DPOPartagé

Etablissements **de santé.**

2019

Bien appliquer le règlement européen sur la protection des données.

Préparé par :

LAURENT DE CAVEL

Délégué à la protection des données
CNIL.

INFORMATIONS

EYE - DPO PARTAGE
123 AVENUE FELIX FAURE
75015 PARIS

01 85 09 15 85
06 60 68 42 42
contact@dpo-partage.fr
ldecavel@dpo-partage.fr
www.dpo-partage.fr

SYNTHESE

En BREF

Tous les établissements de santé sont concernés par le RGPD en tant que responsables de traitement de données personnelles dans leur organisme, et parfois également comme sous-traitants (dans le cadre d'un groupement par exemple).

Le RGPD porte sur **toutes les données personnelles issues des activités de l'établissement de santé**, et pas uniquement sur les données de santé générées par la prise en charge des personnes.

De nombreuses actions sont à mener depuis le 25 mai 2018, y compris pour les établissements qui disposaient déjà d'un correspondant informatique et libertés (CIL). Ces actions s'inscrivent dans la démarche globale de gestion des risques portée par l'établissement pour améliorer la qualité et la sécurité des soins, et s'intègrent notamment aux procédures de conformité de l'établissement, ainsi qu'à la gestion des risques de sécurité des systèmes d'information de l'établissement.

Nouvelle obligation : La désignation obligatoire d'un délégué à la protection des données (DPD / DPO) en cas de traitement à grande échelle des données de santé.

Soumis à une obligation de confidentialité, le DPO veille à l'application du RGPD, conseille son employeur sur les sujets relatifs à la protection des données de santé recueillies par celui-ci. Il est l'interlocuteur de la Cnil. Un salarié en poste peut être chargé de cette mission. Une mutualisation entre plusieurs établissements est également possible (RGPD, art. 47).

Les fonctions suivantes sont susceptibles de donner lieu à un conflit d'intérêts, dans les textes, ils ne peuvent être désigné en tant que DPO : secrétaire général, directeur général des services, directeur général, directeur opérationnel, directeur financier, médecin-chef, responsable du département marketing, responsable des ressources humaines ou responsable du service informatique et/ou information, mais également d'autres rôles à un niveau inférieur de la structure organisationnelle si ces fonctions ou rôles supposent la détermination des finalités et des moyens du traitement.

RGPD DANS LE MEDICAL

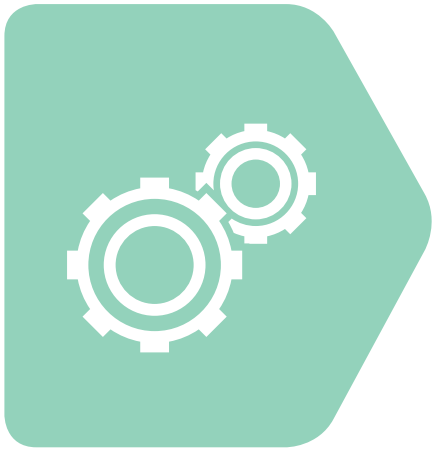
IDENTIFIEZ LA PORTEE DU RGPD DANS VOTRE ETABLISSEMENT

*La démarche de mise en conformité au RGPD concerne **tous les établissements de santé.***
Les obligations à prendre en compte varient en fonction de la qualification du rôle de l'établissement et de la nature des traitements et des données utilisées.

DEUX QUALIFICATIONS JURIDIQUES

D'une manière générale, l'établissement est responsable de multiples traitements de données personnelles, impliquant ou non des données de santé.

Dans certains cas, l'établissement peut être considéré comme un sous-traitant, lorsqu'il agit pour le compte d'un tiers, notamment dans le cadre de certains groupements.



NATURE DES DONNEES

L'établissement traite aussi des données personnelles qui ne sont pas des données de santé (les données de ressources humaines par exemple) pour lesquelles le RGPD s'applique aussi.

L'établissement de santé collecte, génère et traite également des données de santé.

Le RGPD fixe un principe d'interdiction de collecte de ces données de santé en raison de leur sensibilité. Toutefois, ce principe est assorti de plusieurs exceptions. Il est donc possible de créer un traitement de données de santé à caractère personnel lorsque la personne concernée donne son **consentement exprès**. Il y a d'autres fondements possibles, pour les diagnostics médicaux, la prise en charge sanitaire ou sociale, la gestion des systèmes et des services de soins de santé, ou encore, lorsque le traitement est lié à l'intérêt public dans le domaine de la santé publique, aux fins de recherche, de la médecine préventive ou de la médecine du travail.

VOS OBLIGATIONS

DOCUMENTATION INTERNE .01

Tenir une documentation interne (référentiel), décrivant les traitements mis en œuvre et les mesures de mise en conformité de ces traitements.

Dans certains cas (notamment les traitements de recherche), il doit solliciter l'autorisation de la CNIL avant de mettre en œuvre son traitement de données personnelles.

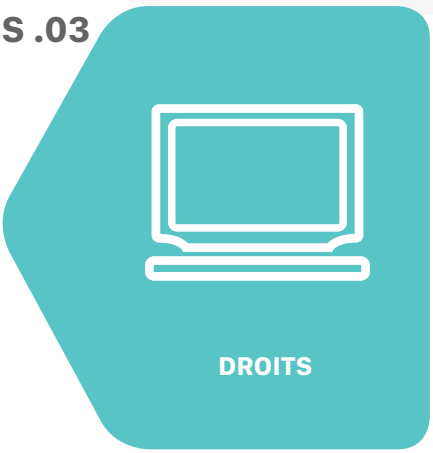
DESIGNATION DPO .02

Désigner un délégué à la protection des données (DPD ou DPO) dans tous les cas : les **établissements public** de santé sont tous concernés par cette obligation, tandis que les **établissements privés de santé** sont potentiellement concernés, selon qu'ils mettent ou non en œuvre un traitement de données sensibles « à grande échelle » (au dela de 250 patients/personnes). La mutualisation d'un DPD entre plusieurs établissements est possible.

Les fonctions suivantes sont susceptibles de donner lieu à un conflit d'intérêts : secrétaire général, directeur général des services, directeur général, directeur opérationnel, directeur financier, médecin-chef, responsable du département marketing, responsable des ressources humaines ou responsable du service informatique et/ou information, mais également d'autres rôles à un niveau inférieur de la structure organisationnelle si ces fonctions ou rôles supposent la détermination des finalités et des moyens du traitement.

ASSURER LE RESPECT DES DROITS DES PERSONNES .03

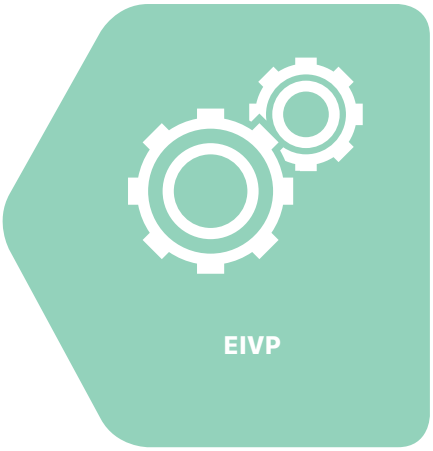
Le **RGPD renforce les droits traditionnels** des personnes concernées par un traitement (droit à l'information sur le traitement, droit d'accès, de rectification, de suppression, ou encore droit d'opposition pour motif légitime) qui sont spécifiquement adaptés au secteur de la santé par le code de santé publique. De nouveaux droits sont prévus, notamment le droit à la **portabilité** des données et le **droit à l'oubli**, qui nécessitent parfois des fonctionnalités spécifiques à prévoir dans les systèmes d'information de l'établissement .



ANALYSE D'IMPACT .04

Réaliser une **analyse de l'impact** du traitement de données portant tant sur les risques sécurités et techniques que sur les risques juridiques pour les personnes, avant de mettre en œuvre certains traitements, notamment ceux portant sur des données de santé à grande échelle.

EIVP (Etude d'Impact sur la Vie Privée)



Encadrement contractuel .05

Porter une attention particulière à l'encadrement contractuel des prestations des tiers fournisseurs de service :

- dès que l'établissement de santé a recours à un prestataire de service dont la prestation implique le traitement des données de santé, il doit **signer avec le prestataire un contrat** (ou, le cas échéant, passer un marché public) décrivant précisément le contenu des prestations (obligations de sécurité et respect des clauses obligatoires prévues par l'article 28 du règlement) ;

- dans le cas où l'établissement de santé n'est pas maître des moyens de travail mis à sa disposition (solutions de type progiciel ou Saas, fournies « telles quelles » par le prestataire), il doit **autant que possible inclure dans le contrat** avec son prestataire des clauses garantissant que celui-ci respecte les principes de la loi Informatique et Libertés.

Procédures sécurisation .06

Il faut mettre en place des **procédures permettant de garantir la sécurité et la confidentialité des données**, dans le respect de la politique générale de sécurité des systèmes d'information de santé (PGSSI-S), et de respecter les obligations liées à la conservation des données (fixer une durée de conservation, organiser les modalités d'archivage, assurer la capacité de restitution des données de santé) ;

Signaler auprès de la CNIL des incidents de sécurité impliquant des données personnelles (obligation qui s'ajoute à l'obligation actuelle de signalement des incidents de sécurité des systèmes d'information de santé prévue à l'article L.1111-8-2 du code de la santé publique).;

DPO EXTERNALISE

Votre projet est pris en main par un expert aguerri et désigné maitrisant les méthodologies et démarches de mise et de maintien en conformité RGPD. Une équipe compétente et des moyens mutualisés vous garantissent une qualité de service et de suivi de la mission.

Les avantages

- DPO en **formation continue et certifié CNIL**,
- Le DPO **ne figure pas dans vos effectifs RH**,
- **Continuité de service DPO**, un consultant DPO PARTAGE peut prendre le relais immédiatement,
- Assurance **Responsabilité Civile Professionnelle** du DPO incluse,
- Budget totalement **maitrisé**.

En tant que DPO désigné par votre structure, auprès de la CNIL, nous serons votre représentant après de la CNIL et l'interlocuteur privilégié pour toutes les demandes pouvant émaner de l'autorité.

Nous serons aussi votre référent CNIL et à ce titre nous réaliserons toutes les tâches et actions nécessaires et liées à notre désignation en tant que DPO.

Nous répondrons à toutes vos questions quant à l'utilisation des données personnelles qui sont à votre disposition.

Notre méthodologie :

- Revue Initiale / Audit,
- Désignation DPO,
- Mise en place du registre,
- Analyse des risques,
- Suivi mensuel et veille,
- Maintien de la conformité.

DPO PARTAGE 80 % de nos clients dans le secteur médical.

DPO signataires de la Charte de déontologie du DPO afin de promouvoir une culture de l'éthique parmi les DPO désignés auprès de la CNIL au titre du RGPD.

Prestations additionnelles

- Rédaction charte informatique,
- Rédaction procédures,
- Assistance label et certification,
- Intervention du DPO auprès des clients, donneurs d'ordres, membres CA,
- Mise en conformité site internet,
- Formation : information du personnel.

Nous vous proposons des formations en e-learning adaptées à votre structure pour chaque type de salariés avec des validations de compétences
- Formations/informations obligatoires.

Transparence

Chaque mois et après chaque intervention, nous vous informons des évolutions en matières de tâches et actions réalisées. Vous bénéficiez d'un tableau de suivi mis à jour après chaque mission.

Vous avez une maîtrise totale de vos coûts liés au RGPD. Il n'y a aucune suprise, nos tarifs incluent toutes les prestations pour une mise en conformité.

Votre DPO est disponible pour répondre à toutes vos questions, il est joignable du Lundi au Samedi de 9h à 19h.
Comme la CNIL, vous bénéficiez des coordonnées personnelles de votre DPO.

Informations :

Délégué à la protection des données

L'usage de la Marque DPO est réservé aux personnes physiques désignées en tant que DPO auprès de la CNIL.

Charte de déontologie du DPO Signataire

DPO PARTAGE METHODOLOGIE

Nous vous accompagnons dans la mise en conformité et le suivi de votre organisme :
- Missions de mise en conformité CNIL et Règlement Européen,
- Sensibilisation des collaborateurs,
- Réalisation d'un diagnostic RGPD de votre organisme dans son ensemble, par service ou par outil,
- Audit de votre organisme, d'un service ou d'un département,
- Désignation en tant que DPO Externe de votre organisme.

AUDIT DE SITUATION / REVUE INITALE

Audit de situation sur quelques jours dans l'ensemble des structures, avec la remise d'un état des lieux (cartographie) et grille d'analyse.

AUDIT FLASH

MISE EN PLACE REGISTRE DE TRAITEMENTS

Mise en place du registre de traitement et des éventuelles analyses d'impact, des processus de gestion de droit des personnes, adaptation du processus collecte de données.

REGISTRE TRAITEMENTS

ANALYSES DES RISQUES

Analyse des risques internes et externes en termes de sécurité, création des processus d'alerte, mise en place des modifications juridiques obligatoires.

Analyses des risques

Désignation en tant que DPO

Validation et documentation de la mise en conformité de la structure et du référentiel.

Désignation DPO