Le DPO et la protection des données personnelles à l'hôpital

Auteur : Christophe PIQUER Mis à jour le 13/07/2024

Le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (RGPD) est le cadre juridique applicable depuis mai 2018 dans toute l'Europe en matière de protection des données personnelles. Il repose sur une logique de conformité dont les acteurs sont responsables. Le délégué à la protection des données (DPO) est au cœur du RGPD.

La protection des données personnelles repose sur 5 règles que sont :

- la finalité du traitement ;
- la pertinence des données collectées ;
- la conservation limitée des données ;
- l'obligation de sécurité et de confidentialité ;
- le respect des droits des personnes.

Conformément à l'article 37.1 du RGPD, la désignation d'un DPO est obligatoire pour les établissements hospitaliers. Celui-ci doit avoir une bonne connaissance du secteur d'activité ainsi que des règles et des procédures, associée à un bon niveau d'expertise en matière de données traitées, de système d'information et des besoins de l'organisme en termes de sécurité et de protection des données. Il faut aussi qu'il fasse preuve d'intégrité et d'éthique professionnelle et qu'il bénéficie d'un bon positionnement au sein de l'organisme.

Le rôle et les missions du DPO sont :

- informer et conseiller ;
- contrôler le respect du RGPD et du droit national en matière de protection des données ;

- conseiller sur la réalisation d'études d'impact sur la protection des données et en vérifier l'exécution ;
- coopérer avec l'autorité de contrôle (CNIL) et être le point de contact de celle-ci ;

La mise en conformité au RGPD se construit en 6 étapes :

1. Désignation d'un DPO ;
2. Cartographie des traitements de données personnelles ;
3. Priorisation des actions à mener ;
4. Gestion des risques ;
5. Organisation des processus ;
6. Documentation de la conformité.

Le DPO est un acteur majeur dans la protection des données personnelles et pas seulement pour celles qui concerneraient les patients. Son rôle n'est pas tant technique mais plutôt axé sur la vérification de la conformité au RGPD et à la « loi informatique et libertés ». Son positionnement institutionnel doit pouvoir lui garantir son indépendance et son intégrité ainsi que les moyens nécessaires pour l'exécution de ses missions.

Image : https://pixabay.com/fr/photos/ordinateur-entreprise-gdpr-3233754/