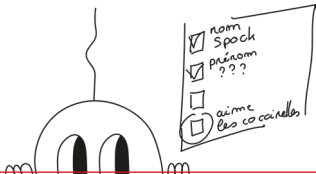




#6

Le RGPD

Le RGPD, vaste sujet qui concerne la quasi totalité des professionnels qui «traitent des données personnelles» et pas que sur leur site internet. Pour comprendre ce que le RGPD change désormais, il est important de bien saisir la définition d'une donnée personnelle, mais également le processus de traitement de données, afin de savoir si vous êtes concerné par l'application de ces nouvelles normes européennes.



La notion de données personnelles

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) ou 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.

La notion de traitement de données

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.

Un « traitement de données personnelles » est donc 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.

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

Le RGPD

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

Qui est concerné ?

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.

