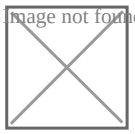

Mise en conformité avec le RGPD : L'urgence de recourir à un professionnel

Commentaire article publié le **25/05/2021**, vu **790 fois**, Auteur : Droit à la justice

Avec la mise en vigueur du Règlement Général sur la Protection des Données (RGPD) le 25 Mai 2018, plus rien ne sera plus comme avant. Décryptage.

Avec la mise en vigueur du Règlement Général sur la Protection des Données (RGPD) le 25 Mai 2018, plus rien ne sera plus comme avant. Le but est d'encadrer le traitement et la circulation des données à caractère personnel sur l'ensemble du territoire européen. Certains pensent à tort que ce règlement ne concerne que l'Europe. Il est en effet temps de mettre vos traitements informatiques en conformité avec le RGPD. Dans le cas contraire, vous vous exposez à de lourdes sanctions.

À qui d'adresse le RGPD ?

Toute entité qui manipule les données personnelles des Européens, qu'il s'agisse d'une entreprise, d'un sous-traitant ou d'une association, est tenue de se conformer à ce règlement. L'application de cette loi ne se limite pas uniquement à l'espace européen. Peu importe la nationalité de l'entreprise ou de l'organisme concerné. Dès lors qu'elle collectionne et gère les données personnelles des personnes pouvant revendiquer la nationalité de l'un des pays d'Europe, le RGPD lui est applicable.

Mieux, n'est pris en compte aucun critère lié à la taille, au secteur d'activité ou au caractère public ou privé. Autant que vous le sachiez, toutes les entreprises sont concernées.

Cependant, la mise en conformité RGPD nécessite de recourir aux services d'un professionnel. L'idéal est de faire appel à un spécialiste du droit. Il faudra toutefois redoubler de vigilance.

Comme l'a révélé la Commission Nationale de l'Informatique et des libertés (CNIL), il existe en la matière des expertises frauduleuses, des prestations « clé en main » et même des démarchages par téléphone dont il faut se méfier. En témoigne la campagne « StopArnaque » lancée par la CNIL.

RGPD : Quelles obligations pour les entreprises ?

Il importe de savoir qu'une donnée personnelle ou donnée à caractère personnel n'est rien d'autre qu'une information relative à une personne physique. Peu importe que cette personne soit identifiée directement ou indirectement. La gestion de ces données porte donc sur plusieurs éléments dont :

- Le nom
- La photographie

- L’adresse IP
- Le numéro de téléphone
- L’identifiant de connexion informatique
- L’adresse postale
- L’empreinte
- Le mail
- Le numéro de sécurité sociale etc.

En ce qui concerne ces données, elles doivent être exactes et tenues régulièrement à jour. La loyauté, la licéité et la transparence sont les critères principaux qui doivent prévaloir dans la manipulation de ces données. On note également que ces données sont conservées dans des délais raisonnables. En effet la conservation doit être proportionnelle à la finalité du traitement. À ce sujet, on distingue trois types d’archivage :

- L’archivage courant
- L’archivage intermédiaire
- L’archivage définitif

Les étapes de la mise en conformité

La mise en conformité passe par sept (7) étapes essentielles. Comme le révèle cette belle phrase, elle n’est pas un état, mais un processus. Il s’agit donc d’atteindre un état de sécurité suffisant. On distingue :

La cartographie des traitements

L’expert commis à cette cause recense de manière guidée, l’ensemble des données personnelles qui font l’objet de traitement par l’entreprise. C’est la première étape du processus. Elle permet d’avoir un état des lieux en ce qui concerne le traitement de données personnelles opéré par l’entreprise.

La cartographie des données comprend plusieurs éléments. En recourant à un professionnel, vous pouvez réaliser efficacement une cartographie des données comme l’exige la mise en conformité RGPD. Ce professionnel pourra mieux intégrer dans le registre des traitements les éléments obligatoires tels que :

- La finalité du traitement
- Les catégories de données
- Les personnes concernées par les données en question
- Les destinataires des données
- Les différentes mesures de sécurité mises en place

La détermination de la finalité des traitements

La détermination de la finalité des traitements est une imposition légale. Lorsque l’entreprise concernée arrive à déterminer la raison pour laquelle elle collecte des données, elle doit s’en tenir à cette finalité initiale. Mention de cette finalité doit figurer dans le registre des traitements des données.

A supposer par exemple, qu’une entreprise informe des personnes que dans le cadre de leur inscription à un service, elle procèdera à la collecte de leurs données personnelles. Faire usage de ces données à des fins commerciales constitue sans nul doute, une atteinte à la mise en

conformité avec le RGPD.

L’information des clients et des collaborateurs

Il ne suffit pas de déterminer la finalité du traitement des données. Encore faudrait-il qu’elle soit portée à la connaissance des personnes dont les données sont traitées. Cette information porte non seulement sur l’objet du traitement mais également sur les droits qui sont reconnus à ces personnes par le RGPD.

La conservation des données pendant une durée adéquate

Le principe de conservation des données est celui-ci : Aucune donnée ne peut faire l’objet d’une conservation illimitée. Le traitement est strictement limité à la durée nécessaire.

Il existe à cet effet des délais légaux de conservation. A défaut, le responsable de traitement des données se fixe un délai au-delà duquel il doit procéder à leur destruction ou à leur anonymisation.

Le choix de la base légale

Tout traitement de données personnelles doit reposer non seulement sur une finalité, mais également sur une base légale. Il existe en effet de nombreuses bases légales figurant dans le RGPD. Le spécialiste en matière juridique chargé de la mise en conformité RGPD, vous aidera à déterminer la base légale la plus appropriée.

L’enjeu du choix de la base légale réside également dans le fait qu’il existe une mise à jour à ce sujet. Prenez garde alors à ne pas retenir une base légale alors qu’elle n’existe plus.

Le recueil du consentement RGPD

Le consentement fait partie de l’une des bases légales du RGPD. Il s’obtient de différentes manières. Il peut s’agir d’une case à cocher ou d’une signature manuscrite. Quoi qu’il en soit, le consentement doit être libre, spécifique, éclairée et ne pas prêter à confusion.

L’une des principales innovations de la mise en conformité RGPD en matière de consentement est liée au fait que le consentement doit être soumis à un droit de retrait, l’obligation de tenir à jour le registre des consentements et la nécessité de recueillir le double consentement en ce qui concerne les mineurs : Consentement de l’autorité parentale et consentement du mineur concerné.

Comme vous l’auriez compris, il est impératif de se conformer au RGPD. Le non-respect expose l’entreprise ou l’organisme mis en cause, à l’une ou l’autre de ces sanctions : Amendes pouvant atteindre 20 millions d’euros ou encore des amendes dans la limite de 4% du chiffre d’affaires annuel mondial total du précédent exercice. En la matière, c’est l’amende la plus élevée qui est appliquée.