# RGPD en EHPAD : comprendre les obligations et mettre en œuvre une démarche de conformité

Dans un EHPAD, la gestion des données personnelles des résidents, des familles et des professionnels constitue un enjeu majeur de confidentialité et de conformité réglementaire. Le Règlement Général sur la Protection des Données (RGPD) impose aux établissements de mettre en place des mesures adaptées pour garantir la protection de ces informations, notamment des données de santé.

Cette formation propose une approche pratique et opérationnelle du RGPD, adaptée aux spécificités du secteur médico-social. Elle permet aux participants de comprendre les principales obligations réglementaires, d'identifier les risques liés aux traitements de données et d'adopter les bonnes pratiques au quotidien.

À travers des exercices et des ateliers de mise en conformité, les participants seront amenés à réaliser une cartographie simplifiée des traitements de données personnelles, évaluer les pratiques existantes et élaborer un plan d'action RGPD adapté à leur établissement.

L'objectif est de leur donner les connaissances, les méthodes et les outils nécessaires pour engager, structurer et maintenir une démarche de conformité RGPD au sein de leur EHPAD.

**Formateur·rice(s) :**

- Charlotte - Pialab Kern

## Objectifs visés

- Comprendre les objectifs du RGPD et son application au secteur médico-social.
- Identifier les données personnelles et les données sensibles traitées dans un EHPAD.
- Comprendre les enjeux de confidentialité et de protection des données des résidents, des familles et des professionnels.
- Comprendre les principes de licéité, transparence, minimisation et limitation de la conservation des données.
- Identifier les bases légales des traitements et les conditions particulières applicables aux données de santé.
- Connaître les droits des résidents et des autres personnes concernées.

## Méthodes d'évaluation

- Quiz
- Cas pratique

- Appliquer les règles de confidentialité lors de l'accès, de l'utilisation et du partage des informations.
- Recenser les traitements de données personnelles réalisés au sein de l'EHPAD.
- Vérifier la conformité des traitements aux principes du RGPD (finalités, bases légales, minimisation, durées de conservation).
- Identifier et évaluer les risques liés à la protection des données personnelles.
- Définir les mesures organisationnelles et techniques nécessaires pour sécuriser les données.
- Mettre en place et actualiser la documentation de conformité (registre, notices d'information, procédures).
- Élaborer un plan d'action et organiser le suivi de la conformité dans la durée.
- Identifier les principaux documents et procédures de conformité : registre des traitements, mention d'information, politiques
- Distinguer les notions de responsable de traitement, de sous-traitant et de délégué à la protection des données (DPO).
- Identifier les responsabilités et obligations du responsable de traitement et de ses sous-traitants.
- Connaître les obligations à respecter dans les relations avec les prestataires externes, notamment en matière de contractualisation et de sécurité des données.
- Identifier les bonnes pratiques permettant d'intégrer la protection des données dans le fonctionnement quotidien de l'établissement.
- Identifier les situations nécessitant une mise à jour de la documentation RGPD.
- Définir les actions de sensibilisation à mettre en place auprès des professionnels de l'EHPAD.

# Déroulé pédagogique

## Journée 1

- Introduction au RGPD et à ses enjeux en EHPAD
- Les principes fondamentaux du RGPD appliqués aux activités de l'EHPAD

- Pause
- Mettre en œuvre une démarche de conformité RGPD en six étapes
- Cas pratique : réaliser une cartographie des traitements de données d'un EHPAD
- Pause déjeuner
- Les mesures organisationnelles et les bonnes pratiques de protection des données
- Les rôles et responsabilités dans la protection des données personnelles
- Pause
- Faire vivre et maintenir la conformité RGPD au quotidien en EHPAD
- Cas pratique : élaborer un plan d'action de mise en conformité RGPD

# Informations complémentaires

**Durée :** 8.25 heures de formation sur 1 jour

**Pré-requis :**

**Public concerné :** Formation ouverte aux personnes salariées dont l’employeur ou un opérateur de compétences finance l’intégralité du coût de la formation.