RGPD et Suivi de Cohortes

Pr Xavier Thirion

Délégué à la Protection des Données de l'Ap-Hm
(DPO)

Mots clés

RGPD : Règlement Général sur la Protection des Données

S’applique à toutes les structures et entreprises de l’UE

Protection des données à caractère personnel

Données sensibles : exemple données de santé

Interdit le traitement de données sensibles à caractère personnel sauf strict respect de la réglementation

Responsable du traitement

Délégué à la Protection des Données (DPO)

Organisme de contrôle en France = CNIL

2019 : Nouvelle version de la loi « Informatique et Libertés »

Clarification de la CNIL concernant les registres et cohortes

Tous les traitements mettant en œuvre un recueil pérenne de données de santé à caractère personnel (cohortes, registres, …) sont assimilés à la constitution d'un **entrepôt de données de santé**

La formalité applicable est une **demande d'autorisation** (Sous-section 1 de la section 3 du chapitre 3 du titre 2 de la Loi Informatique et Libertés)

Les éléments à fournir à la CNIL pour la demande d'autorisation sont énumérés article 33 de la Loi Informatique et Libertés

En pratique

Soit la cohorte a été constituée en vue d'un protocole de recherche particulier et son suivi s'arrête à la fin de l'étude

Soit, et c'est le plus souvent le cas, la cohorte est mise en œuvre de manière pérenne et un certain nombre d'études sont organisées à partir de cette cohorte.

Etape préliminaire obligatoire : l’analyse d’impact

appelée PIA (privacy impact assessement)

appelée aussi AIPD (analyse d'impact relative à la protection des données)

Description PIA (AIPD)

L’analyse d’impact comprend :

- une **description** systématique des **traitements de données** envisagées et leurs **finalités**
- une **évaluation de la nécessité** et de la **proportionnalité** des traitements au regard des finalités
- une **évaluation des risques** sur les droits et libertés des personnes concernées
- les **mesures envisagées** pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du règlement.

Quand réaliser une analyse d'impact ?

Pour les nouveaux traitements :

- avant toute mise en œuvre
- nécessité de la mettre à jour pendant toute la durée du traitement

Pour les anciens traitements déjà en conformité avec la CNIL

- non obligatoire pendant 3 ans (reste 18 mois)
- puis obligatoire pour tous les traitements à risque élevé

Qui doit réaliser l'analyse d'impact ?

Sous la responsabilité du DG :

Une analyse d'impact nécessite la collaboration de 4 types d'acteurs :

- Le chef de projet
- les évaluateurs (RSS et Juristes)
- le DPO
- le validateur (Mme Breton)

Si il y a un sous-traitant, le sous-traitant doit apporter son aide

Analyse d'impact en pratique

Sous contrôle du DPO

Nécessité d'être accompagné par un prestataire compétent

3 phases

- évaluation des risques
- définition des mesures correctrices
- évaluation du risque résiduel après mise en œuvre des mesures correctrices

Le coût peut être important

La durée peut être importante (mise en œuvre des mesures correctives)

Avis du DPO

Elle engage le responsable de traitement (DG de l'Ap-Hm) : décision finale

Quid des cohortes en cours ?

A l'occasion de la moindre demande de modification (durée, personnes concernées, catégories de données traitées…)

La CNIL demande de refaire l'ensemble des démarches d'autorisation selon les nouvelles procédures.

Tous les traitements mis en œuvre avant le RGPD (mai 2018) doivent se mettre en conformité avant mai 2021

Et après

Toutes les études et recherches menées à partir des données recueillies à partir d'un Entrepôt de Données de Santé ou d'un recueil pérenne d'information doivent être menées conformément au CSP et à la Loi Informatique et Libertés :

RIPH ou RNIPH ?

Méthodologies de référence (MR-001, MR-003 ou MR-004 principalement)

Merci de votre attention