

Les nouvelles règles sur la protection des données personnelles rappellent aux entreprises les enjeux du numérique à l'heure où se multiplient les cyber attaques. . .

RGPD - CYBER RISQUE : PROTÉGEZ-VOUS !

Par **Michael Fianza**,
chargé de clientèle
Assurfroid



Connu sous l'acronyme RGPD, le règlement européen N° 2016/679 relatif à la protection des données à caractère personnel, du 27 avril 2016 est entré en vigueur le 25 mai 2018. Il vise à responsabiliser les professionnels qui, dans leur gestion quotidienne, traitent des données personnelles, tels que les données sur leurs clients, leurs salariés, leurs fournisseurs... Cette responsabilisation va s'accroître avec le prélèvement à la source de l'imposition des salariés prévu pour 2019, les entreprises se retrouvant de plus en plus actives, et en première ligne dans la gestion des données, et donc les premières visées en cas d'attaque cyber.

Quels enjeux ?

Face aux risques cyber et à la réglementation RGPD, les entreprises doivent se mettre en ordre de marche pour organiser la gestion de leurs données.

Ce dispositif implique une réorganisation interne des entreprises (allègement des formalités administratives, nomination d'un délégué chargé de la protection des données personnelles, analyse de risque) qui devront désormais s'assurer que tout est mis en œuvre pour être en conformité avec le règlement (mise en place d'un système de contrôle *a posteriori* effectué par la Cnil). Les entreprises devront également veiller à ce que le client soit informé

des droits dont il dispose (droit à la portabilité, retrait de son consentement. . .) mais également respecter des obligations de notifications en cas d'attaque cyber.

Pour mémoire, toutes les entreprises doivent être en ordre de marche depuis le 25 mai 2018. . . À défaut, elles s'exposent à de lourdes amendes (4 % du CA annuel ou 20 M€) en cas de manquements constatés à l'occasion d'un contrôle effectué par la Cnil.

Quelles solutions ?

Sécuriser son système informatique et s'organiser pour être en conformité avec le RGPD.

Le RGPD est l'occasion de mettre à jour son système informatique, de le faire évoluer vers plus de sécurité. L'audit cyber réalisé par des spécialistes de l'informatique, indépendant du prestataire informatique habituel, est l'une des méthodes d'évaluation du risque la plus recommandée pour démarrer la mise en conformité.

Sécuriser juridiquement ses contrats, modifier les clauses des contrats au regard de la réglementation RGPD.

Il semble nécessaire de solliciter ses conseils juridiques en matière de protection de données, les cabinets spécialisés répondront le mieux aux besoins des entreprises et notamment pour mettre à jour les conditions de vente/achat, les contrats de travail, les contrats de sous-traitance

et notamment les contrats avec les prestataires informatiques.

Evaluer et mettre en place des assurances spécialisées face aux attaques cyber et risques RGPD.

Ces assurances peuvent être contractées auprès d'un assureur spécialisé ou d'un courtier comme c'est le cas avec Ofracar - Assurfroid. Au sein du groupe, des spécialistes cyber mettent à disposition des clients un panel de solutions appropriées. Les dirigeants d'entreprises bénéficient alors d'outils pour évaluer leurs risques et mesurer les conséquences financières en cas d'attaque cyber. Quel que soit le prestataire choisi, pour être bien couvert, il faut veiller que les solutions proposées prennent en charge :

- La mise en place d'une cellule de gestion de crise.
- La prise en charge des dommages cyber de l'entreprise et les demandes de rançons.

• Un accompagnement face à une enquête de la CNIL.

• La prise en charge des dommages et intérêts réclamés par les victimes de la cyber attaque.

Avant de contracter, il faut aussi veiller à la disponibilité du service spécialisé de l'assureur avec une réactivité 24H/24 - 7J/7 via un numéro d'urgence. ●

www.assurfroid.fr

Conseils

- Traiter le cyber risque, et notamment depuis le RGPD du 25 mai 2018, comme un risque majeur pour les entreprises ;
- Ne pas considérer que seuls les autres seront victimes d'une cyber attaque... car nous sommes tous reliés par nos outils informatiques les uns aux autres !