



Guide mise en conformité au RGPD



1ER AOUT 2024

**Fédération de l'Exercice Coordonné et des
MAisons de santé en Grand-Est**

Immeuble Thiers Bureaux – 9^{ème} Etage

4, Rue Piroux

54048 NANCY CEDEX

Préambule :

Le **règlement général sur la protection des données (RGPD)** en application depuis le 25 mai 2018 fait suite à la Loi française Informatique et Libertés de 1978. En effet le cadre juridique permettant de protéger les données personnelles évolue et se renforce car il faut suivre les évolutions des technologies et de nos sociétés, qui entraînent une collecte de données personnelles de plus en plus importante (usages accrus du numérique, développement du commerce en ligne...).

Il permet une harmonisation du traitement des données personnelles au niveau européen.

Toute organisme qu'il soit public ou privé, de petite ou de grande taille, dès l'instant qu'il traite des données personnelles doit se mettre en conformité au RGPD.

Quelques définitions :

- ✚ **Donnée personnelle** : toute information se rapportant à une personne physique identifiée ou identifiable

Une personne peut être identifiée :

- ✓ directement (exemple : nom, prénom)
- ✓ ou indirectement (exemple : par un identifiant (n° client), un numéro (de téléphone), une donnée biométrique, plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale, mais aussi la voix ou l'image).

L'identification d'une personne physique peut être réalisée :

- ✓ à partir d'une seule donnée (exemple : numéro de sécurité sociale, ADN)
- ✓ à partir du croisement d'un ensemble de données (exemple : une femme vivant à telle adresse, née tel jour, abonnée à tel magazine et militant dans telle association)

Exemple : une base marketing contenant de nombreuses informations précises sur la localisation, l'âge, les goûts et les comportements d'achats de consommateurs, y-compris si leur nom n'est pas stocké, est considérée comme un traitement de données personnelles, dès lors qu'il est possible de remonter à une personne physique déterminée en se basant sur ces informations.

Source : CNIL

- ✚ **Traitement de donnée personnelle** : 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 ou toute autre forme de mise à disposition, rapprochement).

Exemple : tenue d'un fichier de ses clients, collecte de coordonnées de prospects via un questionnaire, mise à jour d'un fichier de fournisseurs, etc.

Par contre, un fichier ne contenant que des coordonnées d'entreprises (par exemple, entreprise « Compagnie A » avec son adresse postale, le numéro de téléphone de son standard et un email de contact générique « compagnieA@email.fr ») n'est pas un traitement de données personnelles.

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

Un traitement de données doit avoir un objectif, une finalité, c'est-à-dire que vous ne pouvez pas collecter ou traiter des données personnelles simplement au cas où cela vous serait utile un jour. A chaque traitement de données doit être assigné un but, qui doit bien évidemment être légal et légitime au regard de votre activité professionnelle.

Exemple : vous collectez sur vos clients de nombreuses informations, lorsque vous effectuez une livraison, éditez une facture ou, proposez une carte de fidélité. Toutes ces opérations sur ces données constituent votre traitement de données personnelles ayant pour objectif la gestion de votre clientèle.

Source : CNIL

Le RGPD respecte 6 grands principes :

- ✓ Ne collectez que les données qui sont nécessaire
- ✓ Informez les personnes de la collecte de leurs données personnelles ainsi que de leurs droits
- ✓ Facilitez et organisez le recours aux droits des personnes concernant leurs données personnelles
- ✓ Respectez les durées de conservation des données personnelles
- ✓ Sécurisez des données personnelles collectées
- ✓ Maintenez la mise en conformité au RGPD à jour