Le RGPD, c'est quoi ?

Le règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données, ou RGPD) est le texte de - référence européen en matière de protection des données personnelles des résidents de l'UE.

Tous les organismes privés et publics avaient jusqu'au 25 mai 2018 pour se mettre en conformité.

Comment identifier les données personnelles traitées par votre entreprise ?

Ce sont toutes les informations concernant une personne physique identifiée ou identifiable (directement ou indirectement), que cette personne soit un client, un fournisseur, un salarié ou un dirigeant.
Les données personnelles subissent de nombreux types d'opérations qu'elles soient informatiques ou non (papier), notamment : la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.
Ce sont ces traitements de données qui doivent être sécurisés dans le cadre du RGPD (exemples : mailing list, sites internet, fichiers des fournisseurs, des clients, des salariés…).

Le RGPD distingue deux types de responsabilité : le (ou les) responsable(s) de traitement et le sous-traitant.
- Le responsable de traitement est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres (il y a alors co-responsabilité), détermine les finalités (objectif
principal, par exemple : gestion des recrutements, gestion des clients, enquête de satisfaction, surveillance des locaux, etc.) et les moyens du traitement.
- Le sous-traitant est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

Concrètement, que faire ?

1.Désigner un délégué à la protection des données : Il sera le chef d'orchestre de la conformité au RGPD. Il exercera une mission d 'information, de conseil, de contrôle en interne et sera le point de contact avec la Commission nationale de l'informatique et des libertés (CNIL), autorité de contrôle. Pour commencer, il
déterminera le plan d'actions amenant à la conformité globale et informera et sensibilisera les équipes.
2.Cartographier les traitements de données personnelles et prioriser les actions : Il faut recenser de façon précise les traitements de données personnelles et les inscrire dans un registre. La CNIL a élaboré un modèle de registre simple et didactique à destination des TPE/PME qui facilite sa prise en main et sa tenue. Vous pouvez le retrouver sur
www.cnil.fr/fr/rgpd-et-tpepme-un-nouveau-modele-de-registre-plus-simple-et-plus-didactique.
3.Organiser les processus internes et documenter la conformité : Il faut mettre en place des procédures internes qui garantissent la prise en compte de la protection des données à tout moment, en prenant en compte l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement.
4.Maintenir la conformité : Pour prouver votre conformité au règlement, il faut constituer et regrouper la documentation nécessaire. Les actions et documents réalisés à chaque étape doivent être réexaminés et actualisés régulièrement pour assurer une protection des données en continu.

Textes officiels disponibles sur www.cnil.fr/fr/textes-officiels-europeens-protection-donnees