Mis à jour le 09/01/2025

Introduction au RGPD

Qu’est-ce que le RGPD ?

Le **Règlement général sur la protection des données** encadre le traitement des **données à caractère personnel** (DCP) (dématérialisées ou non) sur le territoire de **l’Union européenne**. Il s'adresse à **toutes les organisations**, qu'elles soient **publiques ou privées**.

Les fuites de données ou le stockage non pertinent de données à caractère personnel peuvent avoir des **impacts importants** (pertes financières, usurpations d’identité, atteinte à la réputation, fuite de données, etc.). Le RGPD a pour enjeu d’accompagner les structures dans le traitement et la protection de ces données.

Le règlement prévoit également des sanctions en cas de non-conformité, pouvant aller jusqu’à une **amende administrative** de 20 millions d’euros ou 4% du chiffre d’affaires annuel mondial de l’entreprise.

Ressources utiles

- ANS – Fiche de présentation RGPD [PDF]
- ANSSI – Renforcer la sécurité des données personnelles [Site web]
- CNIL – Guide pratique RGPD [PDF]
- CNIL - Référentiels des durées de conservation dans le secteur de la santé [Site web]
- CNIL – Informer les personnes concernées lors de traitements de données de santé [Site web]
- CNIL – Recherche médicale et cadre légal [Site web]
- CNIL – Violations de données personnelles : Bilan de 5 années de RGPD [Site web]
- CNIL – AIPD : un outil pour construire un traitement respectueux de la vie privée [Webinaire]

Bonnes pratiques afin d’être conforme au RGPD :

- **Définir précisément les finalités de traitement**: Les données doivent être collectées et traitées uniquement pour des objectifs spécifiques, légitimes et explicitement définis.
- **Limiter la collecte de données :** L’entreprise doit collecter seulement les données strictement nécessaires pour atteindre les finalités définies. La collecte de données excessives ou non pertinentes augmente les risques et la surface d’attaque.
- **Limiter la durée de conservation des données :** Les données doivent être conservées uniquement pour la durée nécessaire à l’atteinte des finalités définies. A titre d’exemple, les dossiers médicaux sont conservés au maximum 20 ans et les données d'un prospect ne répondant à aucune sollicitation sont conservables pendant 3 ans maximum.
- **Recueillir le consentement des individus** : Pour manipuler des données personnelles, et à fortiori de santé, **il faut avoir recueilli le consentement explicite de la personne concernée**. Certains traitements peuvent cependant être exemptés de consentement, par exemple s’ils sont nécessaires à la sauvegarde des intérêts vitaux de la personne concernée.
- **Informer de manière transparente les individus :** L’entreprise doit fournir aux personnes concernées des **informations claires, accessibles et compréhensibles** sur les finalités du traitement, les catégories de données collectées et leurs droits (d’accès, de rectification, à l’effacement, de limitation, à la portabilité, d’opposition).
- **Sécuriser les données sensibles :** La pseudo-anonymisation et le chiffrement à l’état de l’art des données sensibles comme les données de santé est fortement recommandé.
- **Réaliser une analyse d’impact relative à la protection des données (AIPD)** en amont du traitement des données s’il est susceptible d’engendrer un risque élevé pour les droits et les libertés des personnes concernées.