La Lettre RESO+

LA FLANDRE ASSURANCES
AUDIT & COURTAGE
Antoine & Philippe Blouin

Editorial

Chers clients, chers partenaires,

L'année 2017 s'est achevée...
Elle a été marquée par de nombreux événements, notamment une reprise économique accompagnée de difficultés de recrutement dans beaucoup de secteurs d'activités, une confiance qui revient peu à peu.

Le monde de l'assurance a fait face encore cette année, et de façon plus accrue, à des catastrophes naturelles – ouragans, séismes – et aussi à de nouveaux risques cyber avec WannaCry en mai... L'industrie de l'assurance doit suivre la mutation des risques...

Nous avions 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) ; nous attirons également votre attention sur le risque Fraude pour lequel nous avons été amenés à intervenir sur des sinistres importants.

Nous sommes heureux de vous présenter également nos équipes d'experts qui vous accompagnent dans la gestion de vos risques, de vos contrats, de vos sinistres...

Avec eux, nous vous présentons ainsi qu'à ceux qui vous entourent, nos meilleurs vœux pour cette nouvelle année 2018 !

Philippe-Hervé et Antoine BLOUIN

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. Nous tâcherons de vous apporter à travers cet article quelques points clés de la mise en conformité de votre entreprise à l'approche de cette réforme.

LA PROTECTION DE LA VIE PRIVEE DES LA CONCEPTION D'UN PROJET

L'approche **« Privacy by design »**, maitre 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. Cette approche devra répondre au renforcement du principe d'autodétermination informationnelle, selon lequel chacun est maître des informations qui le concerne.
Toute personne pourra ainsi récupérer ses données ou les transférer, par le nouveau droit à la **Portabilité**, créé par la RGPD. Le **consentement** des personnes, préalable à tout traitement de donnée, devra être recueilli par le responsable.

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 Assesment (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.

Les Entreprises auront **72 heures** pour déclarer à la CNIL une violation de données à caractère personnel. L'information aux personnes concernées s'impose en cas de risques élevés pour leurs droits et libertés.

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 représenter une marque de confiance.

LA RGDP 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 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 de votre système informatique, réalisé à distance, peut être mis en place à la souscription d'un contrat, afin de vous aider à identifier les faiblesses potentielles de votre réseau.

En cas de piratage et vol de données, **un accompagnement juridique** est inclus concernant 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.

NOUVEAU RÈGLEMENT EUROPÉEN SUR LA PROTECTION DES DONNÉES PERSONNELLES (SUITE)

(RGPD : Règlement Général sur la Protection des Données)

Au-delà de ce règlement européen, une Cyberattaque implique un risque économique fort : la question n'est pas de connaitre 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 Cybercriminalité 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**. Ces postes de garanties restent couverts en cas d'attaque de votre prestataire informatique dans la mesure où, même externalisé, votre système reste sous votre responsabilité.

Enfin, souscrire à un contrat d'assurance Cybercriminalité peut être **mis en avant vis-à-vis des autorités, de vos clients et de vos investisseurs**. La prise en charge de la perte d'exploitation en cas de piratage est une garantie majeure et participe à une démarche de sécurité durable. C'est une des solutions permettant d'assurer la pérennité de votre entreprise face aux risques cyber.

SANCTIONS ADMINISTRATIVES LOURDES PRÉVUES DANS LE RGPD

Les sanctions auxquelles s'exposent les entreprises en cas de non respect des exigences RGPD sont importantes. En cas d'amendes, ces dernières pourraient se retrouver dans des situations délicates financièrement de nature à impacter leur activité : réduction d'effectifs, réorganisation voire arrêt total de l'activité pour les plus petites entreprises.

En effet, l'amende ira jusque **2% du chiffre d'affaires annuel mondial** (jusque 10 millions d'euros) en cas d'absence de désignation d'un délégué à la protection des données quand celle-ci est obligatoire;
Il en est de même en cas absence de notification à l'autorité de contrôle ou à la personne concernée par violation de données à caractère personnel;
L'insuffisance de mesures de sécurité des données, ou encore l'absence de réalisation de l'analyse d'impact évoquée ci-dessus constituent également des infractions au règlement.

Ces amendes **sont multipliées par deux lorsque l'infraction touche au droit des personnes** (soit 4 % du chiffre d'affaires et 20 millions d'euros). Il pourrait par exemple s'agir d'un non-respect des principes de base applicables aux traitements de données à caractère personnel (loyauté, transparence, limitation des finalités, minimisation des données, durée de conservation, etc.) Ou encore d'un non-respect des droits des personnes concernées (information, accès, rectification, effacement, etc.).

Des sanctions pénales sont également prévues : Le détournement de la finalité des données personnelles récoltées, ou le non respect de la loi informatique et liberté sont des infractions passibles de 300 000 € d'amende et 5 ans d'emprisonnement.

Les enjeux de ce nouveau règlement sont donc importants pour les Entreprises, nous vous recommandons de bien vous y préparer et nous nous tenons à votre disposition pour vous y accompagner à travers notre produit CYBERCRIMINALITÉ.

S'ASSURER CONTRE LA FRAUDE ?

Nous évoquions dans notre dernière newsletter les risques liés à la cyber-criminalité et les solutions d'assurances en la matière. Nous voulons attirer votre attention aujourd'hui sur les sinistres de plus en plus fréquents – et sur l'importance de ceux-ci – liés à la fraude.

Fausses factures, usurpation d'identité, faux RIB, fraude au président, intrusion dans vos outils informatiques, 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...

Exemples de détournements d'actifs :
- Achat : Fausses factures, double paiement, détournement de moyens de paiement
- Vente : Détournement de chèques, de facturations
- Paye/RH : salarié fictif, commissions et éléments variables, remboursement de frais
- Stock : avant enregistrement, après enregistrement
- Caisse : avant /après enregistrement, fausses annulations ou remboursements

La « Fraude au Président » ou « social Engineering » :
- Usurpation de l'identité d'un dirigeant
- Usurpation de l'identité d'un partenaire :

Fournisseur et changement de RIB, Client et fausse commande, administration et demande de données bancaires, ...

LA PREVENTION :

Vous pouvez limiter le risque « fraude » en revisitant votre organisation, en instituant des moyens de contrôle :
- Vos procédures comptables / Transferts de fonds / procédures RH
- La prévention des fraudes externes
- L'inventaire / gestion des stocks
- La réalisation d'audit

En renforçant vos procédures informatiques
- Contrôle des accès et habilitations
- Systèmes anti-virus / Fire-walls
- Gestion des mots de passe

LA SOLUTION « ASSURANCE »

Nous avons sélectionné des assureurs spécialisés dans ce domaine avec qui nous travaillons sur des solutions d'assurance « fraude » étudiées selon votre secteur d'activité, votre présence internationale, vos antécédents éventuels et surtout, sur les moyens de contrôle et les procédures informatiques mis en place au sein de votre Entreprise.

L'assurance a pour objet de vous garantir contre le risque de fraude et ses conséquences. Dans ce cadre, les différents types de fraude sont garantis :
- **La fraude interne** commise par un employé comme l'abus de confiance, le détournement de fonds ou de marchandises.
- **La fraude externe** commise par un tiers comme l'escroquerie ou l'usurpation d'identité.
- **La cyberfraude.**

Protection complète, l'assurance contre le risque de fraude couvre vos pertes financières mais également les frais de restauration d'image, de communication, de reconstitution de données et de procédures judiciaires.

Vous limitez ainsi les conséquences de la fraude, aussi bien les pertes financières directes, qu'un éventuel impact négatif sur votre réputation.

L'accompagnement est personnalisé dès la constatation de la fraude et adapté à la taille de votre entreprise dont le siège mais également l'ensemble de vos filiales et succursales situées en France et en Europe sont couvertes.

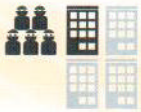
Ce dispositif prévoit de plus une indemnisation rapide, accordée dans les trente jours après l'obtention d'un accord sur son montant, ainsi qu'une tarification adaptée aux besoins de couverture de votre entreprise afin de maîtriser vos coûts.

En vous protégeant contre le risque de fraude, vous pouvez ainsi vous concentrer sur le développement de votre entreprise en toute sécurité, éviter les tensions de trésorerie et protéger votre rentabilité.

Nos équipes sont à votre disposition pour répondre à vos questions.

Étude Euler Hermes - DFCG 2017
De la cyber-criminalité à la fraude : une menace en pleine mutation

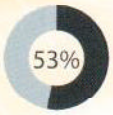
8 entreprises sur 10 ont été victimes (d'au moins) une tentative de fraude sur l'année écoulée



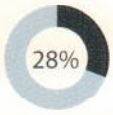
1 entreprise sur 4 a subi plus de 5 tentatives de fraude sur cette même période

1 entreprise sur 5 a subi au moins une fraude avérée

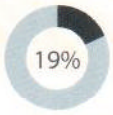
Les dispositifs ayant permis de déjouer ces tentatives de fraudes



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%

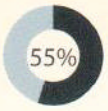
Audit sécurité du système d'informations 45%

Test d'intrusion 29%

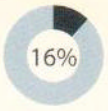
Nouveaux logiciels 24%

Cartographie des risques de fraude 22%

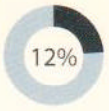
Quelle direction pilote la lutte contre la fraude ?



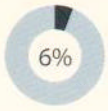
Direction financière



Direction Informatique



Direction générale



Fonction dédiée

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

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

EULER HERMES Our knowledge serving your success **www.eulerhermes.fr**

A company of Allianz

DFCG ASSOCIATION NATIONALE DES DIRECTEURS FINANCIERS ET DE CONTRÔLE DE GESTION

www.dfcg.fr