Les 3 grands principes du RGPD

(Mise à jour : mars 2021)

Au total 99 articles composent le RGPD (Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), auxquels s'ajoutent les 173 paragraphes du considérant qui font partie intégrante du texte.
Autant dire que les exigences issues de ce texte sont massives.
Néanmoins, avec la pratique, je considère 3 grands principes directeurs qui lorsqu'ils sont respectés, permettent d'inscrire votre activité dans le processus de conformité de façon considérable : l'information des personnes concernées - la sécurité du traitement - la suppression des données.

1. L'information des personnes concernées

L'obligation d'information est définie aux articles 12, 13 et 14 du RGPD.
L'idée principale est suivante : « La personne concernée par un traitement de données doit recevoir une information délivrée de façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples. »
En d'autres termes, en tant que responsable du traitement, vous êtes redevable de l'obligation d'information envers les personnes dont vous recueillez les données.

- *Pour des raisons de simplification, le responsable de traitement peut-être considérée comme la personne morale ou son représentant qui recueille les données.*

• A quels moments l'information doit être délivrée ?

Idéalement lors de la première entrée en relation ou en cas de modification substantielle d'un évènement particulier. A défaut, le plus rapidement possible.
Concrètement : L'information devra être fournie lors du premier échange mail ou sur support écrit avec le client (ou prospect).

• Quelles sont les informations à fournir aux personnes concernées?

Il s'agit de :

- Votre identité et vos coordonnées en qualité de responsable de traitement (collecteur des données personnelles). Exemple : Nom commercial, adresse postale, e-mail de contact,…
- La finalité poursuivie par le traitement : En d'autres termes, à quoi vont servir les données collectées. Exemple : Précisez que l'adresse e-mail sera collectée à des fins de prospection commerciale. Notez que cela permet à la personne concernée d'apprécier le caractère proportionné ou non de la donnée collectée en fonction de la finalité poursuivie. En effet, la

collecte d'empreintes digitales à des fins de prospection commerciale paraitra totalement disproportionnée au but poursuivi.

- Les droits des personnes : Il faudra mentionner les droits que confèrent le RGPD aux personnes concernées : Les droits d'accès, de rectification, d'effacement et à la limitation).
- La base légale : Ce qui vous donne le droit de collecter les données personnelles. Il peut s'agir d'une obligation légale, ou du consentement de la personne concernée. Exemple : La loi oblige certaines personnes morales (banque, compagnie d'assurance…) à obtenir et conserver les données permettant l'identification de leur clients.
- Les destinataires des données : Il s'agit des personnes qui auront accès au données personnelles collectées par votre entité. Exemple : Il conviendra de préciser si vous transmettrez les données à vos partenaires ou sous-traitants.
- La durée de conservation : Une mention doit être faite sur la durée pendant laquelle vous conserverez les données. Cette durée varie en fonction de la finalité poursuivie par votre traitement.
- Les coordonnées du délégué à la protection des données : Il conviendra de mentionner les coordonnées de la personne responsable du dispositif RGPD au sein de votre entité telle que son adresse e-mail.
- Le droit d'introduire une réclamation auprès de la CNIL.

2. La sécurité du traitement

Pour information, sur les 12 sanctions prononcées par la CNIL en 2020, le grief de défaut de sécurisation des traitements est apparu à 7 reprises.
Le principe de la sécurité des traitements est prévu à l'article 32 du RGPD.
Rappelons tout d'abord la définition fournie par la CNIL de la notion de traitement : « 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 ou diffusion ou toute autre forme de mise à disposition, rapprochement). »
Notez qu'un traitement de données personnelles n'est pas nécessairement informatisé : les fichiers papier sont également concernés et doivent être protégés dans les mêmes conditions.

Exemples de traitements : tenue du registre des sous-traitants, gestion des paies, gestion des ressources humaines, etc.

Dès lors, en appliquant le principe de sécurité, l'idée à retenir est la suivante : En votre qualité de responsable de traitement, vous devriez prendre des mesures techniques et organisationnelles pour garantir la sécurité de vos traitements. Très concrètement, cela revient à mettre en place des mesures de sécurité au niveau du matériel informatique, et à restreindre la liste des personnes qui auront accès aux données personnelles au sein de votre organisation. Les mesures prises devront être adaptées en fonction du type de données collectées. A titre d'exemple, les mesures de sécurité devront être renforcées en cas de collecte des données de santé (on parle de données sensibles) qu'en cas des données d'identification (exemple : nom ou prénom).
la CNIL a fourni un excellent guide qui vous rappelle les précautions élémentaires qui devraient être mises en œuvre de façon systématique.

Ci-après, la liste non exhaustive des éléments devant faire l'objet de sécurisation dans le cadre de votre activité.

- Matériel informatique : ordinateurs portables, disques durs, serveurs, logiciels, canaux de communication (wifi, fibre optique,…), documents imprimés, photocopie,…
- Les mesures garantissant la sécurité d'accès des données au sein de votre organisation : bien gérer les utilisateurs des données en mettant en place des identifiants uniques et propres à chaque individu, imposer une authentification, prévoir si possible une politique de gestion d'accès aux données, mettre en place un système de journalisation afin de tracer les activités. Ces mesures sont multiples et varient en fonction de la taille de votre activité.

Notez qu'en cas de contrôle, la CNIL évaluera toutes anomalies ou évènements liés à la sécurité, comme les accès frauduleux et les utilisations abusives de données personnelles.

3. La suppression des données :

Evoquons au préalable le principe sous-jacent à celui de la suppression des données, à savoir la fixation de la durée de conservation des données.
En clair, « les données personnelles ne peuvent être conservées indéfiniment ».
Dans certains cas, la durée de conservation est fixée par la règlementation (par exemple, l'article L3243-4 du Code du travail impose à l'employeur de conserver un double du bulletin de paie du salarié pendant 5 ans). Toutefois, pour de nombreux traitements de données, la durée de conservation n'est pas fixée par un texte. Il vous appartient de la déterminer en fonction de la finalité du traitement.

La CNIL a fourni un référentiel des durées de conservation, qui est un vrai outil d'aide à la prise de décision qui vous orientera vers les durées obligatoires ou recommandées pour vos traitements.

Une fois la durée de conservation écoulée, c'est là qu'interviendra la suppression des données.

Le principe de suppression des données est prévu à l'article 17 du RGPD, on parle de Droit à l'effacement («droit à l'oubli») : « l*a personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais, lorsque l'un des motifs suivants s'applique… »*

En pratique, la suppression des données consiste à détruire purement et simplement les données personnelles en votre possession, informatiquement, ou manuellement. Une autre pratique consiste à anonymiser les données concernées afin que leurs auteurs ne soient plus identifiables.

En résumé, voici les étapes à suivre :

I. Informer préalablement les personnes concernées (de façon claire et précise sur tous types de supports) que leurs données seront collectées en indiquant la finalité et on leur rappelant leurs droits

II. Assurer la sécurité de votre(vos) traitement(s) par tous moyens, et donc par conséquent, la sécurité des données collectées.

III. Procéder à la suppression (ou anonymisation) des données une fois la durée de conservation écoulée.

Pour tout un complément d'informations en fonction de votre domaine d'activité, merci de contacter la société Majelink par mail à l'adresse suivante : majelink01@gmail.com