NOTE

Soucieux de toujours être proche de l'actualité et de vous apporter une information claire, et en temps réel, nous vous adressons ci-après une note concernant le Règlement Général sur la Protection des Données (RGPD).

A compter du 25 mai 2018, toutes les entreprises qu'elles soient basées au sein de l'Union Européenne ou non devront être en conformité avec les règles édictées par le règlement européen du 27 avril 2016 relatif à la protection des données personnelles, dès lors qu'elles collectent des données concernant des citoyens européens.

La gestion des ressources humaines est directement impactée au sein des entreprises dans la mesure où elle génère une collecte, un traitement et un stockage de nombreuses données personnelles sur les salariés à l'occasion des recrutements, embauches, payes, entretiens, etc...

En conséquence, il convient de vous mettre en conformité afin d'éviter les sanctions non seulement pécuniaires mais aussi accessoires pouvant avoir un impact sur votre activité.

L'ensemble des questions que vous pourrez vous poser lors de la mise en conformité sont les suivantes : Qu'est-ce que le RGPD ? Quelles sont les données à protéger ? Quelles sont les sanctions en cas de non-conformité ? Quel impact en matière de gestion des ressources humaines ? Comment se mettre en conformité ? Une note d'information pour les salariés ?

Le RGPD introduit un changement majeur dans le domaine de l'informatique et des libertés : le passage d'un système de déclarations obligatoires auprès de la CNIL à un système d'autorégulation dans lequel les entreprises devront être en mesure de prouver à tout moment qu'elles respectent les règles.

Il s'impose dans toutes les entreprises de tous les pays européens et a valeur législative. Contrairement aux directives européennes, il n'est pas nécessaire qu'il soit transposé en droit interne ; il est d'application directe. **Il entre en application le 25 mai 2018.**

Le règlement européen dispose dans son article 32 que : "*le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque*".

Or, il est parfois difficile, lorsque l'on n'est pas familier avec les méthodes de gestion des risques, de mettre en œuvre une telle démarche et de s'assurer que le minimum a bien été fait.

Pour aider les professionnels dans leur mise en conformité, la CNIL publie un guide rappelant les précautions élémentaires devant être mises en œuvre de façon systématique.

Ce guide peut être utilisé dans le cadre d'une gestion des risques, constituée des quatre étapes suivantes :

1. **Recenser les traitements** de données à caractère personnel, les données traitées (ex *: fichiers client, contrats)* et les supports sur lesquels elles reposent.
2. **Apprécier les risques** engendrés par chaque traitement :

- En identifiant les impacts potentiels sur les droits et libertés des personnes concernées, les sources de risques (qui ou quoi pourrait être à l'origine de chaque évènement redouté ?) et les menaces réalisables (qu'est-ce qui pourrait permettre que chaque évènement redouté survienne ?).
- En déterminant les mesures existantes ou prévues qui permettent de traiter chaque risque (ex : contrôle d'accès, sauvegardes, traçabilité, sécurité des locaux, chiffrement, anonymisation)
- En estimant enfin la gravité et la vraisemblance des risques, au regard des éléments précédents (exemple d'échelle utilisable pour l'estimation : négligeable, modérée, importante, maximale).

3. **Mettre en œuvre et vérifier les mesures prévues**.
4. **Faire réaliser des audits de sécurité périodiques**.

La CNIL met à disposition une liste de questions à se poser afin d'évaluer le niveau de sécurité des données personnelles de votre entreprise (voir grille d'analyse ci-jointe).

Sources : LEGISOCIAL - CNIL.FR