Le Contexte réglementaire RGPD

Entré en application le 25 mai 2018, le **Règlement Général sur la Protection des Données** (RGPD) s'inscrit dans la continuité de la Loi française « Informatique et Libertés » de 1978 et **renforce le contrôle** par les citoyens de l'utilisation qui peut être faite des données les concernant.

Ce texte **harmonise** les règles en Europe en offrant un **cadre juridique unique** aux professionnels et permet de développer leurs activités numériques au sein de l'Union européenne en se fondant sur la **confiance des utilisateurs**. Il apporte de nombreuses modifications en matière de sécurité des données à caractère personnel et rend **obligatoire** leur application.

En effet, le non-respect de ces nouvelles obligations entraîne des **sanctions lourdes** (amendes administratives pouvant aller jusqu'à 20 000 000€) *conformément aux articles 83 et 84 du RGPD*.

Le RGPD **s'applique à toute organisation**, publique et privée, qui **traite des données personnelles** pour son compte ou non, dès lors :

- qu'elle est établie sur le territoire de l'Union européenne ;
- que son activité cible directement des résidents européens.

Les spécificités du RGPD

Le RGPD **supprime les déclarations** à effectuer auprès de la CNIL. En contrepartie, les administrations, sociétés et associations traitant des données à caractère personnel, mais aussi leurs prestataires et sous-traitants, sont désormais **pleinement responsables de la protection des données qu'ils traitent.**

Il leur appartient d'**assurer la conformité** au RGPD de leurs traitements de données personnelles dès la conception et tout au long de leur cycle de vie (**Privacy By Design**). Ils doivent être en mesure de démontrer cette conformité à tout moment.

Par définition : une **donnée à caractère personnelle** concerne toute information se rapportant à une personne physique identifiée ou identifiable **directement ou indirectement** (par recoupement).

Un « traitement de données personnelles » est une **opération**, ou ensemble d'opérations, **portant sur des données personnelles**, quel que soit le procédé utilisé.
(*collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission, diffusion).*

Le traitement n'est pas nécessairement informatisé : les fichiers papier sont également concernés et doivent être protégés dans les mêmes conditions.

Chaque traitement de données doit avoir un objectif, une **finalité**, c'est-à-dire qu'on ne peut pas collecter ou traiter des données personnelles simplement au cas où cela serait utile un jour.

Chaque traitement de données doit être légal et légitime au regard de l'activité de l'organisme. Les utilisateurs doivent être informés du traitement qui est fait sur leurs données.

Les traitements doivent en conséquence respecter ces **principes** :

• **Licéité** (Base légale : consentement, contrat, obligation légale, intérêts vitaux, intérêt public, ou intérêt légitime)
• **Finalité** (Ne pas dépasser la limite définie par le traitement initial)
• **Minimisation** (Pertinence/Proportionnalité)
• **Durée limité** (Durée de conservation)
• **Sécurité** (Intégrité/Confidentialité)
• **Droits des personnes** (accès, rectification, droit à l'oubli, information)

Toute personne confiant ses données personnelles établit une relation de confiance et souhaite le **respect de ses droits et de sa vie privée**.

Le RGPD réaffirme les droits pour les personnes concernées, garantissant ainsi la **maîtrise de leurs données**. Respecter ces droits contribue à valoriser une image d'organisme sérieux et responsable.

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 importantes** et entraîner la fuite de données personnelles. Les données personnelles doivent faire l'objet de mesures de sécurité particulières, informatiques et physiques. Protéger son patrimoine informationnel et protéger les personnes concernées des atteintes à leurs données, c'est renforcer la confiance des administrés.

Pour plus d'informations veuillez consulter le site de la CNIL : https://www.cnil.fr/