

QUELLE APPLICATION ET QUELLES SANCTIONS ?

Depuis le 25 mai 2018, toutes les entreprises qui acquièrent, collectent, stockent ou traitent des données doivent être en conformité avec le RGPD. « *Pourtant, selon plusieurs études concordantes au niveau européen, près d'un tiers des entreprises ne sont toujours pas en règle. Le taux varie en fonction des pays et la France se situe plutôt dans la moyenne basse, révèle Gérard Paya. Les grands groupes nationaux et internationaux sont plus en avance que les PME, car ils font face à des risques très élevés en termes de sanctions.* ».

Actuellement, la CNIL peut prononcer des sanctions administratives, dont le plafond est fixé à 3 millions d'euros, mais qui peut être rehaussé à 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial pour les infractions les plus graves. Et ces sanctions administratives peuvent être complétées par des condamnations pénales prévues aux articles 226-16 et R 625-10 du Code pénal, qui visent, dans certaines hypothèses, les dirigeants à titre personnel. Et là aussi les sanctions sont lourdes, puisqu'elles peuvent aller jusqu'à cinq ans d'emprisonnement et 300 000 euros d'amende dans les cas les plus graves.

« *Le RGPD est un texte juridique très complexe. Tout le challenge consiste à le rendre accessible et opérationnel rapidement dans les entreprises, notamment les PME* », précise Gérard Paya, qui a mis au point, avec la 2FPCO, des modules de formation destinés à toutes les entreprises du secteur de l'objet média.

LES GRANDES ÉTAPES DE LA MISE EN CONFORMITÉ

« *Il faut créer une équipe ad hoc et nommer un référent, qui va piloter les différents services qui manipulent des données personnelles au sein de l'entreprise* », explique le consultant, qui a identifié cinq grandes étapes pour se mettre en conformité avec le règlement :

- Comprendre le RGPD (par une recherche personnelle d'informations ou via une formation).
- Construire un registre des traitements de données personnelles (typologie des données collectées, identification de leur caractère sensible ou non sensible, finalité du traitement des données, durée de conservation des données, destination des données).
- Évaluer les risques liés à la confidentialité, la protection et la sécurisation des données personnelles (système informatique, site internet, sous-traitants, etc.).
- Contractualiser les obligations RGPD avec ses prestataires (fournisseurs, sous-traitants).
- Garantir les droits des personnes physiques (notamment l'obligation d'information).

LES OPPORTUNITÉS DE LA RGPD

Au-delà des contraintes légales, Gérard Paya estime que cette mise en conformité doit être l'opportunité de réorganiser les entreprises. Le consultant identifie trois grandes raisons de profiter de la RGPD pour aller au-delà des simples dispositions légales.

- **NETTOYER ET QUALIFIER SES BASES DE DONNÉES :**
 - Vérifier que les bases de données contiennent des contacts réellement actifs.
 - Identifier à quelle fréquence les clients passent commande.
 - Éliminer les données qui ne servent à rien.
 - S'assurer que le sous-traitant informatique ne partage pas les données de l'entreprise avec d'autres sociétés.
- **POUVOIR ÊTRE RÉFÉRENCÉ SI UN CLIENT IMPOSE LA CONFORMITÉ AU RGPD DANS SON CAHIER DES CHARGES (OU DANS UN APPEL D'OFFRES) :**
 - De plus en plus de clients vont demander cette conformité afin de se protéger eux-mêmes.
 - Pouvoir répondre si des clients demandent à exercer leurs droits concernant leurs données personnelles.
 - Savoir quoi faire en cas de vol ou de perte d'intégrité des données personnelles des clients.
 - Être sûr que les données ne sont pas transférées hors de l'Union Européenne.
- **VÉRIFIER QUE L'INFRASTRUCTURE INFORMATIQUE PERMETTE D'ASSURER LA CONFIDENTIALITÉ ET LA SÉCURISATION DES DONNÉES :**
 - Se protéger efficacement contre les attaques informatiques.
 - Revoir son contrat de sous-traitance informatique, afin de clarifier les obligations du sous-traitant (en charge du traitement, votre entreprise sera tenue pour responsable si les données clients sont violées chez le sous-traitant, quel que soit le motif).
 - Sauvegarder régulièrement les données, pour reprendre l'activité en cas d'incident.

LA FORMATION

Gérald PAYA a construit, avec la 2FPCO, un programme de formation RGPD en trois modules, accessible aux adhérents de la Fédération, comme aux non-adhérents, avec une méthodologie et un langage adaptés aux PME, et tenant compte des moyens et ressources disponibles dans les entreprises.

- **MODULES 1 ET 2** en inter-entreprises (deux jours) : acquérir les fondamentaux et initier la mise en conformité.
- **MODULE 3** en intra-entreprise (deux à six jours) : maîtriser la mise en œuvre et créer de la valeur ajoutée (modules 1 et 2 inclus, avec en complément une formation spécifique dotée d'outils complémentaires)

PROCHAINES DATES

— 28 et 29 août 2018 — 18 et 19 sept. 2018 — 11 et 12 sept. 2018

CONTACT : Juliette SALOMÉ (2FPCO) au 01.47.65.84.98
ou juliette.salome@2fpc.com