RGPD :

Les notions clés pour se mettre en conformité

À 10 jours de l'entrée en vigueur du Règlement Général sur la Protection des Données, plus connu sous l'acronyme **RGPD**, Codepi vous propose de faire le tour des notions clés afin de se mettre en conformité.

Le RGPD, qu'est-ce que c'est ?

Le Règlement Général sur la Protection des Données est un nouveau règlement européen qui s'inscrit dans la continuité de la loi française « Informatique et Libertés » de 1978. Ce règlement impose aux entreprises de **se responsabiliser face à la gestion des données** et **d'élaborer elles-mêmes leur programme de conformité** en définissant la façon dont elles répondent aux objectifs fixés par le règlement.

Quand dois-je être prêt ?

La date officielle d'entrée en vigueur est **le 25 mai 2018**. Pas de panique pour autant : les autorités accordent **un délai de 2 ans** pour se mettre en conformité. Des contrôles pourront avoir lieu durant cette période, pour lesquels il faudra être capable de prouver que le processus de mise en conformité est engagé.

Données personnelles et traitement des données personnelles : 2 notions clés

Une donnée personnelle est définie comme toute information se rapportant à une personne physique **identifiée ou identifiable**, à partir **d'une seule donnée** ou **le croisement d'un ensemble de données**, à savoir à titre d'exemple :

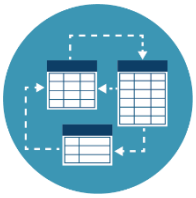
- l'identité (nom, prénom),
- les coordonnées (numéro de téléphone, adresse postale, adresse e-mail),
- les numéros d'identifiant (n° client…),
- les données de localisation,
- les informations relatives à la vie professionnelle,
- les habitudes de consommation,
- l'adresse IP,
- etc…

Au-delà de la collecte des données, le RPDG a pour vocation de **contrôler le traitement** de données à caractère personnel. Le traitement des données est défini comme une **opération** ou un **ensemble d'opérations**, **automatisée ou non, papier ou informatisé**, concernant des données à caractère personnel.

Concrètement, un traitement de données peut prendre la forme suivante : tenue d'un fichier clients, collecte de coordonnées de prospects via un formulaire, mise à jour d'un fichier fournisseurs etc…

Qu'est-ce que ça implique réellement ? Suis-je limité dans mes traitements ?

Bien sûr que non ! Le traitement de données est toujours autorisé, il convient simplement de l'encadrer. Un traitement est légitime dès lors qu'il a **un objectif précis et défini**, en rapport direct avec **l'activité professionnelle**. Cela implique donc de collecter et de conserver **uniquement des données essentielles à l'accomplissement de cet objectif**.



Par où je commence ? Les actions à mener

Le RGPD implique la mise en place de procédures internes conformes au respect des droits des personnes. Pour cela, nous vous conseillons de suivre les différentes étapes détaillées ci-dessous.

1. Cartographier les traitements et établir des registres

Lors d'un contrôle, c'est la tenue de différents registres recensant l'intégralité de vos traitements de données qui prouvera de la mise en conformité. Le modèle soumis par la CNIL (à retrouver ici : https://www.cnil.fr/fr/cartographier-vos-traitements-de-donnees-personnelles) permet de cartographier l'intégralité des traitements.

Pour cela, nous vous conseillons dans un premier temps de recenser **l'intégralité des activités impliquant la collecte de données** et **des fichiers qui en découlent**.

Une fois ce travail effectué, vous serez en mesure de compléter le registre avec les informations considérées comme essentielles, à savoir :

- la description du traitement,
- les acteurs, c'est-à-dire les personnes qui traitent les données,
- la finalité du traitement en question,
- les mesures de sécurité mises en place,
- les catégories de données personnelles concernées,

- la présence de données sensibles ou non,
- le délai de conservation des données.

Un traitement des données personnelles sera considéré conforme dès lors qu'il répond à ces critères.

2. Trier les données

Deux bonnes pratiques à mettre en place dès aujourd'hui : faites le tri et ne gardez pas indéfiniment les données !

La gestion des données est au cœur des problématiques du RGPD. À ce stade, il conviendra de trier les données afin de conserver uniquement celles **nécessaires à l'activité**, dans un délai **raisonnable**.

3. Établir des procédures internes de sensibilisation

Sur le plan organisationnel, le RGPD impose d'engager de nombreuses actions permettant de faire émerger **une véritable culture de la conformité** en matière de données personnelles auprès de tous les salariés.

La mise en place d'une organisation interne via des mesures et des outils va permettre de répondre au **principe d'« accountability »** qui impose aux entreprises d'être en mesure de démontrer, à tout moment, que la protection des données personnelles est **optimale et conforme aux exigences légales**.

Les mesures prisent devront permettre d'assurer le respect de :

- la **« Privacy by design »** qui consiste à prendre les mesures appropriées pour tenir compte de la protection des données dans les projets **dès leur conception** et tout au long de leur cycle de vie.
- la **« Privacy by default »** qui consiste à prendre les mesures techniques et organisationnelles appropriées afin de garantir que, par défaut, **seules les données nécessaires sont collectées et utilisées**.

En pratique, les entreprises devront être en mesure de **prouver et de tracer les actions menées** pouvant notamment prendre la forme de charte d'utilisation, d'un code de conduite, de politique de protection des données à caractère personnel ou encore d'un cahier des charges.

4. Mettre à jour les documents juridiques

Suite à l'entrée en vigueur du RGPD, **tous les documents juridiques** relatifs à la société, notamment les CGU, les CGV, les chartes, les référentiels, les mentions légales d'informations etc. devront être mis à jour afin de faire apparaître les nouvelles normes imposées, tant envers les clients que les sous-traitants.

5. Informer et respecter le droit des personnes

Afin de respecter le principe de **« Transparence »,** informez vos clients du traitement qui sera fait des données collectées. Tous les supports utilisés doivent donc être retravaillés afin de comporter les mentions d'information suivantes :

- la raison pour laquelle ces données sont collectées,
- ce qui vous autorise à traiter ces données,
- les personnes y ayant accès,
- la durée de conservation,
- les modalités selon lesquelles les personnes peuvent exercer leurs droits.

Suite à la collecte, il est indispensable de **permettre aux personnes d'exercer leurs droits**, que ce soit leur droit d'accès, de rectification, d'opposition, d'effacement, à la portabilité ou à la limitation du traitement.

Pour cela, nous vous conseillons de **mettre en place une procédure simple,** via un formulaire de contact, un numéro de téléphone ou une adresse email dédiée, permettant de **garantir un traitement de la demande sous un mois**.

Dans le cas d'une violation de données personnelles, une notification devra être émise à la CNIL dans **un délai maximum de 72 heures** après la prise de connaissance du problème. Ce devoir de réactivité implique la mise en place d'une procédure bien définie en amont.

Qu'est-ce que je risque ?

Suite à une enquête ou à une réclamation, l'autorité de contrôle peut décider de sanctionner par des **mesures correctives**, allant de l'avertissement à la suspension des flux.

En plus de ces mesures, des **amendes** pourront être appliquées, le montant étant fixé en fonction des violations commises. Loin d'être anodines, les amendes peuvent s'élever jusqu'à **10 ou 20 millions d'euros** ou jusqu'à **2% ou 4% du chiffres d'affaires annuel**, à savoir que le montant le plus élevé sera celui retenu.

Des avantages malgré les restrictions ?

Bien que contraignant lors de son application initiale, le RGPD représente des leviers d'avantages concurrentiels. En mettant en place une politique de confidentialité et de protection des données personnelles, vous acquerrez d'autant plus **la confiance de vos clients**.

De plus, limiter la collecte et le traitement de données à un but précis et établi permet à la fois d'**améliorer l'efficacité commerciale** et de **faciliter la gestion de l'activité**.

Enfin, et puisque ce règlement s'applique à toutes les entreprises, les relations entreprises-fournisseurs n'en seront que pérennisées.

Le RGPD requiert donc essentiellement un état des lieux et une bonne organisation interne. Ce nouveau texte de loi étant encore soumis à discussion, certaines évolutions sont à prévoir au fur et à mesure de son application. De bonnes pratiques vont être développées dans les mois à venir, permettant à chaque entreprise de se mettre en conformité en bonne et due forme.

codepi
LE BLOG