RGPD : comment se mettre en conformité ?

Le **règlement européen sur la protection des données (RGPD)** est entré en vigueur le 25 mai 2018. Ce texte introduit également une plus grande responsabilité des entreprises sur les conditions de recueil des données personnelles, leur gestion et leur sécurité.
Cette situation a conduit notamment la Cnil, l'organisme de contrôle de la gestion des données personnelles, à éditer des fiches techniques et un guide afin d'aider les entreprises à entamer une démarche de mise en conformité. Une bonne occasion de s'en inspirer pour présenter les grands principes du RGPD et la marche à suivre pour les appliquer.

QUI EST CONCERNÉ ?

Tout organisme (entreprise, cabinet, association ...), privé ou public, est tenu d'appliquer le RGPD dès lors qu'il collecte ou traite des données personnelles pour son compte ou pour celui d'un tiers. Aucun autre critère, comme l'effectif ou encore le chiffre d'affaires, n'entre ici en ligne de compte. Tous les professionnels libéraux sont donc concernés, ou potentiellement concernés, y compris les plus petits.

UNE DONNÉE PERSONNELLE

Une donnée personnelle est une information qui permet, à elle seule ou en la croisant avec d'autres données, d'identifier une personne soit directement (nom, prénom), soit indirectement (téléphone, courriel, adresse, photo, voix, caractéristiques sociales ou physiques, empreintes, ADN ...). Dès lors qu'il regroupe ce type d'informations, un fichier (papier ou numérique) est considéré comme un traitement de données personnelles et doit ainsi être constitué et géré conformément au RGPD.

RECENSER L'EXISTANT...

Pour se mettre en conformité, le premier travail consiste à recenser l'existant. Ainsi existe-t-il sans doute dans votre structure des fichiers de données personnelles tels que nous venons de les définir (fichiers clients, prospects, fournisseurs, employés, fichiers paie, formations, gestion des accès ...). Tous doivent être recensés dans un registre. Registre dans lequel, pour chaque traitement, doivent être renseignés sa finalité, le type de données personnelles présentes (noms, salaires, adresses ...), les personnes ou les services qui peuvent y accéder et enfin la durée de conservation de ces données.
Sachez à ce titre que des modèles de registres sont téléchargeables sur le site de la Cnil www.cnil.fr

... POUR IDENTIFIER LES ACTIONS À MENER

Le principe du RGPD consiste à responsabiliser les détenteurs de fichiers. Il vous revient donc, en tant que dirigeant, d'adopter une approche raisonnée de ces traitements et de leur gestion. Sachant que les données personnelles ne doivent pas être conservées au-delà de ce qui est nécessaire.

Pour chacun des traitements mis en œuvre, vous devez donc vous poser les questions suivantes

- ***- AI-JE ENCORE BESOIN DE CES INFORMATIONS ?***

Il est possible que vous ayez créé des fichiers il y a quelques années dans un objectif qui n'est plus d'actualité. Si c'est le cas, vous n'avez plus besoin de ces traitements. Supprimez-les.
Vous devez également vérifier que chaque type d'information recueilli pour le traitement est absolument nécessaire. Si ce n'est pas le cas, supprimez les types de données non pertinents.

Enfin, vous devez faire en sorte que vos fichiers soient mis à jour régulièrement. Autrement dit, que les données qui n'ont plus rien à y faire soient supprimées : données relatives à d'anciens clients dans une base clients, informations dont la durée de conservation est dépassée ...

- ***QUI ACCCÈDE À CES DONNÉES ?***

Seules les personnes habilitées doivent pouvoir accéder aux données personnelles. Vous devez donc veiller à les compartimenter (les mettre sous clé s'il s'agit d'informations papier, ou sur un espace à accès restreint lorsqu'elles sont numériques).

- ***CES INFORMATIONS SONT-ELLES PROTÉGÉES ?***

Vous êtes responsable des données personnelles que vous hébergez ou que vous faites héberger par un prestataire. Vous devez donc prendre les mesures nécessaires pour minimiser les risques d'atteinte à leur intégrité et à leur confidentialité. Ainsi, pour chaque traitement, il vous faut évaluer le niveau de sécurité existant (complexité des mots de passe, performance et mise à jour des antivirus, politique de chiffrement, sécurité des locaux, politique de sauvegarde ...) et, le cas échéant, le rehausser.

RESPECTER LES DROITS DES PERSONNES FICHÉES

Les personnes " fichées " ont des droits sur leurs données. Droits que vous devez respecter tant lors de la création qu'au cours de la gestion du traitement.
Ainsi, lorsque vous collectez des données personnelles, vous devez informer les personnes concernées de la finalité du traitement, de la raison de ce recueil de données et du délai pendant lequel elles seront conservées, leur préciser les personnes qui auront accès à ces données (service, prestataire ...) et leur indiquer les modalités d'exercice de leurs droits (via une messagerie, un espace dédié sur un site ...).
Parmi ces droits figurent, notamment, un droit d'accès leur permettant de connaître l'ensemble des données les concernant, un droit de rectification (permettant de les corriger), un droit d'opposition et d'effacement (lorsque le fichier n'est pas obligatoire) ; Il vous revient donc de mettre en place un processus offrant à ces personnes la possibilité d'exercer leurs droits simplement et rapidement.