RGPD & Cybersécurité ... à l'aube de 2020

Olivier Gourio

expert en cyber-sécurité, président d'Expert3

Pas de RGPD sans cybersécurité !
Avec ce règlement Européen, les entreprises doivent garantir le respect de la vie privée des personnes dont elles possèdent les données. La loi les obligeant à se prémunir contre le vol ou la fuite des données personnelles qu'elles détiennent par la mise en place de dispositifs de cybersécurité (chiffrement, sécurisation des postes de travail et des réseaux, politique de mot de passe...).
Et ce, quelles que soient leur taille et leur sensibilité au cyber-risque. Ainsi, 18 mois après sa mise en application, le RGPD est-il parvenu à remplir ses objectifs ? Un point d'étape s'impose pour nos métiers des CHRD.

Rappels sur le RGPD

Le RGPD (ou en anglais « General Data Protection Regulation » ou GDPR) encadre le traitement des données personnelles sur le territoire de l'Union européenne. Née de la volonté de protéger les citoyens d'actes malveillants et /ou d'usages commerciaux abusifs, ce règlement ambitionne de leur donner plus d'autonomie sur leurs données personnelles. Pour mémoire, **les entreprises devaient s'y être préparées en amont afin d'être en conformité à partir du 25 mai 2018.**

L'objectif de ce règlement est bien **de contraindre les entreprises à instaurer des systèmes fiables qui permettront de garantir la sécurité et le contrôle des données personnelles des consommateurs.** En France, régi par la CNIL (Commission Nationale de l'Informatique et des Libertés), le RGPD permet d'harmoniser la législation au sein de l'Union Européenne.

Le principe d'« accountability » ou responsabilisation est un des grands changements de ce règlement. Chaque chef d'entreprise doit gérer sa propre conformité et doit être en mesure d'**en fournir la preuve.**

Trop nombreux sont encore ceux qui imaginant qu'ils ne sont pas concernés ou laisse entendre que le travail a été fait par un prestataire.

Or, c'est avec ces croyances que le risque augmente : en effet si la personne morale est directement en ligne de mire, rappelons que ces sanctions administratives peuvent être complétées par des condamnations pénales (articles 226-16 et suiv. et R 625-10 et suiv. du Code pénal) visant, dans certains cas, les dirigeants à titre personnel.

Aujourd'hui à l'aube de 2020, **la CNIL est bien décidée à mettre un terme à une période de clémence** qu'elle estime avoir suffisamment fait durer pour passer à l'étape suivante : renforcement des contrôles et sanctions... La mise en conformité des entreprises et des organisations est désormais une nécessité absolue.

Alors, comment faire ?

C'est un travail de fond à réaliser dans un temps long mais l'essentiel est de « prendre date » afin de **pouvoir prouver** que vous avez engagé vos chantiers de mise en conformité, avec une priorité : réduire vos risques !

Quelques exemples d'interrogations pour le secteur des CHRD :
- Les données que vous stockez en interne ou en externe sont-elles vraiment protégées ?
- Les données de vos clients et de vos salariés sont-elles stockées chez un de vos sous-traitants ? dans quel pays ? en Europe ?

- Demandez-vous à vos clients un consentement explicite pour certains de vos traitements qui seront fait de leurs données (newsletter par exemple) ?

- Vos collaborateurs sont-ils formés ou à minima sensibilisés aux bases de la cybersécurité ?
- Vos terminaux informatiques (ordinateurs, tablettes et smartphones) sont-ils équipés d'une suite de sécurité ? (Un simple antivirus ne suffit plus)

Particulièrement dans l'hôtellerie, **l'écosystème est prépondérant**. Vous devez vous assurer que tous les prestataires accédant à vos données clients vous garantissent leur sécurité (Clauses contractuelles et process techniques).

PMS, Channel manager, moteur de résa, yield management, e-réputation, informaticien, agence web, vidéosurveillance, il vous faut obtenir de vos partenaires la garantie de leur niveau de conformité au RGPD et de protection aux risques cyber.

Concrètement :

Nettoyez vos bases de données (fichier clients, salariés...)
L'entretien de vos contacts a toujours fait partie des recommandations de la CNIL. Le RGPD impose aux entreprises de s'engager sur une durée de conservation des données à caractère personnel.

C'est aussi mieux gérer votre entreprise : le règlement exige que les données soient pertinentes par rapport à l'objectif pour lequel vous les collectez.

Respectez ces durées de conservation en procédant par exemple à des nettoyages réguliers de votre cardex et de vos fiches de police.

Autre exemple : les données issues de l'encodage de vos clefs pour l'accès aux chambres et aux locaux ainsi que le contrôle des horaires du personnel pourront être conservées 3 mois s'agissant des informations relatives aux déplacements et 5 ans s'agissant des horaires (application du code du travail).

Documentez votre conformité

Les déclarations à la CNIL ne sont plus de rigueur. A contrario, vous devez apporter la preuve à tout moment du bon respect des règles relatives à la protection des données : mise en place d'un registre des activités de traitement, registre de violation de données, process de sécurité, sensibilisation des collaborateurs...

Un plan d'actions s'impose : pour plus d'efficacité, les équipes spécialisées d'Espar6 vous accompagne à travers E6-RGPD, la plateforme numérique de pilotage de votre mise en conformité.

Sécurisez votre entreprise

L'actualité témoigne d'un nombre de plus en plus important de failles de sécurité et d'attaques informatiques. Ces dernières peuvent avoir des conséquences désastreuses sur l'activité de vos entreprises. Certains d'entre vous, qu'Espar6 accompagne, se reconnaîtront, ayant vécu avec leurs équipes des moments particulièrement difficile ces derniers mois...

Ainsi, pour mettre en place une cybersécurité efficace donnant à votre activité une résilience optimale :

Sauvegardez tous vos équipements sans restriction, installez des outils de protection professionnels. Quant aux systèmes « gratuits », on sait que si c'est gratuit... c'est vous le produit !

Et faites-vous accompagner pour simplement assurer la pérennité de vos activités en cas de sinistre...

Conclusion

La donnée, un actif des plus critiques pour vos entreprises
Les cybermenaces sont bien réelles et ne cessent d'évoluer. Depuis quelques années, la question n'est plus de savoir si vous subirez des cyberattaques, mais plutôt quand elles se produiront et quelle sera leur ampleur. La préparation est donc essentielle même pour les plus petits d'entre vous...

Dans ce contexte de cyber risques omniprésents, le RGPD est une occasion forte de se poser les bonnes questions sur son activité et ses process mais cela peut devenir aussi un réel avantage concurrentiel.

En ayant une gestion rigoureuse de vos données, vous gagnez donc en efficacité et en productivité !

Une opportunité de sceller une relation de confiance avec vos interlocuteurs (clients, partenaires, fournisseurs, collaborateurs...) et d'améliorer votre image de marque !

Espar 6 est une société de services et de technologies dont la mission est d'assurer la cyber-sécurité des PME européennes.
Nous améliorons drastiquement la protection des ordinateurs de nos clients et nous formons les salariés à devenir plus vigilants en matière de cyber sécurité. Notre équipe d'ingénieurs, d'experts en cybersécurité et de data scientists est focalisée sur la protection des données de nos clients (RGPD) et plus généralement sur l'amélioration du niveau de la lutte contre la cyber criminalité en Europe.
Espar 6 a développé une plateforme numérique collaborative E6-RGPD pour accompagner les entreprises dans leur programme de mise en conformité en leur donnant « autonomie et cadre réglementaire ».
Contact : Espar System SAS - Mail : contact@espar6.com - site web : www.espar6.com
Tél : +33 (0) 987 388 512
Président : Olivier GOURIO, ex CEO & Fondateur du Groupe Hôtels & Patrimoine