel uit van de groep waartoe de verzekeraar behoort.	
Incidentenregister (IR)	Een medewerker Veiligheidszaken (1) van een Deelnemer conform art. 7.1 van het Protocol Incidentenwaarschuwingssysteem Financiële Instellingen (PIFI), die op grond van hun taak en werkzaamheden rechtstreeks toegang hebben tot het incidentenregister. En medewerkers van het Fraudeloket van het Verbond van Verzekeraars in het kader van hun coördinatiefunctie. Belangrijk: Gevolmachtigden zijn géén Deelnemer aan het PIFI. Zie de kolom Toelichting voor meer informatie.	Een medewerker Veiligheidszaken (1) van een Deelnemer conform art. 7.1 PIFI, uitsluitend als is voldaan aan de vereisten van subsidiariteit en proportionaliteit. En medewerkers van het Fraudeloket van het Verbond van Verzekeraars in het kader van hun coördinatiefunctie. Belangrijk: Gevolmachtigden zijn géén Deelnemer aan het PIFI. Zie de kolom Toelichting voor meer informatie.	Ja , uitsluitend aan een medewerker Veiligheidszaken (1) en het Fraudeloket. En mits is voldaan aan de bepalingen uit artikel 9 PIFI, en in het bijzonder 9.1.	Nee	Alle relevante gegevens van het Incident, mits voldaan wordt aan de voorwaarden als beschreven in art. 3.2 (bij onderzoek) of 3.3 (bij toetsing) PIFI. De interne afwegingen rond de bevraging en verstrekking worden door de respectievelijke afdelingen Veiligheidszaken vastgelegd in de administratie.	De gegevens mogen worden gebruikt conform de doelomschrijving van het PIFI (art. 4.1.1 PIFI) en uitsluitend als door de bron van de informatie is voldaan aan de bepalingen uit art. 9.1 PIFI.	De gegevensverzameling(en) van een PIFI Deelnemer, waarin gegevens zijn vastgelegd voor het ondersteunen van activiteiten gericht op het waarborgen van de veiligheid en de integriteit van de financiële sector, naar aanleiding van of betrekking hebbend op een (mogelijk) incident.	Gevolmachtigden voldoen niet aan de definitie van een Deelnemer conform art. 7.1 van het PIFI, maar kunnen worden gerekend tot de organisatie van de Deelnemer. Hierdoor is het voor gevolmachtigden wel toegestaan te toetsen aan het externe waarschuwingssysteem (EVR) maar hebben ze geen toegang tot de informatie in het Incidentenregister van de afdeling Veiligheidszaken van de PIFI Deelnemer. Om te kunnen toetsen moet de gevolmachtigde bij de volmachtgevende verzekeraar zijn aangehaakt op diens vergunning (van de Autoriteit Persoonsgegevens) tot het verwerken van strafrechtelijke persoonsgegevens ten behoeve van derden. De gevolmachtigde moet bij het treffen van een EVR contact opnemen met de afdeling Veiligheidszaken van de PIFI deelnemende, risicodragende verzekeraar.
Externe verwijzingsregister (EVR)	Een medewerker Veiligheidszaken (1) van een Deelnemer conform art. 7.1 van het Protocol Incidentenwaarschuwingssysteem Financiële Instellingen (PIFI), die op grond van hun taak en werkzaamheden rechtstreeks toegang hebben tot het incidentenregister. Belangrijk: Gevolmachtigden zijn géén Deelnemer aan het PIFI. Zie de kolom Toelichting voor meer informatie.	Een medewerker Veiligheidszaken (1) van een Deelnemer conform art. 7.1 PIFI, die op grond van hun taak en werkzaamheden rechtstreeks toegang hebben tot het incidentenregister. En medewerkers van het Fraudeloket van het Verbond van Verzekeraars in het kader van hun coördinatiefunctie. Belangrijk: Gevolmachtigden zijn géén Deelnemer aan het PIFI. Zie de kolom Toelichting voor meer informatie.	Ja , informatie uit het Incidentenregister mag uitsluitend worden verstrekt aan een medewerker Veiligheidszaken (1) en het Fraudeloket. En mits is voldaan aan de bepalingen uit artikel 9 PIFI, en in het bijzonder 9.1.	Nee	Alle relevante gegevens van het Incident, mits voldaan wordt aan de voorwaarden als beschreven in art. 3.2 (bij onderzoek) of 3.3 (bij toetsing) PIFI. De interne afwegingen rond de bevraging en verstrekking worden door de respectievelijke afdelingen Veiligheidszaken vastgelegd in de administratie.	De gegevens mogen worden gebruikt conform de doelomschrijving van het PIFI (art. 4.1.1 PIFI) en uitsluitend als door de bron van de informatie is voldaan aan de bepalingen uit art. 9.1 PIFI. Belangrijk: Het is niet toegestaan om een verzekeringsaanvraag af te wijzen alleen op grond van de verwijzingsgegevens (de EVR). Er moet altijd een acceptatie-advies geformuleerd worden door Veiligheidszaken op grond van de achterliggende incidentinformatie.	Verwijzingsgegevens van personen die conform art. 5.2 PIFI betrokken zijn geweest bij een gebeurtenis die als gevolg heeft, zou kunnen hebben of heeft gehad dat de belangen, integriteit of veiligheid van de cliënten of medewerkers van een financiële instelling, de financiële instelling zelf of de financiële sector als geheel in het geding zijn of kunnen zijn. Bijvoorbeeld verzekeringsfraude of bij de aanvraag van een verzekering aantoonbaar opzettelijk niet de volledige waarheid vertellen.	Gevolmachtigden voldoen niet aan de definitie van een Deelnemer conform art. 7.1 van het PIFI, maar kunnen worden gerekend tot de organisatie van de Deelnemer. Hierdoor is het voor gevolmachtigden wel toegestaan te toetsen aan het externe waarschuwingssysteem (EVR) maar hebben ze geen toegang tot de informatie in het Incidentenregister van de afdeling Veiligheidszaken van de PIFI Deelnemer. Om te kunnen toetsen moet de gevolmachtigde bij de volmachtgevende verzekeraar zijn aangehaakt op diens vergunning (van de Autoriteit Persoonsgegevens) tot het verwerken van strafrechtelijke persoonsgegevens ten behoeve van derden. De gevolmachtigde moet bij het treffen van een EVR contact opnemen met de afdeling Veiligheidszaken van de PIFI deelnemende, risicodragende verzekeraar.
Ontzegging Rijbevoegdheid	Niet van toepassing	Niet van toepassing	Nee	N.v.t.	Niet van toepassing	Niet van toepassing	Gevalen waarin de rechter heeft bepaald dat betrokkene (tijdelijk) geen motorrijtuig mag besturen. De ontzeggingen rijbevoegdheid zijn zichtbaar in de CIS databank.	Verzekeraars en/of gevolmachtigden mogen deze gegevens alleen gebruiken voor verzekeringen van het verkeersrisico van motorrijtuigen en aanhangwagens. De gegevens van de rijontzeggingen worden aangeleverd door de overheid en niet door verzekeraars of gevolmachtigden. Wanneer een ontzegging van de rijbevoegdheid in de CIS databank geregistreerd is, en betrokkene is het daar niet mee eens, kan CIS of de verzekeraar en/of gevolmachtigde geen bemiddelende rol spelen. Voor een discussie over de juistheid van een geregistreerde rijontzegging moet men contact opnemen met het parket van het Openbaar Ministerie van de Rechtbank, die de rijontzegging heeft opgelegd.

(1) Veiligheidszaken: de persoon of afdeling die verantwoordelijk is voor de verwerking van persoonsgegevens in het kader van het waarborgen van veiligheid en integriteit. Deze medewerkers mogen 1) kennis nemen van, 2) muteren in, en 3) informatie delen uit het incidentenregister van hun organisatie.

DISCLAIMER: Hoewel deze matrix uitsluitend tot doel heeft om verdere verdieping te geven op bestaande regelgeving, gedragscodes en protocollen kunnen hieraan geen rechten worden ontleend. Deze matrix heeft niet het oogmerk om tussen marktpartijen afspraken te maken, die de vrije markwerking zouden kunnen beïnvloeden. Raadpleeg voor alle regels en voorschriften rond informatiedeling altijd actuele protocollen en gedragscodes.
Zonder toestemming van de auteurs mogen in dit overzicht geen wijzigingen worden aangebracht (© Boshuizen, Greijdanus, Van Gaalen, Vijverberg 2022).