RGPD - Règlement Général sur la Protection des Données

Si vous collectez ou bien traitez des données personnelles, alors vous êtes forcément concerné par le RGPD, le Règlement Général sur la Protection des Données, qui s'applique désormais aux organismes publics et privés traitant des données personnelles.
Comprendre le RGPD est alors fondamental, afin de prendre les mesures nécessaires à la garantie d'une utilisation respectueuse de ces données et de la vie privée des personnes concernées.

Que cache le terme « donnée personnelle » ?

Quand on parle d'une **donnée personnelle**, il faut prendre la notion au sens large.
Une information personnelle se réfère à toute information rattachée à une personne identifiée, ou bien identifiable grâce auxdites données. Il peut s'agir de données telles qu'un nom et un prénom, permettant donc une identification directe de la personne concernée, ou bien un numéro de téléphone, un numéro client, des critères génétiques, économiques, des marqueurs sociaux et culturels ou encore la voix ou bien l'image d'une personne, entraînant alors son identification indirecte.
De cette manière, une personne physique peut être identifiée à partir d'un croisement de plusieurs données, ou bien à partir d'une seule donnée comme son ADN ou son numéro de sécurité sociale.

Concrètement, dès lors qu'une base de données comprend une ou plusieurs informations précises permettant de remonter à une personne physique pouvant être identifiée via une ou plusieurs de ces informations, il s'agit bien de traitement de données personnelles.

Que cache le terme de « traitement de données personnelles » ?

La notion de **traitement de données personnelles** dans le cadre du RGPD s'entend également au sens large, le nouveau règlement européen le définissant comme une ou plusieurs opérations visant des données personnelles, et ce, quel que soit le procédé utilisé (collecte directe de données, enregistrement, triage de données, mais aussi organisation, conservation, modification, transfert, utilisation, consultation, diffusion et toute autre forme de disposition de ces données).

Le champ d'application est donc large, le traitement de données personnelles pouvant aller de la simple tenue d'un fichier clients, jusqu'à la mise à jour d'un fichier concernant des fournisseurs, etc.

Il est important de noter que le processus de traitement de données personnelles n'est pas forcément informatisé. En effet, les fichiers de type papier sont aussi soumis aux normes du RGPD et doivent en ce sens bénéficier des mêmes mesures de conservation et de protection des données personnelles.

Concernant le traitement de ces informations, le RGPD est clair : tout traitement de données doit avoir un objectif clairement défini. C'est-à-dire que chaque traitement de données doit servir un but bien précis, en accord avec l'activité professionnelle de l'organisme qui la réalise. Par exemple, collecter des données clients lors d'une livraison ou bien pour éditer une facture est un traitement de données personnelles légitime, ayant pour but la gestion d'une clientèle.

Qui est soumis à la RGPD ?

Le RGPD est susceptible de s'appliquer à tout organisme traitant des données personnelles dans le cadre de son activité ou pour le compte d'un tiers, et ce quels que soient son pays d'implantation, sa taille et son activité. Toute organisation relevant de ce champ d'action, publique comme privée, est concernée dès lors qu'elle se trouve établie sur **le territoire de l'Union européenne** ou bien que son activité cible directement des **citoyens européens**.

Concrètement, une société établie en France et dont l'activité est l'export de produits aux États-Unis est concernée par le RGPD. De même, une société dont le siège se trouve au Maroc et livrant des produits en Espagne est également concernée par le nouveau règlement européen concernant le traitement des données personnelles.

Le RGPD concerne également les sous-traitants dont l'activité est de traiter des données personnelles pour le compte d'autres sociétés.

Les obligations :

Le RGPD dresse une liste d'obligations pour les sociétés qui traitent des données personnelles de leurs utilisateurs ou clients.

Les points essentiels :

- **Licéité du traitement** : le traitement et la collecte de la donnée doivent être effectués uniquement dans une liste de cas défini par le RGPD. Par exemple, la collecte doit être faite uniquement avec le consentement de la personne concernée par la donnée.
- **Finalité du traitement** : la donnée doit être collectée pour répondre à un objectif précis et non pas « au cas où » ou en tant que fin en soi. L'utilisation réelle de la donnée doit correspondre à cet objectif.
- **Minimisation des données** : l'entreprise ne doit collecter et utiliser que les types de données utiles à l'objectif initial (et non des données superflues).
- **Protection particulière des données sensibles** : les données dites sensibles (par exemple, médicales, financières, etc) doivent faire l'objet d'une protection accrue, via un chiffrement des données par exemple.
- **Limitation de la durée de conservation des données** : les données doivent être supprimées lorsqu'elles ne sont plus utiles. La durée de conservation de la donnée dépend de la nature des données. Par exemple, la CNIL recommande de supprimer les coordonnées d'un prospect, en l'absence d'échange, au bout de 3 ans.
- **Obligation de sécurité** : quelle que soit la nature de la donnée concernée, des principes de sécurité doivent être appliqués (chiffrement, limites des accès à la donnée…)
- **Transparence** : les personnes dont les données sont collectées doivent être informées et consentir à la collecte, mais aussi aux finalités et à l'utilisation qui seront faites de la donnée.
- **Droit des personnes** : les droits des personnes dont les données sont collectées sont protégés par le RGPD : droit à l'oubli, droit de s'opposer au traitement, droit d'accès à la donnée…

Ces principes doivent faire l'objet d'un suivi par une personne responsable.

Les applicatifs doivent être pensés avec les principes énoncés précédemment.

Sources originales :

https://donnees-rgpd.fr/definitions/rgpd-pour-les-nuls/

https://www.seald.io/fr/blog/le-rgpd-pour-les-nuls-3-minutes-pour-tout-comprendre