Personnes présentes :

- Nicole FERREIRA, co-directrice Agence SolEn
- Thierry FILHOL, co-directeur Agence SolEn

Webinaire : Les enjeux du RGPD pour les métiers du médico-social

1. La présentation du RGPD

➔ Le RGPD : Règlement Général sur la Protection des Données
➔ Applicable en France depuis le 25/05/2018
➔ Harmonise le droit européen
➔ Renforce la maîtrise des individus sur leurs données dans un contexte de plus en plus numérisé
➔ Concerne tous les organismes (grandes entreprises, PME, TPE, associations)

2. Les sanctions

Jusqu'à 10 ou 20 millions d'euros ou 2 à 4% du chiffre d'affaires mondial
Potentielles poursuites pénales et civiles + Mauvaises réputations / Mauvaises images

3. Le RGPD dans vos structures

- Nom/Prénom
- N° de Sécurité Sociale
- N° de Patient

Les dispositions du RGPD s'appliquent à tous les traitements de données personnelles que les établissements utilisent pour l'exercice de leurs activités professionnelles, que ces traitements soient sous une forme informatique ou papier.

4. Les étapes à suivre

Vous devez donc :

- Disposer d'un registre de traitements de données
- Assurer le droit des personnes
- Disposer d'un DPO (pas obligatoire en EHPAD, mais fortement recommandé. Si non, une personne chargée en interne de la protection des données, qui sera fortement impliquée)
- Mettre en place des procédures garantissant la sécurité et la confidentialité des données

5. Les structures concernées

- Personnes en situation de handicap
- Personnes âgées

6. Les actions clés

1- Désigner un pilote, un DPO, ça rassure
2- Cartographier vos traitements de données personnels (le gros du travail)
3- Prioriser les actions à mener
4- Gérer les risques
5- Organiser les processus internes
6- Documenter la conformité

7. Les risques encourus dans votre métier

Vos structures sont concernées par le RGPD au même titre que les autres établissements publics ou privés du secteur sanitaire. Vous collectez, stockez et utilisez des données à caractère personnel, vous êtes donc des responsables de traitement. Le RGPD a fortement accru le pouvoir de contrôle et de sanction de la CNIL qui peut désormais prononcer des amendes financières et pénales.
Dès lors, le risque de non-conformité est nettement plus important qu'il ne l'était avant la date d'application du RGPD. Les secteurs médico-sociaux, qui traitent des données particulièrement

sensibles, doivent prouver à tout moment leur bonne foi et leur engagement dans la démarche de conformité au RGPD.

8. Les exemples de risques

➔ *L'hôpital de Saint-Gaudens touché par une attaque informatique*
➔ *L'entreprise Pierre Fabre à l'arrêt à la suite d'une cyberattaque*
➔ *Piratage informatique : ce que l'on sait de la fuite de données médicales de près de 500 000 patients français*

9. Le dossier de l'usager

Le dossier de l'usager recueille l'ensemble des informations administratives, socio-éducatives, médicales, paramédicales et professionnelles de la personne accueillie au sein d'un ESMS. L'ensemble de ces données permet d'établir une meilleure compréhension de la situation de l'usager afin d'établir un diagnostic, de concevoir un projet et d'en effectuer son évaluation.
Le dossier de l'usager doit garantir une utilisation fiable des données et de leur traitement, en respectant les conditions de la **CNIL** et du **RGPD**.

10. Le dossier de l'usager dans le format numérique

Pour favoriser l'émergence d'une **société plus inclusive** accélérer la transformation de l'offre et accompagner les pratiques, le numérique apparaît comme un levier majeur. Il permet :

- **D'améliorer l'accompagnement des personnes**, grâce à une meilleure formalisation et circulation des informations entre les professionnels et avec les personnes accompagnées ;
- **D'impliquer davantage les usagers dans leur parcours**,
- De **faciliter l'accès au soin et à l'accompagnement** pour tous,
- De **libérer du temps aux professionnels** pour accompagner les personnes et renforcer la coopération entre acteurs,
- **D'offrir une meilleure connaissance des personnes accompagnées**, contribuant ainsi à un meilleur pilotage des politiques publiques en faveur des plus fragiles.

11. Le Ségur du numérique en santé

Le Ségur du Numérique en santé alloue une enveloppe exceptionnelle de 600 millions d'euros pour le secteur médico-social et social, pour **accélérer la transformation numérique** du secteur et **améliorer la qualité des systèmes d'information**.
Il s'adresse à l'ensemble des établissements en vue de l'acquisition ou la mise à niveau du logiciel du **DUI** (Dossier Usager Informatisé), prise en charge par l'état.
Ce programme a ainsi pour objectif de favoriser le développement de systèmes d'information **conformes à des exigences techniques, fonctionnelles et ergonomiques, permettant la production, la structuration, la conservation et le partage des données, dans le respect des dispositions du code de la santé publique et du RGPD**.
La maîtrise du risque numérique est un axe majeur du Ségur de la santé. Le nouveau référentiel de la HAS en fait d'ailleurs mention. L'accompagnement à la conformité du RGPD est ainsi un **préalable à cette mise à niveau**.

12. Le CPOM

C'est un outil qui favorise la transversalité de l'offre d'accompagnement.
Le CPOM va définir les financements délégués par l'ARS.
Cette démarche permet de renforcer la dimension stratégique à l'aide de projets digitaux et du système d'information sur le moyen terme.
Le CPOM doit inclure le RGPD. Protéger de manière efficace ses données et intégrer le RGPD dans cette démarche permettra de renvoyer une image qualitative de votre structure à l'ARS.

13. Définition du DPO

Le DPO : Délégué de la Protection des Données

Il est la personne en charge de la protection des données à caractère personnel au sein des organismes publics ou privés. Il sera en charge de la gestion des demandes d'exercice des droits pour prémunir des risques.

Le G29 (organisme qui fédère l'ensemble des CNIL européennes) encourage les entreprises non soumises à l'obligation (tels que les EHPAD) de se doter tout de même d'un DPO, en interne ou externalisé.

14. Le rôle du DPO

Le DPO veille à la conformité de son organisme au regard de la réglementation applicable en matière de protection des données personnelles. Il doit :

- Informer, conseiller et être toujours disponible pour toute question
- Contrôler le respect du règlement et du droit national
- Établir une analyse d'impact
- Assurer une coopération avec l'autorité de contrôle locale
- Tenir un registre de traitement

15. Les avantages du DPO externalisé

Le DPO externe est soumis au secret professionnel et à une obligation de confidentialité.
Il est le référent principal en cas de mutualisation.

- Accompagnement par 1 DPO certifié
- Audit et mise en conformité
- Mise en place d'une politique générale de protection des données
- Animation, veille et maintenance
- Gage de neutralité et d'implication de la structure

16. Le focus sur les 4 registres obligatoires

Registre de traitements → Il permet de recenser vos traitements de données et de disposer d'une vue d'ensemble de ce que vous faites avec les données personnelles

Registre des sous-traitants → Il doit contenir toutes les catégories d'activité de traitements de données effectuées pour le compte de clients.

Registre de violations → Tous les organismes qui traitent les données personnelles (responsable de traitement ou sous-traitant) prévoient et mettent en place des procédures globales en matière de violation de données.

Registre des gestions des droits → Il répertorie les demandes et les réponses aux usagers concernant leurs droits d'accès, de rectification, etc.

SolEn - Une Solution pour chaque Entreprise

Nicole FERREIRA : Co-Directrice agence SolEn
07.78.87.61.25
nicole-ferreira@sol-en.fr

Thierry FILHOL
06.89.71.25.80
Thierry-filhol@sol-en.fr