Règlement général sur la protection des données (personnelles)

General Data Protection Regulation

Vendredi 9 décembre 2022

Les bases

- Règlement européen applicable sur tout le territoire de l'EU
- Transposé en droit français le 25 mai 2018
- Un traitement : toute manipulation de données (y compris papier, copie, transfert, etc.)

Objectif RGPD : protéger les droits fondamentaux des personnes (vie privée, utilisation/réutilisation abusive, etc.)

Données personnelles

- Toute donnée liée à une personne physique
- Données identifiantes :
  - Directement (nom, prénom, etc.)
  - Indirectement (date de naissance, ID, n° tél, etc.)
- Données sensibles :
  - code NIR (aka n° Sécurité Sociale), données de santé, opinions, orientations, etc.
- Principe de base : collecte et traitement doivent être licites

Droits des personnes

- Consentement préalable à la collecte des données
- Consentement libre, spécifique et informée
- Préciser la ou les finalités de la collecte / l'usage
- Conservation limitée dans le temps (droit d'oubli)
- Cas des personnes vulnérables
- Droits d'opposition, d'accès, de rectification, de portabilité. Répondre sous 1 mois
- Ces droits sont limités dans certains cas (obligation légale, abus, etc.)

Précautions d’usage en recherche (données personnelles)

- Séparez données primaires (collectées) et secondaires (résultantes)
- Principe de minimisation : seulement le nécessaire
- Anonymisez / pseudonymisez ASAP
- Agrégez ou décorrélez
- Protégez, sauvegardez, supervisez
- Détruisez ASAP

RT et ST

- Le Responsable de Traitement est le donneur d'ordre
  - Toujours responsable
- Le Sous-Traitant opère pour le compte du RT
- Contrat « RGPD » entre RT et ST
- Attention aux transferts hors UE et pays adéquats
- Cloud Act, Privacy Shield, domaines juridiques mouvants

Procédures de mise en conformité

- Conseil auprès du Data Protection Officer
- Inscription au registre des traitements de l'UBO
- Rédaction du protocole de recherche : partie RGPD
- Méthodologies de Référence (MR)
- AIPD : analyse d'impact
- Comité éthique (éventuellement)
- Déclaration « CNIL » spécifique (éventuellement)

Méthodologies de Référence

- 6 MR (cf. cnil.fr)
- La plus courante : MR-004 - « Recherches n'impliquant pas la personne humaine, études et évaluations dans le domaine de la santé »
- → concerne les traitements de données personnelles à des fins d'étude, d'évaluation ou de recherche sans impact sur la santé des personnes concernées

Les risques

- Violation de données : fuite, perte, altération
    - Alerter et informer
    - Remédier
    - (re)sécuriser
- Recours des personnes et des tiers
- Croisement / désanonymisation

Les sanctions

Sanctions

- Financières
- Pénales
- Professionnelles

Impacts :

- Perte d'image, de crédibilité
- Impact sur l'avenir : défiance des tiers
- Injonction à stopper le traitement, à corriger
- Audits subséquents et charge de travail associée

Pour en savoir plus

- Pour l'UBO : dpo@univ-brest.fr
- CNIL :
  https://www.cnil.fr/
  https://www.cnil.fr/fr/comprendre-le-rgpd

« Aussi ouvert que possible, aussi fermé que nécessaire »