Qu’est ce que le RGPD ?

RGPD, ou **R**ègle**m**ent **G**énéral sur la **P**rotection des **D**onnées, est le nouveau texte de référence Européen en matière de protection des données à caractère personnel. Il renforce et unifie la protection des données pour les individus au sein de l'Union Européenne.
Ce règlement remplacera l’actuelle Directive sur la protection des données personnelles et apporte de nombreux changements clés que vous devez connaître. Il étend le champ d’application de la loi sur la protection des données à l’ensemble des entreprises, y compris aux sociétés non-Européennes si ces dernières ciblent des résidents de l'UE.

Le RGPD pour les entreprises

Le RGPD s’applique aux deux types d’échanges sans distinction : **l’adresse email professionnelle d’un individu est désormais considérée comme une donnée personnelle.** Dans les deux cas, vous n'aurez le droit de contacter vos prospects seulement pour la/les raisons que vous aurez mentionné explicitement.

Quand le RGPD sera appliqué ?

Officiellement **dès le 25 mai 2018**, jour à partir duquel les entreprises et autres entités ne respectant pas ces dispositions pourront être exposés à une amende.

A qui le RGPD s’applique-t-il ?

A toutes les sociétés ou entités, quelque soit leur pays d’origine**, collectant ou traitant les données de citoyens Européens**. Cela concerne donc également les tierces parties comme les sociétés d’hébergement de données en ligne (*cloud providers*).

Où le RGPD s'applique-t-il ?

Dans les **28 pays membres de l'Union Européenne** bien sûr, mais il s'étend **aussi à toute entité non-Européenne** dès lors qu'elles collectent et/ou traitent les données de résidents de l'UE.

Le Brexit a-t-il un impact sur cette réglementation pour les citoyens britanniques ?

Oui. Le RGPD étant applicable à toutes entités échangeant des données personnelles de citoyens européens, les citoyens britanniques devront tout de même se soumettre au RGPD si ils veulent continuer à travailler avec des données européennes. De plus, le RGPD est entré en vigueur avant que le Royaume-Uni ne quitte officiellement l'Union Européenne (le 29 mars 2019). Pour continuer leurs échanges avec l'Union Européenne, il leur faudra mettre en place un règlement équivalent de garanties en matière de protection des données.

Quelles sanctions en cas de non-respect des dispositions du RGPD ?

Le RGPD prévoit des amendes de plusieurs paliers : en cas de mauvaise tenue des enregistrements (Article 28), défaut de notification de l'autorité de surveillance et de la personne concernée à propos d'une violation (Articles 31 et 32) ou absence d'évaluations d'impact (Article 33), l'amende peut monter jusqu'à 2% du chiffre d'affaire. L'amende maximale pour les entreprises qui ne respectent pas le RGPD peut monter jusqu'à 4% du chiffre d'affaires ou jusqu'à 20 millions d'euros (la somme la plus importante).

Quels changements majeurs apporte le RGPD ?

- Une définition élargie des données personnelles
- Des droits individuels renforcés en matière de consentement
- Une responsabilisation accrue des entreprises
- Une application extraterritoriale
- L'obligation de mettre en place de mesures préventives de protection des données
- L'obligation d'informer les personnes concernées de toute fuite des données
- La nomination obligatoire d'un Délégué à la Protection des Données
- Des mesures techniques et organisationnelles plus strictes

Une définition élargie des données personnelles

Tout ce qui peut permettre **d'identifier un individu sera compté comme donnée personnelle**, que cela **ait trait à sa vie privée, publique ou professionnelle**. Cela peut être un **nom, l'adresse du domicile, une adresse email, une photo, des données bancaires, biométriques, génétiques, une information médicale, des publications sur les réseaux sociaux, l'adresse IP d'un ordinateur.**

Des droits individuels renforcés en matière de consentement

Cela peut aller **du droit d'accès au droit à l'effacement** en passant par le droit à la portabilité. Les entreprises collectant ou traitant des données **ont l'obligation de clairement communiquer les informations suivantes aux individus dont ils collectent les données :**

- Combien de temps les données seront stockées;
- Si ces données seront transférées à d'autres pays ou non;
- Leur droit de demander l'accès à leurs données;
- Leur droit d'obtenir que leurs données soient modifiées ou effacées dans certaines circonstances;
- Le renforcement des conditions de contrôle. Les entreprises ne pourront plus avoir recours à des Termes & Conditions interminables et truffés de jargon juridique, dans la mesure où la demande de consentement devra être communiquée de manière intelligible et facile d'accès, expliquant clairement à quoi serviront les données demandées. Et il devra être aussi facile à l'utilisateur de donner son consentement que de le reprendre.

Quelles questions dois-je poser à mes prestataires en ce qui concerne le RGPD ?

1. Où sont stockées vos données et applications ?
2. Ces données ont-elles déjà été déplacées en dehors de l'Espace Economique Européen ?
3. Vos données ont-elles déjà été transférées vers un centre de données situé en dehors de l'Union Européenne ?
4. M'informez-vous systématiquement de tout transfert de données ?
5. Avez-vous un Délégué à la Protection des Données ?
6. Quelles procédures de management des risques et de contrôle des données avez-vous déjà mis en place ?
7. Est-ce-que votre gestion des révisions assure un niveau de sécurité suffisant des données ?
8. Qui peut avoir accès à mes données, sous quelles circonstances, et que peuvent-ils voir? Cet accès est-il pisté?
9. Puis-je contrôler vos mesures techniques et de sécurité sur la protection des données ?
10. Avez-vous déjà adhéré aux Binding Corporate Rules ?
11. Vos mesures de protection seront-telles compilantes à temps quand le RGPD prendra effet