

RGPD Démystification & démarche orientée EHPAD

Effigen



INTERVENANTE : LAURENCE BARDE
Associée gérante, en charge de l'offre ESMS

CONSEIL ET FORMATION

www.affigen.com



Jeudi 4 avril 2019

Salons d'Affaires du Centre des Salorges - CCI Nantes

Thème :
«Quelles libertés en EHPAD ?»



Règlement Général de la Protection des Données



Présentation (très rapide !) d'Effigen

Le Quizz... !

RGPD ? Quel contexte, quels enjeux ?

– rappels généraux synthétiques –

Démarche, spécificités et cas d'usages en EHPAD

Un contexte général commun à tous les EHPAD

Démarche commune optimisée possible

Présentation (rapide !) d'Effigen...

Cabinet **conseil & formation**, créé en **2008** et basé à **Nantes**

Habilitation HAS, organisme de formation déclaré

Domaines d'intervention : sanitaire, **médico-social**, Industrie & services

Plus de **40 références clients ESMS, 80%** auprès de structures au service des **personnes âgées** (EHPAD, Foyer-logement, SSIAD)

Missions : **stratégiques, opérationnelles** et visant l'**amélioration continue**

Un cabinet à taille humaine, une équipe de spécialistes...



Des domaines d'intervention ciblés...

Projet
d'établissement

Diagnostic
& préconisations

CPOM

RGPD

Efficiences
organisationnelles

Évaluation
interne

Évaluation
externe

Développement
des compétences

institut
Effigen

LE Quizz... en 10 questions

En 2mn chrono

Répondre de manière spontanée

Comptabiliser vos « oui » et vos « non »

...

Prêt ?

C'est parti !

Le quizz !

Dans ma structure....

- 1) Un DPO a été nommé (*si vous ne savez pas ce que c'est... la réponse est « NON » !*)
- 2) Les collaborateurs sont informés de leurs droits et connaissent le contact RGPD
- 3) Les données à caractère personnel ainsi que les traitements les utilisant ont été inventoriés
- 4) Les usagers et familles connaissent le contact RGPD et leur consentement spécifique et positif de leurs données personnelles leur a été demandé
- 5) Aucune transmission n'est notée sur un cahier (fait exclusivement dans l'outil informatique dédié, accessible via un identifiant et mot de passe personnalisés)
- 6) Seules, les informations personnelles, strictement nécessaires à une prise en charge efficiente, sont stockées et ce uniquement sur la durée nécessaire
- 7) Aucun outil bureautique (Word, Excel) ne contient de données personnelles
- 8) Une messagerie sécurisée est utilisée pour les échanges contenant des données personnes (ex. entre médecins, structures, pour passer une commande de médicaments à l'officine, ...)
- 9) Un contrat de sous-traitance spécifique RGPD a été mis en place avec les fournisseurs concernés (ex. officine, ambulanciers, hébergement informatique,...)
- 10) Un plan d'action a été formalisé pour pallier aux zones à risque identifiées

Le quizz !

Dans ma structure....

- 1) Un DPO a été nommé (*si vous ne savez pas ce que c'est... la réponse est « NON » !*)
- 2) Les collaborateurs sont informés de leurs droits et connaissent le contact RGPD
- 3) Les données à caractère personnel ainsi que les traitements les utilisant ont été inventoriés
- 4) Les usagers et familles connaissent le contact RGPD et leur consentement spécifique et positif de leur données personnelles leur a été demandé
- 5) Aucune transmission n'est faite sur un cahier (fait exclusivement d'un outil informatique dédié, accessible via un identifiant et mot de passe personnalisés)
- 6) Seules, les informations personnelles, strictement nécessaires à une prise en charge efficiente, sont stockées et ce uniquement sur la durée nécessaire
- 7) Aucun outil bureautique (Word, Excel) ne contient de données personnelles
- 8) Une messagerie sécurisée est utilisée pour les échanges contenant des données personnes (ex. entre médecins, structures, pour passer une commande de médicaments à l'officine, ...)
- 9) Un contrat de sous-traitance spécifique RGPD a été mis en place avec les fournisseurs concernés (ex. officine, ambulanciers, hébergement informatique,...)
- 10) Un plan d'action a été formalisé pour pallier aux zones à risque identifiées

RGPD : quel contexte, quels enjeux ?

- Règlement **G**énéral sur la **P**rotection des Données (RGPD)
 - Accroître la protection des **données à caractère personnel (DCP)**
 - Cadre juridique européen imposé: le règlement n° 2016/679
- **1 référent RGPD à désigner** pour chaque structure médico-sociale: Le délégué à la protection des données personnelles **DPD** ou **DPO** « *Data Protection Officer* »
- 1^{er} anniversaire... **les attendus depuis le 25 mai 2018 :**

- **DPO désigné**
- **Inventaire et analyses d'impact réalisés pour les traitements à risque**
- **Plan d'action « raisonnable » établi pour mettre en conformité les « zones à risques »**

- CNIL versus RGPD / CIL versus DPO
 - La « Loi Informatique et Libertés (droit national) : **simple déclaration** préalable de tout traitement des données auprès de la CNIL
 - **RGPD** (cadre juridique européen): au-delà et **approche inversée** ⇒ pas une simple déclaration mais l'existence d'un **processus de protection** :
 - **Cartographier** les risques relatifs aux données à caractère personnel pour chaque traitement
 - **Évaluer** ces risques
 - Mettre en place des **mesures** pour les **réduire et gérer les violations**
 - **Approche non informatique !** 
 - Données pas uniquement informatiques !
 - « Système d'**information** » différent de « système **informatique** »
 - **CIL** : informatique / **DPO** : processus, connaissance métier

En cas d'incident ou de contrôle, la CNIL **audite le processus** et non la présence d'une fiche renseignée

« **Opportunité** » de revue des processus et pratiques sur le terrain

Liens forts avec les autres outils de la loi 2002-2 (CPOM, PE, EI, EE) :
impact sur l'amélioration continue de la qualité

- Rappel des enjeux financiers
 - Avant, avec la CNIL : sanction ~100 à 300 k€
 - Les sanctions financières RGPD... des montant dissuasifs
 - **Jusqu'à 10 millions d'euros** ou, dans le cas d'une entreprise, **2% du chiffre d'affaires** annuel mondial
⇒ manquements notamment au Privacy By Design, Privacy By Default, en matière de PIA, etc.
 - **Jusqu'à 20 millions d'euros** ou, dans le cas d'une entreprise, **4% du chiffre d'affaires** annuel mondial
⇒ manquement notamment aux droits des personnes (droits d'accès, de rectification, d'opposition, de suppression, droit à l'oubli, etc.).
- **Et pénales également** ... ex. 300K€ et 5 ans d'emprisonnement pour chacune des infractions suivantes: Non-respect des formalités préalables, Non-respect de l'article 34 de la loi Informatique et Libertés relatif à l'obligation de sécurité, Détournement de la finalité des données personnelles

Sanctions opposables au médico-social, sur le C.A ou le montant du budget, selon la nature de la structure (publique, privée ou associative)

Un hôpital portugais a « inauguré » les sanctions financières au titre du RGPD en écopant d'une amende de 400 000 euros

(en lien avec la politique d'accès aux bases de données des patients / inspection diligente en juin 2018 suite à alerte émise par l'ordre des médecins)

Démarche, spécificités et cas d'usage en EHPAD

OU

*« Comment mettre en œuvre la RGPD de manière
efficace, en cohérence avec les risques et la taille
de ma structure,
sans partir de la page blanche »*

Savoir-faire

Sensibiliser

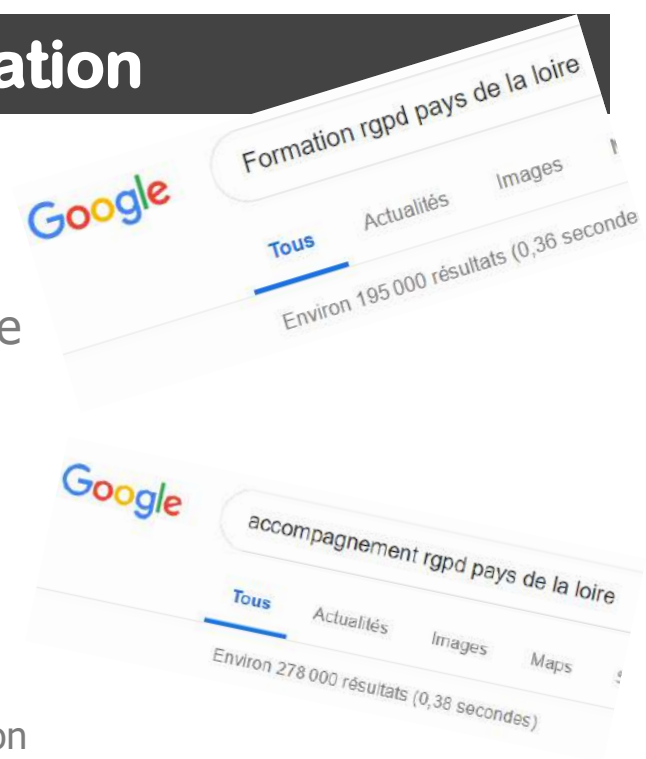
Mettre en œuvre

Nécessité de « **savoir faire** »... la formation

- La « **jungle** » des propositions...
 - Formations payantes, gratuites
 - Souvent abordées sous l'angle informatique
- **La référence : les publications de la CNIL**
 - Très documentées = complexes
 - Pour tout type de structures
 - Néanmoins des publications dédiées :

<https://www.cnil.fr/fr/le-rgpd-applique-au-secteur-de-la-sante>

Depuis tout récemment (mars 2019), mise à disposition d'un MOOC* <https://atelier-rgpd.cnil.fr/>
(public concerné: plutôt le DPO)



Bienvenue sur le MOOC de la CNIL

Vous y trouverez l'ensemble des informations pour vous **initier au RGPD** et débiter ainsi **la mise en conformité de votre organisme**.

Ce dispositif gratuit est accessible jusqu'au mois de septembre 2021.
En suivant l'intégralité de ce MOOC, vous pourrez obtenir une **attestation**.



* **MOOC** : Massive
Open Online Course,
ou Formation en Ligne
Ouverte à Tous (FLOT)

Nécessité de « sensibiliser »... la communication

- **Auprès des collaborateurs, à plusieurs niveaux... (valable pour toutes les structures)**
 - Collecte de **leurs données** personnelles
 - **Droits d'accès** (copie, rectification, effacement « droit à l'oubli », traitement / utilisation)
 - Aux enjeux du RGPD **pour la structure**
 - Interdiction de divulguer des données à des personnes non autorisées, données accessibles à certaines personnes uniquement, sauvegarder régulièrement les fichiers, ...
 - Sécuriser les données (ex : complexifier et modifier régulièrement les mots de passe personnels, verrouiller le poste de travail, ...)

Logique de **responsabilisation de tous les acteurs**
ayant une **implication directe ou indirecte**
dans le traitement des DCP

Nécessité de « savoir »... **mettre en œuvre**

- Comment **ne pas partir de la page blanche** ?
 - **Un outil de référence** ... le logiciel open source PIA facilite la conduite et la formalisation d'analyses d'impact relatives à la protection des données (AIPD) telles que prévues par le RGPD **POUR LES PROCESSUS A RISQUE ELEVE**
<https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil>

130 000
téléchargements
(décembre 2018)

Modulaire pour
s'adapter aux
besoins : modèle PIA
duplicable et
utilisable pour des
traitements similaires

Base de
connaissance
juridique et technique

Graphique état
des risques

**Complexe / intérêt uniquement pour les
traitements à fort risque => à identifier**

The screenshot shows the PIA software interface. At the top, it says 'Pia | analyse d'impact sur la protection des données' and 'privacy impact assessment'. Below this, there are several panels. On the left, there's a 'Voxfood' section. In the center, there are sections for 'Principes fondamentaux' and 'Principes juridiques'. On the right, there's a 'Menaces' section with a list of threats like 'Menaces', 'Agressions', 'Perte d'emploi', etc. Below the 'Menaces' section, there's a risk assessment diagram with a central node 'Accès illégitime à des données' and several branches leading to different risk levels: 'Gravité : Importante', 'Vraisemblance : Maximale', 'Gravité : Limitée', and 'Vraisemblance : Limitée'. The diagram also includes 'Menaces' like 'Consultation ou vol des données', 'Usurpation d'un compte', 'Emploi', 'Entourage', 'Attaquant', and 'Usurpation'.

Comment ne pas partir de la page blanche ?

Le contexte en EHPAD...

- **Temps nécessaire**
pour appréhender le sujet, le mettre en œuvre... en plus des autres tâches quotidiennes
- **Quel profil pour le DPO?**
rappels : indépendance dans l'analyse, absence de conflit d'intérêt, vision transversale des processus,...
- **Plus de 80% du contexte identique pour les EHPAD** en termes de traitements des données et de risques

Mutualiser pour être plus efficient
« ouvrir le champ des possibles »

Plusieurs démarches et approches possibles de mutualisation entre structures

- **Former et sensibiliser de manière transversale**
 - Partager des coûts de formation
 - Mettre en œuvre des supports de sensibilisation communs et les personnaliser au contexte de chaque structure
- **Mener les travaux ensemble** (un DPO par structure)
 - Répartition des tâches sur les 80% identiques
 - Personnalisation, finalisation et pilotage dans chaque structure
- **Utiliser des supports pré-formalisés et orientés EHPAD**
- **Partager un profil professionnel de DPO** « en temps partagé »

- **Utiliser des supports pré-formalisés et orientés EHPAD**

Nécessité de « savoir »... **mettre en œuvre**

Un exemple **concret** de support **pragmatique** et **opérationnel**... la « **boîte à outils** » **RGPD**

Les 6 étapes de la CNIL

-  **Désigner**
un pilote
-  **Cartographier**
vos traitements de données personnelles
-  **Prioriser**
les actions
-  **Gérer**
les risques
-  **Organiser**
les processus internes
-  **Documenter**
la conformité

RAPPELS AMORCE & ETAPES CLES
DPO désigné
Inventaire et analyses d'impact
Plan d'action « zones à risques »



Structure concernée
Localisation
Pilote du processus / Direction*
DPO / Référent RGPD*

* supprimer la mention inutile

TABLEAU DE BORD Cadrage, organisation et pilotage PROCESSUS RGPD

A COMPLETER
A COMPLETER
A COMPLETER
A COMPLETER

INFORMATIONS GENERALES

LEGENDES

Couleurs zones

zone à compléter	
zone complétée automatiquement	
explications d'utilisation	

Statuts avancement

Non commencé	En cours
Finalisé	finalisé/validé
Non concerné	

SOMMAIRE

Classification des onglets/outils par phase du projet

	Accès direct en cliquant sur le thème	STATUTS AVANCEMENT	
CADRAGE	<u>Désigner un DPO</u>	Non concerné	Direction
	<u>Documents à récupérer</u>	DPO	Direction
	<u>Annuaire des acteurs sollicités</u>	DPO	Direction
	<u>Planning mise en œuvre</u>	DPO	Direction
MISE EN ŒUVRE Amorce de la démarche	Inventorier les traitements & usages	DPO	Direction
	Définir les niveaux de risque & prioriser	DPO	Direction
	Elaborer le plan d'action (Quoi/Qui/Quand)	DPO	Direction
MISE EN ŒUVRE Dans la durée	Organiser les processus internes	DPO	Direction
	Documenter la conformité	DPO	Direction
	Planning des travaux	DPO	Direction

Un module PIA avec les processus stratégiques pré-renseignés

(ex. liés à l'utilisation du logiciel de gestion des dossiers des résidents)



analyse d'impact sur la protection des données
privacy impact assessment



LES MESSAGES CLES

« La montagne n'est pas infranchissable ! »

Amorcer la démarche

Réaliser a minima les étapes pour démontrer la recherche de mise en conformité

(désignation DPO, inventaire et identification des risques, plan d'action)

Elaborer un plan d'action raisonnable et réalisable

« L'obligation RGPD, vécue comme contraignante, aura des effets collatéraux positifs ! »

RGPD en Ehpad : ce qui va changer

Page 1/2

Source :

« *Le Mensuel des
maisons de retraite* »

N°212 juin-juillet 2018

Entré en vigueur le 25 mai dernier, le RGPD suscite légitimement des interrogations quant à son contenu et sa mise en œuvre. Christophe Lévy-Dières, avocat associé au cabinet Aston et le cabinet de conseil Burbax Consulting effectuent pour vous une mise au point juridique et pratique.



© Doreen - Fotostock

RGD : quatre lettres formant un nouvel acronyme que vous, directeurs, allez devoir maîtriser. Mais concrètement, de quoi s'agit-il ? Voté par le Parlement européen en mai 2016, le RGPD est le Règlement général sur la protection des données personnelles, ces dernières étant définies comme « toute information se rapportant à une personne physique identifiée ou identifiable ».

Du fait de leurs missions, les Ehpad sont amenés à traiter un grand nombre de données personnelles que ce soit celles des personnes hébergées ou celles relatives à leur fonctionnement interne (salariés, fournisseurs, etc.). Qu'ils relèvent du secteur public ou privé, les établissements sont donc directement impactés par cette nouvelle réglementation.

La protection des données à caractère personnel et la « révolution » du RGPD

Les principes fondamentaux des traitements de données personnelles ont été fixés pour la première fois dans la Loi Informatique et Libertés du 6 janvier 1978. Ces principes ont constitué le socle juridique dans la matière et ont

désormais été unifiés dans l'ensemble du territoire européen. Pour mémoire, ces principes sont la finalité, la loyauté et la licéité dans toute collecte de données personnelles, une protection aux droits des personnes concernées comme le droit d'accès, de rectification et de suppression des données.

Les 99 dispositions du RGPD consacrent et renforcent ces principes, le RGPD prévoyant notamment une protection accrue des données dites « sensibles » comme les données relevant de l'origine raciale, de convictions religieuses ou relatives à la santé. Sur ce dernier point, le RGPD instaure une définition commune des données de santé à l'échelle de l'Union européenne. Il s'agit de « données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne ».

Les Ehpad sont ainsi amenés à prendre en compte ces nouvelles dispositions dans leur gestion quotidienne. Mais plus encore, le RGPD constitue une véritable révolution en ce qu'il impose des changements multiscalaires qu'il est nécessaire de maîtriser au sein des Ehpad.

Le RGPD, un changement de paradigme, de culture et de gouvernance

C'est d'abord un changement de paradigme car une grande partie des formalités préalables auprès de la Commission nationale de l'informatique et des libertés (CNIL) ont complètement disparu (déclaration normale, dispenses, normes, etc.) au profit d'une logique de responsabilisation de tous les acteurs qui peuvent avoir une implication directe ou indirecte dans le traitement de données personnelles, y compris pour les sous-traitants. Désormais le responsable de traitement, c'est-à-dire la personne qui détermine les finalités et les moyens du traitement de données personnelles, n'est pas le seul responsable en cas de violation de la réglementation concernée. Cette responsabilité a été élargie aux sous-traitants. Dit autrement, toute personne prenant part à un traitement de données personnelles est garant de la conformité de ce traitement.

C'est ensuite un changement de culture car au sein des Ehpad doit s'opérer une implantation de nouveaux outils et un ensemble de mesures organisationnelles et techniques capables de supporter les nouvelles obligations imposées par le

Source :

« Le Mensuel des
maisons de retraite »
N°212 juin-juillet 2018

RGPD. Ces mesures doivent envisager la tenue d'un registre complet, exhaustif et à jour de tous les traitements de données personnelles. Elles imposent également la réalisation d'analyses d'impacts en cas de risques aux droits des personnes concernées, notamment sur la collecte, l'utilisation et l'hébergement des données sensibles concernant la santé ainsi que la mise en place d'audits afin d'évaluer les mesures de sécurité pour éviter les fuites de données, entre autres.

En plus de la mise en place de mesures issues du RGPD, dans le cas des Ehpad, une autre obligation est imposée en ce qui concerne l'hébergement des données de santé. En effet, l'article 1111-8 du Code de la santé publique prévoit que l'hébergeur saisi par l'Ehpad (un sous-traitant) doit être titulaire d'un certificat de conformité délivré par la CNIL. Cette obligation trouve également son esprit dans le RGPD car les responsables de traitements ne peuvent faire appel qu'à des sous-traitants qui présentent des garanties suffisantes.

Il y a enfin un changement de gouvernance puisque le RGPD introduit un chef d'orchestre des données personnelles au sein des Ehpad : « le délégué à la protection des données » (DPO en anglais). Sa désignation est obligatoire pour les Ehpad avec une personnalité juridique de droit public et fortement conseillée pour les Ehpad de droit privé. Parmi les missions du DPO : le maintien de la conformité des traitements, l'assistance et la formation des personnels ayant à gérer les traitements, la relation avec les personnes concernées par les traitements et les relations avec l'autorité de contrôle, la CNIL (voir encadré ci-contre).

Le RGPD et la consolidation des droits individuels des personnes

Le renforcement de ces droits concerne notamment :

- **Le droit à l'information et recueil du consentement**

Le RGPD impose la mise à disposition d'une information claire, intelligible et aisément accessible aux

personnes concernées quant à l'utilisation et la protection de leurs données personnelles collectées.

Ils doivent ensuite, en principe, donner leur accord exprès pour le traitement de leurs données. La charge de la preuve du consentement incombe à l'Ehpad et la matérialisation de ce consentement doit être « non ambiguë », en se matérialisant, par exemple, par la signature par d'un document explicite.

- **Les droits d'accès, d'opposition et de rectification**

Toute personne peut accéder à l'ensemble des informations la concernant et en connaître l'origine, accéder aux informations sur lesquelles le responsable du traitement s'est fondé pour prendre une décision la concernant, en obtenir la copie ou exiger que ses données soient, selon les cas, rectifiées, complétées, mises à jour ou supprimées.

- **Le droit à la portabilité des données**

La personne concernée a le droit de récupérer les données qu'elle a four-

nies au responsable de traitement, dans un format structuré, couramment utilisé et lisible par machine, et a le droit de transmettre ces données à un autre responsable du traitement, dans le cas d'un changement d'établissement par exemple.

Le RGPD, des sanctions renforcées

En cas d'insuffisance relative aux dispositions du RGPD, les responsables de traitement des données en général peuvent faire l'objet de la part de la CNIL de sanctions administratives sérieuses comme par exemple le retrait de la certification idoine pour traiter des données à caractère personnel.

Quant aux sanctions pécuniaires, dites amendes administratives, elles peuvent en théorie aller jusqu'à 10 ou 20 millions d'euros. Dans le cas d'une entreprise, cette amende peut s'élever jusqu'à 4% du chiffre d'affaires annuel mondial.

Christophe LEVY-DIERES
Avocat Associé - Aston Avocats

La CNIL autorité de contrôle... et plateforme d'information

Dans le but d'adapter la législation française au droit européen, un projet de loi a définitivement été voté à l'Assemblée nationale le 14 mai. Ce texte adapte la loi informatique et libertés du 6 janvier 1978. Outre la modification du chapitre consacré aux traitements de données à caractère personnel dans le domaine de la santé, il redéfinit les prérogatives de la Commission nationale de l'informatique et des libertés (CNIL), issue de la loi de 1978.

Certes la CNIL demeure l'autorité de contrôle mais elle possède d'abord une mission d'information. L'article premier de la loi du 14 mai dispose en effet que la commission « établit et publie des lignes directrices, recommandations ou référentiels destinés à faciliter la mise en conformité des traitements de données à caractère personnel avec les textes relatifs à la protection des données à caractère personnel ».

C'est dans cette logique que cette dernière a publié un guide pratique, élaboré avec le Conseil national de l'ordre des médecins. Constitué de 6 fiches thématiques, il dresse une liste de bonnes pratiques propres à chacune des fiches en vue d'assurer la transition vers le RGPD. Une transition qui, pour s'effectuer dans de bonnes conditions, passe par diverses étapes détaillées sur le site de la CNIL



CONSEIL ET FORMATION

ÉTABLISSEMENT SOCIAUX ET MÉDICO-SOCIAUX

Habilitation HAS – Organisme déclaré de formation

Merci pour votre attention

RGPD

Démystification & démarche orientée EHPAD

Envoi du support sur demande
Retrouvez-nous sur notre stand !

Contact : Laurence Barde, Associée gérante – En charge de l'offre ESMS
laurence.barde@effigen.com **06.85.06.14.66**

www.effigen.com

1, Domaine de Beauregard – 44240 Sucé-sur-Erdre