QUOI ? POURQUOI ? QUI ? QUAND ?

Le RGPD (ou GDPR en anglais) : règlement général sur la protection des données est le texte de référence européen traitant de la protection des données personnelles des résidents de l'union européenne. Applicable depuis le 25 Mai 2018, le RGPD est venu harmoniser la gestion des données dans la totalité des pays de l'union européenne.

QUI EST CONCERNE ?

Ce règlement concerne tous les acteurs proposant des biens ou des services sur le marché de l'union européenne à partir du moment où leur activité traite les données personnelles des résidents européens. Sont donc concernés, les entreprises, les associations, les organismes publics européens mais aussi les entreprises dont le siège est hors union européenne mais qui opèrent dans l'UE sur des données de ses citoyens.

OBJECTIFS ET ENJEUX

L'objectif majeur du RGPD est de permettre aux citoyens européens d'avoir plus de contrôle et de visibilité sur leurs données privées.

Le principal enjeu pour les entreprises sera donc de savoir où sont les données à un instant précis et comment pouvoir les collecter, les gérer puis parvenir à les transmettre à la personne concernée

SANCTIONS

Il y a des sanctions prévues pour les entreprises non-conformes au RGPD qui peuvent aller jusqu'à 4% du chiffre d'affaire annuel mondial ou 20 millions d'euros. C'est la somme la plus importante entre les deux qui sera versée.

PRINCIPES

5 principes à mettre en œuvre pour assurer une meilleure protection des données personnelles.

- Accountability

C'est à l'entreprise que lui revient la responsabilité de prendre toutes les mesures pour garantir la conformité au RGPD. Cela suggère aussi que l'entreprise doit être capable de prouver qu'elle a respecté ses obligations en termes de protection des données. Chose qui lui sera demandé lors d'un contrôle de La Commission nationale de l'informatique et des libertés (CNIL) par exemple.

- Privacy by design

Le privacy by design signifie que lors de la conception du produit ou du service, l'entreprise doit prendre en considération la protection des données personnelles, le système d'information, la base de données, ...

- Security by default

Le principe de Security by default renforce la sécurité dans le système d'information. Ce dernier doit être sécurisé à différents niveaux pour garantir au mieux la protection et la confidentialité des données. Une fois la conception des produits ou services faite, les standards de protection des données personnelles doivent s'activer par défaut.

- DPO

Le rôle de data protection officer (DPO) est assimilé à un délégué à la protection des données : le DPO doit veiller sur la conformité au RGPD et d'être l'intermédiaire entre son entreprise et les autorités de contrôle (CNIL).

Pour contacter le DPO de Notoriety Group, envoyer votre message à l'adresse : dpo@notoriety-group.com

- Etude d'impact

Le RGPD demande aux entreprises de mener une étude d'impact sur la protection des données personnelles avant de mettre en œuvre de nouveaux traitements de données qui pourraient présenter des risques d'atteintes aux droits et aux libertés individuelles.

L'étude d'impact devra prévoir les mesures nécessaires pour diminuer l'impact des dommages à la protection des données personnelles.