

## Editorial

Chers clients, chers partenaires,

*L'ensemble du cabinet s'associe à moi pour vous présenter, ainsi qu'à vos familles et vos collaborateurs, tous nos vœux de bonheur, santé et prospérité pour cette nouvelle année !*

*L'année 2017 s'est achevée... Elle a été marquée par de nombreux événements, notamment par une confiance qui revient peu à peu et une légère reprise économique que nous espérons durable.*

*Le monde de l'assurance a fait face cette année encore, et de façon plus accrue, à des événements naturels majeurs (ouragans, séismes et feux de forêt) mais aussi à de nouveaux risques technologiques avec WannaCry et autres cyber attaques. L'industrie de l'assurance doit suivre la mutation des risques ...*

*De notre côté, l'année a été marquée par le développement de notre spécialité en Risques Financiers qui englobe l'assurance-crédit du poste client, l'affacturage et les cautions. Ce nouveau service a reçu un accueil très favorable de la part de nos clients et partenaires qui y voient des leviers pour gagner en indépendance vis à vis de leurs banques.*

*Nous avons évoqué dans notre dernière newsletter les risques cyber. Nous revenons sur ces risques avec la nouvelle réglementation européenne sur la protection des données personnelles (R.G.P.D) et nous attirons également votre attention sur les risques Fraude pour lesquels nous pouvons vous accompagner.*

*Nous serons à vos côtés pour faire de 2018 une très belle année !*

**Benoit HEUX**

de juin 2017, nous vous rappelions l'intérêt du contrat cyber, eu égard à la nouvelle réglementation. En effet, le contrat Cybercriminalité peut vous apporter un accompagnement sur les items financiers, juridiques et communication, non négligeable.

Un **audit de vulnérabilité** des infrastructures web externes peut être mis en place à la souscription d'un contrat, réalisé à distance, afin de vous aider à identifier les faiblesses potentielles de votre réseau.

En cas de piratage et vol de données, le **conseil juridique** est accordé concernant notamment vos **obligations de notification aux autorités administratives**. S'y ajoute la prise en charge de sanctions administratives légalement assurables, suite à enquête d'une autorité (CNIL) mais également les frais d'avocat et honoraires d'experts. Au-delà de ce règlement européen,

## NOUVEAU RÈGLEMENT EUROPÉEN SUR LA PROTECTION DES DONNÉES PERSONNELLES

(RGPD : Règlement Général sur la Protection des Données)

**Les données personnelles sont aujourd'hui au centre de vos stratégies et représentent un levier de développement de l'économie numérique... à condition de savoir les exploiter et de les protéger, puisqu'elles touchent à la vie privée et aux libertés fondamentales des personnes.**

**A ce titre, un nouveau règlement européen sur la protection des données personnelles (RGPD : Règlement Général sur la Protection des Données) entre en application le 25 mai 2018, et renouvelle profondément le cadre juridique applicable en la matière.**

### LE PRIVACY BY DESIGN

L'approche « **Privacy by design** », maître mot de la réforme, astreint les entreprises à placer la confidentialité des données au cœur de leurs réflexions, dès la conception d'un nouveau projet (par exemple, chiffrement des données personnelles). **Le Délégué à la Protection des données (DPO)**, en charge de la conformité de tous les traitements de données, devra être associé à chaque stade de la conception d'un nouveau service.

La collecte de données sensibles, par exemple en matière de e-santé, et le Big Data (analyse et prédiction du comportement, achats, déplacements, préférences d'une personne physique) nécessitera un encadrement par la réalisation d'une étude analysant l'**impact sur la vie privée des personnes**, et la mise en œuvre de mesures de sécurité particulières. Ces études seront menées à l'aide d'un document « Privacy Impact Assessment (PIA) », outil clé pour l'entreprise et ses sous-traitants, structurant la démarche. Tout **transfert de données** en dehors de l'Union Européenne est interdit, ou encadré par des mesures type BCR, clauses contractuelles... Il conviendra donc de vérifier ses contrats et de les conformer aux exigences de la CNIL.

**L'efficacité des mesures prises, et l'effectivité de la protection des données devront être justifiées par la mise en œuvre de mécanismes et procédures documentées.** Les entreprises pourront ainsi faire l'objet d'une **certification/un label** « Privacy by design » mis en avant sur certains services, et représentant une marque de confiance.

### LA RGPD ET L'ACCOMPAGNEMENT CYBER

En cas de non respect de la nouvelle réglementation RGPD, les sanctions **administratives** prononcées par les autorités de protection (CNIL) s'avèrent extrêmement lourdes pour les entreprises, et les autorités pourront par exemple ordonner de notifier une violation de données aux personnes concernées. Dans notre newsletter

une Cyberattaque implique un risque économique fort : la question n'est pas de connaître le détail technique d'une attaque mais de comprendre son impact sur l'entreprise, en particulier **en termes d'image, et de pertes financières**.

Là encore, le contrat Cyber supporte les frais de gestion de crise, incluant les services d'assistance de cabinets disponibles 7j/7 24h/24, et prestations de communication interne-externe, pour limiter tout **impact négatif ou atteinte à la réputation**.

Enfin, souscrire à un contrat d'assurance Cyber Risques peut être **mis en avant vis-à-vis des autorités, de vos clients et de vos investisseurs**. En effet, cela participe à une démarche de sécurité durable. C'est une des solutions permettant d'améliorer la pérennité de votre entreprise face aux risques cyber.

# S'ASSURER CONTRE LA FRAUDE ?

Lorsque nous évoquons les risques liés à la cyber-criminalité, nous traitons un type de fraude mais comme le montre l'étude ci-après, la fraude peut prendre bien des formes : fausses factures, usurpation d'identité, faux RIB, fraude au président, détournement de fonds, vol de marchandise... Votre entreprise, quelle que soit sa taille, a peut-être déjà fait l'objet d'une fraude ou d'une tentative de fraude. Des solutions d'assurance spécifiques offrent une protection complète, en couvrant vos pertes financières mais également les frais de restauration d'image, de communication, de reconstitution de données et de procédures judiciaires.

## Étude Euler Hermes - DFCG 2017

### De la cyber-criminalité à la fraude : une menace en pleine mutation



8 entreprises sur 10 ont été victimes (d'au moins) une tentative de fraude sur l'année écoulée



1 entreprise sur 4 a subi plus de 5 tentatives de fraude sur cette même période



1 entreprise sur 5 a subi au moins une fraude avérée

#### Les dispositifs ayant permis de déjouer ces tentatives de fraudes



Réaction ou initiative humaine personnelle



Procédures de contrôle interne



Dispositif technique (IT)



81% des directions financières craignent une accentuation du risque de fraude en 2017 !

#### TOP 5 DES TENTATIVES DE FRAUDES



1 Fraudes au président  
59%



2 Cyber-fraudes  
57%  
(dont 22% d'attaques au ransomware)



3 Fraudes aux Faux fournisseurs  
56%



4 Usurpations d'identité  
(type banques, avocats...)  
29%



5 Fraudes aux Faux clients  
25%



10% des entreprises attaquées subiraient un préjudice supérieur à 100 K€

87% des entreprises redoutent en priorité un impact sur leur trésorerie

#### Les dispositifs permettant de lutter contre ces attaques



Sensibilisation et Formations internes  
89%



Renforcement des procédures de contrôle interne  
80%



Audit sécurité du système d'informations  
45%



Test d'intrusion  
29%



Nouveaux logiciels  
24%



Cartographie des risques de fraude  
22%

#### Quelle direction pilote la lutte contre la fraude ?



Direction financière



Direction Informatique



Direction générale



Fonction dédiée

L'enquête : Avril 2017, 200 entreprises (60% DAF, toutes tailles d'entreprises et tous secteurs d'activité).



63% des entreprises ne disposent pas de plan d'urgence à activer en cas de fraude



[www.eulerhermes.fr](http://www.eulerhermes.fr)

A company of Allianz



ASSOCIATION NATIONALE DES DIRECTEURS FINANCIERS ET DE CONTRÔLE DE GESTION

[www.dfcg.fr](http://www.dfcg.fr)

\* Note savoir au service de votre réussite



Immeuble la Vigie - 3 Impasse de la Vigie  
CS 31872 - 35418 ST MALO Cedex  
Tél : 02.99.81.22.52 - Fax : 02.99.82.89.58  
[contact@heux-assurances.com](mailto:contact@heux-assurances.com) - [www.heux-assurances.com](http://www.heux-assurances.com)

Une publication de la société : SAS HEUX ASSURANCES  
Directeur de la publication : Mr Benoit HEUX  
SAS HEUX ASSURANCES - SOCIÉTÉ DE COURTAGE D'ASSURANCES - N° ORIAS 07 000 340 -  
[www.orias.fr](http://www.orias.fr) - Capital Social de 92.000 Euros - RCS Saint-Malo B 428 763 973  
TVA Intracommunautaire : FR ZK428763973 - APE 6622Z  
Garantie financière de responsabilité civile et professionnelle  
conforme aux articles L 530-1 et L 530-2 du code des Assurances.

Les autres membres du groupe RESO+ :

