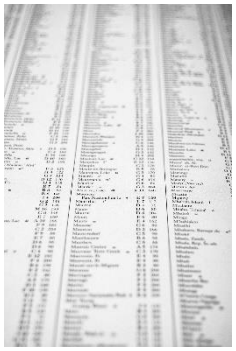
Traitements de données personnelles et registre des activités de traitement à l'hôpital

Auteur : Christophe PIQUER Mis à jour le 15/07/2024



L'obligation de tenir un registre des traitements concerne tous les organismes, publics comme privés et quelle que soit leur taille, dès lors qu'ils traitent des données personnelles. (CNIL).

Qu'est-ce qu'un traitement de données personnelles ?

Définition de la CNIL :

Un traitement de données personnelles est une opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission ou diffusion ou toute autre forme de mise à disposition, rapprochement).

Un traitement de données personnelles n'est pas nécessairement informatisé : les fichiers papier sont également concernés et doivent être protégés dans les mêmes conditions.

Un traitement de données doit avoir un objectif, une finalité déterminée préalablement au recueil des données et à leur exploitation.

Exemples de traitements : tenue du registre des sous-traitants, gestion des paies, gestion des ressources humaines, etc.

Qu'est-ce qu'un registre des activités de traitement ?

Définition de la CNIL :

Le registre est prévu par l'article 30 du RGPD. Il participe à la documentation de la conformité.

Document de recensement et d'analyse, il doit refléter la réalité des traitements de données personnelles et permet d'identifier précisément :

- les parties prenantes (représentant, sous-traitants, co-responsables, etc.) qui interviennent dans le traitement des données,
- les catégories de données traitées,
- à quoi servent ces données (ce que vous en faites), qui accède aux données et à qui elles sont communiquées,
- combien de temps vous les conservez,
- comment elles sont sécurisées.

Au-delà de la réponse à l'obligation prévue par l'article 30 du RGPD, le registre est un outil de pilotage et de démonstration de la conformité au RGPD. Il permet de documenter les traitements de données et de se poser les bonnes questions : ai-je vraiment besoin de cette donnée dans le cadre de mon traitement ? Est-il pertinent de conserver toutes les données aussi longtemps ? Les données sont-elles suffisamment protégées ? Etc.

Sa création et sa mise à jour sont ainsi l'occasion d'identifier et de hiérarchiser les risques au regard du RGPD. Cette étape essentielle permettra d'en déduire un plan d'action de mise en conformité des traitements aux règles de protection des données.

Un registre permet de recenser les traitements de données de chaque structure hospitalière et de disposer d'une vue d'ensemble de ce qui est fait des données personnelles (patients, agents, fournisseurs, prestataires…). Cet outil de mise en conformité au RGPD doit être alimenté et mis à jour régulièrement. Aussi, le DPO demande(ra) aux responsables des traitements de renseigner un fichier pour chaque traitement de données personnelles mis en œuvre dans les unités et services des établissements hospitaliers et de lui retourner pour pouvoir procéder à l'enregistrement ou à la mise à jour dans le registre de l'établissement concerné.

Image : https://pixabay.com/fr/photos/liste-noms-de-famille-tableau-428312/