RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES (RGPD)

QU'EST-CE QUE LE RGPD ?

Le sigle RGPD signifie « Règlement Général sur la Protection des Données » (en anglais « Général Data Protection Régulation » ou GDPR). Le RGPD encadre le traitement des données personnelles sur le territoire de l'Union européenne.

Le contexte juridique s'adapte pour suivre les évolutions des technologies et de nos sociétés (usages accrus du numérique, développement du commerce en ligne…).

Ce nouveau règlement européen 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.

Il harmonise les règles en Europe en offrant un cadre juridique unique aux professionnels. Il permet de développer leurs activités numériques au sein de l'UE en se fondant sur la confiance des utilisateurs.

Depuis mai 2018, le RGPD prévoit des pénalités plus importantes qu'auparavant en cas de mauvaise utilisation des données personnelles. Même si votre entreprise est consciente des changements en profondeur qui s'imposent, vous ne savez peut-être pas par quoi commencer...

RGPD : de quoi parle-t-on ?

Donnée personnelle, traitement de données, RGPD, de quoi s'agit-il ? Sommes nous concernés ?

Qu'est-ce qu'une donnée personnelle ?

La notion de « données personnelles » est à comprendre de façon très large.

Une « donnée personnelle » est « 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.

Qu'est-ce qu'un traitement de données personnelles ?

Cette notion est également très large.

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 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.

Qui est concerné par le RGPD ?

Tout organisme quels que soient sa taille, son pays d'implantation et son activité, peut être concerné.

En effet, 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**,
- ou que son activité cible directement des **résidents européens**.

Par exemple, une société établie en France, qui exporte l'ensemble de ses produits au Maroc pour ses clients moyen-orientaux doit respecter le RGPD.

De même, une société établie en Chine, proposant un site de e-commerce en français livrant des produits en France doit respecter le RGPD.

Le RGPD **concerne aussi les sous-traitants** qui traitent des données personnelles pour le compte d'autres organismes.

Ainsi, si vous traitez ou collectez des données pour le compte d'une autre entité (entreprise, collectivité, association), vous avez des obligations spécifiques pour garantir la protection des données qui vous sont confiées.

Le processus idéal

Voici une approche de quatre mesures qu'il est recommandé de prendre pour savoir quelles données personnelles nous collectons et comment les gérer :

1. IDENTIFIEZ LES DONNÉES QUE NOUS POSSÉDONS

Le meilleur moyen de se conformer au RGPD est de procéder à un audit complet du patrimoine informationnel. Nous devons savoir exactement quelles données la Coopérative détient, que ce soit au format physique ou électronique. Sont concernées aussi toutes les informations partagées avec les fournisseurs et autres tierces parties, ainsi que nos archives.

2. LOCALISEZ LES DONNÉES

Une fois que vous savez ce que vous détenez, il vous faut savoir où se trouvent ces informations. Sont-elles centralisées ou bien réparties sur différents systèmes et dans des formats divers ? Ont-elles été dupliquées? Se trouvent-elles dans un environnement géré ou sur des équipements locaux (notamment des ordinateurs portables et autres équipements nomades) ? Savez vous qui y accède et si elles sont partagées avec des tiers?

3. INTERROGEZ-VOUS SUR LA LÉGITIMITÉ DE DÉTENIR CES DONNÉES

Il s'agit là d'un point important que doit aborder toute entreprise. En effet, il existe tellement de types de données personnelles et de moyens différents de les collecter que chaque situation doit être traitée de manière individuelle. Le RGPD repose sur des principes spécifiques qui vous invitent à vous demander si vous avez le droit de collecter, d'utiliser et de stocker des données personnelles. En cas de doute, interrogez-vous sur la pertinence pour votre activité de détenir des données personnelles actives et archivées.

4. DÉTERMINEZ LA DURÉE NÉCESSAIRE DE CONSERVATION DES DONNÉES EN VOTRE POSSESSION

Le RGPD ne précise pas combien de temps vous devez conserver des données personnelles. Cependant, une durée de conservation doit être définie pour chaque donnée, une durée qui est fonction de la réglementation appropriée et des besoins opérationnels de l'entreprise.

Vous pourrez ensuite créer un programme de conservation des archives qui détaille les données personnelles que vous collectez, pourquoi et pendant combien de temps. N'oubliez pas que le RGPD a introduit le principe du « Droit à l'oubli », ce qui vous obligera certainement à supprimer des données personnelles dès qu'on vous le demande, sauf si vous pouvez avancer une raison valable pour les conserver.

ÉTAPE SUIVANTE

Une fois la lecture de ces étapes terminée, vous disposerez des ingrédients incontournables à portée de main pour réaliser votre mise en conformité dans les règles de l'art du RGPD, notamment :

- Protection des données
- Droits des personnes
- Confidentialité
- Consentement

Comment appliquer le RGPD à sa structure ?

Selon **l'article 5.1 du RGPD**, les données personnelles doivent être :

- Traitées de manière licite, loyale et transparente ;
- Collectées à des fins déterminés, explicites et légitimes ;
- Adéquates, pertinentes et limitées ;
- Exactes et tenues à jour ;
- Conservées pendant une durée raisonnable ;
- Traitées de façon à garantir leur protection.

Pour se mettre en conformité avec le RGPD et respecter les six obligations énoncées par la CNIL ci-dessus, il est important de mettre en place certaines actions essentielles :

Le RGPD au sein des petites structures

Il faut être vigilant et veiller au respect des 5 droits des personnes selon la CNIL :

- le droit d'accès,
- le droit de rectification,
- le droit à l'effacement,
- le droit d'opposition,
- le droit à la portabilité.

Ces droits sont fondamentaux et chaque individu en lien avec la Structure (*client, administrateur, sociétaire, coopérateur, adhérent associatif, membre ou autres*) peut demander si ces droits sont bien respectés.

Procéder à une note explicative des flux de données personnelles. Cette note doit expliquer l'objectif des traitements de données effectués, le type des traitements et le rôle des personnes qui les manipulent. C'est dans ce sens que la CNIL demande à **cartographier les bases de données** de la Structure pour identifier les secteurs d'activité et s'assurer du bon respect du règlement.

Aussi, il est possible d'augmenter la **sécurité des données personnelles** par des actions très simples. Les Structures doivent **mettre à jour leurs antivirus et leurs logiciels** mais aussi changer régulièrement de mots de passe en les rendant complexes. Cela permet d'assurer la sécurité des données personnelles en minimisant le risque de piratage ou de perte de données.

Le RGPD ne soulève finalement pas que l'enjeu de la protection des données personnelles. Cette loi modifie la manière dont les entreprises doivent penser leur approche vis à-vis de leur clientèle en respectant la confidentialité de leurs données. Elle incite donc à repenser leur organisation et leur culture d'entreprise pour se recentrer sur le client. Plutôt que d'envisager le RGPD comme une contrainte, les entreprises doivent l'appréhender comme l'opportunité de renforcer la confiance du client dans leur structure pour finalement augmenter leur satisfaction. La refonte de leur modèle sera dès lors positive.

En annexe, un modèle de protocole que vous pouvez mettre en place au sein de votre association à destination de vos adhérents.

- modèle protocole RGPD