GDPR

A pour objectif premier de protéger les libertés et droits fondamentaux des personnes physiques.

Ce que signifie G D P R : General Data Protection Regulation, en français RGPD

La GDPR est aux données ce qu'est la FINMA aux banques.

La conformité réglementaire n'est pas une option : c'est une **OBLIGATION**.

Les entreprises ou collectivités doivent être en conformité au plus tard le 24 mai 2018.

Sanctions

L'amende à laquelle s'expose les entreprises non-conformes peut aller jusqu'à 4% du chiffre d'affaires ou 20 millions d'euros.
Information de par le législateur en utilisant les organes de presse ou autre à disposition d'une non conformité.

Qui applique les sanctions ?

En Suisse, les sanctions, prononcées par un juge pénal
peuvent atteindre 500 ´000 francs.

Pour les sociétés, l'UE prévoit une amende qui peut atteindre 4% du chiffre d'affaires mondial.

Pourquoi sommes-nous concernés ?

La nouvelle réglementation Européenne pour la protection des données est entrée en vigueur il y a plus d'un an et les entreprises concernées doivent se mettre en conformité avant fin Mai 2018. S'agissant d'une réglementation européenne, la Suisse pourrait ne pas se sentir concernée... Et bien ce serait une "grave" erreur !

A moins d'être une entreprise Suisse n'offrant des services qu'aux helvètes et ne traitant aucune donnée à caractère personnel d'individus membres de l'Union Européenne, vous êtes concernés.

Et cela risque in fine d'être la grande majorité des entreprises (PME ou grands groupes) de la Confédération.

De plus, la Suisse fait partie de cet espace économique et l'harmonisation des règles sera certainement une priorité pour la confédération lors de la révision de la LPD (Loi sur la Protection des Données), et pour les cantons dans le cadre de leur législation locale. Donc autant se préparer.

Qui est concerné ?

Toute organisation privée ou publique traitant les données personnelles de citoyens européens, qu'elle soit établie ou non dans l'UE.

Une entreprise suisse qui traite ou collecte les données de citoyens, de clients, d'employés ou de fournisseurs européens devra s'y conformer.

Le GDPR couvre «toute information se rapportant à une personne physique identifiée ou identifiable» telles que l'origine ethnique ou raciale, orientations religieuses, opinions politiques ou données génétiques.

9 décideur sur 10 pense que cette réforme ne s'applique pas à son entreprise.

Les avantages

- La mise en conformité avec le Règlement permet à une entreprise de renforcer la confiance avec les clients, partenaires et collaborateurs tout en préservant sa réputation et son image de marque.

- Valorisation des données gérées.

L'essentiel à retenir

Légal : Information et consentement des personnes

Nouveaux droits : Droit d'accès et de modification, droit à l'oubli, droit à la portabilité

Méthodologie : Privacy by design, privacy by default

Sécurité : Cryptage, anonymisation, perte des données

Organisation : Registre des traitements, gouvernance des informations

5 changements majeurs dues à la GDPR

1. Désignation d'un délégué à la protection des données (Digital Protection Officer ou DPO) au sein de la société ou aglomération, chargé d'orchestrer la conformité de l'entreprise en la matière.

La fonction est destinée à jouer un rôle prépondérant et à travailler étroitement avec les responsables de la sécurité, mais aussi du marketing, de la conformité ou du département légal.

2. Obligation de notifier dans les 72 heures les autorités et les clients affectés lors d'une fuite de données.

3. Capacité à identifier une violation et à fournir des informations détaillées.

4. Exigence auprès des entreprises qu'elles intègrent la protection des données dès la conception de leurs services et produits.

5. Extension des responsabilités de l'entreprise à ses partenaires et autres sous-traitants intervenant dans le traitement des données. Les entreprises vont devoir démontrer ce qu'elles font pour réduire les risques et sécuriser les données. Elles devront ainsi documenter le traitement des données, l'impact de ce traitement, la sécurité IT de leurs systèmes ou encore les mesures prises en matière de contrôle des accès, de chiffrement ou de pseudonymisation.

Les obstacles à la mise en conformité

- Le premier facteur est le faible niveau de sécurisation des données
- Le manque d'outils de sécurité performants
- Les restrictions techniques liées au service informatique
- Obsolescence des informations juridico-technique
- Manque de ressources financières
- Faible niveau de sécurisation des données
- Manque d'outils de sécurité performants
- Restrictions liées au SI
- Manque de ressources financières

Il est urgent de faire face aux multiples failles, et pour cela, que peut-on préconiser ?

Mise en place d'un processus au sein de l'entreprise afin que les autorités en charge de la protection des données soient informées dans les 72h suivant une faille.

- Pour se prémunir contre les failles
- Sensibilisation des collaborateurs
- Verrouillage des appareils pour éviter la contamination par clés USB infectées
- Intégration de technologies de déchiffrement
- Chiffrement des mots de passe
- Mise en place d'une solution de prévention des failles de données

Merci d'avoir pris connaissance de ce document et nous restons à disposition pour une accompagnement dans vos démarches de mises en conformité.