VERSPIEREN
COURTIER EN ASSURANCES

SÉCUR'INFO

LA LETTRE DES PROFESSIONNELS DE LA SÉCURITÉ

DÉCEMBRE 2017

DOSSIER CYBER

CYBER – ATTAQUES, PERTE DE DONNÉES

Protégez vos entreprises de sécurité des risques de cyber–attaques et de perte de données.
En effet, l'incident de sécurité informatique est une menace réelle qui peut ralentir ou interrompre votre activité.
Concrètement : une perte de chiffre d'affaires.

POURQUOI VOUS ASSURER ?

Les études confirment que 94% des entreprises ont connu une cyber–attaque au cours des 12 derniers mois, 88% des virus fabriqués sur mesure par les hackers ne sont pas détectés par les anti-virus, et 57% des attaques visent les PME.
Dans le cadre de votre activité, vous disposez et détenez les données sensibles de vos clients, employés, fournisseurs... et en êtes responsable.

De plus, à partir du 24 mai 2018, le Règlement Général Européen sur la Protection des Données (GRPD) sera applicable et vous imposera :

- la notification obligatoire à vos clients, employés et partenaires commerciaux pour toute violation de données même celles paraissant de faible importance ;
- une augmentation des niveaux de sanctions (jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires mondial) ;
- des nouvelles mesures obligatoires de sécurisation des données et du système informatique.

L'article se trouvant en page 2 de cette lettre vous apportera plus de précisions.

NOTRE SOLUTION D'ASSURANCE

Le contrat d'assurance Cyber–Attaques couvre :

- **Les dommages subis par l'entreprise :**
  - pertes de revenus ;
  - frais de notification ;
  - maintien de la réputation.
- **Les dommages causés à des tiers :**
  - dommages et intérêts en cas de violation de données personnelles et confidentielles ;
  - transmission de virus.
- **Cyber–extorsion :**
  - frais de négociation ;
  - prise en charge de la rançon ;
  - pertes consécutives de revenus.

LES PLUS VERSPIEREN

- **Notre connaissance du secteur des professionnels de la sécurité depuis plus de 20 ans,** nous permet de proposer un contrat spécialement mis en place pour **faire face aux risques de cyber–attaque encourus par vos entreprises de sécurité.**
- Un panel d'experts spécialisés.

Stéphane Letellier
01 49 64 14 29
sletellier@verspieren.com

L'IMPACT DU RGPD SUR LES MÉTIERS DE LA SURVEILLANCE, GARDIENNAGE, TÉLÉSURVEILLEURS, LES INSTALLATEURS ET INTÉGRATEURS DE SYSTÈMES DE DÉTECTION (PARTIE 1)

Pourquoi le règlement sur la protection des données adopté le 27 avril 2016 et applicable directement en France le 25 mai 2018 intéresse les professionnels de la sécurité ?

Tout d'abord, les métiers de la surveillance, gardiennage, télésurveilleurs, les installateurs et intégrateurs de systèmes de détection sont rattachés au périmètre de la sous-traitance ou à des conventions de prestation de services. Or, Le RGPD impose des obligations nouvelles et spécifiques aux sous-traitants dont la responsabilité est susceptible d'être engagée en cas de manquement.

Ensuite, la raison d'être du règlement est la prise en compte des avancées technologiques, notamment numériques, ce qui cible spécifiquement les métiers de la sécurité. Le RGPD met à jour le cadre législatif actuel (loi informatique et libertés[1]) à l'évolution des nouvelles technologies en facilitant « la libre circulation des données (...), tout en assurant un niveau élevé de protection des données à caractère personnel ».

Si les obligations du règlement sont nombreuses, elles se concentrent sur 3 axes :

- une obligation pour les petites et grandes entreprises d'identifier clairement les traitements qui fonctionnent avec des données personnelles (cartographies et listes des traitements) ;
- obligation d'analyse d'impact (responsable du traitement et sous-traitant) s'agissant des traitements présentant des risques particuliers ;
- une obligation de sécurité renforcée pour le responsable du traitement qui peut être le donneur d'ordre et le sous-traitant.

Le Règlement Général sur la Protection des Données personnelles (RGPD) entrera en application dans moins de 6 mois, en mai 2018.

Le compte à rebours du RGPD s'accélère pour les entreprises qui, pour une part absolument écrasante d'entre elles, sont loin d'un état de conformité acceptable avec les dispositions légales actuelles et, en conséquence, encore plus loin d'une conformité de type RGPD.

Rappelons que ce texte a pour objectif de moderniser le cadre européen de la protection des données à caractère personnel et de réduire, voire de supprimer, les écarts juridiques existant à l'heure actuelle entre les différentes législations des États membres de l'Union européenne.

Les entreprises ont donc encore quelques mois pour repenser totalement leur gouvernance de protection des données personnelles et pour déployer l'ensemble des actions nécessaires pour leur assurer une conformité totale avec le RGPD .

Une vraie difficulté, tant le texte est complexe et technique, qui va imposer aux entreprises qu'elles se plient à de nouvelles obligations.

Qu'on en juge : le RGPD porte, ainsi, en germe près de 400 obligations, dont le contenu est précisé dans 99 articles, eux-mêmes contextualisés dans près de 200 considérants.

Concrètement en quoi les entreprises de surveillance, gardiennage, de télésurveillance, les installateurs et intégrateurs de systèmes de détection sont-ils réellement impactés ? Le RGPD touche-il directement et immédiatement ce secteur ?

Soyons clair, il l'impacte déjà. Pour s'en convaincre, penchons-nous sur l'exemple du tout récent arrêté du 27 juin 2017, portant sur le cahier des charges applicable à la formation initiale aux activités privées de sécurité. Il prévoit dans son article 10 que pour l'obtention de la carte professionnelle autorisant l'exercice d'une activité de vidéoprotection, il conviendra de connaître la réglementation européenne pour la protection des données.
L'absorption du RGPD au secteur de la sécurité est donc actée avant même l'arrivée officielle du règlement.

Plus encore, l'esprit du RGPD est celui d'une mise à jour d'un dispositif existant et non pas d'une véritable révolution juridique. Les professionnels ont eu le temps d'appréhender les enjeux des données à caractère personnel (voir actualité sur la problématique de chantage après vol de données, cyber-attaques, etc.). Dorénavant, ils sont considérés comme pleinement responsables. Les professionnels sont réputés avoir digéré depuis maintenant près de 40 ans les précédentes obligations issues de la loi informatique et libertés[1].

Le régime juridique du règlement européen fait honneur à cette maturité juridique des professionnels car le RGPD, à la différence d'une directive européenne, s'applique directement sans qu'il soit nécessaire de passer par un acte de transposition dans le droit national.

[1] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Plus encore, le RGPD dote la France, comme les autres États membres, d'une puissance de sanction jusque-là inégalée : amendes pouvant atteindre pour les contrevenants 20 millions d'euros ou 4% du chiffre d'affaires annuel (mondial) de l'entreprise, le montant le plus élevé étant celui retenu.

Une étude récente commandée par Véritas[2] fait apparaître, outre l'ampleur des pénalités, que les entreprises interrogées s'inquiètent également de la mauvaise publicité que leur vaudrait une non-conformité avec le nouveau règlement.

Plus concrètement encore, quelle est la feuille de route à tenir ? Que faut-il retenir en priorité pour ceux qui n'ont encore rien entrepris ?

Les principaux chantiers qui devront être menés sont :

- un audit des traitements pour établir la liste des traitements.

Concrètement, chaque entreprise, selon les termes du règlement général sur la protection des données, doit démontrer l'efficacité des mesures prises et l'effectivité de la protection des données qu'elle a mise en place.

Ce principe d' **« accountability »** consiste en un processus permanent et dynamique de mise en conformité d'une entreprise à la réglementation relative à la protection des données grâce à un ensemble de règles, d'outils et de bonnes pratiques correspondantes.

Le respect du principe d'«accountability » n'implique pas seulement d'être en conformité avec le règlement général sur la protection des données, mais également d'être en mesure de démontrer cette conformité.

Quel processus ? Celui d'un audit des traitements qui dressera la cartographie des traitements et des données utilisées et qui sera matérialisé dans un rapport d'audit accompagné de recommandations que l'entreprise s'attachera à mettre en œuvre selon un retro-planning.

Pour compléter cette conformité, certaines mesures pourront être mises en œuvre, à savoir notamment :

- l'adoption de règles internes consistant en des mesures techniques et organisationnelles appropriées. Elles concernent notamment la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, les audits correspondants et la mise en place d'une documentation interne (procédures et politiques internes) ;
- l'obligation de conserver une trace documentaire de tout traitement effectué sous la responsabilité du responsable du traitement ou du sous-traitant (tenue d'un registre des traitements) ;
- la réalisation d'une analyse d'impact pour les traitements présentant des risques particuliers au regard des droits et libertés des personnes concernées ;
- l'adoption de l'approche Privacy by design / Privacy by default[3].

Rappelons au passage que le RGPD, en son article 42, comporte un article dédié à la certification. Il s'agit d'attester « de la conformité avec le règlement des opérations de traitement effectuées par les responsables de traitement et les sous-traitants ».

Dès lors, les entreprises du secteur ont tout intérêt à capitaliser de leur conformité.
En quelque sorte il s'agit d'afficher véritablement que les produits, leurs process et les organisations proposés aux clients sont estampillés RGPD.

À suivre dans le prochain Sécur'Info, l'impact du RGPD sur les métiers de la surveillance, du gardiennage, des télésurveilleurs, des installateurs et intégrateurs de systèmes de détection - Partie 2.
Nous aborderons l'étude d'impact, ainsi que l'obligation de sécurité renforcée pour le donneur d'ordre et le sous-traitant.

Emmanuel WALLE

Avocat, Lexing Alain Bensoussan Avocats
Directeur : Droit du travail – Droit informatique – Droit de la protection des données

[2] Enquête menée par le cabinet Vanson Bourne pour Veritas.
www.veritas.com/content/dam/Veritas/docs/reports/gdpr-report-fr.pdf

[3] Article 25- Alinéa 2 portant sur la « Protection des données dès la conception et protection des données par défaut.

RESPONSABILITÉ CIVILE PROFESSIONNELLE ATTENTATS

NOUVEAU : UN CONTRAT DE RESPONSABILITÉ CIVILE PROFESSIONNELLE ATTENTATS

Le premier contrat d'assurance permettant à vos entreprises de sécurité de se protéger contre les risques de mise en cause suite à des actes de terrorisme et d'attentats.

POURQUOI VOUS ASSURER ?

La responsabilité civile

La responsabilité civile pourrait être recherchée par l'assureur de la victime de dommages matériels ou par le Fonds de garantie des victimes des actes de terrorisme. Mais encore faut-il réunir les conditions de mise en jeu de la responsabilité civile, à savoir, une faute, un dommage et un lien de causalité entre la faute et le dommage. **Par exemple, l'exploitant d'un centre commercial reproche à une société de sécurité de n'avoir pas été suffisamment attentive dans le contrôle des accès.**

La faute inexcusable

La reconnaissance d'une faute inexcusable de l'employeur. Reprocher à l'employeur une faute inexcusable commise à l'encontre du salarié touché par un attentat sur un site dont il avait la surveillance. Cela semble difficile sauf s'il est prouvé que l'employeur n'a pas pris toutes les mesures de sécurité que nécessitait la mission. **Par exemple, le salarié dont la mission est de surveiller un site hautement vulnérable en termes de risque de terrorisme et qui n'aurait reçu aucune formation dans ce domaine.**

La responsabilité de l'employeur du fait de son préposé

Il s'agit de rechercher la responsabilité civile du commettant du fait de son préposé auteur d'un attentat ou acte de terrorisme : le commettant a toujours la possibilité de s'exonérer de sa responsabilité s'il prouve que le préposé a agi hors des fonctions auxquelles il était employé, sans autorisation et à des fins étrangères à ses attributions. Mais encore faut-il prouver l'abus de fonction. Et surtout, l'entreprise de gardiennage est responsable des conséquences des engagements pris envers son client qui se réalisent par l'intermédiaire de ses préposés. En d'autres termes, il peut y avoir abus de fonction en responsabilité civile délictuelle mais aussi en responsabilité civile contractuelle mais encore faut-il le prouver. **Ainsi, il a été jugé qu'en incendiant l'immeuble qu'il surveillait, le préposé transgresse la sécurité que l'entreprise de gardiennage a promis à son client et qu'en conséquence l'employeur ne peut s'en exonérer au prétexte que le préposé a agi à des fins personnelles.**

NOTRE SOLUTION D'ASSURANCE

La responsabilité de votre entreprise de sécurité peut être recherchée selon ces fondements. **Verspieren vous propose le premier contrat d'assurance couvrant la responsabilité civile professionnelle Attentats sur le marché.** Ce contrat garantit les conséquences pécuniaires de la responsabilité civile pouvant vous incomber à la suite de dommages causés aux tiers dans l'exercice de vos activités.

Usuellement, ces dommages sont exclus des contrats d'assurance de responsabilité civile professionnelle. Ce contrat vient donc en complément et ne se substitue pas à votre contrat responsabilité civile professionnelle.

LES PLUS VERSPIEREN

- Premier contrat sur le marché couvrant les risques liés aux actes de terrorisme et attentats.
- Une équipe de spécialistes dédiée à votre accompagnement.

Contactez-nous !

Stéphane Letellier
01 49 64 14 29
sletellier@verspieren.com

OPTIMISEZ LA PROTECTION SOCIALE DE VOS SALARIÉS

Vous recherchez actuellement une protection sociale performante pour l'ensemble de vos salariés ? Ou vous venez d'être résilié par votre assureur ?

Également expert en assurances de personnes, nous pouvons vous construire une solution sur-mesure, tout en respectant les obligations de votre convention collective.

Par ailleurs, vous avez jusqu'au **31 décembre pour mettre en conformité vos contrats santé/prévoyance collectifs avec la législation du contrat responsable.**

Ainsi, pour optimiser vos contrats, nous vous proposons une étude gratuite de votre régime de protection sociale.

Contactez rapidement nos experts santé/prévoyance pour plus d'informations.

E-mail : **contactadp@verspieren.com**

VERSPIEREN
COURTIER EN ASSURANCES

Le Sécur'info est édité par Verspieren
8, avenue du Stade de France – 93210 Saint-Denis
ISSN : 1637-8741 – Dépôt légal à parution
Directeur de la publication :
Claude Delahaye
Rédacteur en chef : Claude Delahaye
Comité de rédaction : Stéphane Letellier,
Emmanuel Walle
Coordination : Marina Corso et Stéphanie Contesse