Commission Cyber

Note Risque de cumuls Cyber en RC

Juin 2024

Executive Summary

In a guide published in 2023, France Assureurs examines the accumulation of standard and cyber insurance policies in France. This note analyzes, from the reinsurers' perspective, scenarios of claims involving both liability and cyber policies. It highlights the difficulty of clearly delineating coverage between these policies, with liability policies generally being on an "all risks except" basis, while cyber policies focus on purely financial damages that are already potentially covered by liability policies but with generally lower limits. Three potential accumulation scenarios are studied: medical, financial, and large-scale cyber-attacks.
Apref recommends paying attention to this issue: while the potential for significant accumulation following a cyber event is accounted for in the structure of cyber treaties, which are almost always well limited per year, this is not necessarily the case in liability treaties.

Synthèse de la note

Dans un guide publié en 2023, France Assureurs examine le cumul des polices standards et cyber en France. La présente note analyse, du point de vue des réassureurs, des scénarios de sinistres impliquant à la fois des polices RC et cyber. Elle souligne la difficulté de délimiter clairement les couvertures entre ces polices, les polices RC étant généralement sur une base « tous risques sauf », tandis que les polices cyber se concentrent sur les dommages purement financiers déjà potentiellement couverts par les polices RC mais avec des limites généralement plus faibles. Trois scénarios de cumul potentiel sont étudiés : médical, financier et attaques informatiques à grande échelle.
L'Apref recommande de porter attention à ce sujet : si le potentiel de cumuls importants à la suite d'un fait générateur cyber est pris en compte par la structure des traités cyber, lesquels sont presque toujours bien limités par année, tel n'est pas nécessairement le cas dans les traités RC.

APREF (Association des Professionnels de la Réassurance en France)
22-24 Rue de Courcelles, 75008 Paris – Tél : +33 (0)1 44 35 31 36 – secretariat@apref.org
www.apref.org

Table de matières

1. Introduction
2. La délimitation entre contrat cyber et contrat RC, un exercice peu aisé
   2.1. Définition du risque cyber
   2.2. Le risque cyber est issu de la digitalisation de la société, et ne coïncide pas avec l'articulation classique des contrats d'assurance
   2.3. Par essence, les polices RC et cyber couvrent à leur manière des sinistres similaires
3. Problématique du cumul en RC
   3.1. Scenario RC médical « corporel »
   3.2. Scenario RC « financier »
   3.3. Scénario d'attaque informatique à large échelle
4. Conclusion

Note Apref

1. Introduction

Dans un guide Cyber[1] publié en 2023, France Assureurs met en lumière la possibilité de cumul entre polices standards et cyber en France. En complément de ce guide, l'objectif de la présente note est d'étudier du point de vue du réassureur, des scénarios qui pourraient déclencher un nombre important de polices de responsabilité civile (RC) et/ou cyber simultanément.
Après avoir présenté le risque cyber et la problématique des cumuls possibles avec les contrats RC, trois scénarios sont présentés et leur potentiel d'accumulation analysé.

[1] *Points d'attention dans la rédaction des contrats d'assurance de dommages aux biens, de responsabilité et cyber face aux risques CYBER* – Frances Assureurs

APREF (Association des Professionnels de la Réassurance en France)
22-24 Rue de Courcelles, 75008 Paris – Tél : +33 (0)1 44 35 31 36 – secretariat@apref.org
www.apref.org

2. La délimitation entre contrat Cyber et contrat RC, un exercice peu aisé !

2.1 Définition du risque Cyber

Avant toute chose, il est primordial de définir le risque cyber. La définition le plus communément acceptée est la suivante :

Tout risque issu de l'utilisation de la technologie de l'information et de la communication qui compromet la Confidentialité et/ou Disponibilité et/ou L'intégrité des données, des infrastructures et systèmes d'informations d'une entreprise, d'une administration ou toutes autres entités.
Cette compromission pouvant résulter d'un **acte malveillant (externe ou interne)** ou être de **nature accidentelle**.

L'arrêté du 13 décembre 2022 relatif à la classification des engagements d'assurance consécutifs aux atteintes aux systèmes d'information et de communication a créé deux catégories ministérielles, ce qui devrait permettre de mesurer le développement de l'assurance cyber en France. Cependant, le risque cyber n'est pas encore considéré comme une branche d'assurance à part entière.

2.2 Le risque cyber est issu de la digitalisation de la société, et ne coïncide pas avec l'articulation classique des contrats d'assurance

L'avènement et la généralisation de l'informatique et des réseaux interconnectés a réduit certains risques (aide à la conduite, domotique, détections de fautes, alertes automatisées, etc.) mais en a créé d'autres, comme les cyber attaques.
Cependant, ces risques directement liés aux technologies ne suivent pas le découpage classique des contrats d'assurance dommages aux biens (DAB) et RC. En effet, une attaque cyber peut donner lieu à des dommages matériels/corporels ou immatériels, elle peut engager la responsabilité de l'assuré, ou non. Les polices d'assurance Cyber viennent finalement combler des déficits de couverture pour des incidents cyber dont les conséquences ne seraient pas, peu ou mal couvertes par des polices DAB ou RC.

APREF (Association des Professionnels de la Réassurance en France)
22-24 Rue de Courcelles, 75008 Paris – Tél : +33 (0)1 44 35 31 36 – secretariat@apref.org
www.apref.org

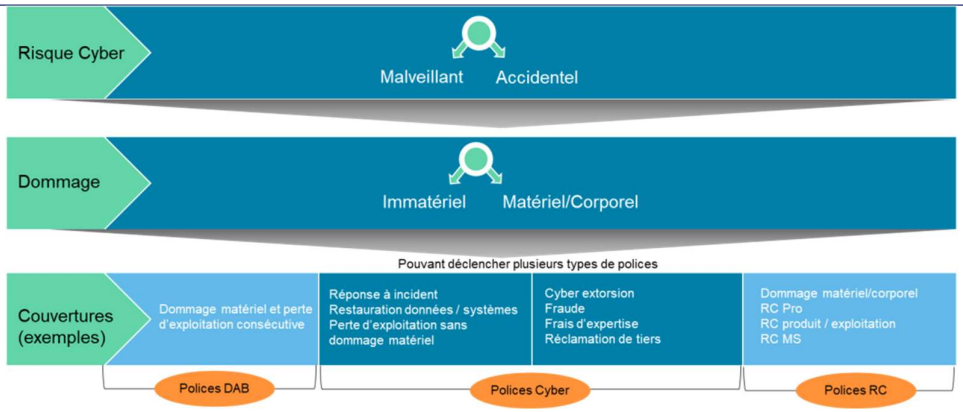


Figure 1 : du fait générateur à la couverture d'assurance (source : SCOR)

2.3 Par essence, les polices RC et Cyber couvrent à leur manière des sinistres similaires

- **Les polices RC sont traditionnellement rédigées sur une base « tous risques sauf »** de telle sorte que le périmètre et l'étendue des garanties dépendent :
  - ✓ Des exclusions
  - ✓ Des sous-limites applicables à telle ou telle garantie (nous trouvons par exemple fréquemment des sous-limites pour les Dommages immatériels non consécutifs – DINC)

  Concernant plus spécifiquement la garantie cyber, les polices RC ont vocation à couvrir les dommages matériels, corporels et dommages immatériels consécutifs. Pour les sinistres immatériels (purement financiers), la couverture est accordée au travers des DINC, avec ou sans sous-limite.
  Depuis le début des années 2020, sous la pression croissante des régulateurs, le marché tente de plus en plus de clarifier la composante cyber des polices RC (introduction d'exclusions plus ou moins larges, comme les DINC ou les attaques cyber malveillantes externes, etc.). La plupart des solutions mises en place pour les portefeuilles de PME (souvent en tacite reconduction) concernent principalement les affaires nouvelles et/ou mouvementées. Pour les grands comptes en revanche, les assureurs ont une approche plus systématique de clarification.

- **Les polices cyber, quant à elles, ont pour vocation de couvrir les dommages purement financiers de l'assuré** à l'exclusion des dommages matériels – corporels et dommages immatériels consécutifs. Elles proposent généralement également des garanties qui couvrent la responsabilité civile de l'assuré, par exemple, en cas d'atteinte à la confidentialité des données ou de transmission de virus à un tiers. Ainsi, et contrairement à la dimension dommages, la police cyber couvre un risque qui est déjà potentiellement couvert par la police RC, mais avec des limites généralement plus faibles.

APREF (Association des Professionnels de la Réassurance en France)
22-24 Rue de Courcelles, 75008 Paris – Tél : +33 (0)1 44 35 31 36 – secretariat@apref.org
www.apref.org

Il paraît donc complexe de définir une frontière précise permettant de séparer les polices RC et cyber[2].

3. Problématique du cumul en RC

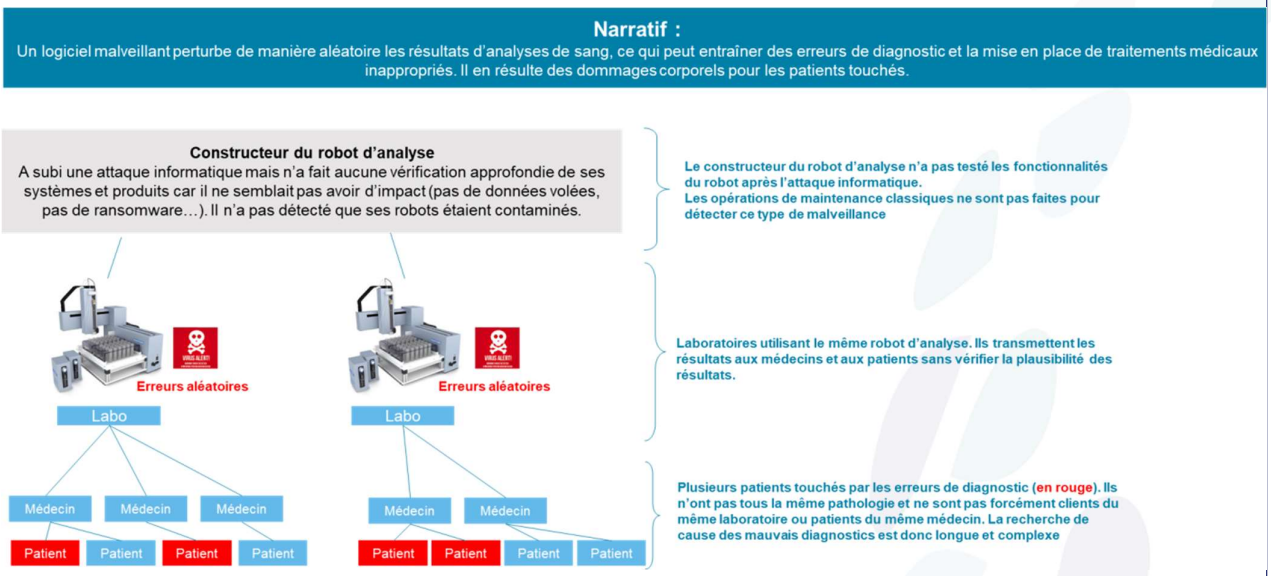
Nous allons, dans cette partie, nous pencher sur la problématique du cumul en RC (polices RC et/ou cyber).

Lorsque nous abordons le sujet du cyber, le risque de cumuls en dommages vient immédiatement à l'esprit (Wannacry – NotPetya pour ne citer que ces deux exemples)**. Mais qu'en est-il en RC ? Ce risque de cumul existe-t-il ?**

L'objectif de l'étude est d'examiner le cumul potentiel entre :

1. Une série de polices RC
2. La police RC et la police cyber

3.1 Scenario RC Médical « Corporel »



Responsabilités :

- Les polices RC professionnelles des professionnels de santé seront donc déclenchées en premier lieu. En effet, l'obligation d'assurance et d'assurer résultant de l'article L. 1142-2 du Code de la Santé Publique impose de garantir les dommages corporels quelle qu'en soit la cause (y compris cyber) dès lors qu'ils surviennent à l'occasion d'un acte de prévention, de diagnostic et de soins

[2] Voir annexe

APREF (Association des Professionnels de la Réassurance en France)
22-24 Rue de Courcelles, 75008 Paris – Tél : +33 (0)1 44 35 31 36 – secretariat@apref.org
www.apref.org

dans les contrats RC pro/RC produit de santé. Ainsi, un professionnel de santé, victime d'une attaque cyber, sera couvert des conséquences dommageables corporelles par son contrat RC professionnelle obligatoire.

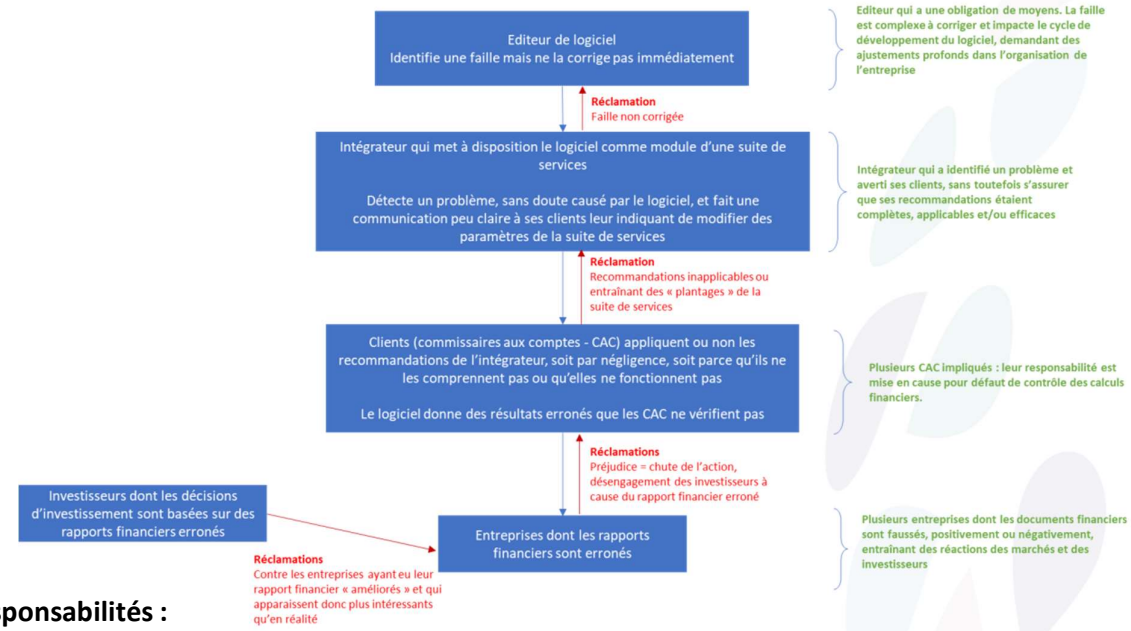
- ❖ La responsabilité des laboratoires pour non-vérification des résultats d'analyse pourrait être mise en cause.
- ❖ La responsabilité du constructeur (notamment dans le cadre d'une action récursoire) relèverait du régime des produits défectueux (*cf. nouvelle directive produits défectueux en cours d'adoption en annexe*).

Cumul :

- Les polices RC professionnelles des professionnels de santé
- Les laboratoires vont subir des pertes d'exploitation le temps de remplacer/mettre à jour les robots, pouvant déclencher les garanties dommages (« 1st party ») de leurs polices cyber

3.2 Scenario RC « financier »

Ce scénario, reposant sur un logiciel financier défectueux, ressemble au cas du logiciel Horizon utilisé par les postes britanniques au tournant des années 2000[3].



Responsabilités :

- Le défaut de contrôle des Commissaires aux comptes (CAC) qui ont certifié des comptes sans avoir effectué les contrôles nécessaires. Leur RC professionnelle pourrait être mise en cause.

[3] Post Office Horizon scandal explained: Everything you need to know | Computer Weekly

APREF (Association des Professionnels de la Réassurance en France)
22-24 Rue de Courcelles, 75008 Paris – Tél : +33 (0)1 44 35 31 36 – secretariat@apref.org
www.apref.org

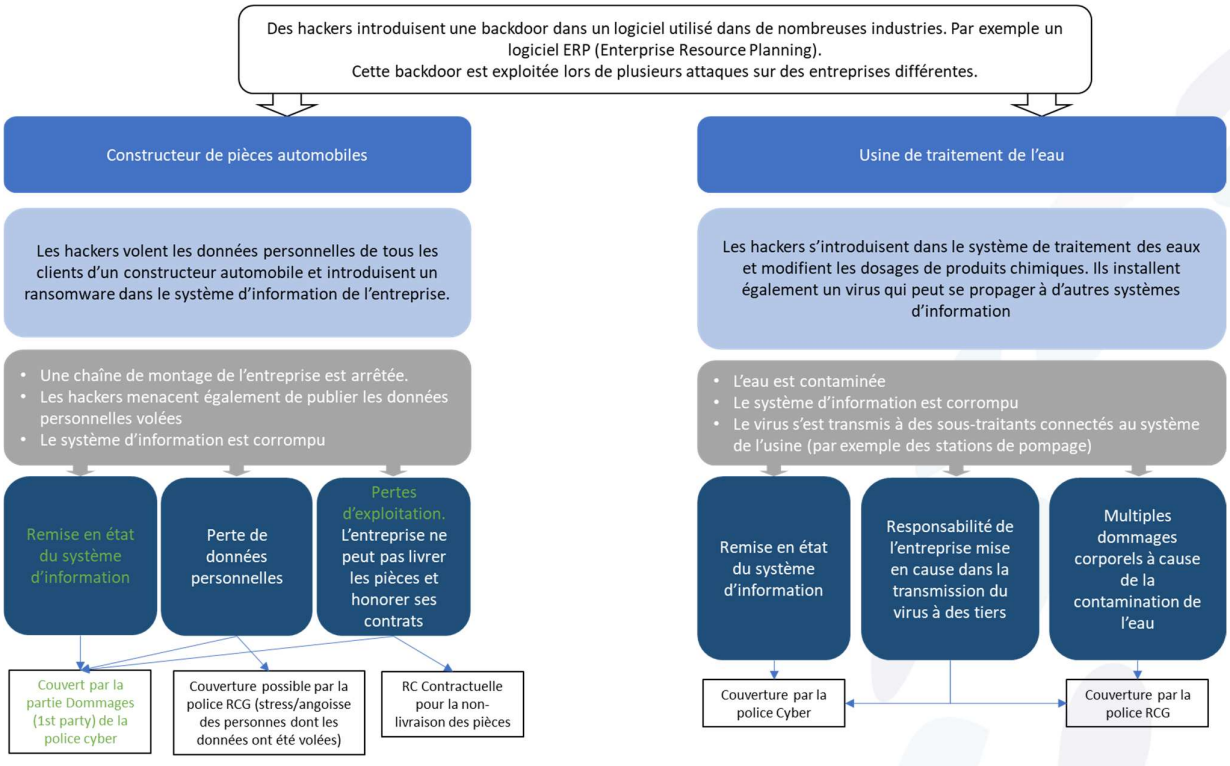
- Des actions récursoires en remontant la chaîne, notamment les polices cyber et RC de l'éditeur de logiciel et de l'intégrateur.

Cumul :

- L'ensemble des polices RC professionnelle des CAC
- Les polices cyber des CAC (partie dommages – 1st party) éventuellement déclenchées (frais supplémentaires, potentielle pertes d'exploitation)

3.3 Scénario d'attaque informatique à large échelle

Ce scénario va toucher des entreprises très variées, dont le point commun est d'utiliser le même logiciel d'Enterprise Resource Planning (ERP). Les conséquences seront donc différentes en fonction de l'activité de la victime mais toutes émaneront d'attaques cyber exploitant la même vulnérabilité informatique.



Cumul :

- Des polices Cyber des différentes entreprises attaquées via leur ERP, dans leur composante « dommages » et/ou RC
- Des polices RCG en cas de dommages corporels physiques (contamination de l'eau) ou psychologiques (stress, angoisse suite à la perte des données) lorsqu'ils sont couverts

APREF (Association des Professionnels de la Réassurance en France)
22-24 Rue de Courcelles, 75008 Paris – Tél : +33 (0)1 44 35 31 36 – secretariat@apref.org
www.apref.org

- De la RC contractuelle pour les entreprises ne pouvant livrer leurs produits/services comme prévu.

4. Conclusion

Il est difficile de tracer une frontière nette entre polices RC et cyber.

Cependant, du point de vue des sinistres individuels, la couverture du cyber dans les polices RC ne devrait pas poser de difficultés particulières et ce au regard des critères d'analyse suivants :

- La sévérité n'est pas impactée par le fait de couvrir ou non des dommages immatériels cyber. La police d'assurances RC pourrait être mise en jeu sur la base de ses limites et sous limites propres comme pour n'importe quel autre sinistre.
- La fréquence pourrait être plus sensible : le péril cyber crée indiscutablement de nouveaux risques (attaques malveillantes), mais l'informatique permet également d'améliorer sensiblement les risques (aides à la conduite pour les véhicules, domotique, détection de fautes…).

Il appartient donc à l'assureur d'ajuster sa tarification et son appétit au risque (exclusion de certaines activités particulièrement exposées soit au risque de sévérité soit au risque de fréquence) pour prendre en compte l'impact de cette exposition et la sinistralité attendue.

En revanche, les scénarios étudiés ci-dessus visent à attirer l'attention des (ré)assureurs sur le fait qu'un fait générateur cyber peut déclencher des responsabilités multiples et entraîner des cumuls non-négligeables.

Les traités Cyber ont pris la mesure de cette exposition en prévoyant des limites annuelles (engagement maximum des réassureurs) : sauf exception, les traités en quote-part comportent un AAL[4] et les traités Stop-Loss sont limités par définition.

En revanche, dans les traités RC qui n'ont pas été prévus pour ces expositions, la prise en compte des cumuls est fortement dépendante de la clause d'agrégation des sinistres (définition de l'événement). Il convient donc, en tant que réassureur, de rester prudent sur les possibilités de couvrir des cumuls importants de façon agrégée dans les traités RC.

[4] Annual aggregate limit

APREF (Association des Professionnels de la Réassurance en France)
22-24 Rue de Courcelles, 75008 Paris – Tél : +33 (0)1 44 35 31 36 – secretariat@apref.org
www.apref.org

Police RC versus police Cyber

Polices RC	Polices cyber
Les polices RC couvrent la responsabilité de l'assuré y compris dans sa dimension cyber, généralement couverte de façon silencieuse. Dès lors, les dommages matériels, corporels et DIC sont pris en charge dans le cadre de la limite de la police. Les dommages immatériels purs sont pris en charge dans le cadre de • La limite de la garantie RC Professionnelle • Ou par la sous limite DINC	Contrairement à la dimension dommages, la police cyber couvre un risque qui est déjà couvert par la police RC. Pourtant, la réalisation effective d'un transfert de risque de la police RC à la police Cyber se heurte pour l'instant aux points suivants : • Les limites Cyber sont généralement bien plus faibles que les sous-limites DINC des polices RC • Comment exclure le risque cyber des polices RC – Comment rédiger cette exclusion ? Passera–t-elle le cap des juridictions, notamment pour les professions réglementées pour lesquelles une exclusion est difficilement envisageable ? • Comment traite-t-on les anciennes polices et les polices sur base tacite reconduction ?
Conclusion : détourer l'exposition Cyber dans les polices RC du cyber n'est pas chose aisée.	

APREF (Association des Professionnels de la Réassurance en France)
22-24 Rue de Courcelles, 75008 Paris – Tél : +33 (0)1 44 35 31 36 – secretariat@apref.org
www.apref.org

Point d'attention sur la nouvelle directive européenne

Responsabilité du fait des produits défectueux
Proposition de Directive adoptée par le Parlement Européen le 2 mars 2024

Pour rappel, la proposition de directive a pour objectif de mettre à jour la réglementation européenne encadrant le régime de la responsabilité civile du fait des produits défectueux, et ce notamment afin de **l'adapter aux évolutions technologiques** (en ce compris les produits numériques dont les logiciels incorporant des technologies d'intelligence artificielle).

Les fabricants de produits seront considérés responsables de la défectuosité d'un **composant** dont ils ont assuré la fabrication, que ce composant **soit matériel ou immatériel, ou constitue un service connexe** (exemple de service connexe : les données de trafic d'un système de navigation)
Maintien du principe de la mise en cause de **l'importateur** (y compris plateforme en ligne) si le fabricant de composant n'est pas établi dans l'UE

Défectuosité d'un produit : définition

- lorsqu'il n'offre pas la sécurité que les consommateurs sont en droit d'attendre à partir d'une utilisation raisonnablement prévisible,
- ou ne suit pas les exigences légales,
- ou ne correspond pas aux besoins spécifiques du groupe d'utilisateurs auquel il est destiné.

Extension à la défectuosité qui affère à un service ou un produit utilisant **l'intelligence artificielle.**
Sont visées par la défectuosité : les techniques d'apprentissage automatique.

La future directive s'appliquera à tous les produits mis sur le marché de l'UE **24 mois après son entrée en vigueur**. Les pays de l'UE auront jusqu'à cette date pour transposer la directive dans leur droit national.

APREF (Association des Professionnels de la Réassurance en France)
22-24 Rue de Courcelles, 75008 Paris – Tél : +33 (0)1 44 35 31 36 – secretariat@apref.org
www.apref.org