NOUVELLE REGLEMENTATION RGPD

Agence d'Attractivité de la Drôme
8, Rue Baudin – CS 40531 – 26004 Valence Cedex
+33 (0) 4 75 82 19 26 – info@drome-attractivite.com

DONNEE PERSONNELLE

Une donnée personnelle est « toute information se rapportant à une personne physique identifiée ou identifiable ».

Une personne peut être identifiée :

- directement (exemple : nom, prénom)
- 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).

TRAITEMENT DE DONNEES PERSONNELLLES

Un **traitement de données personnelles** est une opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé (collecte, conservation, extraction…)
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.

RGPD

Le sigle RGPD signifie **Règlement Général sur la Protection des Données** (en anglais « General Data Protection Regulation » ou GDPR).
Le nouveau règlement européen sur la protection des données personnelles est entré en application le 25 mai 2018 . Son objectif principal est de mieux protéger les données personnelles des résidents de l'Union Européenne.

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.

LES PRINCIPES GENERAUX

- **Transparence** : une information explicite et complète des personnes sur la destination des données collectées
- **Limitation** : les données collectées doivent être exclusivement réservées à la finalité définie au départ
- **Minimisation** : les données doivent être limitées à ce qui est nécessaire au regard des finalités du traitement
- **Exactitude des données** : les demandes de rectification doivent être prises en compte, sans délai
- **Sécurité** : garantir une sécurité des données appropriée
- **Licéité** : le ou les traitements doivent être licites en répondant à l'une des conditions prévues par le règlement
- **Principe de Privacy by design** : tenir compte de la protection des données dans les projets qui les touchent, depuis leur origine
- **Privacy by default** : collecter uniquement les données dont on a besoin sans plus *(si on ne va jamais utiliser une information, on ne la demande pas)*
- **Principe d'accountability** : être en mesure de démontrer que vous respectez le règlement à tout moment (dossier de conformité)

LES PRINCIPES GENERAUX

- **Définir une D.L.C. de la donnée** : limiter la conservation des données dans le temps

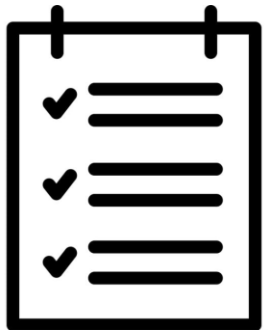
Par exemple :
- pour une transaction en ligne, les coordonnées de la CB du client ne peuvent être conservées que le temps de l'opération de paiement
- un prospect qui ne répond à aucune sollicitation pendant 3 ans doit être supprimé,

On s'accorde à distinguer :
- La base active de gestion courante : données qui sont utilisées au quotidien dans votre activité
- La base intermédiaire avec les informations utiles à un contentieux (factures, devis…)
- La base « archives définitives » qui doit être stockée en dehors de la base courante

et utilisée à titre statistique ou historique

LES ACTIONS A METTRE EN PLACE

- Constituez un registre de vos traitements de données
- Faites le tri dans vos données
- Respectez les droits des personnes
- Sécurisez vos données



LES SANCTIONS

Pour exemple les sanctions peuvent être:

10 millions d'euros ou 2% du CA mondial de la société concernée,
notamment pour des manquements au privacy-by-design *(protéger les données personnelles dès la conception de l'outil)*, au privacy-by-default *(garantir, par défaut, le plus haut niveau possible de protection des données personnelles)* ou encore en matière d'analyse d'impact *(bonnes pratiques destinées à gérer les risques liés au traitement de données personnelles).*

20 millions d'euros ou 4% du CA mondial de la société concernée,
notamment pour des manquements aux droits des *personnes (droits d'accès, de rectification, d'opposition, de suppression, droit à l'oubli, etc)* ou au non-respect des injonctions et mises en demeure.

LES BONS CONSEILS

Etre doté d'un outil de GRC est un avantage indéniable :

- L'hébergement des données en mode SaaS (logiciel à distance) garanti une sauvegarde sécurisée et régulière
- Réagir rapidement aux demandes de données
- Recueillir le consentement préalable du client
- Privilégier la qualité à la quantité
- Purger la base, mettre en place une stratégie de re-contact
- Un logiciel de GRC favorise la segmentation mais revoir régulièrement ses ciblages
- Sensibiliser vos salariés
- Identifier les pratiques à bannir (combien de fichiers « trainent » sur les postes des uns et des autres ?)
- Tracer les opérations de vos sous-traitants qui pourraient avoir accès aux données et couper immédiatement les accès en fin de contrat

LES OPPORTUNITES

Du prêt à porter au sur mesure :

- Pousser la bonne offre à la bonne personne au bon moment : tendre vers l'information sur mesure
- Enrichir une relation personnalisée
- Purger et qualifier (hautement) ses données pour atteindre une meilleure performance
- Réinventer le parcours client en collectant des données en toute confiance

LE VRAI / FAUX

Bien que les données personnelles de mes clients et prospects soient réparties dans plusieurs bases de données, j'ai l'obligation de toutes les répertorier. ☑

Inventorier toutes les données au sein d'une entreprise peut s'avérer difficile, mais vous ne pouvez pas vous y soustraire. Les données personnelles, faisant l'objet de traitements ou étant stockées, présentent un risque de violation et entrent dans le giron du RGPD. Il faut, non seulement, les répertorier mais aussi supprimer celles non utilisées.

Il existe des outils certifiés RGPD dont l'achat permet au responsable de traitement d'être automatiquement et à 100% conforme. ☒

Si la conformité ne tenait qu'à l'acquisition d'une solution, cela se saurait. La conformité au RGPD s'obtient par un effort soutenu combinant des mesures humaines (pour faire évoluer les mentalités et les réflexes), organisationnelles (pour mettre en place les bons processus) et techniques (pour être équipé des bons outils). Côté technique, certains logiciels proposent des fonctionnalités qui assurent la protection de vos données personnelles. Et, si vous choisissez bien, ils peuvent aussi vous aider à fournir les éléments nécessaires pour prouver votre conformité au RGPD.

Je peux recueillir un consentement général de mes contacts en envoyant un email à toute ma base de données ☒

Vos clients et prospects doivent vous donner leur consentement pour un contexte spécifique. Il est impossible d'en obtenir un qui serait commun à diverses utilisations.
Il est donc de votre ressort de leur expliquer comment et pourquoi leurs données personnelles seront utilisées. Pensez aussi à sauvegarder les consentements afin de produire les justificatifs nécessaires en cas d'audit.

Je fais appel à des sous-traitants pour le stockage et/ou le traitement des données personnelles de mes clients. Ils sont désormais, eux aussi, responsables de la protection et de la confidentialité de ces données ☑

C'est l'un des changements majeurs du RGPD. Les sous-traitants doivent, eux aussi, se conformer à de nombreuses obligations. Cette responsabilité concerne vos sous-traitants, où qu'ils soient basés (y compris hors UE) car c'est bien la nationalité de la personne concernée qui prime.

A VOTRE SERVICE

BIBLIOGRAPHIE et SOURCES

- CNIL
- Mission RGPD : la plateforme qui s'occupe de votre conformité RGPD
- E-Deal : Relation client - les clés d'une application de la RGPD réussie

Pour aller plus loin : CNIL RGPD

DRÔME
C'EST MA NATURE

Agence d'Attractivité de la Drôme
8, Rue Baudin – CS 40531 – 26004 Valence Cedex
+33 (0) 4 75 82 19 26 – info@drome-attractivite.com