Règlement général sur la protection des données

Qu'est-ce que c'est ?

- **GDPR** est l'acronyme pour General Data Protection Regulation

Pourquoi la GDPR a-t-elle été mise en place ?

- **Objectifs** :
    - Donner davantage de contrôle aux citoyens européens sur leurs données privées
    - Simplifier les régulations pour les organisations

Qui est concerné ?

- **Cadre d'application** : standard européen applicable à l'intérieur des 28 pays membres de l'UE ainsi qu'aux entreprises hors UE manipulant des données issues d'activités d'organisations européennes ou de résidents européens. Toute organisation manipulant des données personnelles est affectée par la GDPR.
- **Définition** d'une **donnée personnelle** : est considérée comme donnée personnelle toute information concernant un individu, publique ou privée.
- **Amende** : le non-respect d'un article du règlement peut entraîner une amende allant jusqu'à 4% du chiffre d'affaires mondial annuel ou d'un montant maximal de 20 millions d'euros.

Quand la GDPR entrera-t-elle en application ?

- **Date** d'application : 25 mai 2018

Comment se mettre en conformité ?

Concernant les individus sujets à un traitement de données, une organisation est tenue de respecter cinq points :

- **Droit à l'effacement** : un individu a le droit d'obtenir d'une organisation l'effacement de données personnelles le concernant dont elle est responsable.
- **Droit à la portabilité** : un individu a le droit d'obtenir d'une organisation des données personnelles le concernant dont elle est responsable, dans un format clair et lisible. Un individu a le droit de transmettre et/ou de demander la transmission de ces mêmes données à un organisme tiers.
- **Consentement** : un traitement de données personnelles doit être consenti par l'individu qui en constitue l'objet.
- **Répercussions** d'un traitement automatisé sur un individu : aucun traitement de données automatisé (exemple : profiling d'un individu pour analyser ses

performances de travail) ne peut constituer une base de décision pouvant affecter (exemple : licenciement) un individu.
- **Accessibilité** : les informations relatives au traitement des données doivent être transparentes et accessibles (en libre accès ou facilement sur demande).

Concernant l'organisation qui traite les données :

1) Avant traitement

- **Acquisition** et **stockage**: le traitement des données doit être transparent (quelles informations sont collectées et à quelles fins) et justifié (nécessaire à l'activité donnant lieu au traitement). La durée de rétention des données doit être limitée au strict nécessaire.
- **Protection** des données **par design** : toute organisation doit assurer un standard de protection des données dès la phase de conception de tout produit, service ou système impliquant un traitement de données à caractère personnel. Trois possibilités :
    - chiffrage
    - pseudonymisation : remplacer des informations sensibles (informations personnelles identifiables : nom, adresse, donnée génétique, etc.) par des informations moins explicites (exemple : clé d'identification)
    - anonymisation : impossibilité de relier un individu à une donnée
- **Protection** des données **par défaut** : toute organisation doit disposer d'un système d'information sécurisé qui assure la confidentialité de ses utilisateurs (gestion des droits, accès...).
- **Étude d'impact** : une étude d'impact sur la vie privée doit être effectuée avant la mise en place de toute activité qui puisse avoir un impact négatif sur la protection des données, incluant la prévision de mesures préventives minimisant les risques identifiés.

2) Pendant et après traitement

- **Fuite de données** : toute fuite de données doit être signalée dès que possible à l'autorité nationale de protection adéquate.
- Un **délégué à la protection des données** doit être nominé dans toute organisation dont les activités incluent des traitements de données qui exigent un suivi régulier et systématique. Le délégué doit être impliqué dans toute activité relative à la protection des données. Son rôle est de contrôler le respect du règlement, de conseiller le responsable des traitements et de faire le lien avec l'autorité de contrôle et les citoyens qui souhaitent exercer leurs droits.
- **Pour une organisation internationale** : une organisation internationale doit uniquement rendre compte de ses activités à l'autorité nationale de protection des données du pays d'origine de son siège social.

Ressources complémentaires

Pour vous aider à la mise en conformité de votre entreprise, la **CNIL** propose un guide pas-à-pas intuitif sur son site web :
https://www.cnil.fr/fr/principes-cles/reglement-europeen-se-preparer-en-6-etapes

La **régulation complète** adoptée au Parlement européen :
http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf?lipi=urn%3Ali%3Apage%3Ad_flagship3_pulse_read%3Bj0jH6L1wTCeQUzIayrnaJw%3D%3D

Sources

Règlement général sur la protection des données - Wikipédia :
https://fr.wikipedia.org/wiki/R%C3%A8glement_g%C3%A9n%C3%A9ral_sur_la_protection_des_donn%C3%A9es

The general data protection regulation - Conseil de l'Union Européenne :
http://www.consilium.europa.eu/fr/policies/data-protection-reform/data-protection-regulation/

An idiot's guide to GDPR - Sinitta Stuart :
https://www.linkedin.com/pulse/idiots-guide-gdpr-sinitta-stuart

GDPR : que dit le nouveau règlement européen sur les données européennes - Les Échos :
https://www.lesechos.fr/idees-debats/cercle/cercle-147684-la-gdpr-au-dela-des-obligations-une-opportunite-pour-les-entreprises-1196000.php

Salesforce GDPR compliance information - Salesforce :
https://www.salesforce.com/campaign/gdpr/